The Gaussian Multiple Access Wire-Tap Channel with Collective Secrecy Constraints

Ender Tekin
tekin@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). In this scenario, multiple users communicate with an intended receiver in the presence of an intelligent and informed wire-tapper who receives a degraded version of the signal at the receiver. We define a suitable security measure for this multi-access environment. We derive an outer bound for the rate region such that secrecy to some pre-determined degree can be maintained. We also find, using Gaussian codebooks, an achievable such secrecy region. Gaussian codewords are shown to achieve the sum capacity outer bound, and the achievable region concides with the outer bound for Gaussian codewords, giving the capacity region when inputs are constrained to be Gaussian. 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

Shannon, in [1], analyzed secrecy systems in communications and he showed that to achieve perfect secrecy of communications, we must have 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 who has access to a degraded version of the intended receiver's signal. He measured the amount of "secrecy" using the conditional entropy Δ, the conditional entropy of the transmitted message given 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].

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 use the channel at close to 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 and also 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. More recently, Maurer showed in [6] that a public feedback channel can make secret communications possible even when the secrecy capacity is zero.

In [7] we extended these concepts to the GMAC and defined two separate secrecy constraints, which we called *individual* and *collective* secrecy constraints. We concerned ourselves mainly with the *perfect secrecy rate region* for both sets of constraints. For the individual constraints, this corresponds to the entropy of the transmitted messages given the received wire-tapper signal and the other users' transmitted signals being equal to the entropy of the transmitted message. The collective secrecy constraints provided a more relaxed approach and utilized other users' signals as an additional source of secrecy protection. In this paper, we consider the GMAC-WT and focus on the "collective secrecy constraints" for the GMAC-WT, defined in [7] as the normalized entropy of any set of messages conditioned on the wire-tapper's received signal. We consider the general case where a pre-determined level of secrecy is provided. Under these constraints, we find an outer bound for the 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 ignorant to a pre-determined level. We show that when we constrain ourselves to using Gaussian codebooks, these bounds coincide and give the capacity region for Gaussian codebooks. Furthermore, it is shown that Gaussian codebooks achieve sum capacity for the GMAC-WT using simultaneous superposition coding, [8]. We also show that a simple TDMA scheme using the results of [4] for the single-user case also achieves sum capacity, but provides a strictly smaller region than shown in this paper.

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.

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

1-4244-0504-1/06/$20.00 ©2006 IEEE

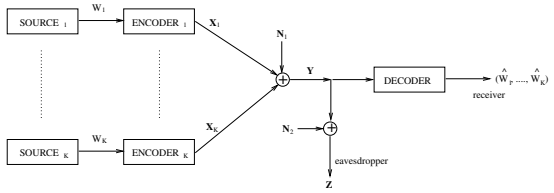

Fig. 1. The GMAC-WT System Model

exact definition of which will be made precise shortly.

The signal at the intended receiver is given by

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

and the wire-tapper receives

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

where each component of $\mathbf{N}_i \sim \mathcal{N}\left(0, \sigma_i^2\right)$, $i = 1, 2$. We also assume the following received power constraints:

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

A. The Secrecy Measure

We aim to provide each user with a pre-determined amount of secrecy. To that end, in [7], we used an approach similar to [4], and defined a set of secrecy constraints using the normalized equivocations for sets of users:

$$\Delta_{\mathcal{S}} \triangleq \frac{H(\mathbf{W}_{\mathcal{S}}|\mathbf{Z})}{H(\mathbf{W}_{\mathcal{S}})} \quad \forall \mathcal{S} \subseteq \mathcal{K} \tag{4}$$

where $\mathcal{K} = \{1, \ldots, K\}$ and $\mathbf{W}_{\mathcal{S}} = \{W_j\}_{j\in\mathcal{S}}$.

As our secrecy criterion, we require that each user $j \in \{1, \ldots, K\}$ must satisfy $\Delta_{\mathcal{S}} \geq \delta$ for all sets $\mathcal{S} \subseteq \mathcal{K}$, and $\delta \in [0, 1]$ is the required level of secrecy. $\delta = 1$ corresponds to *perfect secrecy*, where the wire-tapper is not allowed to get any information; and $\delta = 0$ corresponds to no secrecy constraint. This constraint guarantees that each subset of users maintains a level of secrecy greater than δ. Since this must be true for all sets of users, collectively the system has at least the same level of secrecy. However, if a group of users are somehow compromised, the remaining users may also be vulnerable.

B. The δ-secret rate region

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

$$\frac{1}{n}\log_2 M_k \geq R_k - \epsilon \quad k = 1, \ldots, K \tag{5}$$

$$P_e \leq \epsilon \tag{6}$$

$$\Delta_{\mathcal{S}} \geq \delta \quad \forall \mathcal{S} \subseteq \mathcal{K} \tag{7}$$

where user k chooses one of M_k symbols to transmit according to the uniform distribution, and P_e is the average probability of error. We will call the set of all achievable rates with δ-secrecy, the *δ-secret rate region*, and denote it $\mathcal{C}^{(\delta)}$.

C. Some Preliminary Definitions

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

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

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

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

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*.

III. Outer Bound on the δ-Secret Rate Region

In this section, we present an outer bound on the set of achievable δ-secret rates, denoted $\hat{\mathcal{C}}^{(\delta)}$, and explicitly state the outer bound on the achievable sum-rate with δ-secrecy. We also evaluate this bound assuming we are limited to using Gaussian codebooks for calculation purposes, $\hat{\mathcal{G}}^{(\delta)}$.

Our main result is presented in the following theorem:

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

$$R_{\mathcal{S}} \leq C_{\mathcal{S}}^{(\mathsf{M})} \tag{8}$$

$$R_{\mathcal{S}} \leq \frac{1}{\delta}\left[C_{\mathcal{S}}^{(\mathsf{M})} - C\left(\frac{\sum_{j\in\mathcal{S}} 2^{\frac{2}{n}H(\mathbf{X}_j)}}{2\pi e\left(P_{\mathcal{S}^c}+\sigma_1^2+\sigma_2^2\right)}\right)\right] \tag{9}$$

The set of all $\mathbf{R}$ satisfying (8) and (9) is denoted $\hat{\mathcal{C}}^{(\delta)}$.

Corollary 2.1. The sum-rate with δ-secrecy satisfies

$$C_{sum}^{(\delta)} = \sum_{j=1}^{K} R_j \leq \min\left\{C_{sum}^{(\mathsf{M})}, \frac{C_{sum}^{(\mathsf{M})} - C_{sum}^{(\mathsf{MW})}}{\delta}\right\} \tag{10}$$

Corollary 2.2. The rate-tuples with δ-secrecy using Gaussian codebooks must satisfy (8) and

$$R_{\mathcal{S}} \leq \frac{C_{\mathcal{S}}^{(\mathsf{M})} - \tilde{C}_{\mathcal{S}}^{(\mathsf{MW})}}{\delta} \quad \forall \mathcal{S} \subseteq \mathcal{K} \tag{11}$$

The set of all such $\mathbf{R}$ is denoted $\hat{\mathcal{G}}^{(\delta)}$.

Proof: See Appendix I. □

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

IV. Achievable δ-Secret Rate Regions

A. Gaussian Codebooks

In this section, we find a set of achievable rates using Gaussian codebooks, which we call $\check{\mathcal{G}}^{(\delta)}$, and show that Gaussian codebooks achieve the limit on sum capacity. This region coincides with our previous upper bound evaluated using Gaussian codebooks, $\hat{\mathcal{G}}^{(\delta)}$, giving the full characterization of the δ-secret rate region using Gaussian codebooks, $\mathcal{G}^{(\delta)}$.

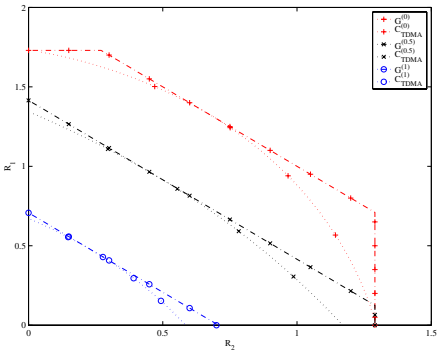

Fig. 2. Regions for $\delta = 0, 0.5, 1$ and $P_1 = 10$, $P_2 = 5$, $\sigma_1^2 = 1$, $\sigma_2^2 = 2$

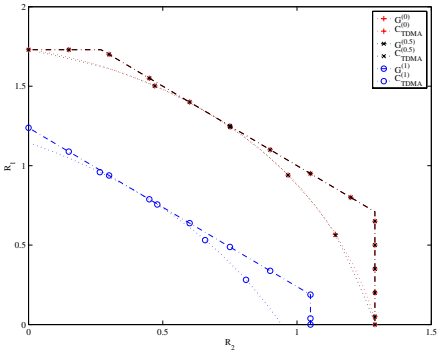

Fig. 3. Regions for $\delta = 0, 0.5, 1$ and $P_1 = 10$, $P_2 = 5$, $\sigma_1^2 = 1$, $\sigma_2^2 = 7$

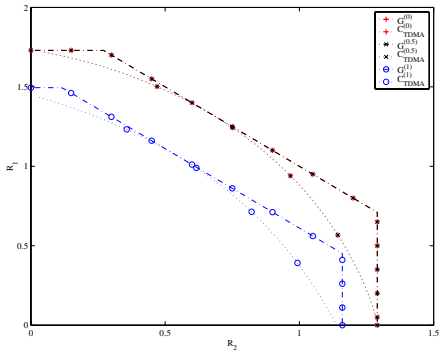

Fig. 4. Regions for $\delta = 0, 0.5, 1$ and $P_1 = 10$, $P_2 = 5$, $\sigma_1^2 = 1$, $\sigma_2^2 = 20$

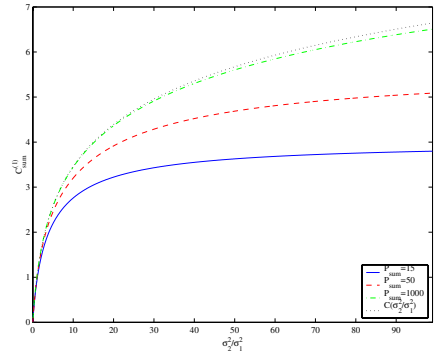

Fig. 5. $C_{sum}^{(1)}$ vs. σ_2^2/σ_1^2. $C(15) = 4$, $C(50) = 5.67$, $C(1000) = 9.97$

Theorem 3. We can transmit with δ-secrecy using Gaussian codebooks at rates satisfying (8) and (11). The region containing all $\mathbf{R}$ satisfying these equations is denoted $\tilde{\mathcal{G}}^{(\delta)}$.

Corollary 3.1. We can transmit with perfect secrecy ($\delta = 1$) using Gaussian codebooks at rates satisfying

$$R_{\mathcal{S}} \leq C_{\mathcal{S}}^{(\mathsf{M})} - \tilde{C}_{\mathcal{S}}^{(\mathsf{MW})} \tag{12}$$

Proof: See Appendix II. The corollary was also presented in [7]. □

B. Time-Division

We can also use a TDMA scheme and the result of [4] to get an achievable region:

Theorem 4. Consider this scheme: Let $\alpha_k \in [0,1]$, $k = 1, \ldots, K$ and $\sum_{k=1}^{K} \alpha_k = 1$. User k only transmits α_k of the time with power $P_{k,max}/\alpha_k$ using the scheme described in [4]. Then, the following set of rates is achievable:

$$\bigcup_{\substack{\mathbf{0} \preceq \boldsymbol{\alpha} \preceq \mathbf{1} \\ \sum_{k=1}^{K} \alpha_k = 1}} \Big\{ \mathbf{R} \colon R_k \leq \alpha_k \frac{C\left(\frac{P_{k,max}}{\alpha_k \sigma_1^2}\right) - C\left(\frac{P_{k,max}}{\alpha_k(\sigma_1^2+\sigma_2^2)}\right)}{\delta},$$

$$R_k \leq \alpha_k C\Big(\frac{P_{k,max}}{\alpha_k \sigma_1^2}\Big),\ k = 1, \ldots, K \Big\} \tag{13}$$

We will call the set of all $\mathbf{R}$ satisfying the above, $\mathcal{C}_{TDMA}^{(\delta)}$.

Proof: Follows directly from [4, Theorem 1] □

V. Numerical Results and Conclusions

Figures 2–4 show the shapes of $\mathcal{G}^{(\delta)}$ for $\delta = 0, 0.5, 1$ for two users. When $\delta = 0$, we are not concerned with secrecy, and the resulting region corresponds to the standard GMAC region, [9]. The region for $\delta = 1$ corresponds to the *perfect secrecy* region - transmitting at rates within this region, it is possible to send zero information to the wire-tapper. The intermediate region, $\delta = 0.5$, can be thought of as constraining at least half the transmitted information to be secret. It can be seen that this enlarges the region from the perfect secrecy case. In Figure 2, it is shown that relaxing this constraint may provide a larger region, the limit of which is the GMAC region. In Figures 3 and 4, however, this region is already equivalent to the GMAC capcity region. Hence, relaxing our secrecy constraints will not result in further improvement in the set of achievable rates. Note that it is possible to send at capacity of the GMAC and still provide a non-zero level of secrecy, the minimum value of which depends on how much extra noise the wire-tapper sees. Also shown in the figures is the regions achievable by the TDMA scheme described in the previous section. Although TDMA achieves the sum capacity with optimum time-sharing parameters, this region is in general contained within $\mathcal{G}^{(\delta)}$.

One important point is the dependence of the perfect secrecy region, $\mathcal{G}^{(1)}$, on σ_2^2. It can easily be shown that as $\sigma_2^2 \to \infty$, the perfect secrecy region coincides with the standard GMAC region, $\mathcal{G}^{(0)}$. Thus, when the wire-tapper sees a much noisier channel than the intended receiver, it is possible to send information with perfect secrecy at close to capacity. However, when this is not the case, $\mathcal{G}^{(1)}$ is limited by the noise powers regardless of how much we increase the input powers, since $\lim_{P_{\mathcal{K}} \to \infty} C_{sum}^{(1)} = C(\sigma_2^2/\sigma_1^2)$.

Another interesting note is that even when a user does not have any information to send, it can still generate and send

random codewords to confuse the eavesdropper and help other users. This can be seen in Figures 2 and 3 as the TDMA region does not end at the "legs" of $\mathcal{G}^{(\delta)}$ when $\mathcal{G}^{(\delta)}$ is not equal to the GMAC capacity region.

APPENDIX I
OUTER BOUNDS

We show that any achievable rate vector, $\mathbf{R}$, needs to satisfy Theorem 2. (8) is due to the converse of the GMAC coding theorem. To see (9), start with a few lemmas:

Lemma 5. Let $\mathbf{X}_{\mathcal{S}} = \{\mathbf{X}_k\}_{k\in\mathcal{S}}$ where $\mathcal{S} \subseteq \mathcal{K}$. Then,

$$R_{\mathcal{S}} \leq \frac{1}{n\delta} I(\mathbf{X}_{\mathcal{S}}; \mathbf{Y}|\mathbf{Z}) + \nu_n \quad \forall \mathcal{S} \subseteq \mathcal{K} \tag{14}$$

where $\nu_n \to 0$ as $\epsilon \to 0$.

Proof: Let $\mathcal{S} \subseteq \mathcal{K}$ and consider the two inequalities:

$$\delta \leq \Delta_{\mathcal{S}} = \frac{H(\mathbf{W}_{\mathcal{S}}|\mathbf{Z})}{\log\left(\prod_{j\in\mathcal{S}} M_j\right)} \leq \frac{H(\mathbf{W}_{\mathcal{S}}|\mathbf{Z})}{n\left(R_{\mathcal{S}} - |\mathcal{S}|\epsilon\right)} \tag{15}$$

$$H(\mathbf{W}_{\mathcal{S}}|\mathbf{Z},\mathbf{Y}) \leq H(\mathbf{W}_{\mathcal{S}}|\mathbf{Y}) \leq H(\mathbf{W}_{\mathcal{K}}|\mathbf{Y}) \leq \eta_n \tag{16}$$

where (16) follows using Fano's Inequality with $\eta_n \to 0$ as $\epsilon \to 0$ and $n \to \infty$. Using (15) and (16), we can write

$$\delta \leq \frac{H(\mathbf{W}_{\mathcal{S}}|\mathbf{Z}) + \eta_n - H(\mathbf{W}_{\mathcal{S}}|\mathbf{Z},\mathbf{Y})}{n\left(R_{\mathcal{S}} - |\mathcal{S}|\epsilon\right)} \tag{17}$$

$$\leq \frac{I(\mathbf{X}_{\mathcal{S}}; \mathbf{Y}|\mathbf{Z}) + \eta_n}{n\left(R_{\mathcal{S}} - |\mathcal{S}|\epsilon\right)} \tag{18}$$

with the last step using $W_{\mathcal{S}} \to \mathbf{X}_{\mathcal{S}} \to \mathbf{Y} \to \mathbf{Z}$. Rearranging and defining $\nu_n \triangleq \frac{\eta_n}{n\delta} + |\mathcal{S}|\epsilon$ completes the proof. □

Lemma 6 (Lemma 10 in [4]). Let $\xi = \frac{1}{n}H(\mathbf{Y})$, then,

$$H(\mathbf{Z}) - H(\mathbf{Y}) \geq n\phi(\xi) \triangleq \frac{n}{2}\log\left[2\pi e\left(\sigma_2^2 + \frac{1}{2\pi e}2^{2\xi}\right)\right] - n\xi \tag{19}$$

Corollary 6.1.

$$H(\mathbf{Z}) - H(\mathbf{Y}) \geq \frac{n}{2}\log\left(1 + \frac{\sigma_2^2}{P_{\mathcal{K}} + \sigma_1^2}\right) \tag{20}$$

Proof: The lemma is given in [4] and its proof is omitted here since it is easily shown using the entropy power inequality, [9]. To see the corollary, write

$$H(\mathbf{Y}) \leq \frac{n}{2}\log\left(2\pi e(P_{\mathcal{K}} + \sigma_1^2)\right) \tag{21}$$

Let $H(\mathbf{Y}) = n\xi$. Then, $\xi \leq \frac{1}{2}\log\left(2\pi e(P_{\mathcal{K}} + \sigma_1^2)\right)$, and since $\phi(\xi)$ is a non-increasing function of ξ, we get $\phi(\xi) \geq \phi\left(\frac{1}{2}\log\left(2\pi e(P_{\mathcal{K}} + \sigma_1^2)\right)\right)$. Then, from Lemma 6,

$$H(\mathbf{Z}) - H(\mathbf{Y}) \geq \frac{n}{2}\log\left(1 + \frac{\sigma_2^2}{P_{\mathcal{K}} + \sigma_1^2}\right) \tag{22}$$

□

Lemma 7. For the GMAC-WT,

$$I(\mathbf{X}_{\mathcal{S}}; \mathbf{Y}|\mathbf{Z}) \leq nC_{\mathcal{S}}^{(\mathsf{M})} - nC\left(\frac{\frac{1}{2\pi e}\sum_{j\in\mathcal{S}} 2^{\frac{2}{n}H(\mathbf{X}_j)}}{P_{\mathcal{S}^c} + \sigma_1^2 + \sigma_2^2}\right) \tag{23}$$

Corollary 7.1. For the GMAC-WT,

$$I(\mathbf{X}_{\mathcal{K}}; \mathbf{Y}|\mathbf{Z}) \leq n\left(C_{sum}^{(\mathsf{M})} - C_{sum}^{(\mathsf{MW})}\right) \tag{24}$$

Proof: Start by writing

$$I(\mathbf{X}_{\mathcal{S}}, \mathbf{Y}|\mathbf{Z}) = H(\mathbf{X}_{\mathcal{S}}|\mathbf{Z}) - H(\mathbf{X}_{\mathcal{S}}|\mathbf{Y},\mathbf{Z}) \tag{25}$$
$$= H(\mathbf{X}_{\mathcal{S}}|\mathbf{Z}) - H(\mathbf{X}_{\mathcal{S}}|\mathbf{Y}) \tag{26}$$
$$= [H(\mathbf{X}_{\mathcal{S}}) - H(\mathbf{X}_{\mathcal{S}}|\mathbf{Y})] - [H(\mathbf{X}_{\mathcal{S}}) - H(\mathbf{X}_{\mathcal{S}}|\mathbf{Z})] \tag{27}$$
$$\leq [H(\mathbf{X}_{\mathcal{S}}|\mathbf{X}_{\mathcal{S}^c}) - H(\mathbf{X}_{\mathcal{S}}|\mathbf{Y},\mathbf{X}_{\mathcal{S}^c})] - [H(\mathbf{X}_{\mathcal{S}}) - H(\mathbf{X}_{\mathcal{S}}|\mathbf{Z})] \tag{28}$$
$$= I(\mathbf{X}_{\mathcal{S}}; \mathbf{Y}|\mathbf{X}_{\mathcal{S}^c}) - I(\mathbf{X}_{\mathcal{S}}; \mathbf{Z}) \tag{29}$$
$$= H(\mathbf{Y}|\mathbf{X}_{\mathcal{S}^c}) - H(\mathbf{Y}|\mathbf{X}_{\mathcal{K}}) - [H(\mathbf{Z}) - H(\mathbf{Z}|\mathbf{X}_{\mathcal{S}})] \tag{30}$$
$$= \sum_{i=1}^n H(Y_i|Y^{i-1}, \mathbf{X}_{\mathcal{S}^c}) - \sum_{i=1}^n H(Y_i|Y^{i-1}, \mathbf{X}_{\mathcal{K}}) - [H(\mathbf{Z}) - H(\mathbf{Z}|\mathbf{X}_{\mathcal{S}})] \tag{31}$$
$$\leq \sum_{i=1}^n H(Y_i|\mathbf{X}_{\mathcal{S}^c,i}) - \sum_{i=1}^n H(Y_i|\mathbf{X}_{\mathcal{K},i}) - [H(\mathbf{Z}) - H(\mathbf{Z}|\mathbf{X}_{\mathcal{S}})] \tag{32}$$
$$\leq \sum_{i=1}^n \frac{1}{2}\log\left[2\pi e\left(P_{\mathcal{S}} + \sigma_1^2\right)\right] - \sum_{i=1}^n \frac{1}{2}\log\left(2\pi e\sigma_1^2\right) - [H(\mathbf{Z}) - H(\mathbf{Z}|\mathbf{X}_{\mathcal{S}})] \tag{33}$$
$$= nC\left(P_{\mathcal{S}}/\sigma_1^2\right) - [H(\mathbf{Z}) - H(\mathbf{Z}|\mathbf{X}_{\mathcal{S}})] \tag{34}$$

where (26) follows from $\mathbf{X}_{\mathcal{S}} \to \mathbf{Y} \to \mathbf{Z}$ and (32) follows using the memoryless property of M. For the term in brackets, start by using the entropy power inequality:

$$2^{\frac{2}{n}H(\mathbf{Z})} \geq 2^{\frac{2}{n}H(\mathbf{Z}|\mathbf{X}_{\mathcal{S}})} + \textstyle\sum_{j\in\mathcal{S}} 2^{\frac{2}{n}H(\mathbf{X}_j)} \tag{35}$$
$$2^{\frac{2}{n}H(\mathbf{Z}) - \frac{2}{n}H(\mathbf{Z}|\mathbf{X}_{\mathcal{S}})} \geq 1 + 2^{-\frac{2}{n}H(\mathbf{Z}|\mathbf{X}_{\mathcal{S}})} \sum_{j\in\mathcal{S}} 2^{\frac{2}{n}H(\mathbf{X}_j)} \tag{36}$$

Then,

$$2^{\frac{2}{n}H(\mathbf{Z}|\mathbf{X}_{\mathcal{S}})} = 2^{\frac{2}{n}\sum_{i=1}^n H(Z_i|Z^{i-1},\mathbf{X}_{\mathcal{S}})} \tag{37}$$
$$\leq 2^{\frac{2}{n}\sum_{i=1}^n H(Z_i|\mathbf{X}_{\mathcal{S},i})} \tag{38}$$
$$\leq 2^{\frac{2}{n}\sum_{i=1}^n \frac{1}{2}\log\left(2\pi e(P_{\mathcal{S}^c} + \sigma_1^2 + \sigma_2^2)\right)} \tag{39}$$
$$= 2\pi e(P_{\mathcal{S}^c} + \sigma_1^2 + \sigma_2^2) \tag{40}$$

Using this in (36), and taking the log we get,

$$H(\mathbf{Z}) - H(\mathbf{Z}|\mathbf{X}_{\mathcal{S}}) \geq \frac{n}{2}\log\left(1 + \frac{\frac{1}{2\pi e}\sum_{j\in\mathcal{S}} 2^{\frac{2}{n}H(\mathbf{X}_j)}}{P_{\mathcal{S}^c} + \sigma_1^2 + \sigma_2^2}\right) \tag{41}$$

which, with (34) completes the proof. To see the corollary,

$$I(\mathbf{X}_{\mathcal{K}}; \mathbf{Y}|\mathbf{Z}) = H(\mathbf{X}_{\mathcal{K}}|\mathbf{Z}) - H(\mathbf{X}_{\mathcal{K}}|\mathbf{Y},\mathbf{Z}) \tag{42}$$
$$= H(\mathbf{X}_{\mathcal{K}}|\mathbf{Z}) - H(\mathbf{X}_{\mathcal{K}}|\mathbf{Y}) \tag{43}$$
$$= [H(\mathbf{Z}|\mathbf{X}_{\mathcal{K}}) + H(\mathbf{X}_{\mathcal{K}}) - H(\mathbf{Z})] - [H(\mathbf{Y}|\mathbf{X}_{\mathcal{K}}) + H(\mathbf{X}_{\mathcal{K}}) - H(\mathbf{Y})] \tag{44}$$
$$= [H(\mathbf{Z}|\mathbf{X}_{\mathcal{K}}) - H(\mathbf{Y}|\mathbf{X}_{\mathcal{K}})] - [H(\mathbf{Z}) - H(\mathbf{Y})] \tag{45}$$
$$= \sum_{i=1}^n [H(Z_i|\mathbf{X}_{\mathcal{K},i}) - H(Y_i|\mathbf{X}_{\mathcal{K},i})] - [H(\mathbf{Z}) - H(\mathbf{Y})] \tag{46}$$
$$= \left[\frac{n}{2}\log\left(2\pi e(\sigma_1^2 + \sigma_2^2)\right) - \frac{n}{2}\log\left(2\pi e\sigma_1^2\right)\right] - [H(\mathbf{Z}) - H(\mathbf{Y})] \tag{47}$$
$$\leq \frac{n}{2}\log\left(1 + \frac{\sigma_2^2}{\sigma_1^2}\right) - \frac{n}{2}\log\left(1 + \frac{\sigma_2^2}{P_{\mathcal{K}} + \sigma_1^2}\right) \tag{48}$$
$$= C_{sum}^{(\mathsf{M})} - C_{sum}^{(\mathsf{MW})} \tag{49}$$

where (43) is due to $\mathbf{X}_{\mathcal{K}} \to \mathbf{Y} \to \mathbf{Z}$ and (46) to the memorylessness of the channels. (48) follows from Corollary 6.1. □

This and Lemma 5, complete the proof of Theorem 2.

Corollary 2.1 follows from Corollary 7.1 and Lemma 5.

Corollary 2.2 follows simply with $H(\mathbf{X}_j) = \frac{n}{2}\log 2\pi e P_j$.

APPENDIX II
ACHIEVABLE RATES

Let $\mathbf{R} = (R_1, \ldots, R_K)$ satisfy (8) and (11). For each user $k \in \mathcal{K}$, consider the scheme:

1) Let $M_k = 2^{n(R_k - \epsilon')}$ where $0 \le \epsilon' < \epsilon$. Let $M_k = M_{ks} M_{k0}$ where $M_{ks} = M_k^{\mu_k}$, $M_{k0} = M_k^{1-\mu_k}$, and $\mu_k \ge \delta$ will be chosen later. Then, $R_k = R_{ks} + R_{k0} + \epsilon'$ where $R_{ks} = \frac{1}{n}\log M_{ks}$ and $R_{k0} = \frac{1}{n}\log M_{k0}$. We can choose ϵ' and n to ensure that M_{ks}, M_{k0} are integers.
2) Generate 3 codebooks $\mathfrak{X}_{ks}, \mathfrak{X}_{k0}$ and $\mathfrak{X}_{kx}$. $\mathfrak{X}_{ks}$ consists of M_{ks} codewords, each component of which is drawn $\sim \mathcal{N}(0, \lambda_{ks}P_k - \varepsilon)$. Codebook $\mathfrak{X}_{k0}$ has M_{k0} codewords with each component randomly drawn $\sim \mathcal{N}(0, \lambda_{k0}P_k - \varepsilon)$ and $\mathfrak{X}_{kx}$ has M_{kx} codewords with each component randomly drawn $\sim \mathcal{N}(0, \lambda_{kx}P_k - \varepsilon)$ where ε is an arbitrarily small number to ensure that the power constraints on the codewords are satisfied with high probability and $\lambda_{ks} + \lambda_{k0} + \lambda_{kx} = 1$. Define $R_{kx} = \frac{1}{n}\log M_{kx}$ and $M_{kt} = M_k M_{kx}$.
3) Each message $W_k \in \{1, \ldots, M_k\}$ is mapped into a message vector $\mathbf{W}_k = (W_{ks}, W_{k0})$ where $W_{ks} \in \{1, \ldots, M_{ks}\}$ and $W_{k0} \in \{1, \ldots, M_{k0}\}$. Since W_k is uniformly chosen, W_{ks}, W_{k0} are also uniformly distributed.
4) To transmit message $W_k \in \{1, \ldots, M_k\}$, user k finds the 2 codewords corresponding to components of $\mathbf{W}_k$ and also uniformly chooses a codeword from $\mathfrak{X}_{kx}$. He then adds all these codewords and transmits the resulting codeword, $\mathbf{X}_k$, so that we are actually transmitting one of M_{kt} codewords. Let $R_{kt} = \frac{1}{n}\log M_{kt} + \epsilon' = R_{ks} + R_{k0} + R_{kx} + \epsilon'$.

We will choose the rates such that for all $\mathcal{S} \subseteq \mathcal{K}$,

$$\sum_{k\in\mathcal{S}} R_{ks} = \sum_{k\in\mathcal{S}} \mu_k R_k \le C_{\mathcal{S}}^{(\mathsf{M})} - \tilde{C}_{\mathcal{S}}^{(\mathsf{MW})} \quad (50)$$

$$\sum_{k=1}^{K}[R_{k0} + R_{kx}] = \sum_{k=1}^{K}[(1-\mu_k)R_k + R_{kx}] = C_{sum}^{(\mathsf{MW})} \quad (51)$$

$$\sum_{k\in\mathcal{S}} R_{kt} = \sum_{k\in\mathcal{S}}[R_k + R_{kx}] \le C_{\mathcal{S}}^{(\mathsf{M})} \quad (52)$$

From (52) and the GMAC coding theorem, with high probability the receiver can decode the codewords with low probability of error. To show $\Delta_{\mathcal{S}} \ge \delta$, $\forall \mathcal{S} \subseteq \mathcal{K}$, we concern ourselves only with MAC sub-code $\{\mathfrak{X}_{ks}\}_{k=1}^{K}$. From this point of view, the coding scheme described is equivalent to each user $k \in \mathcal{K}$ selecting one of M_{ks} messages, and sending a uniformly chosen codeword from among $M_{k0}M_{kx}$ codewords for each. Let $\mathbf{W}_{\mathcal{S}}^{(s)} = \{W_{ks}\}_{k\in\mathcal{S}}$ and $\Delta_{\mathcal{S}}^{(s)} = \frac{H(\mathbf{W}_{\mathcal{S}}^{(s)}|\mathbf{Z})}{H(\mathbf{W}_{\mathcal{S}}^{(s)})}$ and define $\mathbf{X}_\Sigma = \sum_{k=1}^{K}\mathbf{X}_k$. For $\mathcal{K}$ write

$$\Delta_{\mathcal{K}}^{(s)} = \frac{H(\mathbf{W}_{\mathcal{K}}^{(s)}|\mathbf{Z})}{H(\mathbf{W}_{\mathcal{K}}^{(s)})} = \frac{H(\mathbf{W}_{\mathcal{K}}^{(s)}, \mathbf{Z}) - H(\mathbf{Z})}{H(\mathbf{W}_{\mathcal{K}}^{(s)})} \quad (53)$$

$$= \frac{H(\mathbf{W}_{\mathcal{K}}^{(s)}, \mathbf{X}_\Sigma, \mathbf{Z}) - H(\mathbf{X}_\Sigma|\mathbf{W}_{\mathcal{K}}^{(s)}, \mathbf{Z}) - H(\mathbf{Z})}{H(\mathbf{W}_{\mathcal{K}}^{(s)})} \quad (54)$$

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

$$+ \frac{H(\mathbf{X}_\Sigma|\mathbf{W}_{\mathcal{K}}^{(s)}) - H(\mathbf{X}_\Sigma|\mathbf{W}_{\mathcal{K}}^{(s)}, \mathbf{Z})}{H(\mathbf{W}_{\mathcal{K}}^{(s)})} \quad (55)$$

$$= 1 - \frac{I(\mathbf{X}_\Sigma; \mathbf{Z}) - I(\mathbf{X}_\Sigma; \mathbf{Z}|\mathbf{W}_{\mathcal{K}}^{(s)})}{n\left(\sum_{k=1}^{K} R_{ks}\right)} \quad (56)$$

where we used $\mathbf{W}_{\mathcal{K}}^{(s)} \to \mathbf{X}_\Sigma \to \mathbf{Z} \Rightarrow H(\mathbf{Z}|\mathbf{W}_{\mathcal{K}}^{(s)}, \mathbf{X}_\Sigma) = H(\mathbf{Z}|\mathbf{X}_\Sigma)$ to get (56). We will consider the two terms individually. First, we have the trivial bound due to channel capacity:

$$I(\mathbf{X}_\Sigma; \mathbf{Z}) \le nC_{sum}^{(\mathsf{MW})} \quad (57)$$

$I(\mathbf{X}_\Sigma; \mathbf{Z}|\mathbf{W}_{\mathcal{K}}^{(s)}) = H(\mathbf{X}_\Sigma|\mathbf{W}_{\mathcal{K}}^{(s)}) - H(\mathbf{X}_\Sigma|\mathbf{W}_{\mathcal{K}}^{(s)}, \mathbf{Z})$. Since user k sends one of $M_{k0}M_{kx}$ codewords for each message,

$$H(\mathbf{X}_\Sigma|\mathbf{W}_{\mathcal{K}}^{(s)}) = \log\left(\prod_{k=1}^{K} M_{k0}M_{kx}\right) \quad (58)$$

$$= n\sum_{k=1}^{K}[(1-\mu_k)R_k + R_{kx}] \quad (59)$$

We can also write

$$H(\mathbf{X}_\Sigma|\mathbf{W}_{\mathcal{K}}^{(s)}, \mathbf{Z}) \le n\eta_n' \quad (60)$$

where $\eta_n' \to 0$ as $n \to \infty$ since, with high probability, the eavesdropper can decode $\mathbf{X}_\Sigma$ given $\mathbf{W}_{\mathcal{K}}^{(s)}$ due to (51). Using (50), (51), (57), (59) and (60) in (56), we get

$$\Delta_{\mathcal{K}}^{(s)} \ge 1 - \frac{C_{sum}^{(\mathsf{MW})} - \sum_{k=1}^{K}[(1-\mu_k)R_k + R_{kx}] + \eta_n'}{C_{sum}^{(\mathsf{M})} - C_{sum}^{(\mathsf{MW})}} \quad (61)$$

$$= 1 - \frac{\eta_n'}{C_{sum}^{(\mathsf{M})} - C_{sum}^{(\mathsf{MW})}} \to 1 \text{ as } \eta_n' \to 0 \quad (62)$$

Then,

$$H(\mathbf{W}_{\mathcal{K}}^{(s)}|\mathbf{Z}) = H(\mathbf{W}_{\mathcal{K}}^{(s)}) \quad (63)$$

$$H(\mathbf{W}_{\mathcal{S}}^{(s)}|\mathbf{Z}) + H(\mathbf{W}_{\mathcal{S}^c}^{(s)}|\mathbf{Z}) \ge H(\mathbf{W}_{\mathcal{S}}^{(s)}) + H(\mathbf{W}_{\mathcal{S}^c}^{(s)}) \quad (64)$$

As conditioning reduces entropy, we have $H(\mathbf{W}_{\mathcal{S}}^{(s)}|\mathbf{Z}) \le H(\mathbf{W}_{\mathcal{S}}^{(s)})$ and $H(\mathbf{W}_{\mathcal{S}^c}^{(s)}|\mathbf{Z}) \le H(\mathbf{W}_{\mathcal{S}^c}^{(s)})$. Then, from the above equation we conclude that we must have $H(\mathbf{W}_{\mathcal{S}}^{(s)}) = H(\mathbf{W}_{\mathcal{S}}^{(s)}|\mathbf{Z})$, $\forall \mathcal{S} \subset \mathcal{K}$. This makes $\Delta_{\mathcal{S}}^{(s)} = 1$ $\forall \mathcal{S} \subset \mathcal{K}$. The proof is completed by noting that

$$\Delta_{\mathcal{S}} \ge \frac{H(\mathbf{W}_{\mathcal{S}}^{(s)}|\mathbf{Z})}{H(\mathbf{W}_{\mathcal{S}})} = \frac{H(\mathbf{W}_{\mathcal{S}}^{(s)})}{H(\mathbf{W}_{\mathcal{S}})} = \frac{\sum_{k\in\mathcal{S}}\mu_k R_k}{\sum_{k\in\mathcal{S}} R_k} \ge \delta \quad (65)$$

We can think of $\{W_{ks}\}$ as the "protected" messages and $\{W_{k0}\}$ as the "unprotected" messages. The corollary is apparent from (62), and also follows as (11) implies (8) if $\delta = 1$.

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] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inform. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[7] 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.

[8] T. S. Han and K. Kobayashi, "A new achievable rate region for the interference channel," *IEEE Trans. Inform. Theory*, vol. 27, no. 1, pp. 49–60, January 1981.

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