On Secure Signaling for the Gaussian Multiple Access Wire-Tap Channel

Ender Tekin *tekin@psu.edu*
Semih Şerbetli *serbetli@psu.edu*
Aylin Yener *yener@ee.psu.edu*

Wireless Communications and Networking Laboratory
Electrical Engineering Department
The Pennsylvania State University
University Park, PA 16802

***Abstract*— We consider the Gaussian Multiple Access Wire-Tap Channel (GMAC-WT) where multiple users communicate with the intended receiver in the presence of an intelligent and informed wire-tapper (eavesdropper). The wire-tapper receives a degraded version of the signal at the receiver. We assume that the wire-tapper is as capable as the intended receiver, and there is no other shared secret key. We consider two different secure communication scenarios: (i) keeping the wire-tapper totally ignorant of the message of any group of users even if the remaining users are compromised, (ii) using the secrecy of the other users to ensure secrecy for a group of users. We first derive the outer bounds for the secure rate region. Next, using Gaussian codebooks, we show the achievability of a secure rate region for each measure in which the wire-tapper is kept perfectly ignorant of the messages. We also find the power allocations that yield the maximum sum rate, and show that upper bound on the secure sum rate can be achieved by a TDMA scheme. We present numerical results showing the new rate region and compare it with that of the Gaussian Multiple-Access Channel (GMAC) with no secrecy constraints.**

I. Introduction

The notion of communication security is first analyzed by Shannon in [1], where he showed that the necessary and sufficient condition for perfect secrecy is to make the conditional probability of the *cryptogram given a message* independent of the actual transmitted message.

In [2], Wyner applied this concept to the discrete memoryless channel, with a wire-tapper that is modeled as receiving a degraded version of the intended receiver's signal. In this work, the amount of "secrecy" is measured using the conditional entropy $\Delta \triangleq H(S^K|Z^N)$, where S^K is the transmitted symbol, and Z^N is the received signal at the wire-tapper. The region of all possible (R, Δ) pairs is determined, and the existence of a *secrecy capacity*, C_s, for communication below which it is possible to transmit zero information to the wire-tapper is shown [2].

Several research results followed reference [2]. Carleial and Hellman, in [3], showed that it is possible to send several low-rate messages, each completely protected from the wire-tapper individually, and thus use the channel at capacity. The drawback is, in this case, if any of the messages are revealed to the wire-tapper, the others might also be compromised. In [4], the authors extended Wyner's results to Gaussian channels. In addition, they showed that Carleial and Hellman's results in [3] also held for the Gaussian channel [4]. Csiszár and Körner, in [5], 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, and private information to the receiver only.

In this paper, we consider the Gaussian Multiple Access Channel (GMAC) in the presence of a wire-tapper. In order to extend Leung's results to the multiple-access channel, we first define the necessary security measures for keeping the wire-tapper perfectly ignorant of the messages. We consider two different sets of security constraints: (i) 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 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. Under these constraints, we find an outer bound for the perfectly secure rate region. Using random Gaussian codebooks, we find an achievable *secure rate region* for each constraint, where users can communicate with arbitrarily small probability of error with the intended receiver, while the wire-tapper is kept totally ignorant. We then find the optimum power allocation policy that maximizes the secure sum rate. We also show that by using optimum time-sharing, it is possible to achieve the secure sum rate outer bound, as for the standard MAC region [6]. Our results indicate that to maintain secrecy while keeping the data rates close to the maximum requires that the wire-tapper sees a much more noisier version of the signal that the intended receiver gets. Even if the powers of the users are unlimited, the sum rate with the perfect secrecy constraints is limited.

II. System Model and Problem Statement

We consider K users communicating with a receiver in the presence of a wire-tapper, as illustrated in Figure 1.

This work was supported in part by NSF grant CCF 05-14813

1-4244-0132-1/05/$20.00 ©2005 IEEE

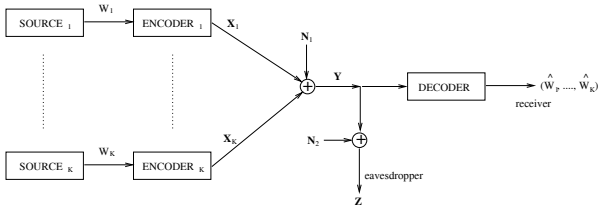

Fig. 1. The GMAC-WT System Model

Transmitter j chooses a message W_j from a set of equally likely messages $\{1, \ldots, M_j\}$. The messages are encoded using $(2^{nR_j}, n)$ codes into $\{X_j^n(W_j)\}$, where $R_j = \frac{1}{n}\log_2 M_j$. The encoded messages are then transmitted, and the intended receiver and the wire-tapper each get a copy Y^n and Z^n. 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 signal at the intended receiver is given by

$$\mathbf{Y} = \sum_{j=1}^{K} \mathbf{X}_j + \mathbf{N}_1 \tag{1}$$

where each component of $\mathbf{N}_1 \sim \mathcal{N}\left(0, \sigma_1^2\right)$. The receiver then uses its decoder to estimate $g(\mathbf{Y}) = (\hat{W}_1, \ldots, \hat{W}_K)$.

The wire-tapper receives

$$\mathbf{Z} = \mathbf{Y} + \mathbf{N}_2 \tag{2}$$

where each component of $\mathbf{N}_2 \sim \mathcal{N}\left(0, \sigma_2^2\right)$.

We will also assume the following power constraints:

$$\frac{1}{n}\sum_{i=1}^{n} X_{ji}^2 \leq P_{j,max},\ j = 1, \ldots, K \tag{3}$$

III. Secrecy Measures

In this section, we define the secrecy measures for the GMAC-WT. We aim to provide each user with perfect secrecy. To that end, we use an approach similar to [4], and define two different sets of secrecy constraints using the normalized equivocations for sets of users.

A. Individual Secrecy

Let us first define

$$\Delta_j^{(I)} \triangleq \frac{H(W_j|\mathbf{X}_{j^c}, \mathbf{Z})}{H(W_j)} \quad \forall j = 1, \ldots, K \tag{4}$$

where j^c is the set of all users except user j. $\Delta_j^{(I)}$ denotes the normalized entropy of user j's message given the received signal at the wire-tapper as well as all the other users' transmitted codewords.

As our secrecy criterion, we require that each user $j \in \{1, \ldots, K\}$ must satisfy $\Delta_j^{(I)} = 1$. This constraint guarantees that information obtained at the wire-tapper about the user j's signal is zero even if all the other users are compromised. Let us define the secrecy measure for a subset of users, $\mathcal{S} \subseteq \mathcal{K} = \{1, \ldots, K\}$, as

$$\Delta_{\mathcal{S}}^{(I)} \triangleq \frac{H(\mathbf{W}_{\mathcal{S}}|\mathbf{X}_{\mathcal{S}^c}, \mathbf{Z})}{H(\mathbf{W}_{\mathcal{S}})} \quad \forall \mathcal{S} \subseteq \mathcal{K} = \{1, \ldots, K\} \tag{5}$$

where $\mathcal{S}^c = \mathcal{K} \setminus \mathcal{S}$. We can show that the individual secrecy constraints $\{\Delta_j^{(I)} = 1\}$ for all users in the set $\mathcal{S}$ result in

$$H(\mathbf{W}_{\mathcal{S}}|\mathbf{X}_{\mathcal{S}^c}, \mathbf{Z}) \geq \sum_{i\in\mathcal{S}} H(W_i|\mathbf{X}_{i^c}, \mathbf{Z}) = \sum_{i\in\mathcal{S}} H(W_i) = H(\mathbf{W}_{\mathcal{S}})$$

Thus, for any set of users $\mathcal{S} \subseteq \mathcal{K} = \{1, \ldots, K\}$, the individual secrecy constraints $\{\Delta_j^{(I)} = 1\}$ for all users in the subset $\mathcal{S}$ also guarantees the joint perfect secrecy of the set $\mathcal{S}$, i.e. $\Delta_{\mathcal{S}}^{(I)} = 1$. By using individual perfect secrecy constraints, we can also provide perfect secrecy for all users.

B. Collective Secrecy

Clearly, (4) is a conservative measure. Let us now define a revised secrecy measure.

$$\Delta_{\mathcal{S}}^{(C)} \triangleq \frac{H(\mathbf{W}_{\mathcal{S}}|\mathbf{Z})}{H(\mathbf{W}_{\mathcal{S}})} \quad \forall \mathcal{S} \subseteq \mathcal{K} \tag{6}$$

We again need to ensure that $\Delta_{\mathcal{S}}^{(C)} = 1\ \forall \mathcal{S} \subseteq \mathcal{K}$. This constraint guarantees that each subset of users maintains perfect secrecy. Since this must be true for all sets of users, collectively the system is secure. These constraints, as expected, lead to a larger rate region than the more strict individual constraints. However, if a group of users are somehow compromised, the remaining users may also be vulnerable.

In this case, it can be shown that perfect secrecy for the set of all users guarantees perfect secrecy for any subset of users.

$$\begin{aligned} H(\mathbf{W}_{\mathcal{S}}|\mathbf{Z}) + H(\mathbf{W}_{\mathcal{S}^c}|\mathbf{Z}) &\geq H(\mathbf{W}_{\mathcal{K}}|\mathbf{Z})) && (7)\\ &= H(\mathbf{W}_{\mathcal{K}}) && (8)\\ &= H(\mathbf{W}_{\mathcal{S}}) + H(\mathbf{W}_{\mathcal{S}^c}) && (9) \end{aligned}$$

which, since conditioning reduces entropy, implies $H(\mathbf{W}_{\mathcal{S}}|\mathbf{Z}) = H(\mathbf{W}_{\mathcal{S}})$.

This is a reversal of what happens for the individual constraints case, where perfect secrecy of individual users leads to perfect secrecy of all sets of users.

IV. Outer Bounds

Our aim here is to find an outer bound for the rate tuples $(R_1, R_2, \ldots, R_K)$ for which the individual or collective secrecy constraints $\Delta_{\mathcal{S}} = 1\, \forall \mathcal{S} \subseteq \mathcal{K}$ can be satisfied.

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

$$P_{\mathcal{S}} \triangleq \sum_{j\in\mathcal{S}} P_j \qquad R_{\mathcal{S}} \triangleq \sum_{j\in\mathcal{S}} R_j$$

$$C_{\mathsf{M},\mathcal{S}} \triangleq C\left(\frac{P_{\mathcal{S}}}{\sigma_1^2}\right) \quad C_{\mathsf{MW},\mathcal{S}} \triangleq C\left(\frac{P_{\mathcal{S}}}{\sigma_1^2+\sigma_2^2}\right)$$

$$C'_{\mathsf{MW},\mathcal{S}} \triangleq C\left(\frac{P_{\mathcal{S}}}{P_{\mathcal{S}^c}+\sigma_1^2+\sigma_2^2}\right)$$

where $C(\xi) \triangleq \frac{1}{2}\log(1+\xi)$. The quantities with $\mathcal{S} = \mathcal{K}$ will sometimes also be used with the subscript *sum*.

A. Individual Secrecy

Theorem 1. For the GMAC-WT, the secure rate-tuples $(R_1, \ldots, R_K)$ such that $\Delta_{\mathcal{S}}^{(I)} = 1$, $\forall \mathcal{S} \subseteq \mathcal{K}$ must satisfy

$$R_{\mathcal{S}} \leq C_{\mathsf{M},\mathcal{S}} - C_{\mathsf{MW},\mathcal{S}} \quad \forall \mathcal{S} \subseteq \mathcal{K} \tag{10}$$

The set of all such rate vectors will be denoted $\mathcal{R}_{out}^{(I)}$.

Proof: We have proved a more general version of the outer bound for any $\Delta \in [0, 1]$, such that $\Delta_{\mathcal{S}} \geq \Delta$ i.e., where secrecy is not necessarily perfect. Due to space constraints, we present a brief outline in Appendix I. □

The maximum sum rate is then bounded by

$$R_{sum} = R_{\mathcal{K}} \leq C\left(\frac{P_{\mathcal{K}}}{\sigma_1^2}\right) - C\left(\frac{P_{\mathcal{K}}}{\sigma_1^2 + \sigma_2^2}\right) \tag{11}$$

B. Collective Secrecy

Theorem 2. For the GMAC-WT, the secure rate-tuples $(R_1, \ldots, R_K)$ such that $\Delta_{\mathcal{S}}^{(C)} = 1$, $\forall \mathcal{S} \subseteq \mathcal{K}$ must satisfy

$$R_{\mathcal{S}} \leq C_{\mathsf{M},\mathcal{S}} - C\left(\frac{\sum_{j \in \mathcal{S}} 2^{\frac{2}{n} H(\mathbf{X}_j)}}{2\pi e \left(P_{\mathcal{S}^c} + \sigma_1^2 + \sigma_2^2\right)}\right) \tag{12}$$

The set of all such $\mathbf{R}$ is designated as $\mathcal{R}_{out}^{(C)}$.

Corollary 2.1. The sum-rate with perfect secrecy satisfies

$$R_{\mathcal{K}} \leq C_{\mathsf{M},\mathcal{K}} - C_{\mathsf{MW},\mathcal{K}} \tag{13}$$

Corollary 2.2. The perfectly secure rate-tuples using Gaussian codebooks must satisfy

$$R_{\mathcal{S}} \leq C_{\mathsf{M},\mathcal{S}} - C'_{\mathsf{MW},\mathcal{S}} \quad \forall \mathcal{S} \subseteq \mathcal{K} \tag{14}$$

This region will be denoted by $\widehat{\mathcal{R}}_{out}^{(C)}$.

Proof: We again have stronger versions of these results. See Appendix I for a brief outline. □

Remark: Since $C_{\mathsf{MW},\mathcal{K}} = C'_{\mathsf{MW},\mathcal{K}}$, Corollary 2.2 indicates that Gaussian codebooks have the same upper bound on sum capacity as what is given by Corollary 2.1.

C. Comments on the Outer Bounds

Note that there is a reduction of $C_{\mathsf{MW},\mathcal{K}} = C\left(\frac{\sum_{i=1}^{K} P_i}{\sigma_1^2 + \sigma_2^2}\right)$ in the sum rate due to providing full secrecy for all users. Thus, by limiting the information at the wire-tapper we also limit our sum rate. The outer bounds are polymatroids as for the general GMAC. Both upper bounds have the same sum-rate bound, but the individual secrecy polymatroid will be contained within the collective secrecy polymatroid.

V. Inner Bounds

In this section, we find coding schemes that provide a rate region close to the outer bound we found for the rate tuples in Section IV. We find a region smaller than the bound given in Theorem 1 for the individual case, while achieving the outer bound for Gaussian codebooks presented in Corollary 2.2.

A. Individual Secrecy

In [4], it has been shown that Gaussian codebooks can be used to maintain secrecy for a single user wire-tap channel. Using a similar approach, we show that an achievable region for perfect secrecy using individual constraints is given by:

Theorem 3. The following region, $\widehat{\mathcal{R}}_{ach}^{(I)}$, is achievable with perfect secrecy for the GMAC-WT using Gaussian codebooks.

$$\widehat{\mathcal{R}}_{ach}^{(I)} = \left\{\mathbf{R} \colon R_{\mathcal{S}} \leq C_{\mathsf{M},\mathcal{S}} - \sum_{j \in \mathcal{S}} C_{\mathsf{MW},j} \quad \forall \mathcal{S} \subseteq \mathcal{K}\right\} \tag{15}$$

Proof: See Appendix II for an outline. □

In this case, the maximum sum rate achievable is given by

$$R_{\mathcal{S}} = C_{\mathsf{M},\mathcal{K}} - \sum_{j=1}^{K} C_{\mathsf{MW},j} \tag{16}$$

Observe that there is a reduction of $\sum_{j=1}^{K} C_{\mathsf{MW},j} \geq C_{\mathsf{MW},sum}$ in the sum rate due to secrecy constraints. This scheme, using stochastic encoding and Gaussian codebooks, achieves a sum rate that is less than the outer bound defined in (11). Also observe that transmission of all the users with their maximum power may not be optimal for this case. To maximize the sum rate, we pose the following power allocation problem:

$$\max_{\mathbf{P}} \; C_{sum} = C_{\mathsf{M},\mathcal{K}} - \sum_{j=1}^{K} C_{\mathsf{MW},j} \quad \text{s. t. } P_j \leq P_{j,max} \tag{17}$$

The solution to this problem is given by the theorem below:

Theorem 4. The optimum power allocation is such that:

- Any given user transmits either with all its power or does not transmit, i.e., $P_j = 0$ or $P_j = P_{j,max}$, $j = 1, \ldots, K$.
- The sum-capacity maximizing set of users who are transmitting with full power, $\mathcal{T}$, should satisfy

$$\frac{\partial C_{sum}}{\partial P_j} > 0 \, \forall j \in \mathcal{T} \Rightarrow \sum_{k \in \mathcal{T}} P_{k,max} \leq P_j + \sigma_2^2, \; \forall j \in \mathcal{T}$$

$$\frac{\partial C_{sum}}{\partial P_j} < 0 \, \forall j \notin \mathcal{T} \Rightarrow \sum_{k \in \mathcal{T}} P_{k,max} \geq \sigma_2^2$$

Proof: The optimum point can be shown to lie on the boundaries, implying P_j is either 0 or $P_{j,max}$ for all $j = 1, \ldots, K$. To see the second part, assume $\mathcal{T}$ is the set of all transmitting users. For all $j \in \mathcal{T}$, we then have $\frac{\partial C_{sum}}{\partial P_j} > 0$, and for all $j \notin \mathcal{T}$, $\frac{\partial C_{sum}}{\partial P_j} < 0$. □

This, in general, does not lead to any closed form solutions. The following special cases are notable:

- If $\sigma_2^2 \leq P_{1,max} \leq P_{2,max} \leq \ldots \leq P_{K,max}$, then only user K transmits.
- If $\sum_{j=1}^{K} P_{j,max} \leq \sigma_2^2$, then all users transmit with maximum power.
- If $P_{1,max} \leq P_{2,max} \leq \ldots \leq \sigma_2^2 \leq P_{j,max} \leq \ldots \leq P_{K,max}$, then either
  - a subset of users from the set $\{1, \ldots, j-1\}$ will transmit with full power, or
  - user K transmits with maximum power.

B. Collective Secrecy

The main result for this section is the following:

Theorem 5. We can transmit with perfect secrecy using Gaussian codebooks at the rates given by

$$R_{\mathcal{S}} \leq C_{\mathsf{M},\mathcal{S}} - C'_{\mathsf{MW},\mathcal{S}}$$

The region containing all such $\mathbf{R}$ is denoted $\widehat{\mathcal{R}}_{ach}^{(C)}$.

Proof: See Appendix II for an outline. □

There are two observations we can make:

1) This is the same region as given in Corollary 2.2, characterizing the rate region for Gaussian codebooks. We will hence call this region $\widehat{\mathcal{C}}^{(C)}$.
2) We can achieve a sum rate of $C_{\mathsf{M},\mathcal{K}} - C'_{\mathsf{MW},\mathcal{K}} = C_{\mathsf{M},\mathcal{S}} - C_{\mathsf{MW},\mathcal{K}}$ which is the outer bound given in Corollary 2.1, proving that Gaussian codebooks achieve the sum capacity for the GMAC-WT.

Remark: The sum capacity maximizing power allocation is easily seen to be $P_j^* = P_{j,max}$ for all users.

VI. Time-Division

We will show that we can achieve the sum capacity bound in the outer bound using TDMA among users, so that each of them sees a single user wire-tap channel.

In this case, an achievable secure rate region, $\widehat{\mathcal{R}}_{TDMA}$, using Gaussian codebooks is given by

$$R_j \leq \alpha_j C\left(\frac{P_j}{\alpha_j \sigma_1^2}\right) - \alpha_j C\left(\frac{P_j}{\alpha_j(\sigma_1^2+\sigma_2^2)}\right) \quad (18)$$

where user j is transmitting for α_j of the time with $\frac{P_j}{\alpha_j}$ power, such that its average transmitted power over a single interval is still P_j. The achievable secure sum rate becomes

$$C_{sum,TS} = \sum_{j=1}^{K} \alpha_j C\left(\frac{P_j}{\alpha_j \sigma_1^2}\right) - \alpha_j C\left(\frac{P_j}{\alpha_j(\sigma_1^2+\sigma_2^2)}\right) \quad (19)$$

Maximizing this quantity over $\{\alpha_j\}$, we get:

$$C_{sum,TS}^* = C\left(\frac{\sum_{j=1}^K P_{j,max}}{\sigma_1^2}\right) - C\left(\frac{\sum_{j=1}^K P_{j,max}}{\sigma_1^2+\sigma_2^2}\right) \quad (20)$$

with

$$\alpha_j^* = \frac{P_{j,max}}{\sum_{j=1}^K P_{j,max}} \quad (21)$$

VII. Numerical Results & Discussions

In this section, we present numerical results for the two-user GMAC-WT. The maximum received powers of the users are $P_{1,max} = 10$, $P_{2,max} = 5$ and the noise variance of the main channel is $\sigma_1^2 = 1$. We compare our achievable rates to the outer bound and the secure sum rate obtained via optimum time sharing for three different wire-tapper noise variances, $\sigma_2^2 = 20, 7$ and 2 in Fig. 2–4, respectively. We observe that we get the least loss in capacity when the wire-tapper is sees a higher noise power than received users' powers. As we get into the higher SNR regimes, to maintain the same level of perfect secrecy, we have to give up more and more actual rate of communication. In addition, using TDMA to provide single-user Gaussian wire-tap channels for all users, it is possible to achieve sum capacity. The time-sharing curves also show that TDMA provides higher secure sum rates when the noise variance of the wire-tap channel is high.

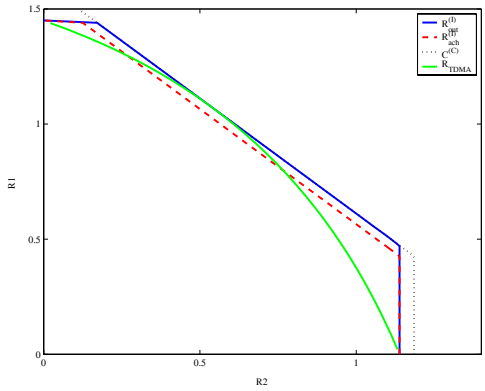

Fig. 2. Two User GMAC-WT: $P_{1,max} = 10$, $P_{2,max} = 5$, $\sigma_1^2 = 1$ and $\sigma_2^2 = 20 \Rightarrow C_{sum} = 1.6112$. Sum rate for individual constraints is maximized by $\mathbf{P}^* = (P_{1,max}, P_{2,max}) \Rightarrow C_{sum}^* = 1.4488$

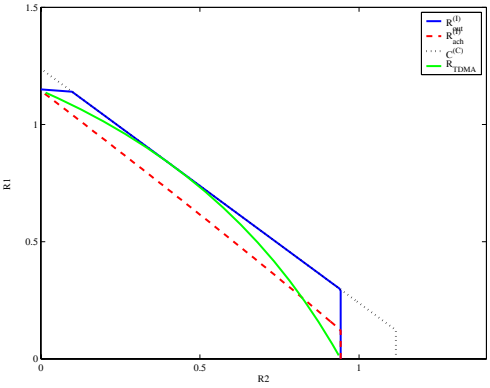

Fig. 3. Two User GMAC-WT: $P_{1,max} = 10$, $P_{2,max} = 5$, $\sigma_1^2 = 1$ and $\sigma_2^2 = 7 \Rightarrow C_{sum} = 1.2182$. Sum rate for individual constraints is maximized by $\mathbf{P}^* = (P_{1,max}, 0) \Rightarrow C_{sum}^* = 1.1448$

Another observation we can make is that even if the user's powers are unlimited, from (11), we can see that the maximum achievable sum rate is limited by the noise powers since

$$C_{sum}^{\infty} \triangleq \lim_{P_{\mathcal{K}} \to \infty} C\left(\frac{P_{\mathcal{K}}}{\sigma_1^2}\right) - C\left(\frac{P_{\mathcal{K}}}{\sigma_1^2+\sigma_2^2}\right) = C\left(\frac{\sigma_2^2}{\sigma_1^2}\right) \quad (22)$$

One interesting thing to note is that for low-noise regimes, when one user is not transmitting any information, we can achieve a rate region greater than the upper bound for the single user constraints as can be seen from Figure 4. This is because such a user can still transmit spurious information in the form of generating $R^{(s)}$ keywords and uniformly choosing one to send. Thus, even though that user might not be able to transmit any useful information with perfect secrecy, it may help the other user(s) increase their rate.

As seen in Figure 4, for the case when the maximum

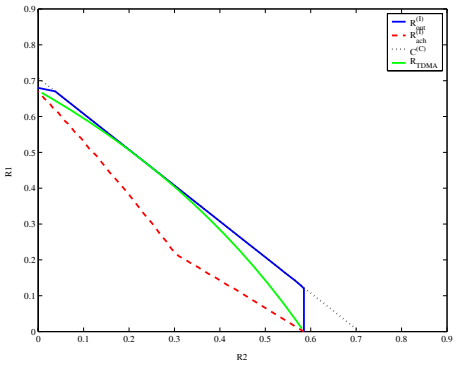

Fig. 4. Two User GMAC-WT: $P_{1,max} = 10$, $P_{2,max} = 5$, $\sigma_1^2 = 1$ and $\sigma_2^2 = 2 \Rightarrow C_{sum} = 0.7075$. Sum rate for individual constraints is maximized by $\mathbf{P}^* = (P_{1,max}, 0) \Rightarrow C^*_{sum} = 0.6720$

powers are larger than σ_2^2, the achievable region is completely contained within the TDMA achievable region. Only when at least one of the users can transmit with power greater than σ_2^2, is the rate region enlarged. This can also be seen from the comments on Theorem 4. Since TDMA also provides a way to satisfy both sets of constraints, the achievable region for individual constraints is in fact given by $\widehat{\mathcal{R}}_{TDMA} \cup \widehat{\mathcal{R}}^{(I)}_{ach}$.

To summarize, we have defined a set of constraints to ensure the non-decodability by the wire-tapper of any user in a multi-user environment while maintaining reliable communications with the intended receiver. Limits on the users' rates to maintain perfect secrecy are found, providing upper bounds on the GMAC-WT secrecy capacity region. We have also found rate regions using Gaussian codebooks achieving perfect secrecy, and the sum-capacity maximizing power allocations for these achievable regions, giving us lower bounds on the capacity region. For the collective secrecy constraints with Gaussian codebooks, the upper and lower bounds coincide, giving the capacity region. It is also shown that Gaussian codebooks achieve the sum capacity for the collective secrecy region. TDMA with optimal time-sharing allows us to achieve the secret sum-capacity with perfect secrecy.

Appendix I
Outer Bounds

We prove stronger results for outer bounds than presented earlier. We find outer bounds such that $\Delta_{\mathcal{S}} \geq \Delta \; \forall \mathcal{S} \subseteq \mathcal{K}$ for any $\Delta \in [0, 1]$. $\Delta = 1$ is then the special case for perfect secrecy.

Proof: [Proof of Theorem 1] The proof is a simple extension of the proof of Lemma 7 in [4]. Specifically, we start with

$$H(\mathbf{W}_{\mathcal{S}}|\mathbf{X}_{\mathcal{S}^c}, \mathbf{Z}, \mathbf{Y}) \leq H(\mathbf{W}_{\mathcal{S}}|\mathbf{X}_{\mathcal{S}^c}, \mathbf{Y}) \leq n\epsilon_n \tag{23}$$

We can then write $nR_{\mathcal{S}}\Delta_{\mathcal{S}} = H(\mathbf{W}_{\mathcal{S}}|\mathbf{X}_{\mathcal{S}^c}, \mathbf{Z})$ which, used with (23), after some algebra, gives

$$nR_{\mathcal{S}}\Delta_{\mathcal{S}} = nC\left(\frac{\sigma_2^2}{\sigma_1^2}\right) - [H(\mathbf{Z}|\mathbf{X}_{\mathcal{S}^c}) - H(\mathbf{Y}|\mathbf{X}_{\mathcal{S}^c})] \tag{24}$$

Using Lemmas 8, 9, 10 in [4], we can write

$$H(\mathbf{Z}|\mathbf{X}_{\mathcal{S}^c}) - H(\mathbf{Y}|\mathbf{X}_{\mathcal{S}^c}) \geq nC\left(\frac{\sigma_2^2}{P_{\mathcal{S}} + \sigma_1^2}\right) \tag{25}$$

Using the above in (24), we arrive at

$$nR_{\mathcal{S}}\Delta_{\mathcal{S}} \leq nC_{\mathsf{M},\mathcal{S}} - nC_{\mathsf{MW},\mathcal{S}} \tag{26}$$

□

Proof: [Proof of Theorem 2] Proceeding similarly to Lemma 6 in [4], we first find that

$$R_{\mathcal{S}} - \epsilon \leq \frac{1}{n} I(\mathbf{X}_{\mathcal{S}}; \mathbf{Y}|\mathbf{Z}) + \delta_n \quad \forall \mathcal{S} \subseteq \mathcal{K} \tag{27}$$

where $\delta_n \to 0$ as $\epsilon \to 0$. We then proceed as in Lemma 7 from [4] to write

$$I(\mathbf{X}_{\mathcal{S}}; \mathbf{Y}|\mathbf{Z}) \leq I(\mathbf{X}_{\mathcal{S}}; \mathbf{Y}|\mathbf{X}_{\mathcal{S}^c}) - I(\mathbf{X}_{\mathcal{S}}; \mathbf{Z}) \tag{28}$$

leading to

$$I(\mathbf{X}_{\mathcal{S}}, \mathbf{Y}|\mathbf{Z}) \leq nC_{\mathsf{M},\mathcal{S}} - nC\left(\frac{\sum_{j\in\mathcal{S}} 2^{\frac{2}{n}H(\mathbf{X}_j)}}{2\pi e\left(P_{\mathcal{S}^c} + \sigma_1^2 + \sigma_2^2\right)}\right) \tag{29}$$

which, together with (27) completes the proof. □

Proof: [Proof of Corollary 2.1] Follows from (28) with $\mathcal{S} = \mathcal{K}$ and using Lemmas 8, 9, 10 from [4]. □

Proof: [Proof of Corollary 2.2] Follows by letting $H(\mathbf{X}_j) = \frac{n}{2}\log(2\pi e P_j)$ in (12). □

Appendix II
Inner Bounds

Proof: [Proof of Theorem 3] Follows by a stochastic encoding scheme similar to [2]. Each user generates $2^{n(R_j + R_j^{(s)})}$ codewords arranged into $2^{n(R_j)}$ codebooks. To send message W_j, user j uniformly chooses one of $2^{nR_j^{(s)}}$ codewords to send. We need to choose $R_j^{(s)} = C_{\mathsf{MW},j}$ to ensure perfect secrecy. This makes $\Delta_j^{(I)} = 1$ for all users j, which in turn yields $\Delta_{\mathcal{S}}^{(I)} = 1$ for all sets of users. □

Proof: [Proof of Theorem 5] We use a similar coding scheme as above, but we need to choose $R_j^{(s)}$ as

$$R_{\mathcal{S}}^{(s)} \leq C_{\mathsf{MW},\mathcal{S}} \quad \forall \mathcal{S} \subset \mathcal{K}, \qquad R_{\mathcal{K}}^{(s)} = C_{\mathsf{MW},\mathcal{K}} \tag{30}$$

and also $R_{\mathcal{S}} + R_{\mathcal{S}}^{(s)} \leq C_{\mathsf{M},\mathcal{S}}$ to ensure perfect secrecy. This makes $\Delta_{\mathcal{K}}^{(C)} = 1$, which in turn yields $\Delta_{\mathcal{S}}^{(C)} = 1 \, \forall \mathcal{S}$. □

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Sys. Tech. J.*, vol. 28, pp. 656–715, 1949.

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

[3] 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.

[4] S. K. Leung-Yan-Cheong and M. E. Hellman, "Gaussian wire-tap channel," *IEEE Trans. Inform. Theory*, vol. 24, no. 4, pp. 451–456, July 1978.

[5] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[6] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York: John Wiley & Sons, 1991.