A New Outer Bound for the Gaussian Interference Channel with Confidential Messages

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*—In this work, we derive new outer bounds for the two-user interference channel with confidential messages. An upper bound is found for the sum rate. When the interfering link of the first user is greater than 1, a new upper bound on $2R_1 + R_2$ is obtained by studying a special form of the three-user interference channel. The bounds are then compared with known bounds for the symmetric interference channel under strong interference regime. In particular, examples are presented to showcase for channel parameters where positive secrecy rates are known to be achievable, the new bounds improve upon the known outer bounds on the secrecy capacity region. It is shown that, in some cases, the $2R_1 + R_2$ bound also improves the bound on the sum rate.**

I. Introduction

In a wireless environment, interference is always present. Traditionally, interference is viewed as a harmful physical phenomenon that should be avoided. Yet, from the secrecy perspective, if interference is more harmful to an eavesdropper, it can be a resource to protect confidential messages. To fully appreciate and evaluate the potential benefit of interference to secrecy, it is therefore important to find the fundamental transmission limits in an multi-user model with interference when secrecy constraints must be met.

The simplest model of this type is the two-user interference channel, which has been studied under several different security constraints up to date. References [1]–[3] have studied the case where each receiver is an eavesdropper for the messages not intended for it. References [4], [5] have considered the case where the eavesdropper is external to both receivers and is interested in the secret messages of both users. Reference [6] has considered the case in the setting of cognitive radios, where both transmitters know one public message and try to send it to both receivers, and only one transmitter has a secret message intended only for its receiver.

For a Gaussian two-user fully connected interference channel with the security constraints as defined in [1], several results have been derived up to date. On the achievability side, reference [1] has derived the achievable rate region when the channel has weak interference. Reference [2] derived the achievable rate region when only one user has secret messages to send. For the converse, reference [1] has derived an outer bound for the discrete memoryless case, which is difficult to evaluate for the Gaussian channel due to the presence of auxiliary random variables. In reference [2], a genie bound for individual rates is derived, which is close to achievable rates with weak interference when the transmission power is small.

In this work, we focus on improving the converse results for this model. Our starting point is the converse proof in [3], which is a sum rate bound derived for a one-sided interference channel under weak interference. From the converse viewpoint, the technique in [3] essentially decomposes the Z-channel into a separate point to point link and a wire-tap channel. In this work, we verify that this technique actually does not rely on whether the channel is under weak interference or not. By converting the fully connected interference channel into the Z-channel and applying this technique, a sum rate bound is obtained.

We next introduce a special form of the three-user interference channel, which we call the "Zigzag" channel, and show that an upper bound on $2R_1 + R_2$ of the two-user case can be derived from the sum rate bound for this three-user channel. When the first user's interfering link channel gain is greater than 1, the sum rate upper bound of the corresponding three-user channel can be derived by combining the techniques in [2], [3]. This leads to our new upper bound for the-two user case.

These bounds are then compared for the symmetric two-user interference channel, in the strong but not very strong interference regime. In particular, we present numerical examples for channel parameters for which, using achievable results from [2], positive secrecy rates are achievable; and therefore deriving upper bounds is of interest. For these examples, the new bound derived from the Zigzag channel improves the previously known outer bounds on the secrecy capacity region. In one example, we observe that this bound even improves the equal rate point.

The rest of the paper is organized as follows: Section II describes the model. Section III derives the upper bounds. Section IV compares these bounds and presents the numerical examples. Section V concludes the paper. The following notation is used throughout the paper: $C(x) = \frac{1}{2}\log_2(1+x)$. $Y_{j,i}$ denotes the ith component of Y_j^n. Y_j^i denotes its first i components.

II. System Model

The Gaussian two-user interference channel with confidential messages is shown in Figure 1. The received signals at the

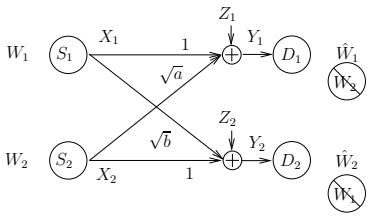

Fig. 1. Two-user interference channel with confidential messages

two receivers can be expressed as

$$Y_1 = X_1 + \sqrt{a}X_2 + Z_1 \tag{1}$$

$$Y_2 = \sqrt{b}X_1 + X_2 + Z_2 \tag{2}$$

where $Z_i, i = 1, 2$ is a zero-mean Gaussian random variable with unit variance.

Let n be the total number of channel uses. Node S_i has the following power constraint:

$$\lim_{n\to\infty} \frac{1}{n} \sum_{j=1}^{n} E\left[X_{i,j}^2\right] \leq P_i \tag{3}$$

where $X_{i,j}$ is the jth component of X_i^n.

Let f_i be the stochastic encoder used by the source node $S_i, i = 1, 2$:

$$X_i^n = f_i\left(W_i\right) \tag{4}$$

Let h_i be the decoder used by the destination node $D_i, i = 1, 2$. Let $\hat{W}_i$ be the estimate of W_i computed by node $D_i, i = 1, 2$.

$$\hat{W}_i = h_i(Y_i^n) \tag{5}$$

We assume there is no common randomness shared by the encoders. This means, the input distribution to the channel is constrained to be

$$\prod_{i=1}^{2} p\left(W_i\right) p\left(X_i^n | W_i\right) \tag{6}$$

Given (6), $X_i^n, i = 1, 2$ are independent from each other.

For D_i to receive W_i reliably, we require

$$\lim_{n\to\infty} \Pr\left(W_i \neq \hat{W}_i\right) = 0 \tag{7}$$

In addition, since W_1 must be kept secret from D_2, and W_2 must be kept secret from D_1, we require

$$\lim_{n\to\infty} \frac{1}{n} H\left(W_1\right) = \lim_{n\to\infty} \frac{1}{n} H\left(W_1 | Y_2^n\right) \tag{8}$$

$$\lim_{n\to\infty} \frac{1}{n} H\left(W_2\right) = \lim_{n\to\infty} \frac{1}{n} H\left(W_2 | Y_1^n\right) \tag{9}$$

Define $R_i = \lim_{n\to\infty} \frac{1}{n} H\left(W_i\right)$. Then the equivocation capacity region of the two-user interference channel with confidential messages is then defined as any rate pair (R_1, R_2) such that (7), (8) and (9) are met.

III. Upper Bounds

A. Invariance property of the secrecy capacity region

Lemma 1: The secrecy capacity region of an interference channel with confidential messages is invariant under a joint channel noise distribution $p(Z_1, Z_2)$, as long as it leads to the same marginal distributions $p(Z_1)$ and $p(Z_2)$.

Remark 1: The same property has been stated for the interference channel in [2] where only one user has secret message to send. Here, we verify this property when both users have secret messages to send.

Proof: From Section II, we can see the secrecy capacity region is defined by the following four joint distributions:

$$p\left(W_i, Y_j^n\right), i = 1, 2, j = 1, 2 \tag{10}$$

Without loss of generality, we examine $p\left(W_1, Y_j^n\right)$. For this term, we have:

$$p\left(Y_j^n | W_1\right) \tag{11}$$

$$= \sum_{X_1^n, X_2^n} p\left(X_1^n X_2^n Y_j^n | W_1\right) \tag{12}$$

$$= \sum_{X_1^n, X_2^n} p\left(X_1^n | W_1\right) p\left(X_2^n\right) p\left(Y_j^n | X_1^n X_2^n\right) \tag{13}$$

$$= \sum_{X_1^n, X_2^n} p\left(X_1^n | W_1\right) p\left(X_2^n\right) \prod_{i=1}^{n} p\left(Y_{j,i} | Y_j^{i-1} X_1^n X_2^n\right) \tag{14}$$

$$= \sum_{X_1^n, X_2^n} p\left(X_1^n | W_1\right) p\left(X_2^n\right) \prod_{i=1}^{n} p\left(Z_{j,i}\right) \tag{15}$$

Hence $p(W_1, Y_j^n)$ only depends on the marginal distribution $p\left(Z_j\right)$. The same holds true for $p(W_2, W_j^n)$. Hence we have the lemma. ■

Remark 2: This invariance property also applies to K-user ($K \geq 3$) interference channel.

B. $R_1 + R_2$

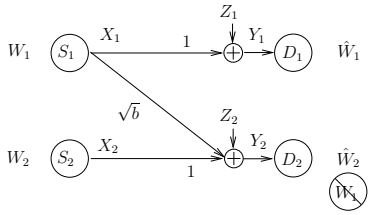

Fig. 2. Z-channel with a confidential message

The channel can be changed into a one-sided interference channel as follows:

1) First we remove the eavesdropper at D_1.
2) Then we reveal the signal X_2^n to node D_1 as genie information. The signals received by node D_1 essentially becomes $X_1^n + Z_1^n, X_2^n$. Since X_2^n is independent from W_1 and $X_1^n + Z_1^n$, node D_1 can discard X_2^n.

The resulting channel is a Z-channel shown in Figure 2. When $b<1$, the outer bound on R_1+R_2 for the Z-channel has been given in [3]:

$$R_1+R_2 \le C\left(P_1\right)+C\left(P_2\right)-C\left(bP_1\right) \tag{16}$$

Here we consider the case when $b \ge 1$. We verify that the techniques from [3] are still useful after combining it with Lemma 1.

Lemma 2:

$$R_1+R_2 \le \min\left\{ \begin{array}{l} \left[C\left(P_1\right)-C\left(bP_1\right)\right]^+ + C\left(P_2\right) \\ \left[C\left(P_2\right)-C\left(aP_2\right)\right] + C\left(P_1\right) \end{array} \right\} \tag{17}$$

Proof: We only prove the first term and focus on the case where $b>1$. The second term can be proved in a similar fashion. Like in [3], we define $V=\sqrt{b}X_1+Z_2$. Hence, we have $Y_2^n=V^n+X_2^n$. Then the sum rate of the corresponding Z-channel can be bounded as:

$$\begin{aligned} & n(R_1+R_2)-n\varepsilon \\ \le & I\left(W_1;Y_1^n\right)-I\left(W_1;Y_2^n\right)+I\left(W_2;Y_2^n\right) && (18)\\ = & I\left(W_1;Y_1^n\right)-I\left(W_1;V^n\right)-I\left(W_1;Y_2^n|V^n\right) \\ & +I\left(W_1;V^n|Y_2^n\right)+I\left(W_2;Y_2^n\right) && (19)\\ \le & I\left(W_1;Y_1^n\right)-I\left(W_1;V^n\right) \\ & +I\left(W_1;V^n|Y_2^n\right)+I\left(W_2;Y_2^n\right) && (20)\\ \le & I\left(W_1;Y_1^n\right)-I\left(W_1;V^n\right) \\ & +I\left(W_1;V^n|Y_2^n\right)+I\left(X_2^n;Y_2^n\right) && (21)\end{aligned}$$

where $\lim_{n\to\infty}\varepsilon=0$. (18) follows from (7), (8) and Fano's inequality. Then, as in [3], we prove

$$I\left(W_1;V^n|Y_2^n\right)+I\left(X_2^n;Y_2^n\right) \le I\left(X_2^n;Y_2^n|X_1^n\right) \tag{22}$$

This is because:

$$\begin{aligned} & I\left(W_1;V^n|Y_2^n\right)+I\left(X_2^n;Y_2^n\right) && (23)\\ \le & I\left(X_1^n;V^n|Y_2^n\right)+I\left(X_2^n;Y_2^n\right) && (24)\\ = & I\left(X_2^n;Y_2^n|X_1^n\right)+I\left(X_2^n;X_1^n\right) \\ & -I\left(X_2^n;X_1^n|Y_2^n\right)+I\left(X_1^n;V^n|Y_2^n\right) && (25)\\ = & I\left(X_2^n;Y_2^n|X_1^n\right)+I\left(X_1^n;V^n|Y_2^n\right) \\ & -I\left(X_1^n;X_2^n|Y_2^n\right) && (26)\\ = & I\left(X_2^n;Y_2^n|X_1^n\right)+I\left(X_1^n;V^n|V^n+X_2^n\right) \\ & -I\left(X_1^n;X_2^n|V^n+X_2^b\right) && (27)\\ = & I\left(X_2^n;Y_2^n|X_1^n\right)+I\left(X_1^n;X_2^n|V^n+X_2^n\right) \\ & -I\left(X_1^n;X_2^n|V^n+X_2^n\right) && (28)\\ = & I\left(X_2^n;Y_2^n|X_1^n\right) && (29)\end{aligned}$$

Note that (26) follows from (6). Note also that to obtain (22), we do not rely on the joint distribution of Z_1, Z_2.

Finally, we prove, for $b \ge 1$, that:

$$I\left(W_1;Y_1^n\right)-I\left(W_1;V^n\right) \le 0 \tag{30}$$

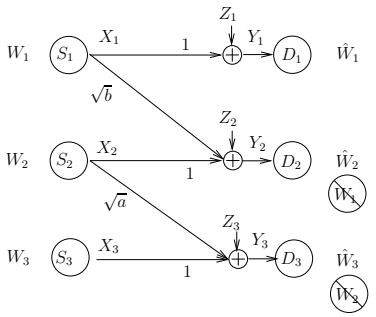

Fig. 3. The Zigzag channel with confidential messages

This is done by manipulating the correlation factor between Z_1, Z_2:

$$\frac{1}{\sqrt{b}}V^n = X_1^n+\frac{1}{\sqrt{b}}Z_2^n \tag{31}$$

$$Y_1^n = X_1^n+Z_1^n = X_1^n+\frac{1}{\sqrt{b}}Z_2^n+\sqrt{1-\frac{1}{b}}\tilde{Z}_1^n \tag{32}$$

where $\tilde{Z}_1^n$ is a Gaussian random vector that has the same distribution as Z_2^n but is independent from Z_2^n. According to Lemma 1, the secrecy capacity of the Z-channel in Figure 2 should remain unchanged. Under this correlation, we have the Markov chain $W_1-V^n-Y_1^n$. Hence, we have

$$\begin{aligned} & I\left(W_1;Y_1^n\right)-I\left(W_1;V^n\right) \\ \le & I\left(W_1;Y_1^n\right)-I\left(W_1;V^nY_1^n\right)=-I\left(W_1;V^n|Y_1^n\right)\le 0 \end{aligned} \tag{33}$$

The lemma follows from the fact that $I\left(X_2^n;Y_2^n|X_1^n\right) \le nC(P_2)$ ■

C. $2R_1+R_2$ when $a>1$

When one of the interfering gains is greater or equal to 1, another bound can be derived. Here, we consider the case where $a \ge 1$, and derive an upper bound on $2R_1+R_2$. To do so, we will first consider the Zigzag channel model shown in Figure 3. The channel outputs are:

$$Y_1=X_1+Z_1, \quad Y_2=\sqrt{b}X_1+X_2+Z_2 \tag{34}$$

$$Y_3=\sqrt{a}X_2+X_3+Z_3 \tag{35}$$

where $Z_i, i=1,2,3$, is a zero-mean Gaussian random variable with unit variance. Let P_i be the power constraint of node S_i. Let g_i be the encoding function used by node S_i and q_i be the decoding function used by node D_i. Node D_i, $i=2,3$, is an eavesdropper for the secret message sent by node S_{i-1}. At the same time, node $D_i, i=1,2,3$ is the intended receiver of the message sent by node S_i.

If the power constraint of the Zigzag channel is such that $P_3=P_1$, then we can make the following statement:

Lemma 3: If a secret rate pair of (R_1,R_2) is achievable in Figure 1, then the rate pair (R_1,R_2,R_1) is also achievable in Figure 3.

Proof: The rate pair (R_1,R_2,R_1) can be achieved as follows: Node $S_i, i=1,2$ uses the same encoder as node $S_i, i=1,2$ in Figure 1: $g_i=f_i, \quad i=1,2$.

Node S_3 uses the same encoder as node S_1: $g_3 = f_1$. The input to the encoder of node S_3 shares the same message set as $\{W_1\}$ but is independent from W_1.

Node D_1 receives $X_1^n + Z_1^n$. At the same time, node D_1 can generate $\tilde{X}_2^n$, that has the same distribution as X_2^n, and feed $\tilde{Y}_1^n = X_1^n + \sqrt{a}\tilde{X}_2^n + Z_1^n$ to the decoder h_1. Since $W_1, \tilde{Y}_1^n$ has the same joint distribution as W_1, Y_1^n, node D_1 can decode W_1 reliably.

Node D_2 uses the same decoder as node D_2 in Figure 1: $q_2 = h_2$.

Node D_3 uses the same decoder as node D_1 in Figure 1: $q_3 = h_1$.

Then it can be verified all reliability transmission conditions and secrecy constraints is met. Hence we proved the lemma. ∎

Next, we apply the technique from [3] to the Zigzag channel, and have the following lemma:

Lemma 4: When $a \geq 1$,

$$\begin{aligned} & n\left(R_1+R_2+R_3\right)-n\varepsilon \\ \leq & I\left(X_1^n X_2^n ; Y_1^n | Y_2^n\right)+I\left(X_3^n ; Y_3^n | X_2^n\right) \end{aligned} \tag{36}$$

where $\lim_{n\to\infty}\varepsilon = 0$

Proof:

$$n(R_1+R_2+R_3)-n\varepsilon \tag{37}$$
$$\begin{aligned} = & I\left(W_1 ; Y_1^n\right)-I\left(W_1 ; Y_2^n\right) \\ & +I\left(W_2 ; Y_2^n\right)-I\left(W_2 ; Y_3^n\right)+I\left(W_3 ; Y_3^n\right) \end{aligned} \tag{38}$$
$$\begin{aligned} \leq & I\left(W_1 ; Y_1^n\right)-I\left(W_1 ; Y_2^n\right) \\ & +I\left(W_2 ; Y_2^n\right)-I\left(W_2 ; Y_3^n\right)+I\left(X_3^n ; Y_3^n\right) \end{aligned} \tag{39}$$

Define $V_3^n = \sqrt{a}X_2^n + Z_3^n$. Hence, $Y_3^n = V_3^n + X_3^n$. Then, for the last three terms in (39), we have:

$$\begin{aligned} & I\left(W_2 ; Y_2^n\right)-I\left(W_2 ; Y_3^n\right)+I\left(X_3^n ; Y_3^n\right) \\ \leq & I\left(W_2 ; Y_2^n\right)-I\left(W_2 ; V_3^n\right)-I\left(W_2 ; Y_3^n | V_3^n\right) \\ & +I\left(W_2 ; V_3^n | Y_3^n\right)+I\left(X_3^n ; Y_3^n\right) \end{aligned} \tag{40}$$
$$\begin{aligned} \leq & I\left(W_2 ; Y_2^n\right)-I\left(W_2 ; V_3^n\right) \\ & +I\left(W_2 ; V_3^n | Y_3^n\right)+I\left(X_3^n ; Y_3^n\right) \end{aligned} \tag{41}$$

Then, we apply the derivation from [3, Appendix] and prove

$$I\left(W_2 ; V_3^n | Y_3^n\right)+I\left(X_3^n ; Y_3^n\right) \leq I(X_3^n ; Y_3^n | X_2^n) \tag{42}$$

The proof is the same as the way we proved (22) and is repeated here for completeness:

$$I\left(W_2 ; V_3^n | Y_3^n\right)+I\left(X_3^n ; Y_3^n\right) \tag{43}$$
$$\leq I\left(X_2^n ; V_3^n | Y_3^n\right)+I\left(X_3^n ; Y_3^n\right) \tag{44}$$
$$\begin{aligned} = & I\left(X_3^n ; Y_3^n | X_2^n\right)+I\left(X_3^n ; X_2^n\right) \\ & -I\left(X_3^n ; X_2^n | Y_3^n\right)+I\left(X_2^n ; V_3^n | Y_3^n\right) \end{aligned} \tag{45}$$
$$= I\left(X_3^n ; Y_3^n | X_2^n\right)-I\left(X_2^n ; X_3^n | Y_3^n\right)+I\left(X_2^n ; V_3^n | Y_3^n\right) \tag{46}$$
$$\begin{aligned} = & I\left(X_3^n ; Y_3^n | X_2^n\right)-I\left(X_2^n ; X_3^n | X_3^n+V_3^n\right) \\ & +I\left(X_2^n ; V_3^n | X_3^n+V_3^n\right) \end{aligned} \tag{47}$$
$$\begin{aligned} = & I\left(X_3^n ; Y_3^n | X_2^n\right)-I\left(X_2^n ; V_3^n | X_3^n+V_3^n\right) \\ & +I\left(X_2^n ; V_3^n | X_3^n+V_3^n\right)=I\left(X_3^n ; Y_3^n | X_2^n\right) \end{aligned} \tag{48}$$

Next we apply (42) to (39) and get:

$$\begin{aligned} & n(R_1+R_2+R_3)-n\varepsilon \\ \leq & I\left(W_1 ; Y_1^n\right)-I\left(W_1 ; Y_2^n\right) \\ & +I\left(W_2 ; Y_2^n\right)-I\left(W_2 ; V_3^n\right)+I\left(X_3 ; Y_3^n | X_2^n\right) \end{aligned} \tag{49}$$
$$\begin{aligned} = & I\left(W_1 ; Y_1^n\right)-I\left(W_1 ; Y_2^n\right) \\ & +I\left(W_2 ; Y_2^n\right)-I(W_2 ; \sqrt{\frac{1}{a}} V_3^n)+I\left(X_3^n ; Y_3^n | X_2^n\right) \end{aligned} \tag{50}$$

Since $a > 1$, we have:

$$Y_2^n = X_2^n + \sqrt{b}X_1^n + Z_2^n \tag{51}$$
$$= X_2^n + \sqrt{b}X_1^n + \sqrt{\frac{1}{a}}Z_3^n + \sqrt{1-\frac{1}{a}}\tilde{Z}_2^n \tag{52}$$
$$\frac{1}{\sqrt{a}}V_3^n = X_2^n + \frac{Z_3^n}{\sqrt{a}} \tag{53}$$

where $\tilde{Z}_2^n$ is a $n \times 1$ vector independent from Z_3^n, with each component distributed as $\mathcal{N}(0,1)$. Therefore

$$\begin{aligned} & I\left(W_2 ; Y_2^n\right)-I(W_2 ; \sqrt{\frac{1}{a}} V_3^n) \\ = & I\left(W_2 ; Y_2^n\right)-I(W_2 ; \sqrt{\frac{1}{a}} V_3^n, Y_2^n) \end{aligned} \tag{54}$$
$$= -I(W_2 ; Y_2^n | \sqrt{\frac{1}{a}} V_3^n) \leq 0 \tag{55}$$

Applying (55) to (50), we have

$$\begin{aligned} & n(R_1+R_2+R_3)-n\varepsilon \\ \leq & I\left(W_1 ; Y_1^n\right)-I\left(W_1 ; Y_2^n\right)+I\left(X_3^n ; Y_3^n | X_2^n\right) \end{aligned} \tag{56}$$

For the first two terms in (56), we have

$$\begin{aligned} & I\left(W_1 ; Y_1^n\right)-I\left(W_1 ; Y_2^n\right) \\ \leq & I\left(W_1 ; Y_1^n | Y_2^n\right) \leq I\left(X_1^n X_2^n ; Y_1^n | Y_2^n\right) \end{aligned} \tag{57}$$

Applying (57) to (56) yields the lemma. ∎

Next, we apply Lemma 1 to tighten the bound given by Lemma 4. Let ρ be the correlation factor between Z_1 and Z_2. Note that (53) only determines the correlation factor between Z_2 and Z_3. Hence we still have the freedom to choose ρ. From [2], we have

$$\lim_{n\to\infty}\frac{1}{n}I\left(X_1^n X_2^n ; Y_1^n | Y_2^n\right) \leq f\left(P_1, P_2, \rho, b, 0\right) \tag{58}$$

where

$$\begin{aligned} & f\left(P_1, P_2, \rho, t, v\right)=\frac{1}{2}\log_2 \\ & \frac{\left(1+P_1+vP_2\right)\left(1+tP_1+P_2\right)-\left(\rho+\sqrt{t}P_1+\sqrt{v}P_2\right)^2}{\left(1-\rho^2\right)\left(1+tP_1+P_2\right)} \end{aligned} \tag{59}$$

The best ρ, as shown in [2], is given by

$$\rho = \frac{(1+t)\,P_1 + (1+v)P_2 + (\sqrt{tv}-1)^2 P_1 P_2 - \sqrt{\Delta}}{2(\sqrt{t}P_1 + \sqrt{v}P_2)} \tag{60}$$

and Δ is given by

$$\Delta = \left[(\sqrt{t}-1)^2 P_1 + (\sqrt{v}-1)^2 P_2 + (\sqrt{tv}-1)^2 P_1 P_2\right] \left[(\sqrt{t}+1)^2 P_1 + (\sqrt{v}+1)^2 P_2 + (\sqrt{tv}-1)^2 P_1 P_2\right] \tag{61}$$

Hence we have the following lemma:

Lemma 5:

$$R_1 + R_2 + R_3 \leq f(P_1, P_2, \rho, b, 0) + C(P_3) \tag{62}$$

This, along with Lemma 3, gives us the following upper bound for the 2-user interference channel with confidential messages:

Theorem 1:

$$2R_1 + R_2 \leq f(P_1, P_2, \rho, b, 0) + C(P_1) \tag{63}$$

From this theorem, we have the following corollary:

Corollary 1: Let $P_1 = P_2 = P$. Then we have

$$\lim_{P\to\infty} 2R_1 + R_2 - \frac{1}{2}\log_2\frac{P}{b+1} - \frac{1}{2}\log_2 P \leq 0 \tag{64}$$

Proof: It can be verified that $\lim_{P\to\infty}\rho = 0$ and

$$\lim_{P\to\infty} f(P, P, \rho, t, 0) - \frac{1}{2}\log_2\frac{P}{1+t} = 0 \tag{65}$$

$$\lim_{P\to\infty} C(P) - \frac{1}{2}\log_2 P = 0 \tag{66}$$

This yields the corollary. ■

IV. Comparison to Known Bounds

In this section, we compare Theorem 1 with several known outer bounds. We focus on the symmetric case $P_1 = P_2 = P$, $a = b$, $1 < a < P + 1$. Including the two bounds derived in this work by leveraging the technique from [2], [3], there are four bounds to compare

1) The genie bound from [2].

$$\bigcap_{p(Z_1,Z_2)} \bigcup_{p(X_1)p(X_2)} \left\{ \begin{array}{l} (R_1, R_2): \\ R_1 \leq \min\{I(X_1, X_2; Y_1|Y_2), I(X_1; Y_1|X_2)\} \\ R_2 \leq \min\{I(X_1, X_2; Y_2|Y_1), I(X_2; Y_2|X_1)\} \end{array} \right\} \tag{67}$$

2) The bound on $R_1 + R_2$ derived in Section III-B.
3) Since $a = b > 1$, the bound derived in Section III-C can be used to bound $2R_1 + R_2$ and $R_1 + 2R_2$.
4) The bound for the strong interference channel without secrecy constraints.

A. Genie Bound

We first examine the equal rate point $R_1 = R_2 = R$. For the genie bound given by (67), since the channel is symmetric, both $I(X_1, X_2; Y_1|Y_2)$ and $I(X_1, X_2; Y_2|Y_1)$ are tightest at the same ρ. Hence

$$R \leq f(P, P, \rho, a, a) \tag{68}$$

When $P \to \infty$, it can be verified that

$$\lim_{P\to\infty} R - \frac{1}{2}\log_2\frac{(a-1)^2 P}{(a+1)} \leq 0 \tag{69}$$

B. Bound without Secrecy Constraints

For the case without secrecy constraints, since $a < P + 1$, we can at least achieve the sum rate such that

$$\lim_{P\to\infty} R_1 + R_2 - C((a+1)P) \geq 0 \tag{70}$$

When $R_1 = R_2 = R$ this means

$$\lim_{P\to\infty} R - \frac{1}{4}\log_2((a+1)P) \geq 0 \tag{71}$$

C. Comparison

From Corollary 1, we have

$$\lim_{P\to\infty} R - \frac{1}{3}\left(\frac{1}{2}\log_2\frac{P}{b+1} + \frac{1}{2}\log_2 P\right) \leq 0 \tag{72}$$

Comparing (72) with (69), we observe when P is large, the bound on $2R_1 + R_2$ is tighter than the genie bound (68) at the equal rate point.

From Lemma 2, when $R_1 = R_2 = R, a = b \geq 1$, we have

$$R \leq 0.5C(P) \tag{73}$$

Comparing (71) with (73), we notice (73) is always tighter.

Comparing (73) with (72), we notice these two bounds may be close to each other when P is close to 1. When P is large, (73) is tighter than (72).

These properties are demonstrated in Figure 4. Here $a = 2$, and P is chosen to be larger than 1, so $1 < a < P + 1$. From [2], in this regime a positive secrecy rate is achievable, hence upper bounding the secrecy rate is of interest. It is shown in Figure 4 that at the equal rate point, the Zigzag channel bound is tighter than the genie bound in the shown range of P. Although not apparent in the figure, it is even tighter than the Z-Channel bound when P is close to 1.

In Figure 5 and Figure 6, we present two numerical examples demonstrating that the new bounds improve previous outer bounds. In Figure 5, we demonstrate the bound $2R_1+R_2$ can indeed be dominant in bounding the sum rate when P is small. When P is large, as shown in Figure 6, it is looser than the Z channel bound in terms of sum rate, but it still helps to provide a tighter region.

Also plotted in Figure 5 and Figure 6 are achievable rates obtained by time sharing between individual achievable rates

derived in [2]. Under the time sharing factor t, when $a = b > 1$, the following rates are achievable:

$$R_1 = t\left(C\left(P_{1,\alpha}\right) - C\left(\frac{aP_{1,\alpha}}{1+P_{2,\alpha}}\right)\right) \tag{74}$$

$$R_2 = (1-t)\left(C\left(P_{2,\beta}\right) - C\left(\frac{aP_{2,\beta}}{1+P_{1,\beta}}\right)\right) \tag{75}$$

$$\text{when} \quad P_{1,\alpha} \le a-1, \quad P_{2,\beta} \le a-1 \tag{76}$$

$$P_{2,\alpha} \ge a-1, \quad P_{1,\beta} \ge a-1 \tag{77}$$

subject to the following average power constraint: $tP_{i,a} + (1-t)P_{i,\beta} \le P, \quad i = 1,2$. In both cases, it is shown that that a positive secrecy rate is achievable with these channel parameters.

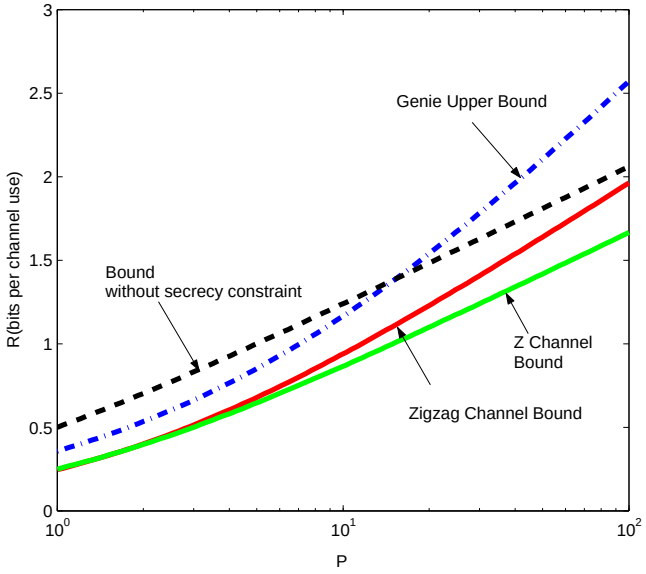

Fig. 4. Comparison to known bounds at equal rate point, $a = 2$

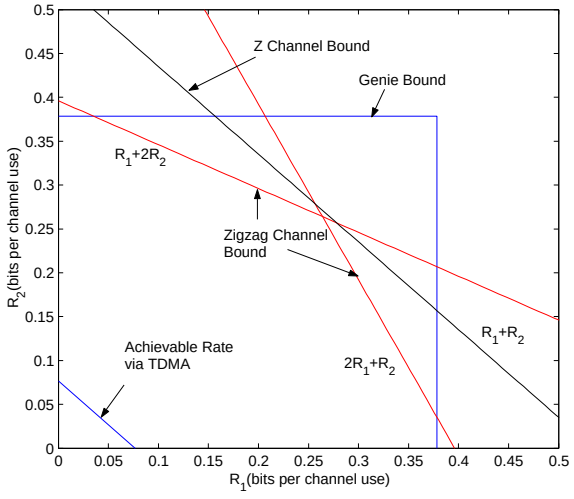

Fig. 5. Comparison of different outer bounds: The new bound can improve equal rate point. $P = 1.1, a = 2$

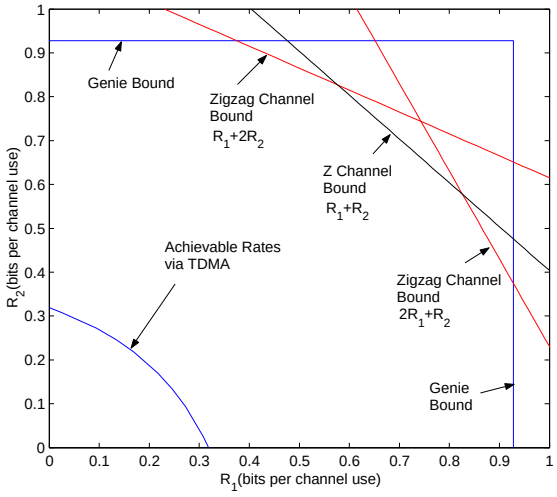

Fig. 6. Comparison of different outer bounds. $P = 6, a = 2$

V. Conclusion

In this work, we have derived outer bounds for the two-user interference channel with confidential messages. A Z-channel based sum rate bound is obtained. When user one's interfering link gains are greater than 1, a new outer bound on $2R_1 + R_2$ is obtained by considering a special form of the three-user interference channel. The outer bounds are compared with known bounds for the symmetric interference channel in strong, but not very strong, interference regime. In particular, examples are presented with channel parameters for which positive secrecy rates are achievable, and the new bounds improve the known outer bounds on the secrecy capacity region. In some cases, the new bound on $2R_1 + R_2$ also improves the bounds on sum rate.

Despite the improvement presented in this paper, we note that the gap of the achievable rate region from the outer bound is still considerably large. Towards that end, our current interest is in the improvement of the achievable rate region.

References

[1] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates. Discrete Memoryless Interference and Broadcast Channels with Confidential Messages: Secrecy Rate Regions. *IEEE Transactions on Information Theory*, 54(6):2493–2507, June 2008.

[2] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor. The Gaussian Wiretap Channel With a Helping Interferer. *IEEE International Symposium on Information Theory*, 2008.

[3] Z. Li, R. D. Yates, and W. Trappe. Secrecy Capacity Region of a Class of One-Sided Interference Channel. *IEEE International Symposium on Information Theory*, July 2008.

[4] E. Ekrem and S. Ulukus. Effects of Cooperation on the Secrecy of Multiple Access Channels with Generalized Feedback. *Annual Conference on Information Sciences and Systems*, March 2008.

[5] O. Koyluoglu and H. El-Gamal. On the Secrecy Rate Region for the Interference Channel. *IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications*, September 2008.

[6] Y. Liang, A. Somekh-Baruch, H. V. Poor, S. Shamai, and S. Verdu. Cognitive Interference Channels with Confidential Messages. Submitted to IEEE Transactions on Information Theory, December, 2007.