The Role of an Untrusted Relay in Secret Communication

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 communication scenario where a source-destination pair wishes to keep the information secret from a relay node despite wanting to enlist its help. A class of relay channels with orthogonal components is considered and an upper bound on the secrecy rate is derived. For the class of relay channels in consideration, we prove the relay and the eavesdropper can be separated to obtain an "enhanced" channel in terms of secrecy capacity. We then consider two special cases of this channel model: (i) the Gaussian orthogonal relay channel, and (ii) the Gaussian Cover-Kim deterministic relay channel. For the former, the upper bound found is tighter than the previously known bound. For the latter, we show that the bound yields the secrecy capacity when the source-destination link is not worse than the source-relay link. This second case also provides the first example where secrecy capacity is achieved with compress-and-forward at the relay.**

I. Introduction

A fundamental approach to information security is founded in information theory where limits of reliable communication can be determined while keeping the information secret from the eavesdropping node(s). The notion of secrecy capacity goes back to the pioneering work of Wyner [1], with much recent attention devoted to a variety of communication scenarios and channel models, thanks primarily to the potential impact on information security for wireless communications, see for example [2]–[4] and references therein.

The three node relay network with the relay being treated as an eavesdropper was first proposed in [5], [6]. In this model, the system designer has the authority to compel the relay to forward the signal using a designated relay scheme, for example via hardware implementation. The relay, in turn, with the knowledge of the coding scheme in use, is free to interpret its received signal to guess the data transmitted by the source. This model is relevant because in real life, seldom is there a "pure" eavesdropper that publicizes its intentions. Instead, a user is more likely to face network resources in the form of channels and routers operating with known protocols but are not guaranteed to be secure. Given the popularity of Wi-Fi in public places today, it is not difficult to envision practical scenarios in the near future where "public" adhoc networks are formed with untrusted relay nodes. It is with this motivation that we aim to understand the role of an untrusted relay in cooperative communications.

Should an untrusted relay node even be enlisted to relay? Several results to date say otherwise: Reference [6] shows that the secrecy capacity is 0 if the relay channel is degraded. The secrecy capacity equals that of the wire-tap channel if the channel is reversely degraded, which means that the relay-to-destination communication is useless [6]. In reference [7], it is proved the relay is again useless in a class of relay networks with orthogonal components, in which the relay and the source communicate with the destination via a multiple access channel as defined in [8].

Interestingly, the answer to the question posed above, can actually be yes. An example was constructed in [7], by using a compress-and-forward scheme, where the relay node can help increase an otherwise zero secrecy rate without having any idea what it is relaying. What is not answered in [7] is how close the achievable secrecy rate is to the secrecy capacity for this example or in general. To that end, clearly, an upper bound is needed.

The known upper bounds for the relay channel with an eavesdropper include one given in [9, Theorem 1] for the model with an external eavesdropper which is not computable for the Gaussian case. A computable bound was provided for the general Gaussian relay channel with a co-located eavesdropper [6], which does not depend on the condition of the relay-to-destination channel. Moreover, the noise correlation of the links may cause the bound to be arbitrarily loose.

In this paper, we focus on a class of relay networks with orthogonal components. In particular, we require that the relay does not interfere with itself, which is the case in Gaussian relay channels. We prove for this case, the relay can be separated from the eavesdropper leading to an "enhanced" channel, which is useful in deriving the upper bound for the secrecy rate. We then set out to assess how good the proposed upper bound is by comparing it to the compress-and-forward type achievable scheme in [7]. First, for the Gaussian orthogonal relay channel [10], we show that the proposed upper bound is tighter than the previously known bound [6]. Next, we consider the Gaussian deterministic relay channel introduced in [11]. We find the secrecy capacity when the source-destination link is not worse than the source-relay link. We observe that, as a consequence of the existence of the noise correlations, the secrecy capacity can exceed the direct link capacity. Thus, an untrusted relay is better than none.

978-1-4244-2571-6/08/$25.00 ©2008 IEEE

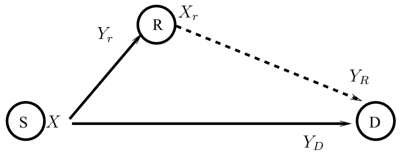

Fig. 1. Relay Channel with Orthogonal Components

II. System Model

The relay network with orthogonal components is defined as:

$$p(Y_D, Y_R, Y_r|X, X_r) = p(Y_D|X)p(Y_r|X, Y_D)p(Y_R|X_r) \quad (1)$$

The symbols are defined as shown in Figure 1. In this network, the relay does not interfere with itself. This can be seen from (1) that Y_r does not dependent on X_r.

The eavesdropper is co-located with the relay and thus has perfect knowledge of both Y_r and X_r. Let W represent the message sent by the source. Then the secrecy rate is defined as the entropy rate of the message conditioned on the signals known to the eavesdropper, i.e., $R_e = \lim_{n\to\infty} H(W|Y_r^n X_r^n)/n$. This is equivalent to the secrecy rate where the relay only knows Y_r^n [7], because given Y_r^n, the processing scheme at the relay is independent from W, therefore $W \to Y_r^n \to X_r^n$ is a Markov chain and $R_e = \lim_{n\to\infty} H(W|Y_r^n)/n$.

Throughout this paper we use the following notation: ε_1 denotes a variable that goes to 0 when n goes to ∞, and $C(x) = \frac{1}{2}\log_2(1+x)$. H represents entropy and h denotes differential entropy. $X_{]i[}$ denotes the set $\{X_j : 1 \le j < i \text{ or } i < j \le n\}$. X_1^i denotes the set $\{X_j : 1 \le j \le i\}$. The set is empty if $i < 1$. Let $\lfloor a \rfloor$ denote the largest integer less than or equal to a.

III. Upper Bound on the Secrecy Rate

The derivation of the upper bound has two steps: (i) we add a second eavesdropper to the relay network, who receives a signal that is statistically equivalent to the signal received by the relay node. (ii) we remove the first eavesdropper.

Suppose the signal received by the second eavesdropper is Y_e. An immediate question is what we mean by "statistical equivalence". This is defined by picking Y_e as follows:

$$\begin{aligned} &p(Y_D, Y_R, Y_r, Y_e|X, X_r) \\ &\quad = p(Y_D|X)p(Y_r|X, Y_D)p(Y_R|X_r)p(Y_e|X, Y_D, Y_r) \quad (2) \\ &p(Y_r|X) = p(Y_e|X) \quad (3) \end{aligned}$$

Note that under this construction, Y_e does not depend on X_r. The reason behind this construction will become clear in the sequel.

Theorem 1: For the relay channel defined by (1), the secrecy capacity of the new two eavesdropper channel defined in (2) and (3) equals the secrecy capacity of the original channel.

Proof: Because of the addition of the second eavesdropper, we know the secrecy capacity of the new channel $\le$ the secrecy capacity of the original channel. Therefore, we only need to show secrecy capacity of the new channel $\ge$ the secrecy capacity of the original channel.

We use $q(.)$ to denote any distribution related to the new channel, and use $p(.)$ for any distribution related to the original channel. Suppose the new channel uses exactly the same coding scheme and the same message sets $\{W\}$ as those of the original channel. Then we can make the following statements:

1) Suppose W can be reliably received by the destination at a rate of R_e in the original channel. Then it must be reliably received by the destination at the same rate in the new channel as well, because these two channels share the same coding scheme and the same channel description.
2) The relay, i.e., the first eavesdropper, is still oblivious the transmitted message W, since we are using exactly the same coding scheme of the original channel.
3) We next show that $H(W|Y_e^n)$ of the new channel equals $H(W|Y_r^n)$ of the original channel. To do that, it is sufficient to prove $q(Y_e^n|W)$ of the new channel equals $p(Y_r^n|W)$ of the original channel, as shown below:

$$\begin{aligned} &q\left(Y_e^n|W\right) \\ &= \sum_{X^n}\prod_{i=1}^n q\left(Y_{e,i}|X^n, Y_{e,1}^{i-1}\right) q\left(X^n|W\right) \quad (4) \\ &\overset{(a)}{=} \sum_{X^n}\prod_{i=1}^n q\left(Y_{e,i}|X_i\right) q\left(X^n|W\right) \quad (5) \\ &\overset{(b)}{=} \sum_{X^n}\prod_{i=1}^n p\left(Y_{r,i}|X_i\right) p\left(X^n|W\right) \quad (6) \\ &\overset{(c)}{=} \sum_{X^n}\prod_{i=1}^n p\left(Y_{r,i}|X^n, Y_{r,1}^{i-1}\right) p\left(X^n|W\right) \quad (7) \\ &= p\left(Y_r^n|W\right) \quad (8) \end{aligned}$$

Here step (c) follows from the relay not interfering itself. Therefore $Y_{r,i} \to X_i \to X_{]i[}Y_{r,1}^{i-1}$ is a Markov Chain. Because we construct the eavesdropper in a way that the relay is not interfering the eavesdropper either, we find that $Y_{e,i} \to X_i \to X_{]i[}Y_{e,1}^{i-1}$ is also a Markov Chain, and hence we have step (a). Step (b) follows from these two channels sharing the same coding scheme. Therefore $p(X^n|W) = q(X^n|W)$. Also by construction we have $q(Y_e|X) = p(Y_r|X)$. ■

Remark 1: Because removing the first eavesdropper will not decrease secrecy rate, this two step argument essentially separates the eavesdropper from the relay. The transformation here shows that a co-located eavesdropper is worse than a separated eavesdropper if these eavesdroppers cannot hear from each other, and each of them receives statistically equivalent signals.

Remark 2: The two step transformation will not work if we have the second eavesdropper first, and then add a co-located eavesdropper to the relay. In this case a coding scheme that works for the original system may not work for the new system. The relaying scheme in the original system may leak information to the newly added co-located eavesdropper.

Remark 3: The two step transformation will not work if the relay has self interference. In this case, in order for the second eavesdropper to receive a statistically equivalent signal, Y_e will depend on X_r. Therefore, the first eavesdropper can help the second eavesdropper. The overall secrecy rate will in general decrease. An example of this is given in [12].

Theorem 2: For an orthogonal relay channel defined in (1), its secrecy rate R_e is upper bounded by

$$\max_{p(X,X_r)} \min \left\{ \begin{array}{l} I(X; Y_D|Y_r) \\ I(X_r; Y_R) + \min_{\mathcal{P}} I(X; Y_D|Y_e) \end{array} \right\} \quad (9)$$

where $\mathcal{P}$ is a set of distribution functions defined in (2) and (3).

Proof: The first term can be obtained by specializing the result from [6]. We proceed to bound the second term:

$$H(W|Y_e^n)$$

$$\overset{(a)}{\leq} I(W; Y_D^n Y_R^n|Y_e^n) + n\varepsilon_1 \quad (10)$$

$$= I(W; Y_D^n|Y_e^n) + I(W; Y_R^n|Y_e^n Y_D^n) + n\varepsilon_1 \quad (11)$$

$$\leq I(WX^n; Y_D^n|Y_e^n) + I(WX_r^n; Y_R^n|Y_e^n Y_D^n) + n\varepsilon_1 \quad (12)$$

$$= I(X^n; Y_D^n|Y_e^n) + I(WX_r^n; Y_R^n|Y_e^n Y_D^n) + n\varepsilon_1 \quad (13)$$

$$= I(X^n; Y_D^n|Y_e^n) + h(Y_R^n|Y_e^n Y_D^n) - \sum_{i=1}^{n} h\left(Y_{R,i}|Y_e^n Y_D^n X_r^n Y_{R,1}^{i-1} W\right) + n\varepsilon_1 \quad (14)$$

$$\overset{(b)}{=} I(X^n; Y_D^n|Y_e^n) + h(Y_R^n|Y_e^n Y_D^n) - \sum_{i=1}^{n} h(Y_{R,i}|X_{r,i}) + n\varepsilon_1 \quad (15)$$

$$\leq I(X^n; Y_D^n|Y_e^n) + \sum_{i=1}^{n} \left(h(Y_{R,i}) - h(Y_{R,i}|X_{r,i})\right) + n\varepsilon_1 \quad (16)$$

$$= h(Y_D^n|Y_e^n) - \sum_{i=1}^{n} h\left(Y_{D,i}|Y_e^n X^n Y_{D,1}^{i-1}\right) + \sum_{i=1}^{n} I(X_{r,i}; Y_{R,i}) + n\varepsilon_1 \quad (17)$$

$$\overset{(c)}{=} h(Y_D^n|Y_e^n) - \sum_{i=1}^{n} h(Y_{D,i}|Y_{e,i} X_i) + \sum_{i=1}^{n} I(X_{r,i}; Y_{R,i}) + n\varepsilon_1 \quad (18)$$

$$\leq \sum_{i=1}^{n} I(X_i; Y_{D,i}|Y_{e,i}) + \sum_{i=1}^{n} I(X_{r,i}; Y_{R,i}) + n\varepsilon_1 \quad (19)$$

$$\leq nI(X; Y_D|Y_e) + nI(X_r; Y_R) + n\varepsilon_1 \quad (20)$$

Here step (a) follows from Fano's inequality. Step (b) follows from the relay destination link being orthogonal to the rest part of the channel. Step (c) follows from the fact that the relay is not interfering the second eavesdropper. Therefore given $Y_{e,i}X_i$, $Y_{e,j}, j > i$ does not provide further information about $Y_{D,i}$. The last two steps are the standard single letterization. ■

Remark 4: In Theorem 2, if Y_e is picked as Y_r, then the second term within the minimum is always bigger than the first term. However, as we will see in the next section, because Y_e can be chosen arbitrarily as long as it is in the set $\mathcal{P}$, the second term can be smaller than the first term if Y_e is chosen properly.

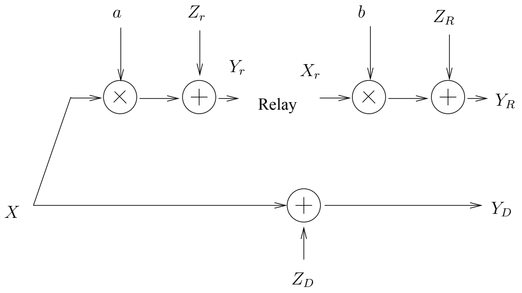

Fig. 2. The Gaussian Orthogonal Relay Channel

IV. The Gaussian Orthogonal Relay Channel

The Gaussian orthogonal relay channel is depicted in Figure 2. In this model, a, b are the channel gains. $Y_D = X + Z_D, Y_r = aX + Z_r, Y_R = bX_r + Z_R$ 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 to be

$$\lim_{n\to\infty} \sum_{i=1}^{n} E[X_{r,i}^2]/n \leq P; \quad \lim_{n\to\infty} \sum_{i=1}^{n} E[X_i^2]/n \leq P. \quad (21)$$

Corollary 1: For the Gaussian orthogonal relay channel with independent noise components, the upper bound on secrecy rate is:

$$\min\left\{ C(b^2P) + [C(P) - C(a^2P)]^+, C\left(\frac{P}{1+a^2P}\right) \right\} \quad (22)$$

Proof: First we notice that (9) is upper bounded by:

$$\min \left\{ \begin{array}{l} \max_{p(X,X_r)} I(X; Y_D|Y_r) \\ \max_{p(X_r)} I(X_r; Y_R) + \min_{\mathcal{P}} \max_{p(X,X_r)} I(X; Y_D|Y_e) \end{array} \right\} \quad (23)$$

To be able to have $p(Y_e|X) = p(Y_r|X)$, we define a Gaussian random variable N_e such that $Y_e = aX + N_e$. Then the set $\mathcal{P}$ can be re-parametrized with the correlation between N_e, N_r and the correlation between N_e, N_D. Under a given correlation, it is known $I(X; Y_D|Y_e)$ and $I(X; Y_r Y_D|Y_e)$ are both maximized under Gaussian distribution [4, Appendix II]. The first term in (23) then becomes $\frac{1}{2}\log_2\left(1 + \frac{P}{1+a^2P}\right)$. To obtain the second term inside the minimum, we pick N_e as follows:

1) If $a < 1$, then $\frac{N_e}{a^2} = N_D + N'$.
2) Otherwise, pick N_e such that $N_D = \frac{N_e}{a^2} + N'$.

In both cases N' is a zero mean Gaussian random variable with appropriate variance so that the equations above hold. Substituting N_e back to (23) yields the second term. ■

In Figure 3, we compare the upper bound with the achievable rates from [7]. The secrecy rate of compress-and-forward and amplify-and-forward are computed from equation (42) and (45) in [7]. The rate is plotted for the source-to-relay channel gain $a = 1$, and varying the relay-to-destination channel gain b. The asymptotic tightness of the upper bound when b goes to ∞ has been discussed in [7, Remark 6]. Here, because of the first term in (22), the upper bound also reflects the channel condition of the orthogonal link, as it decreases when the link between the relay and the destination deteriorates.

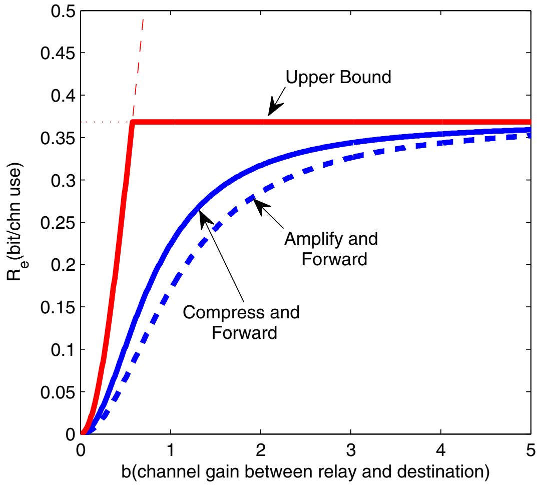

Fig. 3. Secrecy Rate of the Gaussian Orthogonal Relay Channel, $a = 1$

V. The Cover-Kim Deterministic Relay Channel

In this section we investigate the deterministic relay channel of reference [11] whose capacity is established therein. The channel is depicted in Figure 4. Here $Y_D = X + Z$ and $Y_r = \alpha X - Z$, where Z is a zero mean Gaussian random variable with unit variance, i.e., the random variables representing the noise components have a correlation $\rho = -1$. Between the relay and the destination, there is a separate noiseless link with rate R_0. The destination receives side information from the relay via this link in addition to Y_D from the source. The transmission power of the source is constrained to be $\frac{1}{n}\sum_{i=1}^{n} E[X_i^2] \leq P$.

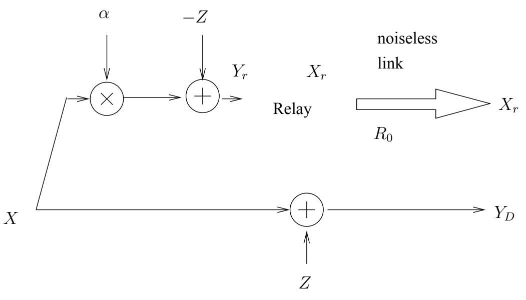

Fig. 4. The Gaussian Cover-Kim Deterministic Relay channel

Theorem 3: For the Gaussian Cover-Kim deterministic channel, the following secrecy rate is achievable:

$$\left[R_0 + C(P) - C\left(\alpha^2 P\right)\right]^+ \tag{24}$$

Proof: Let $\mathcal{C}$ be a random code book with $2^{\lfloor n\left[R_0+C(P)-C\left(\alpha^2P\right)\right]^+\rfloor}2^{\lfloor nC\left(\alpha^2P\right)\rfloor}$ codewords sampled from an i.i.d Gaussian distribution with zero mean and variance P. These codewords are randomly partitioned into $2^{\lfloor n\left[R_0+C(P)-C\left(\alpha^2P\right)\right]^+\rfloor}$ bins with equal size. The bin index of the transmitted codeword is determined by the message W. The actual transmitted codeword is then selected randomly from this bin according to a uniform distribution. The relay uses either hash-and-forward or compress-and-forward as described in [11]. Let $E[P_e|\mathcal{C}]$ be the average error probability over the codebook ensemble $\{\mathcal{C}\}$ that the destination could not correctly determine X^n, hence W, from Y_D^n and side information provided by the relay. It was proved in [11] that $\lim_{n\to\infty} E[P_e|\mathcal{C}] = 0$.

Since each bin is a Gaussian codebook by itself whose rate is below the AWGN channel capacity between the source and the relay, the relay node can determine X^n given W and Y_r^n with high probability using joint typical decoding. Therefore, from Fano's inequality, we have $H\left(X^n|WY_r^n\mathcal{C}\right) \leq n\varepsilon_1$. Then we have:

$$\begin{aligned}
H\left(W|Y_r^n\mathcal{C}\right) =& H\left(X^nW|Y_r^n\mathcal{C}\right) - H\left(X^n|WY_r^n\mathcal{C}\right) && (25)\\
\geq& H\left(X^nW|Y_r^n\mathcal{C}\right) - n\varepsilon_1 && (26)\\
=& H\left(X^n|Y_r^n\mathcal{C}\right) + H\left(W|X^nY_r^n\mathcal{C}\right) - n\varepsilon_1 && (27)\\
=& H\left(X^n|Y_r^n\mathcal{C}\right) - n\varepsilon_1 && (28)\\
=& H\left(X^n|\mathcal{C}\right) - I\left(X^n;Y_r^n|\mathcal{C}\right) - n\varepsilon_1 && (29)\\
\geq& H\left(X^n|\mathcal{C}\right) - I\left(X^n;Y_r^n\right) - n\varepsilon_1 && (30)\\
\geq& H\left(X^n|\mathcal{C}\right) - \sum_{i=1}^{n} I\left(X_i;Y_{r,i}\right) - n\varepsilon_1 && (31)
\end{aligned}$$

Since each code word is selected with equal probability, we have

$$\lim_{n\to\infty}\frac{1}{n}H\left(X^n|\mathcal{C}\right) = C(P) + R_0 \tag{32}$$

Also, $I\left(X_i;Y_{r,i}\right) = C(\alpha^2P)$. Substituting this and (32) into (31), dividing it by n and taking the limit $n \to \infty$, we have (24), which equals $\lim_{n\to\infty}\frac{1}{n}H(W|\mathcal{C})$. Therefore $\lim_{n\to\infty} E[P_e|\mathcal{C}] + \frac{1}{n}I(W;Y_r^n|\mathcal{C}) = 0$. Since both terms inside the limit are non-negative, this proves the existence of at least one codebook with a rate of $\left[R_0 + C(P) - C\left(\alpha^2P\right)\right]^+$ such that both terms are arbitrarily small. Hence we have proved the theorem. ■

Corollary 2: The secrecy rate of the Gaussian Cover-Kim deterministic channel is upper bounded by

$$R_0 + \left[C(P) - C\left(\alpha^2P\right)\right]^+ \tag{33}$$

Proof: The bound follows from Theorem 2 by choosing the appropriate Y_e.

1) If $\alpha \geq 1$, then $Y_e = \alpha X + Z$, $Y_D = X + \frac{Z}{\alpha} + Z'$ $Y_r = X - \frac{Z}{\alpha} - Z'$.

Z' is a zero mean Gaussian random variable with variance $|1-\frac{1}{\alpha^2}|$, and Z' is independent from Z.

2) If $\alpha \leq 1$, then $Y_e = X + Z + Z'$.
Z' is a zero mean Gaussian random variable with variance $|1-\frac{1}{\alpha^2}|$, and Z' is independent from Z.

■

Remark 5: Inspecting (24) and (33), we see that the upper bound and the achievable rate coincide when $\alpha \leq 1$. The secrecy capacity is achieved by compress-and-forward. The upper bound and the achievable rate are plotted in Figure 5 for $R_0 = 0.5$ bits/channel use, and $P = 1$.

Remark 6: The secrecy capacity can exceed the direct link capacity if $R_0 > C(P)$. This is a benefit of the correlation of the noises corrupting the links from the source. If the noises are independent, then the secrecy capacity cannot exceed $C(P)$, as shown below:

Theorem 4: If the relay channel has the property: $p(Y_R, Y_D, Y_r|X, X_r) = p(Y_R|X_r)\,p(Y_r|X)\,p(Y_D|X)$ Then $R_e \leq I(X;Y_D)$.

Proof: First we assume the eavesdropper only knows the transmitted signal of the relay, but does not know the received signal of the relay. Doing this will not decrease the secrecy capacity. Therefore, the signal seen by the eavesdropper is X_r. Next we assume the link between the source and the relay is perfect. This is possible because of the independence condition given above. The source can simulate the channel between the relay node and itself without the knowledge of the channel condition on the direct link. The channel is then transformed into a 2×2 MIMO wiretap channel [3] with input being X, X_r and output being Y_D, Y_R. The eavesdropper receives X_r. Then the secrecy rate is bounded by the upper bound for MIMO wiretap channel.

$$\begin{aligned}
R_e \leq& I(XX_r;Y_DY_R|X_r) && (34)\\
=& I(X;Y_DY_R|X_r) && (35)\\
=& I(X;Y_R|X_r) + I(X;Y_D|Y_RX_r) && (36)\\
=& I(X;Y_D|Y_RX_r) && (37)\\
=& h(Y_D|Y_RX_r) - h(Y_D|Y_RX_rX) && (38)\\
=& h(Y_D|Y_RX_r) - h(Y_D|X) && (39)\\
\leq& h(Y_D) - h(Y_D|X) && (40)\\
=& I(X;Y_D) && (41)
\end{aligned}$$

■

VI. Conclusion

In this paper, we have considered a class of relay networks with orthogonal components where the relay does not interfere with itself, and investigated the secrecy rate when the relay is the eavesdropper. We have shown that, for this type of channels, an "enhanced" channel can be obtained by separating the relay and the eavesdropper, which is useful in deriving the upper bound for the secrecy rate. To evaluate the usefulness of the bound, we have particularized the upper bound to two cases. For the Gaussian orthogonal relay channel we have observed that the bound gets tighter as the relay-to-destination link improves. For the Gaussian Cover-Kim deterministic relay channel, the bound yields the secrecy capacity when the source-destination link is not worse than the source-relay link. The latter thus provides an example where secrecy capacity is achieved via compress-and-forward. Furthermore, the secrecy capacity with the relay as the eavesdropper can exceed the direct link capacity. Our results thus point to the value of cooperation even with secrecy constraints: despite being an untrusted entity, the relay still can still be useful without knowing what it is relaying.

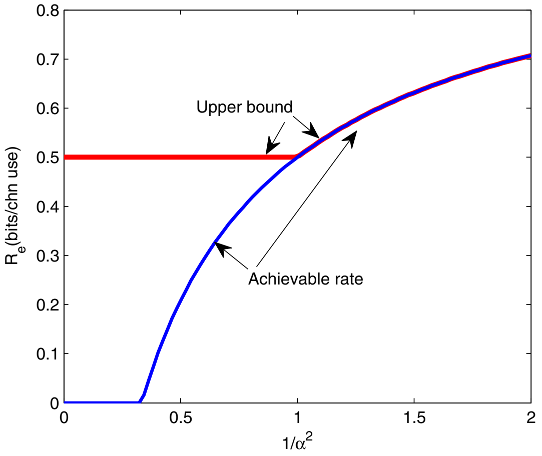

Fig. 5. Secrecy rate for the Gaussian Cover-Kim Deterministic Relay channel

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. *IEEE Transactions on Information Theory-Special Issue on Information Theoretic Security*, 2008.

[3] S. Shafiee, N. Liu, and S. Ulukus. Towards the Secrecy Capacity of the Gaussian MIMO Wire-tap Channel: The 2-2-1 Channel. Submitted to IEEE Transactions on Information Theory, 2007.

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

[5] Y. Oohama. Coding for Relay Channels with Confidential Messages. *Information Theory Workshop*, 2001.

[6] Y. Oohama. Relay Channels with Confidential Messages. Submitted to IEEE Transactions on Information Theory, 2007.

[7] X. He and A. Yener. On the Equivocation Region of Relay Channels with Orthogonal Components. *Annual Asilomar Conference on Signals, Systems, and Computers*, 2007.

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

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

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

[11] T. M. Cover and Y. H. Kim. Capacity of a Class of Deterministic Relay Channels. Submitted to IEEE Transactions on Information Theory, 2006.

[12] X. He and A. Yener. The Role of an Untrusted Relay in Cooperation and Secret Communication. to be submitted to IEEE Transaction on Information Theory, 2008.