The Gaussian Multiple Access Wire-Tap Channel

Ender Tekin, *Student Member, IEEE*, and Aylin Yener, *Member, IEEE*

***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 suitable security measures for this multiaccess environment. Using codebooks generated randomly according to a Gaussian distribution, achievable secrecy rate regions are identified using superposition coding and time-division multiple access (TDMA) coding schemes. An upper bound for the secrecy sum-rate is derived, and our coding schemes are shown to achieve the sum capacity. Numerical results are presented showing the new rate region and comparing it with the capacity region of the Gaussian multiple-access channel (GMAC) with no secrecy constraints, which quantifies the price paid for secrecy.**

***Index Terms*—Secrecy capacity, Gaussian multiple access channel, wire-tap channel.**

I. Introduction

Shannon, in [1], analyzed secrecy systems in a communications scenario where the legitimate parties share a secret key to communicate secretly from a wire-tapper. Shannon showed that, to achieve perfect secrecy of communications, the conditional probability of the *cryptogram given a message* must be 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 Δ, the normalized conditional entropy of the transmitted message given the received signal at the wire-tapper. The region of all possible rate/equivocation, (R, Δ), pairs is determined, and the existence of a positive *secrecy capacity*, C_s, for communication below which it is possible to limit the rate of information leaked to the wire-tapper to arbitrarily small values, 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. 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.

Manuscript received December 22, 2006; revised March 01, 2008, August 22, 2008. Current version published November 21, 2008. This work was supported in part by the National Science Foundation Grant CCF-0514813 "Multiuser Wireless Security," and by the DARPA ITMANET Program by Grant W911NF-07-1-0028. The material in this correspondence was presented in part at the Asilomar Conference on Signals, Systems and Computers, Pacific Grove, CA, November 2005, and at the IEEE International Symposium on Information Theory, Seattle, WA, July2006.

The authors are with the Department of Electrical Engineering, Pennsylvania State University, University Park, PA 16802 USA (e-mail: tekin@psu.edu; yener@ee.psu.edu).

Color versions of Figs.2–4 in this correspondence are available online at http://ieexplore.ieee.org.

Communicated by G. Kramer, Associate Editor for Shannon Theory.

Digital Object Identifier 10.1109/TIT.2008.2006385

Recently, the closely related problem of common randomness and secret key generation has gathered attention. Maurer [6] and Bennett *et al.*, [7] have focused on the process of "distilling" a secret key between two parties in the presence of a wire-tapper, where all parties have partial information about a common random variable. In [6], it was shown that for the case when the wire-tap channel capacity is zero between two users, the existence of a "public" feedback channel that the wire-tapper can also observe can nevertheless enable the two parties to be able to generate a secret key. This discussion was then furthered by [8] and [9] where the secrecy key capacities and *common randomness* capacities, the maximum rates of common randomness that can be generated by two terminals, were developed for several models. References [10]–[13] examined the multi-terminal secret key generation problem. It was also argued in [14], that the secrecy constraint developed by Wyner and later utilized by Csiszár and Körner was "weak" since it only constrained the rate of information leaked to the wire-tapper, rather than the total information. It was shown that Wyner's scenario could be extended to "strong" secrecy for discrete channels with no loss in achievable rates, where the secrecy constraint is placed on the total information obtained by the wire-tapper, as the information of interest might be in the small amount leaked. Maurer also examined the case of active adversaries, where the wire-tapper has read/write access to the channel in [15]–[17].

More recently, the notion of the wire-tap channel has been extended to parallel channels and fading channels [18]–[23]. Broadcast and interference channels with confidential messages were considered in [24]. References [25], [26] examined the so called multiple access channel with confidential messages, where two transmitters try to keep their messages secret from each other while communicating with a common receiver, finding an achievable region, and the capacity region for some special cases.

In this correspondence, we define the Gaussian multiple access wire-tap channel (GMAC-WT) where multiple users are transmitting to a base station in the presence of AWGN, and a wiretapper receives a noisy version of the signal received at the base station. For this new multi-transmitter secrecy paradigm, we first define two separate secrecy constraints, which we call the *individual* and *collective* secrecy constraints. These are 1) 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 2) 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 [27], we concerned ourselves mainly with the *perfect secrecy rate region*[1] for both sets of constraints. In this correspondence, we consider the general case where a predetermined level of secrecy is provided. Using codebooks generated according to a Gaussian distribution and superposition coding, we find the achievable *secrecy rate regions* 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. This scheme achieves the secrecy sum capacity for collective constraints. We also find a secrecy rate region using TDMA and the results of [4] for a single-user. This scheme achieves secrecy sum capacity for both constraints, but is smaller than the region for collective constraints. When individual

[1]We should stress that in our work, we use "perfect secrecy" as used by Wyner rather than Shannon, whereby we require that the *rate*, rather than the total amount, of information leaked to the adversary is negligible. In this sense, it is more accurate to think of it as "approximately perfect secrecy."

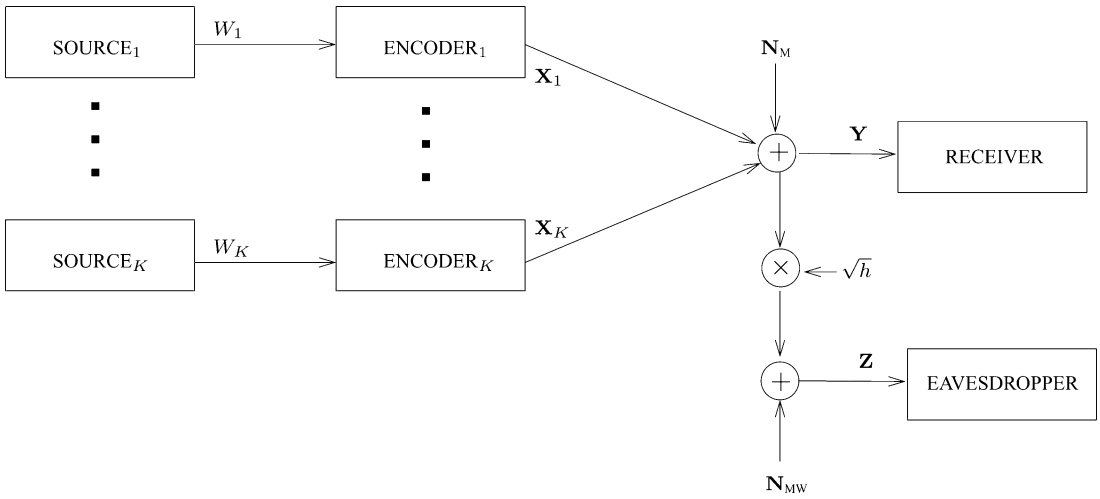

Fig. 1. Equivalent GMAC-WT System Model.

constraints are considered, the achievable region is the convex hull of the union of the superposition coding and TDMA regions.

Finally, a word on notation: Throughout the correspondence, we denote vectors with bold letters, as well as letters with superscripts as the length of the vector whenever necessary. Sets are denoted using a script font. Also, for random variables X, Y, we use $H(X)$ to refer to the entropy of X when it is discrete, $\mathsf{h}(X)$ to refer to the differential entropy when X is continuous, and $I(X;Y)$ to refer to the mutual information of X, Y. All the logarithms are taken to base 2, such that the resulting information theoretic quantities are in bits.

II. System Model and Problem Statement

We consider K users transmitting to a receiver in the presence of a wire-tapper in a Gaussian channel. The model under consideration is presented in Fig. 1. In general, transmitter $k \in \mathcal{K} \triangleq \{1, \ldots, K\}$ chooses a message W_k from a set of equally likely messages $\mathcal{W}_k = \{1, \ldots, M_k\}$. The messages are encoded using $(2^{nR_k}, n)$ codes, mapping 2^{nR_k} messages to codewords $\{\tilde{X}_k^n(W_j)\}$ of length n, 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 wire-tapper get $\tilde{\mathbf{Y}} = \tilde{Y}^n$ and $\tilde{\mathbf{Z}} = \tilde{Z}^n$, respectively. The receiver decodes $\tilde{\mathbf{Y}}$ to get an estimate of the transmitted messages, $\hat{\mathbf{W}}$. We assume that the eavesdropper is intelligent and informed, i.e., it has the same decoding capability and has access to the same information as the legitimate receiver, including all channel parameters. The transmitters would like to communicate with the receiver with arbitrarily low probability of error, while maintaining secrecy to a predetermined level δ. The specific secrecy constraints, $\Delta_{\mathcal{S}}$, will be defined in Section II-A. The signals at the intended receiver and the wiretapper are then given by

$$\tilde{\mathbf{Y}} = \sum_{k=1}^{K} \sqrt{h_k^{\mathrm{M}}}\tilde{\mathbf{X}}_k + \tilde{\mathbf{N}}_{\mathrm{M}} \tag{1a}$$

$$\tilde{\mathbf{Z}} = \sum_{k=1}^{K} \sqrt{h_k^{\mathrm{W}}}\tilde{\mathbf{X}}_k + \tilde{\mathbf{N}}_{\mathrm{W}} \tag{1b}$$

where h_k^{M} is the main channel power gain for user k, h_k^{W} is the eavesdropper channel power gain for user k, and $\tilde{\mathbf{N}}_{\mathrm{M}}, \tilde{\mathbf{N}}_{\mathrm{W}}$ are the additive white Gaussian noise (AWGN) at the intended receiver and eavesdropper, respectively. Each component of $\tilde{\mathbf{N}}_{\mathrm{M}} \sim \mathcal{N}(0, \sigma_{\mathrm{M}}^2)$ and $\tilde{\mathbf{N}}_{\mathrm{W}} \sim \mathcal{N}(0, \sigma_{\mathrm{W}}^2)$. The transmit power constraints are given by $\frac{1}{n}\sum_{i=1}^{n} \tilde{X}_{ki}^2 \le \tilde{P}_k, k = 1, \ldots, K$. Faithful to Wyner's terminology, we refer to this channel model as the Gaussian multiple-access wire-tap channel (GMAC-WT).

Similar to the scaling transformation to put an interference channel in standard form, [28], we can represent any GMAC-WT by an equivalent standard form [29]

$$\mathbf{Y} = \sum_{k=1}^{K} \mathbf{X}_k + \mathbf{N}_{\mathrm{M}} \tag{2a}$$

$$\mathbf{Z} = \sum_{k=1}^{K} \sqrt{h_k}\mathbf{X}_k + \mathbf{N}_{\mathrm{W}} \tag{2b}$$

where

- the codewords $\{\tilde{\mathbf{X}}_k\}$ are scaled to get $\mathbf{X}_k = \sqrt{\frac{h_k^M}{\sigma_{\mathrm{M}}^2}}\tilde{\mathbf{X}}_k$;
- the new power constraints are $\bar{P}_k = \frac{h_k^M}{\sigma_{\mathrm{M}}^2}\tilde{P}_k$;
- the new wiretapper channel gains are $h_k = \frac{h_k^W \sigma_{\mathrm{M}}^2}{h_k^M \sigma_{\mathrm{W}}^2}$;
- the AWGN are normalized by $\mathbf{N}_{\mathrm{M}} = \frac{\tilde{\mathbf{N}}_{\mathrm{M}}}{\sigma_{\mathrm{M}}}$ and $\mathbf{N}_{\mathrm{W}} = \frac{\tilde{\mathbf{N}}_{\mathrm{W}}}{\sigma_{\mathrm{W}}}$.

In this correspondence, we shall examine the case where the wire-tapper receives a *stochastically degraded* version of the signal received at the legitimate receiver, i.e., there exists a distribution $\tilde{p}(z|y)$ such that we can write $p(z|x_1, \ldots, x_K) = \int_{-\infty}^{\infty} p(y|x_1, \ldots, x_K)\tilde{p}(z|y)dy$. Similar to the broadcast channel, since the legitimate receiver and the eavesdropper do not cooperate, noise correlations do not play a role, and as a result, the capacity of the stochastically degraded wire-tap channel is the same as that of the *physically degraded* wire-tap channel, which means $p(y, z|x_1, \ldots, x_K) = p(y|x_1, \ldots, x_K)p(z|y)$. It can easily be shown that the wire-tapper gets a stochastically degraded version of the receiver's signal if $h_1 = \cdots = h_K \equiv h < 1$. Equivalently, we consider the physically degraded case, where the wire-tapper's received signal is a noisier version of the legitimate receiver's scaled received signal, $\mathbf{Z} = \sqrt{h}\mathbf{Y} + \mathbf{N}_{\mathrm{MW}}$, where $\mathbf{N}_{\mathrm{MW}}$ has each component $\sim \mathcal{N}(0, 1-h)$ and is independent of $\mathbf{Y}$. This model is illustrated in Fig. 1. In practical situations, we can think of this as the wire-tapper being outside of a controlled indoor environment, such as in [30] or just being able to wire-tap the receiver rather than receive the signals itself.

A. The Secrecy Measures

Letting $\Delta_{\mathcal{S}}$ be our secrecy constraint for any subset $\mathcal{S}$ of users, we require that $\Delta_{\mathcal{S}} \ge \delta$ for all sets $\mathcal{S} \subseteq \mathcal{K}$, with $\delta \in [0, 1]$ as 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. To that end, we define two sets of secrecy

constraints using the normalized equivocations for sets of users. These are:

1) Individual Secrecy: We define the individual secrecy measure for a subset of users, $\mathcal{S} \subseteq \mathcal{K}$, as

$$\Delta_{\mathcal{S}}^{I} \triangleq \frac{H(\mathbf{W}_{\mathcal{S}}|\mathbf{X}_{\mathcal{S}^c}, \mathbf{Z})}{H(\mathbf{W}_{\mathcal{S}})} \quad \forall \mathcal{S} \subseteq \mathcal{K} = \{1, \ldots, K\} \tag{3}$$

where $\mathbf{W}_{\mathcal{S}} = \{W_k\}_{k \in \mathcal{S}}$. $\Delta_{\mathcal{S}}^{\mathrm{I}}$ denotes the normalized entropy of the transmitted messages of a set $\mathcal{S}$ of users, given the received signal at the wire-tapper as well as the remaining users' transmitted symbols. As our secrecy criterion, this guarantees that the rate of information leaked to the wire-tapper from a group of users is limited even if all the other users' transmitted codewords are compromised. Note that this is a stronger constraint than $H(\mathbf{W}_{\mathcal{S}}|\mathbf{W}_{\mathcal{S}^c}, \mathbf{Z})$, as $H(\mathbf{W}_{\mathcal{S}}|\mathbf{W}_{\mathcal{S}^c}, \mathbf{Z}) \geq H(\mathbf{W}_{\mathcal{S}}|\mathbf{W}_{\mathcal{S}^c}, \mathbf{X}_{\mathcal{S}^c}, \mathbf{Z}) = H(\mathbf{W}_{\mathcal{S}}|\mathbf{X}_{\mathcal{S}^c}, \mathbf{Z})$. In addition, from a practical point of view, if the transmitted messages are compromised either due to byzantine users or some other side information allowing the eavesdropper to decode the transmitted messages of a group of users, there is no reason to expect that the transmitted codewords are not known to the eavesdropper. Thus, this represents a scenario where users do not have to trust each other.

We note that if the individual secrecy constraints for all users in the set $\mathcal{S}$ are satisfied, i.e., $\Delta_k \geq \delta$, $\forall k \in \mathcal{S}$, then the constraint for set $\mathcal{S}$ is also satisfied. To see this, without loss of generality, let $\mathcal{S} = 1, \ldots, S$ where $S \leq K$ and assume $\frac{H(W_k|\mathbf{X}_{k^c}, \mathbf{Z})}{H(W_k)} \geq \delta$. We can write

$$\begin{aligned}
H(\mathbf{W}_{\mathcal{S}}|\mathbf{X}_{\mathcal{S}^c}, \mathbf{Z}) &= \sum_{k=1}^{S} H(W_k|W^{k-1}, \mathbf{X}_{\mathcal{S}^c}, \mathbf{Z}) && (4)\\
&\geq \sum_{k=1}^{S} H(W_k|W^{k-1}, \mathbf{X}_{k^c}, \mathbf{Z}) && (5)\\
&= \sum_{k=1}^{S} H(W_k|\mathbf{X}_{k^c}, \mathbf{Z}) && (6)\\
&\geq \sum_{k=1}^{S} \delta H(W_k) && (7)\\
&= \delta H(\mathbf{W}_{\mathcal{S}}) && (8)
\end{aligned}$$

where (5) follows using conditioning, (6) is due to the fact that W_j is conditionally independent of all W_k given $\mathbf{X}_k, \mathbf{Z}$. Equation (7) comes from our assumption that for all $k \in \mathcal{S}, \Delta_k^{\mathrm{I}} \geq \delta$. Thus, for any subset of users the individual secrecy constraints for all users also guarantee the joint secrecy of the same level for the entire set.

2) Collective Secrecy: Clearly (3) is a conservative measure where users do not place any trust on each other. We now define a revised secrecy measure to take into account the multiaccess nature of the channel where users rely on others to achieve secrecy for the whole group.

$$\Delta_{\mathcal{S}}^{\mathrm{C}} \triangleq \frac{H(\mathbf{W}_{\mathcal{S}}|\mathbf{Z})}{H(\mathbf{W}_{\mathcal{S}})} \quad \forall \mathcal{S} \subseteq \mathcal{K}. \tag{9}$$

Using 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. We require the secrecy constraint to be satisfied separately for each $\mathcal{S} \subseteq \mathcal{K}$, since otherwise it is possible to have $\Delta_{\mathcal{S}}^{\mathrm{C}} \geq \delta$, but $\Delta_{\mathcal{J}}^{\mathrm{C}} < \delta$ for some $\mathcal{J} \subset \mathcal{S}$. However, if $\delta = 1$, i.e., when we require perfect secrecy, we can show that $\Delta_{\mathcal{K}}^{\mathrm{C}} \geq 1 - \epsilon \Rightarrow \Delta_{\mathcal{S}}^{\mathrm{C}} \geq 1 - \epsilon'$ for all $\mathcal{S} \subseteq \mathcal{K}$, where $\epsilon' \to 0$ as $\epsilon \to 0$. To see this, write

$$\begin{aligned}
&H(\mathbf{W}_{\mathcal{S}}|\mathbf{Z}) + H(\mathbf{W}_{\mathcal{S}^c})\\
&\quad \geq H(\mathbf{W}_{\mathcal{S}}|\mathbf{Z}) + H(\mathbf{W}_{\mathcal{S}^c}|\mathbf{W}_{\mathcal{S}}, \mathbf{Z}) && (10)\\
&\quad = H(\mathbf{W}_{\mathcal{K}}|\mathbf{Z}) && (11)\\
&\quad \geq (1 - \epsilon) H(\mathbf{W}_{\mathcal{K}}) && (12)\\
&\quad = (1 - \epsilon)[H(\mathbf{W}_{\mathcal{S}}) + H(\mathbf{W}_{\mathcal{S}^c})] && (13)
\end{aligned}$$

where (11) follows from the chain rule of entropy and (12) from the requirement for perfect secrecy. Comparing the left hand side of (10) and (13), since conditioning cannot increase entropy, we see that we have to have

$$\frac{H(\mathbf{W}_{\mathcal{S}}|\mathbf{Z})}{H(\mathbf{W}_{\mathcal{S}})} \geq 1 - \epsilon' \tag{14}$$

where $\epsilon' \triangleq (1 + \frac{H(\mathbf{W}_{\mathcal{S}^c})}{H(\mathbf{W}_{\mathcal{S}})})\epsilon \to 0$ as $\epsilon \to 0$. Thus, perfect secrecy for the ensemble of users guarantees perfect secrecy for all subsets of users.

B. The δ-Secret Achievable Rate Region

Definition 1 (Achievable Rates With δ-Secrecy): Let $\xi = I$ if using individual constraints, and $\xi = C$ if using collective constraints. The K-tuple rate vector $\mathbf{R} = (R_1, \ldots, R_K)$ is said to be *achievable with δ-secrecy* under constraint ξ, if for any given $\epsilon > 0$ there exists a code of sufficient length n such that

$$\begin{aligned}
\frac{1}{n} \log_2 M_k &\geq R_k - \epsilon, \qquad k = 1, \ldots, K && (15)\\
P_e &\leq \epsilon && (16)\\
\Delta_{\mathcal{S}}^{\xi} &\geq \delta, \qquad \forall \mathcal{S} \subseteq \mathcal{K} && (17)
\end{aligned}$$

where user k chooses one of M_k symbols to transmit according to the uniform distribution, $\Delta_{\mathcal{S}}^{\xi}$ denotes the secrecy constraint, and is given by (3) if $\xi = I$, and by (9) if $\xi = C$. We will call the set of all achievable rates with δ-secrecy, the *δ-secret achievable rate region*, and denote it $\mathcal{C}^{\xi}(\delta)$.

C. Some Preliminary Definitions

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

$$\begin{aligned}
P_{\mathcal{S}} &\triangleq \sum_{k \in \mathcal{S}} \bar{P}_k && (18)\\
R_{\mathcal{S}} &\triangleq \sum_{k \in \mathcal{S}} R_k && (19)\\
C_{\mathcal{S}}^{\mathrm{M}} &\triangleq \frac{1}{2} \log(1 + P_{\mathcal{S}}) && (20)\\
C_{\mathcal{S}}^{\mathrm{W}} &\triangleq \frac{1}{2} \log(1 + hP_{\mathcal{S}}) && (21)\\
\tilde{C}_{\mathcal{S}}^{\mathrm{W}} &\triangleq \frac{1}{2} \log\left(1 + \frac{hP_{\mathcal{S}}}{1 + hP_{\mathcal{S}^c}}\right). && (22)
\end{aligned}$$

Alternately, we also use the subscript *sum* when $\mathcal{S} = \mathcal{K}$. We also define $[\cdot]^+ \triangleq \max\{0, \cdot\}$.

III. Achievable δ-Secrecy Rate Regions

In this section, we find a set of achievable rates using Gaussian codebooks, which we denote by $\mathcal{G}(\delta)$. We first give the achievable regions satisfying the individual and collective secrecy constraints, denoted by $\mathcal{G}^{\mathrm{I}}(\delta)$ and $\mathcal{G}^{\mathrm{C}}(\delta)$ respectively, using superposition coding. We then give the region when TDMA is used, denoted $\mathcal{G}^{\mathrm{T}}(\delta)$, and satisfies both secrecy constraints. For the collective secrecy constraints, the TDMA region is seen to be smaller than the superposition coding region. For the individual constraints, the achievable region is the convex hull of the union of the superposition and TDMA regions, denoted $\mathcal{G}_{\cup}^{\mathrm{I}}(\delta)$.

A. Individual Secrecy

In [4], it has been shown that Gaussian codebooks can be used to maintain secrecy for the single user Gaussian wire-tap channel. Using

a similar approach, we present an achievable region for δ-secrecy using individual secrecy constraints in Theorem 1.

Theorem 1: The following region is achievable with δ-secrecy for the GMAC-WT using Gaussian codebooks.

$$\mathcal{G}^{\mathrm{I}}(\delta)=\left\{\mathbf{R}: R_{\mathcal{S}} \leq \min\left\{C_{\mathcal{S}}^{\mathrm{M}}, \frac{1}{\delta}\left[C_{\mathcal{S}}^{\mathrm{M}}-\sum_{k\in\mathcal{S}} C_k^{\mathrm{W}}\right]^+\right\} \forall \mathcal{S}\subseteq\mathcal{K}\right\}. \tag{23}$$

Proof: **Coding Scheme**: Let $\mathbf{R}=(R_1,\ldots,R_K)$ satisfy (23). For each user $k\in\mathcal{K}$, consider the scheme:

1) Let $M_k=2^{\mathrm{n}(R_k-\epsilon')}$ where $0\leq\epsilon'<\epsilon$. Let $M_k=M_{ks}M_{k0}$ where, for some $1\geq\mu_k\geq\delta$ to be chosen later, $M_{ks}=M_k^{\mu_k}$, $M_{k0}=M_k^{1-\mu_k}$. We then have $R_k=R_{ks}+R_{k0}+\epsilon'$, 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 from $\mathcal{N}(0,\lambda_{ks}\bar{P}_k-\varepsilon)$. Codebook $\mathfrak{X}_{k0}$ has M_{k0} codewords with each component drawn from $\mathcal{N}(0,\lambda_{k0}\bar{P}_k-\varepsilon)$ and $\mathfrak{X}_{kx}$ has M_{kx} codewords with each component drawn from $\mathcal{N}(0,\lambda_{kx}\bar{P}_k-\varepsilon)$. Here, ε is an arbitrarily small number to ensure that the power constraints are satisfied with high probability, and $\lambda_{ks}+\lambda_{k0}+\lambda_{kx}=1$. Define $R_{kx}=\frac{1}{n}\log M_{kx}$ and $M_{kt}=M_kM_{kx}$.
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 $\mathbf{W}_k$ from $\mathfrak{X}_{ks}$ and $\mathfrak{X}_{k0}$, 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 $R_{kt}=\frac{1}{n}\log M_{kt}+\epsilon'=R_{ks}+R_{k0}+R_{kx}+\epsilon'$.

Specifically, the rates are chosen to satisfy $\forall\mathcal{S}\subseteq\mathcal{K}$:

$$\sum_{k\in\mathcal{S}} R_{ks}=\sum_{k\in\mathcal{S}}\mu_kR_k\leq\left[C_{\mathcal{S}}^{\mathrm{M}}-\sum_{k\in\mathcal{S}}C_k^{\mathrm{W}}\right]^+ \tag{24}$$

$$R_{k0}+R_{kx}=(1-\mu_k)R_k+R_{kx}=C_k^{\mathrm{W}},\quad \forall k\in\mathcal{S} \tag{25}$$

$$\sum_{k\in\mathcal{S}} R_{kt}=\sum_{k\in\mathcal{S}}[R_k+R_{kx}]\leq C_{\mathcal{S}}^{\mathrm{M}} \tag{26}$$

Consider the sucode $\{\mathfrak{X}_{ks}\}_{k=1}^K$. 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 $\tilde{\Delta}_k^{\mathrm{i}}=\frac{H(W_{ks}|\mathbf{X}_{k^c},\mathbf{Z})}{H(W_{ks})}$ and write:

$$\begin{aligned}
&H(W_{ks}|\mathbf{X}_{k^c},\mathbf{Z})\\
&\quad=H(W_{ks}|\mathbf{X}_{k^c})-I(W_{ks};\mathbf{Z}|\mathbf{X}_{k^c}) &(27)\\
&\quad=H(W_{ks})-I(W_{ks};\mathbf{Z}|\mathbf{X}_{k^c}) &(28)\\
&\quad=H(W_{ks})-I(W_{ks};\mathbf{Z}|\mathbf{X}_{k^c})+I(W_{ks};\mathbf{Z}|\mathbf{X}_{\mathcal{K}}) &(29)\\
&\quad=H(W_{ks})-\mathsf{h}(\mathbf{Z}|\mathbf{X}_{k^c})+\mathsf{h}(\mathbf{Z}|W_{ks},\mathbf{X}_{k^c})\\
&\qquad+\mathsf{h}(\mathbf{Z}|\mathbf{X}_{\mathcal{K}})-\mathsf{h}(\mathbf{Z}|\mathbf{X}_{\mathcal{K}},W_{ks}) &(30)\\
&\quad=H(W_{ks})-I(\mathbf{X}_k;\mathbf{Z}|\mathbf{X}_{k^c})+I(\mathbf{X}_k;\mathbf{Z}|W_{ks},\mathbf{X}_{k^c}) &(31)
\end{aligned}$$

where (28) follows from the fact that the secret message of user k is independent of the codewords of the remaining users, and (29) follows since the received signal at the eavesdropper is independent of the transmitted secret messages given the actual transmitted codewords. Thus, we have

$$\tilde{\Delta}_k^{\mathrm{i}}=\frac{H(W_{ks}|\mathbf{X}_{k^c},\mathbf{Z})}{H(W_{ks})} \tag{32}$$

$$=1-\frac{I(\mathbf{X}_k;\mathbf{Z}|\mathbf{X}_{k^c})-I(\mathbf{X}_k;\mathbf{Z}|W_{ks},\mathbf{X}_{k^c})}{H(W_{ks})} \tag{33}$$

By the converse to the coding theorem for the Gaussian Multiple Access Channel, we have $I(\mathbf{X}_k;\mathbf{Z}|\mathbf{X}_{k^c})\leq nC_k^{\mathrm{W}}$. We can also write

$$I(\mathbf{X}_k;\mathbf{Z}|W_{ks},\mathbf{X}_{k^c})=H(\mathbf{X}_k|W_{ks},\mathbf{X}_{k^c})-H(\mathbf{X}_k|W_{ks},\mathbf{X}_{k^c},\mathbf{Z}) \tag{34}$$

For each secret message of user k, our coding scheme implies that it sends one of $M_{k0}M_{kx}$ possible codewords. By choosing R_{k0}, R_{kx} to satisfy (25), we guarantee that

$$H(\mathbf{X}_k|W_{ks},\mathbf{X}_{k^c})=H(\mathbf{X}_k|W_{ks})=nC_k^{\mathrm{W}} \tag{35}$$

Also

$$H(\mathbf{X}_k|W_{ks},\mathbf{X}_{k^c},\mathbf{Z})\leq n\delta_n \tag{36}$$

where $\delta_n\to 0$ due to Fano's Inequality. This stems from the fact that given W_{ks}, the sucode for user k is, with high probability, a "good" code for the wiretapper. Combining these in (33), we can write

$$\tilde{\Delta}_k^{\mathrm{i}}\geq 1-\frac{nC_k^{\mathrm{W}}-nC_k^{\mathrm{W}}+n\delta_n}{H(W_{ks})}=1-\epsilon \tag{37}$$

where $\epsilon=\frac{\delta_n}{R_{ks}}\to 0$ as $n\to\infty$. Then, we can write

$$\begin{aligned}
\Delta_k^{\mathrm{I}}&=\frac{H(W_k|\mathbf{X}_{k^c},\mathbf{Z})}{H(W_k)} &(38)\\
&\geq\frac{H(W_{ks}|\mathbf{X}_{k^c},\mathbf{Z})}{H(W_k)} &(39)\\
&\geq\frac{(1-\epsilon)H(W_{ks})}{H(W_k)} &(40)\\
&\geq\frac{(1-\epsilon)\mu_kR_k}{R_k} &(41)\\
&\geq\delta &(42)
\end{aligned}$$

Since (42) holds for all $k=1,\ldots,K$, from (8) we have $\Delta_{\mathcal{S}}^{\mathrm{I}}\geq\delta,\forall\mathcal{S}\subseteq\mathcal{K}$. □

Remark 1: Consistent with the characterization in [5], we can express the achievable rates as

$$R_{\mathcal{S}}\leq C_{\mathcal{S}}^{\mathrm{M}} \tag{43}$$

$$\delta R_{\mathcal{S}}\leq\left[C_{\mathcal{S}}^{\mathrm{M}}-\sum_{k\in\mathcal{S}}C_k^{\mathrm{W}}\right]^+ \tag{44}$$

where for any $\mathcal{S}$, (43) corresponds to the total transmission rate, and (44) corresponds to the portion of this rate that is transmitted in secrecy.

Remark 2: The achievable δ-secrecy sum-rate is given by

$$R_{\mathrm{sum}}^{\mathrm{I}}(\delta)=\min\left\{C_{\mathcal{K}}^{\mathrm{M}},\frac{1}{\delta}\left[C_{\mathcal{K}}^{\mathrm{M}}-\sum_{k=1}^K C_k^{\mathrm{W}}\right]^+\right\} \tag{45}$$

Observe that there is a reduction of $\sum_{k=1}^K C_k^{\mathrm{W}}\geq C_{\mathcal{K}}^{\mathrm{W}}$ in the δ-secrecy sum-rate due to secrecy constraints when the second term is the

minimum. Also observe that the transmission of all the users with their maximum power may not be optimal for this case.

B. Collective Secrecy

Theorem 2: We can transmit with δ-secrecy using Gaussian codebooks at rates in the region $\mathcal{G}^{\mathrm{C}}(\delta)$ defined as

$$\mathcal{G}^{\mathrm{C}}(\delta) \triangleq \left\{ \mathbf{R} : R_{\mathcal{S}} \leq \min \left\{ C^{\mathrm{M}}_{\mathcal{S}}, \frac{1}{\delta}\left[C^{\mathrm{M}}_{\mathcal{S}} - \tilde{C}^{\mathrm{W}}_{\mathcal{S}} \right] \right\} \quad \forall \mathcal{S} \subseteq \mathcal{K} \right\} \tag{46}$$

Proof: Let $\mathbf{R} = (R_1, \ldots, R_K)$ satisfy (46) and assume the coding scheme is the same as described in the individual constraints case, except that instead of (24)–(26), we will choose the rates such that for all $\mathcal{S} \subseteq \mathcal{K}$

$$\sum_{k \in \mathcal{S}} R_{ks} = \sum_{k \in \mathcal{S}} \mu_k R_k \leq C^{\mathrm{M}}_{\mathcal{S}} - \tilde{C}^{\mathrm{W}}_{\mathcal{S}} \tag{47}$$

$$\sum_{k=1}^{K} [R_{k0} + R_{kx}] = \sum_{k=1}^{K} [(1-\mu_k)R_k + R_{kx}] = C^{\mathrm{W}}_{\mathcal{K}} \tag{48}$$

$$\sum_{k \in \mathcal{S}} R_{kt} = \sum_{k \in \mathcal{S}} [R_k + R_{kx}] \leq C^{\mathrm{M}}_{\mathcal{S}}. \tag{49}$$

From (49) and the GMAC coding theorem, with high probability the receiver can decode the codewords with low probability of error. To show $\Delta^{\mathrm{C}}_{\mathcal{S}} \geq \delta, \forall \mathcal{S} \subseteq \mathcal{K}$, we concern ourselves only with MAC subcode $\{\mathfrak{X}_{ks}\}_{k=1}^{K}$. 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 $\mathbf{W}^s_{\mathcal{S}} = \{W_{ks}\}_{k \in \mathcal{S}}$ and $\tilde{\Delta}^{\mathrm{c}}_{\mathcal{S}} = \frac{H(\mathbf{W}^s_{\mathcal{S}}|\mathbf{Z})}{H(\mathbf{W}^s_{\mathcal{S}})}$ and define $\mathbf{X}_{\Sigma} = \sum_{k=1}^{K} \mathbf{X}_k$. For $\mathcal{K}$ write

$$\begin{aligned} H(\mathbf{W}^s_{\mathcal{K}} \mid \mathbf{Z}) &= H(\mathbf{W}^s_{\mathcal{K}}) - I(\mathbf{W}^s_{\mathcal{K}}; \mathbf{Z}) && (50)\\ &= H(\mathbf{W}^s_{\mathcal{K}}) - I(\mathbf{W}^s_{\mathcal{K}}; \mathbf{Z}) + I(\mathbf{W}^s_{\mathcal{K}}; \mathbf{Z}|\mathbf{X}_{\Sigma}) && (51)\\ &= H(\mathbf{W}^s_{\mathcal{K}}) - \mathsf{h}(\mathbf{Z}) + \mathsf{h}(\mathbf{Z}|\mathbf{W}^s_{\mathcal{K}}) \\ &\quad + \mathsf{h}(\mathbf{Z}|\mathbf{X}_{\Sigma}) - \mathsf{h}(\mathbf{Z}|\mathbf{W}^s_{\mathcal{K}}, \mathbf{X}_{\Sigma}) && (52)\\ &= H(\mathbf{W}^s_{\mathcal{K}}) - I(\mathbf{X}_{\Sigma}; \mathbf{Z}) + I(\mathbf{X}_{\Sigma}; \mathbf{Z}|\mathbf{W}^s_{\mathcal{K}}) && (53) \end{aligned}$$

where (51) follows from $\mathbf{W}^s_{\mathcal{K}} \rightarrow \mathbf{X}_{\Sigma} \rightarrow \mathbf{Z}$. Therefore, we have

$$\begin{aligned} \tilde{\Delta}^{\mathrm{c}}_{\mathcal{K}} &= \frac{H(\mathbf{W}^s_{\mathcal{K}}|\mathbf{Z})}{H(\mathbf{W}^s_{\mathcal{K}})} \\ &= 1 - \frac{I(\mathbf{X}_{\Sigma}; \mathbf{Z}) - I(\mathbf{X}_{\Sigma}; \mathbf{Z}|\mathbf{W}^s_{\mathcal{K}})}{H(\mathbf{W}^s_{\mathcal{K}})} \end{aligned} \tag{54}$$

Consider the two terms individually. First, we have the sum-rate bound of the multiple-access channel to the eavesdropper

$$I(\mathbf{X}_{\Sigma}; \mathbf{Z}) \leq n C^{\mathrm{W}}_{\mathcal{K}}. \tag{55}$$

$I(\mathbf{X}_{\Sigma}; \mathbf{Z}|\mathbf{W}^s_{\mathcal{K}}) = H(\mathbf{X}_{\Sigma}|\mathbf{W}^s_{\mathcal{K}}) - H(\mathbf{X}_{\Sigma}|\mathbf{W}^s_{\mathcal{K}}, \mathbf{Z})$. Since user k sends one of $M_{k0}M_{kx}$ codewords for each message, from (48) we have

$$\begin{aligned} H(\mathbf{X}_{\Sigma}|\mathbf{W}^s_{\mathcal{K}}) &= \log \left(\prod_{k=1}^{K} M_{k0} M_{kx} \right) && (56)\\ &= n C^{\mathrm{W}}_{\mathcal{K}}. && (57) \end{aligned}$$

We can also write

$$H(\mathbf{X}_{\Sigma}|\mathbf{W}^s_{\mathcal{K}}, \mathbf{Z}) \leq n\eta'_n \tag{58}$$

where $\eta'_n \rightarrow 0$ as $n \rightarrow \infty$ since, with high probability, the eavesdropper can decode $\mathbf{X}_{\Sigma}$ given $\mathbf{W}^s_{\mathcal{K}}$ due to (48). Using (47), (48), (55), (57) and (58) in (54), we get

$$\tilde{\Delta}^{\mathrm{c}}_{\mathcal{K}} \geq 1 - \frac{C^{\mathrm{W}}_{\mathcal{K}} - C^{\mathrm{W}}_{\mathcal{K}} + \eta'_n}{C^{\mathrm{M}}_{\mathcal{K}} - C^{\mathrm{W}}_{\mathcal{K}}} \rightarrow 1 \text{ as } \eta'_n \rightarrow 0 \tag{59}$$

The proof is completed by noting that due to (14), $\tilde{\Delta}^{\mathrm{c}}_{\mathcal{K}} = 1$ implies $\tilde{\Delta}^{\mathrm{c}}_{\mathcal{S}} = 1$, $\forall \mathcal{S} \subseteq \mathcal{K}$, and writing

$$\Delta^{\mathrm{c}}_{\mathcal{S}} \geq \frac{H(\mathbf{W}^s_{\mathcal{S}}|\mathbf{Z})}{H(\mathbf{W}_{\mathcal{S}})} = \frac{H(\mathbf{W}^s_{\mathcal{S}})}{H(\mathbf{W}_{\mathcal{S}})} = \frac{\sum_{k \in \mathcal{S}} \mu_k R_k}{\sum_{k \in \mathcal{S}} R_k} \geq \delta. \tag{60}$$

□

Remark 3: We note that Theorem 2 can be written as

$$R_{\mathcal{S}} \leq C^{\mathrm{M}}_{\mathcal{S}} \tag{61}$$

$$\delta R_{\mathcal{S}} \leq C^{\mathrm{M}}_{\mathcal{S}} - C^{\mathrm{W}}_{\mathcal{S}} \tag{62}$$

where (61) gives the rate of transmission, and (62) corresponds to the rate with perfect secrecy.

We note that this way the achievable δ-secrecy sum-rate is

$$R^{\mathrm{C}}_{\mathrm{sum}}(\delta) = \min \left\{ C^{\mathrm{M}}_{\mathcal{K}}, \frac{1}{\delta}\left[C^{\mathrm{M}}_{\mathcal{K}} - C^{\mathrm{W}}_{\mathcal{K}} \right] \right\}. \tag{63}$$

C. Time-Division

We can also use TDMA to get an achievable region. Since, in such a scheme, only one user is transmitting at a given time, both sets of constraints collapse down to a set of single-user secrecy constraints, for which the results were given in [4].

Theorem 3: 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 $\bar{P}_k/\alpha_k$ using the scheme described in [4]. The set of all rates achievable by this scheme will be denoted $\mathcal{G}^{\mathrm{T}}(\delta)$, and are given by (64)

$$\mathcal{G}^{\mathrm{T}}(\delta) \triangleq \bigcup_{\substack{\mathbf{0} \preceq \boldsymbol{\alpha} \preceq \mathbf{1} \\ \sum_{k=1}^{K} \alpha_k = 1}} \left\{ \mathbf{R} : R_k \leq \min \left\{ \frac{\alpha_k}{2} \log \left(1 + \frac{\bar{P}_k}{\alpha_k} \right), \frac{\alpha_k}{2\delta} \log \left(\frac{\alpha_k + \bar{P}_k}{\alpha_k + h\bar{P}_k} \right) \right\}, \ k = 1, \ldots, K \right\}. \tag{64}$$

Proof: Follows directly from [4, Th. 1]. □

Note that with this scheme, the achievable δ-secrecy sum-rate is given by

$$R^{\mathrm{T}}_{\mathrm{sum}}(\delta, \boldsymbol{\alpha}) = \sum_{k=1}^{K} \min \left\{ \frac{\alpha_k}{2} \log \left(1 + \frac{\bar{P}_k}{\alpha_k} \right), \frac{\alpha_k}{2\delta} \log \left(\frac{\alpha_k + \bar{P}_k}{\alpha_k + h\bar{P}_k} \right) \right\}. \tag{65}$$

Theorem 4: The above described TDMA scheme achieves a maximum sum-rate of

$$R^{\mathrm{T}}_{\mathrm{sum}}(\delta) = \min \left\{ C^{\mathrm{M}}_{\mathcal{K}}, \frac{1}{\delta}\left[C^{\mathrm{M}}_{\mathcal{K}} - C^{\mathrm{W}}_{\mathcal{K}} \right] \right\} \tag{66}$$

using the optimum time-sharing parameters

$$\alpha^*_k = \frac{\bar{P}_k}{\sum_{j=1}^{K} \bar{P}_j} \tag{67}$$

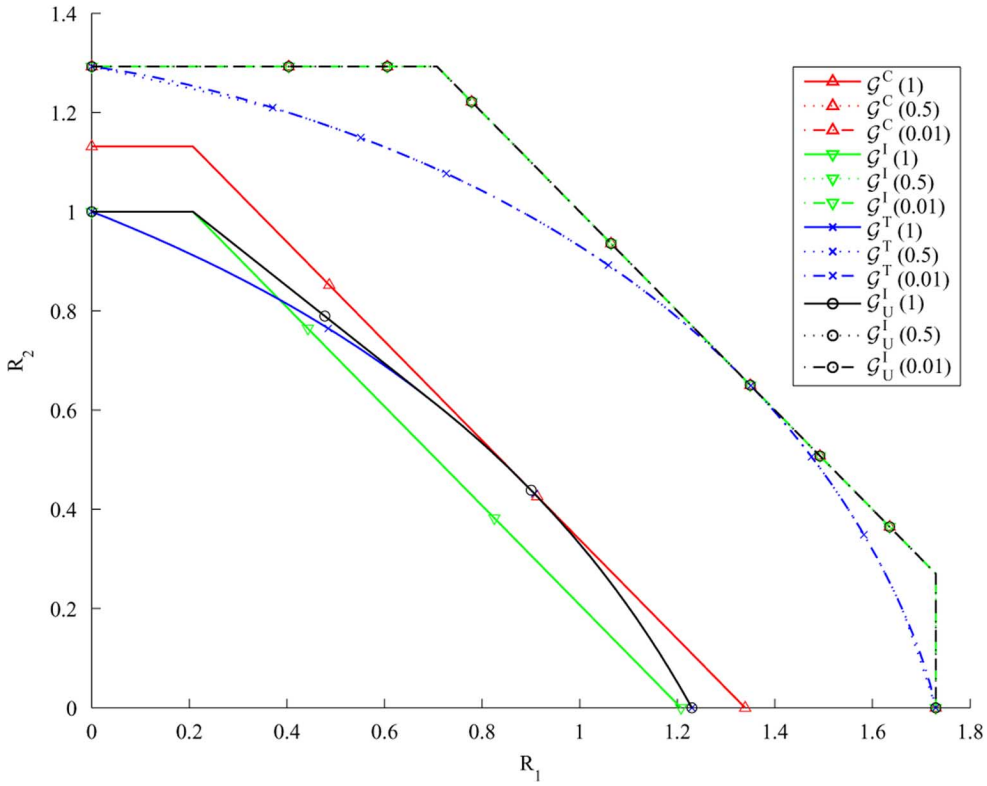

Fig. 2. Achievable rate regions $\mathcal{G}(\delta)$ for $\delta = \{0.01, 0.5, 1\}$. $\bar{P}_1 = 10, \bar{P}_2 = 5$ and $h = 0.1$.

Proof: Maximizing each term in (65) over the time-sharing parameters $\{\alpha_k\}$, is a convex optimization problem over α_k. Taking the derivative of the Lagrangian with respect to α_k and equating it to zero gives (67), which simultaneously minimizes both terms in the minimum. Using this in (65) yields (66). □

Since in this scheme only one user is transmitting at any given time, both individual and collective constraints are satisfied. We see that for collective secrecy constraints, this region is a subset of $\mathcal{G}^{\mathrm{C}}(\delta)$, which was given in (46). For individual secrecy constraints, however, $\mathcal{G}^{\mathrm{T}}(\delta)$ is not necessarily included in $\mathcal{G}^{\mathrm{I}}(\delta)$, which was given in (23). We can then, using time-sharing arguments, find a new achievable region for individual constraints that is the convex-closure of the union of the two regions.

Theorem 5: The following region is achievable for individual secrecy constraints:

$$\mathcal{G}^{\mathrm{I}}_{\mathrm{U}}(\delta) = \text{convex closure of } (\mathcal{G}^{\mathrm{I}}(\delta) \cup \mathcal{G}^{\mathrm{T}}(\delta)). \tag{68}$$

IV. δ-Secrecy Sum Capacity

In this section, we present an upper bound on the δ-secrecy sum-rate, denoted $C_{\mathrm{sum}}(\delta)$, for both individual and collective constraints, and show that this bound matches the δ-secrecy sum-rate achievable under both constraints, giving us the secrecy sum-capacity of GMAC-WT for individual and collective constraints. We note that a sum-rate constraint on both individual and collective constraints can be obtained using the constraints for the set $\mathcal{K}$. In this case, both sets of constraints collapse down to

$$\Delta_{\mathcal{K}} \triangleq \frac{H(\mathbf{W}_{\mathcal{K}}|\mathbf{Z})}{H(\mathbf{W}_{\mathcal{K}})} \geq \delta. \tag{69}$$

Theorem 6: For the GMAC-WT, the δ-secrecy sum-capacity for both individual and collective secrecy constraints is given by

$$C_{\mathrm{sum}}(\delta) = \min\left\{C^{\mathrm{M}}_{\mathcal{K}}, \frac{1}{\delta}\left[C^{\mathrm{M}}_{\mathcal{K}} - C^{\mathrm{W}}_{\mathcal{K}}\right]\right\}. \tag{70}$$

Proof: We first show that the right-hand side of (70) is an upper bound on the δ-secrecy sum-rate for both constraints. Observe that (70) is equal to the secrecy sum-rate achievable in (63) for collective constraints using superposition coding, and by TDMA in (66), which satisfies both collective and individual constraints. Hence, we get the δ-secrecy sum-capacity of the GMAC-WT for both individual and collective constraints.

The first term in the minimum of (70) is due to the converse for the GMAC, since the intended receiver needs to be able to decode the transmitted messages. To see the second term, assume $\delta > 0$. This is without loss of generality, since if $\delta = 0$, we have no secrecy constraint and only the first term applies. We first note that from Fano's inequality, we have

$$H(\mathbf{W}_{\mathcal{K}} \mid \mathbf{Y}, \mathbf{Z}) \leq H(\mathbf{W}_{\mathcal{K}} \mid \mathbf{Y}) \leq n\eta_n \tag{71}$$

where $\eta_n \to 0$ as $n \to \infty$. We then use the constraint in (69) to get

$$\begin{aligned} R_{\mathcal{K}} &= \frac{1}{n}H(\mathbf{W}_{\mathcal{K}}) && (72)\\ &\leq \frac{1}{n\delta}H(\mathbf{W}_{\mathcal{K}}|\mathbf{Z}) && (73)\\ &\leq \frac{1}{n\delta}[H(\mathbf{W}_{\mathcal{K}}|\mathbf{Z}) + n\eta_n - H(\mathbf{W}_{\mathcal{K}}|\mathbf{Y}, \mathbf{Z})] && (74)\\ &= \frac{1}{n\delta}I(\mathbf{W}_{\mathcal{K}}; \mathbf{Y} \mid \mathbf{Z}) + \eta'_n && (75)\\ &\leq \frac{1}{n\delta}I(\mathbf{X}_{\mathcal{K}}; \mathbf{Y} \mid \mathbf{Z}) + \eta'_n && (76) \end{aligned}$$

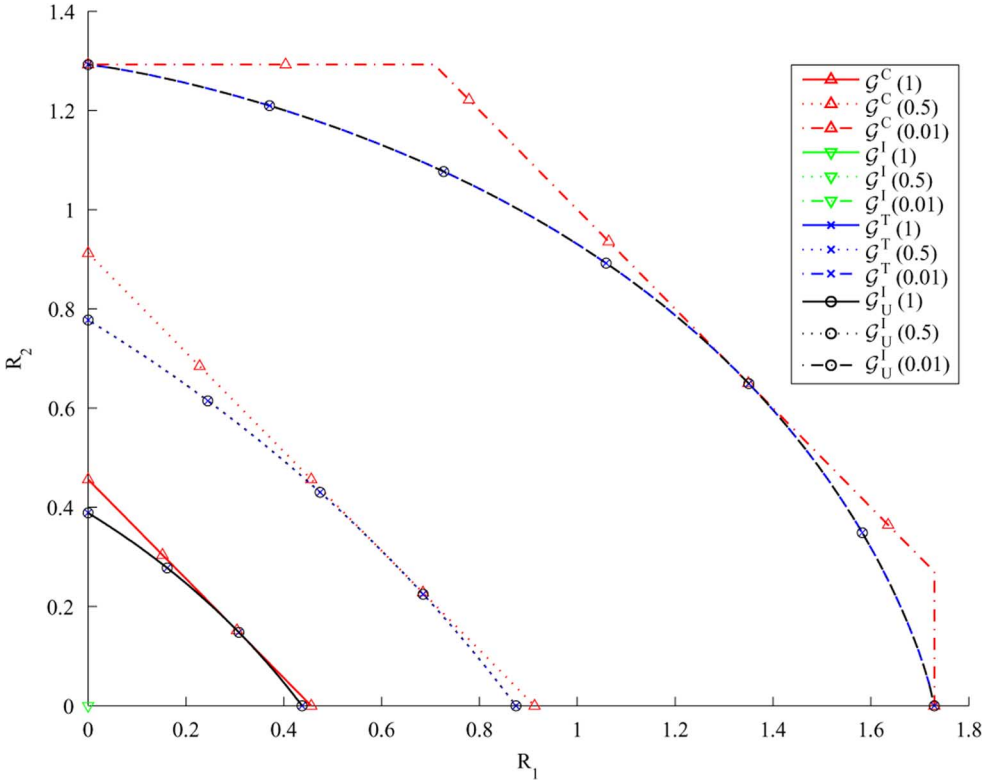

Fig. 3. Achievable rate regions $\mathcal{G}(\delta)$ for $\delta = \{0.01, 0.5, 1\}$. $\bar{P}_1 = 10, \bar{P}_2 = 5$ and $h = 0.5$.

where we used (71) in (74), and $\mathbf{W}_{\mathcal{K}} \rightarrow \mathbf{X}_{\mathcal{K}} \rightarrow \mathbf{Y} \rightarrow \mathbf{Z}$ in the last step. We now adopt [4, Lemma 10] to upper bound the differences between the received signal entropies at the receiver and wire-tapper.

Lemma 7 ([4, Lemma 10]): Let $\xi = \frac{1}{n}\mathsf{h}(\mathbf{Y})$ where $\mathbf{Y}, \mathbf{Z}$ are as given in (2). Then

$$\mathsf{h}(\mathbf{Y}) - \mathsf{h}(\mathbf{Z}) \leq n\xi - n\phi(\xi) \tag{77}$$

where

$$\phi(\xi)\frac{1}{2}\log\left[2\pi e\left(1 - h + \frac{h2^{2\xi}}{2\pi e}\right)\right]. \tag{78}$$

Proof: The proof follows using the entropy power inequality [31]. Recall that we can write $\mathsf{h}(\mathbf{Z}) = \mathsf{h}(\sqrt{h}\mathbf{Y} + \mathbf{N}_{\mathrm{MW}})$. Then, using the entropy power inequality, we have

$$\begin{aligned} 2^{\frac{2}{n}\mathsf{h}(\mathbf{Z})} &= 2^{\frac{2}{n}\mathsf{h}(\sqrt{h}\mathbf{Y}+\mathbf{N}_{\mathrm{MW}})} \\ &\geq 2^{\frac{2}{n}[\mathsf{h}(\mathbf{Y})+n\log\sqrt{h}]} + 2^{\frac{2}{n}\mathsf{h}(\mathbf{N}_{\mathrm{MW}})}. \end{aligned} \tag{79}$$

Now $\mathsf{h}(\mathbf{Y}) = n\xi$ and $\mathsf{h}(\mathbf{N}_{\mathrm{MW}}) = \frac{n}{2}\log[2\pi e(1-h)]$. Hence

$$2^{\frac{2}{n}\mathsf{h}(\mathbf{Z})} \geq h2^{2\xi} + 2\pi e(1-h) \tag{80}$$

which, after taking the log, gives

$$\begin{aligned} \mathsf{h}(\mathbf{Z}) &\geq \frac{n}{2}\log[h2^{2\xi} + 2\pi e(1-h)] && (81) \\ &= \frac{n}{2}\log\left[2\pi e\left(1 - h + \frac{h2^{2\xi}}{2\pi e}\right)\right] && (82) \end{aligned}$$

subtracting from $\mathsf{h}(\mathbf{Y}) = n\xi$ completes the proof of the lemma. □

Corollary 7.1:

$$\mathsf{h}(\mathbf{Y}) - \mathsf{h}(\mathbf{Z}) \leq n\left[C^{\mathrm{M}}_{\mathcal{K}} - C^{\mathrm{W}}_{\mathcal{K}}\right]. \tag{83}$$

Proof: From the converse to the GMAC coding theorem, we can show that

$$\mathsf{h}(\mathbf{Y}) \leq \frac{n}{2}\log(2\pi e(1+P_{\mathcal{K}})). \tag{84}$$

Let $\mathsf{h}(\mathbf{Y}) = n\xi$. Then, $\xi \leq \frac{1}{2}\log(2\pi e(1+P_{\mathcal{K}}))$, and since $\phi(\xi)$ is a nonincreasing function of ξ, we get $\phi(\xi) \geq \phi(\frac{1}{2}\log(2\pi e(1+P_{\mathcal{K}})))$. Thus

$$\begin{aligned} &\mathsf{h}(\mathbf{Y}) - \mathsf{h}(\mathbf{Z}) \\ &\quad\leq \frac{n}{2}\log(2\pi e(1+P_{\mathcal{K}})) \\ &\qquad - \frac{n}{2}\log[2\pi e(1-h+h(1+P_{\mathcal{K}}))] && (85) \\ &\quad= n\left[C^{\mathrm{M}}_{\mathcal{K}} - C^{\mathrm{W}}_{\mathcal{K}}\right]. && (86) \end{aligned}$$

Now, we can use (76) to write

$$\begin{aligned} &I(\mathbf{X}_{\mathcal{K}}; \mathbf{Y} \,|\, \mathbf{Z}) \\ &\quad= I(\mathbf{X}_{\mathcal{K}}; \mathbf{Y}, \mathbf{Z}) - I(\mathbf{X}_{\mathcal{K}}; \mathbf{Z}) && (87) \\ &\quad= I(\mathbf{X}_{\mathcal{K}}; \mathbf{Y}) + I(\mathbf{X}_{\mathcal{K}}; \mathbf{Z}|\mathbf{Y}) - I(\mathbf{X}_{\mathcal{K}}; \mathbf{Z}) && (88) \\ &\quad= I(\mathbf{X}_{\mathcal{K}}; \mathbf{Y}) - I(\mathbf{X}_{\mathcal{K}}; \mathbf{Z}) && (89) \\ &\quad= \mathsf{h}(\mathbf{Y}) - \mathsf{h}(\mathbf{Y}|\mathbf{X}_{\mathcal{K}}) - \mathsf{h}(\mathbf{Z}) + \mathsf{h}(\mathbf{Z}|\mathbf{X}_{\mathcal{K}}) && (90) \\ &\quad= \sum_{i=1}^{n}[\mathsf{h}(Z_i|\mathbf{X}_{\mathcal{K},i}) - \mathsf{h}(Y_i|\mathbf{X}_{\mathcal{K},i})] \\ &\qquad + [\mathsf{h}(\mathbf{Y}) - \mathsf{h}(\mathbf{Z})] && (91) \\ &\quad= \left[\frac{n}{2}\log(2\pi e) - \frac{n}{2}\log(2\pi e)\right] \end{aligned}$$

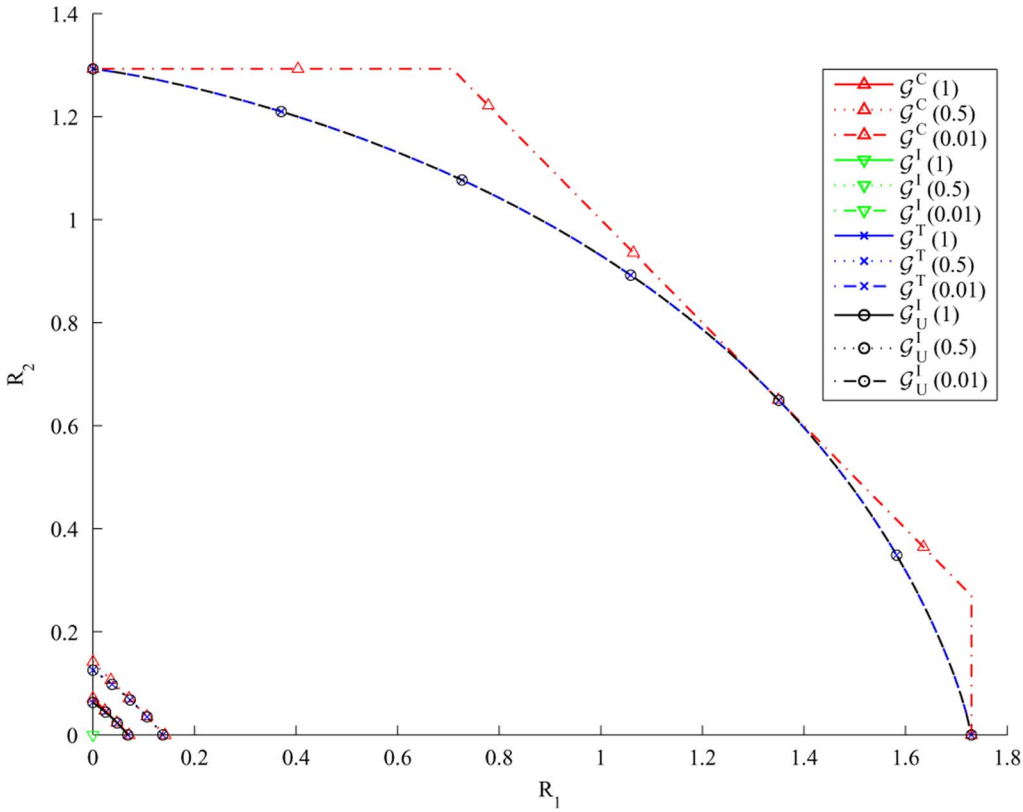

Fig. 4. Achievable rate regions $\mathcal{G}(\delta)$ for $\delta = \{0.01, 0.5, 1\}$. $\bar{P}_1 = 10, \bar{P}_2 = 5$ and $h = 0.9$.

$$+ [\mathsf{h}(\mathbf{Y}) - \mathsf{h}(\mathbf{Z})] \tag{92}$$
$$= \mathsf{h}(\mathbf{Y}) - \mathsf{h}(\mathbf{Z}) \tag{93}$$
$$\leq n \left[C_{\mathcal{K}}^{\mathrm{M}} - C_{\mathcal{K}}^{\mathrm{W}} \right] \tag{94}$$

where we used $\mathbf{X}_{\mathcal{K}} \rightarrow \mathbf{Y} \rightarrow \mathbf{Z}$ to get (88), and applied Corollary 7.1 in the last step. Using (94) in (76) completes the proof. □

To see when the secrecy constraint is more constraining on the sum-rate than the decodability constraint, we can also write (70) as

$$C_{\mathrm{sum}}(\delta) = \begin{cases} \frac{1}{2}\log(1+P_{\mathcal{K}}), & \text{if } \delta \leq 1 - \frac{\log(1+hP_{\mathcal{K}})}{\log(1+P_{\mathcal{K}})} \\ \frac{1}{2\delta}\log\left(\frac{1+P_{\mathcal{K}}}{1+hP_{\mathcal{K}}}\right), & \text{if } \delta \geq 1 - \frac{\log(1+hP_{\mathcal{K}})}{\log(1+P_{\mathcal{K}})}. \end{cases} \tag{95}$$

V. Numerical Results and Observations

An interesting point to note is that the secrecy sum-capacity $C_{\mathrm{sum}}(\delta)$ is upper bounded by $\frac{1}{2\delta}\log(\frac{1+P_{\mathcal{K}}}{1+hP_{\mathcal{K}}})$, which is an increasing function of $P_{\mathcal{K}}$ for $h < 1$, but as $P_{\mathcal{K}} \rightarrow \infty, C_{\mathrm{sum}}(\delta)$ is upper bounded by $-\frac{1}{2\delta}\log h$. We see that regardless of how much power we have available, the δ-secrecy sum-capacity with a nonzero level of secrecy is limited by the channel's degradedness, h, and the level of secrecy required, δ. Also, it is inversely proportional to the level of secrecy desired, δ, but inversely proportional to the logarithm of h, the degradedness of the channel. Since in the range $[0, 1]$, $\log(x)$ goes to 0 faster than $-x^{-1}$, an increase in h affects δ-secrecy sum-capacity more than a similar increase in δ. This can be seen in Figs. 2, 3, and 4 which show the region $\mathcal{G}$ for $\delta = 0.01, 0.5, 1$ and $h = 0.1, 0.5, 0.9$ for two users. When $\delta \rightarrow 0$, we are not concerned with secrecy, and the resulting region corresponds to the standard GMAC region, [31]. The region for $\delta = 1$ corresponds to the *perfect secrecy* region, i.e., transmitting at rates within this region, it is possible to limit the rate of information leakage to the wire-tapper to arbitrarily small values. It is seen that relaxing the secrecy constraint may provide a larger region, the limit of which is the GMAC region. 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 the level of degradedness, h. Especially when the degradedness is high, i.e., $h \rightarrow 0$, then we note that the achievable secrecy regions for $\delta = 0.01$ and $\delta = 0.5$ coincide with the GMAC region without the secrecy constraint. As $h \rightarrow 1$, the advantage over the wire-tapper disappears, and the achievable secrecy sum-rate is reduced. Also shown in the figures are the regions achievable by the TDMA scheme described in the previous section. Although TDMA achieves the secrecy sum capacity with optimum time-sharing parameters, this region is in general contained within $\mathcal{G}^{\mathrm{C}}(\delta)$. Depending on h and δ, the TDMA region is sometimes a superset of $\mathcal{G}^{\mathrm{I}}(\delta)$, as observed in Figs. 2 and 3, sometimes a subset of $\mathcal{G}^{\mathrm{I}}(\delta)$, as observed in Fig. 4 when $\delta = 0.01$ or $\delta = 0.5$, and sometimes the two regions can be used with time-sharing to enlarge the achievable region with individual constraints, see Fig. 4, $\delta = 1$. Close examination of these figures show that when the eavesdropper has a much worse channel, i.e., low h, and the secrecy constraint δ is low, then $\mathcal{G}^{\mathrm{I}}(\delta)$ gives a larger region. However, as we increase the secrecy constraint and the eavesdropper has a less noisy version of the intended receiver's signal, the TDMA region becomes more dominant.

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 when considering the collective secrecy constraints[2]. This can be seen in Figs. 2, 3, and –4 as the TDMA region does not end at the "legs" of $\mathcal{G}^{\mathrm{C}}(\delta)$ when $\mathcal{G}^{\mathrm{C}}(\delta)$ is not equal to the GMAC capacity region. In addition, as noted in [3], the intended receiver decodes the codeword transmitted completely, and as

[2]This general idea is explored in detail in our follow-up work [32], [33].

such $\lfloor \frac{1}{\delta} \rfloor$ low-rate messages can be transmitted each in perfect secrecy by the users.

VI. Conclusion

We have examined secure communications in a multiple access channel in the presence of a wire-tapper. Defining the appropriate secrecy measures, we have found achievable secrecy rate regions, and established the secrecy sum capacity of the GMAC-WT.

A main contribution of this correspondence is that, we show that the multiple-access nature of the channel can be utilized to improve the secrecy of the system. Allowing confidence in the secrecy of all users, the secrecy rate of a user is improved since the undecoded messages of any set of users acts as additional noise at the wire-tapper and precludes it from decoding the remaining set of users.

The results in this correspondence are based on the wire-tapper having access to a degraded version of the intended receiver's signal. The case where the eavesdropper's received signal is not necessarily degraded, i.e., different h_k for different users k, termed the General Gaussian multiple access wire-tap channel, is explored in our follow-up work, [33]. Reference [33] found achievable rates, the capacity region for this model, however, is still open. The secrecy constraints in this correspondence are assumed to be identical across the users. It might be interesting to explore heterogeneous scenarios where users might have different secrecy requirements. We assume in this correspondence that the eavesdropper's channel gains are known to the legitimate parties. These channel gains may not be easy to obtain in practice. If the eavesdropper is known to be outside a certain area, we might opt to have a worst case system design, considering the boundary of the "secure" area.

Finally, we remark that information theoretic secrecy has attracted a lot of attention in the research community including various multi-terminal formulations since the submission of this work, for which we refer the reader to [33] and the references therein.

References

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

[2] A. Wyner, "The wire-tap channel," *Bell Syst. 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. Inf. Theory*, vol. IT-23, no. 3, pp. 387–390, May 1977.

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

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

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

[7] C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.

[8] R. Ahslwede and I. Csiszár, "Common randomness in information theory and cryptography, part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[9] R. Ahslwede and I. Csiszár, "Common randomness in information theory and cryptography, Part II: CR capacity," *IEEE Trans. Inf. Theory*, vol. 44, no. 1, pp. 225–240, Jan. 1998.

[10] S. Venkatesan and V. Anantharam, "The common randomness capacity of a pair of independent discrete memoryless channels," *IEEE Trans. Inf. Theory*, vol. 44, no. 1, pp. 215–224, Jan. 1998.

[11] S. Venkatesan and V. Anantharam, "The common randomness capacity of a network of discrete memoryless channels," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 367–387, Mar. 2000.

[12] I. Csiszár and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 344–366, Mar. 2000.

[13] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3047–3061, Dec. 2004.

[14] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Proc. EUROCRYPT 2000, Lecture Notes in Comput. Sci.*, Berlin, Germany, May 2000, vol. 1807, pp. 351–368.

[15] U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels—Part I: Definitions and a completeness result," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 822–831, Apr. 2003.

[16] U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels—Part II: The simulatability condition," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 832–838, Apr. 2003.

[17] U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels—Part III: Privacy amplification," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 839–851, Apr. 2003.

[18] H. Yamamoto, "On secret sharing communication systems with two or three channels," *IEEE Trans. Inf. Theory*, vol. IT-32, no. 3, pp. 387–393, May 1986.

[19] H. Yamamoto, "A coding theorem for secret sharing communication systems with two Gaussian wiretap channels," *IEEE Trans. Inf. Theory*, vol. 37, no. 3, pp. 634–638, May 1991.

[20] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Seattle, WA, Jul. 9–14, 2006, pp. 356–360.

[21] P. K. Gopala, L. Lai, and H. ElGamal, "On the secrecy capacity of fading channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Nice, France, Jun. 2007.

[22] Y. Liang and V. Poor, "Secure communication over fading channels," in *Proc. Allerton Conf. Commun. Control Comput.*, Monticello, IL, Sep. 27–29, 2006.

[23] L. Zang, R. Yates, and W. Trappe, "Secrecy capacity of independent parallel channels," in *Proc. Allerton Conf. Commun. Control Comput.*, Monticello, IL, Sep. 27–29, 2006.

[24] R. Liu, I. Maric, R. D. Yates, and P. Spasojevic, "Discrete memoryless interference and broadcast channels with confidential messages," in *Proc. Allerton Conf. Commun. Control Comput.*, Monticello, IL, Sep. 27–29, 2006.

[25] Y. Liang and V. Poor, "Generalized multiple access channels with confidential messages," *IEEE Trans. Inf. Theory*, to appear.

[26] R. Liu, I. Maric, R. D. Yates, and P. Spasojevic, "The discrete memoryless multiple access channel with confidential messages," in *Proc. IEEE Int. Symp. Inf. Theory*, Seattle, WA, Jul. 9–14, 2006, pp. 957–961.

[27] E. Tekin, S. Serbetli, and A. Yener, "On secure signaling for the Gaussian multiple access wire-tap channel," in *Proc. Asilomar Conf. Signal Syst. Comput.*, Asilomar, CA, Oct. 28–Nov. 1 2005, pp. 1747–1751.

[28] A. B. Carleial, "Interference channels," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 1, pp. 60–70, Jan. 1978.

[29] E. Tekin and A. Yener, "The Gaussian multiple-access wire-tap channel with collective secrecy constraints," in *Proc. IEEE Int. Symp. Inf. Theory*, Seattle, WA, Jul. 9–14, 2006, pp. 1164–1168.

[30] V. Korjik, V. Yakovlev, and I. Babkov, "The wire-tap channel concept against eavesdropping of indoor radio telephone," in *Proc. 8th IEEE Int. Symp. Pers., Indoor and Mobile Radio Commun.*, Sep. 1997, vol. 2, pp. 477–479.

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

[32] E. Tekin and A. Yener, "Achievable rates for the general Gaussian multiple access wire-tap channel with collective secrecy," in *Proc. Allerton Conf. Commun. Control Comput.*, Monticello, IL, Sep. 27–29, 2006.

[33] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wire-tap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.