Open access • Journal Article • DOI:10.1109/TSP.2013.2247600

# Secure Communication Via an Untrusted Non-Regenerative Relay in Fading Channels — Source link

Jing Huang, Amitav Mukherjee, A. Lee Swindlehurst

**Institutions:** University of California, Irvine, Hitachi

**Published on:** 01 May 2013 - IEEE Transactions on Signal Processing (IEEE)

**Topics:** Relay channel, Relay, Fading, Jamming and Transmission (telecommunications)

# Secure Communication Via an Untrusted Non-Regenerative Relay in Fading Channels

Jing Huang, *Student Member, IEEE*, Amitav Mukherjee, *Member, IEEE*, and A. Lee Swindlehurst, *Fellow, IEEE*

***Abstract*—We investigate a relay network where the source can potentially utilize an untrusted non-regenerative relay to augment its direct transmission of a confidential message to the destination. Since the relay is untrusted, it is desirable to protect the confidential data from it while simultaneously making use of it to increase the reliability of the transmission. We first examine the secrecy outage probability (SOP) of the network assuming a single antenna relay, and calculate the exact SOP for three different schemes: direct transmission without using the relay, conventional non-regenerative relaying, and cooperative jamming by the destination. Subsequently, we conduct an asymptotic analysis of the SOPs to determine the optimal policies in different operating regimes. We then generalize to the multi-antenna relay case and investigate the impact of the number of relay antennas on the secrecy performance. Finally, we study a scenario where the relay has only a single RF chain which necessitates an antenna selection scheme, and we show that unlike the case where all antennas are used, under certain conditions the cooperative jamming scheme with antenna selection provides a diversity advantage for the receiver. Numerical results are presented to verify the theoretical predictions of the preferred transmission policies.**

***Index Terms*—Cooperative jamming, outage probability, physical layer security, relay networks, wiretap channel.**

## I. Introduction

THE broadcast characteristic of the wireless medium facilitates a number of advanced communication protocols at the physical layer, such as cooperative communications with the aid of relay nodes. Since relays can overhear signals emanating from a source and rebroadcast them towards the intended destination, the reliability of the transmission can be improved via diversity. However, the broadcast property also makes it difficult to shield information from being leaked to unintended receivers (eavesdroppers), which has led to an intensive study of improving information security at the physical layer of wireless networks [1].

The foremost metric of physical-layer information security is the secrecy capacity, which quantifies the maximal transmission rate at which the eavesdropper is unable to decode any of the confidential data. An alternative secrecy criterion that has recently been investigated for fading channels is the secrecy outage probability (SOP), from which one can determine the likelihood of achieving a certain secrecy rate [2].

In the context of single-input single-output (SISO) relay channels, the SOP has been investigated in [3]–[5] for networks composed of external eavesdroppers that are distinct from the source/sink and relay nodes. Secrecy may still be an issue even in the absence of external eavesdroppers, since one may desire to keep the source signal confidential from the relay itself in spite of its assistance in forwarding the data to the destination [6]. The relay is in effect also an eavesdropper, even though it complies with the source's request to forward messages to the destination. For example, an *untrusted relay* may belong to a heterogeneous network without the same security clearance as the source and destination nodes. This scenario has been studied in [7], [8] where the authors presented bounds on the achievable secrecy rate. Furthermore, they showed that non-regenerative or amplify-and-forward (AF) and compress-and-forward relaying (including a direct link) admit a non-zero secrecy rate even when the relay is untrusted, which does not hold for decode-and-forward relaying.

Our paper analyzes a three-node relay network where the source can potentially utilize a multi-antenna untrusted relay to augment the direct link to its destination. In [9], the authors considered the joint source/relay beamforming design problem for secrecy rate maximization via an AF multi-antenna relay. In realistic fading channels, the secrecy outage probability is a more meaningful metric compared to the ergodic secrecy rate, which is ill-defined under finite delay constraints. Thus, unlike [9], in this work we focus on the SOP of the AF relaying protocol, which is chosen due to its increased security vis-à-vis decode-and-forward and lower complexity compared to compress-and-forward.

When multiple antennas are employed in relay networks, any potential performance benefits must be balanced against increased hardware complexity and power consumption. As a reduced-complexity solution that can maintain full diversity, antenna selection has received extensive attention in AF relay networks, for example in cases where only one RF chain is available at the relay [10]. In [11], a low-complexity near-optimal antenna selection algorithm was proposed for maximizing the achievable rate. The bit error rate performance obtained

Manuscript received July 08, 2012; revised November 26, 2012; accepted February 04, 2013. Date of publication February 15, 2013; date of current version April 24, 2013. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Ta-Sung Lee. This work was supported by the U.S. Army Research Office MURI Grant W911NF-07-1-0318, and by the National Science Foundation by Grant CCF-1117983. The material in this paper was presented in part at the Thirty-Seventh IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), Kyoto, Japan, March 2012, and the IEEE International Conference on Communications (ICC), Ottawa, ON, Canada, June 2012.

J. Huang and A. L. Swindlehurst are with the Center for Pervasive Communications and Computing, University of California, Irvine, CA 92697 USA (e-mail: jing.huang@uci.edu; swindle@uci.edu).

A. Mukherjee is with Hitachi America, Ltd., Santa Clara, CA 95050 USA (e-mail: amitav.mukherjee@hal.hitachi.com).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSP.2013.2247600

by choosing the best antenna pairs over both relay hops was examined in [12]. However, the open problem addressed in our paper is the tradeoff between the diversity gain for the legitimate receiver versus the inadvertent diversity gain of the information leaked to the untrusted relay in the first hop.

In this paper, we calculate the exact SOP with a multi-antenna relay for three different transmission policies: (1) direct transmission (DT) where the relay is considered as a pure eavesdropper, (2) conventional AF relaying, and (3) cooperative jamming (CJ) by the destination in the first hop to selectively degrade the relay's eavesdropping capability. There are scenarios (with different SNR, number of antennas, channel gains, *etc.* ) where each of these three schemes demonstrates a performance advantage over the other two. Our analysis allows these performance transitions to be determined. We also conduct an asymptotic analysis for the special case of a single-antenna relay and elicit the optimal policies for different power budgets and channel gains. Secrecy is typically compromised when a multi-antenna relay is employed, especially as the number of relay antennas grows large. We show that the secrecy performance improves when the relay can only perform antenna selection instead of beamforming, but in nearly all cases the SOP still grows with the number of relay antennas. A non-increasing SOP is shown to only be obtained when the CJ scheme is used and the second-hop CSI can be hidden from the relay.

The remainder of this work is organized as follows. The mathematical models of the AF relaying and cooperative jamming approaches are introduced in Section II. The secrecy outage probabilities of direct transmission, AF relaying, and cooperative jamming with a multi-antenna relay are examined in Section III, and the specialization to a relay employing antenna selection is presented in Section IV. Selected numerical results are shown in Section V, and we conclude in Section VI.

## II. Mathematical Model

We consider a half-duplex two-hop relaying network composed of a source (Alice), a destination (Bob), and an untrusted relay that when active employs the AF protocol. Alice and Bob are both single-antenna nodes, and the relay is assumed to be equipped with $K$ antennas. The channel is assumed to be quasi-static (constant during the two hops) with Rayleigh fading and a direct link between Alice and Bob is assumed to be available. We also assume all nodes in the network have the same power budget $P$.

### A. Relay Protocol

For AF relaying, during the first phase the relay receives

$$\mathbf{y}_R = \mathbf{h}_{A,R} x_A + \mathbf{n}_R \tag{1}$$

where $x_A$ is the zero-mean signal transmitted by Alice with variance $\mathbb{E}\{x_A^H x_A\} = P$, $\mathbf{h}_{A,R} = [h_{A,1}, h_{A,2}, \ldots, h_{A,K}]^T$ is the complex circularly symmetric Gaussian channel vector with covariance matrix $\mathbf{C}_{A,R} = diag\{\bar{\gamma}_{A,1}, \bar{\gamma}_{A,2}, \ldots, \bar{\gamma}_{A,K}\}$, and $\mathbf{n}_R$ is additive white Gaussian noise with covariance $N_0\mathbf{I}$. For the moment, we assume spatially white noise with no jamming present; the case of cooperative jamming will be discussed separately. In general, we will use $\mathbf{h}_{i,j}$ to represent the channel vector between node $i$ and $j$, with $i, j \in \{A, B, R\}$ denoting which of the terminals is involved. Let $\gamma_{i,j} \triangleq |h_{i,j}|^2$ be the instantaneous squared channel strength, so that $\gamma_{i,j}$ is exponentially distributed with hazard rate $\frac{1}{\bar{\gamma}_{i,j}}$, i.e. $\gamma_{i,j} \sim \exp(\frac{1}{\bar{\gamma}_{i,j}})$. The probability density function (p.d.f.) of $\gamma_{i,j}$ is given by

$$p_{\gamma_{i,j}}(x) = \frac{1}{\bar{\gamma}_{i,j}} e^{-\frac{x}{\bar{\gamma}_{i,j}}}, \quad x \geq 0. \tag{2}$$

When the relay has $K$ RF chains and can implement beamforming, we assume that, for purposes of forwarding the message, the relay adopts maximum ratio combining (MRC) for reception and maximum ratio transmission (MRT) for transmission. Thus, the output of the relay receiver is given by

$$\tilde{y}_R = \sqrt{\sum\nolimits_{i=1}^{K} |h_{A,i}|^2} x_A + \frac{\sum_{i=1}^{K} h_{A,i}^H n_i}{\sqrt{\sum_{i=1}^{K} |h_{A,i}|^2}}.$$

The relay then transmits the signal $\mathbf{x}_R = \frac{\sqrt{P}}{\sigma} \frac{\mathbf{h}_{R,B}^H}{\|\mathbf{h}_{R,B}\|} \tilde{y}_R$, where $\sigma = \sqrt{\mathbb{E}\{\|\tilde{y}_R\|^2\}}$ and $\mathbf{h}_{R,B} = [h_{1,B}, h_{2,B}, \ldots, h_{K,B}]$. The received signal at Bob over both phases is then given by

$$\mathbf{y}_B = \begin{bmatrix} h_{A,B} \\ \frac{\sqrt{P}}{\sigma} \sqrt{\sum_{i=1}^{K} |h_{i,B}|^2} \sqrt{\sum_{i=1}^{K} |h_{A,i}|^2} \end{bmatrix} x_A + \begin{bmatrix} n_{B1} \\ \frac{\sqrt{P}}{\sigma} \sqrt{\frac{\sum_{i=1}^{K} |h_{i,B}|^2}{\sum_{i=1}^{K} |h_{A,i}|^2}} \sum_{i=1}^{K} h_{A,i}^H n_i + n_{B2} \end{bmatrix}, \tag{3}$$

where we assume that $n_{B1}$ and $n_{B2}$ are uncorrelated Gaussian noise variables with variance $N_0$. The subscripts 1 and 2 refer to the first and second transmission phases, respectively. Since the antennas on the relay are much closer together compared to their distances to the source and the destination, we assume $\{\bar{\gamma}_{A,i}\}_{i=1}^K = \bar{\gamma}_{A,R}$ and $\{\bar{\gamma}_{i,B}\}_{i=1}^K = \bar{\gamma}_{R,B}$.

We assume Alice uses a codebook $\mathcal{C}(2^{nR_0}, 2^{nR_s}, n)$ where $R_s$ is the intended secrecy rate ($R_s \leq R_0$), $n$ is the codeword length, $2^{nR_0}$ is the size of the codebook, and $2^{nR_s}$ is the number of confidential messages to transmit. The $2^{nR_0}$ codewords are randomly grouped into $2^{nR_s}$ bins. To send confidential message $w \in \{1, \cdots, 2^{nR_s}\}$, Alice will use a stochastic encoder to randomly select a codeword from bin $w$ and send it over the channel. Since in our model the untrusted relay only wiretaps in the first phase, and since the AF and CJ schemes are mathematically equivalent to a one-stage $1 \times 2$ SIMO wiretap channel [8], [13] a conventional wiretap code can be applied. The achievable secrecy rate is then the same as for the equivalent one-hop channel: i.e., $R_s = [I_B - I_E]^+$ where $[x]^+ \triangleq \max\{0, x\}$, $I_B$ is the mutual information for the legitimate link and $I_E$ is the mutual information for the eavesdropper link.

### B. Cooperative Jamming

Various cooperative jamming schemes involving the transmission of artificial interference have been proposed in previous work for improving secrecy [5], [14]–[17]. In this paper, as an alternative to the traditional AF protocol, we assume a half-duplex cooperative jamming scheme where Bob forfeits information from Alice during the first phase in favor of transmitting

a jamming signal. Under this model, the received signal at the relay is

$$\mathbf{y}_R = \mathbf{h}_{A,R} x_A + \mathbf{h}_{R,B} z_B + \mathbf{n}_R \tag{4}$$

where $z_B$ is the jamming signal transmitted by Bob with power $\mathbb{E}\{z_B^H z_B\} = P$. Similar to the AF scheme, during the second phase, the relay scales $\mathbf{y}_R$ and forwards it to Bob, and thus the received signal at Bob can be written as

$$\begin{aligned} y_B =& \frac{\sqrt{P}}{\sigma} \sqrt{\sum_{i=1}^{K} |h_{i,B}|^2 \sum_{i=1}^{K} |h_{A,i}|^2} x_A \\ &+ \frac{\sqrt{P}}{\sigma} \sqrt{\frac{\sum_{i=1}^{K} |h_{i,B}|^2}{\sum_{i=1}^{K} |h_{A,i}|^2}} \left( \sum_{i=1}^{K} h_{i,B}^H h_{A,i} z_B + \sum_{i=1}^{K} h_{A,i}^H n_i \right) \\ &+ n_{B2} \end{aligned} \tag{5}$$

where we assume a reciprocal channel between the relay and Bob: $\mathbf{h}_{R,B} = \mathbf{h}_{B,R}^H$. Note that the intentional interference term can be removed by Bob since $z_B$ is known to him.

While we assume that the relay forwards the output of the MRC beamformer to Bob, when computing the mutual information available to the relay we assume that she can perform MMSE (maximum SINR) beamforming to counteract the jamming from Bob. Recall that since Bob is the source of the interference, he can subtract its contribution from the signal forwarded by the relay regardless of the choice of receive beamformer employed at the relay.

## III. Transmission With an Untrusted Relay

### A. Single-Antenna Relay

We begin with the case where the relay employs a single antenna. In this section, we will calculate the exact SOP expressions for the DT, AF and CJ schemes and analyze the corresponding asymptotic behavior under limiting conditions on the power budgets and channel gains.

*1) DT:* Direct transmission refers to the case where Alice uses a single-hop transmission to communicate with Bob rather than cooperating with the relay. As illustrated later, in some cases this strategy provides better secrecy performance than AF and CJ. Under DT, the relay is simply treated as a pure eavesdropper. Thus the model will be simplified to a traditional wiretap channel with Rayleigh fading, which has been fully characterized in [2], for example. Since the channel gains are assumed to be quasi-static, the achievable secrecy rate for one channel realization is given by

$$R_s^{DT} = \left[ I_B^{DT} - I_R^{DT} \right]^+ \tag{6}$$

where $I_B^{DT}$ and $I_R^{DT}$ represent the mutual information between Alice and Bob, and between Alice and the relay respectively, and are given by $I_B^{DT} = \log_2(1 + (\frac{P}{N_0})|h_{A,B}|^2)$ and $I_R^{DT} = \log_2(1 + (\frac{P}{N_0})|h_{A,R}|^2)$.

When $K = 1$, the probability of a positive secrecy rate is given by [2]

$$\begin{aligned} \mathcal{P}_{pos}^{DT} &= \mathcal{P}\left( I_B^{DT} - I_R^{DT} > 0 \right) = \mathcal{P}\left( |h_{A,B}|^2 > |h_{A,R}|^2 \right) \\ &= \frac{\bar{\gamma}_{A,B}}{\bar{\gamma}_{A,R} + \bar{\gamma}_{A,B}}. \end{aligned} \tag{7}$$

It is interesting to note that, in the presence of fading, a nonzero secrecy rate exists even when $\bar{\gamma}_{A,R} > \bar{\gamma}_{A,B}$, i.e. when the eavesdropper's channel is on average better than the legitimate channel [2] (although the probability of such an event is less than 1/2). Eq. (7) also indicates that Alice will be unable to reliably transmit secret messages when $\bar{\gamma}_{A,R} \to \infty$, e.g., when the untrusted relay is proximate to Alice.

The outage probability for a target secrecy rate $R$ is given by [2]

$$\begin{aligned} \mathcal{P}_{out}^{DT}(R) &= \mathcal{P}\left\{ I_B^{DT} - I_R^{DT} < R \right\} \\ &= \mathcal{P}\left\{ \frac{1 + \rho|h_{A,B}|^2}{1 + \rho|h_{A,R}|^2} < 2^R \right\} \\ &= 1 - \frac{\bar{\gamma}_{A,B}}{2^R \bar{\gamma}_{A,R} + \bar{\gamma}_{A,B}} e^{-\frac{2^R - 1}{\rho \bar{\gamma}_{A,B}}}, \end{aligned} \tag{8}$$

where $\rho \triangleq \frac{P}{N_0}$ is the transmit SNR. The secrecy outage probability is a criterion that indicates the fraction of fading realizations where a secrecy rate $R$ cannot be supported, and also provides a security metric for the case where Alice and Bob have no CSI for the eavesdropper [2]. However, we recognize the alternative definition of SOP that was recently proposed in [18], which provides a more explicit measurement of security level by only considering secrecy outage events conditioned on a reliable legitimate link. The secrecy outage results presented in this work can be reformulated according to this alternative definition in a straightforward manner.

*2) AF:* When the untrusted AF relay is employed for cooperation, the channel is equivalent to the conventional wiretap channel where Bob receives the signal from two orthogonal channels [8], and thus the achievable secrecy rate can be computed from $R_s^{AF} = [I_B^{AF} - I_R^{AF}]^+$, where

$$I_B^{AF} = \frac{1}{2} \log_2 \left( 1 + \rho|h_{A,B}|^2 + \rho \frac{|h_{R,B}|^2 |h_{A,R}|^2}{|h_{R,B}|^2 + \bar{\gamma}_{A,R} + \frac{1}{\rho}} \right) \tag{9}$$

and

$$I_R^{AF} = \frac{1}{2} \log_2 \left( 1 + \rho|h_{A,R}|^2 \right). \tag{10}$$

Therefore, the probability of achieving a positive secrecy rate for AF relaying is formulated as

$$\mathcal{P}_{pos}^{AF} = \mathcal{P}\left\{ |h_{A,B}|^2 + \frac{|h_{R,B}|^2 |h_{A,R}|^2}{|h_{R,B}|^2 + \bar{\gamma}_{A,R} + \frac{1}{\rho}} > |h_{A,R}|^2 \right\}. \tag{11}$$

In Appendix A, we show that this probability is given by

$$\mathcal{P}_{pos}^{AF} = \mu_1(\beta_1 - 1) e^{\mu_1 \beta_1} \mathrm{Ei}(-\mu_1 \beta_1) + 1 \tag{12}$$

where $\mu_1 = \frac{\bar{\gamma}_{A,R} + 1/\rho}{\bar{\gamma}_{R,B}}$, $\beta_1 = 1 + \frac{\bar{\gamma}_{A,R}}{\bar{\gamma}_{A,B}}$ and $\mathrm{Ei}(\cdot)$ is the exponential integral $\mathrm{Ei}(x) = \int_{-\infty}^{x} e^t t^{-1} dt$.

The outage probability of the AF scheme for a given secrecy rate $R$ can be written as

$$\mathcal{P}_{out}^{AF}(R) = \mathcal{P}\left\{\frac{1+\rho|h_{A,B}|^2+\rho\frac{|h_{R,B}|^2|h_{A,R}|^2}{|h_{R,B}|^2+\bar{\gamma}_{A,R}+\frac{1}{\rho}}}{1+\rho|h_{A,R}|^2} < 2^{2R}\right\}, \tag{13}$$

and the exact SOP is given by the following proposition.

*Proposition 1:* The secrecy outage probability for AF relaying can be expressed as

$$\mathcal{P}_{out}^{AF}(R) = 1 - \frac{\bar{\gamma}_{A,B}\left[\mu_1(\beta_2-1)e^{\mu_1\beta_2}\mathrm{Ei}(-\mu_1\beta_2)+1\right]}{(2^{2R}-1)\bar{\gamma}_{A,R}+\bar{\gamma}_{A,B}} e^{-\frac{2^{2R}-1}{\rho\bar{\gamma}_{A,B}}} \tag{14}$$

where $\mu_1 = \frac{\bar{\gamma}_{A,R}+1/\rho}{\bar{\gamma}_{R,B}}$, $\beta_2 = \frac{2^{2R}\bar{\gamma}_{A,R}+\bar{\gamma}_{A,B}}{(2^{2R}-1)\bar{\gamma}_{A,R}+\bar{\gamma}_{A,B}}$, and $R$ is the target secrecy rate.

*Proof:* See Appendix B. ∎

For the high SNR regime, (13) can be approximated as

$$\mathcal{P}_{out}^{AF}(R) \simeq \mathcal{P}\left(\frac{|h_{A,B}|^2+\frac{|h_{R,B}|^2|h_{A,R}|^2}{|h_{R,B}|^2+\bar{\gamma}_{A,R}}}{|h_{A,R}|^2} < 2^{2R}\right), \tag{15}$$

which is a function independent of $\rho$. This indicates that the AF scheme does not approach zero SOP even as the transmit power is increased. Intuitively, this is reasonable since any increase in the transmit power will bolster the SNR at both the legitimate user and the eavesdropper. The asymptotic value of the SOP at high SNR will be characterized in Section III-B.

*3) CJ:* As mentioned above, for the CJ approach we assume Bob ignores the direct link and transmits a jamming signal during the first phase. According to the signal model in Section II-B, we have the following expression for the mutual information between Alice and Bob in this case:

$$I_B^{CJ} = \frac{1}{2}\log_2\left(1+\rho\frac{|h_{R,B}|^2|h_{A,R}|^2}{|h_{R,B}|^2+\bar{\gamma}_{A,R}+\bar{\gamma}_{R,B}+\frac{1}{\rho}}\right) \tag{16}$$

$$I_R^{CJ} = \frac{1}{2}\log_2\left(1+\frac{|h_{A,R}|^2}{|h_{R,B}|^2+\frac{1}{\rho}}\right), \tag{17}$$

and the corresponding probability of a positive secrecy rate is given by

$$\mathcal{P}_{pos}^{CJ} = \mathcal{P}\left\{\rho\frac{|h_{R,B}|^2}{|h_{R,B}|^2+\bar{\gamma}_{A,R}+\bar{\gamma}_{R,B}+\frac{1}{\rho}} > \frac{1}{|h_{R,B}|^2+\frac{1}{\rho}}\right\} = e^{-\frac{1}{\bar{\gamma}_{R,B}}\sqrt{\frac{\bar{\gamma}_{A,R}+\bar{\gamma}_{R,B}+\frac{1}{\rho}}{\rho}}}. \tag{18}$$

From (18), we see that $\mathcal{P}_{pos}^{CJ}$ is a monotonically increasing function of $\bar{\gamma}_{R,B}$ when $\bar{\gamma}_{A,R}$ is fixed. In other words, CJ is not appropriate when the second hop channel is weak. This is not surprising since, when CJ is employed, the half-duplex constraint for Bob means that the information from the direct link is ignored, and Bob relies heavily on the second hop to obtain the information from Alice.

The outage probability in this case can be expressed as

$$\mathcal{P}_{out}^{CJ}(R) = \mathcal{P}\left(\frac{1+\rho\frac{|h_{R,B}|^2|h_{A,R}|^2}{|h_{R,B}|^2+\bar{\gamma}_{A,R}+\bar{\gamma}_{R,B}+\frac{1}{\rho}}}{1+\frac{|h_{A,R}|^2}{|h_{R,B}|^2+\frac{1}{\rho}}} < 2^{2R}\right), \tag{19}$$

and the exact SOP expression is provided in the following proposition.

*Proposition 2:* The secrecy outage probability for the CJ scheme is given by

$$\mathcal{P}_{out}^{CJ}(R) = 1 - \frac{1}{\bar{\gamma}_{R,B}}\int_t^\infty e^{-\frac{2^{2R}-1}{\bar{\gamma}_{A,R}\phi(z)}-\frac{z}{\bar{\gamma}_{R,B}}}dz, \tag{20}$$

where

$$\phi(z) = \frac{\rho z}{z+\bar{\gamma}_{A,R}+\bar{\gamma}_{R,B}+\frac{1}{\rho}} - \frac{2^{2R}}{z+\frac{1}{\rho}}, \tag{21}$$

$$t = \frac{(2^{2R}-1)}{2\rho} + \frac{\sqrt{(2^{2R}-1)^2+\rho 2^{2R+1}\left(\bar{\gamma}_{A,R}+\bar{\gamma}_{R,B}+\frac{1}{\rho}\right)}}{2\rho}. \tag{22}$$

*Proof:* See Appendix C. ∎

It is important to note at this point that we have assumed each node transmits at its maximum power budget $P$. It is straightforward to formulate a secrecy outage minimization problem subject to various power constraints for the transmission strategies discussed above, but obtaining closed-form solutions to these problems appears to be intractable. Thus our theoretical analysis will focus on the case where all nodes transmit with full power, but in the simulations presented later we will show examples of the performance gain that can be obtained with an optimal power allocation.

### *B. Asymptotic Behavior*

Based on the above analytical expressions, we see that the choice of which scheme (DT, AF or CJ) to employ depends on the specific power budgets and channel gains; each of these methods is optimal for different operating regimes. Next, we investigate the asymptotic behavior of the outage probability to determine conditions under which each approach offers the best performance.

*1) Case of $\rho \to \infty$:* From (8), we have

$$\lim_{\rho\to\infty}\mathcal{P}_{out}^{DT} = 1 - \frac{\bar{\gamma}_{A,B}}{2^R\bar{\gamma}_{A,R}+\bar{\gamma}_{A,B}}, \tag{23}$$

and according to (14),

$$\lim_{\rho\to\infty}\mathcal{P}_{out}^{AF} = 1 - \frac{\bar{\gamma}_{A,B}\left[\mu_1'(\beta_1-1)e^{\mu_1'\beta_1}\mathrm{Ei}\left(-\mu_1'\beta_1\right)+1\right]}{(2^{2R}-1)\bar{\gamma}_{A,R}+\bar{\gamma}_{A,B}} \tag{24}$$

where $\mu_1' = \frac{\bar{\gamma}_{A,R}}{\bar{\gamma}_{R,B}}$. Therefore, both $\mathcal{P}_{out}^{DT}$ and $\mathcal{P}_{out}^{AF}$ converge to nonzero constants as $\rho \to \infty$. For CJ, however, according to (20)–(22), we have

$$\lim_{\rho\to\infty}\mathcal{P}_{out}^{CJ} = 1 - \frac{1}{\bar{\gamma}_{R,B}}\int_0^\infty e^{-\frac{z}{\bar{\gamma}_{R,B}}}dz = 0, \tag{25}$$

which shows that CJ is preferable for $\rho \to \infty$, or high SNR or transmit power scenarios.

*2) Case of $\bar{\gamma}_{A,B} \to \infty$ or 0:* From (8) and (14), it is also straightforward to obtain that $\mathcal{P}_{out}^{DT}, \mathcal{P}_{out}^{AF} \to 0$ as $\bar{\gamma}_{A,B} \to \infty$. When $\bar{\gamma}_{A,B}$ is sufficiently large, using the fact that $1 - e^x = x + O(x^2)$, we can observe that with respect to $\bar{\gamma}_{A,B}$, both DT and AT decay proportionally to $1/\bar{\gamma}_{A,B}$. Conversely, we also have that $\mathcal{P}_{out}^{DT}, \mathcal{P}_{out}^{AF} \to 1$ as $\bar{\gamma}_{A,B} \to 0$. Since $\mathcal{P}_{out}^{CJ}$ does not depend on $\bar{\gamma}_{A,B}$, we can conclude that the DT and AF schemes are better than CJ when the direct link is significantly stronger than the others, while CJ will perform better when the direct link is weak.

*3) Case of $\bar{\gamma}_{R,B} \to \infty$ or 0:* Since $\mathcal{P}_{out}^{DT}$ is not a function of $\bar{\gamma}_{R,B}$, it will be the same as in (8). When $\bar{\gamma}_{R,B} \to \infty$, according to (14) and using the result that $x\mathrm{Ei}(-x) \to 0$ as $x \to 0$ [5], we have

$$\lim_{\bar{\gamma}_{R,B}\to\infty} \mathcal{P}_{out}^{AF} = 1 - \frac{\bar{\gamma}_{A,B}}{(2^{2R}-1)\bar{\gamma}_{A,R} + \bar{\gamma}_{A,B}} e^{-\frac{2^{2R}-1}{\rho\bar{\gamma}_{A,B}}}. \quad (26)$$

For CJ when $\bar{\gamma}_{R,B} \to \infty$, intuitively the cooperative jamming support from Bob can fully prevent the relay from eavesdropping, and thus we will have the following lemma whose proof is given in Appendix D.

*Lemma 1:* When $\bar{\gamma}_{R,B} \to \infty$, outage events will only depend on the relay link, and the outage probability in (19) will converge to:

$$\lim_{\bar{\gamma}_{R,B}\to\infty} \mathcal{P}_{out}^{CJ} = \mathcal{P}\left(1 + \rho\frac{|h_{R,B}|^2|h_{A,R}|^2}{|h_{R,B}|^2 + \bar{\gamma}_{A,R} + \bar{\gamma}_{R,B} + \frac{1}{\rho}} < 2^{2R}\right). \quad (27)$$

Based on Lemma 1 and following the same approach as in Appendix C, we have

$$\lim_{\bar{\gamma}_{R,B}\to\infty} \mathcal{P}_{out}^{CJ} = \lim_{\bar{\gamma}_{R,B}\to\infty} 1 - \frac{1}{\bar{\gamma}_{R,B}} \int_0^\infty e^{-\frac{2^{2R}-1}{\bar{\gamma}_{A,R}\phi'(z)} - \frac{z}{\bar{\gamma}_{R,B}}} dz \quad (28)$$

where

$$\phi'(z) = \frac{\rho z}{z + \bar{\gamma}_{A,R} + \bar{\gamma}_{R,B} + \frac{1}{\rho}}.$$

Further manipulation of (28) reveals

$$\begin{aligned}\lim_{\bar{\gamma}_{R,B}\to\infty} \mathcal{P}_{out}^{CJ} &= \lim_{\bar{\gamma}_{R,B}\to\infty} 1 - \frac{1}{\bar{\gamma}_{R,B}} \int_0^\infty e^{-\frac{2^{2R}-1}{\bar{\gamma}_{A,R}\phi'(z)} - \frac{z}{\bar{\gamma}_{R,B}}} dz \\ &= 1 - e^{-\frac{2^{2R}-1}{\rho\bar{\gamma}_{A,R}}} \sqrt{\frac{4(2^{2R}-1)}{\rho\bar{\gamma}_{A,R}}} \\ &\quad \times \mathrm{K}_1\left(\sqrt{\frac{4(2^{2R}-1)}{\rho\bar{\gamma}_{A,R}}}\right), \end{aligned} \quad (29)$$

where $\mathrm{K}_1(\cdot)$ is the modified Bessel function of the second kind, and [19eq. 3.324.1] is used to obtain (29). Therefore, as $\bar{\gamma}_{RB} \to \infty$, the outage probability for all schemes converges to different constants, and the analysis does not reveal an advantage of one method over another.

When $\bar{\gamma}_{RB} \to 0$, CJ is obviously not applicable since $\mathcal{P}_{out}^{CJ} \to 1$. For the the AF scheme, applying a procedure similar to that in Appendix D on (13), the outage probability will converge to

$$\begin{aligned}\lim_{\bar{\gamma}_{RB}\to 0} \mathcal{P}_{out}^{AF} &= \mathcal{P}\left\{\frac{1}{2}\log_2\left(\frac{1+\rho|h_{A,B}|^2}{1+\rho|h_{A,R}|^2}\right) < R\right\} \quad (30) \\ &\geq \mathcal{P}\left\{\log_2\left(\frac{1+\rho|h_{A,B}|^2}{1+\rho|h_{A,R}|^2}\right) < R\right\} \quad (31)\end{aligned}$$

where (31) is equal to $\mathcal{P}_{out}^{DT}$. Thus, DT is a better choice when $\bar{\gamma}_{RB} \to 0$ due to the resource division factor 1/2.

*4) Case of $\bar{\gamma}_{A,R} \to 0$:* In this case, it is easy to verify from (20) that, for CJ,

$$\lim_{\bar{\gamma}_{A,R}\to 0} \mathcal{P}_{out}^{CJ} = 1, \quad (32)$$

since $t \to \infty$ as $\bar{\gamma}_{A,R} \to 0$ and the result of the integral in (20) approaches 0. However, for DT and AF, the outage probability will converge to constants given by

$$\lim_{\bar{\gamma}_{A,R}\to 0} \mathcal{P}_{out}^{DT} = 1 - e^{-\frac{2^R-1}{\rho\bar{\gamma}_{A,B}}} \quad (33)$$

$$\lim_{\bar{\gamma}_{A,R}\to 0} \mathcal{P}_{out}^{AF} = 1 - e^{-\frac{2^{2R}-1}{\rho\bar{\gamma}_{A,B}}}. \quad (34)$$

Similar to the case in Section III-B-3, we see from the above equations that $\lim_{\bar{\gamma}_{A,R}\to 0} \mathcal{P}_{out}^{AF} \geq \lim_{\bar{\gamma}_{A,R}\to 0} \mathcal{P}_{out}^{DT}$, i.e., the SOP of the DT scheme is lower than that of the AF scheme and thus DT is preferred in this case.

### C. Multi-Antenna Relay

In this section, we generalize our analysis to the case of a multi-antenna relay. We will theoretically characterize the SOP and the impact of the number of relay antennas on the secrecy performance.

*1) Direct Transmission (DT):* Similar to the expression in (8), when the relay uses multiple antennas and MRC beamforming, the outage probability for a given target secrecy rate $R$ is given by

$$\mathcal{P}_{out}^{DT}(R) = \mathcal{P}\left\{\log_2\left(\frac{1+\rho|h_{A,B}|^2}{1+\rho\sum_{i=1}^K |h_{A,i}|^2}\right) < R\right\}. \quad (35)$$

Denote $X = |h_{A,B}|^2$ and $Y = \sum_{i=1}^K |h_{A,i}|^2$, and recall that $X \sim \exp(\frac{1}{\bar{\gamma}_{A,R}})$. Since $Y$ can be rewritten as $\frac{\bar{\gamma}_{A,R}}{2}\sum_{i=1}^{2K}\alpha_i^2$ where $\{\alpha\}_{i=1}^{2K}$ are $2K$ independent standard normal Gaussian random variables (r.v.s), $\sum_{i=1}^{2K}\alpha_i^2$ has a central chi-square distribution with $2K$ degrees of freedom. Therefore, we have

$$\mathcal{P}_Y(y) = \frac{y^{K-1}}{\bar{\gamma}_{A,R}^K(K-1)!} e^{-\frac{y}{\bar{\gamma}_{A,R}}} \quad (36)$$

and thus

$$\begin{aligned}\mathcal{P}_{out}^{DT} &= \mathbb{E}_Y\left\{F_X\left(\frac{2^R-1}{\rho} + 2^R Y\right)\right\} \\ &= 1 - \int_0^\infty \mathcal{P}_Y(y) e^{-\frac{1}{\bar{\gamma}_{A,B}}\left(\frac{2^R-1}{\rho} + 2^R Y\right)} dy \\ &= 1 - \left(\frac{\bar{\gamma}_{A,B}}{2^R\bar{\gamma}_{A,R} + \bar{\gamma}_{A,B}}\right)^K e^{-\frac{2^R-1}{\rho\bar{\gamma}_{A,B}}}. \end{aligned} \quad (37)$$

It can be seen from (37) that the SOP of the DT scheme will approach unity as $K$ grows, which is also consistent with the intuition that the presence of more antennas at the eavesdropper will result in a deterioration in secrecy performance.

*2) Amplify-and-Forward (AF):* According to the signal model (1) and (3), the outage probability in (13) for a target secrecy rate $R$ and $K$ antennas at the relay can be written as

$$P_{out}^{AF}(R) = \mathcal{P}\left\{\frac{1+\rho|h_{A,B}|^2+\rho\frac{\sum_{i=1}^{K}|h_{i,B}|^2\sum_{i=1}^{K}|h_{A,i}|^2}{\sum_{i=1}^{K}|h_{i,B}|^2+K\bar{\gamma}_{A,R}+\frac{K}{\rho}}}{1+\rho\sum_{i=1}^{K}|h_{A,i}|^2} < 2^{2R}\right\}. \quad (38)$$

The exact SOP is given by the following proposition:

*Proposition 3:* The secrecy outage probability for AF relaying with $K$ relay antennas is

$$\begin{aligned}\mathcal{P}_{out}^{AF}(R) = 1 &- \left[1+\frac{\bar{\gamma}_{A,R}(2^{2R}-1)}{\bar{\gamma}_{A,B}}\right]^{-K} e^{-\frac{2^{2R}-1}{\rho\bar{\gamma}_{A,B}}} \\ &+ \int_0^{\infty}\int_{\frac{(1+\rho y)(2^{2R}-1)}{\rho}}^{2^{2R}y+\frac{2^{2R}-1}{\rho}} \frac{y^{K-1}}{\bar{\gamma}_{A,B}\bar{\gamma}_{A,R}^{K}(K-1)!} \\ &\times F_V\left(2^{2R}+\frac{2^{2R}-1-\rho x}{\rho y}\right) \\ &\times e^{-\frac{x}{\bar{\gamma}_{A,B}}-\frac{y}{\bar{\gamma}_{A,R}}}dxdy, \end{aligned} \quad (39)$$

where $R$ is the target secrecy rate, and the c.d.f. of $V$ is

$$F_V(v) = 1-\sum_{n=0}^{K-1}\frac{1}{n!}\left[\frac{vK\left(\bar{\gamma}_{A,R}+\frac{1}{\rho}\right)}{\bar{\gamma}_{R,B}(1-v)}\right]^{n} e^{-\frac{vK\left(\bar{\gamma}_{A,R}+\frac{1}{\rho}\right)}{\bar{\gamma}_{R,B}(1-v)}}. \quad (40)$$

*Proof:* Defining $X = |h_{A,B}|^2$, $Y = \sum_{i=1}^{K}|h_{A,i}|^2$, and $V = \frac{\sum_{i=1}^{K}|h_{i,B}|^2}{\sum_{i=1}^{K}|h_{i,B}|^2+K\bar{\gamma}_{A,R}+K/\rho}$, according to (38) the SOP is given by

$$\mathcal{P}_{out}^{AF}(R) = \mathcal{P}\{1+\rho X-\rho(2^{2R}-V)Y < 2^{2R}\}. \quad (41)$$

In order to obtain the SOP, we first compute the c.d.f. of $V$. It is obvious that $F_V(v)=1$ when $v\geq 1$ due to the fact that $V\leq 1$. When $v<1$,

$$\begin{aligned} F_V(v) &= \mathcal{P}\left\{\frac{\sum_{i=1}^{K}|h_{i,B}|^2}{\sum_{i=1}^{K}|h_{i,B}|^2+K\left(\bar{\gamma}_{A,R}+\frac{1}{\rho}\right)} \leq v\right\} \\ &= \mathcal{P}\left\{\sum_{i=1}^{K}|h_{i,B}|^2 \leq \frac{vK\left(\bar{\gamma}_{A,R}+\frac{1}{\rho}\right)}{1-v}\right\} \\ &= \mathcal{P}\left\{\sum_{i=1}^{2K}\alpha_i^2 \leq 2\frac{vK\left(\bar{\gamma}_{A,R}+\frac{1}{\rho}\right)}{\bar{\gamma}_{R,B}(1-v)}\right\} \\ &\overset{a}{=} 1-\sum_{n=0}^{K-1}\frac{1}{n!}\left[\frac{vK\left(\bar{\gamma}_{A,R}+\frac{1}{\rho}\right)}{\bar{\gamma}_{R,B}(1-v)}\right]^{n} e^{-\frac{vK\left(\bar{\gamma}_{A,R}+\frac{1}{\rho}\right)}{\bar{\gamma}_{R,B}(1-v)}} \end{aligned}$$

where (a) results because $\{\alpha_i\}_{i=1}^{2K}$ are $2K$ independent standard normal Gaussian r.v.s and thus $\sum_{i=1}^{2K}\alpha_i^2$ has a central chi-square distribution with $2K$ degrees of freedom.

Recall that the p.d.f.s for $X$ and $Y$ are $\mathcal{P}_X(x)=\frac{1}{\bar{\gamma}_{A,B}}e^{-\frac{x}{\bar{\gamma}_{A,B}}}$ and $\mathcal{P}_Y\frac{(y)=(y^{K-1}}{\bar{\gamma}_{A,R}^{K}(K-1)!}e^{-\frac{y}{\bar{\gamma}_{A,R}}}$, so the SOP can be written as

$$\begin{aligned}\mathcal{P}_{out}^{AF}(R) &= \mathbb{E}_Y\mathbb{E}_X\left\{F_V\left(2^{2R}+\frac{2^{2R}-1-\rho X}{\rho Y}\right)\right\} \\ &= \int_0^{\infty}\int_{x_l}^{x_u} F_V\left(2^{2R}+\frac{2^{2R}-1-\rho X}{\rho Y}\right) \\ &\quad\times \mathcal{P}_X(x)\mathcal{P}_Y(y)dxdy \\ &\quad+\int_0^{\infty}\int_0^{x_l}\mathcal{P}_X(x)\mathcal{P}_Y(y)dxdy, \end{aligned} \quad (42)$$

where the limits $x_l=\frac{(1+\rho y)(2^{2R}-1)}{\rho}$ and $x_u=2^{2R}y+\frac{2^{2R}-1}{\rho}$ can be derived from the fact that $0\leq V\leq 1$. With some further manipulations, the first term in (42) can be computed as

$$\begin{aligned}\int_0^{\infty}\int_0^{x_l}\mathcal{P}_X(x)\mathcal{P}_Y(y)dxdy &= 1-\int_0^{\infty}\frac{y^{K-1}}{\bar{\gamma}_{A,R}^{K}(K-1)!} \\ &\quad\times e^{-y\left(\frac{1}{\bar{\gamma}_{A,R}}+\frac{2^{2R}-1}{\bar{\gamma}_{A,B}}\right)-\frac{2^{2R}-1}{\rho\bar{\gamma}_{A,B}}} \\ &= 1-\left[1+\frac{\bar{\gamma}_{A,R}}{\bar{\gamma}_{A,B}}(2^{2R}-1)\right]^{-K} \\ &\quad\times e^{-\frac{2^{2R}-1}{\rho\bar{\gamma}_{A,B}}}. \end{aligned} \quad (43)$$

Inserting $\mathcal{P}_X(x)$, $\mathcal{P}_Y(y)$, $F_V(v)$ and (43) to (42), the SOP for the multi-antenna case is then obtained. ■

*Corollary 1:* The secrecy outage probability of AF relaying approaches unity as the number of relay antennas grows: $\mathcal{P}_{out}^{AF}\to 1$ as $K\to\infty$.

*Proof:* According to (39) in Proposition 3, since $\left[1+\frac{\bar{\gamma}_{AR}(2^{2R}-1)}{\bar{\gamma}_{AB}}\right]^{-K} e^{-\frac{2^{2R}-1}{\rho\bar{\gamma}_{AB}}}$ converges to 0 as $K$ grows, and since the third term in (39) is non-negative, the corollary follows in a straightforward manner. ■

*3) Cooperative Jamming (CJ):* According to (4) and (5), the mutual information between Alice and Bob can be expressed as

$$I_B^{CJ}=\frac{1}{2}\log_2\left(1+\rho\frac{\sum_{i=1}^{K}|h_{i,B}|^2\sum_{i=1}^{K}|h_{A,i}|^2}{\sum_{i=1}^{K}|h_{i,B}|^2+K\bar{\gamma}_{A,R}+K\bar{\gamma}_{R,B}+\frac{K}{\rho}}\right).$$

As discussed above, when computing the mutual information available to the relay, we assume the use of an optimal MMSE receive beamformer that allows the relay to maximize her SINR [16], i.e.,

$$\mathbf{w}=\mathcal{G}\left(\mathbf{h}_{A,R}\mathbf{h}_{A,R}^H, \mathbf{h}_{R,B}\mathbf{h}_{R,B}^H+\frac{1}{\rho}\mathbf{I}_K\right), \quad (44)$$

where $\mathcal{G}(\mathbf{A},\mathbf{B})$ is the operator that returns the eigenvector associated with the largest generalized eigenvalue of the matrix pencil $(\mathbf{A},\mathbf{B})$. Since $\mathbf{h}_{A,R}\mathbf{h}_{A,R}^H$ is rank one, we can explicitly obtain the MMSE beamformer

$\mathbf{w} = (\frac{\mathbf{h}_{R,B}\mathbf{h}_{R,B}^H+\frac{1}{\rho}\mathbf{I}_K)^{-1}\mathbf{h}_{A,R}}{\|(\mathbf{h}_{R,B}\mathbf{h}_{R,B}^H+\frac{1}{\rho}\mathbf{I}_K)^{-1}\mathbf{h}_{A,R}\|}$, and thus the mutual information between Alice and the relay is given by

$$I_R^{CJ} = \frac{1}{2}\log_2\left(1+\mathbf{h}_{A,R}^H\left(\mathbf{h}_{R,B}\mathbf{h}_{R,B}^H+\frac{1}{\rho}\mathbf{I}_K\right)^{-1}\mathbf{h}_{A,R}\right).$$

Therefore, the secrecy outage probability of the CJ scheme can be written as

$$\mathcal{P}_{out}^{CJ} = \mathcal{P}\left\{\frac{1+\rho\frac{\sum_{i=1}^K|h_{i,B}|^2\sum_{i=1}^K|h_{A,i}|^2}{\sum_{i=1}^K|h_{i,B}|^2+K\bar{\gamma}_{A,R}+K\bar{\gamma}_{R,B}+\frac{K}{\rho}}}{1+\mathbf{h}_{A,R}^H\left(\mathbf{h}_{R,B}\mathbf{h}_{R,B}^H+\frac{1}{\rho}\mathbf{I}_K\right)^{-1}\mathbf{h}_{A,R}} < 2^{2R}\right\}. \quad (45)$$

Unlike the analysis for the AF scheme, (45) is more complicated and it is unclear how to obtain a closed-form SOP expression. Instead, we focus here on finding an asymptotic SOP with respect to the transmit SNR and the number of relay antennas, as detailed in the following corollaries.

*Corollary 2:* When $K > 1$, the secrecy outage probability of the CJ scheme approaches a constant as $\rho \to \infty$.

*Proof:* When $\rho \to \infty$, the receive beamformer in (44) converges to $\mathbf{w} \in \mathcal{N}(\mathbf{h}_{R,B})$ where $\mathcal{N}(\cdot)$ represents the null space operator. As a result, $I_R^{CJ} \to \frac{1}{2}\log_2(1+\rho\mathbf{h}_{A,R}^H\mathbf{h}_{A,R})$ and thus we have

$$\mathcal{P}_{out}^{CJ} \simeq \mathcal{P}\left\{\frac{\frac{\sum_{i=1}^K|h_{i,B}|^2\sum_{i=1}^K|h_{A,i}|^2}{\sum_{i=1}^K|h_{i,B}|^2+K\bar{\gamma}_{A,R}+K\bar{\gamma}_{R,B}}}{\sum_{i=1}^K|h_{A,i}|^2} < 2^{2R}\right\} \quad (46)$$

which is a nonzero constant independent of $\rho$. ∎

Recall from the previous section that unlike the above corollary, when $K = 1$ the SOP of CJ converges to zero, which indicates a more favorable scenario for using CJ. Clearly, this is due to the fact that a relay with multiple antennas is able to suppress the jamming signal from Bob. This point is formalized in the following corollary.

*4) Corollary 3:* The secrecy outage probability of the CJ scheme approaches unity as the number of relay antennas grows: $\mathcal{P}_{out}^{CJ} \to 1$ as $K \to \infty$.

*Proof:* Using the Sherman-Morrison formula, we have

$$\left(\mathbf{h}_{R,B}\mathbf{h}_{R,B}^H+\frac{1}{\rho}\mathbf{I}_K\right)^{-1} = \rho\mathbf{I}_K - \rho^2\frac{\mathbf{h}_{R,B}\mathbf{h}_{R,B}^H}{1+\rho\|\mathbf{h}_{R,B}\|^2} \quad (47)$$

and thus (45) can be rewritten as

$$\begin{aligned}\mathcal{P}_{out}^{CJ} &= \mathcal{P}\left\{\frac{1+\rho\frac{\sum_{i=1}^K|h_{i,B}|^2\sum_{i=1}^K|h_{A,i}|^2}{\sum_{i=1}^K|h_{i,B}|^2+K\bar{\gamma}_{A,R}+K\bar{\gamma}_{R,B}+\frac{K}{\rho}}}{1-\rho^2\mathbf{h}_{A,R}\mathbf{G}\mathbf{h}_{A,R}^H+\rho\sum_{i=1}^K|h_{A,i}|^2} < 2^{2R}\right\} \\ &\overset{a}{\geq} \mathcal{P}\left\{\frac{1+\rho\sum_{i=1}^K|h_{A,i}|^2}{1-\rho^2\mathbf{h}_{A,R}\mathbf{G}\mathbf{h}_{A,R}^H+\rho\sum_{i=1}^K|h_{A,i}|^2} < 2^{2R}\right\} \quad (48)\end{aligned}$$

where $\mathbf{G} = \frac{\mathbf{h}_{R,B}\mathbf{h}_{R,B}^H}{1+\rho\|\mathbf{h}_{R,B}\|^2}$ and inequality (a) holds since $\frac{\sum_{i=1}^K|h_{i,B}|^2}{\sum_{i=1}^K|h_{i,B}|^2+K\bar{\gamma}_{A,R}+K\bar{\gamma}_{R,B}+\frac{K}{\rho}} \leq 1$. Since $\mathbf{G}$ is a unit-rank Hermitian matrix, it can be seen that $\mathbf{h}_{A,R}\mathbf{G}\mathbf{h}_{A,R}^H$ is exponentially distributed as $\exp(\frac{1}{\bar{\gamma}_{A,R}\lambda_G})$ where $\lambda_G$ is the largest eigenvalue of $\mathbf{G}$ and $\lim_{K\to\infty}\lambda_G = \frac{1}{\rho}$. Consequently, $\mathbf{h}_{A,R}\mathbf{G}\mathbf{h}_{A,R}^H$ is not a function of $K$ as $K \to \infty$. On the other hand, $\sum_{i=1}^K|h_{A,i}|^2$ is obviously an increasing function of $K$ and $\sum_{i=1}^K|h_{A,i}|^2 \to \infty$ as $K \to \infty$. Therefore, the lower bound in (48) approaches unity and the proof is complete. ∎

Corollarys 1 and 3 provide pessimistic conclusions regarding secrecy for an untrusted relay implementing beamforming with a large number of antennas. However, in the next section, we show that if the relay is forced to perform antenna selection (e.g., because it only has a single RF chain), under certain conditions an increase in the number of relay antennas actually improves secrecy. It is also worth noting that in this paper we adopt a relaying protocol where Alice does not transmit information signals to Bob in the second phase, and thus the conclusions obtained above may not hold for other relaying protocols, such as those where Alice can transmit signals in the second phase (e.g. Protocol III in [20]).

## IV. Secrecy With Relay Antenna Selection

In this section, we consider a scenario where the untrusted relay must perform antenna selection for receive and transmit, rather than beamforming. In particular, we assume the untrusted relay chooses the receive antenna with the largest channel gain for maximizing her wiretapping ability in the first hop, while still assisting Alice by using the best transmit antenna to forward the message to Bob in the second hop. Such behavior is consistent with a relay that is untrusted but not malicious. This follows a similar CSI-based antenna selection approach assumed in traditional relaying systems [3], [10], [12]. Since the relay loses the flexibility of using beamforming to cope with the artificial jamming signals, and since Bob is still able to enjoy a diversity benefit due to antenna selection, a secrecy performance improvement is expected for the CJ scheme. We will characterize the SOP for AF and CJ and study the impact of the number of relay antennas. We let $m$ and $n$ respectively denote the indices of the receive and transmit antenna used by the relay.

### A. Direct Transmission (DT)

In this scheme, the untrusted relay chooses the best antenna to wiretap the signal from Alice, and the resulting SOP can be found by a straightforward extension of (35), which in this case becomes

$$\mathcal{P}_{out}^{DT}(R) = \mathcal{P}\left\{\log_2\left(\frac{1+\rho|h_{A,B}|^2}{1+\rho|h_{A,m^*}|^2}\right) < R\right\}, \quad (49)$$

where $m^* = \arg\max_m\{|h_{A,m}|^2\}$. Assume $Z = |h_{A,B}|^2$, $Y = |h_{A,m}|^2$ and $Y^* = |h_{A,m^*}|^2$. Since $|h_{A,m^*}|^2$ increases as $K$ grows, it is obvious that $\mathcal{P}_{out}^{DT}(R) \to 1$ as $K \to \infty$. To obtain

the exact SOP, since $Z$ and $Y$ are both exponentially distributed, using the theory of order statistics [21] we have

$$p_{Y^*}(y) = \frac{K}{\bar{\gamma}_{A,R}} \sum_{n=0}^{K-1} \binom{K-1}{n} (-1)^n e^{-\frac{y}{\bar{\gamma}_{A,R}}(n+1)}. \quad (50)$$

Therefore, the SOP can be computed as

$$\begin{aligned}\mathcal{P}_{out}^{DT} &= \mathbb{E}_{Y^*}\left\{F_Z\left(\frac{2^R-1}{\rho} + 2^R Y^*\right)\right\} \\ &= 1 - K\sum_{n=0}^{K-1}\binom{K-1}{n}\frac{(-1)^n \bar{\gamma}_{A,B}}{2^R\bar{\gamma}_{A,R} + \bar{\gamma}_{A,B}(n+1)} \\ &\quad \times e^{-\frac{2^R-1}{\rho\bar{\gamma}_{A,B}}}. \end{aligned} \quad (51)$$

### B. Amplify-and-Forward (AF)

Here we consider two cases, one where the relay has Bob's CSI for the second hop, and one where it does not. The latter case corresponds to the scenario where Bob is a passive receiver or where he simply does not transmit training data to the relay.

*1) Relaying With Second-Hop CSI:* Similar to (13), the SOP of the AF scheme with antenna selection for a given secrecy rate $R$ is given by

$$\mathcal{P}_{out}^{AF}(R) = \mathcal{P}\left\{\frac{1}{2}\log_2\left(\frac{1+\rho|h_{A,B}|^2 + \rho\frac{|h_{n^*,B}|^2|h_{A,m^*}|^2}{|h_{n^*,B}|^2+\bar{\gamma}_{A,R}+\frac{1}{\rho}}}{1+\rho|h_{A,m^*}|^2}\right) < R\right\},$$

where the receive and transmit antennas on the relay are selected using the following criteria:

$$m^* = \arg\max_m \left\{|h_{A,m}|^2\right\} \quad (52)$$

$$n^* = \arg\max_n \left\{|h_{n,B}|^2\right\}. \quad (53)$$

These criteria are obtained assuming that the untrusted relay will maximize her SNR for wiretapping first with (52) and then consider offering assistance to Bob with (53). An exact expression for the SOP in this case is given by the following proposition.

*Proposition 4:* The secrecy outage probability for AF relaying with antenna selection can be expressed as

$$\begin{aligned}\mathcal{P}_{out}^{AF}(R) &= 1 - K^2\sum_{m=1}^{K}\sum_{n=1}^{K}\binom{K-1}{m}\binom{K-1}{n}(-1)^{m+n} \\ &\quad \times \frac{\bar{\gamma}_{A,B}}{(2^{2R}-1)\bar{\gamma}_{A,R} + \bar{\gamma}_{A,B}(n+1)} e^{-\frac{2^{2R}-1}{\rho\bar{\gamma}_{A,B}}} \\ &\quad \times \Big[\mu(\beta_n - 1)e^{\mu\beta_n(m+1)}\mathrm{Ei}\left(-\mu\beta_n(m+1)\right) \\ &\quad + \frac{1}{m+1}\Big] \end{aligned} \quad (54)$$

where $\mu = \frac{\bar{\gamma}_{A,R}+1/\rho}{\bar{\gamma}_{R,B}}$, $\beta_n = \frac{2^{2R}\bar{\gamma}_{A,R}+\bar{\gamma}_{A,B}(n+1)}{(2^{2R}-1)\bar{\gamma}_{A,R}+\bar{\gamma}_{A,B}(n+1)}$, $R$ is the target secrecy rate, and $\mathrm{Ei}(\cdot)$ is the exponential integral $\mathrm{Ei}(x) = \int_{-\infty}^{x} e^t t^{-1} dt$.

*Proof:* Define $X = |h_{A,B}|^2$, $Y = |h_{A,m}|^2$, $V = \frac{|h_{n,B}|^2}{|h_{n,B}|^2+\bar{\gamma}_{A,R}+1/\rho}$, $Y^* = |h_{A,m^*}|^2$, $V^* = \frac{|h_{n^*,B}|^2}{|h_{n^*,B}|^2+\bar{\gamma}_{A,R}+1/\rho}$, and note that the p.d.f. of $Y^*$ is given in (50). For V, using the Jacobian transformation, we have

$$p_V(v) = \frac{\bar{\gamma}_{A,R} + \frac{1}{\rho}}{\bar{\gamma}_{R,B}(1-v)^2} e^{-\frac{(\bar{\gamma}_{A,R}+1/\rho)v}{\bar{\gamma}_{R,B}(1-v)}},$$

and the p.d.f. of $V^*$ can be expressed using order statistics as

$$p_{V^*}(v) = \frac{K\mu}{(1-v)^2}\sum_{m=0}^{K-1}\binom{K-1}{m}(-1)^m e^{-\frac{\mu v}{1-v}(m+1)}, \quad (55)$$

where $\mu = \frac{\bar{\gamma}_{A,R}+1/\rho}{\bar{\gamma}_{R,B}}$. The proof of (54) is completed by inserting (50) and (55) into

$$P_{out}^{AF}(R) = \mathcal{P}\{Z < 2^{2R}\} = \mathbb{E}_{V^*}\left\{\mathbb{E}_{Y^*}\left\{F_{Z|Y^*,V^*}(2^{2R})\right\}\right\}$$

where $Z = \frac{1+\rho X+\rho V^* Y^*}{1+\rho Y^*}$. ∎

*Corollary 4:* The secrecy outage probability of AF relaying approaches unity as the number of relay antennas grows: $\mathcal{P}_{out}^{AF} \to 1$ as $K \to \infty$.

*Proof:* This corollary can be proved by showing that a lower bound for $\mathcal{P}_{out}^{AF}$ goes to 1 as $K \to \infty$. Following the notation in the proof of Proposition 4, we have

$$\begin{aligned}\mathcal{P}_{out}^{AF}(R) &= \mathcal{P}\left(\frac{1+\rho X+\rho V^*Y^*}{1+\rho Y^*} < 2^{2R}\right) \\ &\overset{a}{\geq} \mathcal{P}\left(\frac{1+\rho X+\rho Y^*}{1+\rho Y^*} < 2^{2R}\right) \quad (56) \\ &\overset{b}{\geq} \mathcal{P}\left(\frac{X}{Y^*} < 2^{2R}-1\right) \\ &= \mathcal{P}\left(\min_m\left\{\frac{|h_{A,B}|^2}{|h_{A,m}|^2}\right\} < 2^{2R}-1\right) \\ &\overset{c}{=} 1 - \left[1 - \frac{\bar{\gamma}_{A,R}(2^{2R}-1)}{\bar{\gamma}_{A,B}+\bar{\gamma}_{A,R}(2^{2R}-1)}\right]^K, \quad (57)\end{aligned}$$

where it is obvious that (57) converges to 1 as $K$ goes to $\infty$. Inequality (a) holds since $V^* \leq 1$. The fraction in (56) is a quasi-linear function of $\rho$, and is monotonically increasing with respect to $\rho$ since $X + Y^* \geq Y^*$; thus inequality (b) is obtained by letting $\rho \to \infty$. To obtain (c), we have used the result in (65) that

$$\mathcal{P}\left\{\frac{|h_{A,B}|^2}{|h_{A,m}|^2} \leq u\right\} = \frac{\bar{\gamma}_{A,R}u}{\bar{\gamma}_{A,B}+\bar{\gamma}_{A,R}u}.$$

∎

Corollary 4 shows that although both the relay and Bob receive diversity gain from an increasing number of relay antennas, the untrusted relay accrues a proportionally greater benefit to the detriment of the information confidentiality.

*2) Relaying Without Second-Hop CSI:* In this case, the relay is forced to choose a random antenna for the second hop transmission, and the exact SOP is simply a special case of (54):

$$\begin{aligned}P_{out}^{AF}(R) &= \mathbb{E}_V\left\{\mathbb{E}_{Y^*}\left\{F_{Z|Y^*,V}(2^{2R})\right\}\right\} \\ &= 1 - K\sum_{n=1}^{K}\binom{K-1}{n}(-1)^n \\ &\quad \times \frac{\bar{\gamma}_{A,B}\left[\mu(\beta_n-1)e^{\mu\beta_n}\mathrm{Ei}(-\mu\beta_n)+1\right]}{(2^{2R}-1)\bar{\gamma}_{A,R}+\bar{\gamma}_{A,B}(n+1)} e^{-\frac{2^{2R}-1}{\rho\bar{\gamma}_{A,B}}} \end{aligned} \quad (58)$$

where $\mu$ and $\beta_n$ were given in Proposition 4. It is obvious that the performance in this case is always worse than the case where the second-hop CSI is available. However, we will see below that for CJ, the lack of second-hop CSI can lead to improved secrecy.

### C. Cooperative Jamming (CJ)

The relay's antenna selection protocol is slightly different in this case since the relay must account for the interference from Bob in the first hop.

*1) Relaying With Second-Hop CSI:* We first consider the case where the relay possesses the CSI for the second-hop. Similar to (19), the corresponding SOP for the CJ protocol is given by

$$\mathcal{P}_{out}^{CJ}(R) = \mathcal{P}\left(\frac{1+\rho\frac{|h_{n^*,B}|^2|h_{A,m^*}|^2}{|h_{n^*,B}|^2+\bar{\gamma}_{A,R}+\bar{\gamma}_{R,B}+\frac{1}{\rho}}}{1+\frac{|h_{A,m^*}|^2}{|h_{m^*,B}|^2+\frac{1}{\rho}}} < 2^{2R}\right) \quad (59)$$

but in this case the receive and transmit antenna at the relay are selected by

$$m^* = \arg\max_m \left\{\frac{|h_{A,m}|^2}{|h_{m,B}|^2}\right\} \quad (60)$$

$$n^* = \arg\max_n \left\{|h_{n,B}|^2\right\}. \quad (61)$$

where (60) indicates that to improve its performance, the relay chooses its receive antenna to maximize the ratio of the power of Alice's signal to the power of Bob's jamming. It is difficult to exactly calculate the SOP in this case. However, it can still be observed that $\mathcal{P}_{out}^{CJ} \to 1$ as $K \to \infty$ since the denominator in (59) tends to increase with the growth of $K$, while the numerator in (59) is upper bounded by $1+\rho|h_{A,m^*}|^2$ which will not necessarily increase as $K$ grows. However, as explained next, a different conclusion is obtained if the relay does not possess Bob's CSI.

*2) Relaying Without Second-Hop CSI:* Here we assume that the relay has no information about $h_{R,B}$, which applies to the case where Bob transmits no training data to the relay, and jams only when Alice is transmitting so the relay cannot collect interference information. Alternatively, a more advanced training sequence design, such as the methods for discriminatory channel estimation in [22], [23], can be applied to prevent the relay from acquiring CSI from Bob. Thus, the relay uses the receive antenna with the largest channel gain during the first hop, and then uses either the same or some random antenna for transmission during the second hop. In this case, the SOP is given by a slightly different expression than (59):

$$\mathcal{P}_{out}^{CJ}(R) = \mathcal{P}\left(\frac{1+\rho\frac{|h_{m^*,B}|^2|h_{A,m^*}|^2}{|h_{m^*,B}|^2+\bar{\gamma}_{A,R}+\bar{\gamma}_{R,B}+\frac{1}{\rho}}}{1+\frac{|h_{A,m^*}|^2}{|h_{m^*,B}|^2+\frac{1}{\rho}}} < 2^{2R}\right) \quad (62)$$

where $m^* = \arg\max_m\{|h_{A,m}|^2\}$. Note that since $|h_{m^*,B}|^2$ is independent of $|h_{A,m^*}|^2$, it is equivalent to selecting the transmit antenna randomly. Therefore, following the result in Appendix C, we can compute the SOP as

$$\begin{aligned}\mathcal{P}_{out}^{CJ}(R) &= \mathcal{P}\left(\phi\left(|h_{m^*,B}|^2\right)|h_{A,m^*}|^2 < 2^{2R}-1\right)\\ &= \frac{1}{\bar{\gamma}_{R,B}}\int_0^t e^{-\frac{z}{\bar{\gamma}_{R,B}}}dz\\ &\quad+\frac{1}{\bar{\gamma}_{R,B}}\int_t^\infty\left[1-e^{-\frac{2^{2R}-1}{\bar{\gamma}_{A,R}\phi(z)}}\right]^K e^{-\frac{z}{\bar{\gamma}_{R,B}}}dz \quad (63)\\ &= \left(1-e^{-\frac{t}{\bar{\gamma}_{R,B}}}\right)\\ &\quad+\frac{1}{\bar{\gamma}_{R,B}}\sum_{n=0}^{K}\binom{K}{n}(-1)^n\int_t^\infty e^{-\frac{(2^{2R}-1)n}{\bar{\gamma}_{A,R}\phi(z)}-\frac{z}{\bar{\gamma}_{R,B}}}dz, \quad (64)\end{aligned}$$

where $\phi(z)$ and $t$ are provided in (74) and (77) respectively. According to (63) and (64), we can also give the following corollary.

*Corollary 5:* Without second-hop CSI at the relay, the SOP of the CJ scheme with antenna selection decreases as $K$ grows and converges to $1-e^{\frac{-t}{\bar{\gamma}_{R,B}}}$, where

$$t=\frac{(2^{2R}-1)}{2\rho}+\frac{\sqrt{(2^{2R}-1)^2+\rho 2^{2R+1}\left(\bar{\gamma}_{A,R}+\bar{\gamma}_{R,B}+\frac{1}{\rho}\right)}}{2\rho}.$$

This corollary indicates that if the second-hop CSI can be hidden from the relay, although the legitimate user loses the diversity benefits that come from transmit antenna selection, the overall secrecy performance is still improved since the relay loses the diversity gain due to cooperative jamming, while the legitimate user can still achieve a diversity gain from the first-hop antenna selection.

## V. Numerical Results

In this section, we present numerical examples of the outage performance for the DT, AF and CJ transmission schemes in both single-antenna and multi-antenna scenarios. The SOP is computed for various values of the transmit powers, average channel gains, and number of antennas. In all cases, the normalized target secrecy rate is set to $R = 0.1$ bits per channel use as assumed in [2], [3].

### A. Single-Antenna Case

Fig. 1 depicts the outage probability as a function of the transmit SNR $\rho$, assuming the average channel gains are $\bar{\gamma}_{A,B} = \bar{\gamma}_{A,R} = 0$ dB, $\bar{\gamma}_{R,B} = 5$ dB. The analytical SOP results for DT, AF and CJ are evaluated through (8), (14) and (20), and are seen to agree well with the simulations, exactly predicting the performance cross-over points. Ignoring the available relay link and treating it as a pure adversary as in DT is clearly suboptimal for medium to high SNR regimes. This figure shows that when $\rho \to \infty$, the outage probability converges to a constant for DT and AF while it goes to 0 for CJ,

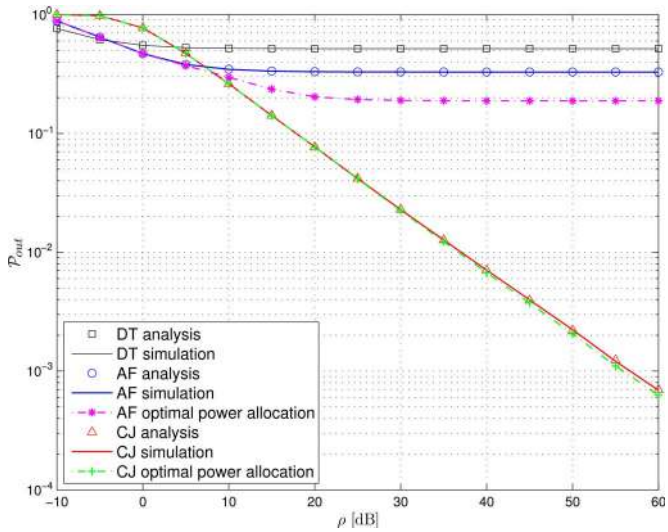


Fig. 1. Outage probability versus $\rho$, single antenna relay, $\bar{\gamma}_{A,B} = \bar{\gamma}_{A,R} = 0$ dB, $\bar{\gamma}_{R,B} = 5$ dB, analytical results computed with (8) for DT, (14) for AF, and (20) for CJ.

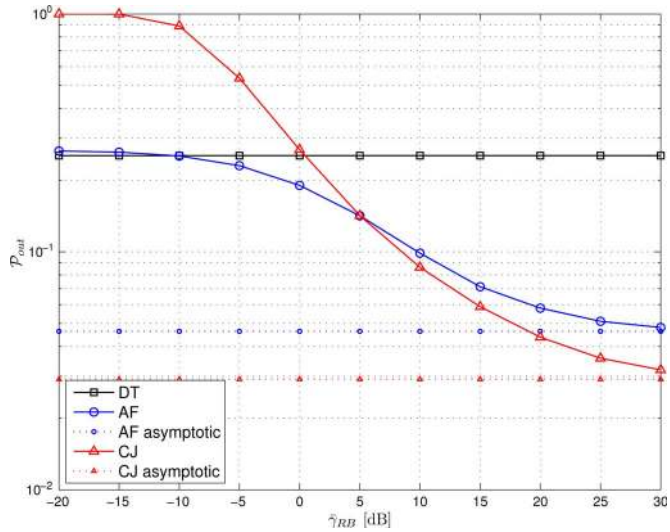


Fig. 2. Outage probability versus $\bar{\gamma}_{R,B}$, single-antenna relay, $\bar{\gamma}_{A,B} = 5$ dB, $\bar{\gamma}_{A,R} = 0$ dB, $\rho = 15$ dB, asymptotic results computed with (26) for AF, and (29) for CJ.

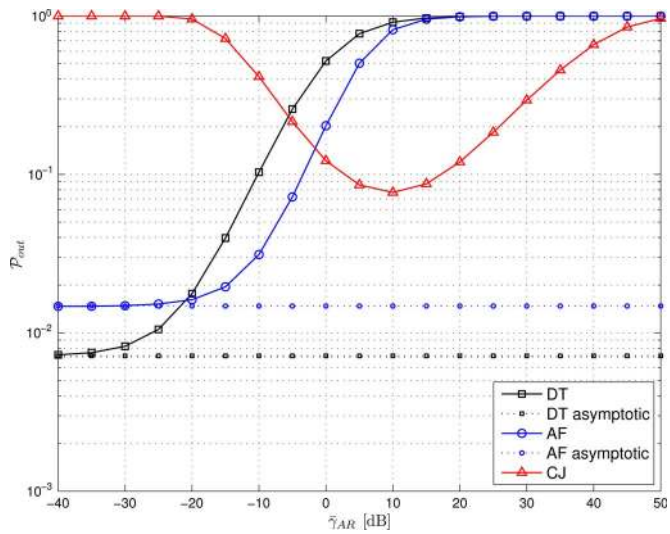


Fig. 3. Outage probability versus $\bar{\gamma}_{A,R}$, single-antenna relay, $\bar{\gamma}_{A,B} = 0$ dB, $\bar{\gamma}_{R,B} = 5$ dB, $\rho = 20$ dB, asymptotic results computed with (33) for DT, and (34) for AF.

which agrees with the discussion in Section III-B-1. This is due to the fact that the jamming signals from Bob only selectively interfere with the untrusted relay and have no impact on the overall two-hop data signal reception. Therefore, the outage performance for CJ is better than AF for high SNR, while the converse is true in the low SNR regime. We also show in this figure the SOPs for AF and CJ assuming an optimal power allocation obtained by direct numerical optimization. It can be seen that the performance gap between the fixed and optimal power allocations is more obvious for AF than for the CJ scheme, since AF utilizes the direct link between Alice and Bob and thus the secrecy performance is more sensitive to the power allocation. The figure also illustrates that the performance under the optimal power allocation still follows the asymptotic analysis conducted in Section III-B.

The impact of $\bar{\gamma}_{R,B}$ on performance is illustrated in Fig. 2, where $\bar{\gamma}_{A,B} = 5$ dB, $\bar{\gamma}_{A,R} = 0$ dB, and $\rho = 15$ dB. Observe that when $\bar{\gamma}_{R,B} \to 0$, the outage probability for CJ approaches 1, due to its sensitivity to the quality of the second hop, while the performance of both DT and AF converges to nonzero constant values. Although not obvious, DT still exhibits a gain over AF due to its efficient resource usage, as can be seen from (30) and (31). Note that from (31), we expect that this gain will increase with a higher target secrecy rate $R$. It is also worth noting that although this figure shows that CJ has the best performance as $\bar{\gamma}_{R,B} \to \infty$, the relative performance of these schemes will change with different values of $\bar{\gamma}_{A,R}$ and $\bar{\gamma}_{A,B}$, and thus we can not draw any definite conclusions in this asymptotic case.

Fig. 3 depicts the impact of the first hop channel gain $\bar{\gamma}_{A,R}$ on the outage performance, where $\bar{\gamma}_{A,B} = 0$ dB, $\bar{\gamma}_{A,R} = 5$ dB, and $\rho = 20$ dB. It is interesting to see that when $\bar{\gamma}_{A,R}$ is either extremely small or large, CJ approaches outage. This is because when $\bar{\gamma}_{A,R} \to \infty$, the untrusted relay is nearly colocated with Alice and secure transmission is impossible. On the other hand, when $\bar{\gamma}_{A,R} \to 0$, it is hard to establish a reliable relay link from Alice to Bob without the direct link, and thus the outage probability will also approach unity. Therefore, CJ can only achieve its best performance for in-between values of $\bar{\gamma}_{A,R}$. Again, our analysis allows the optimal operating regime for CJ to be determined. Also, as $\bar{\gamma}_{A,R} \to 0$, the asymptotic results validate the analytical expectations in (33) and (34) which predict that DT will asymptotically outperform AF. Therefore, the outage performance in Fig. 2 and Fig. 3 agrees with the analytical prediction in Section III-B-1 that DT is preferred when either relay hop is weak.

Fig. 4 shows the performance as a function of $\bar{\gamma}_{A,B}$, with $\bar{\gamma}_{A,R} = 2$ dB, $\bar{\gamma}_{R,B} = 10$ dB and $\rho = 10$ dB. It is shown that when $\bar{\gamma}_{A,B}$ is small, CJ is the best scheme since both DT and AF will be in outage. Conversely, with large $\bar{\gamma}_{A,B}$, the outage probability for DT and AF decays to 0. Moreover, as discussed

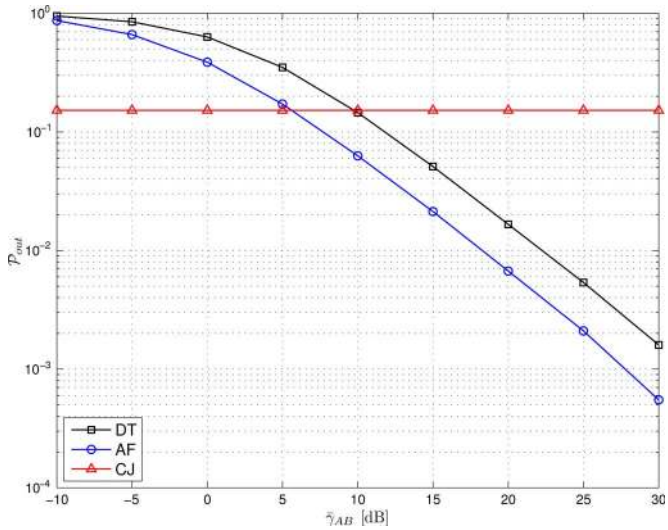


Fig. 4. Outage probability versus $\bar{\gamma}_{A,B}$, single-antenna relay, $\bar{\gamma}_{A,R} = 2$ dB, $\bar{\gamma}_{R,B} = 10$ dB, $\rho = 10$ dB.

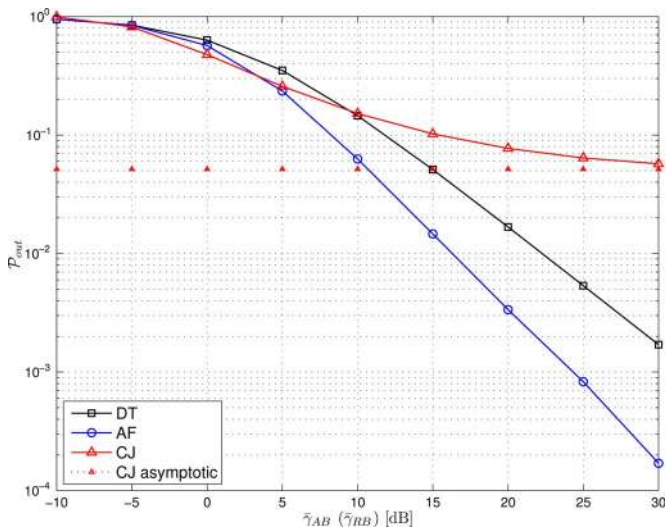


Fig. 5. Outage probability versus $\bar{\gamma}_{A,B}$, single-antenna relay, $\bar{\gamma}_{R,B} = \bar{\gamma}_{A,B}$, $\bar{\gamma}_{A,R} = 2$ dB, $\rho = 10$ dB, asymptotic results computed with (29).

in Section III-B-2, the outage probability for both DT and AF is seen to decay as $1/\bar{\gamma}_{A,B}$.

In Fig. 5, the outage performance is shown when $\bar{\gamma}_{A,B}$ and $\bar{\gamma}_{R,B}$ both increase simultaneously, where $\bar{\gamma}_{A,R} = 2$ dB and $\rho = 10$ dB. Note that since the performance of CJ does not depend on the direct link, the asymptotic SOP of CJ can still be characterized via (29), which indicates that the SOP of CJ will converge to a constant. On the other hand, we see that AF outperforms the other schemes since its outage probability decays to zero faster. This is due to the fact that when only $\bar{\gamma}_{A,B}$ increases, the outage probability of DT and AF decays with the same slope (see Fig. 4), and when $\bar{\gamma}_{R,B}$ also increases at the same time, AF will enjoy a better second hop channel (and thus the outage probability decays faster), which does not benefit DT.

### B. Multi-Antenna Case

Fig. 6 compares the multi-antenna SOP as a function of the number of relay antennas $K$ for average channel gains $\bar{\gamma}_{A,B} =$ 5 dB, $\bar{\gamma}_{A,R} = 0$ dB and $\bar{\gamma}_{R,B} = 10$ dB with $\rho = 30$ dB. As seen from the DT and AF curves, the exact analytical SOP for the multi-antenna scenario derived in (37) and (39) agrees very well with the simulations. When all available antennas are used at the untrusted relay, the figure shows that the SOPs of all schemes converge to unity as $K$ grows, as predicted in Section III-C. Moreover, we see that when $K$ changes from 1 to 2, the SOP of CJ increases rapidly, because multi-antenna receive beamforming at the relay can suppress the intentional interference from Bob, rendering CJ ineffective. Also, the performance achieved by an optimal power allocation is shown in the figure, and we see a slight reduction in the outage probability for both AF and CJ. Consistent with the result in Fig. 1, the performance gain of power allocation for CJ is not obvious when $K = 1$.

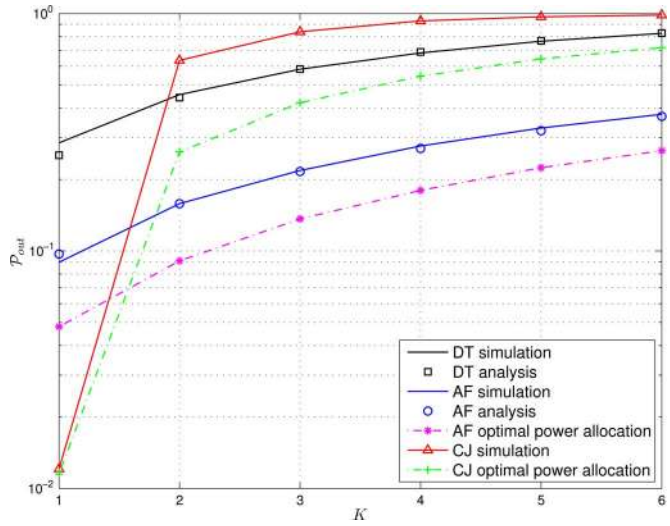


Fig. 6. Outage probability versus number of relay antennas, multi-antenna relay, $\bar{\gamma}_{A,B} = 5$ dB, $\bar{\gamma}_{A,R} = 0$ dB, $\bar{\gamma}_{R,B} = 10$ dB, $\rho = 30$ dB, analytical results computed with (37) for DT, (39) for AF.

The secrecy performance for various relaying schemes with antenna selection is shown in Figs. 7 and 8. In Fig. 7, the SOP is evaluated as a function of $\rho$ for $\bar{\gamma}_{A,B} = 5$ dB, $\bar{\gamma}_{A,R} = 0$ dB and $\bar{\gamma}_{R,B} = 5$ dB with six antennas employed at the relay. We see that the analytical results derived in (51), (54) and (64) respectively match the simulations for DT, AF and CJ without the second-hop CSI. The schemes with antenna selection show properties similar to those for a single-antenna relay in Fig. 1 as $\rho$ increases; i.e. the SOP of DT and AF converges to constants and that of CJ decays to zero. As expected, CJ with second-hop CSI decays to zero faster than CJ without CSI, since in the former approach the best transmit antenna at the relay is chosen, and such diversity gain is more obvious with larger $\rho$, as seen in the numerator of (59).

The SOP of relaying schemes with and without antenna selection for increasing $K$ is depicted in Fig. 8, and again we see that the SOP of DT and AF converges to unity. For both the AF and CJ schemes, the antenna selection schemes demonstrate lower SOP. This is due to the fact that the relay loses the array gain under antenna selection, and this gain is more beneficial to the relay than to Bob. We also see the significantly improved secrecy that results for CJ when the relay can

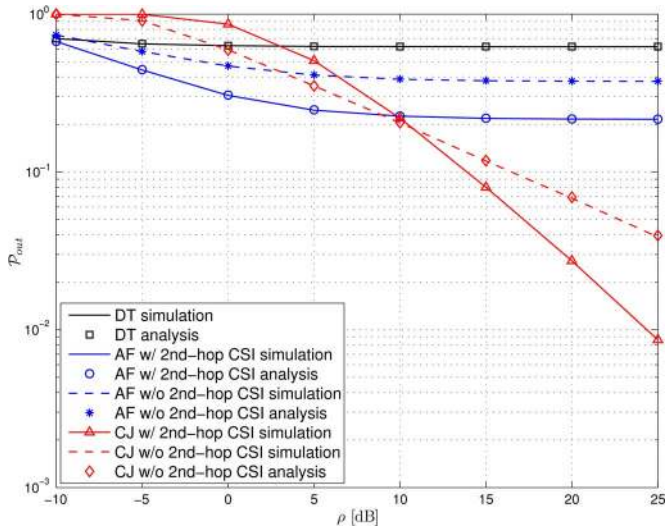


Fig. 7. Outage probability versus $\rho$, multi-antenna relay ($K = 6$) with antenna selection, $\bar{\gamma}_{A,B} = 5$ dB, $\bar{\gamma}_{A,R} = 0$ dB, $\bar{\gamma}_{R,B} = 5$ dB, analytical results computed with (51) for DT, (54) and (58) for AF, and (64) for CJ.

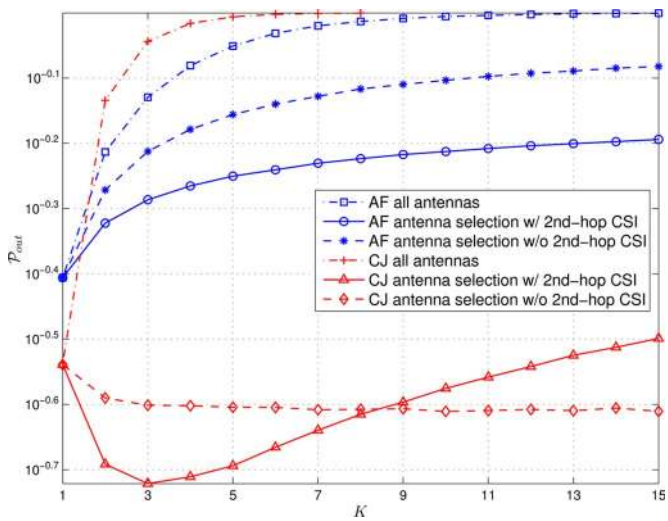


Fig. 8. Outage probability versus number of relay antennas, $\bar{\gamma}_{A,B} = \bar{\gamma}_{A,R} = 0$ dB, $\bar{\gamma}_{R,B} = 2$ dB, $\rho = 12$ dB.

only perform antenna selection instead of beamforming. Interestingly, the SOP of CJ with second-hop CSI decreases first and then gradually increases as the number of relay antennas grows. This is because the second-hop diversity gain at first outweighs the first-hop diversity for the relay, and then there is a diminishing marginal return for the second-hop with larger $K$ ($\frac{|h_{n^*,B}|^2}{|h_{n^*,B}|^2+\bar{\gamma}_{A,R}+\bar{\gamma}_{R,B}+\frac{1}{\rho}} \to 1$ as $K \to \infty$ in (59)) and the secrecy performance gradually degrades. However, when the relay does not have second-hop CSI, the SOP monotonically decreases with $K$ and converges to $1 - e^{-\frac{t}{\bar{\gamma}_{R,B}}}$, which validates Corollary 5. Therefore, for large $K$, in order to maintain confidentiality, CJ should be used with the second-hop CSI concealed from the untrusted relay.

## VI. Conclusions

This paper has analyzed a three-node network where the source can potentially utilize an untrusted multi-antenna relay to supplement the direct link to its destination. The untrusted relay is in effect an eavesdropper, although also assisting the source with cooperative transmission. We derived the exact secrecy outage probability of three different transmission policies: direct transmission without using the relay, conventional non-regenerative relaying, and cooperative jamming by the destination. The SOP computation allows performance transitions between the three algorithms to be determined for different scenarios. An asymptotic analysis of the outage probabilities is also conducted to elicit the optimal policies for different operating regimes. When the relay has a large number of antennas, we showed that the SOP for all three approaches converges to unity. However, when antenna selection is used at the relay, the secrecy performance for all schemes is improved, and the CJ scheme in particular can obtain a significant diversity gain with a moderate growth in the number of antennas. Moreover, if the destination conceals its CSI from the relay, secrecy will not be compromised as the antenna number grows. Our theoretical predictions were validated via various numerical examples.

## Appendix A
## Probability of Positive Secrecy Rate for AF

Assuming all channels $\gamma_{ij}$ are independent, define two random variables $U$ and $V$ as

$$U = \frac{|h_{A,B}|^2}{|h_{A,R}|^2}, \quad V = \frac{|h_{R,B}|^2}{|h_{R,B}|^2 + \bar{\gamma}_{A,R} + \frac{1}{\rho}}.$$

The c.d.f. of $U$ is given by

$$\begin{aligned} F_U(u) &= \mathcal{P}\left\{\frac{|h_{A,B}|^2}{|h_{A,R}|^2} \le u\right\} \\ &= \int_0^\infty \int_0^{yu} p_{|h_{A,B}|^2}(x) p_{|h_{A,R}|^2}(y) dx dy \\ &= \frac{\bar{\gamma}_{A,R} u}{\bar{\gamma}_{A,B} + \bar{\gamma}_{A,R} u}. \end{aligned} \tag{65}$$

Differentiating $F_U(u)$ with respect to $u$, we obtain the p.d.f. of $U$ as $p_U(u) = \frac{\bar{\gamma}_{A,B}\bar{\gamma}_{A,R}}{(\bar{\gamma}_{A,B}+\bar{\gamma}_{A,R}u)^2}$. For $V$, the c.d.f. is given by

$$\begin{aligned} F_V(v) &= \mathcal{P}\left\{\frac{|h_{R,B}|^2}{|h_{R,B}|^2 + \bar{\gamma}_{A,R} + \frac{1}{\rho}} \le v\right\} \\ &= \mathcal{P}\left\{|h_{R,B}|^2 \le g(v)\right\} \\ &= 1 - e^{-\frac{g(v)}{\bar{\gamma}_{R,B}}} \end{aligned} \tag{66}$$

where $g(v) = \frac{\bar{\gamma}_{A,R} + \frac{1}{\rho} v}{1-v}$. Differentiating $F_V(v)$ with respect to $v$, we have

$$p_V(v) = \frac{\bar{\gamma}_{A,R} + \frac{1}{\rho}}{(1-v)^2 \bar{\gamma}_{R,B}} e^{-\frac{(\bar{\gamma}_{A,R}+\frac{1}{\rho})v}{\bar{\gamma}_{R,B}(1-v)}}. \tag{67}$$

Next, we can calculate $\mathcal{P}_{pos}^{AF}$ as

$$\begin{aligned} \mathcal{P}_{pos}^{AF} &= \mathcal{P}\left\{\frac{|h_{A,B}|^2}{|h_{A,R}|^2} + \frac{|h_{R,B}|^2}{|h_{R,B}|^2 + \bar{\gamma}_{A,R} + \frac{1}{\rho}} > 1\right\} \\ &= \mathcal{P}\{U + V > 1\}. \end{aligned} \tag{68}$$

Since $U$ and $V$ are independent,

$$\begin{aligned}\mathcal{P}_{pos}^{AF} &= \int_0^1 \int_{1-v}^{\infty} p_{U,V}(u,v)dudv \\ &= \int_0^1 \int_{1-v}^{\infty} p_U(u)p_V(v)dudv \\ &= \int_0^1 \int_{1-v}^{\infty} \frac{\bar{\gamma}_{A,B}\bar{\gamma}_{A,R}\left(\bar{\gamma}_{A,R}+\frac{1}{\rho}\right)e^{-\frac{(\bar{\gamma}_{A,R}+\frac{1}{\rho})v}{\bar{\gamma}_{R,B}(1-v)}}}{\bar{\gamma}_{R,B}(\bar{\gamma}_{A,B}+\bar{\gamma}_{A,R}u)^2(1-v)^2}dudv \\ &= \mu_1 \int_0^{\infty} \frac{x+1}{x+\beta_1}e^{-\mu_1 x}dx \qquad (69) \\ &= \mu_1 \left[\int_0^{\infty} \frac{x}{x+\beta_1}e^{-\mu_1 x}dx + \int_0^{\infty} \frac{1}{x+\beta_1}e^{-\mu_1 x}dx\right] \\ &= \mu_1(\beta_1-1)e^{\mu_1\beta_1}\mathrm{Ei}(-\mu_1\beta_1)+1, \qquad (70)\end{aligned}$$

where in (69), we use the transformation $x = \frac{v}{1-v}$, $\mu_1 = \frac{\bar{\gamma}_{A,R}+\frac{1}{\rho}}{\bar{\gamma}_{R,B}}$ and $\beta_1 = 1+\frac{\bar{\gamma}_{A,R}}{\bar{\gamma}_{A,B}}$. Eq. (70) is obtained using the identity in [19eq. 3.353.5].

## Appendix B
## Proof of Proposition 1

Let $X = |h_{A,B}|^2$ and $Y = |h_{A,R}|^2$ be exponentially distributed random variables and define

$$\begin{aligned}Z &= \frac{1+\rho|h_{A,B}|^2+\rho\frac{|h_{R,B}|^2|h_{A,R}|^2}{|h_{R,B}|^2+\bar{\gamma}_{A,R}+\frac{1}{\rho}}}{1+\rho|h_{A,R}|^2}, \\ V &= \frac{|h_{R,B}|^2}{|h_{R,B}|^2+\bar{\gamma}_{A,R}+\frac{1}{\rho}},\end{aligned}$$

where the p.d.f. of $V$ is given by (67). We thus have

$$\begin{aligned}P_{out}^{AF} &= \mathcal{P}\left(\frac{1+\rho X+\rho YV}{1+\rho Y} < 2^{2R}\right) \\ &= \mathbb{E}_V\left\{\mathbb{E}_Y\left\{F_{Z|Y,V}(2^{2R})\right\}\right\} \\ &= 1-\frac{\bar{\gamma}_{A,R}+\frac{1}{\rho}}{\bar{\gamma}_{A,R}\bar{\gamma}_{R,B}}e^{-\frac{2^{2R}-1}{\rho\bar{\gamma}_{A,B}}} \\ &\quad \times \int_0^1 \int_0^{\infty} \frac{1}{(1-v)^2}e^{-\frac{(2^{2R}-v)y}{\bar{\gamma}_{A,B}}-\frac{y}{\bar{\gamma}_{A,R}}-\frac{(\bar{\gamma}_{A,R}+\frac{1}{\rho})v}{\bar{\gamma}_{R,B}(1-v)}}dydv \\ &= 1-\frac{\bar{\gamma}_{A,B}\left(\bar{\gamma}_{A,R}+\frac{1}{\rho}\right)}{\bar{\gamma}_{R,B}}e^{-\frac{2^{2R}-1}{\rho\bar{\gamma}_{A,B}}} \\ &\quad \times \int_0^1 \frac{1}{(2^{2R}\bar{\gamma}_{A,R}+\bar{\gamma}_{A,B}-\bar{\gamma}_{A,R}v)(1-v)^2} \\ &\quad \times e^{-\frac{\left(\bar{\gamma}_{A,R}+\frac{1}{\rho}\right)v}{\bar{\gamma}_{R,B}(1-v)}}dv \\ &= 1-\frac{\mu_1\bar{\gamma}_{A,B}e^{-\frac{2^{2R}-1}{\rho\bar{\gamma}_{A,B}}}}{(2^{2R}-1)\bar{\gamma}_{A,R}+\bar{\gamma}_{A,B}}\int_0^{\infty}\frac{x+1}{x+\beta_2}e^{-\mu_1 x}dx \qquad (71) \\ &= 1-\frac{\bar{\gamma}_{A,B}\left[\mu_1(\beta_2-1)e^{\mu_1\beta_2}\mathrm{Ei}(-\mu_1\beta_2)+1\right]}{(2^{2R}-1)\bar{\gamma}_{A,R}+\bar{\gamma}_{A,B}} \\ &\quad \times e^{-\frac{2^{2R}-1}{\rho\bar{\gamma}_{A,B}}} \qquad (72)\end{aligned}$$

where in (71), we use the transformation $x = \frac{v}{1-v}$, $\mu_1 = \frac{\bar{\gamma}_{A,R}+\frac{1}{\rho}}{\bar{\gamma}_{R,B}}$, $\beta_2 = \frac{2^{2R}\bar{\gamma}_{A,R}+\bar{\gamma}_{A,B}}{(2^{2R}-1)\bar{\gamma}_{A,R}+\bar{\gamma}_{A,B}}$, and the result in (69)–(70) is applied to obtain (72).

## Appendix C
## Proof of Proposition 2

The outage probability for a given secrecy rate $R$ is given by

$$\begin{aligned}\mathcal{P}_{out}^{CJ} &= \mathcal{P}\left(\frac{1+\rho\frac{|h_{R,B}|^2|h_{A,R}|^2}{|h_{R,B}|^2+\bar{\gamma}_{A,R}+\bar{\gamma}_{R,B}+\frac{1}{\rho}}}{1+\frac{|h_{A,R}|^2}{|h_{R,B}|^2+\frac{1}{\rho}}} < 2^{2R}\right) \\ &= \mathcal{P}\left(\phi\left(|h_{R,B}|^2\right)|h_{A,R}|^2 < 2^{2R}-1\right), \qquad (73)\end{aligned}$$

where

$$\phi(z) = \frac{\rho z}{z+\bar{\gamma}_{A,R}+\bar{\gamma}_{R,B}+\frac{1}{\rho}} - \frac{2^{2R}}{z+\frac{1}{\rho}}. \qquad (74)$$

Then, we have

$$\begin{aligned}\mathcal{P}_{out}^{CJ} &= \int_t^{\infty} F_{|h_{A,R}|^2}\left(\frac{2^{2R}-1}{\phi(z)}\right)p_{|h_{R,B}|^2}(z)dz \\ &\quad + \int_0^t \left[1-F_{|h_{A,R}|^2}\left(\frac{2^{2R}-1}{\phi(z)}\right)\right]p_{|h_{R,B}|^2}(z)dz \\ &= \int_t^{\infty}\left[1-e^{-\frac{2^{2R}-1}{\bar{\gamma}_{A,R}\phi(z)}}\right]p_{|h_{R,B}|^2}(z)dz \\ &\quad + \int_0^t p_{|h_{R,B}|^2}(z)dz \\ &= 1-\frac{1}{\bar{\gamma}_{R,B}}\int_t^{\infty} e^{-\frac{2^{2R}-1}{\bar{\gamma}_{A,R}\phi(z)}-\frac{z}{\bar{\gamma}_{R,B}}}dz \qquad (75)\end{aligned}$$

where

$$\phi(z)\begin{cases}\geq 0, & z \geq t \\ < 0, & 0 \leq z < t\end{cases} \qquad (76)$$

and

$$t = \frac{(2^{2R}-1)}{2\rho} + \frac{\sqrt{(2^{2R}-1)^2+\rho 2^{2R+1}\left(\bar{\gamma}_{A,R}+\bar{\gamma}_{R,B}+\frac{1}{\rho}\right)}}{2\rho}. \qquad (77)$$

## APPENDIX D
## PROOF OF LEMMA 1

Define $X = \rho\frac{|h_{R,B}|^2|h_{A,R}|^2}{|h_{R,B}|^2+\bar{\gamma}_{A,R}+\bar{\gamma}_{R,B}+\frac{1}{\rho}}$. The outage probability of CJ with $\bar{\gamma}_{R,B} \to \infty$ is written as

$$\begin{aligned}
&\lim_{\bar{\gamma}_{R,B}\to\infty} \mathcal{P}_{out}^{CJ} \\
&= \lim_{\bar{\gamma}_{R,B}\to\infty} \mathcal{P}\left(\frac{1+X}{1+\frac{|h_{A,R}|^2}{|h_{R,B}|^2+\frac{1}{\rho}}} < 2^{2R}\right) \\
&= \lim_{\bar{\gamma}_{R,B}\to\infty} \left\{ \mathcal{P}\left(\frac{1+X}{1+\frac{|h_{A,R}|^2}{|h_{R,B}|^2+\frac{1}{\rho}}} < 2^{2R} \middle| |h_{R,B}|^2 \geq \sqrt{\bar{\gamma}_{R,B}}\right)\right. \\
&\quad \times \mathcal{P}\left(|h_{R,B}|^2 \geq \sqrt{\bar{\gamma}_{R,B}}\right) \\
&\quad + \mathcal{P}\left(\frac{1+X}{1+\frac{|h_{A,R}|^2}{|h_{R,B}|^2+\frac{1}{\rho}}} < 2^{2R} \middle| |h_{R,B}|^2 < \sqrt{\bar{\gamma}_{R,B}}\right) \\
&\quad \left. \times \mathcal{P}\left(|h_{R,B}|^2 < \sqrt{\bar{\gamma}_{R,B}}\right) \right\}.
\end{aligned}$$

Since $|h_{R,B}|^2$ follows the exponential distribution, i.e. $|h_{R,B}|^2 \sim \exp(\frac{1}{\bar{\gamma}_{R,B}})$, we have $\lim_{\bar{\gamma}_{R,B}\to\infty} \mathcal{P}(|h_{R,B}|^2 \geq \sqrt{\bar{\gamma}_{R,B}}) = 1$ and $\lim_{\bar{\gamma}_{R,B}\to\infty} \mathcal{P}(|h_{R,B}|^2 < \sqrt{\bar{\gamma}_{R,B}}) = 0$. So the SOP of CJ is given by

$$\begin{aligned}
&\lim_{\bar{\gamma}_{R,B}\to\infty} \mathcal{P}_{out}^{CJ} \\
&= \lim_{\bar{\gamma}_{R,B}\to\infty} \mathcal{P}\left(\frac{1+X}{1+\frac{|h_{A,R}|^2}{|h_{R,B}|^2+\frac{1}{\rho}}} < 2^{2R} \middle| |h_{R,B}|^2 \geq \sqrt{\bar{\gamma}_{R,B}}\right).
\end{aligned}$$

Under the condition that $|h_{R,B}|^2 \geq \sqrt{\bar{\gamma}_{R,B}}$, we have

$$\frac{1+X}{1+\frac{|h_{A,R}|^2}{\sqrt{\bar{\gamma}_{R,B}}+\frac{1}{\rho}}} \leq \frac{1+X}{1+\frac{|h_{A,R}|^2}{|h_{R,B}|^2+\frac{1}{\rho}}} \leq 1+X$$

and consequently,

$$\begin{aligned}
&\mathcal{P}\left\{\frac{1+X}{1+\frac{|h_{A,R}|^2}{\sqrt{\bar{\gamma}_{R,B}}+\frac{1}{\rho}}} < 2^{2R}\right\} \\
&\quad \geq \mathcal{P}\left\{\frac{1+X}{1+\frac{|h_{A,R}|^2}{|h_{R,B}|^2+\frac{1}{\rho}}} < 2^{2R} \middle| |h_{R,B}|^2 \geq \sqrt{\bar{\gamma}_{R,B}}\right\} \\
&\quad \geq \mathcal{P}\{1+X < 2^{2R}\}. \qquad (78)
\end{aligned}$$

Because $\mathcal{P}\{\frac{1+X}{1+\frac{|h_{A,R}|^2}{\sqrt{\bar{\gamma}_{R,B}}+\frac{1}{\rho}}} < 2^{2R}\}$ is continuous with respect to $\bar{\gamma}_{R,B}$, which can be verified by showing that the function inside the probability integral is differentiable (results in Appendix C can be reused, but we skip the details here due to space constraints), we have

$$\begin{aligned}
&\lim_{\bar{\gamma}_{R,B}\to\infty} \mathcal{P}\left\{\frac{1+X}{1+\frac{|h_{A,R}|^2}{\sqrt{\bar{\gamma}_{R,B}}+\frac{1}{\rho}}} < 2^{2R}\right\} \\
&\qquad = \lim_{\bar{\gamma}_{R,B}\to\infty} \mathcal{P}\{1+X < 2^{2R}\}. \qquad (79)
\end{aligned}$$

Combining (78) and (79), the conclusion in Lemma 1 can be inferred and the proof is completed.

## REFERENCES


[1] Y. Liang, H. V. Poor, and S. Shamai, "Information theoretic security," *Found. Trends in Commun. Inf. Theory*, vol. 5, no. 4–5, pp. 355–580, 2008.

[2] 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.

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

[4] I. Krikidis, "Opportunistic relay selection for cooperative networks with secrecy constraints," *IET Commun.*, vol. 4, no. 15, pp. 1787–1791, Oct. 2010.

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

[6] Y. Oohama, "Coding for relay channels with confidential messages," in *Proc. IEEE Inf. Theory Workshop*, Sep. 2001, pp. 87–89.

[7] X. He and A. Yener, "Two-hop secure communication using an untrusted relay," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, pp. 1–13, 2009.

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

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

[10] G. Amarasuriya, C. Tellambura, and M. Ardakani, "Feedback delay effect on dual-hop MIMO AF relaying with antenna selection," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Dec. 2010, pp. 1–5.

[11] Y. Zhang, G. Zheng, C. Ji, K.-K. Wong, D. J. Edwards, and T. Cui, "Near-optimal joint antenna selection for amplify-and-forward relay networks," *IEEE Trans. Wireless Commun.*, vol. 9, no. 8, pp. 2401–2407, Aug. 2010.

[12] J.-B. Kim and D. Kim, "End-to-end BER performance of cooperative MIMO transmission with antenna selection in Rayleigh fading," in *Proc. 40th Asilomar Conf. Signals, Syst. Comput.*, Oct. 2006, pp. 1654–1657.

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

[14] E. Tekin and A. Yener, "The general gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

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

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

[17] J. Huang and A. L. Swindlehurst, "Robust secure transmission in MISO channels based on worst-case optimization," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 1696–1707, Apr. 2012.

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

[19] I. S. Gradshteyn and I. M. Ryzhik, *Tables of Integrals, Series, Products*, 7th ed. New York: Academic, 2007.

[20] R. Nabar, H. Bolcskei, and F. Kneubuhler, "Fading relay channels: Performance limits and space-time signal design," *IEEE J. Sel. Areas Commun.*, vol. 22, no. 6, pp. 1099–1109, Aug. 2004.

[21] A. Papoulis, *Probability, Random Variables, Stochastic Processes*, 4th ed. New York, NY, USA: McGraw-Hill, 2002.

[22] T.-H. Chang, W.-C. Chiang, Y.-W. Hong, and C.-Y. Chi, "Training sequence design for discriminatory channel estimation in wireless MIMO systems," *IEEE Trans. Signal Process.*, vol. 58, no. 12, pp. 6223–6237, Dec. 2010.

[23] C.-W. Huang, T.-H. Chang, X. Zhou, and Y. Hong, "Two-way discriminatory channel estimation for non-reciprocal wireless MIMO channels," in *Proc. 45th Asilomar Conf. Signals, Syst., Comput.*, Nov. 2011, pp. 202–206.

**Jing Huang** (S'10) received the B.S. degree in communication engineering from Jilin University, Changchun, China, in 2006, and the M.S. degree in communications and information systems from Beijing University of Posts and Telecommunications, Beijing, China, in 2009.

He is currently working towards the Ph.D. degree at the Department of Electrical Engineering and Computer Science, University of California, Irvine. He was an intern at Broadcom Corp., Sunnyvale, CA, during the spring and summer 2012. His research interests include cooperative communications, applied signal processing, and radio resource management in wireless networks.

**Amitav Mukherjee** (S'06–M'13) received the B.S. degree from the University of Kansas, Lawrence, in 2005, the M.S. degree from Wichita State University, Wichita, KS, in 2007, and the Ph.D. degree from the University of California, Irvine, in 2012, all in electrical engineering.

Dr. Mukherjee is currently with the Wireless Systems Research Laboratory of Hitachi America Ltd., Santa Clara, CA. From 2010 to 2012, he held internships with Qualcomm Inc., San Diego, CA; Mitsubishi Electric Research Labs (MERL), Cambridge, MA; Nokia Research Center, Helsinki, Finland; Intel Corporation, Santa Clara, CA; and Nokia Research Center, Berkeley, CA. His research interests encompass statistical signal processing and wireless communications, with more than 50 publications and eight pending patents in these areas.

Dr. Mukherjee received the Best Student Paper Award at SPAWC 2010, Marrakech, and has served as a TPC member for several IEEE Vehicular Technology Conferences.

**A. Lee Swindlehurst** (S'83–M'84–SM'99–F'04) received the B.S. (*summa cum laude*) and M.S. degrees in electrical engineering from Brigham Young University, Provo, UT, in 1985 and 1986, respectively, and the Ph.D. degree in electrical engineering from Stanford University, Stanford, CA, in 1991.

From 1986 to 1990, he was with ESL, Inc., Sunnyvale, CA, where he was involved in the design of algorithms and architectures for several radar and sonar signal processing systems. He was on the faculty of the Department of Electrical and Computer Engineering, Brigham Young University, from 1990 to 2007, where he was a Full Professor and served as Department Chair from 2003 to 2006. During 1996–1997, he held a joint appointment as a visiting scholar at both Uppsala University, Uppsala, Sweden, and at the Royal Institute of Technology, Stockholm, Sweden. From 2006 to 2007, he was on leave working as Vice President of Research for ArrayComm LLC , San Jose, CA. He is currently a Professor of Electrical Engineering and Computer Science at the University of California at Irvine. His research interests include sensor array signal processing for radar and wireless communications, detection and estimation theory, and system identification. He has more than 200 publications in these areas.

Dr. Swindlehurst is a past Secretary of the IEEE Signal Processing Society, past Editor-in-Chief of the IEEE JOURNAL OF SELECTED TOPICS IN SIGNAL PROCESSING, and past member of the Editorial Boards for the *EURASIP Journal on Wireless Communications and Networking*, IEEE SIGNAL PROCESSING MAGAZINE, and the IEEE TRANSACTIONS ON SIGNAL PROCESSING. He is a recipient of several paper awards: the 2000 IEEE W. R. G. Baker Prize Paper Award, the 2006 and 2010 IEEE Signal Processing Society's Best Paper Award, the 2006 IEEE Communications Society Stephen O. Rice Prize in the Field of Communication Theory, and is coauthor of a paper that received the IEEE Signal Processing Society Young Author Best Paper Award in 2001.