Adaptive Resource Allocation for Secure Two-Hop Communication

Khoa T. Phan, Yi Hong, and Emanuele Viterbo
Department of Electrical and Computer Systems Engineering, Monash University, VIC, Australia
Email: {khoa.phan, yi.hong, emanuele.viterbo}@monash.edu

***Abstract*—This paper develops novel transmission schemes to support secure dual-hop Alice–Ray–Bob relaying communication in the presence of a passive eavesdropper (Eve). Due to unknown eavesdropper channel conditions, data transmissions from Alice (to Ray) and from Ray (to Bob) are required to satisfy the secrecy constraint in terms of maximum acceptable secrecy outage probability (SOP). The throughput maximization problem is studied for two scenarios: 1) fixed (Alice and Ray) power allocation; and 2) adaptive power allocation. The resulting constrained optimization problems are solved using the Lagrangian approach. In each frame, either Alice or Ray or neither can be scheduled for transmission depending on the instantaneous main channel conditions. Numerical results demonstrate the effectiveness of the proposed schemes over the existing schemes under various secrecy constraint and signal-to-noise power ratio (SNR) regimes.**

***Index Terms*—Dual-hop relaying, secrecy outage probability, adaptive link scheduling, throughput maximization.**

I. INTRODUCTION

Physical layer security is one of the promising techniques for wireless secure communications, which aims at exploiting physical layer properties of the communication systems, such as interference, noise, and wireless fading. The security measure is *secrecy capacity* that was introduced in [1], where a 3-node wiretap model Alice–Bob–Eve has been considered. Secrecy capacity characterizes the maximum transmission rate from the transmitter (Alice) to the receiver (Bob), below which the eavesdropper (Eve) is unable to obtain any information. Subsequent studies on secrecy capacity of a wiretap fading channel model have been provided in [2]. It is assumed that channel state information (CSI) of both main and eavesdropper channels is available at Alice to compute secrecy capacity and enable secure encoding. However, in many scenarios, the CSI of a passive Eve is very unlikely to be unveiled at Alice, and thus it is more realistic to assume that Alice knows the statistics of the eavesdropper channel only (in addition to the CSI of the main channel). Due to fading characteristics, a secrecy outage event is deemed to occur when the instantaneous capacity to Eve is larger than secrecy rate [3]– [6].

Consider the wiretap fading model Alice–Bob–Eve. Supporting secure communication can be challenging with a small secrecy outage probability (SOP) requirement, especially when the eavesdropper channel is moderately degraded (relative to the main channel). This motivates the potential deployment of a relay (Ray) and dual-hop relaying protocol to enhance secure communication between Alice and Bob, where Ray locates between Alice and Bob. With suitable Ray location, the main Alice–Ray and Ray–Bob channels can be stronger than the eavesdropper Alice–Eve and Ray–Eve channels due to shorter communication distances, thereby possibly reducing SOP and/or increasing secrecy rates. In addition, we can also improve security by exploiting the fading diversity of the main channels, where Alice or Ray can be adaptively scheduled to make a transmission depending upon instantaneous channel conditions. In such cases, Ray is required to buffer the received packets from Alice [7]. It is worth noting that jamming signals or artificial noise techniques etc. can also be employed to enhance security in dual-hop communications [8]– [11]. However, such techniques are out of the scope of our work.

Specifically, our work studies throughput–optimal adaptive link scheduling (ALS) problem for secure dual-hop Alice–Ray–Bob buffer-aided relaying communications. Due to unknown eavesdropper channel conditions, the secrecy constraint is imposed in terms of maximum allowable SOP to control the risk of secrecy outage. Different from [10], [12] etc. assuming that Eve monitors Ray–Bob transmission only, our work considers a more realistic scenario where Eve monitors both Alice–Ray and Ray–Bob transmissions [11]. Our main contributions are summarized below.

1) We formulate the throughput-optimal ALS problem and derive the optimal solution using Lagrangian approach, which takes into account both fading distributions and secrecy constraint. In each frame, either Alice or Ray can be scheduled for data transmission depending on instantaneous channel conditions. When the channel conditions are below certain thresholds, no transmission occurs in order to prevent secrecy outage. Further, we revisit the special case when Eve monitors Ray–Bob transmission only (see [12] with a sub-optimal ALS solution), and obtain an optimal solution.

2) The above study is extended by considering jointly ALS and power allocation for further throughput enhancement.

3) We numerically demonstrate that the throughput of our scheme outperforms other known schemes: 1) Fixed link scheduling (FLS); 2) Non-buffer relaying; 3) Direct Alice–Bob communication. Compared to direct transmission scheme, ALS is more advantageous when Ray is located at mid-way between Alice and Bob. The proposed ALS scheme outperforms both FLS and non-buffer relaying schemes. The ALS scheme with adaptive power allocation can provide significant capacity gains over fixed power allocation at low signal-to-noise power ratios (SNRs).

978-1-5386-1734-2/18/$31.00 ©2018 IEEE

II. Mathematical model

A. Transmission model

We consider a dual-hop decode-and-forward half-duplex relaying communication, where Alice (A) communicates with Bob (B) via an intermediate Ray (R) using the same frequency with bandwidth B (Hz). Ray can buffer the received data from Alice before forwarding them to Bob later. Moreover, there is a passive Eve (E) trying to eavesdrop the communication between Alice and Bob.

1) Channel model: We assume block-fading channels with fading block duration being equal to the transmission frame T (seconds), i.e., the channel power gains remain unchanged during a frame but vary independently from frame to frame. For notational simplicity, we normalize $TB = 1$ w.l.o.g. Let $h_A[t]$, $h_{AE}[t]$, $h_B[t]$, and $h_{RE}[t]$, denote the normalized channel power gains in frame t of the Alice–Ray (A–R), Alice–Eve (A–E), Ray–Bob (R–B), and Ray–Eve (R–E) channels, respectively. Moreover, $h_i[t], i \in \{A, AE, B, RE\}$ are assumed to be independent under some fading distributions (i.e., Rayleigh, Nakagami etc.) and means $\bar{h}_i$. Let us denote the probability distribution functions (pdf) and cumulative distribution functions (cdf) of the random channel power gains as $f_{h_i}(h_i)$, and $F_{h_i}(h_i), i \in \{A, AE, B, RE\}$.

Let P_A and P_R denote the transmit powers of Alice and Ray, respectively. Without loss of generality (w.l.o.g.), we assume $P_A = P_R = P$. Thus, $Ph_i[t], i \in \{A, AE, B, RE\}$ is the instantaneous link SNR in frame t. We assume that instantaneous link SNR is available at the corresponding link receiver. Furthermore, it is assumed that, in frame t, Alice knows $h_A[t]$ and Ray knows $h_B[t]$ to adaptively vary the secrecy rates. Furthermore, Alice and Ray do not know $h_{AE}[t]$, and $h_{RE}[t]$, respectively (e.g., passive Eve), although they are assumed to know the fading statistics (e.g., distributions) of $h_{AE}[t]$, and $h_{RE}[t]$ [3]– [6].

2) Adaptive link scheduling (ALS): Due to half-duplex constraint, at most one of Alice or Ray is allowed to transmit in each frame t. Let $\phi_A[t], \phi_B[t] \in \{0, 1\}$ denote binary (link scheduling) variables for frame t, where we set $\phi_A[t] = 1$ if Alice transmits (e.g., active A–R link) and otherwise, $\phi_A[t] = 0$. Similarly, $\phi_B[t] = 1$ if Ray transmits (e.g., active R–B link) and otherwise $\phi_B[t] = 0$. We require:

$$\phi_A[t] + \phi_B[t] \leq 1, \forall t.$$

Note that it is a possible scenario that none of Alice or Ray is transmitting in a frame.

If $\phi_A[t] = 1$, then Alice transmits data to Ray with secrecy rate $r_{AS}[t] > 0$ (b/s/Hz). We assume that Alice always has data to transmit. Since Alice does not know $h_{AE}[t]$, the following secrecy constraint is imposed [3], [4], [12]:

$$\text{Prob}\big(r_{AE}[t] > r_A[t] - r_{AS}[t]\big) \leq \zeta_{\text{sop}}, \tag{1}$$

where $\text{Prob}(A)$ denotes the probability of event A, $\zeta_{\text{sop}} \in (0, 1)$ is the maximum allowable SOP, and the rates are given by:

$$r_i[t] = \log_2(1 + Ph_i[t]), i \in \{A, AE\}.$$

Note that when (1) is satisfied, the risk of secrecy outage is under control, and Ray can decode the messages from Alice correctly since $r_{AS}[t] < r_A[t]$. On the other hand, if $\phi_B[t] = 1$, then Ray transmits its currently buffered data to Bob with secrecy rate $r_{RS}[t] > 0$ (b/s/Hz). Similarly, the following secrecy constraint is imposed:

$$\text{Prob}\big(r_{RE}[t] > r_B[t] - r_{RS}[t]\big) \leq \zeta_{\text{sop}}, \tag{2}$$

where the rates are given by:

$$r_i[t] = \log_2(1 + Ph_i[t]), i \in \{B, RE\}.$$

A smaller ζ_{sop} implies more stringent secrecy constraint.

3) SOP constraint manipulation: After some manipulations, the secrecy constraint (1) can be equivalently expressed as the following two conditions:

$$0 < r_{AS}[t] \leq r_A[t] - r_A^{\min}, \;\; r_A[t] > r_A^{\min} \tag{3}$$

where $r_A^{\min}$ can be derived from the cdf $F_{h_{AE}}(h_{AE})$ as:

$$r_A^{\min} = \log_2(1 + Ph_A^{\min}), \quad h_A^{\min} = F_{h_{AE}}^{-1}(1 - \zeta_{\text{sop}})$$

where $F_{h_{AE}}^{-1}$ is the inverse function of $F_{h_{AE}}$, i.e., $F_{h_{AE}}^{-1}(F_{h_{AE}}(h_{AE})) = h_{AE}$. Similarly, the secrecy constraint (2) can be written as:

$$0 < r_{RS}[t] \leq r_B[t] - r_B^{\min}, \;\; r_B[t] > r_B^{\min} \tag{4}$$

and

$$r_B^{\min} = \log_2(1 + Ph_B^{\min}), \quad h_B^{\min} = F_{h_{RE}}^{-1}(1 - \zeta_{\text{sop}}).$$

where $F_{h_{RE}}^{-1}$ is the inverse function of $F_{h_{RE}}$.

As an example, for Rayleigh fading eavesdropper channels, we have:

$$h_A^{\min} = -\bar{h}_{AE} \log(\zeta_{\text{sop}}), \quad h_B^{\min} = -\bar{h}_{RE} \log(\zeta_{\text{sop}}).$$

4) Throughput: Denote $Q[t] \geq 0$ as the queue length of the Ray buffer in frame $t = 1, 2, \ldots$. Then, the corresponding queue length (or queue state) evolution is given as:

$$Q[t+1] = Q[t] - \min\big\{Q[t], \phi_B[t] r_{RS}[t]\big\} + \phi_A[t] r_{AS}[t]. \tag{5}$$

The second term on the right side of (5) is indeed the actual data arriving at Bob in frame t (i.e, the throughput). The (secrecy) throughput is defined as:

$$\begin{aligned} \tau &= \lim_{\mathcal{T}\to\infty} \frac{1}{\mathcal{T}} \sum_{t=1}^{\mathcal{T}} \min\big\{Q[t], \phi_B[t] r_{RS}[t]\big\} \\ &= \mathbb{E}\big[\min\big\{Q[t], \phi_B[t] r_{RS}[t]\big\}\big], \end{aligned} \tag{6}$$

where $\mathbb{E}[.]$ denotes the statistical expectation operator.

Similarly, the average arrival rate to Ray buffer is:

$$\lambda = \mathbb{E}\big[\phi_A[t] r_{AS}[t]\big]. \tag{7}$$

Due to flow conservation rule, it holds true that: $\lambda \geq \tau$. The average service rate is also defined as:

$$\mu = \mathbb{E}\big[\phi_B[t] r_{RS}[t]\big]. \tag{8}$$

Remark 1: It is true that $\tau = \min\{\lambda, \mu\}$.

Remark 2: In order to maximize the throughput τ, we should maximize λ and μ. Hence, in frame t, when $\phi_A[t] = 1$ (or $\phi_B[t] = 1$), it is optimal for Alice (or Ray) to transmit with the largest possible secrecy rate $r_{AS}[t] = r_A[t] - r_A^{\min}$ (or $r_{RS}[t] = r_B[t] - r_B^{\min}$, respectively). Moreover, in frame

t, if either $r_A[t] > r_A^{\min}$ or $r_B[t] > r_B^{\min}$, then $\phi_A[t] = 1$ or $\phi_B[t] = 1$, respectively. Also, if both $r_A[t] > r_A^{\min}$ and $r_B[t] > r_B^{\min}$, whether Alice or Ray transmits depending on the optimal ALS scheme as we study in the following.

III. Optimal adaptive link scheduling

In this section, we will formulate the throughput-optimal ALS problem and present the optimal solution using Lagrangian approach for constrained optimization.

A. Problem formulation

The throughput-optimal ALS problem can be cast as:

$$\max_{\phi_A[t],\phi_B[t],\forall t} \quad \min\{\lambda, \mu\} \tag{9a}$$

$$\text{such that: } r_A[t] > \phi_A[t] r_A^{\min}, \forall t, \tag{9b}$$

$$r_B[t] > \phi_B[t] r_B^{\min}, \forall t, \tag{9c}$$

$$\phi_A[t] + \phi_B[t] \le 1, \phi_A[t], \phi_B[t] \in \{0,1\}, \forall t. \tag{9d}$$

B. Optimal solution

We first look at the largest and smallest arrival and service rates and respective transmission schemes.

Consider the following transmission scheme $(\phi_A^\dagger[t], \phi_B^\dagger[t])$:

$$(\phi_A^\dagger[t], \phi_B^\dagger[t]) = \begin{cases} (1,0), & r_A[t] > r_A^{\min}, \\ (0,1), & r_B[t] > r_B^{\min}, \ \texttt{and} \ r_A[t] \le r_A^{\min}, \\ (0,0), & \texttt{otherwise}. \end{cases}$$

Alice transmits whenever its main channel condition satisfies the SOP constraint. On the other hand, Ray transmits when its main channel condition satisfies the SOP constraint and Alice does not transmit. Such scheme leads to the largest arrival rate and smallest service rate:

$$\lambda^{\max} = \mathbb{E}[\phi_A^\dagger[t](r_A[t] - r_A^{\min})], \ \mu^{\min} = \mathbb{E}[\phi_B^\dagger[t](r_B[t] - r_B^{\min})].$$

Hence, if $\lambda^{\max} \le \mu^{\min}$, then $(\phi_A^\ddagger[t], \phi_B^\ddagger[t])$ is the solution of (9a)–(9d) with optimal throughput $\lambda^{\max}$.

Consider another scheme $(\phi_A^\ddagger[t], \phi_B^\ddagger[t])$ as follows:

$$(\phi_A^\ddagger[t], \phi_B^\ddagger[t]) = \begin{cases} (1,0), & r_A[t] > r_A^{\min}, \ \texttt{and} \ r_B[t] \le r_B^{\min}, \\ (0,1), & r_B[t] > r_B^{\min}, \\ (0,0), & \texttt{otherwise}. \end{cases}$$

The above scheme results in the smallest arrival and largest service rates:

$$\lambda^{\min} = \mathbb{E}[\phi_A^\ddagger[t](r_A[t] - r_A^{\min})], \ \mu^{\max} = \mathbb{E}[\phi_B^\ddagger[t](r_B[t] - r_B^{\min})].$$

Hence, if $\lambda^{\min} \ge \mu^{\max}$, then $(\phi_A^\ddagger[t], \phi_B^\ddagger[t])$ is the solution of (9a)–(9d) with optimal throughput $\mu^{\max}$.

If none of the above schemes are optimal, (i.e., $\lambda^{\max} > \mu^{\min}$ and $\lambda^{\min} < \mu^{\max}$), then the optimal solution $(\phi_A^*[t], \phi_B^*[t])$ of (9a)–(9d) should ensure equal arrival and service rates such that $\max\{\lambda^{\min}, \mu^{\min}\} < \tau^* = \lambda^* = \mu^* < \min\{\lambda^{\max}, \mu^{\max}\}$ [7]. Such rates can be obtained by allowing both Alice and Ray having chances to transmit when $r_A[t] > r_A^{\min}$ and $r_B[t] > r_B^{\min}$.

The scheme $(\phi_A^*[t], \phi_B^*[t])$ can be obtained by solving the reformulated problem of (9a)–(9d) assuming $\lambda = \mu$:

$$\max_{\phi_A[t],\phi_B[t],\forall t} \quad \mathbb{E}\big[(r_A[t] - r_A^{\min})\phi_A[t]\big] \tag{10a}$$

such that:

$$\mathbb{E}\big[(r_A[t] - r_A^{\min})\phi_A[t]\big] = \mathbb{E}\big[(r_B[t] - r_B^{\min})\phi_B[t]\big], \tag{10b}$$

$$\text{Constraints (9b)–(9d).} \tag{10c}$$

To solve (10a)–(10c), we employ the Lagrangian approach for constrained optimization. Specifically, by absorbing the rate equality constraint into the Lagrangian function, we come up with the following Lagrangian maximization problem:

$$\begin{aligned} \max_{\phi_A[t],\phi_B[t],\forall t} \quad & \mathbb{E}\big[(1-\xi)(r_A[t] - r_A^{\min})\phi_A[t] \\ & + \xi(r_B[t] - r_B^{\min})\phi_B[t]\big] \\ \text{such that:} \quad & \text{Constraints (9b)–(9d)} \end{aligned} \tag{11}$$

where ξ is the Lagrange multiplier associated with the rate constraint. Note that $\xi \in (0,1)$ to avoid trivial solutions, which are clearly not optimal.

Now if we can solve (11) for the optimal solution $\phi_A^*[t]$, and $\phi_B^*[t], \forall t$, and the multiplier ξ is determined so that the equality constraint is satisfied:

$$\mathbb{E}\big[\phi_A^*[t](r_A[t] - r_A^{\min})\big] = \mathbb{E}\big[\phi_B^*[t](r_B[t] - r_B^{\min})\big] \tag{12}$$

then, from the Lagrangian sufficiency theorem, $\phi_A^*[t]$, and $\phi_B^*[t], \forall t$ is also the optimal solution of (10a)–(10c).

Now, to solve (11), we can see that in order to maximize the expectation value under constraints in each frame, we have to maximize the term inside the expectation operator in each frame. Hence, the optimal solution $(\phi_A^*[t], \phi_B^*[t])$ in frame t of (11) is determined as:

$$\begin{aligned} \max_{\phi_A[t],\phi_B[t]} \quad & (1-\xi)(r_A[t] - r_A^{\min})\phi_A[t] + \xi(r_B[t] - r_B^{\min})\phi_B[t] \\ \text{such that:} \quad & r_A[t] > \phi_A[t] r_A^{\min}, \\ & r_B[t] > \phi_B[t] r_B^{\min}, \\ & \phi_A[t] + \phi_B[t] \le 1, \phi_A[t], \phi_B[t] \in \{0,1\}. \end{aligned} \tag{13}$$

The solution of (13) can be easily obtained using inspection as follows:

$$(\phi_A^*[t], \phi_B^*[t]) = \begin{cases} (1,0), & r_A[t] > \max\Big\{r_A^{\min}, \frac{\xi}{1-\xi}(r_B[t] - r_B^{\min}) + r_A^{\min}\Big\}, \\ (0,1), & r_B[t] > \max\Big\{r_B^{\min}, \frac{1-\xi}{\xi}(r_A[t] - r_A^{\min}) + r_B^{\min}\Big\}, \\ (0,0), & \texttt{otherwise}. \end{cases}$$

Then, ξ is determined such that (12) is satisfied. We then obtain the solution for (10a)–(10c).

Remark 3: On the existence and uniqueness of ξ. It can be seen that the left-hand and right-hand sides of (12) are decreasing, and increasing with increasing $\xi \in (0,1)$, respectively. Moreover, we have:

$$\lim_{\xi \to 0} \mathbb{E}\big[\phi_A^*[t](r_A[t] - r_A^{\min})\big] = \lambda^{\max},$$

$$\lim_{\xi \to 1} \mathbb{E}\big[\phi_A^*[t](r_A[t] - r_A^{\min})\big] = \lambda^{\min},$$

$$\lim_{\xi \to 0} \mathbb{E}\big[\phi_B^*[t](r_B[t] - r_B^{\min})\big] = \mu^{\min},$$

$$\lim_{\xi \to 1} \mathbb{E}\big[\phi_B^*[t](r_B[t] - r_B^{\min})\big] = \mu^{\max}.$$

Hence, under the assumption $\lambda^{\max} > \mu^{\min}$ and $\lambda^{\min} < \mu^{\max}$, there exists a unique ξ satisfying (12), which can be efficiently computed using a bi-section search algorithm. We omit the details due to space limitation.

C. Special case: Eve eavesdrops Ray's transmission only

Most existing works have assumed that Eve eavesdrops the transmission from Ray to Bob only, i.e., Eve is outside of the communication range of Alice [12] etc. In our model, this case can be modeled as $\bar{h}_{AE} = 0$, and hence, $h_A^{\min} = r_A^{\min} = 0$.

For simplicity, consider the case without maximum average power constraint as in [12]. Omitting the details, the optimal ALS scheme can be obtained as follows:

$$(\phi_A^*[t], \phi_B^*[t]) = \begin{cases} (0,1), & r_B[t] > \frac{1-\xi}{\xi} r_A[t] + r_B^{\min}, \\ (1,0), & \texttt{otherwise}. \end{cases}$$

The multiplier $\xi \in (0,1)$ is determined such that:

$$\mathbb{E}\big[\phi_A^*[t] r_A[t]\big] = \mathbb{E}\big[\phi_B^*[t](r_B[t] - r_B^{\min})\big].$$

In [12], it is assumed that when Ray transmits, he transmits with fixed rate r_{RS}. Hence, to ensure secrecy constraint satisfaction, we have $r_{RS} \in (0, r_B[t] - r_B^{\min}]$. Using the proposed approach, we can derive the optimal transmission scheme in this case as:

$$(\phi_A^*[t], \phi_B^*[t]) = \begin{cases} (0,1), & r_B[t] > r_{RS} + r_B^{\min}, \\ & \text{and } r_A[t] < \frac{\xi}{1-\xi} r_{RS}, \\ (1,0), & \texttt{otherwise}. \end{cases} \tag{14}$$

Also, the multiplier ξ is determined such that:

$$\mathbb{E}\big[\phi_A^*[t] r_A[t]\big] = \mathbb{E}\big[\phi_B^*[t] r_{RS}\big].$$

Note that (14) corrects the result derived in [12] which is claimed to be optimal.

IV. Joint Adaptive Link Scheduling and Power Allocation

A. Problem formulation

Previously, we have assumed fixed Alice and Ray transmit powers P. This section considers adaptive Alice and Ray power allocation to exploit the temporal fading diversity for further potential throughput enhancement. More specifically, in frame t, denote Alice and Ray transmit powers as $P_A[t]$ and $P_R[t]$, respectively. If $\phi_A[t] = 1$ then $P_A[t] > 0$ and $P_R[t] = 0$ while if $\phi_B[t] = 1$ then $P_A[t] = 0$ and $P_R[t] > 0$. Then, the average power is given by:

$$\mathbb{E}\big[\phi_A[t] P_A[t] + \phi_B[t] P_R[t]\big]. \tag{15}$$

Note that in order to have $\phi_A[t] = 1$ and $P_A[t] > 0$, a necessary condition is $h_A[t] > h_A^{\min}$. Then, the secrecy rate for Alice is given by:

$$r_{AS}[t] = \log_2(1 + P_A[t] h_A[t]) - \log_2(1 + P_A[t] h_A^{\min}). \tag{16}$$

Analogously, for $\phi_B[t] = 1$ and $P_R[t] > 0$, we have:

$$r_{RS}[t] = \log_2(1 + P_R[t] h_B[t]) - \log_2(1 + P_R[t] h_B^{\min}) \tag{17}$$

which is feasible for $h_B[t] > h_B^{\min}$ only.

The allocation problem can be cast as:

$$\max_{P_A[t], P_R[t], \phi_A[t], \phi_B[t], \forall t} \quad \mathbb{E}\big[\phi_A[t] r_{AS}[t]\big] \tag{18a}$$

such that:

$$\mathbb{E}\big[\phi_A[t] r_{AS}[t]\big] = \mathbb{E}\big[\phi_B[t] r_{RS}[t]\big], \tag{18b}$$

$$\mathbb{E}\big[\phi_A[t] P_A[t] + \phi_B[t] P_R[t]\big] \le P^{\max}, \tag{18c}$$

$$h_A[t] > \phi_A[t] h_A^{\min}, \forall t, \tag{18d}$$

$$h_B[t] > \phi_B[t] h_B^{\min}, \forall t, \tag{18e}$$

$$\phi_A[t] + \phi_B[t] \le 1, \forall t, \tag{18f}$$

$$P_A[t], P_R[t] \ge 0, \phi_A[t], \phi_B[t] \in \{0,1\}, \forall t \tag{18g}$$

where $P^{\max}$ is the maximum average power constraint.

B. Optimal solution

Similar to the fixed power allocation case, we use Lagrangian approach to solve (18a)–(18g). We have the following problem:

$$\begin{aligned} \max_{P_A[t], P_R[t], \phi_A[t], \phi_B[t], \forall t} \quad & \mathbb{E}\Big[(1-\omega)\phi_A[t] r_{AS}[t] \\ & + \omega \phi_B[t] r_{RS}[t] - \sigma\big(\phi_A[t] P_A[t] + \phi_B[t] P_R[t]\big)\Big] \\ \text{such that:} \quad & \text{Constraints (18d)–(18g)} \end{aligned} \tag{19}$$

where ω, and $\sigma > 0$ are the Lagrange multipliers associated with the equality constraint (18b) and inequality constraint (18c), respectively. Again, we can see that $\omega \in (0,1)$ to avoid trivial solutions.

To solve (19), we need maximize the term inside the expectation operator in each frame t as in the case of fixed power allocation, i.e.,

$$\begin{aligned} \max_{P_A[t], P_R[t], \phi_A[t], \phi_B[t], \forall t} \quad & (1-\omega)\phi_A[t] r_{AS}[t] \\ & + \omega \phi_B[t] r_{RS}[t] - \sigma\big(\phi_A[t] P_A[t] + \phi_B[t] P_R[t]\big) \\ \text{such that:} \quad & h_A[t] > \phi_A[t] h_A^{\min}, \\ & h_B[t] > \phi_B[t] h_B^{\min}, \\ & \phi_A[t] + \phi_B[t] \le 1, \\ & P_A[t], P_R[t] \ge 0, \phi_A[t], \phi_B[t] \in \{0,1\}. \end{aligned} \tag{20}$$

Before solving (20), first assume $h_A[t] > h_A^{\min}$ and consider $\phi_A[t] = 1$ and corresponding power allocation problem in frame t for Alice as follows:

$$\begin{aligned} \arg\max_{P_A[t] \ge 0} \; (1-\omega)\Big(& \log_2(1 + P_A[t] h_A[t]) \\ & - \log_2(1 + P_A[t] h_A^{\min})\Big) - \sigma P_A[t]. \end{aligned} \tag{21}$$

We can verify that (21) is a convex optimization problem due to the concavity of the objective function. We can derive the optimal power allocation for Alice as:

$$P_A^*[t] = \begin{cases} \frac{1}{2}\Bigg[\sqrt{\Big(\frac{1}{h_A^{\min}} - \frac{1}{h_A[t]}\Big)^2 + \frac{4(1-\omega)}{\sigma \log(2)}\Big(\frac{1}{h_A^{\min}} - \frac{1}{h_A[t]}\Big)} \\ \quad - \Big(\frac{1}{h_A^{\min}} + \frac{1}{h_A[t]}\Big)\Bigg], & h_A[t] - h_A^{\min} > \frac{\sigma \log(2)}{1-\omega} \\ 0, & \text{otherwise.} \end{cases} \tag{22}$$

The secrecy rate allocation for Alice is thus:

$$r_{AS}^*[t] = \log_2(1 + P_A^*[t]h_A[t]) - \log_2(1 + P_A^*[t]h_A^{\min}). \quad (23)$$

Next, assume $h_B[t] > h_B^{\min}$ and consider $\phi_B[t] = 1$, we derive the optimal power and secrecy rate allocation for Ray as follows:

$$P_R^*[t] = \begin{cases} \frac{1}{2}\left[\sqrt{\left(\frac{1}{h_B^{\min}} - \frac{1}{h_B[t]}\right)^2 + \frac{4\omega}{\sigma\log(2)}\left(\frac{1}{h_B^{\min}} - \frac{1}{h_B[t]}\right)} \right. \\ \quad \left. -\left(\frac{1}{h_B^{\min}} + \frac{1}{h_B[t]}\right)\right], & h_B[t] - h_B^{\min} > \frac{\sigma\log(2)}{\omega} \\ 0, & \text{otherwise} \end{cases} \quad (24)$$

and

$$r_{RS}^*[t] = \log_2(1 + P_R^*[t]h_B[t]) - \log_2(1 + P_R^*[t]h_B^{\min}). \quad (25)$$

Using the above derivations, we can obtain the optimal joint link scheduling and power allocation solution of (20) by considering the following scenarios:

Scenario 1: $h_A[t] \le h_A^{\min} + \frac{\sigma\log(2)}{1-\omega}$ and $h_B[t] \le h_B^{\min} + \frac{\sigma\log(2)}{\omega}$: $(\phi_A^*[t], \phi_B^*[t]) = (0, 0)$.

Scenario 2: $h_A[t] > h_A^{\min} + \frac{\sigma\log(2)}{1-\omega}$ and $h_B[t] \le h_B^{\min} + \frac{\sigma\log(2)}{\omega}$: $(\phi_A^*[t], \phi_B^*[t]) = (1, 0)$.

Scenario 3: $h_A[t] \le h_A^{\min} + \frac{\sigma\log(2)}{1-\omega}$ and $h_B[t] > h_B^{\min} + \frac{\sigma\log(2)}{\omega}$: $(\phi_A^*[t], \phi_B^*[t]) = (0, 1)$.

Scenario 4: $h_A[t] > h_A^{\min} + \frac{\sigma\log(2)}{1-\omega}$ and $h_B[t] > h_B^{\min} + \frac{\sigma\log(2)}{\omega}$.

The link scheduling solution is determined as:

$$(\phi_A^*[t], \phi_B^*[t]) = \begin{cases} (1, 0), & (1-\omega)r_{AS}^*[t] - \sigma P_A^*[t] \\ & \quad \ge \omega r_{RS}^*[t] - \sigma P_R^*[t] \\ (0, 1), & \text{otherwise}. \end{cases}$$

The multipliers $\omega > 0$ and $\sigma > 0$ satisfy:

$$\mathbb{E}\left[\phi_A^*[t]r_{AS}^*[t]\right] = \mathbb{E}\left[\phi_B^*[t]r_{RS}^*[t]\right]$$
$$\mathbb{E}\left[\phi_A^*[t]P_A^*[t] + \phi_B^*[t]P_R^*[t]\right] = P^{\max}.$$

V. Numerical results

A. System configurations

We consider Rayleigh fading channels and assume the distance from Alice to Bob is normalized to 1. Under dual-hop relaying, we assume Alice, Ray, and Bob are located on a straight line, where the Alice–Ray distance and Ray–Bob distance are $d_{R,x} \in (0, 1)$ and $1 - d_{R,x} \in (0, 1)$, respectively. In a 2-D plane, we can assume Alice, Ray, and Bob are located at points with coordinates $(0, 0)$, $(d_{R,x}, 0)$, and $(1, 0)$.

Denote the average channel power gain of the Alice–Bob link as $\bar{h}_{AB}$. We assume $\bar{h}_A = \bar{h}_{AB}/d_{R,x}^{\gamma}$, and $\bar{h}_B = \bar{h}_{AB}/(1 - d_{R,x})^{\gamma}$, where γ is the path-loss exponent. In the following, we set $\gamma = 2$.

We assume that Eve is located at point with coordinate $(d_{E,x}, d_{E,y})$. Hence, the distances between Alice and Eve and between Ray and Eve can be computed as $d_{AE} = (d_{E,x}^2 + d_{E,y}^2)^{1/2}$, and $d_{RE} = ((d_{E,x} - d_{R,x})^2 + d_{E,y}^2)^{1/2}$, respectively. Hence, we have $\bar{h}_{AE} = \bar{h}_{AB}/d_{AE}^{\gamma}$, and $\bar{h}_{RE} = \bar{h}_{AB}/d_{RE}^{\gamma}$. W.l.o.g., we normalize $\bar{h}_{AB} = 0$ dB.

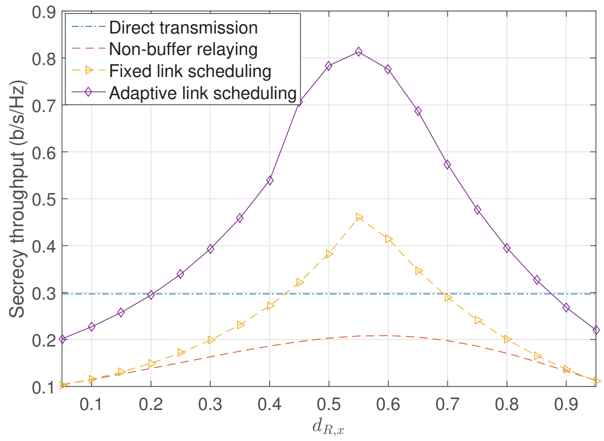


Fig. 1. Secrecy throughput versus Ray location $d_{R,x}$.

The performance of the proposed ALS schemes is compared with that of the benchmark schemes: buffer-aided relaying with fixed link scheduling (FLS), non-buffer relaying, and direct Alice–Bob transmission. For simulation instances, we ensure the same average power consumption $P^{\max}$ and end-to-end SOP $\zeta_{\text{sop}}^{\text{e2e}} = 1 - (1 - \zeta_{\text{sop}})^2$ for the transmission schemes.

B. Fixed power allocation

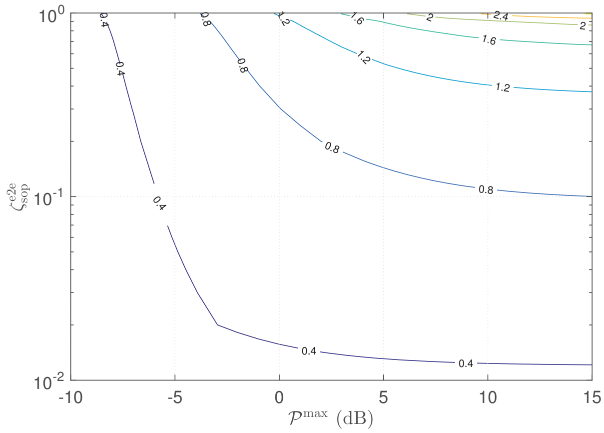
Let us fix Eve's location $d_{E,x} = d_{E,y} = 1.5\sqrt{2}/2$ (i.e., $d_{AE} = 1.5$). In this case, the eavesdropper Alice–Eve link is 3.52 dB less than the Alice–Bob link.

We first investigate the effects of Ray's location on the performance of the transmission schemes. Let $P^{\max} = 10$ dB and $\zeta_{\text{sop}}^{\text{e2e}} = 10^{-1}$. In Fig. 1, we plot the throughputs of the transmission schemes versus $d_{R,x} \in (0, 1)$. We can see that ALS scheme significantly outperforms FLS and non-buffer relaying schemes due to its capability to exploit the fading diversity. Moreover, it can be observed that Ray's location has profound effects on the performance of the relaying schemes. If Ray is deployed near Alice or Bob, ALS scheme performs worse than direct transmission, while when Ray is located near mid-way between Alice and Bob, ALS scheme is more efficient.

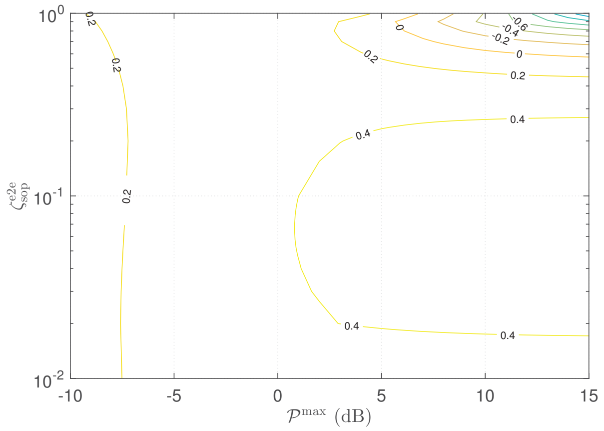
The above experiment shows that deploying Ray equidistant between Alice and Bob attains good throughput for relaying schemes. Hence, in the following, we assume $d_{R,x} = .5$. We next investigate the performance of ALS scheme under different $\zeta_{\text{sop}}^{\text{e2e}}$ and $P^{\max}$. Fig. 2 displays the contour throughput plots of ALS scheme and its potential throughput gains/losses over direct transmission. As the SNR increases and/or the secrecy constraint becomes less stringent, higher throughput can be achieved as expected. Also, ALS scheme outperforms direct transmission in most cases, except for sufficiently large SNR and loose secrecy constraint. This is consistent with the fact that relaying is beneficial at low SNRs.

C. Adaptive power allocation

We assume that $d_{AE} = d_{RE} = 1.5$, i.e., Eve is equidistant from Alice and Ray. Fix $\zeta_{\text{sop}}^{\text{e2e}} = 10^{-1}$. Fig. 3 plots the throughputs of ALS schemes with fixed and adaptive power



(a) Throughput of the ALS scheme



(b) Throughput difference between the ALS and direct transmission schemes

Fig. 2. Contour plots versus $(P^{\max}, \zeta_{\text{sop}}^{\text{e2e}})$.

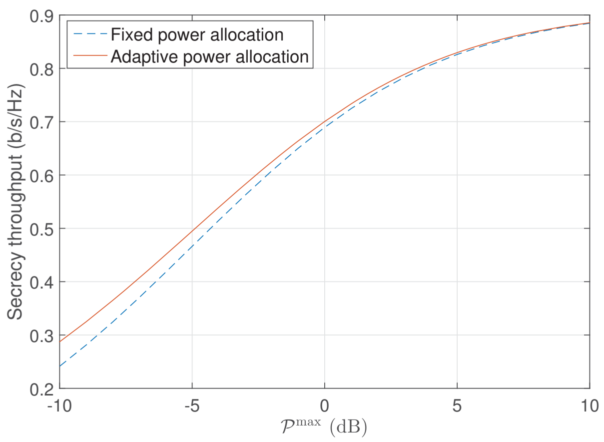


Fig. 3. Throughput versus $P^{\max}$.

allocation versus $P^{\max}$. We can observe that the gains due to adaptive power allocation are more noticeable at low SNRs than at high SNRs. Since the secrecy rate function is concave increasing with power, adaptive power allocation is more effective at low SNRs to vary the secrecy rates. At high SNRs, varying the power will not affect much the secrecy rates.

VI. Conclusions

We have explored the potential deployment of a relay (Ray) and studied corresponding transmission schemes in supporting secure Alice–Bob communication over fading channels. Toward practical secure communications, we assumed that only the statistics of the eavesdropper channels are available to the transmitters (in addition to CSI of the main channels). We have studied the adaptive link scheduling problem for throughput maximization for two scenarios: 1) fixed (Alice and Ray) power allocation; and 2) adaptive power allocation. The constrained optimization problems are solved using Lagrangian approach and convex optimization. Simulation results demonstrate the effectiveness of the developed transmission schemes over several benchmark schemes.

Acknowledgment

This work is supported by the Australian Research Council Discovery Project (ARC DP160100528).

References

[1] A.D. Wyner, "The Wire-tap Channel," *Bell System Tech. J.*, vol. 54, no. 8, pp. 1355–1387, October 1975.

[2] 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.

[3] 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. 302–304, Mar. 2011.

[4] X. Zhang, X. Zhou, and M. R. McKay, "On the Design of Artificial-Noise-Aided Secure Multi-Antenna Transmission in Slow Fading Channels," *IEEE Trans. Veh. Tech.*, vol. 62, no. 5, pp. 2170–2181, Jun. 2013.

[5] 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.

[6] S. Liu, Y. Hong, and E. Viterbo, "Practical Secrecy using Artificial Noise," *IEEE Commun. Lett.*, vol. 17, no. 7, pp. 1483–1486, July 2013.

[7] N. Zlatanov, R. Schober, and P. Popovski, "Buffer-Aided Relaying with Adaptive Link Selection," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 8, pp. 1530–1542, Aug. 2013.

[8] I. Krikidis, J. S. Thompson, and S. Mclaughlin, "Relay Selection for Secure Cooperative Networks with Jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5010, Oct. 2009.

[9] G. Chen, Z. Tian, Y. Gong, Z. Chen, J. A. Chambers, "Max-ratio Relay Selection in Secure Buffer-aided Cooperative Wireless Networks," *IEEE Trans. on Infor. Forensics and Security*, vol. 9, no. 4, pp. 719–729, April 2014

[10] Y. Zou, X. Wang, and W. Shen, "Optimal Relay Selection for Physical-Layer Security in Cooperative Wireless Networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.

[11] L. Fang, N. Yang, T. Q. Duong, M. Elkashlan, and G. K. Karagiannidis, "Exploiting Direct Links for Physical Layer Security in Multi-User Multi-Relay Networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 6, pp. 3856–3867, June 2016.

[12] J. Huang, and A. L. Swindlehurst, "Buffer-Aided Relaying for Two-Hop Secure Communication," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 152–164, Jan. 2015.

[13] B. Zhou, Y. Liu, and M. Tao, "Adaptive Scheduling for OFDM Bidirectional Transmission with A Buffered Relay," in *Proc. IEEE WCNC*, Shanghai, China, April 2013.