Link Selection for Secure Two-Hop Transmissions in Buffer-Aided Relay Wireless Networks

Ji He*, Yuanyu Zhang+, Yulong Shen* and Xiaohong Jiang+
*School of Computer Science and Technology, Xidian University, China
+School of Systems Information Science, Future University Hakodate, Japan
Email: jhe_1@stu.xidian.edu.cn, yy90zhang@gmail.com,
ylshen@mail.xidian.edu.cn, jiang@fun.ac.jp

***Abstract*—This paper investigates the link selection problem for a two-hop relay wireless network consisting of one source-destination pair, one decode-and-forward (DF) relay with infinite buffer and one external eavesdropper overhearing both the source-relay and relay-destination links. To ensure the security of both links, we design a new link selection scheme to assign the current time slot to the source-relay link, or the relay-destination link or no link based on the quality of both links as well as their relative quality. We then derive the closed-form expressions for both the secrecy throughput of the concerned network and the secrecy outage probability (SOP) of both links under the new link selection scheme. The optimal parameters of the proposed link selection scheme are further determined to maximize the secrecy throughput under the two SOP constraints. Finally, numerical results are provided to illustrate the impact of the SOP constraints on the optimal secrecy throughput.**

***Index Terms*—Two-hop relay wireless network, link selection, secrecy throughput optimization, secrecy outage probability.**

I. INTRODUCTION

The two-hop relay wireless networks, where each source packet can be transmitted directly or via a relay node to its destination, have become a basic building block for more sophisticated relaying networks. The broadcast nature of wireless medium makes communication over wireless channels susceptible to the eavesdropping attacks of unintended recipients (i.e., eavesdroppers). As a result, the security of two-hop relay networks remains one of the major challenges.

Traditionally, data is secured by applying cryptographic schemes in the upper layers of the network protocol stack. Although these cryptographic methods have shown their effectiveness in wired networks, the inherent difficulty of secret key distribution and management without centralized control may significantly limit their applications in decentralized wireless networks. This motivates the introduction of physical layer (PHY) security technology recently to provide security guarantee for wireless communications. PHY security exploits the inherent randomness of noise and wireless channels to provide the information-theoretic security, which has been regarded as the strongest form of security irrespective of the computing power of eavesdroppers. Since no secret keys are required, PHY security has been recognized as a highly promising approach to providing an everlasting security guarantee for wireless communications.

Recently, designing relaying schemes to improve the PHY security performances of two-hop wireless networks have received extensive attention [1-6], since these relaying schemes have been proved to be effective in increasing the secrecy capacity and reducing the secrecy outage probability (SOP), i.e., the probability that the instantaneous secrecy capacity is less than some threshold. These works can be roughly divided into two categories based on whether the relays are equipped with buffer or not. For the works considering relays without buffer, they mainly focus on selecting the best relay to help forward the source packet to its destination, like [1]-[3]. For the works considering relays with buffer, the goal of relaying schemes is to select the best link from multiple source-relay links and relay-destination links to conduct the transmission in current time slot. For example, the author in [4] proposed a max-ratio (MR) link selection scheme to maximize the instantaneous secrecy capacity of the selected link in a two-hop wireless network with one source, one destination, one eavesdropper and multiple relays. This scheme selects the link that can achieve the highest channel gain ratio, i.e., the ratio of the intended receiver channel gain to the eavesdropper channel gain. The best link selection problem in a two-hop wireless network with one source, multiple destinations, multiple eavesdroppers and multiple relays was considered in [5] based on the maximum likelihood (ML) link criterion, which has been shown to outperform the MR link selection scheme in [4] in terms of improving the secrecy rate. Notice that [4] and [5] analyzed either the SOP or the expected secrecy capacity of the selected link, whereas the end-to-end secrecy throughput which models the average number of bits that securely arrive at the destination per time slot remains largely unknown. One recent work has been reported to investigate the secrecy throughput of a two-hop wireless network with one source-destination pair, one relay with infinite buffer and one eavesdropper overhearing only the relay-destination link [6]. Actually, in real-life environment, the eavesdropper may be interested in both the source-relay link and relay-destination link in order to maximize the quality of intercepted signals, which represents a more hazardous eavesdropping scenario.

This paper considers the link selection problem for a two-hop wireless network with one source-destination pair, one relay with infinite buffer and one eavesdropper that can

978-1-4673-9803-9/15 $31.00 © 2015 IEEE
DOI 10.1109/NaNA.2016.44

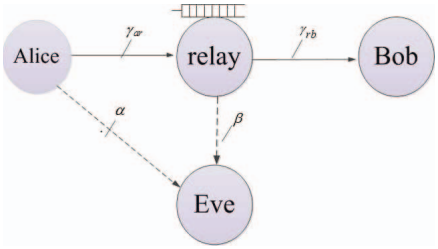

Fig. 1. System Model comprising a source (Alice), a half-duplex relay equipped with the infinite buffer, a destination (Bob) and an eavesdropper (Eve).

overhear both the source-relay and relay-destination links. In particular, to ensure the security of both links, we design a new link selection scheme to assign the current time slot to the source-relay link, or the relay-destination link or no link based on the quality of both links as well as their relative quality. We then derive the closed-form expressions for both the secrecy throughput and the SOP of both links under the new link selection scheme. The optimal parameters of the proposed link selection scheme are further determined to maximize the secrecy throughput under the two SOP constraints. Finally, numerical results are provided to illustrate the impact of the SOP constraints on the optimal secrecy throughput.

The remainder of this paper is organized as follows. Section II introduces the system model and section III presents the proposed link selection scheme. Section IV analyzes the SOP and secrecy throughput, and also solves the secrecy throughput optimization problem. Numerical results and the corresponding discussions are given in section V. Finally, section VI concludes this paper.

II. SYSTEM MODEL AND TRANSMISSION MODE

In this section, we present the system model and introduce the transmission model.

A. System Model

In this paper, we consider a two-hop relay network comprising one source node (Alice), one destination node (Bob), one DF relay and one external eavesdropper (Eve). The relay is equipped with an infinite buffer and Eve can intercept the messages from both Alice and the relay. All the nodes are under the half-duplex constraint, therefore the relay cannot transmit and receive simultaneously. Fig.1 schematically presents the system model.

In order to focus on the effect of link selection scheme on the secrecy throughput, we assume that direct link between Alice and Bob is not available due to path loss and shadowing effects, and they only can communicate via relay. In our model, a slow, fat, block Rayleigh fading environment is assumed, where the channel remain constant during one time slot, but change independently from one time slot to next. In the k-th time slot, we assume the complex channel gain for the link i-j is denoted as $h_{ij}(k)$, where $i, j \,\epsilon\, \{a, r, b, e\}$ represent any two of the four nodes (Alice, relay, Bob and Eve). We also assume the fixed transmit power for Alice and relay is denoted by p_a and p_r, respectively. Hence at time slot k, the instantaneous signal-to-noise-ratio (SNR) for each link can be written as $\gamma_{ar}(k) = p_a|h_{ar}(k)|^2/\delta_r^2$, $\gamma_{rb}(k) = p_r|h_{rb}(k)|^2/\delta_b^2$, $\gamma_{re}(k) = p_r|h_{re}(k)|^2/\delta_e^2$ and $\gamma_{ae}(k) = p_a|h_{ae}(k)|^2/\delta_e^2$ as labeled in Fig.1, where δ_r^2, δ_b^2 and δ_e^2 are the noise variances at the relay, Bob and Eve, respectively. Each link SNRs $\gamma_{ij}(k)$ is exponentially distributed with parameters $1/\overline{\gamma}_i$ with probability density function (i.e., p.d.f) given by

$$f_{ij}(k) = \frac{1}{\overline{\gamma}_i} e^{-\frac{x}{\overline{\gamma}_i}}, x \geq 0. \tag{1}$$

In this paper, we assume Alice and relay have perfect instantaneous CSI of relay and Bob respectively, but neither of them knows the instantaneous CSI of Eve. We assume the encoder will set a fixed value for the positive secrecy rate R_s, hence the secrecy outage event [7] may occur in the first hop and second hop.

The SOP will be analyzed in section IV and the mode of transmission is discussed in the following.

B. Transimission Mode

Based on above assumption, we consider adaptive transmission mode, i.e., Alice and relay adjust their transmission rates to close to their instantaneous capacities without causing transmission outage. We consider that relay works in three modes, i.e., receiving, forwarding and idle.

Relay receives: For a given time slot k, if Alice is selected to transmit, it will transmit with rate

$$S_{ar}(k) = \log_2 (1 + \gamma_{ar}(k)). \tag{2}$$

Then the relay appends the $S_{ar}(k)$ data bits received from Alice to the queue in its buffer. So at the end of k-th time slot, the data bits in the buffer are denoted as

$$Q(k) = Q(k-1) + S_{ar}(k), \tag{3}$$

where $Q(k-1)$ represents the maximal number of data bits that can be sent in the buffer queue of relay at the end of time slot $k-1$.

Relay forwards: If the relay is selected for transmission, the relay will transmit with the following rate

$$R_{rb}(k) = \min \{\log_2 (1 + \gamma_{rb}(k)), Q(k-1)\}. \tag{4}$$

Hence the remaining number of data bits in the buffer is given by

$$Q(k) = Q(k-1) - R_{rb}(k). \tag{5}$$

Relay is idle: In consider of security, the relay is allowed to stop working temporarily. If the relay does not work at time slot k, the transmission rates for Alice and relay are zero, i.e.,

$S_{ar}(k) = R_{rb}(k) = 0$, and the number of bits at time slot k equals to the one at time slot k-1, i.e., $Q(k) = Q(k-1)$.

III. LINK SELECTION CRITERION FOR ADAPTIVE TRANSMISIION RATE

In this section, we establish a link selection policy to ensure the transmission security further, and the transmission probability for Alice and relay are analyzed for the new link policy.

A. Link Selection Policy

In two-hop relay networks [8] [9] [10], the relay either receives the message from Alice or transmits the message to Bob during each time slot. But considering the two eavesdropper channels in our network, there will be such a situation that the Alice-relay and relay-Bob channels are worse than the eavesdropping channels, respectively. No matter which link is selected to transmit, the information security cannot be ensured. Based on the above considerations and assumptions, we establish the following link selection criterion:

$$I_{k\in\{1,\ldots,N\}} = \begin{cases} 1 & \gamma_{rb}(k) \geq \beta \quad and \quad \frac{\gamma_{rb}}{\beta} \geq \frac{\gamma_{ar}}{\alpha} \\ 0 & \gamma_{ar}(k) \geq \alpha \quad and \quad \frac{\gamma_{ar}}{\alpha} > \frac{\gamma_{rb}}{\beta} \\ -1 & otherwise, \end{cases} \tag{6}$$

where β and α are two non-negative decision thresholds for the link selection policy. $I_k = 1$ ($I_k = 0$) indicates the relay (Alice) transmits the data bits, and $I_k = -1$ indicates that the relay remains idle in the k-th time slot. The condition $\gamma_{rb}(k) \geq \beta$ ($\gamma_{ar}(k) \geq \alpha$) is used to ensure a higher quality of the link from relay to Bob (from Alice to relay) and provide good secrecy performance.

Based on the link selection policy (6), the transmission rate for Alice and relay can be generally written as

$$S_{ar}(k) = (1 - |I_k|)S(k) \tag{7}$$

$$R_{rb}(k) = \{|\frac{1}{2} + I_k| - \frac{1}{2}\}R(k), \tag{8}$$

respectively, where $S(k) = \log_2(1 + \gamma_{ar}(k))$ and $R(k) = \min\{\log_2(1 + \gamma_{rb}(k)), Q(k-1)\}$.

B. Transmission Probability

The probability that relay operates in receiving mode is denoted by P_r and given by

$$\begin{aligned} P_r &= \mathbb{P}[\gamma_{rb} \geq \beta, \frac{\gamma_{rb}}{\beta} \geq \frac{\gamma_{ar}}{\alpha}] \\ &= \mathbb{P}[\gamma_{rb} \geq \max\{\beta, \frac{\beta}{\alpha}\gamma_{ar}\}] \\ &= \mathbb{P}[\gamma_{rb} \geq \beta, \gamma_{ar} \leq \alpha] + \mathbb{P}[\gamma_{rb} \geq \frac{\beta}{\alpha}\gamma_{ar}, \gamma_{ar} \geq \alpha] \\ &= \mathbb{P}[\gamma_{rb} \geq \beta]P_r[\gamma_{ar} \leq \alpha] + \mathbb{P}[\gamma_{rb} \geq \frac{\beta}{\alpha}\gamma_{ar}, \gamma_{ar} \geq \alpha] \\ &= e^{-\frac{\beta}{\overline{\gamma}_b}} - \frac{\beta\overline{\gamma}_a}{\beta\overline{\gamma}_a + \alpha\overline{\gamma}_b} e^{-(\frac{\beta}{\overline{\gamma}_b} + \frac{\alpha}{\overline{\gamma}_a})}. \end{aligned} \tag{9}$$

By symmetry, the probability that relay operates in the forwarding mode for Alice P_f can be written by

$$\begin{aligned} P_f &= \mathbb{P}[\gamma_{ar} \geq \alpha, \frac{\gamma_{ar}}{\alpha} > \frac{\gamma_{rb}}{\beta}] \\ &= e^{-\frac{\alpha}{\overline{\gamma}_a}} - \frac{\alpha\overline{\gamma}_b}{\alpha\overline{\gamma}_b + \beta\overline{\gamma}_a} e^{-(\frac{\beta}{\overline{\gamma}_b} + \frac{\alpha}{\overline{\gamma}_a})}. \end{aligned} \tag{10}$$

So the probability that relay remains idle P_i is given as

$$\begin{aligned} P_i &= 1 - P_f - P_r \\ &= 1 - (e^{-\frac{\beta}{\overline{\gamma}_b}} + e^{-\frac{\alpha}{\overline{\gamma}_a}}) - e^{-(\frac{\beta}{\overline{\gamma}_b} + \frac{\alpha}{\overline{\gamma}_a})} \end{aligned} \tag{11}$$

IV. ESTABLISHMENT OF OPTIMAL PROBLEM

In this section, the corresponding secrecy throughput and secrecy transmission probability(SOP) are derived and secrecy throughput optimization problem is solved.

A. Secrecy Throughput

According to [11], the mean arrival rate R_{in} in the buffer queue of the relay as is

$$\begin{aligned} R_{in} &= \lim_{N\to\infty} \frac{1}{N} \sum_{k=1}^{N} S_{ar}(k) \\ &= \lim_{N\to\infty} \frac{1}{N} \sum_{k=1}^{N} (1 - |I_k|)S(k) \end{aligned} \tag{12}$$

And the mean departure rate R_{out} of data bits (i.e., the secrecy throughput T) is given by

$$\begin{aligned} R_{out} &= \lim_{N\to\infty} \frac{1}{N} \sum_{k=1}^{N} R_{rb}(k) \\ &= \lim_{N\to\infty} \frac{1}{N} \sum_{k=1}^{N} (|\frac{1}{2} + I_k| - \frac{1}{2})\min\{R_s, Q(k-1)\}. \end{aligned} \tag{13}$$

We note that $R_{in} \geq R_{out}$ is valid because of the buffer relay protocol and when $R_{in} > R_{out}$, the queue of the buffer is said to be unstable or in the absorbing state [8]. In our network system, we have the following lemma:

Lemma 1: when the secrecy throughput reached the maximum, the buffer queue is always at the edge of non-absorbing where

$$\begin{aligned} &\lim_{N\to\infty} \frac{1}{N} \sum_{k=1}^{N} (|\frac{1}{2} + I_k| - \frac{1}{2})\min\{R_s, Q(k-1)\} \\ &= \lim_{N\to\infty} \frac{1}{N} \sum_{k=1}^{N} (|\frac{1}{2} + I_k| - \frac{1}{2})R_s \end{aligned}$$

Proof: Because the lemma is an extension of theorem 1 and 2 [6] [9] in our network scene with the relay having three states, we just provide a brief proof. Let us denote the sets of indices k with $I_k \leq 0$ by M and $I_k = 1$ by $\overline{M}$. Because of the law of the conservation of flow, $R_{in} > R_{out}$ is valid.

The policy can be always improved by moving some of the indices k in M to $\overline{M}$ to increase the throughput until the queue is non-absorbing, i.e. $R_{in} = R_{out}$. Then if we move the indices further, both R_{in} and R_{out} will decrease. Thus the necessary condition which maximizes secrecy throughput is that the buffer queue is at the edge of non-absorbing. Under the optimal link policy, we have $R_{in} = R_{out} \leq \lim_{N\to\infty} \frac{1}{N}\sum_{k=1}^{N}(|\frac{1}{2}+I_k|-\frac{1}{2})R_s$. Since the transmission from absorbing to non-absorbing state is continuous, $R_{out} < \lim_{N\to\infty} \frac{1}{N}\sum_{k=1}^{N}(|\frac{1}{2}+I_k|-\frac{1}{2})R_s$ does not hold. Therefore the $R_{in} = R_{out} = \lim_{N\to\infty} \frac{1}{N}\sum_{k=1}^{N}(|\frac{1}{2}+I_k|-\frac{1}{2})R_s$ holds at the optimal point. Because R_s is a fixed scalar, the throughput is written as

$$T = \mathbb{E}\{(|\frac{1}{2}+I_k|-\frac{1}{2})R_s\} = P_r R_s \tag{14}$$

Based on new link selection criterion (6), the mean arrival rate (12) can be calculated as

$$\begin{aligned}
R_{in} &= \mathbb{E}\{(1-|I_k|)S_{ar}(k)\} \\
&= \int_{\alpha}^{+\infty}\int_{0}^{\beta} \frac{1}{\overline{\gamma}_b\,\overline{\gamma}_a} e^{-(\frac{y}{\overline{\gamma}_b}+\frac{x}{\overline{\gamma}_a})}\log_2(1+x)\,dy\,dx \\
&\quad + \int_{\beta}^{+\infty}\int_{\frac{\alpha}{\beta}\gamma_{rb}}^{+\infty} \frac{1}{\overline{\gamma}_b\,\overline{\gamma}_a} e^{-(\frac{y}{\overline{\gamma}_b}+\frac{x}{\overline{\gamma}_a})}\log_2(1+x)\,dx\,dy \\
&= \frac{1}{\ln 2} e^{\frac{1}{\overline{\gamma}_a}} E_1(\frac{\alpha+1}{\overline{\gamma}_a}) \\
&\quad - \frac{1}{\ln 2}\frac{\alpha\overline{\gamma}_b}{\alpha\overline{\gamma}_b+\beta\overline{\gamma}_b} e^{(\frac{1}{\overline{\gamma}_a}+\frac{\beta}{\alpha\overline{\gamma}_b})} E_1[(\frac{\beta}{\alpha\overline{\gamma}_b}+\frac{1}{\overline{\gamma}_a})(\alpha+1)] \\
&\quad + \log_2(1+\alpha)(e^{-\frac{\alpha}{\overline{\gamma}_a}} - \frac{\alpha\overline{\gamma}_b}{\alpha\overline{\gamma}_b+\beta\overline{\gamma}_a} e^{-(\frac{\beta}{\overline{\gamma}_b}+\frac{\alpha}{\overline{\gamma}_a})}),
\end{aligned} \tag{15}$$

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

B. Secrecy Outage Probability

The secrecy throughput represents the transmission efficiency for data, and the SOP is also an important security metric, because it indicates the likelihood of achieving a certain positive secrecy rate. More recently, a better expression for the SOP is given as $P_{sop} = \mathbb{P}\{C_e > R_b - R_s|\text{message transimission}\}$ in [12].

In the first hop, the transmission rate $S_{ar}(k)$ is adjusted to close to the capacity $C(k)$, so the SOP is written as

$$\begin{aligned}
P^a_{sop} &= \mathbb{P}[C_e > C_a - R_s|\gamma_{ar} \geq \max(\alpha, \frac{\alpha}{\beta}\gamma_{rb})] \\
&= \mathbb{P}[C_e > C_a - R_s, \gamma_{ar} \geq \max(\alpha, \frac{\alpha}{\beta}\gamma_{rb})]/P_f \\
&= \Big\{\mathbb{P}[\alpha \leq \gamma_{ar} < (2^{R_s}(1+\overline{\gamma}_e)-1), \gamma_{rb} \leq \beta] \\
&\quad + \mathbb{P}[\frac{\alpha}{\beta}\gamma_{rb} \leq \gamma_{ar} \leq (2^{R_s}(1+\gamma_e)-1), \gamma_{rb} \geq \beta]\Big\}/P_f \\
&= \Big\{e^{-(\frac{\alpha}{\overline{\gamma}_a}+\frac{\beta}{\overline{\gamma}_b}+\frac{\beta+1-2^{R_s}}{2^{R_s}\overline{\gamma}_e})} \frac{2^{R_s}\,\overline{\gamma}_e}{2^{R_s}\,\overline{\gamma}_e+\overline{\gamma}_a} \frac{1}{1+\alpha\overline{\gamma}_b+\frac{\alpha\,\overline{\gamma}_b}{\beta\,2^{R_s}\,\overline{\gamma}_e}} \\
&\quad +(1-e^{\frac{\beta}{\overline{\gamma}_b}})\frac{2^{R_s}\overline{\gamma}_e}{2^{R_s}\overline{\gamma}_e+\overline{\gamma}_a} e^{-(\frac{\alpha}{\overline{\gamma}_a}+\frac{\alpha+1-2^{R_s}}{2^{R_s}\overline{\gamma}_e})}\Big\}\frac{1}{P_f}.
\end{aligned} \tag{16}$$

In the second hop, the number $Q(k-1)$ of the data bits in the buffer queue should be considered. Hence the SOP can be given by

$$\begin{aligned}
P^r_{sop} &= \mathbb{P}[C_e > C_b - \min\{R_s, Q(k-1)\}|\gamma_{rb} \geq \max(\beta, \frac{\beta}{\alpha}\gamma_{ar})] \\
&\leq \mathbb{P}[C_e > C_b - R_s|\gamma_{rb} \geq \max(\beta, \frac{\beta}{\alpha}\gamma_{ar})] \\
&= \mathbb{P}[C_e > C_b - R_s, \gamma_{rb} \geq \max(\beta, \frac{\beta}{\alpha}\gamma_{ar})]/P_r \\
&= \{\mathbb{P}[\beta \leq \gamma_{rb} < (2^{R_s}(1+\overline{\gamma}_e)-1), \gamma_{ar} \leq \alpha] \\
&\quad + \mathbb{P}[\frac{\beta}{\beta}\gamma_{ar} \leq \gamma_{rb} \leq (2^{R_s}(1+\gamma_e)-1), \gamma_{ar} \geq \alpha]\}/P_r \\
&= \Big\{e^{-(\frac{\alpha}{\overline{\gamma}_a}+\frac{\beta}{\overline{\gamma}_b}+\frac{\beta+1-2^{R_s}}{2^{R_s}\overline{\gamma}_e})} \frac{2^{R_s}\,\overline{\gamma}_e}{2^{R_s}\,\overline{\gamma}_e+\overline{\gamma}_b} \frac{1}{1+\beta\overline{\gamma}_a+\frac{\beta\,\overline{\gamma}_a}{\alpha\,2^{R_s}\,\overline{\gamma}_e}} \\
&\quad +(1-e^{\frac{\alpha}{\overline{\gamma}_a}})\frac{2^{R_s}\overline{\gamma}_e}{2^{R_s}\overline{\gamma}_e+\overline{\gamma}_b} e^{-(\frac{\beta}{\overline{\gamma}_b}+\frac{\beta+1-2^{R_s}}{2^{R_s}\overline{\gamma}_e})}\Big\}\frac{1}{P_r}.
\end{aligned} \tag{17}$$

As mentioned above, when using the optimal link selection policy, the buffer queue is at the edge of non-absorption, and the probability of $R_s > Q(k)$ is negligible. Hence the upper bound for the SOP is tight.

C. Secrecy Throughput Optimization under SOP Constraints

In this section, we aim to establish the optimal problem that maximizes the secrecy throughput under SOP constraints. We first need to optimize the positive secrecy rate R_s and the desired transmission threshold α, β to make the link selection policy optimal. Then the secrecy throughput optimization under SOP constraints can be formulated as

$$\max_{R_s,\alpha,\beta} \quad P_r(\alpha,\beta)R_s \tag{18a}$$

$$s.t. P^a_{sop}(R_s,\alpha,\beta) \leq \nu \tag{18b}$$

$$P^r_{sop}(R_s,\alpha,\beta) \leq \mu \tag{18c}$$

$$P_i(\alpha,\beta) \leq \theta \tag{18d}$$

$$R_{in} = R_{out} \tag{18e}$$

$$R_s > 0, \alpha \geq 0, \beta \geq 2^{R_s}-1, \tag{18f}$$

where (18b) and (18c) are given in (16) and (17), respectively. The parameters ν, μ respectively represent the desired values for the SOP in the first and second hop. The (18d) means the probability that the relay neither receives nor transmits should be restricted appropriately, otherwise the secrecy throughput would be effected seriously. (18e) can be exactly obtained by (14) and (15). In (18f), the expression $\beta \geq 2^{R_s}-1$ always holds, because the encoding at the relay requires that $C_b = \log_2(1+\gamma_{rb}) \geq R_s$.

We notice that if the values for any two among R_S, α and β are known, the value for the other one can always be obtained by solving (18e). Hence the closed-form solution to the problem can be obtained by two dimension searching.

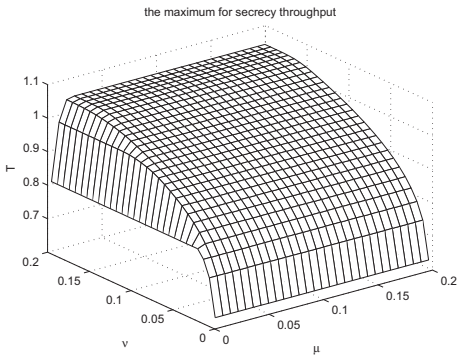

Fig. 2. the maximum for secrecy throughput T under the desired SOP ν in first hop and the desired SOP μ in second hop with $\overline{\gamma}_a = 5\,dB$, $\overline{\gamma}_b = 15\,dB$, $\overline{\gamma}_e = 0.5\,dB$

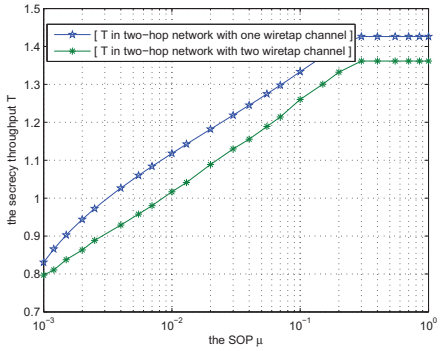

Fig. 3. the trade-off between the secrecy throughput T and the SOP in second hop in differnt network scene with $\overline{\gamma}_a = 5\,dB$, $\overline{\gamma}_b = 15\,dB$, $\overline{\gamma}_e = 0.5\,dB$.

V. NUMERICAL RESULTS AND DISCUSSION

In this section, we evaluate the performance for the new link selection in our network scene, and provide the exact numerical results that maximal secrecy throughput under SOP constraints.

The Fig.2 shows the exact value for the maximal secrecy throughput increases as the upper bound of the desired SOPs ν and μ increase based on the new link selection policy, which indicates that the average number of bits at the destination per time slot will increase when we simultaneously relax the requirement for security. In Fig.2, the trade-off can be observed clearly between the secrecy throughput T and the SOPs ν, μ. Further, we notice that the value of the secrecy throughput reaches the maximum, when the values for ν and μ close to 0.2 with assuming the average SNRs are $\overline{\gamma}_a = 5\,dB$, $\overline{\gamma}_b = 15\,dB, \overline{\gamma}_e = 0.2\,dB$.

The Fig.3 shows the trade-off between the secrecy throughput T and the SOP μ in second-hop in different two-hop relaying network. One is in the network scene with only one eavesdropping channel from relay to Bob [6], another is in our network system. For better comparability, we relax the constraint for the SOP ν in first-hop (i.e., $P^a_{sop} \leq 1$. Fig.3 indicates that the eavesdropping channel from Alice to Eve has an significant effect on the secrecy throughput in two-hop relay network.

VI. CONCLUSIONS

This paper has considered a two-hop relaying network where both the source and relay be wiretapped by a same eavesdropper. Unlike conventional link selection criterion that schedules transmission only through the strongest link, the proposed selection policy fully considers the flexibility of the relay equipped with buffer and the security. We assume the relay has three working states, so the relay will remain idle when the equality of the Alice-relay and relay-Bob channel is worse than the eavesdropping links. We derived the maximal value for the secrecy throughput under SOP constraints in first and second hop.

Interesting topics for future work include the minimum of the SOP under secrecy throughput and the relay with finite buffer in our two-hop relaying network.The new link selection also can be researched in more complex wireless network.

REFERENCES

[1] Zou Y, Wang X, Shen W, "Optimal Relay Selection for Physical-Layer Security in Cooperative Wireless Networks[J]," Selected Areas in Communications IEEE Journal on, 2013, 31(10):2099-2111.

[2] Krikidis I, "Opportunistic relay selection for cooperative networks with secrecy constraints[J]," Communications Iet, 2010, 4(15):1787-1791.

[3] Bao V N Q, Linh-Trung N, Debbah M, "Relay Selection Schemes for Dual-Hop Networks under Security Constraints with Multiple Eavesdroppers[J]," Wireless Communications IEEE Transactions on, 2013, 12(12):6076-6085.

[4] Chen G, Tian Z, Gong Y, et al, "Max-Ratio Relay Selection in Secure Buffer-Aided Cooperative Wireless Networks[J]," IEEE Transactions on Information Forensics Security, 2014, 9(4):719-729.

[5] Lu X, Lamare R C D, Lamare R C D, " Buffer-Aided Relay Selection for Physical-Layer Security in Wireless Networks[C]," WSA 2015; 19th International ITG Workshop on Smart Antennas; Proceedings of. VDE, 2015:1 - 5.

[6] Huang J, Swindlehurst A L, "Buffer-Aided Relaying for Two-Hop Secure Communication[J]," IEEE Transactions on Wireless Communications, 2015, 14(1):152-164.

[7] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2515C2534, Jun. 2008.

[8] N. Zlatanov, R. Schober, and P. Popovski, "Throughput and Diversity Gain of Buffer-Aided Relaying," IEEE Global Telecommunication Conference, pp. 1-6, Dec. 2011

[9] Nikola Zlatanov, Robert Schober, and Petar Popovski, "Buffer-Aided Relaying with Adaptive Link Selection", IEEE Journal on Selected Areas in Communications., vol. 31, no. 8, pp. 1530 C 1542, Aug. 2013.

[10] Bao VNQ, Linh-Trung N, Debbah M, "Relay Selection Schemes for Dual-Hop Networks under Security Constraints with Multiple Eavesdroppers[J]," Wireless Communications IEEE Transactions on, 2013, 12(12):6076-6085.

[11] Leonidas Georgiadis, Michael J. Neely and Leandros Tassiulas, Resource Allocation and Cross Layer Control in Wireless Networks, Now Publishers Inc, 2006.

[12] X. Zhou, M. R. McKay, B. Maham, and A. Hjorungnes, Rethinking the secrecy outage formulation: A secure transmission design perspective, IEEE Commun. Lett., vol. 15, no. 3, pp. 302C304, Mar. 2011.