On the Equivocation Region of Relay Channels with Orthogonal Components

Xiang He   Aylin Yener
Wireless Communications and Networking Laboratory
Electrical Engineering Department
The Pennsylvania State University, University Park, PA 16802
xxh119@psu.edu   *yener@ee.psu.edu*

***Abstract*—We consider the secrecy rate of a relay network where an eavesdropper is co-located with the relay node. This exemplifies a scenario where the relay node is not malicious by nature, but is located in an "untrusted region", and hence is potentially compromised. Given that the aim now is to keep the relay node completely oblivious to the information sent from the source to the destination, an interesting question is whether the relay node should be deployed at all. We investigate this question for two types of relay networks with orthogonal components. For the first model, we find the equivocation capacity region and prove the relay node should not be deployed. For the second model, we present an achievable secrecy rate based on compress-and-forward, and conclude that the relay node is potentially useful as it can, without being able to decode the source data, facilitate secret communication between the source and the destination that would not be possible without the relay.**

I. Introduction

As the radio channel continues to become the primary communication medium of choice, the challenges associated with wireless communication become more important to overcome for designers and researchers alike. Among the most prevalent of these challenges is to provide secure information transfer. A fundamental approach to this problem is founded in information theory, where limits of reliable communication can be determined while keeping the information secret from the eavesdropping node(s). The secrecy measure is defined as the entropy rate of the transmitted message conditioned on the signals received by the eavesdropper. Wyner in [1] defined the notion secrecy capacity and the equivocation capacity region, i.e., the region defined by the reliable transmission rates and secrecy measures, and found the secrecy capacity of a point-to-point discrete memoryless channel where an eavesdropper (wire-tapper) gets a degraded copy of the received signal. A significant research effort followed this work, most of which are recent work that concentrate on more complicated system models inspired by wireless communication scenarios; see [2] and references therein.

In contrast to what is desired in information theoretic secrecy, cooperative communication [3] encourages sharing information. Cooperation, which emerged as a new paradigm that is particularly useful and necessary for wireless networks, enables nodes help each other by relaying messages. Intuitively, one might expect a trade-off between providing secrecy and employing cooperative communication techniques. In particular, one might easily envision a scenario where sources may wish to be helped by relays in order to better reach their destinations, but may also wish that the relaying nodes stay oblivious to the information they are sending. The simplest such scenario, first proposed by Oohama [4], is a classical three-node relay network where the relay node is also the eavesdropper from whom the information is to be kept secret. In addition, several references have considered the relay channel where the eavesdropper is an external node [5]–[7]. In reference [4], an achievable rate is given based on partial decode and forward [8]. It was shown that a non-zero secrecy rate is *not* possible for the *degraded* relay network [9].

In this work, we revisit the model in [4] where the relay is also the eavesdropper and ask the following question: With the eavesdropper knowing everything the relay knows, should the relay node be deployed at all? The question arises naturally since the current state-of-the-art provides a non-zero secrecy rate for the relay network by simply not using the relay-to-destination link.

We investigate this question for two types of relay networks with orthogonal components proposed in [10] and [11] respectively. The system models are described in Section II. In Section III, we find the equivocation rate region for the first model and show that the relay node *is not* useful in achieving non-zero secrecy rate and consequently should not be deployed. In Section IV, we consider the second model, provide a non-zero secrecy rate based on compress-and-forward, and show that this rate may not be achievable without the relay-destination link. Thus, for this model, we conclude that the relay node *is* actually useful, while being completely oblivious to the information transfered from the source to the destination.

II. System Model and the Equivocation Region

The two models of the relay network with orthogonal components are depicted in Figures 1 and 2 respectively. In model 1, the relay and the source communicate with the destination via a multiple access channel, with its input being X_D, X_r and output being Y. The source and the relay communicate via a channel orthogonal to the channel used by the source and the relay to transmit to the destination. The input and the output of this channel are denoted by X_R and Y_r respectively.

978-1-4244-2110-7/08/$25.00 ©2007 IEEE

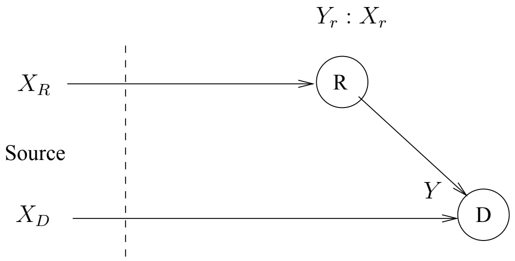

Fig. 1. Relay Channel with Orthogonal Components: Model 1

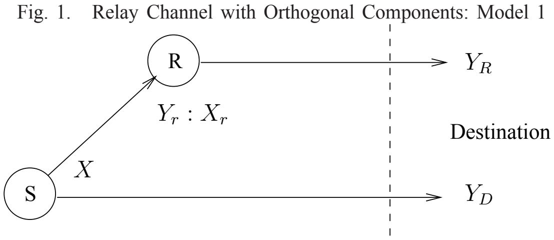

Fig. 2. Relay Channel with Orthogonal Components: Model 2

Thus, the overall channel description is:

$$p\left(Y_r, Y|X_R, X_D, X_r\right) = p\left(Y|X_D, X_r\right) p\left(Y_r|X_R, X_r\right) \quad (1)$$

The capacity of this network without the secrecy constraint was found in [10].

As shown in Figure 2, for Model 2, the source communicates with the relay and the destination via a broadcast channel, and the relay communicates with the destination via a separate (orthogonal) link. Thus, we have:

$$p\left(Y_D, Y_R, Y_r|X, X_r\right) = p\left(Y_r, Y_D|X\right) p\left(Y_R|X_r\right) \quad (2)$$

This network is dual to Model 1 in structure. However, its capacity remains an open problem except for some special cases given in [12].

For both models, we assume that there is an eavesdropper at the relay node, with perfect knowledge of the signal Y_r and X_r. The message sent by the source to the destination is W, which is transmitted over n channel uses. The message decoded by the destination is $\hat{W}$. The equivocation rate region is defined by all rate pairs (R_1, R_e) described by:

$$\begin{aligned}
&R_1 = \lim_{n\to\infty} \frac{1}{n} \log|W| \\
&R_e = \lim_{n\to\infty} \frac{1}{n} H\left(W|X_r^n, Y_r^n\right) = \lim_{n\to\infty} \frac{1}{n} H\left(W|Y_r^n\right) \\
&\text{s.t.} \lim_{n\to\infty} \frac{1}{n} \Pr\left(W \neq \hat{W}\right) = 0
\end{aligned}$$

Here $|W|$ is the cardinality of the message set W. X_r^n and Y_r^n are the signals transmitted and received by the relay over n channel uses respectively. $W \to Y_r^n \to X_r^n$ forms a Markov chain because the processing done at the relay is independent from the transmitted message W, given the received signal at the relay.

III. Equivocation Capacity Region of Model 1

Theorem 1: The equivocation region is given by

$$\bigcup_{\substack{p(X_r)\\ p(X_D|X_r)\\ p(X_R|X_r)}} \left\{ \begin{array}{l} (R_1, R_e): \\ 0 \le R_1 \le \min \left\{ \begin{array}{l} I\left(X_D, X_r; Y\right), \\ I\left(X_R; Y_r|X_r\right) \\ +I\left(X_D; Y|X_r\right) \end{array} \right\} \\ 0 \le R_e \le \min\{I\left(Y; X_D|X_r\right), R_1\} \end{array} \right\} \quad (3)$$

Proof: The converse for R_1 is given in [10] using the cut set bound. The converse for R_e follows from the observation: $H\left(W|X_r^n, Y_r^n\right) \le H\left(W|X_r^n\right)$. Therefore, we consider the same network in which the wiretapper only knows the transmitted signal X_r^n of the relay, but not its received signal Y_r^n. Next we combine the relay node with the source node and the model becomes a wiretap channel as in [1] with X_D, X_r as input, and X_r is known by the relay node. Since any communication scheme feasible for the old network is also feasible for the new network, R_e for the new network cannot be smaller than R_e for the old network. Finally, the following well-known outer bound (4) [13, Equation (57)] [14, section V, lemma 1] is used to bound R_e, where Y is the received signal by the destination, Y_e is the received signal by the eavesdropper. Substituting X_r for Y_e and X_D, X_r for X, we get the desired result.

$$R_e \le I\left(X; Y|Y_e\right) = I\left(X_D X_r; Y|X_r\right) = I\left(X_D; Y|X_r\right) \quad (4)$$

Achievability follows from the partial decode and forward scheme in [4, Theorem 1]. Reference [4] states the rate region (5) below is achievable for a general relay network with conditional probability $p(Y_1, Y|X_1, X_2)$, where X_1,X_2 are the signals transmitted by the source and the relay respectively. Y_1,Y are the signals received by the relay and the destination respectively. R_0 is the rate of information that must be correctly received by both the relay and the destination. The auxiliary random variable U decides how much information the relay could decode.

$$\bigcup_{\substack{p(U,X_1,X_2)\\ p(Y_1,Y|X_1,X_2)}} \left\{ \begin{array}{l} R_0 \le \min\{I\left(U; Y_1|X_2\right), I\left(U, X_2; Y\right)\} \\ R_1 + R_0 \le I\left(X_1; Y|UX_2\right) \\ +\min\{I\left(U; Y_1|X_2\right), I\left(U, X_2; Y\right)\} \\ R_e \le \left[I\left(X_1; Y|UX_2\right) - I\left(X_1; Y_1|UX_2\right)\right]^+ \\ 0 \le R_e \le R_1 \end{array} \right\} \quad (5)$$

In (5), we let $R_0 = 0, X_1 = X_D, X_R, U = X_R, Y_1 = Y_r, X_2 = X_r$, and restrict the union to be over the probability distributions of the form $p(X_r)p(X_D|X_r)p(X_R|X_r)$, and we obtain:

$$\begin{aligned}
&I\left(X_1; Y|UX_r\right) - I\left(X_1; Y_1|UX_r\right) && (6)\\
=&I\left(X_R X_D; Y|X_R X_r\right) - I\left(X_R X_D; Y_r|X_R X_r\right) && (7)\\
=&I\left(X_D; Y|X_R X_r\right) - I\left(X_D; Y_r|X_R X_r\right) && (8)
\end{aligned}$$

$$\begin{aligned} =&H\left(Y|X_R X_r\right) - H\left(Y|X_D X_R X_r\right) \\ &- I\left(X_D;Y_r|X_R X_r\right) \end{aligned} \tag{9}$$

$$\overset{(a)}{=}H\left(Y|X_r\right) - H\left(Y|X_D X_r\right) - I\left(X_D;Y_r|X_R X_r\right) \tag{10}$$

$$=I\left(X_D;Y|X_r\right) - I\left(X_D;Y_r|X_R X_r\right) \tag{11}$$

$$\overset{(b)}{=}I\left(X_D;Y|X_r\right) \tag{12}$$

where step (a) follows from $X_R \rightarrow X_r \rightarrow Y$ being a Markov chain [10] and $X_R \rightarrow X_r X_D \rightarrow Y$ being a Markov chain. Step (b) follows from $X_D \rightarrow X_R X_r \rightarrow Y_r$ being a Markov chain [10]. Moreover, the bound on R_1 can be expressed as:

$$I\left(X_1;Y|UX_2\right) + \min\{I\left(U;Y_1|X_2\right), I\left(U,X_2;Y\right)\} \tag{13}$$

$$=\min\left\{\begin{array}{l} I\left(UX_1X_2;Y\right), \\ I\left(U;Y_1|X_2\right) + I\left(X_1;Y|UX_2\right) \end{array}\right\} \tag{14}$$

$$\overset{(c)}{=}\min\left\{\begin{array}{l} I\left(X_1X_2;Y\right), \\ I\left(U;Y_1|X_2\right) + I\left(X_1;Y|UX_2\right) \end{array}\right\} \tag{15}$$

where step (c) follows from $U \rightarrow X_1X_2 \rightarrow Y$ being a Markov chain.

Note that (15) is the same as Equation (2) in [10], therefore from the same argument therein, we obtain:

$$\min\left\{\begin{array}{l} I\left(X_1X_2;Y\right), \\ I\left(U;Y_1|X_2\right) + I\left(X_1;Y|UX_2\right) \end{array}\right\} \tag{16}$$

$$=\min\left\{\begin{array}{l} I\left(X_D,X_r;Y\right), \\ I\left(X_R;Y_r|X_r\right) + I\left(X_D;Y|X_r\right) \end{array}\right\} \tag{17}$$

By substituting (17) and (12) into (5), we find that the rate pair in (3) is achievable. ■

Remark 1: It is shown in [4, Lemma 3] that the achievable rate region (5) is convex. Therefore the rate region of (3) is also convex.

Remark 2: By letting $R_e = R_1$, we obtain the secrecy capacity of the network given by (18).

$$S = \max_{p(X_r)p(X_D|X_r)} I\left(Y;X_D|X_r\right) \tag{18}$$

$$= I\left(Y;X_D|X_r = x_r\right) \tag{19}$$

It is readily seen that in this case the relay to destination link is not useful. On the other hand, if $R_e < R_1$, from the coding scheme it can shown the secret information is only mapped to signal transmitted via X_D, which means the secret information should not pass through the relay node. These two observations combined lead to the conclusion that the relay-to-destination link is indeed *not useful* in improving the secrecy rate of the system.

A direct extension of the above result can be readily made to the Gaussian case. [1] The channel is defined as [10]:

$$Y_r = aX_R + Z_1, \quad Y = bX_r + X_D + Z \tag{20}$$

where Z_1 and Z are independent zero mean real Gaussian random variables with variance N. The transmit power constraints on the source and the relay are given by:

$$\frac{1}{n}\sum_{i=1}^{n}\left(X_{R,i}^2 + X_{D,i}^2\right) \leq P, \quad \frac{1}{n}\sum_{i=1}^{n} X_{r,i}^2 \leq \gamma P \tag{21}$$

Corollary 1: For the Gaussian relay network described above, the equivocation region is given by (22).

$$\bigcup_{0\leq v,\rho\leq 1}\left\{\begin{array}{l} R_1 \leq \min\left\{\begin{array}{l} C\left(\frac{(v+b^2\gamma+2b\rho\sqrt{v\gamma})P}{N}\right), \\ C\left(\frac{a^2(1-v)P}{N}\right) \\ \quad +C\left(\frac{v\left(1-\rho^2\right)P}{N}\right) \end{array}\right\} \\ 0 \leq R_e \leq \min\{C\left(\frac{v\left(1-\rho^2\right)P}{N}\right), R_1\} \end{array}\right\} \tag{22}$$

where $C(x) = \frac{1}{2}\log(1+x)$.

Proof: The proof is the same as in reference [10, Section III]. The three terms: $I(X_D,X_r;Y), I(X_R;Y_r|X_r), I(X_D;Y|X_r)$ are maximized simultaneously when X_r, X_D, X_R are chosen to be zero mean and jointly Gaussian with the following parameters: $Var[X_r] = \gamma P, Var[X_R] = (1-v)P, Var[X_D] = vP, E[X_rX_D] = \rho P\sqrt{v\gamma}, E[X_RX_D] = 0$. ■

IV. An Achievable Region for Model 2

In this section, we first derive an achievable region for the general relay network under compress-and-forward scheme, then specialize it to the second type of relay network.

Theorem 2: For a relay network with conditional distribution $p(Y,Y_r|X,X_r)$, with X, X_r being the input from the source and the relay respectively, and Y_r,Y being the signals received by the relay and the destination respectively, the following region of rate pairs (R_1,R_e) is achievable.

$$\bigcup\left\{\begin{array}{ll} R_e \leq R_1 \leq & I\left(X;Y\hat{Y}_r|X_r\right) \\ 0 \leq R_e \leq & [I\left(X;Y\hat{Y}_r|X_r\right) - I\left(X,Y_r|X_r\right)]^+ \end{array}\right\} \tag{23}$$

where $I(X_r;Y) > I(\hat{Y}_r;Y_r|YX_r)$ and the union is taken over $p(X)p(X_r)p(Y,Y_r|X,X_r)p(\hat{Y}_r|Y_r,X_r)$.

Proof: The coding scheme uses the compress-and-forward scheme in [9, Theorem 6] with the codebook used by the source node being further binned randomly to several groups. Suppose there are 2^{nC} groups, each containing 2^{nB} codewords. Correspondingly, the codeword transmitted as the kth block is indexed by label b_k, c_k. Suppose $W_1(k)$ is the message transmitted by the source at the kth block. Let $R_1 = \log|W_1(k)|/n$. Then the messages are mapped to the codebook as follows.

1) If $R_1 > C$, c_k is the group index determined from $W_1(k)$. The codewords in group c_k are partitioned into $2^{n(R_1-C)}$ subsets. The subset is chosen according to the unmapped part of $W_1(k)$. Then b_k is selected from this chosen subset according to a uniform distribution.

[1] Proofs follow by replacing entropy with differential entropy whenever necessary.

2) If $R_1 \leq C$, c_k is still determined by $W_1(k)$. b_k is randomly chosen from group c_k according to a uniform distribution.

Based on this mapping ,we can lower bound the equivocation rate as follows.

$$
\begin{aligned}
& H\left(W_1\left(k\right)|Y_r^n\left(k\right), X_r^n(k)\right) && (24)\\
=& H\left(W_1\left(k\right), Y_r^n\left(k\right)|X_r^n(k)\right) - H\left(Y_r^n\left(k\right)|X_r^n(k)\right) && (25)\\
=& H\left(W_1\left(k\right), Y_r^n\left(k\right), X^n\left(k\right)|X_r^n(k)\right)\\
& - H\left(X^n\left(k\right)|X_r^n(k), W_1\left(k\right), Y_r^n\left(k\right)\right)\\
& - H\left(Y_r^n\left(k\right)|X_r^n(k)\right) && (26)\\
=& H\left(W_1\left(k\right), X^n\left(k\right)|X_r^n(k)\right)\\
& + H\left(Y_r^n\left(k\right)|W_1\left(k\right), X_r^n(k), X^n\left(k\right)\right)\\
& - H\left(X^n\left(k\right)|X_r^n(k), W_1\left(k\right), Y_r^n\left(k\right)\right)\\
& - H\left(Y_r^n\left(k\right)|X_r^n(k)\right) && (27)\\
\geq& H\left(X^n\left(k\right)|X_r^n(k)\right) + H\left(Y_r^n\left(k\right)|X_r^n(k), X^n\left(k\right)\right)\\
& - H\left(X^n\left(k\right)|X_r^n(k), W_1\left(k\right), Y_r^n\left(k\right)\right)\\
& - H\left(Y_r^n\left(k\right)|X_r^n(k)\right) && (28)
\end{aligned}
$$

We proceed to bound each of the four terms in (28). We use $\delta_n, \delta'_n, \delta''_n, \delta'''_n$ for variables converging to zero when $n \to \infty$.

1) $H(X^n(k)|X_r^n(k)) = H(X^n(k)) = n(B + min\{C, R_1\}) + n\delta_n$. The first equality comes from the fact that $X_r^n(k)$ is computed from blocks received before k and therefore is independent from $X^n(k)$. The second equality comes from the mapping.
2) $H(Y_r^n(k)|X_r^n(k), X^n(k)) = nH(Y_r|X_r, X) + n\delta'_n$. This follows from the fact the channel is memoryless and the codebook is composed of i.i.d sequences.
3) To bound the 3rd term, first we notice c_k is decided by $W_1(k)$. We proceed to impose the following condition on B:

$$B \leq I(X; Y_r|X_r) \qquad (29)$$

If this constraint is met, the eavesdropper can estimate b_k from the following set: $\{b : X^n(b, c_k), Y_r^n(k), X_r^n(k)$ are jointly typical$\}$. This set should contain only b_k with probability close to 1. From Fano's inequality, we have $H(X^n(k)|X_r^n(k), W_1(k), Y_r^n(k)) = n\delta''_n$.
4) $H(Y_r^n(k)|X_r^n(k)) = nH(Y_r|X_r) + n\delta'''_n$ Again this follows from the fact the codewords are constructed with i.i.d sequences and the channel is memoryless.

By substituting these results into (28), we get

$$
\begin{aligned}
& H\left(W_1\left(k\right)|Y_r^n\left(k\right), X_r^n\left(k\right)\right) && (30)\\
\geq& n(B + \min\left\{C, R_1\right\}) - nH\left(Y_r|X_r X\right)\\
& + nH\left(Y_r|X_r\right) + n\epsilon_n && (31)\\
=& n\left(B + \min\left\{C, R_1\right\}\right) - nI\left(Y_r; X|X_r\right) + n\epsilon_n && (32)
\end{aligned}
$$

where $\epsilon_n = \delta_n + \delta'_n - \delta''_n + \delta'''_n \to 0$ as $n \to \infty$.

If $R_1 \leq C$, then (32) leads to:

$$
\begin{aligned}
& 0 \leq R_e \leq B + R_1 - I\left(X; Y_r|X_r\right)\\
& 0 \leq R_1 \leq C
\end{aligned}
\qquad (33)
$$

where (B, C) is within the region defined by:

$$
\left\{
\begin{array}{l}
B + C \leq I\left(X; Y, \hat{Y}_r|X_r\right)\\
0 \leq B \leq I\left(X; Y_r|X_r\right), 0 \leq C
\end{array}
\right\}
\qquad (34)
$$

If $C \leq R_1 \leq B + C$, then (6) becomes (35). Again (B, C) must be within the region defined by (34).

$$
\begin{aligned}
& 0 \leq R_e \leq B + C - I\left(X; Y_r|X_r\right)\\
& C \leq R_1 \leq B + C
\end{aligned}
\qquad (35)
$$

Finally, (33) and (35) can be shown to be the region given by:

$$
\begin{aligned}
& R_e \leq R_1 \leq I\left(X; Y, \hat{Y}_r|X_r\right)\\
& 0 \leq R_e \leq I\left(X; Y, \hat{Y}_r|X_r\right) - I\left(X; Y_r|X_r\right)
\end{aligned}
\qquad (36)
$$

where the constraint $I(X_r; Y) > I(\hat{Y}_r; Y_r|Y X_r)$ is due to compress-and-forward. ■

Remark 3: Achievable rates using compress-and-forward scheme under secrecy constraints have been given in references [5] and [6]. However, in these models, the wiretapper and the eavesdropper are not co-located which brings difficulty to bounding the equivocation rate. The current state-of-art addresses this problem by either using a suboptimal decoding scheme which ignores the relay's self-interference [5, Equation (49)] or by employing a deterministic encoder at the source node [6, step (c) Equation (18)] . While these design choices are useful for the case where the eavesdropper is physically separated from the relay, they may yield a smaller achievable rate if applied directly to the case where the relay and the eavesdropper are co-located.

Corollary 2: For model 2 defined by (2), the achievable rate region in (23) can be expressed as:

$$
\bigcup \left\{
\begin{array}{rl}
R_e \leq R_1 \leq & I\left(X; Y_D\hat{Y}_r|X_r Y_R\right)\\
0 \leq R_e \leq & [I\left(X; Y_D\hat{Y}_r|X_r Y_R\right) - I\left(X; Y_r\right)]^+
\end{array}
\right\}
\qquad (37)
$$

where $I(X_r; Y_R) > I(\hat{Y}_r; Y_r|Y_D Y_R X_r)$ and the union is taken over $p(X)p(X_r)p(Y_D Y_r|X)p(Y_R|X_r)p(\hat{Y}_r|Y_r X_r)$.

Proof: (37) follows from (23) by letting $Y = \{Y_D, Y_R\}$ and using the following two Markov chains:

$$X \to X_r \to Y_R \qquad (38)$$

$$X_r \to Y_R \to Y_D \qquad (39)$$

It follows from (38) and (39) that $I(X_r; Y_R Y_D) = I(X_r; Y_R)$ and $I(X; Y_R Y_D \hat{Y}_r|X_r) = I(X; Y_D\hat{Y}_r|X_r Y_R)$. Also here $I(X; Y_r|X_r) = I(X; Y_r)$. ■

Next, we apply Corollary 2 to the Gaussian case, which is defined as:

$$
\begin{aligned}
Y_D &= X + Z_D\\
Y_r &= aX + Z_r\\
Y_R &= bX_r + Z_R
\end{aligned}
\qquad (40)
$$

where Z_D, Z_r, Z_R are independent zero-mean Gaussian random variables with unit variance. The transmit power of the source and the relay are constrained by $E[X_r^2] = E[X^2] \leq P$.

Corollary 3: For the Gaussian relay network defined in (40), the following rate region is achievable.

$$0 \le R_e \le R_1 \le \frac{1}{2}\log_2\left(1+P+\frac{a^2P}{1+\sigma_Q^2}\right) \tag{41}$$

$$R_e \le \frac{1}{2}\left[\log_2\left(1+P+\frac{a^2P}{1+\sigma_Q^2}\right)-\log_2\left(1+a^2P\right)\right]^+ \tag{42}$$

$$\text{where } \sigma_Q^2 = \frac{\left(a^2+1\right)P+1}{b^2P\left(P+1\right)} \tag{43}$$

Proof: (41) and (42) follow from letting $X \sim \mathcal{N}(0,P), X_r \sim \mathcal{N}(0,P), \hat{Y}_r = Y_r + Z_Q, Z_Q \sim \mathcal{N}(0,\sigma_Q^2)$, and Z_Q is independent from all the other variables. The region (R_1, R_e) is maximized where σ_Q^2 is minimum, and (43) follows from $I(X_r;X_R) > I(\hat{Y}_r;Y_r|Y_DY_RY_r)$. ■

Remark 4: Suppose $a > 1$. Without the channel between relay and destination, the secrecy capacity is known to be 0 [13]. We also know that a non-zero secrecy rate cannot be achieved with decode-and-forward. However, if b is large enough, a non-zero secrecy rate can be achieved with compress-and-forward, as shown by (42). This is an example where the relay-to-destination link helps to achieve a non-zero secrecy rate when the relay and the eavesdropper are co-located.

Remark 5: Like the cooperative jamming/noise forward scheme in [2] and [5], the relay transmits a signal that is independent from the message when $R_1 = R_e$. However, instead of being a deaf relay like the scheme shown in [5], here the relay *must listen* to the source in order for it to provide useful side information to the destination.

Remark 6: A trivial upper bound on the secrecy rate is $\frac{1}{2}\log_2(1+\frac{P}{a^2P+1})$. This can be obtained by combining the relay with the destination or the relay with the source, and applying the bound in (18). It can also be obtained by specializing the outer bound of [4, section VI.C Theorem 7]. We observe that by letting $b \to \infty$, we will have $\sigma_Q \to 0$, and R_e in (43) will approach this outer bound asymptotically.

Remark 7: The amplify and forward scheme can also be used at the relay. In this case, the relay output is given by:

$$X_r = \frac{\sqrt{P}}{\sqrt{a^2P+1}}Y_r \tag{44}$$

The relay network is then equivalent to a Gaussian Wire-tap channel where the legitimate receiver has two antennas. The achievable secrecy rate is computed from $I(X;Y_RY_D) - I(X;Y_r)$ [15] and is given by:

$$R_e \le \frac{1}{2}\left[\log\left(1+\left(1+\xi\right)P\right)-\log\left(1+a^2P\right)\right]^+ \tag{45}$$

where

$$\begin{aligned}\xi &= \frac{a^2\beta^2b^2}{1+\beta^2b^2} \quad \text{and} \\ \beta^2 &= \frac{P}{\left(a^2P+1\right)}.\end{aligned}$$

Observe that amplify-and-forward can also achieve a non-zero secrecy rate given a large enough b. However, comparing it to (42), we find that the secrecy rate given by amplify-and-forward is strictly smaller than the secrecy rate achievable by compress-and-forward.

V. Conclusion

In this paper, we have considered two relay channel models with orthogonal components, where the relay is the eavesdropper. For the first model, we have found the capacity-equivocation region and proved that the relay-destination link does not help in increasing secrecy rate, and therefore the relay should not be deployed if perfect secrecy is desired. For the second model, we have provided an achievable rate based on compress-and-forward. We have presented an example where a non-zero secrecy rate is achievable under this scheme, in which the relay-to-destination link plays a central role. Thus, we conclude that, for this model, the relay can help the source and the destination to communicate despite being subjected to the secrecy constraint.

References

[1] A.D. Wyner. The Wire-tap Channel. *Bell System Technical Journal*, 54(8):1355–1387, 1975.

[2] E. Tekin and A. Yener. The General Gaussian Multiple Access and Two-Way Wire-Tap Channels: Achievable Rates and Cooperative Jamming. 2007. to appear in IEEE Transactions on Information Theory, Special issue on Information Theoretic Security.

[3] A. Sendonaris, E. Erkip, and B. Aazhang. User cooperation diversity. Part I. System description. *IEEE Transactions on Communications*, 51(11):1927–1938, 2003.

[4] Y. Oohama. Relay Channels with Confidential Messages. 2006. submitted to IEEE Transactions on Information Theory, Special issue on Information Theoretic Security.

[5] L. Lai and H. El Gamal. The Relay-Eavesdropper Channel: Cooperation for Secrecy. 2006. submitted to IEEE Transactions on Information Theory.

[6] M. Yuksel and E. Erkip. Secure Communication with a Relay Helping the Wiretapper. *IEEE Information Theory Workshop*, 2007.

[7] M. Yuksel and E. Erkip. The Relay Channel with a Wiretapper. *Annual Conference on Information Sciences and Systems*, 2007.

[8] G. Kramer, M. Gastpar, and P. Gupta. Cooperative Strategies and Capacity Theorems for Relay Networks. *IEEE Transactions on Information Theory*, 51(9):3037–3063, 2005.

[9] T. Cover and AE Gamal. Capacity Theorems for the Relay Channel. *IEEE Transactions on Information Theory*, 25(5):572–584, 1979.

[10] AE Gamal and S. Zahedi. Capacity of a Class of Relay Channels with Orthogonal Components. *IEEE Transactions on Information Theory*, 51(5):1815–1817, 2005.

[11] Y. Liang and V.V. Veeravalli. Cooperative Relay Broadcast Channels. *IEEE Transactions on information theory*, 53(3):900–928, 2007.

[12] Y. Liang and VV Veeravalli. Gaussian Orthogonal Relay Channels: Optimal Resource Allocation and Capacity. *IEEE Transactions on Information Theory*, 51(9):3284–3289, 2005.

[13] S. Leung-Yan-Cheong and M. Hellman. The Gaussian Wire-tap Channel. *IEEE Transactions on Information Theory*, 24(4):451–456, 1978.

[14] A. Khisti and G. Wornell. Secure Transmission with Multiple Antennas: The MISOME Wiretap Channel. 2007. Submitted to IEEE Transactions on Information Theory.

[15] I. Csiszar and J. Korner. Broadcast Channels with Confidential Messages. *IEEE Transactions on Information Theory*, 24(3):339–348, 1978.