

The Relay Channel with a Wire-tapper

Melda Yuksel and Elza Erkip

Department of Electrical and Computer Engineering

Polytechnic University

Brooklyn, New York 11201-3840

Email: myukse01@utopia.poly.edu

Abstract—In this work a relay channel with a wire-tapper is studied for both discrete memoryless and Gaussian channels. The wire-tapper receives a physically degraded version of the destination’s signal. We find inner and outer bounds for the capacity–equivocation rate region. We also argue that when the destination receives a physically degraded version of the relay’s signal, inner and outer bounds meet for some special cases.

I. INTRODUCTION

The relay channel was introduced by van der Meulen [1], and further studied by Cover and El Gamal [2]. Using a relay increases achievable rates and robustness against channel variations with respect to direct communication, which makes the relay channel important and relevant for today’s large network, high rate applications. Recently, the relay channel has been studied extensively, [3], [4], [5], we refer the reader to the references in [5] for an extensive list. Although the capacity of the general relay channel has been an open problem for more than thirty years, the capacity is known for some special cases such as the physically degraded relay channel.

In large networks not all users are legitimate, but some are illegitimate, passive listeners. The building block of such a network is the wire-tap channel, which was introduced by Wyner [6]. In the wire-tap channel the source and the destination aim to keep their communication as secret as possible from the passive listener, the wire-tapper. The system performance measures for the wire-tap channel are the main channel capacity, the capacity between the source and the legitimate destination, and the equivocation rate, the level of obscurity at the wire-tapper. Wyner investigates the case when the wire-tapper receives a degraded version of the destination’s signal, resulting in an equivalent degraded broadcast channel [6]. In [7], these results are extended to less noisy and more capable broadcast channels, and in [8] to Gaussian channels. Recent advances in information theoretic secrecy include [9], [10], [11]. In [10], the authors study a multiple access channel with a degraded wire-tapper. Generalized multiple access channels with confidential messages are studied [9]. In [11] the authors investigate interference and broadcast channels in which each receiver’s message should be kept confidential from the other receiver. In addition to the above mentioned work, [12], [13], [14] provide an information theoretic security analysis for wireless channels.

¹This material is based upon work partially supported by the NSF under Grant No. 0093163.

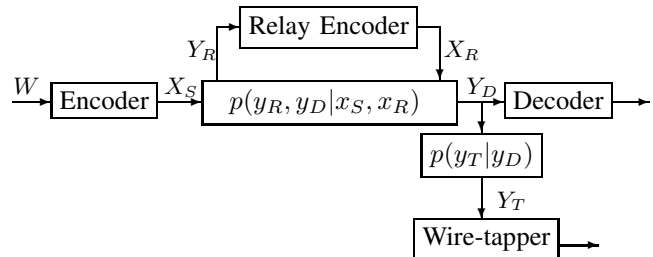


Fig. 1. The system model.

In this work we study the relay channel with a wire-tapper, and study the impact of the relay on secure communications. We first examine the physically degraded relay channel with a physically degraded wire-tapper, and find inner and outer bounds on the capacity–equivocation rate region and on the secrecy capacity for both discrete memoryless and Gaussian channels. We show that inner and outer bounds meet for some special cases. We also argue that the inner and outer bounds we find still hold even if the source–relay–destination channel is not physically degraded. Our work is done concurrently with and independently from [15], where for a general relay–wire-tap channel, an outer bound on the capacity–equivocation rate region is found and different relaying strategies are compared.

The organization of the paper is as follows. Section II introduces the system model. Section III presents the upper bounds and achievability results for the capacity–equivocation rate region for discrete memoryless channels. Section IV extends the results to Gaussian channels. Finally, Section V concludes the paper.

II. SYSTEM MODEL

In this section we describe the relay channel with a wire-tapper, and explain the necessary performance measures. In the rest of the paper we will use X^n and X_i^n to denote vectors (X_1, X_2, \dots, X_n) and $(X_i, X_{i+1}, \dots, X_n)$ respectively, and $X \rightarrow Y \rightarrow Z$ means X, Y and Z form a Markov chain.

The discrete memoryless relay channel with a wire-tapper consists of two finite input alphabets \mathcal{X}_S and \mathcal{X}_R , and three finite output alphabets $\mathcal{Y}_R, \mathcal{Y}_D, \mathcal{Y}_T$, where the subscripts S, R, D and T denote the source, the relay, the destination and the wire-tapper respectively.

Although in the rest of the paper we will clearly explain if we need the relay to be physically degraded or not, here we

define the physically degraded relay channel with a physically degraded wire-tapper. This channel is expressed as

$$\begin{aligned} & p(y_R, y_D, y_T | x_S, x_R) \\ &= p(y_R | x_S, x_R) p(y_D | x_R, y_R) p(y_T | y_D), \end{aligned} \quad (1)$$

where $(x_S, x_R) \in \mathcal{X}_S \times \mathcal{X}_R$, $y_R \in \mathcal{Y}_R$, $y_D \in \mathcal{Y}_D$ and $y_T \in \mathcal{Y}_T$. The channel is shown in Fig. 1.

The channel is memoryless, that is $(y_{R,i}, y_{D,i}, y_{T,i})$ depends on the past and current (x_S^i, x_R^i) only through the current transmitted symbols $(x_{S,i}, x_{R,i})$. Therefore

$$\begin{aligned} & p(w, x_S^n, x_R^n, y_R^n, y_D^n, y_T^n) \\ &= p(w) \prod_{i=1}^n p(x_{S,i} | w) p(x_{R,i} | y_{R,i}^{i-1}) p(y_{R,i}, y_{D,i}, y_{T,i} | x_{S,i}, x_{R,i}), \end{aligned}$$

where w denotes the message.

A $(2^{nR}, n)$ code for the relay channel consists of a message set, a source encoder, a set of relay functions and a decoder at the destination. The message W is uniformly distributed over the message set $\mathcal{W} = \{1, 2, \dots, 2^{nR}\}$. The encoder at the source, $\mathcal{W} \rightarrow \mathcal{X}_S^n$, maps each message $w \in \mathcal{W}$ to a codeword $x_S^n \in \mathcal{X}_S^n$. The set of relay functions $\{f_i\}_{i=1}^n$ are such that $x_{R,i} = f_i(Y_{R,1}, Y_{R,2}, \dots, Y_{R,i-1})$, where $i = 1, \dots, n$. Finally, the decoder at the destination $g : \mathcal{Y}_D^n \rightarrow \mathcal{W}$ maps y_D^n to $w \in \mathcal{W}$.

If a message $w \in \mathcal{W}$ is sent, let $P(g(y_D^n) \neq w | w \text{ is sent})$ be the conditional probability of error. Then the average probability of error of the code is

$$P_e^{(n)} = \frac{1}{|\mathcal{W}|} \sum_{w \in \mathcal{W}} P(g(y_D^n) \neq w | w \text{ is sent}).$$

The equivocation rate at the wire-tapper, which describes the confusion of the wire-tapper about the message W given its observation Y_T^n , is defined as

$$R_e = \frac{1}{n} H(W | Y_T^n).$$

For the relay channel with a wire-tapper a rate–equivocation rate pair (R, R_e) is achievable if there exists a sequence of $(2^{nR}, n)$ codes with $P_e^{(n)} \rightarrow 0$ as n goes to infinity and

$$\lim_{n \rightarrow \infty} \frac{1}{n} H(W | Y_T^n) \geq R_e.$$

The capacity–equivocation rate region, \mathcal{C} , is the closure of the set of all achievable rate–equivocation pairs (R, R_e) , and the secrecy capacity, C_s , is the largest achievable R_e such that $R = R_e$.

Note that if the relay does not transmit anything, $f_i = \emptyset$, for all i , then the above system becomes equivalent to that of the wire-tap channel [6], [7]; on the other hand if the wire-tapper does not hear anything, $Y_T = \emptyset$, then the channel reduces to the relay channel of [2].

The above definitions for discrete memoryless channels also extend to discrete time additive white Gaussian noise channels, which we study in Section IV.

III. DISCRETE MEMORYLESS CHANNELS

In this section we find two outer bounds and an inner bound on the capacity–equivocation rate region.

Theorem 1: For the physically degraded relay channel with a physically degraded wire-tapper given in (1), the capacity–equivocation rate region is contained in $\hat{\mathcal{C}}_1 \cap \hat{\mathcal{C}}_2$, where $\hat{\mathcal{C}}_1$ and $\hat{\mathcal{C}}_2$ are given by

$$\begin{aligned} \hat{\mathcal{C}}_1 &= \bigcup_{p(x_S, x_R)} \left\{ \begin{array}{l} 0 \leq R_e \leq R \\ R \leq I(X_S, X_R; Y_D), \\ R_e \leq I(X_S, X_R; Y_D) - I(X_S, X_R; Y_T) \end{array} \right\}, \\ \hat{\mathcal{C}}_2 &= \bigcup_{p(q)p(x_S, x_R|q)} \left\{ \begin{array}{l} 0 \leq R_e \leq R \\ R \leq I(X_S; Y_R | X_R, Q), \\ R_e \leq I(X_S; Y_R | X_R, Q) - I(X_S, X_R; Y_T | Q) \end{array} \right\}. \end{aligned}$$

Moreover, the region $\check{\mathcal{C}}$,

$$\check{\mathcal{C}} = \bigcup_{p(x_S, x_R)} \left\{ \begin{array}{l} 0 \leq R_e \leq R \\ R \leq \min\{I(X_S, X_R; Y_D), I(X_S; Y_R | X_R)\} \\ R_e \leq \min\{I(X_S, X_R; Y_D), I(X_S; Y_R | X_R)\} \\ \quad - I(X_S, X_R; Y_T) \end{array} \right\}$$

is achievable.

Corollary 1: For the physically degraded relay channel with a physically degraded wire-tapper given in (1), the secrecy capacity is upper bounded by

$$\begin{aligned} \hat{C}_s &= \max_{p(q)p(x_S, x_R|q)} \{ \min\{I(X_S, X_R; Y_D) - I(X_S, X_R; Y_T), \\ & \quad I(X_S; Y_R | X_R, Q) - I(X_S, X_R; Y_T | Q)\} \}. \end{aligned}$$

Moreover, a perfect secrecy rate \check{C}_s

$$\begin{aligned} \check{C}_s &= \max_{p(x_S, x_R)} \{ \min\{I(X_S, X_R; Y_D) - I(X_S, X_R; Y_T), \\ & \quad I(X_S; Y_R | X_R) - I(X_S, X_R; Y_T)\} \} \end{aligned}$$

is achievable.

Observing the regions in Theorem 1, it is easy to see that these regions are quite similar except the Q variable in region $\hat{\mathcal{C}}_2$. Also if $I(X_S, X_R; Y_D) \leq I(X_S; Y_R | X_R)$, the inner and outer bounds meet, $\check{\mathcal{C}} = \hat{\mathcal{C}}_1$, and we achieve the capacity–equivocation rate region.

Note that if the source–relay–destination channel were not physically degraded, then we could replace all the $I(X_S; Y_R | X_R, Q)$ terms in $\hat{\mathcal{C}}_2$ with $I(X_S; Y_R Y_D | X_R, Q)$ and this modified $\hat{\mathcal{C}}_2$ would still constitute an outer bound. $\hat{\mathcal{C}}_1$ and the achievable region $\check{\mathcal{C}}$ would not change. A similar argument also holds for \hat{C}_s and \check{C}_s .

Next, we find an upper bound to the capacity–equivocation rate region in Section III-A. Then in Section III-B, we propose an achievable scheme.

A. Upper Bounds

In this subsection we find an upper bound on the capacity–equivocation rate region. We will use Fano’s inequality

$$H(W|Y_D^n) \leq nRP_e^{(n)} + 1 \triangleq n\delta_n. \quad (2)$$

As the message can be decoded from Y_D^n , $P_e^{(n)} \rightarrow 0$, and δ_n , defined as $RP_e^{(n)} + 1/n$, also goes to zero as $n \rightarrow \infty$.

In the following inequalities we will use the subscripts $(\tilde{S}, \tilde{S}^{(c)})$ to denote a pair of sets. $(\tilde{S}, \tilde{S}^{(c)})$ either stands for $(\{S\}, \{R, D\})$ or $(\{S, R\}, \{D\})$. Thus, if $(\tilde{S}, \tilde{S}^{(c)}) = (\{S\}, \{R, D\})$, then $X_{\tilde{S}} = X_S$, and $Y_{\tilde{S}^{(c)}} = (Y_R, Y_D)$; and if $(\tilde{S}, \tilde{S}^{(c)}) = (\{S, R\}, \{D\})$, then $X_{\tilde{S}} = (X_S, X_R)$, and $Y_{\tilde{S}^{(c)}} = Y_D$.

To find an upper bound on the equivocation rate we write:

$$\begin{aligned} nR_e &= H(W|Y_T^n) \\ &= H(W|Y_T^n) - H(W|Y_T^n, Y_{\tilde{S}^{(c)}}^n) \\ &\quad + H(W|Y_T^n, Y_{\tilde{S}^{(c)}}^n) \end{aligned} \quad (3)$$

$$\begin{aligned} &\leq I(W; Y_{\tilde{S}^{(c)}}^n | Y_T^n) + n\delta_n \\ &= \sum_{i=1}^n I(W; Y_{\tilde{S}^{(c)}, i} | Y_T^n, Y_{\tilde{S}^{(c)}}^{i-1}) + n\delta_n \\ &= \sum_{i=1}^n \left[H(Y_{\tilde{S}^{(c)}, i} | Y_T^n, Y_{\tilde{S}^{(c)}}^{i-1}) \right. \\ &\quad \left. - H(Y_{\tilde{S}^{(c)}, i} | Y_T^n, Y_{\tilde{S}^{(c)}}^{i-1}, W) \right] + n\delta_n \\ &\leq \sum_{i=1}^n \left[H(Y_{\tilde{S}^{(c)}, i} | Y_{T, i}, Y_{\tilde{S}^{(c)}}^{i-1}) \right. \\ &\quad \left. - H(Y_{\tilde{S}^{(c)}, i} | Y_{T, i}, Y_{\tilde{S}^{(c)}}^{i-1}, W, X_{\tilde{S}, i}, X_{\tilde{S}^{(c)}, i}) \right] \\ &\quad + n\delta_n \end{aligned} \quad (4)$$

$$\begin{aligned} &= \sum_{i=1}^n \left[H(Y_{\tilde{S}^{(c)}, i}, Y_{T, i} | Y_{\tilde{S}^{(c)}}^{i-1}) - H(Y_{T, i} | Y_{\tilde{S}^{(c)}}^{i-1}) \right. \\ &\quad \left. - H(Y_{\tilde{S}^{(c)}, i}, Y_{T, i} | Y_{T, i+1}, Y_{\tilde{S}^{(c)}}^{i-1}, W, X_{\tilde{S}, i}, X_{\tilde{S}^{(c)}, i}) \right. \\ &\quad \left. + H(Y_{T, i} | Y_{T, i+1}, Y_{\tilde{S}^{(c)}}^{i-1}, W, X_{\tilde{S}, i}, X_{\tilde{S}^{(c)}, i}) \right] + n\delta_n \\ &= \sum_{i=1}^n \left[H(Y_{\tilde{S}^{(c)}, i}, Y_{T, i} | Y_{\tilde{S}^{(c)}}^{i-1}, X_{\tilde{S}^{(c)}, i}) \right. \\ &\quad \left. - H(Y_{T, i} | Y_{\tilde{S}^{(c)}}^{i-1}) \right. \\ &\quad \left. - H(Y_{\tilde{S}^{(c)}, i}, Y_{T, i} | Y_{\tilde{S}^{(c)}}^{i-1}, X_{\tilde{S}, i}, X_{\tilde{S}^{(c)}, i}) \right. \\ &\quad \left. + H(Y_{T, i} | Y_{\tilde{S}^{(c)}}^{i-1}, X_{\tilde{S}, i}, X_{\tilde{S}^{(c)}, i}) \right] + n\delta_n \end{aligned} \quad (5)$$

$$\begin{aligned} &= \sum_{i=1}^n \left[I(X_{\tilde{S}, i}; Y_{\tilde{S}^{(c)}, i}, Y_{T, i} | Y_{\tilde{S}^{(c)}}^{i-1}, X_{\tilde{S}^{(c)}, i}) \right. \\ &\quad \left. - I(X_{\tilde{S}, i}, X_{\tilde{S}^{(c)}, i}; Y_{T, i} | Y_{\tilde{S}^{(c)}}^{i-1}) \right] + n\delta_n \end{aligned} \quad (6)$$

$$\begin{aligned} &= \sum_{i=1}^n \left[I(X_{\tilde{S}, i}; Y_{\tilde{S}^{(c)}, i} | Y_{\tilde{S}^{(c)}}^{i-1}, X_{\tilde{S}^{(c)}, i}) \right. \\ &\quad \left. - I(X_{\tilde{S}, i}, X_{\tilde{S}^{(c)}, i}; Y_{T, i} | Y_{\tilde{S}^{(c)}}^{i-1}) \right] + n\delta_n \end{aligned} \quad (7)$$

$$\begin{aligned} &= n \frac{1}{n} \sum_{i=1}^n \left[I(X_{\tilde{S}, M}; Y_{\tilde{S}^{(c)}, M} | Y_{\tilde{S}^{(c)}}^{M-1}, X_{\tilde{S}^{(c)}, M}, M = i) \right. \\ &\quad \left. - I(X_{\tilde{S}, M}, X_{\tilde{S}^{(c)}, M}; Y_{T, M} | Y_{\tilde{S}^{(c)}}^{M-1}, M = i) \right] \\ &\quad + n\delta_n \end{aligned} \quad (8)$$

$$\begin{aligned} &= nI(X_{\tilde{S}, M}; Y_{\tilde{S}^{(c)}, M} | Y_{\tilde{S}^{(c)}}^{M-1}, X_{\tilde{S}^{(c)}, M}, M) \\ &\quad - nI(X_{\tilde{S}, M}, X_{\tilde{S}^{(c)}, M}; Y_{T, M} | Y_{\tilde{S}^{(c)}}^{M-1}, M) + n\delta_n \\ &= nI(X_{\tilde{S}, Q}; Y_{\tilde{S}^{(c)}, Q} | X_{\tilde{S}^{(c)}, Q}, Q) \\ &\quad - nI(X_{\tilde{S}, Q}, X_{\tilde{S}^{(c)}, Q}; Y_{T, Q} | Q) + n\delta_n. \end{aligned} \quad (9)$$

As conditioning reduces entropy, the third term in (3) is less than the left hand side in (2). The first term in (4) follows because conditioning reduces entropy. In the second term Y_T^{i-1} is removed as $Y_{\tilde{S}^{(c)}, i} \rightarrow (Y_{T, i}^n, Y_{\tilde{S}^{(c)}}^{i-1}) \rightarrow Y_T^{i-1}$, and $X_{\tilde{S}, i}$ and $X_{\tilde{S}^{(c)}, i}$ are appended as conditioning reduces entropy. The first term in (5) follows because $X_{\tilde{S}^{(c)}, i}$ is a function of the past received symbols $Y_{\tilde{S}^{(c)}}^{i-1}$; the third and fourth terms follow because the channel is memoryless and the channel outputs $(Y_{\tilde{S}^{(c)}, i}, Y_{T, i})$ depend only on the channel inputs $(X_{\tilde{S}, i}, X_{\tilde{S}^{(c)}, i})$. To obtain the first term in (6) we combined the first and third terms in (5). Similarly for the second term in (6) we combined the second and fourth terms in (5). The first term in (7) follows because $X_{\tilde{S}, i} \rightarrow Y_{\tilde{S}^{(c)}, i} \rightarrow Y_{T, i}$ given $X_{\tilde{S}^{(c)}, i}$. In (8) we introduced the independent time-sharing random variable M , uniformly distributed on $\{1, 2, \dots, n\}$, and in (9) we simply named $Q = (Y_{\tilde{S}^{(c)}}^{M-1}, M)$. This Q satisfies $Q \rightarrow (X_{\tilde{S}, Q}, X_{\tilde{S}^{(c)}, Q}) \rightarrow (Y_{\tilde{S}^{(c)}, Q}, Y_{T, Q})$. Note that when $Y_{\tilde{S}^{(c)}}$ changes Q also changes. When $Q = (Y_D^{i-1}, M)$, one can prove that the equivocation rate upper bound in region $\hat{\mathcal{C}}_1$ is larger than the one in (9). We omit this part of the proof due to space limitation. For $Q = (Y_R^{i-1} Y_D^{i-1}, M)$ we obtain the equivocation rate bound of $\hat{\mathcal{C}}_2$ of Theorem 1.

The upper bound on rate R follows from the max-flow min-cut bound [2], which results in

$$R \leq I(X_{\tilde{S}, Q}; Y_{\tilde{S}^{(c)}, Q} | X_{\tilde{S}^{(c)}, Q}, Q). \quad (10)$$

Note that both (9) and (10) are valid even if the source–relay–destination channel is not physically degraded. For the physically degraded case

$$I(X_{S, Q}; Y_{D, Q}, Y_{R, Q} | X_{R, Q}, Q) = I(X_{S, Q}; Y_{R, Q} | X_{R, Q}, Q),$$

and the bounds (9) and (10) become tighter. In addition to these bounds we have

$$\begin{aligned} R_e &= \frac{1}{n} H(W | Y_T^n) \\ &\leq \frac{1}{n} H(W) \\ &= R. \end{aligned}$$

Hence we established the regions $\hat{\mathcal{C}}_1$ $\hat{\mathcal{C}}_2$ of Theorem 1.

B. Achievability

In this subsection we propose an achievable scheme.

We fix a distribution $p(x_S, x_R)$ and assume the source and the relay perform block Markov superposition coding, and

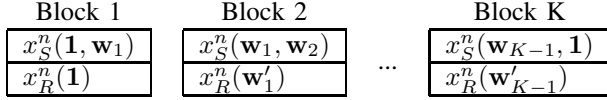


Fig. 2. The relaying scheme that achieves the region $\tilde{\mathcal{C}}$ given in Theorem 1.

the destination does backward decoding. For the encoding-decoding structure we propose in this subsection, we assume that $R > R' - I(X_S, X_R; Y_T)$ and $R' > I(X_S, X_R; Y_T)$. When any one of these conditions are not satisfied, the problem simplifies significantly, and we will discuss those cases at the end of this section. In addition to these, we assume $I(X_S, X_R; Y_T) < I(X_S; Y_R|X_R)$, as otherwise the equivocation rate upper bound is equal to zero, and the problem becomes equivalent to a relay channel with no secrecy constraints.

We define the following

$$\begin{aligned} A &= 2^{n(R' - I(X_S, X_R; Y_T))} \\ B &= 2^{nI(X_S, X_R; Y_T)} \\ J &= 2^{n[R - (R' - I(X_S, X_R; Y_T))]} \end{aligned}$$

and the sets

$$\begin{aligned} \mathcal{A} &= 1, \dots, A & \mathcal{B} &= 1, \dots, B \\ \mathcal{J} &= 1, \dots, J & \mathcal{W} &= \mathcal{A} \times \mathcal{J} \end{aligned}$$

Furthermore, $h : \mathcal{B} \rightarrow \mathcal{J}$ is a partitioning \mathcal{B} into \mathcal{J} subsets with nearly equal size, where nearly equal size means $\|h^{-1}(j_1)\| \leq 2\|h^{-1}(j_2)\|, \forall j_1, j_2 \in \mathcal{J}$.

The source encoder maps $\mathbf{w} = (a, j)$ into (a, b) , where b is chosen uniformly from the set $h^{-1}(j) \subset \mathcal{B}$.

The relay generates a code book that consist of $2^{nR'}$ codewords, labeled $x_R^n(\mathbf{s})$, $\mathbf{s} = (s_a, s_b)$, $s_a = 1, \dots, A$, $s_b = 1, \dots, B$. Each symbol $x_{Ri}(\mathbf{s})$, $i = 1, 2, \dots, n$, is generated independently according to $p_{X_R}(\cdot)$.

For each $x_R^n(\mathbf{s})$, source generates $2^{nR'}$ codewords, $x_S^n(\mathbf{s}, \mathbf{w})$, $\mathbf{w} = (w_a, w_b)$, $w_a = 1, \dots, A$, $w_b = 1, \dots, B$, with each symbol, $x_{Si}(\mathbf{s}, \mathbf{w})$ i.i.d. distributed as $p_{X_S|X_R}(\cdot|x_{Ri}(\mathbf{s}))$.

The encoding is carried over K blocks. To send $\mathbf{w}_k = (w_{a,k}, w_{j,k})$ with a certain equivocation in block k , the source first finds $(w_{a,k}, w_{b,k})$ such that b is chosen uniformly from the set $h^{-1}(j)$. The source transmits $x_S^n(\mathbf{w}_{k-1}, \mathbf{w}_k)$ in each block k , for which $(w_{a,0}, w_{b,0}) = (w_{a,K}, w_{b,K}) = (1, 1) = \mathbf{1}$. Similarly, the relay sends $x_R^n(\mathbf{s}_k)$ in block k . In the first block $\mathbf{s}_k = (s_{a,1}, s_{b,1}) = \mathbf{1}$.

After the transmission of block k , the relay, assuming it has correctly decoded \mathbf{w}_{k-1} , attempts to find an estimate \mathbf{w}'_k such that

$$(x_S^n(\mathbf{w}_{k-1}, \mathbf{w}'_k), x_R^n(\mathbf{w}_{k-1}), y_{R,k}^n)$$

are jointly typical. If

$$R' \leq I(X_S; Y_R|X_R), \quad (11)$$

then the relay decodes the source message reliably and obtains $\mathbf{w}'_k = \mathbf{w}_k$ with high probability. Then it sets $\mathbf{s}_{k+1} = \mathbf{w}'_k$. The encoding structure is depicted in Fig. 2.

The destination starts decoding after all K blocks are received and moves backwards. At block K , the destination looks for an $\tilde{\mathbf{w}}_{K-1}$ such that

$$(x_S^n(\tilde{\mathbf{w}}_{K-1}, \mathbf{1}), x_R^n(\tilde{\mathbf{w}}_{K-1}), y_{D,K}^n)$$

are jointly typical. The destination will be able to locate a unique $\tilde{\mathbf{w}}_{K-1} = \mathbf{w}_{K-1}$ with high probability if

$$R' \leq I(X_S, X_R; Y_D). \quad (12)$$

Once the destination decodes \mathbf{w}_{K-1} , it can move backwards to decode $\mathbf{w}_{K-2}, \dots, \mathbf{w}_1$.

The wire-tapper also performs backward decoding, and starts trying to decode after all K blocks are received. At block K , its equivocation for the message \mathbf{W}_{K-1} is

$$\begin{aligned} &H(\mathbf{W}_{K-1}|Y_{T,K}^n) \\ &= H(\mathbf{W}_{K-1}, Y_{T,K}^n) - H(Y_{T,K}^n) \\ &= H(\mathbf{W}_{K-1}, Y_{T,K}^n, X_{S,K}^n) \\ &\quad - H(X_{S,K}^n|\mathbf{W}_{K-1}, Y_{T,K}^n) - H(Y_{T,K}^n) \\ &= H(\mathbf{W}_{K-1}, X_{S,K}^n) + H(Y_{T,K}^n|\mathbf{W}_{K-1}, X_{S,K}^n) \\ &\quad - H(X_{S,K}^n|\mathbf{W}_{K-1}, Y_{T,K}^n) - H(Y_{T,K}^n) \\ &\geq H(\mathbf{W}_{K-1}, X_{S,K}^n) + H(Y_{T,K}^n|\mathbf{W}_{K-1}, X_{S,K}^n, X_{R,K}^n) \\ &\quad - H(X_{S,K}^n|\mathbf{W}_{K-1}, Y_{T,K}^n) - H(Y_{T,K}^n) \\ &= H(\mathbf{W}_{K-1}, X_{S,K}^n) + H(Y_{T,K}^n|X_{S,K}^n, X_{R,K}^n) \\ &\quad - H(X_{S,K}^n|\mathbf{W}_{K-1}, Y_{T,K}^n) - H(Y_{T,K}^n) \\ &\geq H(X_{S,K}^n) + H(Y_{T,K}^n|X_{S,K}^n, X_{R,K}^n) \\ &\quad - H(X_{S,K}^n|\mathbf{W}_{K-1}, Y_{T,K}^n) - H(Y_{T,K}^n). \end{aligned} \quad (13)$$

To calculate the first term in (13) we first argue that

$$\frac{P(X_{S,K}^n(\mathbf{W}_K = ((\mathbf{w}_K)_i, \mathbf{1})))}{P(X_{S,K}^n(\mathbf{W}_K = ((\mathbf{w}_K)_j, \mathbf{1})))} \leq 2,$$

for all $i, j = 1, 2, \dots, 2^{nR}$. The proof follows probability calculations, which we omit here due to space limitation. Next, using the above result and [9, Lemma 6] we find that

$$H(X_{S,K}^n) \geq nR' - 1.$$

As the channel is memoryless, the second term in (13) is equal to

$$H(Y_{T,K}^n|X_{S,K}^n, X_{R,K}^n) = nH(Y_T|X_S, X_R).$$

The third term in (13) is equal to zero because

$$0 \leq H(X_{S,K}^n|\mathbf{W}_{K-1}, Y_{T,K}^n) \leq H(X_{S,K}^n|\mathbf{W}_{K-1}) = 0.$$

Finally, for the fourth term we have

$$H(Y_{T,K}^n) = nH(Y_T),$$

because the channel is memoryless and each $(x_{S,i}, x_{R,i})$ pair is chosen independent and identically distributed.

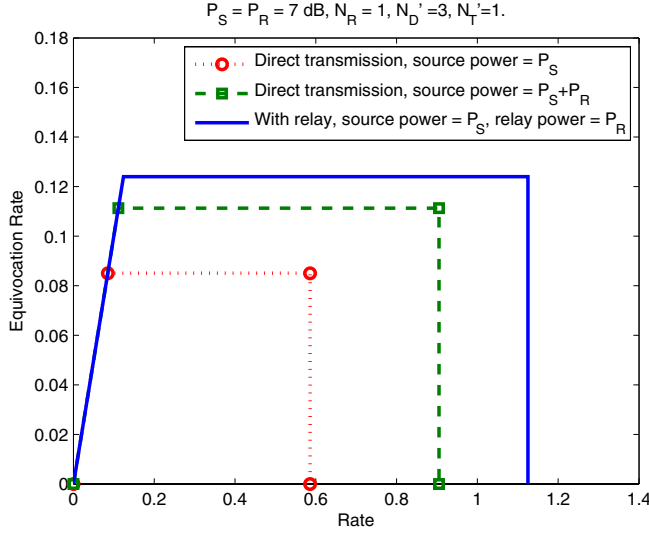


Fig. 3. The achievable rate–equivocation rate region for the physically degraded Gaussian relay channel with a physically degraded wire-tapper versus capacity–equivocation rate regions for direct transmission (no relay). To achieve the best secrecy rate $\alpha^* = 0.75$, $\beta^* = 1$, $\gamma^* = 1$. Secrecy capacity for direct transmission is equal to 0.0851 and 0.113, when source power is P_S and $P_S + P_R$ respectively. The achievable secrecy rate with relay is 0.1240.

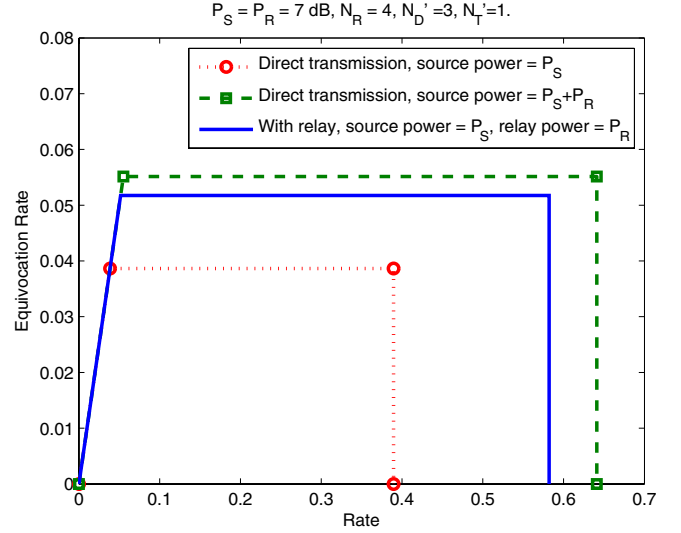


Fig. 4. The achievable rate–equivocation rate region for the physically degraded Gaussian relay channel with a physically degraded wire-tapper versus capacity–equivocation rate regions for direct transmission (no relay). To achieve the best secrecy rate $\alpha^* = 0.99$, $\beta^* = 1$, $\gamma^* = 0.58$. Secrecy capacity for direct transmission is equal to 0.0386 and 0.0551, when source power is P_S and $P_S + P_R$ respectively. The achievable secrecy rate with relay is 0.0517.

Overall,

$$\begin{aligned} & \frac{1}{n} H(\mathbf{W}_{K-1} | Y_{T,K}^n) \\ & \geq R' - \frac{1}{n} + H(Y_T | X_S, X_R) - H(Y_T) \\ & = R' - I(X_S, X_R; Y_T) - \frac{1}{n} \end{aligned}$$

For block k , the wire-tapper's confusion about \mathbf{W}_{k-1} is equal to

$$\begin{aligned} & H(\mathbf{W}_{k-1} | Y_{T,k}^n) \\ & \geq H(\mathbf{W}_{k-1} | Y_{T,k}^n, \mathbf{W}_k) \\ & = \sum p(\mathbf{W}_k = \mathbf{w}_k) H(\mathbf{W}_{k-1} | Y_{T,k}^n, \mathbf{W}_k = \mathbf{w}_k), \end{aligned}$$

for which a similar analysis as in block K results in

$$\frac{1}{n} H(\mathbf{W}_{k-1} | Y_{T,k}^n, \mathbf{W}_k = \mathbf{w}_k) \geq R' - I(X_S, X_R; Y_T) - \frac{1}{n}.$$

As R' is upper bounded by the minimum of (11) and (12), we can choose $R' = \min\{I(X_S; Y_R | X_R), I(X_S, X_R; Y_D)\} - \epsilon$ and we conclude that for each message \mathbf{w}_k , this code book structure achieves an equivocation rate of

$$\begin{aligned} R_e & = \min\{I(X_S; Y_R | X_R), I(X_S, X_R; Y_D)\} \\ & \quad - I(X_S, X_R; Y_T) - \epsilon - \frac{1}{n}. \end{aligned}$$

Until now, we assumed that $R > R' - I(X_S, X_R; Y_T)$. If this condition is not satisfied, we set $\mathcal{J} = 1$. The source encoder maps $\mathbf{w} = (a, j)$ into (a, b) , where b is chosen uniformly from the set \mathcal{B} . In this case perfect secrecy is achieved. On the other hand, if $R' < I(X_S, X_R; Y_T)$, then

no secrecy is achieved and $R_e = 0$. Thus, by changing R and R' , we can use this code book structure to achieve various rate–equivocation rate pairs.

IV. GAUSSIAN CHANNELS

In this section, we extend our achievability results to Gaussian channels. For the Gaussian channel with a physically degraded relay and a physically degraded wire-tapper, the channel input-output relations are

$$Y_{R,i} = X_{S,i} + Z_{R,i} \quad (14)$$

$$Y_{D,i} = Y_{R,i} + X_{R,i} + Z'_{D,i} \quad (15)$$

$$Y_{T,i} = Y_{D,i} + Z'_{T,i}. \quad (16)$$

Note that the total noise at the destination and at the wire-tapper are equal to $Z_{R,i} + Z'_{D,i}$ and $Z_{R,i} + Z'_{D,i} + Z'_{T,i}$ respectively. Here $Z_{R,i}$, $Z'_{D,i}$ and $Z'_{T,i}$ are i.i.d. with distributions $\mathcal{N}(0, N_R)$, $\mathcal{N}(0, N'_D)$, and $\mathcal{N}(0, N'_T)$ respectively. The power constraints of the source and relay are

$$\frac{1}{n} \sum_{i=1}^n x_{S,i}^2(w) \leq P_S, \quad w \in \{1, 2, \dots, 2^{nR}\} \quad (17)$$

and

$$\frac{1}{n} \sum_{i=1}^n x_{R,i}^2(y_{R,1}, y_{R,2}, \dots, y_{R,i-1}) \leq P_R, \quad (18)$$

where $(y_{R,1}, y_{R,2}, \dots, y_{R,i-1}) \in \mathbb{R}^n$.

We will use the notation $C(x) = \frac{1}{2} \log(1+x)$, and $f(\alpha, \beta, \gamma, P_S, P_R) = \beta P_S + \gamma P_R + 2\sqrt{(\beta - \alpha)P_S\gamma P_R}$ in the rest of this section.

Theorem 2: For the physically degraded Gaussian relay channel with a physically degraded wire-tapper, given in (14)–(18), the rate–equivocation rate region $\hat{\mathcal{C}}^G$ is achievable, where

$$\hat{\mathcal{C}}^G = \bigcup_{0 \leq \alpha \leq 1, \alpha \leq \beta \leq 1, 0 \leq \gamma \leq 1} \begin{cases} 0 \leq R_e \leq R \\ R \leq \min \left\{ C \left(\frac{f(\alpha, \beta, \gamma, P_S, P_R)}{N_R + N_D'} \right), C \left(\frac{\alpha P_S}{N_R} \right) \right\} \\ R_e \leq \min \left\{ C \left(\frac{f(\alpha, \beta, \gamma, P_S, P_R)}{N_R + N_D'} \right), C \left(\frac{\alpha P_S}{N_R} \right) \right\} \\ - \min \left\{ C \left(\frac{f(\alpha, \beta, \gamma, P_S, P_R)}{N_R + N_D + N_T} \right), C \left(\frac{\alpha P_S}{N_R} \right) \right\} \end{cases}.$$

To achieve the region stated in Theorem 2, we choose X_R and \tilde{X}_R independently as $X_R \sim \mathcal{N}(0, \gamma P_R)$, $\tilde{X}_R \sim \mathcal{N}(0, \alpha P_S)$ and form

$$X_S = \sqrt{\frac{(\beta - \alpha) P_S}{\gamma P_R}} X_R + \tilde{X}_R.$$

In the above expressions the parameter γ shows the relay’s participation level in the communication. Although for the physically degraded relay channel it is always optimal to use the relay with full power, this may not be the case when there is a wire-tapper. The parameter α is related to the coherent combining gain of the source and relay signals at the destination, or at the wire-tapper. It also shows the fresh information rate the source sends to the relay. In addition to these, the parameter β shows the fraction of source power the system operates at. Although we are unable to prove at this point, we conjecture that the optimal β should be 1. This is because operating at a lower source power neither benefits the secrecy rate, nor the source–relay–destination channel capacity.

In Fig. 3 and Fig. 4 we illustrate the achievable rate–equivocation rate regions for two scenarios. We also show direct transmission capacity–equivocation rate regions for comparison. If there is an individual power constraint on the source and the relay, using the relay is always advantageous, and the rate–equivocation rate region is considerably enlarged. However, when we compare the relay channel to direct transmission when the source has the total power, $P_S + P_R$, this is not always the case. (Note that this is also the case for the relay channel without the wire-tapper.) Fig. 3, illustrates this case when $P_S = P_R = 7$ dB, $N_R = 1$, $N_D' = 3$, and $N_T' = 1$. In this case, using the relay performs better than direct transmission under both individual and total power constraints, and the system benefits from using the relay with full power ($\gamma^* = 1$). However, when the relay has more noise, it is no longer beneficial to use the relay with full power to achieve the best secrecy rate. Fig. 4 illustrates the case when $P_S = P_R = 7$ dB, $N_R = 4$, $N_D' = 3$, $N_T' = 1$ for which optimal $\gamma^* = 0.58$. In fact, for some cases, optimal γ^* may be 0, and the relay will not participate in the communication. This is because, the relay helps both the destination and the wire-tapper simultaneously. It is advantageous to use the relay whenever it is more helpful to the destination than to the

wire-tapper in terms of information rates. Note that to achieve the source–relay–destination channel capacity with no secrecy constraints, we still need to choose $\gamma = 1$.

V. CONCLUSION

In this work we study the relay channel with a wire-tapper. In this network, the source seeks relay’s help for transmitting its messages to the destination securely, keeping the wire-tapper as confused about the messages as possible. We established inner and outer bounds on the rate–equivocation rate region for the relay channel with a physically degraded wire-tapper for both discrete memoryless and discrete time additive white Gaussian noise channels. We also discussed the special cases for which these bounds meet. For Gaussian channels, the achievable scheme we proposed suggests that using the relay with full power is not always advantageous in the presence of a wire-tapper. The relay’s transmission helps both the destination and the wire-tapper and is only useful when it contributes more to the destination. Future work includes extending our results to channels in which we can relax the degradedness assumption on the wire-tapper. This includes the cases when the source–relay–destination channel is either more capable or less noisy than the source–relay–wire-tapper channel.

REFERENCES

- [1] E. C. van der Meulen, “Three-terminal communication channels,” *Advances in Applied Probability*, vol. 3, p. 121, 1971.
- [2] T. M. Cover and A. E. Gamal, “Capacity theorems for the relay channel,” *IEEE IT*, vol. 25, no. 5, p. 572, September 1979.
- [3] A. Sendonaris, E. Erkip, and B. Aazhang, “User cooperation diversity—Part I, Part II,” *IEEE Trans. Commun.*, vol. 51, no. 11, p. 1927, November 2003.
- [4] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, “Cooperative diversity in wireless networks: Efficient protocols and outage behavior,” *IEEE IT*, vol. 50, no. 12, p. 3062, December 2004.
- [5] G. Kramer, M. Gastpar, and P. Gupta, “Cooperative strategies and capacity theorems for relay networks,” *IEEE IT*, vol. 51, no. 9, p. 3037, 2005.
- [6] A. D. Wyner, “The wire-tap channel,” *The Bell System Technical Journal*, vol. 54, p. 1355, October 1975.
- [7] I. Csiszár and J. Körner, “Broadcast channels with confidential messages,” *IEEE IT*, vol. 24, no. 3, p. 339, May 1978.
- [8] S. K. Leung-Yan-Cheong and M. E. Hellman, “The Gaussian wire-tap channel,” *IEEE IT*, vol. 24, no. 4, p. 451, July 1978.
- [9] Y. Liang and H. V. Poor, “Generalized multiple access channels with confidential messages,” April 2006, submitted to IEEE IT.
- [10] E. Tekin and A. Yener, “The Gaussian multiple access wire-tap channel,” May 2006, submitted to IEEE IT.
- [11] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, “Discrete memoryless interference and broadcast channels with confidential messages,” in *Proceedings of 44th Allerton Conference on Communication, Control and Computing*, September 2006.
- [12] P. Parada and R. Blahut, “Secrecy capacity of SIMO and slow fading channels,” in *Proceedings of IEEE ISIT*, 2005.
- [13] P. K. Gopala, L. Lai, and H. E. Gamal, “On the secrecy of capacity of fading channels,” October 2006, submitted to IEEE IT.
- [14] J. Barros and M. R. D. Rodrigues, “Secrecy capacity of wireless channels,” in *Proceedings of IEEE ISIT*, 2006.
- [15] L. Lai and H. E. Gamal, “The relay-eavesdropper channel: Cooperation for secrecy,” December 2006, submitted to IEEE IT.