Secrecy outage analysis and power allocation for decode-and-forward relay systems

Mujun Qian†, Chen Liu†, Youhua Fu†
†National and Local Joint Engineering Laboratory of RF Integration and Micro-Assembly Technology, Nanjing University of Posts and Telecommunications, No. 9 Wenyuan Road, Qixia District, Nanjing, People’s Republic of China
✉ E-mail: liuch@njupt.edu.cn

Abstract: The decode-and-forward multi-relay system with the presence of an eavesdropper is researched in this study. Two widely used transmission schemes are considered, namely, the best-relay selection scheme and the all-relay-based beamforming scheme. To be specific, the former scheme adopts only the single best relay among all the candidate relays that have succeeded in decoding the source signal to assist the transmission, whereas the all-relay-based beamforming scheme allows all the candidates to assist the source simultaneously in a beamforming manner. The authors reveal that in both schemes, if the total transmit power of the two hops is constrained, contradiction exists between the two means of improving physical-layer security: (i) letting more relays succeed in decoding the source signal; (ii) increasing the transmit power of the selected relay(s). The authors thus analyse the secrecy outage behaviour of the two schemes and derive expressions of secrecy outage probability (SOP), based on which, the optimal power allocation solutions are obtained. It is demonstrated that in both schemes, the analysis results match well with the simulation results. Moreover, the proposed power allocation solutions surpass the conventional average power solution in SOP in both schemes.

1 Introduction

The broadcast nature of wireless medium makes wireless communications susceptible to wiretapping since malicious users can readily overhear messages that are being exchanged between legitimate users. As a result, enhancing system security in wireless communication networks has drawn a lot of attention in recent years. At present, cryptographic techniques are widely used in modern communication systems as the major approach to prevent interception [1, 2]. Secret keys are utilised to encrypt messages, without which, the malicious users cannot understand the message even if they have the message. However, with the rapid development of processors, it becomes easier and easier to crack keys even if the long ones. Therefore, the issue of wireless transmission security becomes more and more critical. It is by all means necessary to further enhance system security through physical-layer security (PLS) techniques, which exploit the characteristics of channels to fight against eavesdropping.

Research on PLS was pioneered by Wyner [3] who proved that safe communication without secret keys is possible if the eavesdropping channel (the channel from source to eavesdropper) is a degraded version of the main channel (the channel from source to legitimate destination). Secrecy capacity was developed as the difference between the capacities of the main channel and the eavesdropping channel [4]. Currently, it is a widely used measurement of PLS performance, which indicates the maximal communication rate that can be achieved safely. When secrecy capacity falls below a certain target secrecy rate, secrecy outage happens. The secrecy outage probability (SOP) is also a widely used measurement of PLS performance [5]. Note that the PLS technique can be utilised in various wireless communication systems along with many other techniques, such as the joint use of PLS and interference alignment [6, 7], and the joint use of PLS and energy harvesting [8]. Hence, the research of PLS has attracted a lot of attention in recent years.

As a matter of fact, the broadcast nature of wireless medium does not only bring the vulnerability to eavesdropping, it also brings the feasibility of user cooperation where ideal users are adopted as relays to form a virtual multiple-input–multiple-output system. It has been proved to be a promising technique to enlarge signal coverage and improve system capacity and reliability [9, 10]. Among all kinds of different relaying methods, amplify-and-forward (AF) and decode-and-forward (DF) are the two most popular protocols. In AF protocol, the relays simply forward a scaled version of the signals they received; while in DF protocol, the relays decode the source signal and forward the re-encoded signal.

Recently, user cooperation has also demonstrated its capability of combating eavesdropping [11]. A lot of efforts have been made in this area for better use of relays, such as relay selection [12] and cooperative beamforming [13–16]. In [12], a best-relay selection strategy was introduced in DF and AF relay networks, where only the single best relay that can achieve the maximal secrecy capacity was adopted to forward the source signal. Beamforming schemes for one-way and two-way relay networks with all available relays adopted were studied in [13, 14], respectively, subject to a total power constraint. A beamforming scheme with individual power constraints was proposed in [15]. Robust beamforming design with imperfect channel state information (CSI) was investigated in [16]. Cooperative jamming [17] is also an effective way to enhance PLS, which uses relays to send artificial noises to confuse eavesdroppers. However, for relay systems without direct link between source and destination, relays cannot all act as pure jammers, otherwise no message will be delivered to destination. Hence, cooperative jamming cannot be applied alone in this scenario. Actually, this technique is now usually applied along with relay selection and cooperative beamforming [18–20]. In addition to the various means of making better use of relays, the authors of [21] showed that in a cognitive radio network assisted by an AF relay, loosening the requirement of reliability can also improve the transmission security. As a matter of fact, security-reliability tradeoff is also a hot topic recently.

In this paper, we consider a cooperative communication system with multiple relays and an eavesdropper. To avoid noise propagation problem, the DF protocol is adopted. Two transmission schemes are considered, namely the best-relay selection (BRS) scheme and the all-relay-based beamforming (ARB) scheme. The first one selects the single best relay to forward the information bearing signal, while the second one uses multiple relays to forward the source signal in a beamforming
manner. These two schemes are classical and have been investigated in some other works, e.g., [12–15]. However, our work is still different from the previous ones. Most previous works concerning relay selection and multi-relay beamforming with DF protocol do not consider the source transmission rate, thus do not consider whether the relays can successfully decode the source signal. For example, in [12], the proposed relay selection method requires the source to adjust its transmission rate according to the channels of both hops to assure successful decoding at the selected relay and the destination. Similar source transmission rate adjustment is also required in [15]. While in [13], the authors assumed that all the relays can successfully decode. By contrast, in our work, it is taken into consideration that some of the source-to-relay (SR) channels may experience severe fading, so that their capacities may fall below the source transmission rate, which leads to decoding failure at these relays. We exploit only the relays that can successfully decode the source signal (called candidate relays) to avoid decoding error propagation. Clearly, the collection of candidate relays (called decoding set) in our work is a random variable depending on the SR channels, while in previous works, the collection of candidate relays is fixed to the collection of all relays in system.

Various works have verified that PLS performance will be improved if more relays can be utilised [12–14]. In the system we are considering, having more candidate relays is equivalent to higher transmit power in the first hop. However, if the total transmit power is constrained, it is also equivalent to lower transmit power in the second hop, which affects PLS performance as well. The first contribution of this paper is that we theoretically proved that in both BRS and ARB schemes, secrecy capacity monotonically increases with the transmit power in the second hop, which was only verified by simulation results in previous works [14, 20]. This means the aforementioned effect of lower transmit power in the second hop on PLS is negative. Hence, the consequence of considering the decoding set lies in the power allocation between the two hops. To achieve better PLS performance, the transmit powers need to be appropriately allocated. Motivated by this, we propose optimal power allocation solutions for both schemes. The objective is the SOP since secrecy capacity cannot reflect the influence of the transmit power in the first hop. Proposing the optimal power allocation solutions is the second contribution of this paper. As far as we know, no existing work has investigated this power allocation problem.

The remainder of this paper is organised as follows. Section 2 establishes the system model with two different transmission schemes. Section 3 carries out the security performance analysis of the two schemes, based on which, Section 4 proposes to allocate power between the two hops in order to minimise the SOP. Numerical results are presented in Section 5 which validate our theoretical analysis on SOP, and demonstrate the advantage of our proposed power allocation solutions by using the conventional average power allocation as a benchmark solution. Concluding remarks are provided in Section 6.

## 2 System model

Consider a DF relay system consisting of a source-destination pair, $M$ relays $\mathcal{R} = \{1, 2, \ldots, M\}$ and an eavesdropper as shown in Fig. 1. Each node is equipped with a single antenna working in half-duplex mode. Let $h_s \sim \mathcal{CN}(0, \sigma_s^2)$, $h_d \sim \mathcal{CN}(0, \sigma_d^2)$ and $h_e \sim \mathcal{CN}(0, \sigma_e^2)$ be the fading coefficients of the channels from the source to the $i$th relay, from the $i$th relay to the destination and from the $i$th relay to the eavesdropper, respectively. All the instantaneous CSIs are assumed to be available at the $M$ relays so that they can perform essential tasks like relay selection and beamforming. These CSIs can be obtained by using channel estimators surveyed in [22].

In the first hop, the source broadcasts $\sqrt{P_s}$ where $s$ is normalised as $E[|s|^2] = 1$ and $P_s$ is the transmit power of the source node. The received signal at the $i$th relay is expressed as

$$y_i = \sqrt{P_s}h_{si}s + n_i$$

where $n_i \sim \mathcal{CN}(0, \sigma_i^2)$ is the additive white Gaussian noise (AWGN). The capacity between the source and the $i$th relay is

$$C_i = \frac{1}{2}\log_2(1 + |y_i|\gamma_i)$$

Note that some of the relays may fail to decode the source signal if their channels experience deep fading or the transmit power of the source node is not high enough. Therefore, to avoid the forwarding of decoding error, only the relays that succeed in decoding are considered as candidate relays, the collection of which is defined as decoding set $\mathcal{D}$. Assume the source transmits with rate $R_s$. For the $i$th relay to successfully decode the source signal, the channel capacity in (2) should be no less than $R_s$, i.e.

$$y_i \geq P_s/\sigma_i^2$$

The event $\mathcal{D} = \mathcal{D}_m$ is equivalent to

$$C_{id} \geq R_s, \forall i \in \mathcal{D}_m$$

where $\mathcal{D}_m = \mathcal{R} - \mathcal{D}_m$ is the complementary set.

### 2.1 Best-relay selection

In the BRS scheme, if $\mathcal{D} = \emptyset$, the best candidate in $\mathcal{D}$ that can achieve the maximum secrecy capacity is selected to forward the desired signal in the second hop. Without loss of generality, assume $i \in \mathcal{D}$ is the one. Then the received signals at the destination and the eavesdropper are, respectively, expressed as

$$y_D = \sqrt{P_R}h_{id}s + n_D$$

and

$$y_E = \sqrt{P_R}h_{ie}s + n_E$$

where $P_R$ is the transmit power in the second hop, $n_D$ and $n_E$ are, respectively, the AWGNs at the destination and the eavesdropper, both following a $\mathcal{CN}(0, \sigma_i^2)$ distribution.

From (3) and (4), the secrecy capacity is

$$C_i^{BRS} = \left[\frac{1}{2}\log_2\left(1 + \frac{1 + \gamma_i}{1 + \gamma_E}\right)\right]$$

where $\gamma_i = P_R/\sigma_i^2(a^*) = \max\{a, 0\}$. Therefore, the best relay is

$$\text{BestRelay} = \arg\max_i \frac{1 + \gamma_i}{1 + \gamma_E}$$
and the secrecy capacity of this scheme is
\[
C_{s}^{\text{BRS}} = \left\{ \max_{\{i \in \mathcal{D}\}} \frac{1}{2} \log \left( \frac{1 + \sigma_{w} |h_{D|i}|^{2}}{1 + \gamma |h|^{2}} \right) \right\}.
\] (7)

2.2 All-relay-based beamforming
The BRS scheme is easy to implement. It does not require synchronisation between relays. However using only one relay to assist the transmission causes some loss in PLS performance. Hence, for the purpose of higher security, we also consider to adopt all candidate relays in \(\mathcal{D}\) and perform relay beamforming.

In the ARB scheme, all the relays in \(\mathcal{D}\) simultaneously forward the source signal in a beamforming manner in the second hop. Specifically, the transmit signal of the \(i\)th relay (if \(i \in \mathcal{D}\)) is
\[
t_{i} = \sqrt{P_{R}w_{i}}s
\] (8)
where \(w_{i}\) is the beamforming weight of the \(i\)th relay. If \(i \notin \mathcal{D}\), it remains silent in the second hop.

Let \(h_{RD}\) and \(h_{RE}\) denote the channels from the relays in \(\mathcal{D}\) to the destination and to the eavesdropper, respectively, and \(w\) denote the beamforming vector. For example, if \(\mathcal{D}\) = \{1, 3, 4, 6\}, \(h_{RD} = (h_{1d}, h_{3d}, h_{4d}, h_{6d})^{T}\), \(h_{RE} = (h_{1e}, h_{3e}, h_{4e}, h_{6e})^{T}\), and \(w = (w_{1}, w_{3}, w_{4}, w_{6})^{T}\). The respective received signals at the destination and the eavesdropper can be expressed as
\[
y_{D} = \sqrt{P_{R}w^{H}h_{RD}s} + n_{D}
\] (9)
and
\[
y_{E} = \sqrt{P_{R}w^{H}h_{RE}s} + n_{E}
\] (10)
where \(w^{H}w = 1\).

From (9) and (10), the secrecy capacity can be written as
\[
C_{s}^{\text{ARB}} = \frac{1}{2} \log \left( \frac{1 + \sigma_{w} |h_{D|i}|^{2}}{1 + \gamma |h_{D|i}|^{2}} \right).
\] (11)

Apparently, to maximise \(C_{s}^{\text{ARB}}\) requires to solve a generalised Rayleigh quotient problem, which can be transformed in to a Rayleigh quotient [23]. The optimal solution to \(w\) is
\[
w_{\text{opt}} = \arg \max_{w} \frac{1 + \sigma_{w} |h_{D|i}|^{2}}{1 + \gamma |h_{D|i}|^{2}} \left( |I + \sigma_{w} h_{D|i} h_{D|i}^{H} | \right)
\] (12)
where \(u_{\text{max}}(\cdot)\) represents the unit-norm eigenvector of a matrix corresponding to its largest eigenvalue. Thus, the secrecy capacity of this scheme is shown as
\[
C_{s}^{\text{ARB}} = \frac{1}{2} \log \left( \frac{1 + \sigma_{w} |h_{D|i}|^{2}}{1 + \gamma |h_{D|i}|^{2}} \right).
\] (13)

3 Security performance analysis
As can be noted, higher transmit power in the first hop leads to more relays in the decoding set. It has been verified by previous works that having more candidate relays enhances system security, no matter how many relays are selected to forward the desired signal. In other words, higher transmit power in the first hop yields better PLS performance.

However, if the total transmit power is constrained, the effect of higher transmit power in the first hop on PLS performance is twofold. On one hand, it allows more relays to succeed in decoding the source signal, which upgrades system security. On the other hand, it leads to lower transmit power in the second hop, which degrades system security (as will be proved in this section). Since the instantaneous secrecy capacities in (7) and (13) are based on a certain decoding set, they cannot reflect the effect of \(P_{s}\) on the overall PLS performance. Hence, SOP will be analysed in this section and used as the optimisation objective in the next section.

3.1 Best-relay selection
Using reduction to absurdity, it can be easily proved that for a certain \(\mathcal{D}\), if \(k \in \mathcal{D}\) is the best relay when \(P_{D} = P_{D}^{k}\), for any \(P_{D}^{k} > P_{D}^{k}\), it is still the best relay. Let \(C_{s}^{\text{BRS}}(P_{D}^{k})\) and \(C_{s}^{\text{BRS}}(P_{D}^{k})\) denote the secrecy capacities achieved by \(P_{D}^{k}\) and \(P_{D}^{k}\), respectively. It can be obtained that
\[
C_{s}^{\text{BRS}}(P_{D}^{k}) - C_{s}^{\text{BRS}}(P_{D}^{k}) = \left( \frac{1}{2} \log \left( \frac{1 + \sigma_{w}^{k} |h_{D|i}|^{2}}{1 + \gamma |h_{D|i}|^{2}} \right) \right) - \left( \frac{1}{2} \log \left( \frac{1 + \sigma_{w}^{k} + P_{D}^{k} |h_{D|i}|^{2}}{1 + \gamma |h_{D|i}|^{2}} \right) \right) \leq 0.
\] (14)

That is, for a certain \(\mathcal{D}\), \(C_{s}^{\text{BRS}}\) monotonically increases with \(P_{D}\).

As a result, if \(P_{D} + P_{s}\) is constrained, a tradeoff between more candidate relays and higher \(P_{D}\) is essential in improving PLS performance. Since the secrecy capacity of the BRS scheme cannot reflect the effect of \(P_{s}\), we now calculate the SOP of this scheme.

\[
P_{D}^{\text{opt}} = \text{Pr}(C_{s}^{\text{BRS}} < R_{D} | \mathcal{D} = \emptyset) \text{Pr}(\mathcal{D} = \emptyset)
\] (15)
\[
+ \sum_{m=1}^{M} \text{Pr}(C_{s}^{\text{BRS}} < R_{D} | \mathcal{D} = \mathcal{D}_{m}) \text{Pr}(\mathcal{D} = \mathcal{D}_{m})
\]

\[
\text{Pr}(C_{s}^{\text{BRS}} < R_{D} | \mathcal{D} = \emptyset) \text{Pr}(\mathcal{D} = \emptyset) = \text{Pr}(\mathcal{D} = \emptyset) = \prod_{i=1}^{M} \text{Pr}(b_{i} \geq \bar{P}_{s}) < \gamma_{i}
\] (16)

According to the law of total probability, the SOP of the BRS scheme is (see (15)). Since secrecy outage event definitely happens when \(\mathcal{D} = \emptyset\), we have (see (16)). Noting that \(X_{i} = |b_{i}|^{2}\) follows an exponential distribution with mean \(\sigma_{b,1}\), we derive the probability of an empty decoding set as
\[
\text{Pr}(\mathcal{D} = \emptyset) = \prod_{i=1}^{M} \left( 1 - \exp \left( - \frac{A_{i}}{\sigma_{b,1}} \right) \right) \]
\[
= \prod_{i=1}^{M} \left( \exp \left( \frac{A_{i}}{\sigma_{b,1}} \right) - 1 \right)
\] (17)
where \(A_{i} = (2^{\sigma_{b,1}} - 1)/\gamma_{i}\).

Similarly to \(\text{Pr}(\mathcal{D} = \emptyset)\), the probability of \(\mathcal{D} = \mathcal{D}_{m}\) can be obtained as
\[
\text{Pr}(\mathcal{D} = \mathcal{D}_{m}) = \prod_{i \in \Omega_{m}} \text{Pr}(b_{i} \geq A_{i}) \prod_{i \notin \Omega_{m}} \text{Pr}(b_{i} < A_{i})
\] (18)
\[
= \prod_{i \in \Omega_{m}} \exp \left( \frac{A_{i}}{\sigma_{b,1}} \right) \prod_{i \notin \Omega_{m}} \left( 1 - \exp \left( \frac{A_{i}}{\sigma_{b,1}} \right) \right)
\]
\[
= \prod_{i \in \Omega_{m}} \left( 1 - \frac{1}{\theta_{i}} \right)^{2^{\sigma_{b,1}} - 1} \exp \left( - \frac{A_{i}}{\sigma_{b,1}} \right)
\] (19)

One can also derive that (see (19)) where \(\theta_{i} = \sigma_{b,1}/\sigma_{b,1}\) is the main-to-eavesdropper ratio (MER) [24], \(A_{i} = (2^{\sigma_{b,1}} - 1)/\gamma_{i}\). The detailed calculation of (19) is given in Appendix 1. Substituting (17)–(19) into (15), we have the SOP of the BRS scheme as
The secrecy capacity in (13) equals to $C_{SOP}^{ARB} = (1/2) \log_2 \lambda_{max}(Z)^2$ where (see (21)) with $U A^{1/2} H^H$ being the eigenvalue decomposition (EVD) of $(I - \gamma \hat{h}_{RE} \hat{h}_{RE}^H (1 + \gamma || h_{RE} ||^2))^{1/2}$. Sherman-Morrison equation [25] is used to derive (21). By defining $x = \sqrt{\gamma} U A^{1/2} H^H Y$ and $y = \sqrt{(1/(1 + \gamma || h_{RE} ||^2))} \hat{h}_{RE}$, $\lambda_{max}(Z)$ is re-written as $\lambda_{max}(Z) = 1 + \max(2xH - yy^H)$.

**Lemma 1:** [26] Let $r$ and $s$ be two known non-zero vectors.

(i) If $r = \xi s$ for a certain scalar $\xi$, $r^H - sH$ has only one non-zero eigenvalue equal to $(\xi - 1) || s ||^2$ with the associated unit-norm eigenvector $s/ || s ||$.

(ii) If $r^H s = 0$, $r^H - sH$ has only two non-zero eigenvalues $\lambda_1 = || r ||^2 - c_1^2 || s ||^2 > 0$, $\lambda_2 = || r ||^2 - c_1^2 || s ||^2 < 0$,

with associated unit-norm eigenvectors

$u_1 = c_1^{-1/2} (r + c_1 e^{-j \phi} s)$,

$u_2 = c_1^{-1/2} (r + c_1 e^{j \phi} s)$.

where

$c_1 = || r ||^2 + c_1 || s ||^2 - 2 c_1 || s ||^2$,

$c_2 = || r ||^2 || s ||^2 - \sqrt{(|| r ||^2 + || s ||^2)^2 - 4 || s ||^4}$,

$c_3 = || r ||^2 + c_1 || s ||^2 - 2 c_1 || s ||^2$,

$c_4 = \sqrt{(|| r ||^2 + || s ||^2)^2 - 4 || s ||^4}$.

and $\phi = \angle(r^H s)$ is the angle of $r^H s$.

This lemma was given in [26] without proof. In [27], the derivation of eigenvalues in case (ii) was provided, but no derivation of the rest. In this paper, the complete proof of this lemma is given in Appendix 2.

Using Lemma 1, we obtain (see (26)) where $e = || h_{RE} ||^2$, $c = || h_{RE} ||^2$, $v = (c/e) - e$, $f(\gamma) = \gamma/((1 + \gamma|| h_{RE} ||^2)$, and $u = \sum_{i=1}^M \hat{h}_{RE}^H$ with $u_1, u_2, \ldots, u_M$ being the orthonormal bases of the null space of $h_{RE}$. It can be observed that $\lambda_{max}(Z)$ is a monotone increasing function in $\gamma$, thus also in $P_R$. As a consequence, when $P_S + P_R$ is constrained, enhancing PLS through increasing candidate relays and through increasing $P_R$ conflict with each other in the ARB scheme, as well as in the BRS scheme. Thus, it is also important to allocate the transmit powers appropriately in the ARB scheme.

$$
\lambda_{max}(Z) = 1 + \frac{1}{2} \left( f(\gamma) + u_f(1 + \gamma \gamma) + 2 u(1 + 2e)(1 + \gamma \gamma) \right)
$$

$$
P_{out}^{ARB} = \Pr\left(C_{SOP}^{ARB} < R_{i} \mid \mathcal{D} = \emptyset \right) \Pr(\mathcal{D} = \emptyset)
$$

$$
P_{out}^{BRS} = \prod_{i=1}^M \left[ 1 - \exp\left(-\frac{\lambda_1}{\sigma_{d1}} \right) \prod_{j=1}^M \left[ 1 - \exp\left(-\frac{\lambda_2}{\sigma_{d2}} \right) \right] \right]
$$

The SOP of the ARB scheme can be expressed as (see (27)). Substituting (13), (17) and (18) into (27), we have (see (28)).

The conditional probability $Pr[\lambda_{max}(Z) < 2^R_i \mid \mathcal{D} = \mathcal{D}_m]$ represents the probability of secrecy outage under a certain decoding set. To obtain the closed-form expression of it requires to know the cumulative distribution function (CDF) of $\lambda_{max}(Z)$, which is quite challenging. Consequently, it is difficult to derive the general closed-form expression of $P_{out}^{ARB}$. However, the numerical results of $Pr[\lambda_{max}(Z) < 2^R_i \mid \mathcal{D} = \mathcal{D}_m]$ can be utilised to obtain the overall SOP in (28).

**4 Optimal power allocation**

Section 3 revealed the fact that in both schemes, the power allocation between the two hops needs to be delicately handled. Hence, this section provides power allocation solutions to lower the SOP.

Assume the total transmit power is constrained by $P_S + P_R = P$. Let $P_S = aP$. Then $a$ is the power splitting ratio that is to be optimised. Apparently, $a$ should satisfy $0 < a < 1$.

**4.1 Best-relay selection**

To achieve the minimum SOP of the BRS scheme, the following optimisation problem needs to be solved:

$$
\min_a \quad P_{out}^{BRS}
$$

s.t. \quad 0 < a < 1.

Obviously, it is hard to obtain the optimal power allocation solution from the expression of $P_{out}^{BRS}$ in (20). We need to simplify the expression first.

Let $\Lambda = \sigma_{d2}^2 (2^R - 1)/P$; then $\Lambda = \Lambda_1/\alpha$, $\Lambda = \Lambda_1/(1 - \alpha)$. Define the following functions

$$
f(\alpha) = \exp\left(-\frac{\Lambda}{\sigma_{d1}^2} \right)
$$

$$\tilde{f}(\alpha) = 1 - f(\alpha).
$$

$$g(\alpha) = \exp\left(-\frac{\Lambda}{\sigma_{d2}^2(1 - \alpha)} \right)
$$

$$\tilde{g}(\alpha) = 1 - \frac{1}{\sigma_{d2}^2(1 - \alpha) + 1} g(\alpha).
$$

The SOP in (20) is now re-written as
\[P_{\text{out,flow}} = \lim_{\eta \to \infty} \lim_{P_{S} \to \infty} P_{\text{out}}^{\text{BRS}} = \frac{2^{\frac{\eta R}{2}}}{2^{\frac{\eta R}{2}} + \theta} \]

which is referred to as the SOP floor. This floor indicates that the SOP of BRS scheme has an unbreakable lower bound no matter how high powers the source and the selected relay transmit with. It is the best secrecy outage performance that a relay system with a BRS scheme can achieve. This SOP floor can be found in the simulation results in [20], but the authors of [20] did not provide any theoretical analysis.

Remark 2: The location of the eavesdropper only affects the value of the MER, i.e. \( \theta \). It can be observed from (32) that \( \theta \) has no influence on the optimum of \( \alpha \) which is determined by the term \( 1/(\sigma_{e}^2(1 - \alpha^2)) - 1/(\sigma_{e}^2\alpha) \). However, \( \theta \) do have influence on the value of \( dP_{\text{out}}^{\text{BRS}}/d\alpha \), which is the decreasing or increasing speed of \( P_{\text{out}}^{\text{BRS}} \) over \( \alpha \). More specifically, larger the RE distance is, the faster the SOP drops before \( \alpha \) reaches its optimum, and the slower the SOP raises after the optimum.

4.2 All-relay-based beamforming

To achieve the minimum SOP of the ARB scheme requires to solve the following optimisation problem:

\[
\begin{align*}
\min_{\alpha} & \quad P_{\text{out}}^{\text{ARB}} \\
\text{s.t.} & \quad 0 < \alpha < 1
\end{align*}
\]

Since the closed-form expression of \( P_{\text{out}}^{\text{ARB}} \) cannot be derived, the optimal power splitting ratio cannot be derived either. However, if \( \alpha = 0 \) or 1, \( P_{\text{out}}^{\text{ARB}} = 1 \); if \( \alpha \) is a little greater than 0 or lesser than 1, \( P_{\text{out}}^{\text{ARB}} \) will be lesser than 1. Hence, we surmise that \( dP_{\text{out}}^{\text{ARB}}/d\alpha \) might be an anti-unimodal function in \( \alpha \). In fact, this surmise can be verified by simulation results, which will be shown in the following section.

The ternary search method is utilised in this paper to find the optimal power splitting ratio in the ARB scheme. Since each time of ternary search eliminates at least 1/3 of the search area and 

\[
(2/3)^n \]

is already smaller than 0.001, it takes at most 18 times of search to find the optimum of \( \alpha \) if the accuracy of it is set to 0.001.

5 Simulation results

This section verifies the accuracy of our SOP analysis and the effectiveness of the proposed power allocation. Assume \( \sigma_{d} = d_{\text{SR}} \), \( \sigma_{d} = d_{\text{RD}} \), \( \sigma_{e} = d_{\text{RE}} \), where \( d_{\text{SR}}, d_{\text{RD}} \) and \( d_{\text{RE}} \) denote the distances from the source to the relays, from the relays to the destination and from the relays to the eavesdropper, respectively, and \( \eta = 4 \) is the path loss exponent. All AWGNs follow a \( \chi^2(0, 1) \) distribution.

5.1 Simulation results of the BRS scheme

We first compare the analysis results with the Monte–Carlo simulation results to validate the SOP analysis of the BRS scheme. We consider two cases of the eavesdropper’s location, i.e. two different values of the MER. From Fig. 2, it can be observed that for both cases, the analysis results match well with the simulation results, and as has been pointed out in the previous section, the SOP tends to a constant when the transmit powers tend to infinity. Moreover, the SOP floor in (34) equals 0.0016 when \( \theta = 16 \), this value also tallies with the simulation results in the case of \( d_{\text{RD}} = 2d_{\text{RD}} \).

Fig. 3 illustrates the relationship between the SOP of the BRS scheme and the power splitting ratio \( \alpha = P_{S}/P \). Comparing the two curves corresponding to \( d_{\text{RD}} = 1 \), we can see that the SOP obtains its minimum value at the same power splitting ratio due to the unchanged \( d_{\text{RD}}/d_{\text{SR}} \), regardless of the MER. However, the MER affects the slope of the curves, as has been mentioned in
does not have a closed-form expression, we obtain its value by Monte–Carlo simulations and substitute the value into (28) to get the analysis results in Fig. 5. The simulation results in Fig. 8 and Fig. 9 demonstrate a correspondence to the inherent relationship between the optimum of \( \alpha \) and the distances between the nodes. The simulation results are shown in Figs. 6 and 7. It can be seen that in ARB scheme, the optimum of \( \alpha \) changes with the location of the destination, but does not change with the MER, which means the eavesdropper’s location has nothing to do with the optimal power allocation, just as in the BRS scheme. As a matter of fact, when \( \alpha \) is small, there exists a certain value of \( \alpha \) which makes the advantage and the disadvantage of the fourth case cancel out. That is, the system in the fourth case could have the same performance as in the first case when a certain power allocation scheme is applied.

Fig. 3 SOP versus power splitting ratio in the BRS scheme. \( M = 4, P = 20 \text{ dB}, d_{SR} = 1 \text{ m}, R_s = 1 \text{ bps/Hz} \)

Remark 2. Moreover, according to (33), when \( d_{SR} = d_{RD} = 1 \text{ m} \), the optimal value for \( \alpha \) is 0.5, and when \( d_{SR} = 1 \text{ m} \) and \( d_{RD} = 2 \text{ m} \), the optimal value is 0.2. These values also match with the simulation results in Fig. 3, which verifies the correctness of our derivation.

It can be noted from Fig. 3 that the two curves corresponding to the first case \( (d_{RD} = 1 \text{ m}, d_{RE} = d_{RD}) \) and the fourth case \( (d_{RD} = 2 \text{ m}, d_{RE} = 2d_{RD}) \) have an intersection point. Compared with the system in the first case, the system in the fourth enjoys the advantage of larger MER, but suffers from the disadvantage of larger RD distance. For a certain \( \alpha \), if it is small, the transmit power of the relays is high, then the advantage of larger MER overcomes the disadvantage of larger RD distance. In other words, although the capacity of the legitimate link in the fourth case is smaller than that in the first case, \( C_s \) in the fourth case could still be larger than that in the first case, given enough high \( P_R \). Meanwhile, if \( \alpha \) is large, only few power is allocated to the relays, then the advantage of larger MER cannot be fully exploited and the disadvantage of larger RD distance overwhelms. This yields smaller \( C_s \), and thus higher SOP. Therefore, it is reasonable that there exists a certain value of \( \alpha \) which makes the advantage and the disadvantage of the fourth case cancel out. That is, the system in the fourth case could have the same performance as in the first case when a certain power allocation scheme is applied.

Fig. 4 provides the comparison of the optimal power allocation solution with the widely used average power allocation where \( P_s = P_R = P/2 \). One can observe that optimal power allocation outperforms average power allocation in BRS scheme. Meanwhile, as \( P \to \infty \), the SOPs of both power allocation solutions converge to the same SOP floor. As a matter of fact, when \( P = \infty \), the transmit powers of both hops will be very high, no matter which power allocation solution is applied. In that case, for both power allocation solutions, secrecy outage happens when \( \max_{\mathcal{D}_M} |h_{ds}f(h_{ds})| < 2^{\frac{P}{2}} \), the probability of which can be proved to be equal to the one in (34) after some simple calculation of the CDF of \( |h_{ds}|/|h_{ds}| \).

5.2 Simulation results of the ARB scheme

Let us first compare the analysis results of SOP in the ARB scheme with the simulation results. Since the conditional probability \( \Pr[\alpha = \alpha |Z] < 2^{\frac{P}{2}} | \mathcal{D} = \mathcal{D}_M \] does not have a closed-form expression, we obtain its value by Monte–Carlo simulations and substitute the value into (28) to get the analysis results in Fig. 5. While the simulation results in Fig. 5 are obtained purely by Monte–Carlo simulations and each data point was averaged over 1,000,000 independent channel realisations.

From Fig. 5, one can observe that the simulation results of the ARB scheme also match well with the simulation results. Although the SOP is too complicated to do asymptotic analysis on, the simulation results show that there does not exist a SOP floor, thus increasing the transmit powers can always improve PLS in the ARB scheme.

In the BRS scheme, the optimum of \( \alpha \) is determined by the SR and RD distances, and is irrelevant with the RE distance. However, in the ARB scheme, it is difficult to draw similar conclusions through theoretical analysis. Hence, we use simulations to reveal the inherent relationship between the optimum of \( \alpha \) and the distances between the nodes. The simulation results are shown in Figs. 6 and 7. It can be seen that in ARB scheme, the optimum of \( \alpha \) changes with the location of the destination, but does not change with the MER, which means the eavesdropper’s location has nothing to do with the optimal power allocation, just as in the BRS scheme. As a matter of fact, the optimum of \( \alpha \) in the BRS scheme is irrelevant with the number of relays, \( M \), either, which can be noted from (33). However we cannot obtain the relevance or irrelevance between them in the ARB scheme through theoretical analysis yet. However, the simulation results in Fig. 8 and Fig. 9 demonstrate a correspondence. It can be seen that in the case of \( d_{RD} = 1 \text{ m} \), the minimum of SOP appears at \( \alpha = 0.6 \) when \( M = 4 \), but when \( M = 10 \), it appears at \( \alpha = 0.65 \); whereas in the case of \( d_{RD} = 2 \text{ m} \), these two minima appear at 0.3 when \( M = 4 \) and 0.4 when \( M = 10 \). This implies that as the number of relays increases, more power should
be allocated to the first hop to allow more relays succeed in decoding the source signal and participate in the second hop of transmission in the ARB scheme.

The comparison between the optimal power allocation and the conventional average power allocation in the ARB scheme is given in Fig. 10. The power splitting ratio is obtained by utilising the ternary search method and the accuracy is set to 0.05. As shown in this figure, the SOP achieved by the proposed optimal power allocation solution is lesser over the whole power range, thus validates the effectiveness of the proposed power allocation solution.

6 Conclusion

This paper studied the secrecy outage behaviour of a DF relay system in the presence of an eavesdropper. Two widely used transmission schemes are considered, namely, the best-relay selection scheme and the all-relay-based beamforming scheme. We revealed that in both schemes, enhancing PLS through allowing more relays to succeed in decoding the source signal and through increasing the transmit power of relays conflict with each other. Hence, the SOP minimisation problem was addressed subject to a total transmit power constraint of the two hops. For the BRS scheme, we obtained the closed-form expressions of the SOP and the optimal power splitting ratio. Whilst for the ARB scheme, a general closed-form expression of SOP is difficult to derive, so we draw help from numerical results of the probability of secrecy outage under a certain decoding set to obtain the overall SOP of the ARB scheme, and utilised the ternary search to find the optimal power splitting ratio. Simulation results showed that the theoretical
analysis of SOP in both schemes matches well with the simulation results, and the proposed power allocation solutions outperform the conventional average power allocation.

7 Acknowledgments

This work was supported by the Natural Science Foundation of China under grants nos. 61372126 and 61302101 and by the Natural Science Foundation of Jiangsu Province of China under grants no. BK20130874.

8 References

[1] Menezes, A., Van, O., Vanstone, S.: ‘Handbook of applied cryptography’ (CRC Press, Boca Raton, 1996)
[2] Kartalopoulos, S.: ‘A primer on cryptography in communications’, IEEE Commun. Mag., 2003, 41, (11), pp. 146–151
[3] Wyner, A.: ‘The wiretap channel’, Bell Syst. Tech. J., 1975, 54, (8), pp. 1355–1387
[4] Gopala, P., Lai, L., Gamal, H.: ‘On the secrecy capacity of fading channels’, IEEE Trans. Inf. Theory, 2008, 54, (10), pp. 4687–4698
[5] Bloch, M., Barron, J., Rodrigues, R., et al.: ‘Wireless information-theoretic security’, IEEE Trans. Inf. Theory, 2008, 54, (6), pp. 2515–2534
[6] Zhao, N., Yu, F., Li, M., et al.: ‘Privacy issues in interference-alignment-based wireless networks’, IEEE Commun. Mag., 2016, 54, (8), pp. 162–168
[7] Zhao, N., Yu, F., Sun, H., et al.: ‘Adaptive power allocation schemes for spectrum sharing in interference-alignment-based cognitive radio networks’, IEEE Trans. Veh. Technol., 2016, 65, (5), pp. 3700–3714
[8] Zhang, J., Yuan, C., Wen, C., et al.: ‘Large system secrecy rate analysis for SWIP MIMO wiretap channels’, IEEE Trans. on Information Forensics Sec., 2016, 11, (1), pp. 74–85
[9] Sendonaris, A., Erkip, E., Zhang, B.: ‘User cooperation diversity, part I: system description’, IEEE Trans. Commun., 2003, 51, (11), pp. 1927–1938
[10] Sendonaris, A., Erkip, E., Zhang, B.: ‘User cooperation diversity, part II: implementation aspects and performance analysis’, IEEE Trans. Commun., 2003, 51, (11), pp. 1939–1948
[11] Zou, Y., Zha, J., Wang, X., et al.: ‘Improving physical-layer security in wireless communications using diversity techniques’, IEEE Netw., 2015, 29, (1), pp. 2–8
[12] Zou, Y., Wang, X., Shen, W.: ‘Optimal relay selection for physical-layer security in cooperative wireless cooperative networks’, IEEE J. Sel. Areas Commun., 2013, 31, (10), pp. 2099–2111
[13] Lu, D., Han, Z., Petropulu, A., et al.: ‘Improving wireless physical-layer security via cooperating relays’, IEEE Trans. Signal Process., 2011, 58, (3), pp. 1875–1888
[14] Wang, H., Yu, Q., Xia, X.: ‘Distributed beamforming for physical-layer security of two-way relay networks’, IEEE Trans. Signal Process., 2012, 60, (7), pp. 3532–3545
[15] Zhang, J., Gansury, M.: ‘Collaborative relay beamforming for secrecy’, Proc. IEEE Int. Conf. Commun. Services, South Africa, 2010, pp. 1–5
[16] Wang, X., Wang, K., Zhang, X.: ‘Secure relay beamforming with imperfect channel side information’, IEEE Trans. Veh. Technol., 2013, 62, (5), pp. 2140–2150
[17] Zheng, G., Choo, L., Wong, K.: ‘Optimal cooperative jamming to enhance physical layer security using relays’, IEEE Trans. Signal Process., 2011, 59, (3), pp. 1317–1322
[18] Liu, Y., Li, J., Petropulu, A.: ‘Destination assisted cooperative jamming for wireless physical-layer security’, IEEE Trans. on Information Forensics Sec., 2013, 8, (4), pp. 682–694
[19] Wang, C., Wang, H.: ‘Robust joint beamforming and jamming for secure AF networks: low-complexity design’, IEEE Trans. Veh. Technol., 2014, 64, (5), pp. 2192–2198
[20] Krikidis, I., Thompson, J., McLaughlin, S.: ‘Relay selection for secure cooperative networks with jamming’, IEEE Veh. Wires. Commun., 2009, 8, (10), pp. 5003–5011
[21] Gu, Q., Wang, G., Guo, L., et al.: ‘Security-reliability performance of cognitive AF relay-based wireless communication system with channel estimation error’, EURASIP J. Adv. Signal Process., 2014, 2014, (28), pp. 1–11
[22] Wang, G., Liu, Q., He, R., et al.: ‘Acquisition of channel state information in heterogeneous cloud radio access networks: challenges and research directions’, IEEE Veh. Technol. Commun., 2015, 22, (3), pp. 100–117
[23] Gradshteyn, I., Ryzhik, I.: ‘Variational principles’, in Jeffery, A. (Ed.): ‘Table of integrals, series, and products’ (Academic Press, New York, 2007, 7th edn.), p. 1091
[24] Zou, Y., Li, X., Liang, Y.: ‘Secrecy outage and diversity analysis of cognitive radio systems’, IEEE J. Sel. Areas Commun., 2014, 32, (11), pp. 2222–2236
[25] Press, W., Teukolsky, S., Vetterling, W., et al.: ‘Numerical recipes: the art of scientific computing’ (Cambridge University Press, New York, 2007, 3rd ed.)
[26] Li, J., Petropulu, A.: ‘Optimal input covariance for achieving secrecy capacity in Gaussian MIMO wiretap channels’, Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing, Dallas, USA, 2010, pp. 3360–3363
[27] Zappone, A., Lin, P., Jorswieck, E.: ‘Energy efficiency in secure multi-antenna systems’, http://arXiv.org/abs/1505.02385, 2015

9 Appendix

IEE Commun., 2017, Vol. 11 Iss. 12, pp. 1886-1894

This is an open access article published by the IET under the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0/)
\[(x^H r + c |r|^2 s) = [r |r|^2 - x (c |r|^2)] = 0 \quad \text{for} \quad x \neq 0 \quad \text{and} \quad c \neq 0 \quad \text{(40)}\]

Setting the left-hand side of (40) to zero, we obtain \(x = c e^{j(\pi - \phi)}\). Substituting \(x\) into the right-hand side of (40), the right-hand side also equals zero. Thus, \(\tilde{u}_1 = r + c e^{j(\pi - \phi)} s\) is the eigenvector corresponding to \(\lambda_1\). (24) can be derived through normalising \(\tilde{u}_1\).

The unit-norm eigenvector of \(rr^H - ss^H\) corresponding to \(\lambda_2\) can be derived in a similar way.