

Achievable Rates for the General Gaussian Multiple Access Wire-Tap Channel with Collective Secrecy

Ender Tekin and Aylin Yener

Abstract— We consider the General Gaussian Multiple Access Wire-Tap Channel (GGMAC-WT). In this scenario, multiple users communicate with an intended receiver in the presence of an intelligent and informed eavesdropper who is as capable as the intended receiver, but has different channel parameters. We aim to provide perfect secrecy for the transmitters in this multi-access environment. Using Gaussian codebooks, an achievable secrecy region is determined and the power allocation that maximizes the achievable sum-rate is found. Numerical results showing the new rate region are presented. It is shown that the multiple-access nature of the channel may be utilized to allow users with zero single-user secrecy capacity to be able to transmit in perfect secrecy. In addition, a new collaborative scheme is shown that may increase the achievable sum-rate. In this scheme, a user who would not transmit to maximize the sum rate can help another user who (i) has positive secrecy capacity to increase its rate, or (ii) has zero secrecy capacity to achieve a positive secrecy capacity.

I. INTRODUCTION

The wire-tap channel was first analyzed by Wyner in [1], where a wire-tapper has access to a degraded version of the intended receiver's signal in a single-user communications scenario. He measured the amount of "secrecy" using the conditional entropy of the transmitted message given the received signal at the wire-tapper, and determined the region of all possible Rate/Wiretapper Equivocation pairs. Wyner showed the existence of a *secrecy capacity*, C_s , for communication below which it is possible to transmit zero information to the wire-tapper. Carleial and Hellman, in [2], showed that it is possible to transmit several low-rate messages at perfect secrecy to achieve an overall rate closer to capacity. In [3], the authors extended Wyner's results to Gaussian channels and also showed that Carleial and

Hellman's results hold for Gaussian channels as well. Csiszár and Körner, in [4], showed that Wyner's results can be extended to weaker, so called "less noisy" and "more capable" channels. Furthermore, they analyzed the more general case of sending common information to both the receiver and the wire-tapper.

More recently, the notion of the wire-tap channel was extended to parallel channels, [5], [6], relay channels, [7], and fading channels, [8]. Multiple-access channels were considered in [9]–[11]. In [9], [10], the wire-tapper gets a degraded version of a GMAC uplink signal, and it is shown that the nature of the channel allows an improvement in the individual achievable rates over the single-user channel while having the same limitation on the sum-rate. In [11], there is no external eavesdropper, but the two transmitters try to keep their messages secret from each other.

In [9], we considered the Gaussian Multiple Access Wire-Tap Channel (GMAC-WT) and defined two separate secrecy constraints: (i) the *individual* secrecy constraints, the normalized entropy of any set of messages conditioned on the transmitted codewords of the other users and the received signal at the wire-tapper, and (ii) the *collective* secrecy constraints, the normalized entropy of any set of messages conditioned on the wire-tapper's received signal. The first set of constraints is more conservative to ensure secrecy of any subset of users even when the remaining users are compromised. The second set of constraints ensures the collective secrecy of any set of users, utilizing the secrecy of the remaining users. In [9], we considered a scenario where the wire-tapper received a physically degraded version of the receiver's signal and examined the *perfect secrecy rate regions* for both sets of constraints. We generalized this to a pre-determined level of secrecy, $0 \leq \delta \leq 1$, in [10], [12]. In this paper, we utilize the collective secrecy constraints with perfect secrecy, and consider the more general case where the eavesdrop-

The authors are with the Wireless Communications and Networking Laboratory, Dept. of Electrical Engineering, The Pennsylvania State University, University Park, PA 16802 tekin@psu.edu, yener@ee.psu.edu

This work has been supported in part by NSF grant CCF-0514813 "Multiuser Wireless Security"

per's ¹ signal is not necessarily degraded, but is at an overall disadvantage compared to the receiver, which we model as a set of received power constraints. Under these constraints, using random Gaussian codebooks, we find an achievable *secure rate region*, where users can communicate with arbitrarily small probability of error with the intended receiver under perfect secrecy from the eavesdropper. For this achievable rate region, we find the transmit powers that maximize the sum rate. We also find the sum-rate maximizing power allocation, and users with “good” channels - those with standardized channel gains below a certain threshold - transmit with maximum power, and those with “bad” channels, below this threshold, do not transmit. Next, we show that a non-transmitting user can help increase the secrecy capacity for a transmitting user by effectively “jamming” the eavesdropper, or even enable secret communications that would not be possible in a single-user scenario. We term this scheme *collaborative secrecy*.

II. SYSTEM MODEL AND PROBLEM STATEMENT

We consider K users communicating with a receiver in the presence of an eavesdropper. Transmitter $k = 1, \dots, K$ chooses a message W_k from a set of equally likely messages $\mathcal{W}_k = \{1, \dots, M_k\}$. The messages are encoded using $(2^{nR_k}, n)$ codes into $\{\tilde{X}_k^n(W_k)\}$, where $R_k = \frac{1}{n} \log_2 M_k$. The encoded messages $\{\tilde{\mathbf{X}}_k\} = \{\tilde{X}_k^n\}$ are then transmitted, and the intended receiver and the eavesdropper each get a copy $\mathbf{Y} = Y^n$ and $\mathbf{Z} = Z^n$. The receiver decodes $\hat{\mathbf{W}}$. We would like to communicate with the receiver with arbitrarily low probability of error, while maintaining perfect secrecy, the exact definition of which will be made precise shortly.

The signals at the intended receiver and the eavesdropper are given by

$$\mathbf{Y} = \sum_{k=1}^K \sqrt{h_k^{(M)}} \tilde{\mathbf{X}}_k + \tilde{\mathbf{N}}^{(M)} \quad (1)$$

$$\mathbf{Z} = \sum_{k=1}^K \sqrt{h_k^{(W)}} \tilde{\mathbf{X}}_k + \tilde{\mathbf{N}}^{(W)} \quad (2)$$

where $\tilde{\mathbf{N}}^{(M)}, \tilde{\mathbf{N}}^{(W)}$ are the AWGN, i.e., $\tilde{\mathbf{N}}^{(M)} \sim \mathcal{N}(\mathbf{0}, \sigma_M^2 \mathbf{I})$ and $\tilde{\mathbf{N}}^{(W)} \sim \mathcal{N}(\mathbf{0}, \sigma_W^2 \mathbf{I})$. We also assume

¹Henceforth, we will refer to the adversary as the eavesdropper rather than the wire-tapper since the communication situation modeled is a more general model that is more appropriate for wireless communications

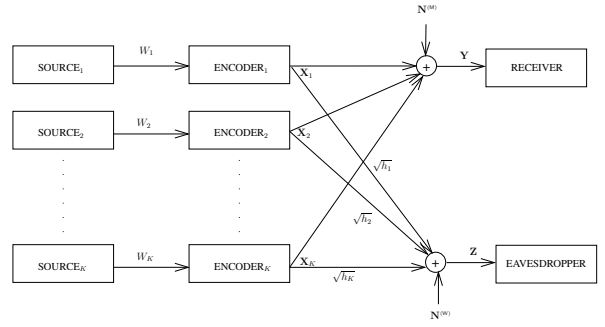


Fig. 1. Equivalent General Gaussian Multiple-Access Wire-Tap Channel (GGMAC-WT) system model.

the following transmit power constraints:

$$\frac{1}{n} \sum_{i=1}^n \tilde{X}_{ki}^2 \leq \tilde{P}_{k,max}, \quad k = 1, \dots, K \quad (3)$$

Similar to the scaling transformation to put an interference channel in standard form, [13], we can represent any GMAC-WT by an equivalent standard form as in [12]:

$$\mathbf{Y} = \sum_{k=1}^K \mathbf{X}_k + \mathbf{N}^{(M)} \quad (4a)$$

$$\mathbf{Z} = \sum_{k=1}^K \sqrt{h_k} \mathbf{X}_k + \mathbf{N}^{(W)} \quad (4b)$$

where

- the original codewords $\{\tilde{\mathbf{X}}\}$ are scaled to get $\mathbf{X}_k = \sqrt{\frac{h_k^{(M)}}{\sigma_M^2}} \tilde{\mathbf{X}}_k$.
- The eavesdropper's new channel gains are given by $h_k = \frac{h_k^{(W)} \sigma_M^2}{h_k^{(M)} \sigma_W^2}$.
- The noise vectors are normalized such that $\mathbf{N}^{(M)} = \frac{1}{\sigma_M} \tilde{\mathbf{N}}^{(M)}$ and $\mathbf{N}^{(W)} = \frac{1}{\sigma_W} \tilde{\mathbf{N}}^{(W)}$.

In [9], we examined the special case of the eavesdropper getting a degraded version of the received signal, which is equivalent to $h_1 = h_2 = \dots = h_K \equiv h < 1$. In this paper, we look at the more general case where this is not necessarily true. The model is illustrated in Figure 1.

We use the collective secrecy constraints defined in [9] to take into account the multi-access nature of the channel.

$$\Delta_S^{(C)} \triangleq \frac{H(\mathbf{W}_S | \mathbf{Z})}{H(\mathbf{W}_S)} \quad \forall \mathcal{S} \subseteq \mathcal{K} \triangleq \{1, \dots, K\} \quad (5)$$

We constrain each subset of users to maintain perfect secrecy, i.e. $\Delta_S^{(C)} \geq 1 - \epsilon$ for all sets \mathcal{S} such that $H(\mathbf{W}_S) > 0$. Since this must be true for all sets of users, collectively the system has perfect secrecy.

However, if a group of users are somehow compromised, the remaining users may also be vulnerable. Note that providing $\Delta_{\mathcal{K}}^{(C)} \geq 1 - \frac{\epsilon}{r}$, where $r \geq \sum_{k=1}^K R_k / \min_{k: R_k > 0} R_k$ guarantees the perfect secrecy of all subsets as seen by the following argument:

$$H(\mathbf{W}_{\mathcal{K}}|\mathbf{Z}) \geq H(\mathbf{W}_{\mathcal{K}}) - \frac{\epsilon}{r}H(\mathbf{W}_{\mathcal{K}}) \quad (6)$$

$$\begin{aligned} H(\mathbf{W}_{\mathcal{S}}|\mathbf{Z}) &\geq H(\mathbf{W}_{\mathcal{S}}) + H(\mathbf{W}_{\mathcal{S}^c}|\mathbf{W}_{\mathcal{S}}) \\ &\quad - H(\mathbf{W}_{\mathcal{S}^c}|\mathbf{W}_{\mathcal{S}}, \mathbf{Z}) - \frac{\epsilon}{r}H(\mathbf{W}_{\mathcal{K}}) \end{aligned} \quad (7)$$

$$\geq H(\mathbf{W}_{\mathcal{S}}) - \frac{\epsilon}{r}H(\mathbf{W}_{\mathcal{K}}) \quad (8)$$

$$\frac{H(\mathbf{W}_{\mathcal{S}}|\mathbf{Z})}{H(\mathbf{W}_{\mathcal{S}})} \geq 1 - \frac{H(\mathbf{W}_{\mathcal{K}})}{H(\mathbf{W}_{\mathcal{S}})} \frac{\epsilon}{r} \quad (9)$$

$$\Delta_{\mathcal{S}}^{(C)} \geq 1 - \epsilon \quad (10)$$

Definition 1 (Achievable rates). The rate vector $\mathbf{R} = (R_1, \dots, R_K)$ is said to be *achievable with perfect secrecy* if for any given $\epsilon > 0$ there exists a code of sufficient length n such that

$$\frac{1}{n} \log_2 M_k \geq R_k - \epsilon \quad k = 1, \dots, K \quad (11)$$

$$P_e \leq \epsilon \quad (12)$$

$$\Delta_{\mathcal{S}}^{(C)} \geq 1 - \epsilon \quad \forall \mathcal{S} \subseteq \mathcal{K} = \{1, \dots, K\} \quad (13)$$

where user k chooses one of M_k symbols to transmit according to the uniform distribution and

$$P_e = \frac{1}{\prod_{k=1}^K M_k} \sum_{\mathbf{W} \in \mathcal{W}_1 \times \mathcal{W}_2 \times \dots \times \mathcal{W}_K} \Pr\{\hat{\mathbf{W}} \neq \mathbf{W} | \mathbf{W} \text{ was sent}\}. \quad (14)$$

is the average probability of error. We will denote the set of all achievable rates with perfect secrecy \mathcal{C}_s .

Before we state our results, we define the following quantities for any $\mathcal{S} \subseteq \mathcal{K}$.

$$\begin{aligned} C_{\mathcal{S}}^{(M)} &\triangleq g\left(\sum_{k \in \mathcal{S}} P_k\right), & C_{\mathcal{S}}^{(W)} &\triangleq g\left(\sum_{k \in \mathcal{S}} h_k P_k\right) \\ \tilde{C}_{\mathcal{S}}^{(M)} &\triangleq g\left(\frac{\sum_{k \in \mathcal{S}} P_k}{1 + \sum_{k \in \mathcal{S}^c} P_k}\right) \\ \tilde{C}_{\mathcal{S}}^{(W)} &\triangleq g\left(\frac{\sum_{k \in \mathcal{S}} h_k P_k}{1 + \sum_{k \in \mathcal{S}^c} h_k P_k}\right) \end{aligned}$$

where $g(\xi) \triangleq \frac{1}{2} \log(1 + \xi)$ and $\mathcal{S}^c = \mathcal{K} \setminus \mathcal{S}$. The quantities with $\mathcal{S} = \mathcal{K}$ will sometimes also be used with the subscript *sum*. Note that these quantities are functions of $\{P_k\}_{k=1}^K$. We also define the following set of allowable powers such that $C_{\mathcal{S}}^{(M)} \geq \tilde{C}_{\mathcal{S}}^{(W)}$:

$$\mathcal{P} \triangleq \left\{ \mathbf{P} = (P_1, \dots, P_K) : \right.$$

$$\left. \begin{aligned} P_{k,max} &\geq P_k \geq 0, \quad k = 1, \dots, K, \\ \phi_{\mathcal{S}}(\mathbf{P}) &\geq 0 \quad \forall \mathcal{S} \subseteq \mathcal{K} \end{aligned} \right\} \quad (15)$$

where

$$\phi_{\mathcal{S}}(\mathbf{P}) \triangleq \sum_{k \in \mathcal{S}} P_k - \frac{\sum_{k \in \mathcal{S}} h_k P_k}{1 + \sum_{k \in \mathcal{S}^c} h_k P_k} \quad (16)$$

Note that if $h_k \leq 1 \forall k$, we are left with $\mathcal{P} \equiv \{\mathbf{P} : P_{k,max} \geq P_k \geq 0, k = 1, \dots, K\}$. On the other hand, if $h_k > 1, \forall k$, then the constraint for set \mathcal{K} forces $P_k = 0, \forall k$.

III. ACHIEVABLE RATES

Here, we present an achievable region using Gaussian codebooks. The proof is very similar to the proof of the achievable region presented in [10]. Note that, when $h_1 = \dots = h_K < 1$, the region reduces to the special case examined in [9], [10], [12].

Theorem 2. We can transmit with perfect secrecy using Gaussian codebooks at rates satisfying

$$\sum_{k \in \mathcal{S}} R_k \leq C_{\mathcal{S}}^{(M)} - \tilde{C}_{\mathcal{S}}^{(W)} \quad \forall \mathcal{S} \subseteq \mathcal{K} \quad (17)$$

where $\mathbf{P} \in \mathcal{P}$. The region containing all \mathbf{R} satisfying these equations is denoted \mathcal{G}_s .

Proof: Let $\mathbf{R} = (R_1, \dots, R_K)$ satisfy (17). For user $k \in \mathcal{K}$, consider the scheme:

- 1) Let $M_k = 2^{n(R_k - \epsilon')}$ where $0 \leq \epsilon' < \epsilon$ where ϵ' is chosen to ensure that M_k is an integer.
- 2) Generate 2 codebooks \mathfrak{X}_k and \mathfrak{X}_{kx} . \mathfrak{X}_k consists of M_k codewords, each component of which is drawn $\sim \mathcal{N}(0, \lambda_k P_k - \epsilon)$. Codebook \mathfrak{X}_{kx} has M_{kx} codewords with each component randomly drawn $\sim \mathcal{N}(0, (1 - \lambda_k)P_k - \epsilon)$ where ϵ is arbitrarily small to ensure that the power constraints on the codewords are satisfied with high probability. Define $R_{kx} = \frac{1}{n} \log M_{kx}$ and $M_{kt} = M_k M_{kx}$. Then $R_{kt} = \frac{1}{n} \log M_{kt} = R_k + R_{kx} + \epsilon'$.
- 3) To transmit message $W_k \in \{1, \dots, M_k\}$, user k finds the codeword corresponding to W_k in \mathfrak{X}_k and also uniformly chooses a codeword from \mathfrak{X}_{kx} which are then added and the resulting codeword, \mathbf{X}_k , is sent so that we are actually transmitting one of M_{kt} codewords.

The specific rates are chosen such that $\forall \mathcal{S} \subseteq \mathcal{K}$ the following are satisfied:

$$\sum_{k \in \mathcal{S}} R_k \leq C_{\mathcal{S}}^{(M)} - \tilde{C}_{\mathcal{S}}^{(W)} \quad (18)$$

$$\sum_{k=1}^K R_{kx} = C_{sum}^{(W)} \quad (19)$$

$$\sum_{k \in \mathcal{S}} R_{kt} \leq C_{\mathcal{S}}^{(M)} \quad (20)$$

From (20) and the GMAC coding theorem, with high probability the receiver can decode the codewords with low probability of error. We now need to show that the secrecy constraints are satisfied. Note that since the secrecy of the overall system ensures the secrecy of each subset, we only need to show that the coding scheme described achieves $\Delta_{\mathcal{K}} \geq 1 - \epsilon$. We concern ourselves only with MAC sub-code $\{\mathfrak{X}_k\}_{k=1}^K$. From this point of view, the coding scheme described is equivalent to each user $k \in \mathcal{K}$ selecting one of M_k messages, and sending a uniformly chosen codeword from among M_{kx} codewords for each. Define $\mathbf{X}_{\Sigma} = \sum_{k=1}^K \sqrt{h_k} \mathbf{X}_k$.

$$H(\mathbf{W}_{\mathcal{K}}|\mathbf{Z}) \tag{21}$$

$$= H(\mathbf{W}_{\mathcal{K}}, \mathbf{Z}) - H(\mathbf{Z}) \tag{22}$$

$$= H(\mathbf{W}_{\mathcal{K}}, \mathbf{X}_{\Sigma}, \mathbf{Z}) - H(\mathbf{X}_{\Sigma}|\mathbf{W}_{\mathcal{K}}, \mathbf{Z}) - H(\mathbf{Z}) \tag{23}$$

$$= H(\mathbf{W}_{\mathcal{K}}) + H(\mathbf{Z}|\mathbf{W}_{\mathcal{K}}, \mathbf{X}_{\Sigma}) - H(\mathbf{Z}) + H(\mathbf{X}_{\Sigma}|\mathbf{W}_{\mathcal{K}}) - H(\mathbf{X}_{\Sigma}|\mathbf{W}_{\mathcal{K}}, \mathbf{Z}) \tag{24}$$

$$= H(\mathbf{W}_{\mathcal{K}}) - I(\mathbf{X}_{\Sigma}; \mathbf{Z}) + I(\mathbf{X}_{\Sigma}; \mathbf{Z}|\mathbf{W}_{\mathcal{K}}) \tag{25}$$

where we used $\mathbf{W}_{\mathcal{K}} \rightarrow \mathbf{X}_{\Sigma} \rightarrow \mathbf{Z} \Rightarrow H(\mathbf{Z}|\mathbf{W}_{\mathcal{K}}, \mathbf{X}_{\Sigma}) = H(\mathbf{Z}|\mathbf{X}_{\Sigma})$ to get (25). We will consider the two terms individually. First, we have the trivial bound due to channel capacity:

$$I(\mathbf{X}_{\Sigma}; \mathbf{Z}) \leq nC_{sum}^{(w)} \tag{26}$$

Now write

$$I(\mathbf{X}_{\Sigma}; \mathbf{Z}|\mathbf{W}_{\mathcal{K}}) = H(\mathbf{X}_{\Sigma}|\mathbf{W}_{\mathcal{K}}) - H(\mathbf{X}_{\Sigma}|\mathbf{W}_{\mathcal{K}}, \mathbf{Z}) \tag{27}$$

Since user k sends one of M_{kx} codewords for each message,

$$H(\mathbf{X}_{\Sigma}|\mathbf{W}_{\mathcal{K}}) = \log(M_{1x}M_{2x}) \tag{28}$$

$$= n(R_{1x} + R_{2x}) = nC_{sum}^{(w)} \tag{29}$$

We can also write

$$H(\mathbf{X}_{\Sigma}|\mathbf{W}_{\mathcal{K}}, \mathbf{Z}) \leq n\xi_n \tag{30}$$

where $\xi_n \rightarrow 0$ as $n \rightarrow \infty$ since, with high probability, the eavesdropper can decode \mathbf{X}_{Σ} given $\mathbf{W}_{\mathcal{K}}$ due to (19). Note that the individual rates are unimportant - as far as the eavesdropper is concerned, it is receiving one of $nC_{sum}^{(w)}$ codewords with equal probability for each (W_1, W_2) pair. Using (18), (19), (26), (29) and (30) in (25), we get

$$H(\mathbf{W}_{\mathcal{K}}|\mathbf{Z}) \geq H(\mathbf{W}_{\mathcal{K}}) - nC_{sum}^{(w)} + nC_{sum}^{(w)} - n\xi_n \tag{31}$$

$$= H(\mathbf{W}_{\mathcal{K}}) - n\xi_n \tag{32}$$

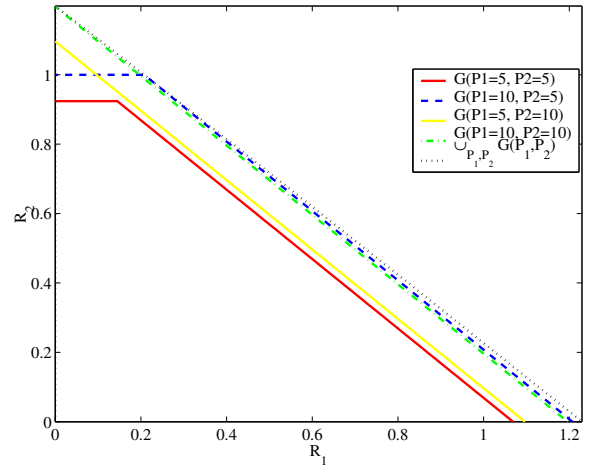


Fig. 2. Achievable rate region for $h_1 = .1, h_2 = .2, P_{1,max} = 10, P_{2,max} = 10$

and dividing both sides by $H(\mathbf{W}_{\mathcal{K}})$ gives

$$\Delta_{\mathcal{K}}^{(C)} \geq 1 - \frac{\xi_n}{\sum_{k=1}^K R_k} \tag{33}$$

completing the proof. An intuitive way of looking at this is as “capacity stuffing with superfluous information”. For each message pair, the eavesdropper can decode the extra “sum-codeword” transmitted if it knew which messages were sent, but since this information arrives at its capacity, it cannot gain any information about the actual transmitted messages. For a single-user system consisting of user k , if $h_k \geq 1$, then the secrecy capacity for that user would have been 0. However, the multi-access nature of the channel enables a different user j with $h_j < 1$ to “help” such a user achieve a non-zero rate with perfect secrecy. \square

IV. MAXIMIZATION OF SUM RATE

The achievable region given in Theorem 2 depends on the transmit powers. We are naturally interested in the power allocation $\mathbf{P}^* = (P_1^*, \dots, P_K^*)$ that would maximize the total throughput, i.e. the sum rate. However, the sum rate maximization is a non-trivial problem since the powers have to be constrained to \mathcal{P} . WLOG, assume that the users are ordered such that $h_1 \leq h_2 \leq \dots \leq h_K$.

$$\max_{\mathbf{P} \in \mathcal{P}} C_{sum}^{(M)} - C_{sum}^{(w)} \tag{34}$$

$$= \max_{\mathbf{P} \in \mathcal{P}} g\left(\sum_{k=1}^K P_k\right) - g\left(\sum_{k=1}^K h_k P_k\right) \tag{35}$$

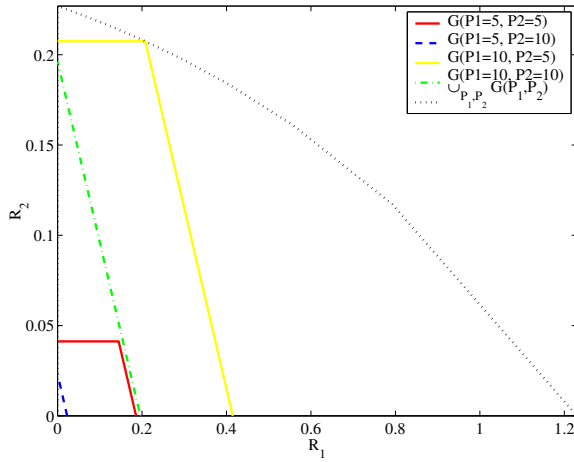


Fig. 3. Achievable rate region for $h_1 = .1, h_2 = 1.4, P_{1,max} = 10, P_{2,max} = 10$

$$= \min_{\mathbf{P} \in \mathcal{P}} \frac{1}{2} \log \rho(\mathbf{P}) \quad (36)$$

$$\equiv \min_{\mathbf{P} \in \mathcal{P}} \rho(\mathbf{P}) \quad (37)$$

where we used the monotonicity of the log function and

$$\rho(\mathbf{P}) \triangleq \frac{1 + \sum_{k=1}^K h_k P_k}{1 + \sum_{k=1}^K P_k} \quad (38)$$

We start with writing the Lagrangian to be minimized,

$$\mathcal{L}(\mathbf{P}, \boldsymbol{\mu}) = \rho(\mathbf{P}) - \sum_{k=1}^K \mu_{1k} P_k + \sum_{k=1}^K \mu_{2k} (P_k - P_{k,max}) - \sum_{S \subseteq \mathcal{K}} \mu_{3S} \phi_S(\mathbf{P}) \quad (39)$$

Equating the derivative of the Lagrangian to zero, we get

$$\frac{\partial \mathcal{L}(\mathbf{P}, \boldsymbol{\mu})}{\partial P_j} = \dot{\rho}^{(j)}(\mathbf{P}) - \mu_{1j} + \mu_{2j} - \sum_{S \subseteq \mathcal{K}} \mu_{3S} \dot{\phi}_S^{(j)}(\mathbf{P}) = 0 \quad (40)$$

where

$$\dot{\rho}^{(j)}(\mathbf{P}) \triangleq \frac{\partial \rho(\mathbf{P})}{\partial P_j} = \frac{h_j - \rho(\mathbf{P})}{1 + \sum_{k=1}^K P_k} \quad (41)$$

$$\dot{\phi}_S^{(j)}(\mathbf{P}) \triangleq \frac{\partial \phi_S(\mathbf{P})}{\partial P_j} = \begin{cases} 1 - \frac{h_j}{1 + \sum_{k \in S^c} h_k P_k}, & \text{if } j \in S \\ \frac{h_j \sum_{k \in S} h_k P_k}{(1 + \sum_{k \in S^c} h_k P_k)^2}, & \text{if } j \notin S \end{cases} \quad (42)$$

We begin with the following lemma:

Lemma 3. Let \mathbf{P}^* be the optimum power allocation. For a user $k \in \mathcal{K}$, if $h_k \geq 1$, then $P_k^* = 0$.

Proof: Assume this statement is wrong, i.e., let $\mathcal{T} = \{k \in \mathcal{K} : h_k \geq 1, P_k^* > 0\} \neq \emptyset$. Consider \mathbf{Q} such that $Q_k = P_k^*$, $k \notin \mathcal{T}$ and $Q_k = 0$, $k \in \mathcal{T}$. In other words, for a user k , $Q_k = P_k^*$ if $h_k < 1$ and $Q_k = 0$ if $h_k \geq 1$. We first check to see whether $\mathbf{Q} \in \mathcal{P}$.

Since $\mathbf{P}^* \in \mathcal{P}$, $\mathbf{P}_{max} \succeq \mathbf{Q} \succeq \mathbf{0}$, so we only need to check if $\phi_S(\mathbf{Q}) \geq 0 \forall S$.

$$\phi_S(\mathbf{Q}) = \sum_{j \in S} Q_j - \frac{\sum_{j \in S} h_j Q_j}{1 + \sum_{j \in S^c} h_j Q_j} \quad (43)$$

$$= \sum_{j \in S - \mathcal{T}} Q_j + \sum_{j \in S \cap \mathcal{T}} Q_j - \frac{\sum_{j \in S - \mathcal{T}} h_j Q_j + \sum_{j \in S \cap \mathcal{T}} h_j Q_j}{1 + \sum_{j \in S^c} h_j Q_j} \quad (44)$$

$$= \sum_{j \in S - \mathcal{T}} P_j^* - \frac{\sum_{j \in S - \mathcal{T}} h_j P_j^*}{1 + \sum_{j \in S^c} h_j Q_j} \quad (45)$$

$$\geq \sum_{j \in S - \mathcal{T}} P_j^* - \sum_{j \in S - \mathcal{T}} h_j P_j^* \quad (46)$$

$$\geq 0 \quad (47)$$

since all users $k \in S - \mathcal{T}$ must have $h_k < 1$. The proof will be complete if we can show that this new power allocation also increases the sum rate achieved, or equivalently decreases ρ . Begin by writing

$$\rho(\mathbf{Q}) = \frac{1 + \sum_{k=1}^K h_k Q_k}{1 + \sum_{k=1}^K Q_k} \quad (48)$$

$$= \frac{1 + \sum_{k \in \mathcal{T}} h_k Q_k + \sum_{k \in \mathcal{T}^c} h_k Q_k}{1 + \sum_{k \in \mathcal{T}} Q_k + \sum_{k \in \mathcal{T}^c} Q_k} \quad (49)$$

$$= \frac{1 + \sum_{k \in \mathcal{T}^c} h_k P_k^*}{1 + \sum_{k \in \mathcal{T}^c} P_k^*} \quad (50)$$

$$\leq \frac{1 + \sum_{k \in \mathcal{T}^c} h_k P_k^* + \sum_{k \in \mathcal{T}} h_k P_k^*}{1 + \sum_{k \in \mathcal{T}^c} P_k^* + \sum_{k \in \mathcal{T}} P_k^*} \quad (51)$$

$$= \rho(\mathbf{P}^*) \quad (52)$$

where we have used $\frac{a}{b} \leq \frac{a+c}{b+d}$ if $\frac{a}{b} \leq 1$ and $\frac{c}{d} \geq 1$ when $a, b, c, d \geq 0$. \square

This lemma basically states that to maximize the sum-rate, any user who has a better or equivalent eavesdropper channel must cease transmission. Now, we look at the optimum power allocation among the remaining users. This is stated in the below lemma:

Theorem 4. The optimum power allocation \mathbf{P}^* satisfies $P_k^* = P_{k,max}$ for $k = 1, \dots, l$ and $P_k^* = 0$ for $k = l + 1, \dots, K$ where l is some limiting user such

that

$$h_l < \frac{1 + \sum_{k=1}^l h_k P_{k,max}}{1 + \sum_{k=1}^l P_{k,max}} \leq h_{l+1} \quad (53)$$

Proof: From Lemma 3, we see that if $h_k \geq 1$, then $P_k^* = 0$ for all $k \in \mathcal{S}$. Thus, we have $\phi_{\mathcal{S}}(\mathbf{P}^*) \geq 0$ with equality if and only if $P_k^* = 0$ for all $k \in \mathcal{S}$. Then, from the supplementary conditions, we must have $\mu_{3\mathcal{S}} = 0$ for all \mathcal{S} containing a transmitting user, and $\sum_{k \in \mathcal{S}} P_k^* = 0$ for all \mathcal{S} not containing a transmitting user. As a result, $\mu_{3\mathcal{S}} \dot{\phi}_{\mathcal{S}}^{(j)}(\mathbf{P}^*) = 0$, $\forall \mathcal{S} \subseteq \mathcal{K}$. Then, it is easy to see that $P_j^* = P_{j,max}$ if $h_j < \rho(\mathbf{P}^*)$ and $P_j^* = 0$ if $h_j > \rho(\mathbf{P}^*)$. A user j may have $0 < P_j^* < P_{j,max}$ iff $h_j = \rho(\mathbf{P}^*)$. However, then the sum rate is independent of that user's power, so we could set $P_j^* = 0$ without any loss in sum rate achievable, and conserve power. The next step is to find this limiting user l . It is easy to see that this user must satisfy (53), and can be found in at most K steps. \square

V. SECRECY THROUGH COLLABORATION

In the previous section, we showed that the sum secrecy rate is maximized when users with $h_k \geq 1$ do not transmit. An interesting question in this case, is whether such a user can somehow help increase the secrecy capacity for another user that has $h_k < 1$ and is transmitting at full power. We will show that this is possible in some cases, namely by using the fact that a user with $h_k \geq 1$ can have a 'more adverse' effect on the eavesdropper than on the intended receiver. We will consider the two-user scenario and examine two cases:

A. $h_1 < 1 \leq h_2$

Consider the same case examined in the previous section: $h_1 < 1 \leq h_2$. The sum-rate achievable with perfect secrecy was shown to be $C_s = g(P_{1,max}) - g(h_1 P_{1,max})$ with $P_1 = P_{1,max}$, $P_2 = 0$. User 2, rather than sit idle, can help user 1 by generating white noise and sending this across the channel. This will create additional noise at the intended receiver, but even more additional noise at the eavesdropper's receiver. Since the secrecy capacity in the now single-user channel is known to be the difference of the channel capacities, this scheme may increase the secrecy capacity by reducing the eavesdropper's channel capacity more than it does the intended receiver's. The problem at hand can be written as:

$$\begin{aligned} & \max_{(P_1, P_2)} g\left(\frac{P_1}{1+P_2}\right) - g\left(\frac{h_1 P_1}{1+h_2 P_2}\right) \\ & \text{s. t. } 0 \leq P_1 \leq P_{1,max}, 0 \leq P_2 \leq P_{2,max} \end{aligned} \quad (54)$$

Start by writing the Lagrangian using the monotonicity of log:

$$\begin{aligned} \mathcal{L}(\mathbf{P}, \boldsymbol{\mu}) = & -\frac{(1+P_1+P_2)(1+h_2 P_2)}{(1+P_2)(1+h_1 P_1+h_2 P_2)} \\ & - \sum_{k=1}^2 \mu_{1k} P_k + \sum_{k=1}^2 \mu_{2k} (P_k - P_{k,max}) \end{aligned} \quad (55)$$

Consider user 1:

$$\begin{aligned} \frac{\partial \mathcal{L}(\mathbf{P}, \boldsymbol{\mu})}{\partial P_1} = & \frac{\Psi_1(P_2)}{(1+P_2)(1+h_1 P_1+h_2 P_2)^2} \\ & - \mu_{11} + \mu_{21} = 0 \end{aligned} \quad (56)$$

where

$$\Psi_1(P_2) = -(1+h_2 P_2)[(1-h_1) + (h_2-h_1)P_2] \quad (57)$$

$\Psi_1(P_2)$ is always negative due to $h_1 < 1 \leq h_2$. Hence, we must have $\mu_{21} > 0 \Rightarrow P_1 = P_{1,max}$. Now examine user 2:

$$\begin{aligned} \frac{\partial \mathcal{L}(\mathbf{P}, \boldsymbol{\mu})}{\partial P_2} = & \frac{\Psi_2(P_1, P_2)}{(1+P_2)^2(1+h_1 P_1+h_2 P_2)^2} \\ & - \mu_{21} + \mu_{22} = 0 \end{aligned} \quad (58)$$

where

$$\Psi_2(P_1, P_2) = P_1 h_2 (h_2 - h_1) (P_2 - p^{(1)}) (P_2 - p^{(2)}) \quad (59)$$

$$p^{(1)} = \frac{-h_2(1-h_1) + \sqrt{D}}{h_2(h_2-h_1)}, \quad (60)$$

$$p^{(2)} = \frac{-h_2(1-h_1) - \sqrt{D}}{h_2(h_2-h_1)}, \quad (61)$$

$$D = h_1 h_2 [(h_2-1) + (h_2-h_1)P_1] (h_2-1) \quad (62)$$

We already know that $P_1 = P_{1,max}$. Note that if $\Psi_2(P_{1,max}, P_2) > 0$, then we must have $\mu_{21} > 0 \Rightarrow P_2 = 0$. On the other hand, if $\Psi_2(P_{1,max}, P_2) < 0$, then $\mu_{22} > 0 \Rightarrow P_2 = P_{2,max}$. Only when $\Psi_2(P_{1,max}, P_2) = 0$ do we have $0 < P_2 < P_{2,max}$. It is easy to see that $D \geq (h_2-1)\sqrt{h_1 h_2} \geq 0$ and hence $p^{(2)} < 0$. $\Psi_2(P_{1,max}, P_2)$ is an upright parabola with respect to P_2 with at least one negative root. As a result, if the other root, $p^{(1)}$ is also negative, then $\Psi_2(P_{1,max}, P_2) > 0 \Rightarrow P_2 = 0$. An example is when $h_2 = 1 \Rightarrow p^{(1)} = p^{(2)}$. If $p^{(1)}$ is positive, then we have two possibilities, either P_2 lies between the roots, in which case $\Psi_2(P_{1,max}, P_2) < 0 \Rightarrow P_2 = P_{2,max}$, or $P_2 \geq p^{(1)}$. Since the latter would imply $\Psi_2(P_{1,max}, P_2) > 0$ and hence $P_2 = 0$, it is not

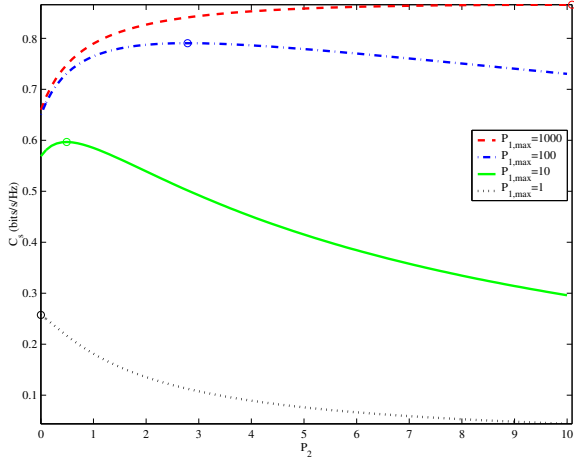


Fig. 4. Sum capacity as a function of P_2 with different $P_{1,max}$ for $P_{2,max} = 10$, $h_1 = .4$, $h_2 = 1.4$

possible. Thus, the optimal solution is

$$P_1 = P_{1,max}, \quad P_2 = \begin{cases} 0, & \text{if } p^{(1)} \leq 0 \\ p^{(1)}, & \text{if } 0 < p^{(1)} \leq P_{2,max} \\ P_{2,max}, & \text{if } p^{(1)} > P_{2,max} \end{cases} \quad (63)$$

The condition to have $p^{(1)} \leq 0$ is equivalent to $P_{1,max} \leq \frac{1-h_1h_2}{h_1(h_2-h_1)}$. Note that if $h_1h_2 \geq 1$, regardless of $P_{1,max}$, user 2 can always help increase the secrecy capacity.

B. $1 \leq h_1 < h_2$

Now consider the case where neither user could transmit in the region given in Section 3. We are motivated by the previous result to see whether user 2 can actually make it possible for user 1 to transmit with perfect secrecy. Our optimization problem and the Lagrangian are the same as given in (54) and (55). This time $\Psi_1(P_2)$ has a single root with $P_2 \geq 0$, and is not necessarily negative. Depending on its value, we will have different optimum P_1 values. Thus,

- (i) $P_2 < \frac{h_1-1}{h_2-h_1} \Rightarrow \Psi_1(P_2) > 0 \Rightarrow \mu_{11} > 0 \Rightarrow P_1 = 0$.
- (ii) $P_2 = \frac{h_1-1}{h_2-h_1} \Rightarrow \Psi_1(P_2) = 0 \Rightarrow \mu_{11} = \mu_{21} = 0$.
- (iii) $P_2 > \frac{h_1-1}{h_2-h_1} \Rightarrow \Psi_1(P_2) < 0 \Rightarrow \mu_{21} > 0 \Rightarrow P_1 = P_{1,max}$.

Now look at user 2. Again, $D > 0$ and $\Psi_2(P_1, P_2)$ is an upright parabola of P_2 . However, this time we are guaranteed a positive root as $p^{(1)} > 0$, and the solution for P_2 depends on $p^{(2)}$. Consider each of the above cases: In (i) and (ii), $C_s = 0$ regardless of P_1 , so we are not interested in P_2 . Consider case (iii): We then

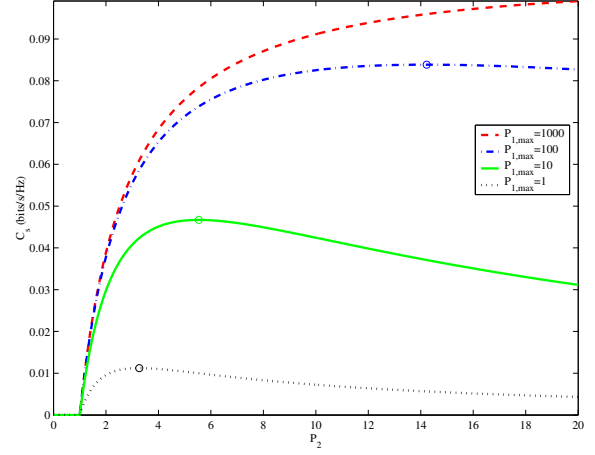


Fig. 5. Sum capacity as a function of P_2 with different $P_{1,max}$ for $P_{2,max} = 20$, $h_1 = 1.2$, $h_2 = 1.4$

have $P_2 > p^{(2)}$. If $P_2 < p^{(1)}$, then $\Psi_2(P_1, P_2) < 0$, and $P_2 = P_{2,max}$. If $P_2 \geq p^{(1)}$, then $\Psi_2(P_1, P_2) \geq 0$. Since we cannot have $\mu_{21} > 0$ at the same time, the only solution is $P_2 = p^{(1)}$. Summarizing, we get

$$\mathbf{P} = \begin{cases} (0, 0), & \text{if } P_{2,max} \leq \frac{h_1-1}{h_2-h_1} \\ (P_{1,max}, P_{2,max}), & \text{if } \frac{h_1-1}{h_2-h_1} < P_{2,max} \leq p^{(1)} \\ (P_{1,max}, p^{(1)}), & \text{if } P_{2,max} > p^{(1)} \end{cases} \quad (64)$$

Note that the solution is of the same form as the previous case. As long as user 2 has enough power to make user 1's effective channel better than the eavesdropper's, user 1 can transmit at full power as in the previous setting. User 1 could also have helped user 2, but it is better for the "worse" user to help the "better" user to maximize the sum rate.

VI. CONCLUSIONS

In this paper, we found an achievable rate region for the General Gaussian Multiple-Access Wire-Tap Channel (GGMAC-WT), in which a second wireless receiver is eavesdropping on the uplink of a GMAC. We also showed that the sum-rate is maximized when only users with "better" channels to the intended receiver as opposed to the eavesdropper transmit, and they do so using all their available power. Moreover we have explored the possibility of the users with worse channels to the intended receiver helping the transmitting users by jamming. This scheme, which we term *collaborative secrecy*, is analyzed for the two user case.

REFERENCES

- [1] A. Wyner, "The wire-tap channel," *Bell Sys. Tech. J.*, vol. 54, pp. 1355–1387, 1975.

- [2] A. B. Carleial and M. E. Hellman, "A note on Wyner's wiretap channel," *IEEE Trans. Inform. Theory*, vol. 23, no. 3, pp. 387–390, May 1977.
- [3] S. K. Leung-Yan-Cheong and M. E. Hellman, "Gaussian wiretap channel," *IEEE Trans. Inform. Theory*, vol. 24, no. 4, pp. 451–456, July 1978.
- [4] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
- [5] H. Yamamoto, "On secret sharing communication systems with two or three channels," *IEEE Trans. Inform. Theory*, vol. 32, no. 3, pp. 387 – 393, May 1986.
- [6] —, "A coding theorem for secret sharing communication systems with two Gaussian wiretap channels," *IEEE Trans. Inform. Theory*, vol. 37, no. 3, pp. 634 – 638, May 1991.
- [7] Y. Oohama, "Coding for relay channels with confidential messages," in *Proc. Of IEEE Information Theory Workshop*, 2001, pp. 87 – 89.
- [8] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. Of Int. Symp. Inf. Theory (ISIT)*, 2006.
- [9] E. Tekin, S. Şerbetli, and A. Yener, "On secure signaling for the Gaussian multiple access wire-tap channel," in *Proc. 2005 Asilomar Conf. On Signals, Systems, and Computers*, Asilomar, CA, November 2005.
- [10] E. Tekin and A. Yener, "The gaussian multiple-access wiretap channel with collective secrecy constraints," in *Proc. Int. Symp. On Inf. Theory (ISIT)*, Seattle, WA, July 9–14, 2006.
- [11] Y. Liang and V. Poor, "Generalized multiple access channels with confidential messages," in *Proc. Of IEEE Int. Symp. Inf. Theory (ISIT)*, 2006.
- [12] E. Tekin and A. Yener, "The Gaussian multiple-access wiretap channel with collective secrecy constraints," *IEEE Trans. Inform. Theory*, submitted for publication.
- [13] A. B. Carleial, "Interference channels," *IEEE Trans. Inform. Theory*, vol. 24, no. 1, pp. 60–70, January 1978.