

Approximate secrecy capacity region of an asymmetric MAC wiretap channel within $\frac{1}{2}$ bits

Sanjay Karmakar and Anirban Ghosh

Abstract—We consider a 2-user Gaussian Multiple-Access Wiretap channel (GMAC-WT), with the Eavesdropper (E) having access to signal from only one (say, T_2) of the two transmitters. We characterize the capacity region of this channel approximately within .5 bits, where the approximation is in terms of only T_1 's rate or the sum-rate depending on the relative strength of the eavesdropper's channel. However, the approximation is .5 bits independent of channel coefficients or operating Signal-to-Noise Ratios (SNR). To prove this approximate result we propose two different coding schemes, namely, the *power adaptation* and the *time sharing* coding schemes and derive their corresponding achievable rate regions. Both of them use Gaussian input distribution. To establish the approximate capacity, we first derive supersets to the capacity region and then show that corresponding to each rate pair at the boundary of these supersets there exists an achievable rate pair in one of the aforementioned achievable rate regions which are within $\frac{1}{2}$ bits to the former pair. In comparison to a very recent result (Xie and Ulukus, ISIT 2013) on a GMAC-WT showing the requirement of interference alignment (IA) to achieve even the degrees of freedom performance, the result of this paper is surprising: our channel model is an interesting variation of the GMAC-WT for which IA is not necessary and Gaussian signalling is sufficient to achieve the entire capacity region within .5 bits.

I. INTRODUCTION

The concept of secrecy in a communication system was first introduced by Shannon in [1] and was considered from an information theoretic perspective by Wyner in [2] and Csiszar and Korner in [3]. These pioneering works on discrete memoryless wiretap channels has been complemented by characterizing the capacity of SISO Gaussian Wiretap channel in [4], the capacity of a fading SISO wiretap channel in [5] and a MIMO wiretap channel in [6].

In recent years, interest has shifted towards analyzing the secrecy capacity of multi-user networks. Multiple-access Wiretap channel is one such network where two or more users (T_i , $i = 1, 2, \dots$) communicate to a legitimate receiver (D) in presence of a malicious Eavesdropping receiver (E). The GMAC-WT was introduced in [7] and assuming that the composite signal received by E is a degraded version of the composite signal received by D the authors have characterized the sum-rate capacity of this channel. In contrast to this in [8] the authors consider a GMAC-WT where in the composite signal received at E the two users are degraded in different manner. However, such an asymmetric model makes the problem even harder to analyze and only approximate capacity within .5 bits of *individual transmitters* was characterized for

the GMAC-WT. In [9], the authors found outer and inner bound to the deterministic MAC-WT and have shown that for a degraded channel they are same. Whereas in [10] only an achievable rate region for the channel was found.

The lack of capacity results for the *asymmetric* GMAC-WT motivates us to consider the channel shown in Fig. 1, where the eavesdropper (E) can observe only the second transmitter's signal, as a result the signal from T_1 is automatically hidden from E. Clearly, this is an *asymmetric* GMAC-WT; *asymmetric* in the sense that the gains of the channels terminating at D are not similar to those of the channels terminating at E. In particular, the channel gain of the T_1 -E link is always zero while that of the T_1 -D link is not. This makes it different from that of [7] as well since E receives the signals from the two users through two differently degraded channels and not similarly degraded channels. As a result, in our channel model there are scenarios in which the sum-rate capacity is achieved when one of the users are not transmitting at all (e.g., see Fig. 4). Such a scenario does not arise in the symmetrically degraded channel configuration of [7]. In the sequel, we shall refer to this channel as a *Gaussian Multiple-Access Wiretap Channel with One Secrecy Constrained User* (GMAC-WT-OSCU). Such a channel model can arise in a wireless network where two users are trying to communicate to a central access point while an eavesdropper can hear the signal from only one of them because of shadowing, distance or another layer of encryption. A class of MAC-WT-OSCU was also considered in [11], however, that class does not include the Gaussian noise model adopted in this paper. In [12], only the sum-rate capacity of the GMAC-WT-OSCU was characterized approximately within $\frac{1}{2}$ bits. Here we generalize the results of [12] and characterize the entire capacity region of the channel within an approximation of 0.5 bits, where the approximation is in terms of T_1 's rate or the sum-rate when the T_1 -E channel is *moderately noisy* and *very noisy*,¹ respectively. We devise two coding schemes with Gaussian input which can achieve the aforementioned approximation. To prove the proximity of these achievable regions' boundaries to that of the capacity region we prove novel weighted sum-rate outer bounds. In certain operating rate regimes the aforementioned two set of boundaries coincide with each other characterizing the *exact capacity region boundary*. We derive explicit characterization of such rate regimes. To the best of our knowledge, this is the first result of the characterization of the capacity region for a asymmetric GMAC-WT channel.

The rest of the paper is organized as follows. In section

The authors are with the Department of Electrical and Computer Engineering, North Dakota State University, Fargo, ND, 58103 USA e-mail: (sanjay.karmakar@ndsu.edu), (anirban.ghosh@ndsu.edu).

¹A more detailed definition of this terms can be found in Section II.

II, we shall describe the system model, some definitions of measure of performance and some preliminary mathematical notations. In subsection III-A and III-B, we derive achievable rate regions for two different coding schemes and two supersets containing the secrecy capacity region of the channel, respectively. Using these results in subsection III-C we characterize the approximate capacity region of the channel. Conclusion follows in section IV.

Notations 1: The probability distribution function (pdf) of a Gaussian random vector with mean zero and Covariance matrix Q shall be denoted by $\mathcal{N}(0, Q)$. Trace and determinant of a square matrix, S will be denoted by $\text{Tr}(S)$ and $|S|$, respectively. For any two arbitrary real numbers $a, b > a$, $[a, b]$, represents the interval of real numbers from a to b , and $(a)^+$ represents $\max\{a, 0\}$.

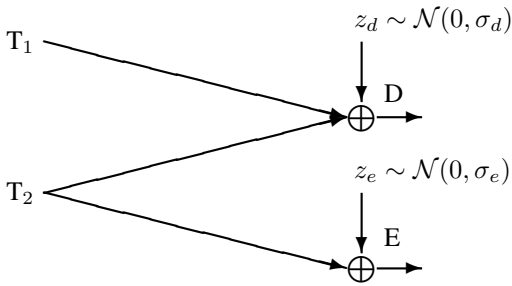


Fig. 1: The MAC-WC with one user requiring secrecy.

II. SYSTEM MODEL AND PRELIMINARIES

The canonical channel model for a 2-user GMAC-WT is given by (e.g., Equations (2a,b) in [7])

$$y_d = x_1 + x_2 + z_d; \quad (1)$$

$$\hat{y}_e = h_1 x_1 + h_2 x_2 + \hat{z}_e, \quad (2)$$

where h_1 and h_2 are the channel coefficients and $z_d, \hat{z}_e \sim \mathcal{N}(0, 1)$ are mutually independent additive Gaussian noises at D and E respectively. We shall refer to a GMAC-WT with $h_1 = h_2$ as a *Symmetric* GMAC-WT and when $h_1 \neq h_2$, we shall call it an *Asymmetric* GMAC-WT (AGMAC-WT). In this paper, we consider a special class of the AGMAC-WT, where $h_1 = 0$, i.e., T_1 's message is not audible at all at the eavesdropping node E and therefore T_1 in our channel model is secure by default. T_2 's message on the other hand is observed through the channel with channel coefficient h_2 by E and should be kept secret from it. A schematic diagram of this channel model is shown in Figure 1. For this special case, the aforementioned input-output equations take the following form

$$y_d = x_1 + x_2 + z_d; \quad (3)$$

$$y_e = x_2 + z_e, \quad (4)$$

where $z_e = \frac{1}{h_2} \hat{z}_e$. In the rest of the paper, we shall denote the variances of the Gaussian additive noise at D and E by σ_d and σ_e , respectively with the understanding that $\sigma_d = 1$ and $\sigma_e = \frac{1}{h_2^2}$. Using the result in [4] it can be easily proved

that when $\sigma_e \leq \sigma_d$, the secrecy capacity of the second user is 0, even in the absence of T_1 . Thus in the sequel, we shall assume that $\sigma_d < \sigma_e$. We also assume that an n -letter extension of this channel contains n such i.i.d. components, i.e., $z_d^n \sim \mathcal{N}(0, \sigma_d I_n)$ and $z_e^n \sim \mathcal{N}(0, \sigma_e I_n)$. The signals transmitted by T_1 and T_2 are assumed to satisfy the following average power constraints

$$\text{Tr}(Q_k) \leq nP_k, \quad k = 1, 2, \quad (5)$$

where Q_k is the covariance matrix of the n -length channel input sequence x_k^n at T_k .

We assume that both T_1 and T_2 have messages \mathcal{W}_1 and \mathcal{W}_{2s} respectively for the legitimate receiver D . In addition to D , the eavesdropping user (E) also knows the coding scheme used by the transmitters and is capable of processing its received signal. Let us assume that T_1 and T_2 want to transmit their messages at rates R_1 and R_{2s} , respectively. Suppose, given a message pair $\mathcal{W}_1(i), \mathcal{W}_{2s}(j)$, $i \in \{1, \dots, 2^{nR_1}\}$ and $j \in \{1, \dots, 2^{nR_{2s}}\}$, T_k chooses a codeword $x_k^n \in \mathcal{C}_k(n)$ and sends it through the channel, where $\mathcal{C}_k(n)$ is the codebook of the k -th transmitter containing n -length codewords which satisfy the power constraint in equation (5). Also assume that, the legitimate receiver (D) recovers $\mathcal{W}_1(\hat{i})$ and $\mathcal{W}_{2s}(\hat{j})$ from the received signal. Then the probability of detection error can be denoted as $P_e(n) = \Pr((i, j) \neq (\hat{i}, \hat{j}))$.

A rate pair (R_1, R_{2s}) is said to be *achievable* if there exists $\mathcal{C}_k(n)$, $k = 1, 2$ such that $P_e(n) \rightarrow 0$ and

$$I(\mathcal{W}_{2s}; y_e^n) < \epsilon \quad (6)$$

with arbitrarily small $\epsilon > 0$, as $n \rightarrow \infty$. Note that the aforementioned condition is equivalent of an *equivocation* of 1 according to the definitions of [3], because

$$\begin{aligned} I(\mathcal{W}_{2s}; y_e^n) < \epsilon &\Rightarrow h(\mathcal{W}_{2s}) < h(\mathcal{W}_{2s} | y_e^n) + \epsilon \\ 1 - \epsilon' &< \frac{h(\mathcal{W}_{2s} | y_e^n)}{h(\mathcal{W}_{2s})}, \end{aligned} \quad (7)$$

where the right hand side of the above equation represents the *equivocation* and $\epsilon' = \frac{\epsilon}{h(\mathcal{W}_{2s})}$ can be made arbitrarily small.

The capacity region denoted by $\mathcal{C}_{\text{GMAC-WT-OSCU}}$, of the GMAC-WT with one secrecy seeking transmitter is defined as the closure of the set of achievable rate pairs. Clearly, $\mathcal{C}_{\text{GMAC-WT-OSCU}}$ is a function of P_1, P_2, σ_d and σ_e , however for brevity of notations we shall not denote them explicitly. In the sequel, whenever we say a rate pair is achievable it should be understood that they are achievable while the secrecy constraint of (6) is met. The same is true for achievable rate regions and supersets to the capacity region.

While results on *asymmetric* GMAC-WT is much fewer than that available for *Symmetric* GMAC-WT, none of them considers the capacity region for the channel. The closest result to such characterization was reported in [8] where the authors have shown that the *individual capacity*² of the users on a

²For a 2-transmitter channel, individual capacity of T_k , refer to the maximum rate achievable by T_k while operating within the capacity region of the channel, i.e., $\max_{(R_1, R_2) \in \mathcal{C}} R_k$, where \mathcal{C} represents the capacity region of the channel. In general, it is not equal to (and can be larger than) the capacity of T_k when the other user is silent.

degraded AGMAC-WT can be achieved within .5 bits. In this paper however, we shall characterize the entire capacity region of the GMAC-WT-OSCU, with an approximation margin of at most .5 bits either in the rate of T_1 or in sum-rate. To make this notion more concrete we define the following:

Definition 1 (Capacity within a bits in T_1 's rate):³ An achievable region, \mathcal{R} is said to be within a bits in T_1 's rate to the capacity region, if for any given rate pair $(R_1, R_{2s}) \in \mathcal{C}_{\text{GMAC-WT-OSCU}}$, the rate pair $((R_1 - a)^+, R_{2s}) \in \mathcal{R}$.

Definition 2 (Capacity within a bits in sum rate): An achievable region, \mathcal{R} is said to be within a bits in sum rate to the capacity region, if for any given rate pair $(R_1, R_{2s}) \in \mathcal{C}_{\text{GMAC-WT-OSCU}}$, the rate pair $((R_1 - a_1)^+, (R_{2s} - a_2)^+) \in \mathcal{R}$, for arbitrary $a_1, a_2 \geq 0$ such that $(a_1 + a_2) = a$.

In this paper, depending on the relative value of additive Gaussian noise variance at E with respect to that of the sum of signal power at T_1 and variance of noise power at D we divide the GMAC-WT-OSCU into two classes: 1) GMAC-WT-OSCU with *very noisy* eavesdropper if $(P_1 + \sigma_d) < \sigma_e$; and 2) GMAC-WT-OSCU with *moderately noisy* eavesdropper if $(P_1 + \sigma_d) \geq \sigma_e$. In the sequel, capacity region of channels with *moderately noisy* E will be characterized within 0.5 bits in T_1 's rate and the capacity region of channels with *very noisy* E will be characterized within 0.5 bits in sum-rate. However, this 0.5 bit approximation is independent of the channel parameters⁴ and operating SNR.

A. Some preliminaries

A Gaussian Wiretap Channel (WC) with the transmitter T having an average power constraint of P , one legitimate receiver (D) with additive noise variance σ_1 and an eavesdropper (E) with additive Gaussian noise variance σ_2 will be referred to as a *simple* $T(P) \rightarrow D(\sigma_1) \rightarrow E(\sigma_2)$ WC. The capacity of such a channel with perfect secrecy (i.e., secrecy constraint (6)) was found in [4] to be

$$C_{\text{WT}}(P, \sigma_1, \sigma_2) = \frac{1}{2} \left[\log \left(1 + \frac{P}{\sigma_1} \right) - \log \left(1 + \frac{P}{\sigma_2} \right) \right]. \quad (8)$$

We shall denote the capacity of a point-to-point channel with signal-to-noise ratio of α by $C(\alpha)$, i.e., $C(\alpha) = \frac{1}{2} \log(1 + \alpha)$ and use the short hand notation $f(\alpha)$ for $0.5 \log(\alpha)$. We also note that, if we denote $C_s(\beta)$ as

$$C_s(\beta) = \frac{1}{2} \left[\log \left(1 + \frac{\beta P_2}{\sigma_d} \right) - \log \left(1 + \frac{\beta P_2}{\sigma_e} \right) \right], \quad (9)$$

$$\begin{aligned} &= \frac{1}{2} \left[\log(\sigma_d + \beta P_2) - \log(\sigma_e + \beta P_2) + \log(\sigma_e \sigma_d^{-1}) \right], \\ &= -.5 \log \left(1 + \frac{(\sigma_e - \sigma_d)}{\sigma_d + \beta P_2} \right) + .5 \log(\sigma_e \sigma_d^{-1}), \end{aligned} \quad (10)$$

then $C_s(\beta)$ is a continuous and monotonically increasing function of $\beta \in [0, 1]$. We also use the notations

$$C_{\text{MAC-WT}} = C((P_1 + P_2)\sigma_d^{-1}) - C(P_2\sigma_e^{-1}). \quad (11)$$

³Note that this definition of approximation is different from some earlier definitions used in the context of Interference channels [13].

⁴Recall from the channel normalization in (4) that, σ_e incorporates the channel strength of the T_2 -D link.

III. MAIN RESULTS

A. Achievable rate regions

For the two types of channels defined in section II namely the GMAC-WT-OSCU with *moderately noisy* (i.e., $(P_1 + \sigma_d) \geq \sigma_e$) and *very noisy* (i.e., $(P_1 + \sigma_d) < \sigma_e$) E, in this section we shall define two different coding schemes and derive explicit expressions for their corresponding achievable rate regions. Our first coding scheme namely the *power adaptation* coding scheme, however can operate on both types of channels and can achieve the following rate region.

Lemma 1 (Power adaptation achievable region): For a given $\beta \in [0, 1]$, $\mathcal{R}_{\text{PA}}(\beta)$ represents an achievable secrecy rate region for the 2-user GMAC-WT-OSCU of Fig.1, where

$$\mathcal{R}_{\text{PA}}(\beta) = \left\{ (R_1, R_{2s}) : \begin{aligned} R_1 &\leq C(P_1(\sigma_d + \beta P_2)^{-1}); \\ R_{2s} &\leq C_s(\beta); \end{aligned} \right\}.$$

Therefore, $\mathcal{R}_{\text{PA}} = \cup_{\{\beta \in [0, 1]\}} \mathcal{R}_{\text{PA}}(\beta)$ is also an achievable region.

Example 1: As an example, the achievable region of the *power adaptation coding scheme* of Lemma 1 is depicted in Fig.2 for a GMAC-WT-OSCU with $P_1 = 82$, $P_2 = 20$, $\sigma_d = .1$ and $\sigma_e = 8$. Note that this channel parameters falls into the regime where E is *moderately noisy*.

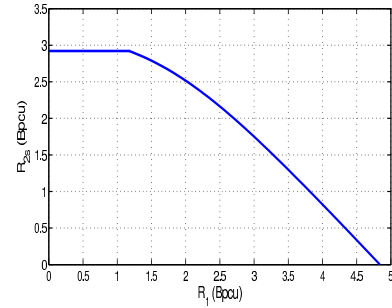


Fig. 2: The Power adaptation achievable rate region, with $P_1 = 82$, $P_2 = 20$, $\sigma_d = .1$ and $\sigma_e = 8$.

Proof of Lemma 1: Skipped for space constraint and can be found in [14]. ■

It will be shown in [14] that, to achieve a rate pair in $\mathcal{R}_{\text{PA}}(\beta)$, T_2 restricts its transmit power to βP_2 and therefore, we call it the *power adaptation* coding scheme. In contrast to this, next we shall derive an achievable rate region where both the users transmit using their entire available power. The rate region specified in Lemma 2 is achievable only on a 2-user GMAC-WT-OSCU with *very noisy* eavesdropper.

Lemma 2: Let \mathcal{R}_{TS} represents the following rate region.

$$\begin{aligned} \mathcal{R}_{\text{TS}} = \{ (R_1, R_{2s}) : & R_1 \leq C(P_1\sigma_d^{-1}) \triangleq C_1; \\ & R_{2s} \leq C(P_2\sigma_d^{-1}) - C(P_2\sigma_e^{-1}); \\ & R_1 + R_{2s} \leq C((P_1 + P_2)\sigma_d^{-1}) - C(P_2\sigma_e^{-1}) \}, \end{aligned}$$

then, \mathcal{R}_{TS} is an achievable rate region on the 2-user GMAC-WT-OSCU of Figure.1, with $(P_1 + \sigma_d) < \sigma_e$.

We call it the *time sharing* coding scheme because to achieve the maximum sum-rate achieving rate pairs in \mathcal{R}_{TS} ,

users T_1 and T_2 uses time sharing strategy between two interesting operating points, namely point B and C in Fig. 3.

Remark 1: Figure 3 depicts the general shape of \mathcal{R}_{TS} .

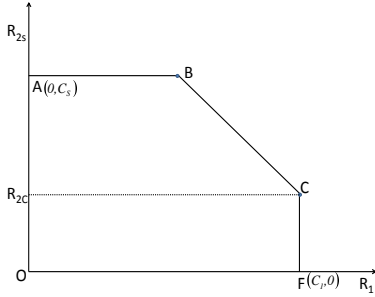


Fig. 3: The time-sharing achievable rate region.

In this figure, $R_{2C} = C_{WT}(P_2, (P_1 + \sigma_d), \sigma_e)$ (recall equation (8)) represents (as we shall see in more details in the proof) a secret rate that T_2 can achieve treating T_1 's message as noise. If $(P_1 + \sigma_d) \geq \sigma_e$ then the aforementioned decoding scheme will result in an $R_{2C} \leq 0$. This happens because in this case, the joint contribution of T_1 's signal and the additive noise at D makes the T_2 -D link a degraded version of the T_2 -E link and therefore, no secret information can be conveyed to D. This is why in Lemma 2 we need the condition $(P_1 + \sigma_d) < \sigma_e$.

In order to evaluate the closeness to optimality of these coding schemes we need good outer bounds to compare them with, which we find in the next subsection.

B. Supersets to the capacity region

In this subsection, first we derive two different rate regions which contains the capacity region of the GMAC-WT-OSCU depending on the channel parameters. To derive these regions we use outer bound on the individual rate (R_1) of T_1 , individual rate (R_{2s}) of T_2 and the weighted sum of their individual rates ($wR_1 + R_{2s}$), for various values of the weighting parameter $w \in [0, 1]$ as shown in Theorem 1 below.

Theorem 1: If (R_1, R_{2s}) is an achievable rate pair on the GMAC-WT-OSCU of Fig. 1 then,

$$R_1 \leq C(P_1 \sigma_d^{-1}), \quad (12)$$

$$R_{2s} \leq C(P_1 \sigma_d^{-1}) - C(P_2 \sigma_e^{-1}) = C_s(1), \quad (13)$$

$$(wR_1 + R_{2s}) \leq \frac{w}{2} \log \left(1 + \frac{P_1}{\sigma_d + \lambda^*} \right) + 0.5w + \frac{1}{2} \log \left(1 + \frac{\lambda^*}{\sigma_d} \right) - \log \left(1 + \frac{\lambda^*}{\sigma_e} \right), \quad (14)$$

where for $(P_1 + \sigma_d) < \sigma_e$,

$$\lambda^* = P_2, \quad \forall w \in [0, 1] \quad (15)$$

and when $(P_1 + \sigma_d) \geq \sigma_e$,

$$\lambda^* = \begin{cases} 0, & \text{if } w_1 \leq w \leq 1; \\ \min\{P^*, P_2\}, & \text{if } w_2 \leq w \leq w_1; \\ P_2, & \text{if } 0 \leq w \leq w_2; \end{cases} \quad (16)$$

with $P^* = \frac{\sigma_e(w_1 - w)}{(w - w_2)}$, where

$$w_1 = \frac{(P_1 + \sigma_d)(\sigma_e - \sigma_d)}{P_1 \sigma_e} \text{ and } w_2 = \frac{(\sigma_e - \sigma_d)}{P_1}. \quad (17)$$

Lemma 3: For any $\beta \in [0, 1]$, let $\mathcal{C}_1^u(\beta)$ be a rate region defined as

$$\mathcal{C}_1^u(\beta) = \left\{ (R_1, R_{2s}) : R_{2s} \leq C(\beta P_2 \sigma_d^{-1}) - C(\beta P_2 \sigma_e^{-1}), \right. \\ \left. R_1 \leq \min \left\{ C(P_1 \sigma_d^{-1}), C(P_1(\sigma_d + \beta P_2)^{-1}) + \frac{1}{2} \right\} \right\},$$

then, $\cup_{\beta \in [0, 1]} \mathcal{C}_1^u(\beta) \supseteq \mathcal{C}_{\text{GMAC-WT-OSCU}}$.

Proof of Lemma 3: Follows from Theorem 1, skipped for space constraint and can be found in [14]. ■

Example 2: To illustrate the benefit of such simpler description of previous section's outer bounds in the form of rate regions containing the capacity regions we depict in Fig. 4 the rate region \mathcal{C}_1^u of Lemma 3 for the channel parameters that was considered in Example 1.

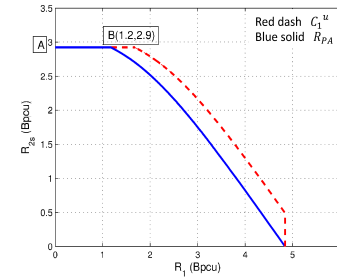


Fig. 4: Rate region containing the capacity region of a GMAC-WT-OSCU, with $P_1 = 82$, $P_2 = 20$, $\sigma_d = .1$ and $\sigma_e = 8$.

The following Corollary to Lemma 3 characterizes the interplay between the components of an achievable rate pair as it moves through the capacity region. It describes how T_2 's rate of communication restricts the rate at which T_1 can communicate.

Corollary 1 (Corollary to Lemma 3): Given an achievable rate pair (R_1, R_{2s}) , if for any $\beta \in [0, 1]$, $R_{2s} = C_s(\beta)$ (e.g., equation (10)) then the corresponding rate for T_1 must satisfy the following outer bound

$$R_1 \leq \frac{1}{2} \log \left(1 + \frac{P_1}{\beta P_2 + \sigma_d} \right) + 0.5.$$

Next, we consider the complimentary case of an GMAC-WT-OSCU channel with $(P_1 + \sigma_d) < \sigma_e$, i.e., a very noisy eavesdropper.

Lemma 4: Let \mathcal{C}_2^u represents a set of non-negative rate tuples defined as,

$$\mathcal{C}_2^u = \left\{ (R_1, R_{2s}) : R_1 \leq C(P_1 \sigma_d^{-1}); \right. \\ \left. R_{2s} \leq C(P_2 \sigma_d^{-1}) - C(P_2 \sigma_e^{-1}); \right. \quad (18)$$

$$\left. R_1 + R_{2s} \leq C((P_1 + P_2) \sigma_d^{-1}) - C(P_2 \sigma_e^{-1}) + \frac{1}{2} \right\}. \quad (19)$$

then, $\mathcal{C}_2^u \supseteq \mathcal{C}_{\text{GMAC-WT-OSCU}}$ if $(P_1 + \sigma_d) < \sigma_e$.

Proof of Lemma 4: Follows from Theorem 1 by putting $w = 1$. ■

Example 3: As an example of a GMAC-WT-OSCU with very noisy eavesdropper, we consider the channel with $P_1 = 10$, $P_2 = 10$, $\sigma_d = .1$ and $\sigma_e = 100$ and depict in Fig. 5 the capacity region outer bound that was derived in Lemma 4. To

compare its closeness to achievable rate region of Lemma 1 we also plot the achievable region \mathcal{R}_{TS} .

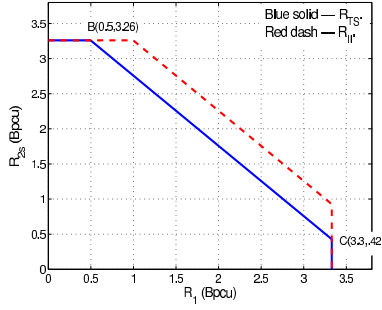


Fig. 5: \mathcal{R}_{TS} and \mathcal{C}_2^u for a GMAC-WT-OSCU, with $P_1 = 10$, $P_2 = 10$, $\sigma_d = .1$ and $\sigma_e = 100$.

It is easy to observe that in both figures 4 and 5, the boundaries of the rate regions containing capacity regions of the channels are very close to the boundary of the corresponding achievable rate regions, irrespective of whether the eavesdropper is *very noisy* or *moderately noisy*. This observation raise the following interesting questions: How the gap between the boundaries of the achievable regions and outer bounds vary with channel parameters, or, what fraction of the entire capacity region of the GMAC-WT-OSCU can be achieved by the *power adaptation* and the *time-sharing* coding schemes. In the next subsection we find answers to these questions.

C. Approximate capacity regions

Theorem 2 (moderately noisy eavesdropper): The achievable rate region \mathcal{R}_{PA} is within 0.5 bits to the capacity region of the channel in T_1 's rate, when the eavesdropper is *moderately noisy*, i.e., $(P_1 + \sigma_d) \geq \sigma_e$.

Proof of Theorem 2: Let $(R'_1, R'_{2s}) \in \mathcal{C}_{\text{GMAC-WT-OSCU}}$, then by Lemma 3 we know that $(R_1, R_{2s}) \in \mathcal{C}_2^u(\beta)$ for some $\beta \in [0, 1]$, i.e.,

$$0 \leq R'_{2s} \leq C_s(\beta), \text{ for some } 0 \leq \beta \leq 1.$$

Since $C_s(\beta)$ is an increasing function of β , from the intermediate value theorem, there is a $0 \leq \beta_0 \leq \beta$, for which

$$R'_{2s} = C_s(\beta_0),$$

then, from Corollary 1 we have

$$R'_1 \leq C(P_1(\beta_0 P_2 + \sigma_d)^{-1}) + \frac{1}{2}.$$

However, we know from Lemma 1 that for any $\beta_0 \in [0, 1]$,

$$(C(P_1(\beta_0 P_2 + \sigma_d)^{-1}), C_s(\beta_0)) \in \mathcal{R}_{PA},$$

which in turn imply that $((R'_1 - \frac{1}{2})^+, R'_{2s}) \in \mathcal{R}_{PA}$ and is achievable by the *power adaptation scheme*. ■

A similar approximation can be proved for GMAC-WC-OSCU with *very noisy* E which we prove next.

Theorem 3 (very noisy eavesdropper): The achievable rate region \mathcal{R}_{TS} of Lemma 2 is within 0.5 bits to the capacity region of the channel in sum rate, when the eavesdropper is *very noisy*, i.e., $(P_1 + \sigma_d) < \sigma_e$.

Proof of Theorem 3: The proof is by contradiction; it can be shown that for any $(R'_1, R'_{2s}) \in \mathcal{C}_{\text{GMAC-WT-OSCU}}$ and $a_1, a_2 \geq 0$ such that $(a_1 + a_2) = .5$ if we assume $((R'_1 - a_1)^+, (R'_{2s} - a_2)^+) \notin \mathcal{C}_{\text{GMAC-WT-OSCU}}$ then that leads to $(R'_1 + R'_{2s}) > C_{\text{MAC-WT}} + .5$, which is contradicts our initial assumption. ■

To summarize, in comparison to earlier results such as [8], the result of this paper is stronger in the following aspects: 1) We provide approximate characterization of the entire *capacity region*; 2) both the achievable schemes of this paper allow each user to achieve their individual capacities; and finally, 3) we provide partial characterization of the exact capacity region boundary as well.

IV. CONCLUSION

We characterize the capacity region of the 2-user GMAC-WT-OSCU approximately within 0.5 bits. We have derived achievable rate regions corresponding to two different coding schemes, namely, *power adaptation* and *time sharing* coding schemes, which are approximate capacity optimal in the *moderately noisy* and *very noisy* regimes, respectively. Interestingly, for the channel configuration considered here Gaussian input at both the transmitters are sufficient to achieve capacity region within 0.5 bits and interference alignment is not required.

REFERENCES

- [1] C. E. Shannon, "Communication theory of secrecy systems," *Bell syst. Tech. J.*, vol. 28, pp. 656–715, 1949.
- [2] A. Wyner, "The wiretap channel," *Bell syst. Tech. J.*, vol. 54, pp. 1355–1387, 1975.
- [3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. on Inform. Th.*, vol. 24, pp. 339–348, May, 1978.
- [4] S. K. Leung-Yan-Cheong and M. E. Hellman, "The gaussian wire-tap channel," *IEEE Trans. on Inform. Th.*, vol. 24, pp. 451–456, Jul, 1978.
- [5] P. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, pp. 5059–5067, Nov, 2008.
- [6] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Transactions on Information Theory*, vol. 57, pp. 4961–4971, Aug, 2011.
- [7] E. Tekin and A. Yener, "The gaussian multiple-access wire-tap channel," *IEEE Transactions on Information Theory*, vol. 54, pp. 5747–5755, Dec, 2008.
- [8] E. Ekrem and S. Ulukus, "On the secrecy of multiple access wiretap channel," in *46th Annual Allerton Conference on Communication, Control, and Computing*, Sep, 2008, pp. 1014–1021.
- [9] V. Jahandideh, S. Salimi, and M. Salmasizadeh, "Deterministic multiple access wiretap channel," in *IEEE International Conference on Information Theory and Information Security (ICITIS)*, 2010, Dec 2010, pp. 998–1001.
- [10] M. Wiese and H. Boche, "An achievable region for the wiretap multiple-access channel with common message," in *Proc. IEEE Int. Symp. on Inform. Th., St. Petersburg, Russia*, Jul, 2012.
- [11] N. Liu and W. Kang, "The secrecy capacity region of a special class of multiple access channels," in *Proc. IEEE Int. Symp. on Inform. Th., St. Petersburg, Russia*, Jul, 2011, pp. 623–627.
- [12] S. Karmakar, "On the sum-rate capacity of a 2-user Multiple Access Wiretap Channel with one secret user," in *Proc. of 4th Int. Conf. on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE)*, Aalborg, Denmark, May, 2014.
- [13] S. Karmakar and M. K. Varanasi, "The capacity region of the MIMO interference channel and its reciprocity to within a constant gap," *IEEE Trans. on Inform. Th.*, vol. 59, pp. 4781–4797, Aug, 2013.
- [14] S. Karmakar, "Approximate secrecy capacity region of an asymmetric mac wiretap channel within 1/2 bits," Apr, 2015, to be Submitted to IEEE Transactions on Information Theory.