The General Gaussian Multiple-Access and Two-Way Wiretap Channels: Achievable Rates and Cooperative Jamming

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

***Abstract*—The general Gaussian multiple-access wiretap channel (GGMAC-WT) and the Gaussian two-way wiretap channel (GTW-WT) are considered. In the GGMAC-WT, multiple users communicate with an intended receiver in the presence of an eavesdropper who receives their signals through another GMAC. In the GTW-WT, two users communicate with each other over a common Gaussian channel, with an eavesdropper listening through a GMAC. A secrecy measure that is suitable for this multiterminal environment is defined, and achievable secrecy rate regions are found for both channels. For both cases, the power allocations maximizing the achievable secrecy sum rate are determined. It is seen that the optimum policy may prevent some terminals from transmission in order to preserve the secrecy of the system. Inspired by this construct, a new scheme *cooperative jamming* is proposed, where users who are prevented from transmitting according to the secrecy sum rate maximizing power allocation policy "jam" the eavesdropper, thereby helping the remaining users. This scheme is shown to increase the achievable secrecy sum rate. Overall, our results show that in multiple-access scenarios, users can help each other to collectively achieve positive secrecy rates. In other words, cooperation among users can be invaluable for achieving secrecy for the system.**

***Index Terms*—Confidential messages, Gaussian multiple-access channel (GMAC), Gaussian two-way channel, secrecy capacity, wiretap channel.**

I. Introduction

GAUSSIAN multiple-access channels and two-way channels are two of the earliest channels that were considered in the literature. The multiple-access channel capacity region was determined in [1] and [2]. The two-way channel was initially examined by Shannon [3], where he found inner and outer bounds for the general two-way channel and determined the capacity region for some special cases. In [4], it was shown that the inner bound found by Shannon was not tight in general. The capacity region of the Gaussian two-way channel was found by Han [5]. A related, somewhat more general case called two-user channels was studied in [6] and [7]. For a comprehensive review of these channels, the reader is referred to [8].

A rigorous analysis of information theoretic secrecy was first given by Shannon in [9]. In this work, Shannon showed that to achieve *perfect secrecy* in communications, which is equivalent to providing no information to an enemy cryptanalyst, the conditional probability of the cryptogram given a message must be independent of the actual transmitted message. In other words, the *a posteriori* probability of a message must be equivalent to its *a priori* probability.

In [10], Wyner applied this concept to the discrete memoryless channel. He defined the wiretap channel, where there is a wire tapper who has access to a degraded version of the intended receiver's signal. Using the normalized conditional entropy Δ of the transmitted message given the received signal at the wire tapper as the secrecy measure, he found the region of all possible (R, Δ) pairs, and the existence of a *secrecy capacity*, C_s, the rate up to which it is possible to limit the rate of information transmitted to the wire tapper to arbitrarily small values.

In [11], it was shown that for Wyner's wiretap channel, 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. However, if any of the messages are available to the wire tapper, the secrecy of the rest may also be compromised. Leung-Yan-Cheong and Hellman [12] extended Wyner's results in [10] and Carleial and Hellman's results in [11] to Gaussian channels. The seminal work by Csiszár and Körner [13] generalized Wyner's results to "less noisy" and "more capable" channels. Furthermore, it examined sending common information to both the receiver and the wire tapper, while maintaining the secrecy of some private information that is communicated to the intended receiver only. Maurer and Wolf [14] suggested that the secrecy constraint developed by Wyner needed to be strengthened, since it constrains the rate of information leaked to the wire tapper, rather than the total information, and the information of interest might be in this small amount. It was then shown that the results of [10] and [11] can be extended to "strong" secrecy constraints for discrete channels, where the limit is on the total leaked information rather than just the rate, with no loss in achievable rates [14].

In the past two decades, common randomness has emerged as a valuable resource for secret key generation [15], [16]. In [15], it was shown that the existence of a "public" feedback channel can enable the two parties to be able to generate a secret key even

Manuscript received November 23, 2006; revised October 1, 2007. This work was supported by the National Science Foundation under Grant CCF-0514813 "Multiuser Wireless Security" and the DARPA ITMANET Program under Grant W911NF-07-1-0028. The material in this papers was presented in part at the Allerton Conference on Communications, Control, and Computing, Monticello, IL, September 2006, and at the International Symposium on Information Theory, Nice, France, June 2007.

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).

Communicated by Y. Zheng, Guest Editor for Special Issue on Information Theoretic Security.

Color versions of Figs. 3–11 in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2008.921680

when the wiretap capacity is zero. Ahslwede and Csiszár [17], [18] examined the secret key capacity and *common randomness* capacity, for several channels. These results also benefit from [14] to provide "strong" secret key capacities. Maurer also examined the case of active adversaries, where the wire tapper has read/write access to the channel in [19]–[21]. The secret key generation problem was investigated from a multiparty point of view in [22] and [23]. Notably, Csiszár and Narayan considered the case of multiple terminals where a number of terminals try to distill a secret key and a subset of these terminals can act as helper terminals to the rest in [24] and [25].

Recently, several new models have emerged, examining secrecy for parallel channels [26], [27], relay channels [28], and fading channels [29], [30]. Fading and parallel channels were examined together in [31] and [32]. Broadcast and interference channels with confidential messages were considered in [33]. Liang and Poor [34] and Liu *et al.* [35] examined the multiple-access channel with confidential messages where two transmitters try to keep their messages secret from each other while communicating with a common receiver. In [34], an achievable region was found in general, and the capacity region was found for some special cases. Multiple-input–multiple-output (MIMO) channels were considered in [36] and [37].

In [38]–[41], we investigated multiple-access channels where transmitters communicate with an intended receiver in the presence of an external wire tapper from whom the messages must be kept confidential. In [38]–[40], we considered the case where the wire tapper gets a degraded version of a GMAC signal, and defined two separate secrecy measures extending Wyner's measure to multiuser channels to reflect the level of trust the network may have in each node. Achievable rate regions were found for different secrecy constraints, and it was shown that the secrecy sum capacity can be achieved using Gaussian inputs and stochastic encoders. In addition, time-division multiple access (TDMA) was shown to also achieve the secrecy sum capacity. Gaussian and binary additive two-way wiretap channels were examined in [42].

In this paper, we consider the general Gaussian multiple-access wiretap channel (GGMAC-WT) and the Gaussian two-way wiretap channel (GTW-WT), both of which are of interest in wireless communications as they correspond to the case where a single physical channel is utilized by multiple transmitters, such as in an ad hoc network. We consider an external *eavesdropper*[1] that receives the transmitters' signals through a general Gaussian multiple-access channel (GGMAC) in both system models. We utilize a suitable secrecy constraint that is the normalized conditional entropy of the transmitted secret messages given the eavesdropper's signal, corresponding to the "collective secrecy" constraints used in [40]. We show that satisfying this constraint implies the secrecy of the messages for all users. In both scenarios, transmitters are assumed to have one secret and one open message to transmit. This is different from [40] in that the secrecy rates are not constrained to be at least a fixed portion of the overall rates. We find an achievable secrecy rate region, where users can communicate with arbitrarily small probability of error with the intended receiver under *perfect secrecy* from the eavesdropper, which corresponds to the result of [40] for the degraded case. We note that, in accordance with the recent literature, when we use the term perfect secrecy, we are referring to "weak" secrecy, where the *rate* of information leaked to the adversary is limited. As such, this can be thought of as "almost perfect secrecy." We also find the sum-rate maximizing power allocations for the general case, which is more interesting from a practical point of view. It is seen that as long as the users are not *single-user decodable* at the eavesdropper, a secrecy-rate tradeoff is possible between the users. Next, we show that a nontransmitting user can help increase the secrecy capacity for a transmitting user by effectively "jamming" the eavesdropper, and even enable secret communications that would not be possible in a single-user scenario. We term this new scheme *cooperative jamming*. The GTW-WT is shown to be especially useful for secret communications, as the multiple-access nature of the channel hurts the eavesdropper without affecting the communication rate. This is because the transmitted messages of each user essentially help hide the other user's secret messages, and reduce the extra randomness needed in wiretap channels to confuse the eavesdropper.

The rest of this paper is organized as follows. Section II describes the system model for the GGMAC-WT and GTW-WT and the problem statement. Section III describes the general achievable rates for the GGMAC-WT and the GTW-WT. Sections IV and V give the secrecy sum rate maximizing power allocations, and the achievable rates with cooperative jamming. Section VI gives our numerical results followed by our conclusions and future work in Section VII.

II. System Model and Problem Statement

We consider K users communicating in the presence of an eavesdropper who has the same capabilities. Each transmitter $k \in \mathcal{K} \triangleq \{1,\dots,K\}$ has two messages, W_k^s which is secret and W_k^o which is open,[2] from two sets of equally likely messages $\mathcal{W}_k^s = \{1,\dots,M_k^s\}$, $\mathcal{W}_k^o = \{1,\dots,M_k^o\}$. Let $\mathbf{W}_k = (W_k^s, W_k^o)$, $\mathcal{W}_k = \mathcal{W}_k^s \times \mathcal{W}_k^o$, $M_k = M_k^s M_k^o$, $\mathbf{W}_{\mathcal{S}}^o = \{W_k^o\}_{k\in\mathcal{S}}$, and $\mathbf{W}_{\mathcal{S}}^s = \{W_k^s\}_{k\in\mathcal{S}}$. The messages are encoded using $(2^{nR_k}, n)$ codes into $\{X_k^n(\mathbf{W}_k)\}$, where $R_k = \frac{1}{n}\log_2 M_k = \frac{1}{n}\log_2 M_k^s + \frac{1}{n}\log_2 M_k^o = R_k^s + R_k^o$. The encoded messages $\{\mathbf{X}_k\} = \{\tilde{X}_k^n\}$ are then transmitted. We assume the channel parameters are universally known, and that the eavesdropper also has knowledge of the codebooks and the coding scheme. In other words, there is no shared secret. The two channels we consider in this paper are described next.

A. GGMAC-WT

This is a scenario where the users communicate with a common base station in the presence of an eavesdropper, where both channels are modeled as Gaussian multiple-access channels as shown in Fig. 1. The intended receiver and the wire tapper receive $\tilde{\mathbf{Y}} = \tilde{Y}^n$ and $\tilde{\mathbf{Z}} = \tilde{Z}^n$, respectively. The receiver decodes $\tilde{\mathbf{Y}}$ to get an estimate of the transmitted messages $\hat{\mathbf{W}}_{\mathcal{K}}^s, \hat{\mathbf{W}}_{\mathcal{K}}^o$. We would like to communicate with the

[1]Even though we faithfully follow Wyner's terminology in naming the channels, admittedly in wireless system models, *eavesdropper* is a more appropriate term for the adversary.

[2]We would like to stress that *open* is not the same as *public*, i.e., we do not impose a decodability constraint for the open messages at the eavesdropper.

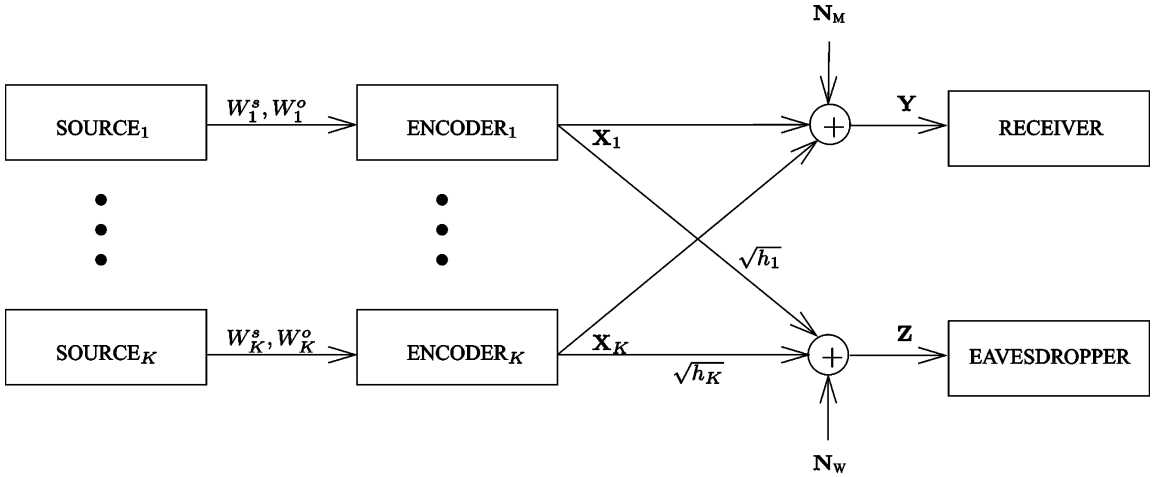

Fig. 1. Standardized GMAC-WT system model.

receiver with arbitrarily low probability of error, while keeping the wire tapper (eavesdropper) ignorant of the secret messages $\mathbf{W}_1^s$. The signals at the intended receiver and the wire tapper are 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 $\tilde{\mathbf{N}}_{\mathrm{M}}$ and $\tilde{\mathbf{N}}_{\mathrm{W}}$ are the additive white Gaussian noise (AWGN), $\tilde{\mathbf{X}}_k$ is the transmitted codeword of user k, and h_k^{M} and h_k^{W} are the channel gains of user k to the intended receiver (*main* channel M), and the eavesdropper (*wiretap* channel W), respectively. Each component of $\tilde{\mathbf{N}}_{\mathrm{M}} \sim \mathcal{N}\left(0, \sigma_{\mathrm{M}}^2\right)$ and $\tilde{\mathbf{N}}_{\mathrm{W}} \sim \mathcal{N}\left(0, \sigma_{\mathrm{W}}^2\right)$. We also assume the following transmit power constraints:

$$\frac{1}{n}\sum_{i=1}^{n} \tilde{X}_{ki}^2 \leq \tilde{\bar{P}}_k, \qquad k = 1, \ldots, K. \tag{2}$$

Similar to the scaling transformation to obtain the standard form of the interference channel [43], we can represent any GMAC-WT by an equivalent standard form [40]

$$\mathbf{Y} = \sum_{k=1}^{K} \mathbf{X}_k + \mathbf{N}_{\mathrm{M}} \tag{3a}$$

$$\mathbf{Z} = \sum_{k=1}^{K} \sqrt{h_k}\mathbf{X}_k + \mathbf{N}_{\mathrm{W}} \tag{3b}$$

where, for each k, we have the following:

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

We can show that the eavesdropper gets a stochastically degraded version of the receiver's signal if $h_1 = \ldots = h_K \equiv h < 1$. We considered this special case in [39] and [40].

B. GTW-WT

In this scenario, two transmitter/receiver pairs communicate with each other over a common channel. Each receiver $k = 1, 2$ gets $\tilde{\mathbf{Y}}_k = \tilde{Y}_k^n$ and the eavesdropper gets $\tilde{\mathbf{Z}} = \tilde{Z}^n$. Receiver k decodes $\tilde{\mathbf{Y}}_k$ to get an estimate of the transmitted messages of the other user. The users would like to communicate the open and secret messages with arbitrarily low probability of error, while maintaining secrecy of the secret messages. The signals at the intended receiver and the wiretapper are given by

$$\tilde{\mathbf{Y}}_1 = \tilde{\mathbf{X}}_1 + \sqrt{h_2^{\mathrm{M}}}\tilde{\mathbf{X}}_2 + \tilde{\mathbf{N}}_1 \tag{4a}$$

$$\tilde{\mathbf{Y}}_2 = \sqrt{h_1^{\mathrm{M}}}\tilde{\mathbf{X}}_1 + \tilde{\mathbf{X}}_2 + \tilde{\mathbf{N}}_2 \tag{4b}$$

$$\tilde{\mathbf{Z}} = \sqrt{h_1^{\mathrm{W}}}\tilde{\mathbf{X}}_1 + \sqrt{h_2^{\mathrm{W}}}\tilde{\mathbf{X}}_2 + \tilde{\mathbf{N}}_{\mathrm{W}} \tag{4c}$$

where $\tilde{\mathbf{N}}_k \sim \mathcal{N}\left(0, \sigma_k^2\right)$ and $\tilde{\mathbf{N}}_{\mathrm{W}} \sim \mathcal{N}\left(0, \sigma_{\mathrm{W}}^2\right)$. We also assume the same power constraints given in (2) (with $K = 2$), and again use an equivalent standard form as illustrated in Fig. 2

$$\mathbf{Y}_1 = \sqrt{\alpha_1}\mathbf{X}_1 + \mathbf{X}_2 + \mathbf{N}_1 \tag{5a}$$

$$\mathbf{Y}_2 = \mathbf{X}_1 + \sqrt{\alpha_2}\mathbf{X}_2 + \mathbf{N}_2 \tag{5b}$$

$$\mathbf{Z} = \sqrt{h_1}\mathbf{X}_1 + \sqrt{h_2}\mathbf{X}_2 + \mathbf{N}_{\mathrm{W}} \tag{5c}$$

where we have the following:

- the codewords $\{\tilde{\mathbf{X}}\}$ are scaled to get $\mathbf{X}_1 = \sqrt{\frac{h_1^{\mathrm{M}}}{\sigma_2^2}}\tilde{\mathbf{X}}_1$ and $\mathbf{X}_2 = \sqrt{\frac{h_2^{\mathrm{M}}}{\sigma_1^2}}\tilde{\mathbf{X}}_2$;
- the maximum powers are scaled to get $\bar{P}_1 = \frac{h_1^{\mathrm{M}}}{\sigma_2^2}\tilde{\bar{P}}_1$ and $\bar{P}_2 = \frac{h_2^{\mathrm{M}}}{\sigma_1^2}\tilde{\bar{P}}_2$;
- the transmitters' new channel gains are given by $\alpha_1 = \frac{\sigma_2^2}{h_1^{\mathrm{M}}\sigma_1^2}$ and $\alpha_2 = \frac{\sigma_1^2}{h_2^{\mathrm{M}}\sigma_2^2}$;
- the wiretapper's new channel gains are given by $h_1 = \frac{h_1^{\mathrm{W}}\sigma_2^2}{h_1^{\mathrm{M}}\sigma_{\mathrm{W}}^2}$ and $h_2 = \frac{h_2^{\mathrm{W}}\sigma_1^2}{h_2^{\mathrm{M}}\sigma_{\mathrm{W}}^2}$;

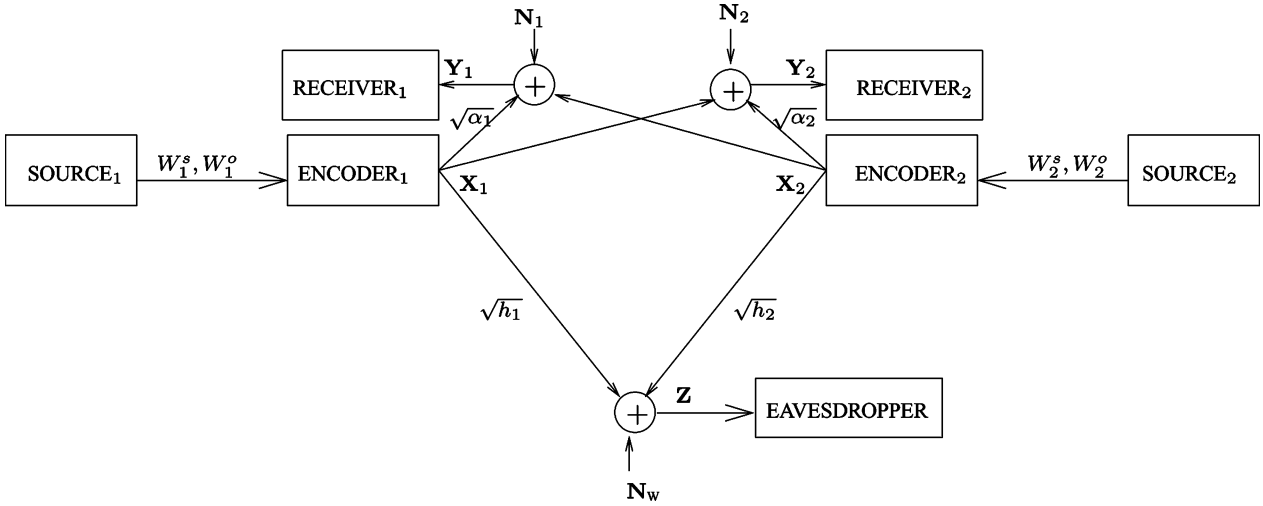

Fig. 2. Standardized GTW-WT system model.

- the noises are normalized by $\mathbf{N}_k = \frac{1}{\sigma_k^2}\tilde{\mathbf{N}}_k$, $k = 1, 2$ and $\mathbf{N}_{\mathrm{W}} = \frac{1}{\sigma_{\mathrm{W}}^2}\tilde{\mathbf{N}}_{\mathrm{W}}$.

C. Preliminary Definitions

In this section, we present some useful preliminary definitions including the secrecy constraint we will use. In particular, the secrecy constraint we used is the "collective secrecy constraint" we defined in [38] and [40], and it is suitable for the multiaccess nature of the systems of interest.

Definition 1 (Collective Secrecy Constraint): We use the normalized joint conditional entropy of the transmitted messages given the eavesdropper's received signal as our secrecy constraint, i.e.,

$$\Delta_{\mathcal{S}} \triangleq \frac{H(\mathbf{W}_{\mathcal{S}}^s|\mathbf{Z})}{H(\mathbf{W}_{\mathcal{S}}^s)} \tag{6}$$

for any set $\mathcal{S} \subseteq \mathcal{K}$ of users. For perfect secrecy of all transmitted secret messages, we would like

$$\Delta_{\mathcal{K}} = \frac{H(\mathbf{W}_{\mathcal{K}}^s|\mathbf{Z})}{H(\mathbf{W}_{\mathcal{K}}^s)} \to 1. \tag{7}$$

Assume $\Delta_{\mathcal{K}} \geq 1 - \epsilon$ for some arbitrarily small ϵ as required. Then

$$\begin{aligned} H(\mathbf{W}_{\mathcal{K}}^s|\mathbf{Z}) &\geq H(\mathbf{W}_{\mathcal{K}}^s) - \epsilon H(\mathbf{W}_{\mathcal{K}}^s) && (8)\\ H(\mathbf{W}_{\mathcal{S}}^s|\mathbf{Z}) &\geq H(\mathbf{W}_{\mathcal{S}}^s) + H(\mathbf{W}_{\mathcal{S}^c}^s|\mathbf{W}_{\mathcal{S}}^s) \\ &\quad - \epsilon H(\mathbf{W}_{\mathcal{K}}^s) - H(\mathbf{W}_{\mathcal{S}^c}^s|\mathbf{W}_{\mathcal{S}}^s, \mathbf{Z}) && (9)\\ &\geq H(\mathbf{W}_{\mathcal{S}}^s) - \epsilon H(\mathbf{W}_{\mathcal{K}}^s) && (10)\\ \Delta_{\mathcal{S}} &\geq 1 - \epsilon' && (11) \end{aligned}$$

where $\epsilon' \triangleq \frac{H(\mathbf{W}_{\mathcal{K}}^s)}{H(\mathbf{W}_{\mathcal{S}}^s)}\epsilon \to 0$ as $\epsilon \to 0$. If $H(\mathbf{W}_{\mathcal{S}}^s) = 0$, then we define $\Delta_{\mathcal{S}} = 1$. Thus, the perfect secrecy of the system implies the perfect secrecy of any group of users, guaranteeing that when the system is secure, so is each individual user.

Definition 2 (Achievable Rates): Let $\mathbf{R}_k = (R_k^s, R_k^o)$. The rate vector $\mathbf{R} = (\mathbf{R}_1, \ldots, \mathbf{R}_K)$ is said to be *achievable* if for any given $\epsilon > 0$ there exists a code of sufficient length n such that

$$\frac{1}{n}\log M_k^s \geq R_k^s - \epsilon, \qquad k = 1, \ldots, K \tag{12a}$$

$$\frac{1}{n}\log M_k^o \geq R_k^o - \epsilon, \qquad k = 1, \ldots, K \tag{12b}$$

and

$$P_e = \frac{1}{\prod_{k=1}^K M_k} \sum_{\mathbf{W} \in \times_{k=1}^K \mathcal{W}_k} P\{\hat{\mathbf{W}} \neq \mathbf{W} | \mathbf{W} \text{ sent}} \leq \epsilon\} \tag{12c}$$

is the average probability of error. In addition, we need

$$\Delta_{\mathcal{K}} \geq 1 - \epsilon \tag{12d}$$

where $\Delta_{\mathcal{K}}$ denotes our secrecy constraint and is defined in (7). We will call the set of all achievable rates, the *secrecy-capacity region*, and denote it $\mathcal{C}^{\mathrm{MA}}$ for the GGMAC-WT, and $\mathcal{C}^{\mathrm{TW}}$ for the GTW-WT, respectively.

Before we state our results, we also define the following notation, which will be used extensively in the rest of this paper:

$$[\xi]^+ \triangleq \max[\xi, 0] \tag{13}$$

$$C_{\mathcal{S}}^{\mathrm{M}}(\mathbf{P}) \triangleq \frac{1}{2}\log\left(1 + \sum\nolimits_{k\in\mathcal{S}} P_k\right), \qquad \mathcal{S} \subseteq \mathcal{K} \tag{14}$$

$$C_{\mathcal{S}}^{\mathrm{W}}(\mathbf{P}) \triangleq \frac{1}{2}\log\left(1 + \sum\nolimits_{k\in\mathcal{S}} h_k P_k\right), \qquad \mathcal{S} \subseteq \mathcal{K} \tag{15}$$

$$\tilde{C}_{\mathcal{S}}^{\mathrm{W}}(\mathbf{P}) \triangleq \frac{1}{2}\log\left(1 + \frac{\sum_{k\in\mathcal{S}} h_k P_k}{1 + \sum_{k\in\mathcal{S}^c} h_k P_k}\right), \qquad \mathcal{S} \subseteq \mathcal{K} \tag{16}$$

$$\mathcal{P} \triangleq \left\{\mathbf{P} : 0 \leq P_k \leq \bar{P}_k, \forall\, k\right\} \tag{17}$$

$$\bar{\mathbf{P}} \triangleq \left\{\bar{P}_1, \ldots, \bar{P}_K\right\}. \tag{18}$$

Last, we informally call the kth user *strong* if $h_k \leq 1$, and *weak* if $h_k > 1$. This is a way of indicating whether the intended receiver or the wiretapper is at a more of an advantage concerning that user, and is equivalent to stating whether the single-user secrecy capacity of that user is positive or zero. We later extend this concept to refer to users who can achieve positive secrecy rates and those who cannot. In addition, we will say that a user is *single-user decodable* if its rate is such that it can be decoded by treating the other user as noise. A user group $\mathcal{S}$ is single-user decodable by the eavesdropper if

$C_{\mathcal{S}}^{\mathrm{M}}(\mathbf{P}) \leq \tilde{C}_{\mathcal{S}}^{\mathrm{W}}(\mathbf{P})$. Our achievable rates cannot guarantee secrecy for such a group of users.

III. Achievable Secrecy Rate Regions

A. GGMAC-WT

In this section, we present our main results for the GGMAC-WT. We first define two separate regions and then give an achievable region.

Definition 3 (GGMAC-WT Superposition Region): Let $X_k \sim \mathcal{N}(0, P_k)$ for all k. Then, the superposition region $\mathcal{G}^{\text{MA-SUP}}(\mathbf{P})$ is given by

$$\mathcal{G}^{\text{MA-SUP}}(\mathbf{P}) \triangleq \left\{ \mathbf{R} : \begin{array}{l} \sum_{k\in\mathcal{S}} (R_k^s + R_k^o) \leq I(\mathbf{X}_{\mathcal{S}}; Y|\mathbf{X}_{\mathcal{S}^c}), \forall\, \mathcal{S} \subseteq \mathcal{K} \\ \sum_{k\in\mathcal{S}} R_k^s \leq [I(\mathbf{X}_{\mathcal{S}}; Y|\mathbf{X}_{\mathcal{S}^c}) - I(\mathbf{X}_{\mathcal{S}}; Z)]^+, \forall\, \mathcal{S} \subseteq \mathcal{K} \end{array} \right\} \tag{19}$$

which can be written as

$$\mathcal{G}^{\text{MA-SUP}}(\mathbf{P}) = \left\{ \mathbf{R} : \begin{array}{l} \sum_{k\in\mathcal{S}} (R_k^s + R_k^o) \leq \frac{1}{2}\log\left(1+\sum_{k\in\mathcal{S}} P_k\right), \forall\, \mathcal{S}\subseteq\mathcal{K} \\ \sum_{k\in\mathcal{S}} R_k^s \leq \frac{1}{2}\left[\log\left(1+\sum_{k\in\mathcal{S}} P_k\right) - \log\left(1+\frac{\sum_{k\in\mathcal{S}} h_k P_k}{1+\sum_{k\in\mathcal{S}^c} h_k P_k}\right)\right]^+, \forall\, \mathcal{S}\subseteq\mathcal{K} \end{array} \right\}. \tag{20}$$

Definition 4 (GGMAC-WT TDMA Region): Let $\{\alpha_k\}$ be such that $0 \leq \alpha_k \leq 1$ for all k and $\sum_{k=1}^K \alpha_k = 1$. Let $X_k \sim \mathcal{N}(0, P_k/\alpha_k)$ for all k. Then, the TDMA region $\mathcal{G}^{\text{MA-TDMA}}$ is given by

$$\mathcal{G}^{\text{MA-TDMA}}(\mathbf{P}, \boldsymbol{\alpha}) \triangleq \left\{ \mathbf{R} : \begin{array}{l} R_k^s + R_k^o \leq \alpha_k I(X_k; Y|\mathbf{X}_{k^c}),\ \forall\, k\in\mathcal{K} \\ R_k^s \leq \alpha_k [I(X_k; Y|\mathbf{X}_{k^c}) - I(X_k; Z|\mathbf{X}_{k^c})]^+,\ \forall\, k\in\mathcal{K} \end{array} \right\} \tag{21}$$

which is equivalent to

$$\mathcal{G}^{\text{MA-TDMA}}(\mathbf{P}, \boldsymbol{\alpha}) = \left\{ \mathbf{R} : \begin{array}{l} R_k^s + R_k^o \leq \frac{\alpha_k}{2}\log\left(1+\frac{P_k}{\alpha_k}\right),\ \forall\, k\in\mathcal{K} \\ R_k^s \leq \frac{\alpha_k}{2}\left[\log\left(1+\frac{P_k}{\alpha_k}\right) - \log\left(1+\frac{h_k P_k}{\alpha_k}\right)\right]^+, \forall\, k\in\mathcal{K} \end{array} \right\}. \tag{22}$$

Remark 1: The superposition and TDMA regions can also be written as follows:

$$\mathcal{G}^{\text{MA-SUP}}(\mathbf{P}) = \left\{ \mathbf{R} : \begin{array}{l} \sum_{k\in\mathcal{S}} (R_k^s + R_k^o) \leq C_{\mathcal{S}}^{\mathrm{M}}(\mathbf{P}),\ \forall\, \mathcal{S}\subseteq\mathcal{K} \\ \sum_{k\in\mathcal{S}} R_k^s \leq \left[C_{\mathcal{S}}^{\mathrm{M}}(\mathbf{P}) - \tilde{C}_{\mathcal{S}}^{\mathrm{W}}(\mathbf{P})\right]^+, \forall\, \mathcal{S}\subseteq\mathcal{K} \end{array} \right\} \tag{23}$$

$$\mathcal{G}^{\text{MA-TDMA}}(\mathbf{P}, \boldsymbol{\alpha}) = \left\{ \mathbf{R} : \begin{array}{l} R_k^s + R_k^o \leq \alpha_k C_k^{\mathrm{M}}\left(\frac{\bar{P}_k}{\alpha_k}\right),\ \forall\, k\in\mathcal{K} \\ R_k^s \leq \alpha_k\left[C_k^{\mathrm{M}}\left(\frac{\bar{P}_k}{\alpha_k}\right) - C_k^{\mathrm{W}}\left(\frac{\bar{P}_k}{\alpha_k}\right)\right]^+,\ \forall k\in\mathcal{K} \end{array} \right\} \tag{24}$$

in accordance with the definitions in (14)–(16).

Theorem 1: The rate region given below is achievable for the GGMAC-WT

$$\mathcal{G}^{\mathrm{MA}} = \text{convex closure of } \left[\left(\bigcup_{\mathbf{P}\in\mathcal{P}} \mathcal{G}^{\text{MA-SUP}}(\mathbf{P})\right) \bigcup \left(\bigcup_{\substack{0\leq\boldsymbol{\alpha}\leq 1 \\ \sum_k \alpha_k = 1}} \mathcal{G}^{\text{MA-TDMA}}(\bar{\mathbf{P}}, \boldsymbol{\alpha})\right)\right]. \tag{25}$$

Proof: We first show that the superposition encoding rate region given in (20) for a fixed power allocation is achievable. Consider the following coding scheme for rates $\mathbf{R} \in \mathcal{G}^{\text{MA-SUP}}(\mathbf{P})$ for some $\mathbf{P} \in \mathcal{P}$.

Superposition Encoding Scheme: For each user k, consider the following scheme.

1) Generate three codebooks $\mathfrak{X}_k^s$, $\mathfrak{X}_k^o$, and $\mathfrak{X}_k^x$. $\mathfrak{X}_k^s$ consists of M_k^s codewords, each component of which is drawn from $\mathcal{N}(0, \lambda_k^s P_k - \varepsilon)$. Codebook $\mathfrak{X}_k^o$ has M_k^o codewords with each component randomly drawn from $\mathcal{N}(0, \lambda_k^o P_k - \varepsilon)$ and $\mathfrak{X}_k^x$ has M_k^x codewords with each component randomly drawn from $\mathcal{N}(0, \lambda_k^x P_k - \varepsilon)$ where ε is an arbitrarily small number to ensure that the power constraints on the codewords are satisfied with high probability and $\lambda_k^s + \lambda_k^o + \lambda_k^x = 1$. Define $R_k^x = \frac{1}{n}\log M_k^x$ and $M_k^t = M_k^s M_k^o M_k^x$.

2) To transmit message $\mathbf{W}_k = (W_k^s, W_k^o) \in \mathcal{W}_k^s \times \mathcal{W}_k^o$, user k finds the two codewords corresponding to components of $\mathbf{W}_k$ and also uniformly chooses a codeword W_k^x from $\mathfrak{X}_k^x$. User k then adds all these codewords and transmits the resulting codeword $\mathbf{X}_k$, so that it actually transmits one of M_k^t codewords. Let $R_k^t = \frac{1}{n}\log M_k^t = R_k^o + R_k^s + R_k^x$. Note that since all codewords are chosen uniformly, user k essentially transmits one of $M_k^o M_k^x$ codewords at random for each message W_k^s, and its overall rate of transmission is R_k^t.

Specifically, we choose the rates to satisfy

$$\sum_{k\in\mathcal{S}}(R_k^s+R_k^o+R_k^x) \le \frac{1}{2}\log\left(1+\sum_{k\in\mathcal{S}}P_k\right) \qquad \forall\, \mathcal{S}\subseteq\mathcal{K} \quad (26)$$

$$\sum_{k\in\mathcal{S}}(R_k^o+R_k^x) \le \frac{1}{2}\log\left(1+\sum_{k\in\mathcal{S}}h_kP_k\right) \qquad \forall\, \mathcal{S}\subseteq\mathcal{K},$$
with equality if $\mathcal{S}=\mathcal{K}$ (27)

$$\sum_{k\in\mathcal{S}}R_k^s \le \frac{1}{2}\left[\log\left(1+\sum_{k\in\mathcal{S}}P_k\right) - \log\left(1+\frac{\sum_{k\in\mathcal{S}}h_kP_k}{1+\sum_{k\in\mathcal{S}^c}h_kP_k}\right)\right]^+ \quad \forall\, \mathcal{S}\subseteq\mathcal{K} \quad (28)$$

which we can also write as

$$\sum\nolimits_{k\in\mathcal{S}}(R_k^s+R_k^o+R_k^x) \le C_{\mathcal{S}}^{\mathrm{M}} \qquad \forall\, \mathcal{S}\subseteq\mathcal{K} \quad (29)$$

$$\sum\nolimits_{k\in\mathcal{S}}(R_k^o+R_k^x) \le C_{\mathcal{S}}^{\mathrm{W}} \qquad \forall\, \mathcal{S}\subseteq\mathcal{K},$$
with equality if $\mathcal{S}=\mathcal{K}$ (30)

$$\sum\nolimits_{k\in\mathcal{S}}R_k^s \le \left[C_{\mathcal{S}}^{\mathrm{M}}-\tilde{C}_{\mathcal{S}}^{\mathrm{W}}\right]^+ \qquad \forall\, \mathcal{S}\subseteq\mathcal{K}. \quad (31)$$

Note that if (31) is zero for a group of users, we cannot achieve secrecy for those users. When $\mathcal{S}=\mathcal{K}$, if the sum capacity of the main channel is less than that of the eavesdropper channel, i.e., $C_{\mathcal{K}}^{\mathrm{M}} \le C_{\mathcal{K}}^{\mathrm{W}}$, secrecy is not possible for the system. Assume this quantity is positive. To ensure that we can mutually satisfy both (30) and (31), we can reclassify some open messages as secret. Clearly, if we can guarantee secrecy for a larger set of messages, secrecy is achieved for the original messages. From the first set of conditions in (25) and the GMAC coding theorem [44] with high probability the receiver can decode the codewords with low probability of error. To show the secrecy condition in (12), first note that the coding scheme described is equivalent to each user k selecting one of M_k^s messages, and sending a uniformly chosen codeword from among $M_k^o M_k^x$ codewords for each. Define $\mathbf{X}_\Sigma = \sum_{k=1}^K \sqrt{h_k}\mathbf{X}_k$, and we have

$$H(\mathbf{W}_{\mathcal{K}}^s|\mathbf{Z}) = H(\mathbf{W}_{\mathcal{K}}^s) - I(\mathbf{W}_{\mathcal{K}}^s;\mathbf{Z}) \quad (32)$$
$$= H(\mathbf{W}_{\mathcal{K}}^s) - I(\mathbf{W}_{\mathcal{K}}^s;\mathbf{Z}) + I(\mathbf{W}_{\mathcal{K}}^s;\mathbf{Z}|\mathbf{X}_\Sigma) \quad (33)$$
$$= H(\mathbf{W}_{\mathcal{K}}^s) - \mathsf{h}(\mathbf{Z}) + \mathsf{h}(\mathbf{Z}|\mathbf{W}_{\mathcal{K}}^s) + \mathsf{h}(\mathbf{Z}|\mathbf{X}_\Sigma) - \mathsf{h}(\mathbf{Z}|\mathbf{W}_{\mathcal{K}}^s,\mathbf{X}_\Sigma) \quad (34)$$
$$= H(\mathbf{W}_{\mathcal{K}}^s) - I(\mathbf{X}_\Sigma;\mathbf{Z}) + I(\mathbf{X}_\Sigma;\mathbf{Z}|\mathbf{W}_{\mathcal{K}}^s) \quad (35)$$

where we used $\mathbf{W}^s \to \mathbf{X}_\Sigma \to \mathbf{Z}$, and thus we have $\mathsf{h}(\mathbf{Z}|\mathbf{W}^s,\mathbf{X}_\Sigma) = \mathsf{h}(\mathbf{Z}|\mathbf{X}_\Sigma)$ to get (35). We will consider the two terms individually. First, we have the trivial bound due to channel capacity

$$I(\mathbf{X}_\Sigma;\mathbf{Z}) \le nC_{\mathcal{K}}^{\mathrm{W}}(\mathbf{P}). \quad (36)$$

Now write

$$I(\mathbf{X}_\Sigma;\mathbf{Z}|\mathbf{W}_{\mathcal{K}}^s) = H(\mathbf{X}_\Sigma|\mathbf{W}_{\mathcal{K}}^s) - H(\mathbf{X}_\Sigma|\mathbf{W}_{\mathcal{K}}^s,\mathbf{Z}). \quad (37)$$

Since user k independently sends one of $M_k^o M_k^x$ codewords equally likely for each secret message

$$H(\mathbf{X}_\Sigma|\mathbf{W}_{\mathcal{K}}^s) = \log\left(\prod_{k=1}^K (M_k^o M_k^x)\right) \quad (38)$$
$$= n\left(\sum_{k=1}^K (R_k^o + R_k^x)\right) \quad (39)$$
$$= nC_{\mathcal{K}}^{\mathrm{W}}(\mathbf{P}). \quad (40)$$

We can also write

$$H(\mathbf{X}_\Sigma|\mathbf{W}_{\mathcal{K}}^s,\mathbf{Z}) \le n\delta_n \quad (41)$$

where $\delta_n \to 0$ as $n \to \infty$ since, with high probability, the eavesdropper can decode $\mathbf{X}_\Sigma$ given $\mathbf{W}_{\mathcal{K}}^s$ due to (30) and code generation. Using(36), (37), (40), and (41) in (35), we get

$$H(\mathbf{W}_{\mathcal{K}}^s|\mathbf{Z}) \ge H(\mathbf{W}_{\mathcal{K}}^s) - nC_{\mathcal{K}}^{\mathrm{W}}(\mathbf{P}) + nC_{\mathcal{K}}^{\mathrm{W}}(\mathbf{P}) - n\delta_n \quad (42)$$
$$= H(\mathbf{W}_{\mathcal{K}}^s) - n\delta_n. \quad (43)$$

Now, let us consider the TDMA region given in (22). This region is obtained when users who can achieve single-user secrecy use a single-user wiretap code as in [12] in a TDMA schedule, where the time share of each user k is given by $0 \le \alpha_k \le 1$ and $\sum_{k=1}^K \alpha_k = 1$. A transmitter k who can achieve secrecy, i.e., having $h_k < 1$, transmits for α_k portion of the time when all other users are silent, using $\frac{\bar{P}_k}{\alpha_k}$ power, satisfying its average power constraint over the TDMA time frame. This approach was used in [40] to achieve secrecy sum capacity for individual constraints. When the channel is degraded, i.e., $h_k = h$ for all $k \in \mathcal{K}$, then for collective constraints the TDMA region is seen to be a subset of the superposition region. However, this is not necessarily true for the general case, and by time sharing between the two schemes, we can generally achieve a larger achievable region, given in (25). □

We remark that it is possible to further divide the "open" messages to get more sets of "private" messages, which are also perfectly secret, i.e., if we let $\mathcal{W}_k^o = \acute{\mathcal{W}}_k^s \times \acute{\mathcal{W}}_k^o, \forall\, k$, then as long as we impose the same restrictions on $\acute{\mathbf{R}}^s$ as $\mathbf{R}^s$, we can achieve perfect secrecy of $\acute{\mathbf{W}}^s$, as in [12]. However, this does not mean that we have perfect secrecy at channel capacity, as the secrecy subcodes carry information about each other.

Observe that even for $K=2$ users, a rate point in this region is four dimensional, and hence cannot be accurately drawn. We can instead focus on the secrecy rate region, the region of all achievable $\mathbf{R}^s$. The subregions $\mathcal{G}^{\text{MA-SUP}}$ and $\mathcal{G}^{\text{MA-TDMA}}$ are shown for different channel gains in Fig. 3 for fixed transmit powers, and $K=2$ users. Fig. 4 represents how these regions change with different transmit powers when the channel gains

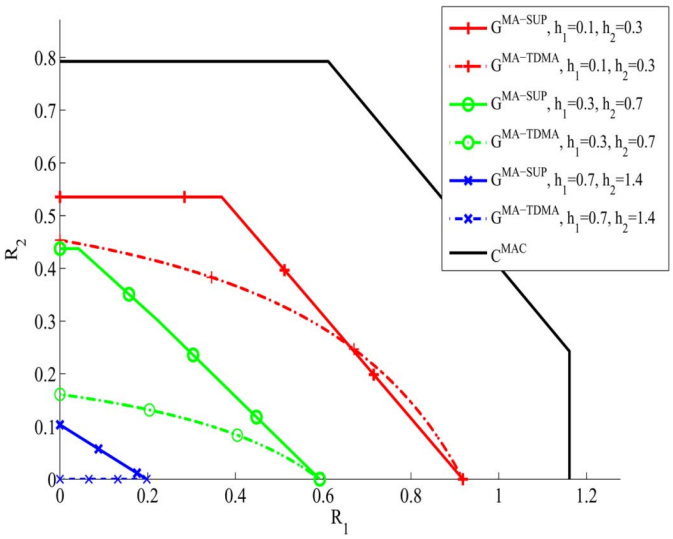

Fig. 3. GGMAC-WT achievable regions for different channel parameters $\mathcal{G}^{\mathrm{MA}}(P_1 = 4, P_2 = 2)$.

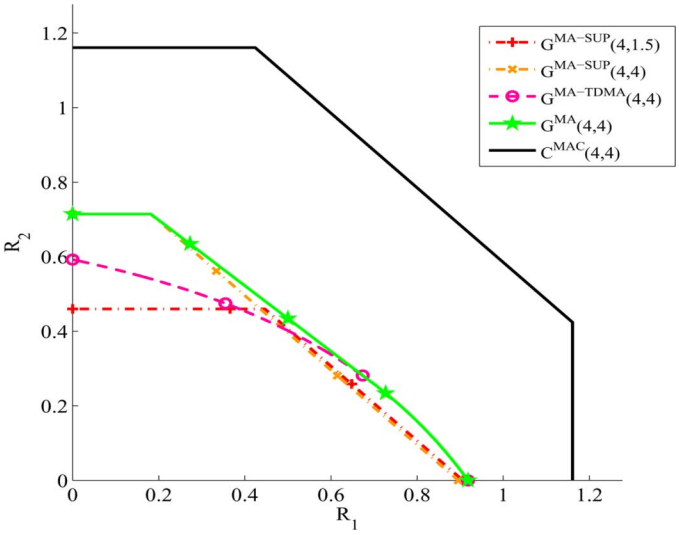

Fig. 4. GGMAC-WT achievable secrecy region when $\bar{P}_1 = 4$, $\bar{P}_2 = 4$, $h_1 = 0.1$, and $h_2 = 0.3$.

are fixed. For the case shown, we need the convex hull operation, as the achievable region is a combination of different superposition and TDMA regions. Note also that the main extra condition for the superposition region is on the total extra randomness added. As a result, it is possible for "stronger" users to help "weak" users by contributing more to the necessary extra number of codewords, which is the sum capacity of the eavesdropper. Such a weak user only has to make sure that it is not single-user decodable, provided the stronger users are willing to sacrifice some of their own rate and generate more superfluous codewords. In other words, we see that users in a set $\mathcal{S}$ are further protected from the eavesdropper by the fact that users in set $\mathcal{S}^c$ are also undecodable, compared to the single-user case. The TDMA region, on the other hand, does not allow users to help each other this way. As such, only users whose channel gains allow them to achieve secrecy on their own are allowed to transmit.

For the special degraded case of $h_1 = \cdots = h_K \triangleq h \leq 1$, the perfect secrecy rate region for R_k^s becomes the region given by [40, Th. 1] for $\delta = 1$. We also observe that even though there is a limit on the secrecy sum rate achieved by our scheme, it is possible to send open messages to the intended receiver at rates such that the sum of the secrecy rate and open rate for all users is in the capacity region of the MAC to the intended receiver. Even though we cannot send at capacity with secrecy, the codewords used to confuse the eavesdropper may be used to communicate meaningful information to the intended receiver.

B. GTW-WT

In this section, we present an achievable region for the GTW-WT using a superposition coding similar to that used to achieve the region $\mathcal{G}^{\text{MA-SUP}}$ for the GGMAC-WT. We first define the following.

Definition 5 (GTW-WT Superposition Region $\mathcal{G}^{\mathrm{TW}}(\mathbf{P})$): Let $X_k \sim \mathcal{N}(0, P_k)$. Then, the GTW-WT superposition region $\mathcal{G}^{\mathrm{TW}}(\mathbf{P})$ is given by

$$\mathcal{G}^{\mathrm{TW}}(\mathbf{P}) = \Bigg\{\mathbf{R}: R_k^s + R_k^o \leq I(X_k;Y|X_{k^c}),\ k=1,2 \\ \sum_{k\in\mathcal{S}} R_k^s \leq \Bigg[\sum_{k\in\mathcal{S}} I(X_k;Y|X_{k^c}) - I(X_{\mathcal{K}};Z)\Bigg]^+, \forall\, \mathcal{S}\subseteq\mathcal{K}\Bigg\} \tag{44}$$

which can be written as

$$\mathcal{G}^{\mathrm{TW}}(\mathbf{P}) = \Bigg\{\mathbf{R}: R_k^s + R_k^o \leq \frac{1}{2}\log(1+P_k),\ k=1,2 \\ \sum_{k\in\mathcal{S}} R_k^s \leq \frac{1}{2}\Bigg[\sum_{k\in\mathcal{S}} \log(1+P_k) - \log\left(1+\frac{\sum_{k\in\mathcal{S}} P_k}{1+\sum_{k\in\mathcal{S}^c} P_k}\right)\Bigg]^+, \forall\, \mathcal{S}\subseteq\mathcal{K}\Bigg\}. \tag{45}$$

Remark 2: We can also write this region more compactly as the following:

$$\mathcal{G}^{\mathrm{TW}}(\mathbf{P}) = \Bigg\{\mathbf{R}: R_k^s + R_k^o \leq C_k^{\mathrm{M}}(\mathbf{P}),\ k=1,2 \\ \sum_{k\in\mathcal{S}} R_k^s \leq \Bigg[\sum_{k\in\mathcal{S}} C_k^{\mathrm{M}}(\mathbf{P}) - \tilde{\mathbf{C}}_{\mathcal{S}}^{\mathrm{W}}(\mathbf{P})\Bigg]^+, \forall\, \mathcal{S}\subseteq\mathcal{K}\Bigg\}. \tag{46}$$

Theorem 2: The rate region given below is achievable for the GTW-WT

$$\text{convex closure of } \bigcup_{\mathbf{P}\in\mathcal{P}} \mathcal{G}^{\mathrm{TW}}(\mathbf{P}). \tag{47}$$

Proof: The proof is very similar to the proof of Theorem 1. We use the same coding scheme as Theorem 1, but the main difference is that we choose the rates to satisfy

$$R_k^s + R_k^o + R_k^x \le \frac{1}{2}\log(1+P_k), \qquad k=1,2 \tag{48}$$

$$\sum_{k\in\mathcal{S}} (R_k^o + R_k^x) \le \frac{1}{2}\log\left(1+\sum_{k\in\mathcal{S}} h_k P_k\right), \qquad \forall\, \mathcal{S}\subseteq\mathcal{K}$$
$$\text{with equality if } \mathcal{S}=\mathcal{K} \tag{49}$$

$$\sum_{k\in\mathcal{S}} R_k^s \le \frac{1}{2}\left[\sum_{k\in\mathcal{S}}\log(1+P_k) - \log\left(1+\frac{\sum_{k\in\mathcal{S}} P_k}{1+\sum_{k\in\mathcal{S}^c} P_k}\right)\right]^+, \quad \forall\, \mathcal{S}\subseteq\mathcal{K} \tag{50}$$

or equivalently

$$R_k^s + R_k^o + R_k^x \le C_k^{\mathrm{M}}, \qquad k=1,2 \tag{51}$$

$$\sum_{k\in\mathcal{S}} (R_k^o + R_k^x) \le C_{\mathcal{S}}^{\mathrm{W}}, \qquad \forall\, \mathcal{S}\subseteq\mathcal{K},$$
$$\text{with equality if } \mathcal{S}=\mathcal{K} \tag{52}$$

$$\sum_{k\in\mathcal{S}} R_k^s \le \left[\sum_{k\in\mathcal{S}} C_k^{\mathrm{M}} - C_{\mathcal{S}}^{\mathrm{W}}\right]^+, \qquad \forall \mathcal{S}\subseteq\mathcal{K} \tag{53}$$

assuming (53) is positive. The decodability of $\mathbf{W}_{\mathcal{K}}^s$ from $\mathbf{Y}_1$ and $\mathbf{Y}_2$ comes from (51) and the capacity region of the Gaussian two-way channel [5]. This gives the first set of terms in the achievable region. The key here is that since each transmitter knows its own codeword, it can *subtract its self-interference* from the received signal and get a clear channel. Therefore, the Gaussian two-way channel decomposes into two parallel channels.

The second group of terms in (45), resulting from the secrecy constraint, can be shown the same way as the proof of Theorem 1, since $\mathbf{Z}$ has the same form for both channels. In other words, as far as the eavesdropper is concerned, the channel is still a GMAC with $K=2$ users. As such, we need to send $C_{\mathcal{K}}^{\mathrm{W}}$ extra codewords in total, which need to be shared by the two terminals provided they are not single-user decodable. □

For different channel gains, the region of all R^s satisfying (45) is shown in Fig. 5. Since we require four dimensions for an accurate depiction of the complete rate region, we only focus on our main interest, i.e., the secrecy rate region. Fig. 6 shows the achievable secrecy rate region as a function of transmit powers. We note that higher powers always result in a larger region. We indicate the constraint on the overall rates, corresponding to the capacity region of the Gaussian two-way channel, by the dotted line. Note that the secrecy region has a structure similar to the GGMAC-WT with $K=2$. As far as the eavesdropper is concerned, there is no difference between the two channels. However, since the main channel between users decomposes into two parallel channels, higher rates can be achieved between

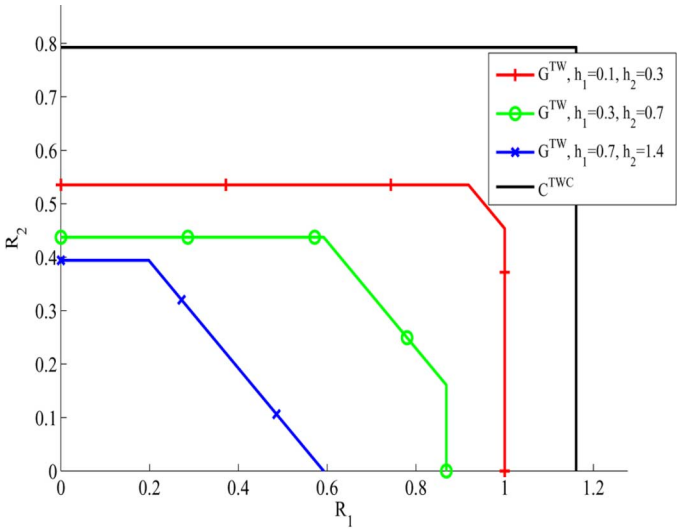

Fig. 5. GTW-WT achievable regions for different channel parameters $\mathcal{G}^{\mathrm{TW}}(P_1=4, P_2=2)$.

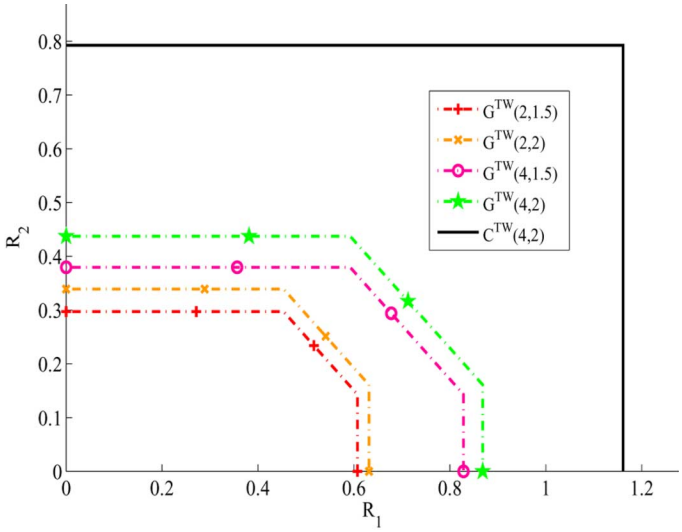

Fig. 6. GTW-WT achievable secrecy region when $\bar{P}_1=4$, $\bar{P}_2=2$, $h_1=0.3$, and $h_2=0.7$.

the legitimate terminals (users). Thus, in effect, each user's transmitted codewords act as a *secret key* for the other user's transmitted codewords, requiring fewer extraneous codewords overall to confuse the eavesdropper, and a larger secrecy region. We note that a user may either achieve secrecy or not, depending on whether it is single-user decodable. As a result, TDMA does not enlarge the region, since each user can at least achieve their single-user secrecy rates. To see this, note that the constraint on the secrecy sum rate can be written as

$$\begin{aligned}&\log(1+P_1)+\log(1+P_2)-\log(1+h_1P_1+h_2P_2)\\ &\quad=\log(1+P_1)-\log(1+h_1P_1)\\ &\qquad+\log(1+P_2)-\log\left(1+\frac{h_2P_2}{1+h_1P_1}\right) \qquad (54)\\ &\quad\ge\log(1+P_1)-\log(1+h_1P_1)\\ &\qquad+\log(1+P_2)-\log(1+h_2P_2) \qquad (55)\end{aligned}$$

so that transmitting in the two-way channel always provides an advantage over the single-user channels.

IV. Maximization of Sum Rate

The achievable regions given in Theorems 1 and 2 depend on the transmit powers. We are, thus, naturally interested in the power allocation $\mathbf{P}^*$ that would maximize the total secrecy sum rate. Recall that the standardized channel gain for user k is $h_k = \frac{h_k^{\mathrm{W}}\sigma_{\mathrm{M}}^2}{h_k^{\mathrm{M}}\sigma_{\mathrm{W}}^2}$, and that the higher h_k is, the better the corresponding eavesdropper channel. Without loss of generality, assume that users are ordered in terms of increasing standardized eavesdropper channel gains, i.e., $h_1 \leq \cdots \leq h_K$. Note that we only need to concern ourselves with the case $h_1 < \cdots < h_K$, since we can combine users with the same channel gains into one superuser. We can then split the resulting optimum power allocation for a superuser among the actual constituting users in any way we choose, since they would all result in the same sum rate. In addition, from a physical point of view, assuming that the channel parameters are drawn according to a continuous distribution and then fixed, the probability that two users would have the same exact standardized channel gain is zero.

A. GGMAC-WT

We first examine the superposition region given in (20). The secrecy sum rate achievable with superposition coding for the GGMAC-WT was given in Theorem 1 as

$$R_{sum}^{\text{MA-SUP}} = \frac{1}{2}\left[\log\left(1+\sum_{k=1}^{K} P_k\right) - \log\left(1+\sum_{k=1}^{K} h_k P_k\right)\right]^+ \tag{56}$$

and we would like to find the power allocation that maximizes this quantity. Stated formally, we are interested in the transmit powers that solve the following optimization problem:

$$\begin{aligned}&\max_{\mathbf{P}\in\mathcal{P}} \frac{1}{2}\left[\log\left(1+\sum\nolimits_{k=1}^{K} P_k\right) - \log\left(1+\sum\nolimits_{k=1}^{K} h_k P_k\right)\right] \\ &\quad = \min_{\mathbf{P}\in\mathcal{P}} \frac{1}{2}\log\phi_{\mathcal{K}}(\mathbf{P}) &(57)\\ &\quad \equiv \min_{\mathbf{P}\in\mathcal{P}} \phi_{\mathcal{K}}(\mathbf{P}) &(58)\end{aligned}$$

where

$$\phi_{\mathcal{S}}(\mathbf{P}) \triangleq \frac{1+\sum_{k\in\mathcal{S}} h_k P_k}{1+\sum_{k\in\mathcal{S}} P_k}, \qquad \mathcal{S}\subseteq\mathcal{K} \tag{59}$$

and $\mathcal{S}=\mathcal{K}$ yields (58). In obtaining (58), we simply used the monotonicity of the log function. The solution to this problem is given below.

Theorem 3: The secrecy sum-rate maximizing power allocation for $\mathcal{G}^{\text{MA-SUP}}$ satisfies $P_k^* = \bar{P}_k$ if $k \leq T$ and $P_k^* = 0$ is $k > T$ where $T \in \{0,\ldots,K\}$ is some limiting user satisfying

$$h_T < \frac{1+\sum_{k=0}^{l} h_k \bar{P}_k}{1+\sum_{k=0}^{l} \bar{P}_k} \leq h_{T+1} \tag{60}$$

and we define $h_0 \triangleq 0$ and $\bar{P}_0 \triangleq 0$. Note that this allocation shows that only a subset of the strong users must be transmitting.

Proof: We start with writing the Lagrangian to be minimized

$$\mathcal{L}(\mathbf{P},\boldsymbol{\mu}) = \phi_{\mathcal{K}}(\mathbf{P}) - \sum_{k=1}^{K}\mu_{1k}P_k + \sum_{k=1}^{K}\mu_{2k}(P_k-\bar{P}_k). \tag{61}$$

Equating the derivative of the Lagrangian to zero, we get

$$\frac{\partial\mathcal{L}(\mathbf{P}^*,\boldsymbol{\mu})}{\partial P_j^*} = \dot{\phi}_{\mathcal{K}}^{(j)}(\mathbf{P}^*) - \mu_{1j} + \mu_{2j} = 0 \tag{62}$$

where we define

$$\dot{\phi}_{\mathcal{S}}^{(j)}(\mathbf{P}) \triangleq \frac{h_j - \phi_{\mathcal{S}}(\mathbf{P})}{1+\sum_{k\in\mathcal{S}} P_k} \tag{63}$$

for any set $\mathcal{S}\subseteq\mathcal{K}$.

It is easy to see that if $h_j > \phi_{\mathcal{K}}(\mathbf{P}^*)$, then $\mu_{1j} > 0$, and we have $P_j^* = \bar{P}_j$. If $h_j < \phi_{\mathcal{K}}(\mathbf{P}^*)$, then we similarly find that $P_j^* = 0$. Finally, if $h_j = \phi_{\mathcal{K}}(\mathbf{P}^*)$, then we also have

$$h_j = \frac{1+\sum_{k\in\mathcal{K}\setminus j} h_k P_k^*}{1+\sum_{k\in\mathcal{K}\setminus j} h_k P_k^*} \tag{64}$$

and $\phi_{\mathcal{K}}(\mathbf{P}^*) = \phi_{\mathcal{K}\setminus j}(\mathbf{P}^*)$ does not depend on P_j, so we can set $P_j^* = 0$ with no effect on the secrecy sum rate. Thus, we have $P_j^* = \bar{P}_j$ if $h_j < \phi_{\mathcal{K}}(\mathbf{P}^*)$, and $P_j^* = 0$ if $h_j \geq \phi_{\mathcal{K}}(\mathbf{P}^*)$. Then, the optimal set of transmitters is of the form $\mathcal{T} = \{1,\ldots,T\}$ since if a user T is transmitting, all users such that $h_k < h_T$ must also be transmitting. We also note that $\phi_{\mathcal{K}}(\mathbf{P}^*) = \phi_{\mathcal{T}}(\bar{\mathbf{P}})$. Let T be the last user satisfying this property, i.e., $h_T < \phi_{\mathcal{T}}(\bar{\mathbf{P}})$ and $h_{T+1} \geq \phi_{\mathcal{T}\cup\{T+1\}}(\bar{\mathbf{P}})$. Note that

$$h_T < \frac{1+\sum_{k=1}^{T} h_k\bar{P}_k}{1+\sum_{k=1}^{T}\bar{P}_k} = \frac{1+\sum_{k=1}^{T-1} h_k\bar{P}_k + h_T\bar{P}_T}{1+\sum_{k=1}^{T-1}\bar{P}_k+\bar{P}_T} \tag{65}$$

$$h_{T-1} < h_T < \frac{1+\sum_{k=1}^{T-1} h_k\bar{P}_k}{1+\sum_{k=1}^{T-1}\bar{P}_k} = \phi_{\mathcal{T}\setminus\{T\}}(\bar{\mathbf{P}}). \tag{66}$$

In other words, all sets $\mathcal{S}=\{1,\ldots,S\}$ for $S\leq T$ also satisfy this property and are viable candidates for the optimal set of transmitting users. Therefore, we can claim that $\mathcal{T}$ is the optimum set of transmitting users, since from above we can iteratively see that $\phi_{\mathcal{T}}(\bar{\mathbf{P}}) < \phi_{\mathcal{S}}(\bar{\mathbf{P}})$ for all $S<T$. □

Note that, for the special case of $K=2$ users, the optimum power allocation is

$$(P_1^*,P_2^*) = \begin{cases} (\bar{P}_1,\bar{P}_2), & \text{if } h_1<1,\ h_2 < \frac{1+h_1\bar{P}_1}{1+\bar{P}_1} \\ (\bar{P}_1,0), & \text{if } h_1<1,\ h_2 \geq \frac{1+h_1\bar{P}_1}{1+\bar{P}_1} \\ (0,0), & \text{otherwise.}\end{cases} \tag{67}$$

We also need to consider the TDMA region. In this case, the maximum achievable secrecy sum rate is

$$\max_{\substack{0\leq\boldsymbol{\alpha}\leq 1\\ \sum_k\alpha_k=1}} \sum_{k=1}^{K}\frac{\alpha_k}{2}\left[\log\left(1+\frac{\bar{P}_k}{\alpha_k}\right) - \log\left(1+\frac{h_k\bar{P}_k}{\alpha_k}\right)\right]. \tag{68}$$

This is a simple complex optimization problem that can easily be solved numerically. For the degraded case, we can obtain a closed form solution: $\alpha_k = \frac{\bar{P}_k}{\sum_k \bar{P}_k}$ as in [40]. In general, we cannot obtain such a solution. However, it is trivial to note that users with $h_k \geq 1$ should not be transmitting in this scheme. The secrecy sum rate is then the maximum of the solutions given by the superposition and TDMA regions.

B. GTW-WT

Now, we will examine the power allocation that maximizes the secrecy sum rate given in Theorem 2 as

$$R_{\text{sum}}^{\text{TW}}=\frac{1}{2}\Big[\log(1+P_1)+\log(1+P_2)-\log(1+h_1P_1+h_2P_2)\Big]^+. \tag{69}$$

This problem is formally stated below

$$\max_{\mathbf{P}\in\mathcal{P}}\frac{1}{2}[\log(1+P_1)+\log(1+P_2)-\log(1+h_1P_1+h_2P_2)] \equiv \min_{\mathbf{P}\in\mathcal{P}}\psi_{\mathcal{K}}(\mathbf{P}) \tag{70}$$

where

$$\psi_{\mathcal{S}}(\mathbf{P})\triangleq\frac{1+\sum_{k\in\mathcal{S}}h_kP_k}{\prod_{k\in\mathcal{S}}(1+P_k)} \tag{71}$$

and $\mathcal{S}=\mathcal{K}$ yields (70). The optimum power allocation is stated below.

Theorem 4: The secrecy sum-rate maximizing power allocation for the GTW-WT is given by

$$(P_1^*,P_2^*)=\begin{cases}(\bar{P}_1,\bar{P}_2), & \text{if } h_1\le 1+h_2\bar{P}_2,\ h_2<1+h_1\bar{P}_1\\ (\bar{P}_1,0), & \text{if } h_1<1,\ h_2\ge 1+h_1\bar{P}_1\\ (0,0), & \text{otherwise.}\end{cases} \tag{72}$$

Proof: The Lagrangian is

$$\mathcal{L}(\mathbf{P},\boldsymbol{\mu})=\psi_{\mathcal{K}}(\mathbf{P})-\sum_{k=1}^{2}\mu_{1k}P_k+\sum_{k=1}^{2}\mu_{2k}(P_k-\bar{P}_k). \tag{73}$$

Equating the derivative of the Lagrangian to zero for user j, we get

$$\frac{\partial\mathcal{L}(\mathbf{P}^*,\boldsymbol{\mu})}{\partial P_j^*}=\dot{\psi}_{\mathcal{K}}^{(j)}(\mathbf{P}^*)-\mu_{1j}+\mu_{2j}=0 \tag{74}$$

where

$$\dot{\psi}_{\mathcal{K}}^{(j)}(\mathbf{P})\triangleq\frac{h_j-\frac{1+\sum_{k\in\mathcal{K}}h_kP_k}{1+P_j}}{\prod_{k\in\mathcal{K}}(1+P_k)}. \tag{75}$$

An argument similar to the one for the GGMAC-WT establishes that if $h_j>\left(1+\sum_{k\in\mathcal{K}}h_kP_k\right)/(1+P_j)$, or equivalently, if $h_j>1+h_{j^c}P_{j^c}^*$, then $P_j^*=0$. When equality is satisfied, then $\dot{\psi}_{\mathcal{K}}^{(j)}(\mathbf{P})=0$ regardless of P_j, and as such $\psi_{\mathcal{K}}(\mathbf{P})$ can be seen to not depend on P_j. To conserve power, we again set $P_j=0$ in this case. On the other hand, if $h_j<\left(1+\sum_{k\in\mathcal{K}}h_kP_k\right)/(1+P_j)$, then $P_j^*=\bar{P}_j$.

Consider user 1. If $P_1^*=0$, and $P_2^*>0$, this implies that $h_2<1$. Since $h_1\le h_2<1$, we cannot have $P_1^*=0$. As a consequence of this contradiction, we see that $P_2^*=0$ whenever $P_1^*=0$. Assume $P_1^*=\bar{P}_1$, and consider the two alternatives for P_2^*. We will have $P_2^*=0$ if $h_2\ge 1+h_1\bar{P}_1$; and $P_2^*=\bar{P}_2$ if $h_2<1+h_2\bar{P}_1$. These cases correspond to $h_1<1$ and $h_1<1+h_2\bar{P}_2$, respectively. Thus, we have (72) as the secrecy sum-rate maximizing power allocation. □

Remark 3: Observe that the solution in Theorem 4 has a structure similar to that in Theorem 3. In summary, it is seen that as long as a user is not single-user decodable, it should be transmitting with maximum power. Hence, when both users can be made to be nonsingle-user decodable, then the maximum powers will provide the largest secrecy sum rate. If this is not the case, then the user who is single-user decodable cannot transmit with nonzero secrecy and will just make the secrecy sum-rate constraint tighter for the remaining user by transmitting open messages.

Comparing (72) to (67), we see that the same form of solutions is found, but the range of channel gains where transmission is possible is larger, showing that GTW-WT allows secrecy even when the eavesdropper's channel is not very weak.

V. Secrecy Through Cooperative Jamming

In Section IV, we found the secrecy sum-rate maximizing power allocations. For both the GGMAC-WT and the GTW-WT, if the eavesdropper is not "disadvantaged enough" for some users, then these users' transmit powers are set to zero. We posit that such a user may be able to "help" a transmitting user, since it can cause more harm to the eavesdropper than to the intended receiver. We only consider the superposition region, since in the TDMA region a user has a dedicated time slot, and hence does not affect the others. We will next show that this type of cooperative behavior is indeed useful, notably exploiting the fact that the established achievable secrecy sum rate is a difference of the sum-capacity expressions for the intended channel(s) and the eavesdropper's channel. As a result, reducing the latter more than the former actually results in an *increase* in the achievable secrecy sum rate.

Formally, the scheme we are considering implies partitioning the set of users $\mathcal{K}$ into a set of transmitting users $\mathcal{T}$ and a set of jamming users $\mathcal{T}^c=\mathcal{K}-\mathcal{T}$. If a user k is jamming, then it transmits $\mathbf{X}_k\sim\mathcal{N}(P_k^*\mathbf{I},\mathbf{0})$ instead of codewords. In this case, we can show that we can achieve higher secrecy rates when the "weaker" users are jamming. We also show that the GTW-WT has an additional advantage compared to the GGMAC-WT; that is the fact that the receiver already knows the jamming sequence. As such, this scheme only harms the eavesdropper and not the intended receivers, achieving an even higher secrecy sum rate. Once again, without loss of generality, we consider $h_1<\cdots<h_K$. In addition, we will assume that a user can either take the action of transmitting its information or jamming the eavesdropper, but not both. It is readily shown in Section V-A that we do not lose any generality by doing so, and that splitting the power of a user between the two actions is suboptimal from the secrecy sum-rate maximization point of view.

A. GGMAC-WT

The problem is formally presented below

$$\max_{\mathcal{T}\subseteq\mathcal{K},\mathbf{P}\in\mathcal{P}}\frac{1}{2}\left[\log\left(1+\frac{\sum_{k\in\mathcal{T}}P_k}{1+\sum_{k\in\mathcal{T}^c}P_k}\right)-\log\left(1+\frac{\sum_{k\in\mathcal{T}}h_kP_k}{1+\sum_{k\in\mathcal{T}^c}h_kP_k}\right)\right] \tag{76}$$

$$\equiv\min_{\mathcal{T}\subseteq\mathcal{K},\mathbf{P}\in\mathcal{P}}\frac{\phi_{\mathcal{K}}(\mathbf{P})}{\phi_{\mathcal{T}^c}(\mathbf{P})} \tag{77}$$

where we recall that $\phi_{\mathcal{S}}(\mathbf{P})$ is given by (59), such that

$$\phi_{\mathcal{K}}(\mathbf{P}) = \frac{1+\sum_{k\in\mathcal{K}} h_k P_k}{1+\sum_{k\in\mathcal{K}} P_k} \tag{78}$$

$$\phi_{\mathcal{T}^c}(\mathbf{P}) = \frac{1+\sum_{k\in\mathcal{T}^c} h_k P_k}{1+\sum_{k\in\mathcal{T}^c} P_k}. \tag{79}$$

To see that a user should not be splitting its power among jamming and transmitting, it is sufficient to note that regardless of how a user splits its power, $\phi_{\mathcal{K}}(\mathbf{P})$ will be the same, and the user only affects $\phi_{\mathcal{T}^c}(\mathbf{P})$. Assume the optimum solution is such that user j splits its power, so $j \in \mathcal{T}$ and $j \in \mathcal{T}^c$. Then, it is easy to see that if $h_j < \phi_{\mathcal{T}^c}(\mathbf{P}^*)$, the sum rate is increased when that user uses its jamming power to transmit, and when $h_j > \phi_{\mathcal{T}^c}(\mathbf{P}^*)$, the sum rate is increased when the user uses its transmit power to jam. When $h_j = \phi_{\mathcal{T}^c}(\mathbf{P}^*)$, then regardless of how its power is split, the sum rate is the same, and we can assume user j either transmits or jams.

Note that we must have $\phi_{\mathcal{K}}(\mathbf{P}) \le \phi_{\mathcal{T}^c}(\mathbf{P})$ to have a nonzero secrecy sum rate, and $\phi_{\mathcal{T}^c}(\mathbf{P}) > 1$ to have an advantage over not jamming. This scheme can be shown to achieve the following secrecy sum rate.

Theorem 5: The secrecy sum rate using cooperative jamming is

$$R_{sum}^{\text{SUP-MA-CJ}} = \frac{1}{2}\log\left(1+\frac{\sum_{k\in\mathcal{T}} P_k^*}{1+\sum_{k\in\mathcal{T}^c} P_k^*}\right) - \frac{1}{2}\log\left(1+\frac{\sum_{k\in\mathcal{T}} h_k P_k^*}{1+\sum_{k\in\mathcal{T}^c} h_k P_k^*}\right) \tag{80}$$

where $\mathcal{T}$ is the set of transmitters and the optimum power allocation is of the form

$$\underbrace{\{\underbrace{1,\ldots,T}_{P_k^*=\bar{P}_k},\underbrace{T+1,\ldots,J-1}_{P_k^*=0},}_{\text{transmitting, i.e.,}k\in\mathcal{T}}\underbrace{\underbrace{J}_{P_J^*},\underbrace{J+1,\ldots,K}_{P_k^*=\bar{P}_k}\}}_{\text{jamming, i.e.,}k\in\mathcal{T}^c}$$

with

$$P_J^* = \left[\min\left\{\bar{P}_J, \frac{-c_2+\sqrt{c_2^2-4c_1c_3}}{2c_1}\right\}\right]^+ \tag{81}$$

and

$$c_1 = h_J\left(h_J\sum_{k\in\mathcal{T}} P_k^* - \sum_{k\in\mathcal{T}} h_k P_k^*\right) \tag{82}$$

$$c_2 = h_J\left(2+\sum_{k\in\mathcal{K}\setminus J} h_k P_k^* + \sum_{k\in\mathcal{T}^c\setminus J} h_k P_k^*\right)\sum_{k\in\mathcal{T}} P_k^* - h_J\left(2+\sum_{k\in\mathcal{K}\setminus J} P_k^* + \sum_{k\in\mathcal{T}^c\setminus J} P_k^*\right)\sum_{k\in\mathcal{T}} h_k P_k^* \tag{83}$$

$$c_3 = \left(1+\sum_{k\in\mathcal{K}\setminus J} h_k P_k^*\right)\left(1+\sum_{k\in\mathcal{T}^c\setminus J} h_k P_k^*\right)\sum_{k\in\mathcal{T}} P_k^* - h_J\left(1+\sum_{k\in\mathcal{K}\setminus J} P_k^*\right)\left(1+\sum_{k\in\mathcal{T}^c\setminus J} P_k^*\right)\sum_{k\in\mathcal{T}} h_k P_k^* \tag{84}$$

whenever the positive real root exists, and 0 otherwise.

Proof: We first solve the subproblem of finding the optimal power allocation for a set of given transmitters $\mathcal{T}$. The solution to this will also give us insight into the structure of the optimal set of transmitters $\mathcal{T}^*$. We start with writing the Lagrangian

$$\mathcal{L}(\mathbf{P},\boldsymbol{\mu}) = \frac{\phi_{\mathcal{K}}(\mathbf{P})}{\phi_{\mathcal{T}^c}(\mathbf{P})} - \sum_{k=1}^{K}\mu_{1k}P_k + \sum_{k=1}^{K}\mu_{2k}(P_k-\bar{P}_k). \tag{85}$$

The derivative of the Lagrangian depends on the user

$$0 = \frac{\partial\mathcal{L}(\mathbf{P}^*,\boldsymbol{\mu})}{\partial P_j^*} = \begin{cases} \frac{\dot{\phi}_{\mathcal{K}}^{(j)}(\mathbf{P}^*)}{\phi_{\mathcal{T}^c}(\mathbf{P}^*)} - \mu_{1j} + \mu_{2j}, & \text{if } j\in\mathcal{T} \\ \frac{\dot{\phi}_{\mathcal{K}}^{(j)}(\mathbf{P}^*)\phi_{\mathcal{T}^c}(\mathbf{P}^*) - \phi_{\mathcal{K}}(\mathbf{P}^*)\dot{\phi}_{\mathcal{T}^c}^{(j)}(\mathbf{P}^*)}{\phi_{\mathcal{T}^c}^2(\mathbf{P}^*)} + \mu_{2j}, & \text{if } j\in\mathcal{T}^c \end{cases} \tag{86}$$

since a user $j \in \mathcal{T}^c$ satisfies $P_j^* > 0$, it must have $\mu_{1j} = 0$.

Consider a user $j \in \mathcal{T}$. The same argument as in the sum-rate maximization proof leads to $P_j^* = \bar{P}_j$ if $h_j < \phi_{\mathcal{K}}(\mathbf{P}^*)$ and $P_1^* = 0$ if $h_j \ge \phi_{\mathcal{K}}(\mathbf{P}^*)$. Now examine a user $j \in \mathcal{T}^c$. We can write (86) as

$$\frac{\rho_j(\mathbf{P}^*)}{\left(1+\sum_{k\in\mathcal{K}} P_k\right)^2\left(1+\sum_{k\in\mathcal{T}^c} h_k P_k\right)^2} + \mu_{2j} = 0 \tag{87}$$

where

$$\rho_j(\mathbf{P}) \triangleq -h_j\left(1+\sum_{k\in\mathcal{K}} P_k\right)\left(1+\sum_{k\in\mathcal{T}^c} P_k\right)\sum_{k\in\mathcal{T}} h_k P_k + \left(1+\sum_{k\in\mathcal{K}} h_k P_k\right)\left(1+\sum_{k\in\mathcal{T}^c} h_k P_k\right)\sum_{k\in\mathcal{T}} P_k. \tag{88}$$

Let

$$\Phi_{\mathcal{T}}(\mathbf{P}) \triangleq \phi_{\mathcal{K}}(\mathbf{P})\phi_{\mathcal{T}^c}(\mathbf{P})\frac{\sum_{k\in\mathcal{T}} P_k}{\sum_{k\in\mathcal{T}} h_k P_k}. \tag{89}$$

Then, we have $\rho_j(\mathbf{P}) \le 0$ iff $h_j \ge \Phi_{\mathcal{T}}(\mathbf{P})$, and $\rho_j(\mathbf{P}) \ge 0$ iff $h_j \le \Phi_{\mathcal{T}}(\mathbf{P})$. Thus, we again find that we must have $h_j \ge \Phi_{\mathcal{T}}(\mathbf{P}^*)$ for all $j \in \mathcal{T}^c$. Also, if $h_j > \Phi_{\mathcal{T}}(\mathbf{P}^*)$, then $P_j^* = \bar{P}_j$. Only if $h_j = \Phi_{\mathcal{T}}(\mathbf{P}^*)$, can we have $0 < P_j^* < \bar{P}_j$. Now, since $\phi_{\mathcal{T}^c}(\mathbf{P}^*) \ge \phi_{\mathcal{K}}(\mathbf{P}^*)$, we must have $\phi_{\mathcal{T}^c}(\mathbf{P}^*) \ge \phi_{\mathcal{K}}(\mathbf{P}^*) \ge \left(\sum_{k\in\mathcal{T}} h_k P_k^*\right) / \left(\sum_{k\in\mathcal{T}} P_k^*\right)$. Thus, we find that $\Phi_{\mathcal{T}}(\mathbf{P}^*) \ge \phi_{\mathcal{K}}(\mathbf{P}^*)$. Then, we know that for a given set of transmitters $\mathcal{T}$, the solution is such that all users $j \in \mathcal{T}$ transmit with power $\bar{P}_j$ if $h_j \le \phi_{\mathcal{K}}(\mathbf{P}^*)$. In the set of jammers $\mathcal{T}^c$, all users have $h_j \ge \Phi_{\mathcal{T}}(\mathbf{P}^*) \ge \phi_{\mathcal{T}^c}(\mathbf{P}^*) \ge \phi_{\mathcal{K}}(\mathbf{P}^*)$, and when this inequality is not satisfied with equality, the jammers jam with maximum power. If the equality is satisfied for some users j, their jamming powers can be found from solving $h_j = \Phi_{\mathcal{T}}(\mathbf{P}^*)$. By rearranging terms in (88), we note that the optimum power allocation for this user, call it user J, is found by solving the quadratic

$$\rho_J(\mathbf{P}^*) = c_1 P_J^{*2} + c_2 P_J^* + c_3 = 0 \tag{90}$$

the solution of which is given in (81).

Note that (90) defines an (upright) parabola. If the root given in (90) exists and is positive, then $P_J^* = \min \bar{P}_j, P_J^*$. This comes

from the fact that if $P_J^* > \bar{P}_J$, then $\rho_J(\mathbf{P}) < 0$ for all $0 < P_J < \bar{P}_J$, and we must have $\mu_{2J} > 0$. If, on the other hand, (90) gives a complex or negative solution, then the parabola does not intersect the P_J axis, and is always positive. Hence, $h_J < \Phi_{\mathcal{T}}(\mathbf{P}^*)$, and J does not belong to $\mathcal{T}^c$, i.e., $P_J^* = 0$.

The form of this solution is intuitively pleasing, since it makes more sense for "weaker" users to jam as they harm the eavesdropper more than they do the intended receiver. What we see is that all transmitting users j, such that $P_j^* > 0$, transmit with maximum power as long as their standardized channel gain h_j is less than some limit $\phi_{\mathcal{K}}(\mathbf{P}^*)$, and all jamming users must have $h_j > \phi_{\mathcal{K}}(\mathbf{P}^*)$.

We claim that all users in $\mathcal{T}^*$ must have $h_j < \Phi_{\mathcal{T}^*}(\mathbf{P}^*)$ and all users in $\mathcal{T}^{*c}$ have $h_j \geq \Phi_{\mathcal{T}^*}(\mathbf{P}^*)$. To make this argument, we need to show that a $\mathcal{T}$ such that there exists some $m \in \mathcal{T}$ with $P_m^* = 0$ and $n \in \mathcal{T}^c$ such that $h_m > h_n$ cannot be the optimum set. To see this, let P^* be the optimum power allocation for a set $\mathcal{T}$. Consider a new power allocation and set such that $\mathcal{U} = \mathcal{T} \setminus \{m\}$, i.e., user m is now jamming, and let $Q_k = P_k^*$, $\forall\, k \neq m, n$, $Q_m = \pi$ and $Q_n = P_n^* - \pi$, for some small π. We then have

$$\frac{\phi_{\mathcal{K}}(\mathbf{Q})}{\phi_{\mathcal{U}^c}(\mathbf{Q})} = \frac{1+\sum_{k\in\mathcal{K}} h_k Q_k}{1+\sum_{k\in\mathcal{K}} Q_k} \frac{1+\sum_{k\in\mathcal{U}^c} Q_k}{1+\sum_{k\in\mathcal{U}^c} h_k Q_k} \tag{91}$$

$$= \frac{1+\sum_{k\in\mathcal{K}} h_k P_k^* + (h_m - h_n)\pi}{1+\sum_{k\in\mathcal{K}} P_k^*} \times \frac{1+\sum_{k\in\mathcal{T}^c} P_k^*}{1+\sum_{k\in\mathcal{T}^c} h_k P_k^* + (h_m - h_n)\pi} \tag{92}$$

$$< \frac{1+\sum_{k\in\mathcal{K}} h_k P_k^*}{1+\sum_{k\in\mathcal{K}} P_k^*} \frac{1+\sum_{k\in\mathcal{T}^c} P_k^*}{1+\sum_{k\in\mathcal{T}^c} h_k P_k^*} \tag{93}$$

$$= \frac{\phi_{\mathcal{K}}(\mathbf{P}^*)}{\phi_{\mathcal{T}^c}(\mathbf{P}^*)} \tag{94}$$

which is a lower value for the objective function, proving that $(\mathcal{T}, P^*)$ is not optimum. This shows that all users $j \in \mathcal{T}^{*c}$ must have $h_j > h_k$ for all users $k \in \mathcal{T}^*$. Since the last user in $\mathcal{T}^{*c}$ has $h_j = \Phi_{\mathcal{T}^*}(\mathbf{P}^*)$, necessarily $h_j \geq \Phi_{\mathcal{T}^*}(\mathbf{P}^*)$ for all $j \in \mathcal{T}^{*c}$, and $h_j < \Phi_{\mathcal{T}^*}(\mathbf{P}^*)$ for all $j \in \mathcal{T}^*$.

Summarizing, the optimum power allocation is such that there is a set of transmitting users $\{1, \ldots, T\}$ with $P_k^* = \bar{P}_k$ for $k = 1, \ldots, T$, there is a set of silent users $\{T+1, \ldots, J-1\}$, and there is a set of jamming users $\{J, \ldots, K\}$ with $P_k^* = \bar{P}_k$ for $k = J+1, \ldots, K$ and P_J^* is found from $h_J = \Phi_{\mathcal{T}}(\mathbf{P}^*)$. This is what is presented in the statement in Theorem 5.

Note that to find T and J, we can simply do an exhaustive search as we have narrowed the number of possible optimal sets to $K(K-1)$ instead of $2^K - 1$ and found the optimal power allocations for each. □

Two-user GGMAC-WT: For illustration purposes, let us consider the familiar case with $K = 2$ transmitters. In this case, we know that either user 2 jams, or no user does. The solution can be found from comparing the two cases. If, without jamming, user 2 can transmit, then it is optimal for it to continue to transmit, and jamming will not improve the sum rate. Otherwise, user 2 may be jamming to improve the secrecy rate of user 1. The optimum power allocation for user 1 is equivalent to $P_1^* = \bar{P}_1$ if $h_1 < \phi_{\mathcal{K}}(\mathbf{P}^*)$ and $P_1^* = 0$ if $h_1 \geq \phi_{\mathcal{K}}(\mathbf{P}^*)$. The power for user 2 is found from (81). For two users, we can simply write (90) as

$$P_1^* h_2 (h_2 - h_1)(P_2^* - p)(P_2^* - \bar{p}) = 0 \tag{95}$$

where

$$p = \frac{-h_2(1-h_1) + \sqrt{D}}{h_2(h_2 - h_1)} \tag{96}$$

$$\bar{p} = \frac{-h_2(1-h_1) - \sqrt{D}}{h_2(h_2 - h_1)} \tag{97}$$

$$D = h_1 h_2 (h_2 - 1)[(h_2 - 1) + (h_2 - h_1)P_1^*]. \tag{98}$$

If $h_1 < 1$, we automatically have $P_1^* = \bar{P}_1$. In addition, we have $\bar{p} < 0$, so we only need to concern ourselves with the possibly positive root p. We first find when $P_2^* = 0$. We see that $\rho_2(\mathbf{P}) \geq 0$ for all $\mathbf{P} \in \mathcal{P}$ if $p < 0$, equivalent to having two negative roots, or $D < 0 \Rightarrow h_2 \leq \phi_1(\bar{P}_1)$, equivalent to having no real roots of $\rho_2(\mathbf{P})$. Now examine when $0 < P_2^* < \bar{P}_2$. This is possible if and only if $\rho_2(\mathbf{P}^*) = 0$. Since $P_1^* > 0$, this happens only when $h_1 = h_2$ or $P_2^* = p > 0$. However, if $h_1 = h_2$, we are better off transmitting than jamming. The last case to examine is when $P_2^* = \bar{P}_2$. This implies that $\rho_2(\bar{\mathbf{P}}) < 0$, and it is satisfied when $p > \bar{P}_2$.

Assume $h_2 > h_1 \geq 1$. In this case, we are guaranteed $p \geq 0$. If $P_1^* = 0$, then we must have $P_2^* = 0$ since the secrecy rate is 0. We would like to find when we can have $P_1^* > 0$. Since $h_1 < \phi_2(P_2^*)$, we must have $P_2^* > \frac{h_1 - 1}{h_2 - h_1} \geq 0$, and $\rho_2(\bar{P}, P_2^*) \leq 0$. This implies $\bar{p} \leq P_2^* \leq p$. It is easy to see that $P_2^* = \min\{p, \bar{P}_2\}$ if $\frac{h_1-1}{h_2-h_1} < \min\{p, \bar{P}_2\}$ and $P_2^* = 0$ otherwise.

Thus, for $K = 2$ users, the solution simplifies to (99) shown at the bottom of the page, where

$$p = \frac{h_1 - 1}{h_2 - h_1} + \frac{\sqrt{h_1 h_2 (h_2 - 1)\left[(h_2 - 1) + (h_2 - h_1)\bar{P}_1\right]}}{h_2(h_2 - h_1)}. \tag{100}$$

This solution can be checked to be in accordance with the sum-rate maximizing power allocation of Theorem 3. We note that in the case unaccounted for in (99), i.e., when $h_1 \leq 1$ and $h_2 \leq \frac{1+h_1\bar{P}_1}{1+\bar{P}_1}$, both users should be transmitting. In general, the solution shows that the "weaker" user should jam if it is not

$$(P_1^*, P_2^*) = \begin{cases} (\bar{P}_1, 0), & \text{if } h_1 \leq 1,\ \frac{1+h_1\bar{P}_1}{1+\bar{P}_1} \leq h_2 \leq 1 \\ \left(\bar{P}_1, \left[\min\{p, \bar{P}_2\}\right]^+\right), & \text{if } h_2 > 1 \geq h_1 \\ (0, 0), & \text{if } h_2 > h_1 \geq 1,\ \frac{h_1-1}{h_2-h_1} \geq \bar{P}_1 \\ (\bar{P}_1, \min\{p, \bar{P}_2\}), & \text{if } h_2 > h_1 \geq 1,\ \frac{h_1-1}{h_2-h_1} < \bar{P}_1. \end{cases} \tag{99}$$

single-user decodable, and if it has enough power to make the other user "strong" in the new effective channel.

B. GTW-WT

Once again, we propose to maximize the secrecy sum rate using cooperative jamming when useful. This problem is formally stated as follows:

$$\max_{\substack{\mathcal{T}\subseteq\mathcal{K},\\ \mathbf{P}\in\mathcal{P}}} \frac{1}{2}\left[\sum_{k\in\mathcal{T}}\log\left(P_k\right)-\log\left(1+\frac{\sum_{k\in\mathcal{T}}h_kP_k}{1+\sum_{k\in\mathcal{T}^c}h_kP_k}\right)\right] \equiv \min_{\mathcal{T}\subseteq\mathcal{K}}\min_{\mathbf{P}\in\bar{\mathcal{P}}}\frac{\psi_{\mathcal{K}}(\mathbf{P})}{\psi_{\mathcal{T}^c}(\mathbf{P})} \quad (101)$$

where we recall that $\psi_{\mathcal{S}}(\mathbf{P})$ is given by (71) and

$$\psi_{\mathcal{K}}(\mathbf{P})=\frac{1+\sum_{k\in\mathcal{K}}h_kP_k}{\prod_{k\in\mathcal{K}}(1+P_k)} \quad (102)$$

$$\psi_{\mathcal{T}^c}(\mathbf{P})=\frac{1+\sum_{k\in\mathcal{T}^c}h_kP_k}{\prod_{k\in\mathcal{T}^c}(1+P_k)}. \quad (103)$$

Note that $\mathcal{K}=\{1,2\}$ since there are only two terminals. A similar argument to the GGMAC-WT case can easily be used to establish that we can assume a user to be either transmitting or jamming, but not both. Since the jamming user is also the receiver that the other user is communicating with and knows the transmitted signal, this scheme entails no loss of capacity as far as the transmitting user is concerned. The optimum power allocations are given as follows.

Theorem 6: The achievable secrecy sum rate for the collaborative scheme described is

$$R_{sum}^{\text{TW-CJ}}=\sum_{k\in\mathcal{T}}\frac{1}{2}\log\left(P_k^*\right)-\frac{1}{2}\log\left(1+\frac{\sum_{k\in\mathcal{T}}h_kP_k^*}{1+\sum_{k\in\mathcal{T}^c}h_kP_k^*}\right) \quad (104)$$

where $\mathcal{T}$ is the set of transmitting users and the optimum power allocations are given by (105) shown at the bottom of the page.

Proof: Similar to the GGMAC-WT, we start with the subproblem of finding the optimal power allocation given a jamming set. The Lagrangian is given by

$$\mathcal{L}(\mathbf{P},\boldsymbol{\mu})=\frac{\psi_{\mathcal{K}}(\mathbf{P})}{\psi_{\mathcal{T}^c}(\mathbf{P})}-\sum_{k=1}^{2}\mu_{1k}P_k+\sum_{k=1}^{2}\mu_{2k}(P_k-\bar{P}_k). \quad (106)$$

Taking the derivative we have

$$0=\frac{\partial\mathcal{L}(\mathbf{P}^*,\boldsymbol{\mu})}{\partial P_j^*} =\begin{cases}\frac{\dot{\psi}_{\mathcal{K}}^{(j)}(\mathbf{P}^*)}{\psi_{\mathcal{T}^c}(\mathbf{P}^*)}-\mu_{1j}+\mu_{2j}, & \text{if } j\in\mathcal{T}\\ \frac{\dot{\psi}_{\mathcal{K}}^{(j)}(\mathbf{P}^*)\psi_{\mathcal{T}^c}(\mathbf{P}^*)-\psi_{\mathcal{K}}(\mathbf{P}^*)\dot{\psi}_{\mathcal{T}^c}^{(j)}(\mathbf{P}^*)}{\psi_{\mathcal{T}^c}^2(\mathbf{P}^*)}+\mu_{2j}, & \text{if } j\in\mathcal{T}^c\end{cases} \quad (107)$$

since a user $j\in\mathcal{T}^c$ satisfies $P_j^*>0$, it must have $\mu_{1j}=0$.

Consider user $j\in\mathcal{T}$. We again argue that if $h_j>\frac{1+\sum_{k\in\mathcal{K}}h_kP_k}{1+\bar{P}_j}$, then $P_j^*=0$ and if $h_j<\frac{1+\sum_{k\in\mathcal{K}}h_kP_k}{1+\bar{P}_j}$, then $P_j^*=\bar{P}_j$. Now examine a user $j\in\mathcal{T}^c$. It is easy to see that since such a user only harms the jammer, the optimal jamming strategy should have $P_j^*=\bar{P}_j$, i.e., the maximum power. This can also be seen by noting that (107) for this case simplifies to

$$\frac{-h_j\sum_{k\in\mathcal{T}}h_kP_k^*}{\left(1+\sum_{k\in\mathcal{T}^c}h_kP_k^*\right)^2\left(\prod_{k\in\mathcal{K}}(1+P_k^*)\right)^2}+\mu_{2j}=0 \quad (108)$$

and hence we must have $\mu_{2j}>0\Rightarrow P_j^*=\bar{P}_j$ for all $j\in\mathcal{T}^c$.

The jamming set will be one of $\emptyset,\{1\},\{2\}$, since there is no point in jamming when there is no transmission. Also, if any of the two users is jamming, by the argument above, $P_j^*=\bar{P}_j$, $j=1,2$. We can easily see that jamming by a user j only offers an advantage if $h_j>1$, i.e., $\psi_{\mathcal{T}^c}(\mathbf{P})>1$ iff $h_j>1$ for $j\in\mathcal{T}^c$. Thus, when $h_1<h_2\leq 1$, both users should be transmitting instead of jamming. However, when any user has $h_j>1$, jamming always does better than the case when both users are transmitting. In this case, $\psi_j(\bar{\mathbf{P}})\geq\psi_{j^c}(\bar{\mathbf{P}})$ for some user j, and the objective function in (101) is minimized when this user is jamming, and the other one is transmitting. If, however, $h_{j^c}>1+h_j\bar{P}_j$, then it will not transmit, and we should not be jamming. Consolidating all of these results, we come up with the power allocation in Theorem 6. □

Remark 4: A sufficient, but not necessary condition for the weaker user to be the jamming user is if $h_2\bar{P}_2>h_1\bar{P}_1$; this case corresponds to having higher signal-to-noise ratio (SNR) at the eavesdropper for the original, nonstandardized model. This can be interpreted as "jam with maximum power if it is possible to change user 1's effective channel gain such that it is no longer single-user decodable." For the simple case of equal power constraints $\bar{P}_1=\bar{P}_2=\bar{P}$, it is easily seen that user 1 should never be jamming. The optimal power allocation in that case reduces to

$$(P_1^*,P_2^*)=\begin{cases}(\bar{P},\bar{P}),\ \text{both transmit}, & \text{if } h_1<h_2\leq 1\\ (\bar{P},\bar{P}),\ 1\text{ transmits},\ 2\text{ jams}, & \text{if } h_1<1+h_2\bar{P}\\ (0,0), & \text{otherwise.}\end{cases} \quad (109)$$

VI. Numerical Results

In this section, we present numerical results to illustrate the achievable rates obtained, as well as the cooperative jamming scheme and its effect on achievable secrecy sum rates.

As mentioned earlier in this paper, examples of achievable secrecy rate regions are given in Figs. 4 and 6 for the GGMAC-WT with $K=2$ and GTW-WT, respectively. Comparing Figs. 4 and 6, we see that the GTW-WT achieves a larger secrecy rate region

$$(P_1^*,P_2^*)=\begin{cases}(\bar{P}_1,\bar{P}_2),\ \text{both transmit}, & \text{if } h_1<h_2\leq 1\\ (\bar{P}_1,\bar{P}_2),\ 1\text{ transmits},\ 2\text{ jams}, & \text{if } h_1\leq 1<h_2\\ (\bar{P}_1,\bar{P}_2),\ 1\text{ transmits},\ 2\text{ jams}, & \text{if } 1<h_1<1+h_2\bar{P}_2,\ \psi_2(\bar{\mathbf{P}})>\psi_1(\bar{\mathbf{P}})\\ (\bar{P}_1,\bar{P}_2),\ 2\text{ transmits},\ 1\text{ jams}, & \text{if } 1<h_1<h_2<1+h_1\bar{\mathbf{P}}_1,\psi_1(\bar{\mathbf{P}})>\psi_2(\bar{\mathbf{P}})\\ (0,0), & \text{otherwise.}\end{cases} \quad (105)$$

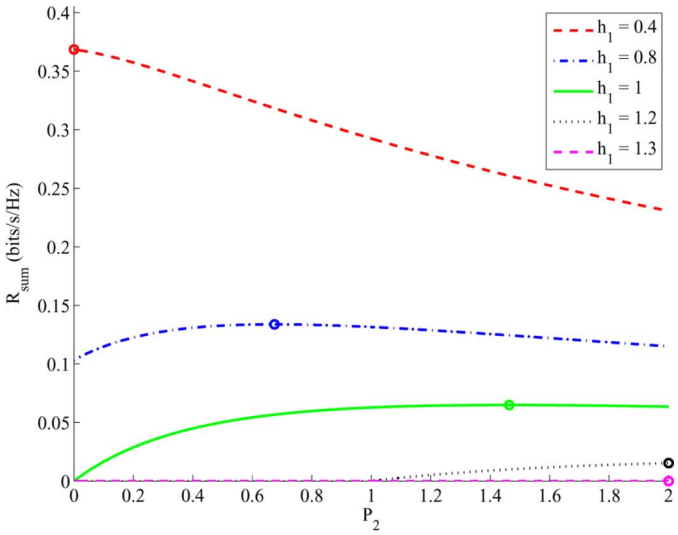

Fig. 7. GGMAC-WT cooperative jamming secrecy sum rate as a function of P_2 with different h_1 for $\bar{P}_1 = \bar{P}_2 = 2$ and $h_2 = 1.4$. The circles indicate optimum jamming power.

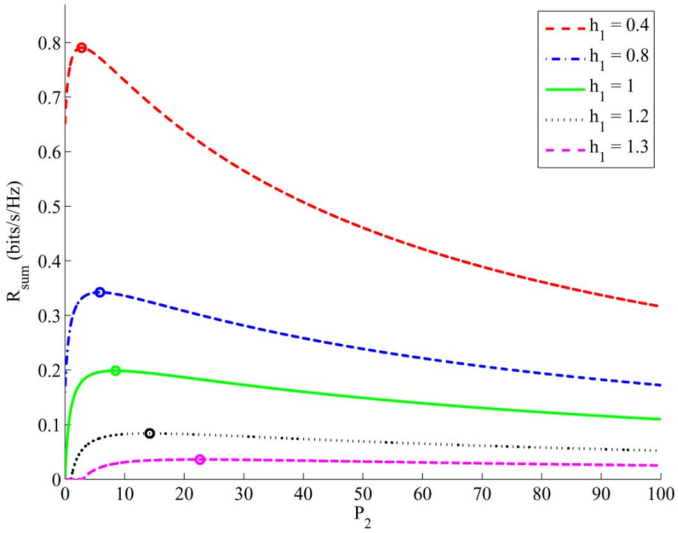

Fig. 8. GGMAC-WT cooperative jamming secrecy sum rate as a function of P_2 with different h_1 for $\bar{P}_1 = \bar{P}_2 = 100$ and $h_2 = 1.4$. The circles indicate optimum jamming power.

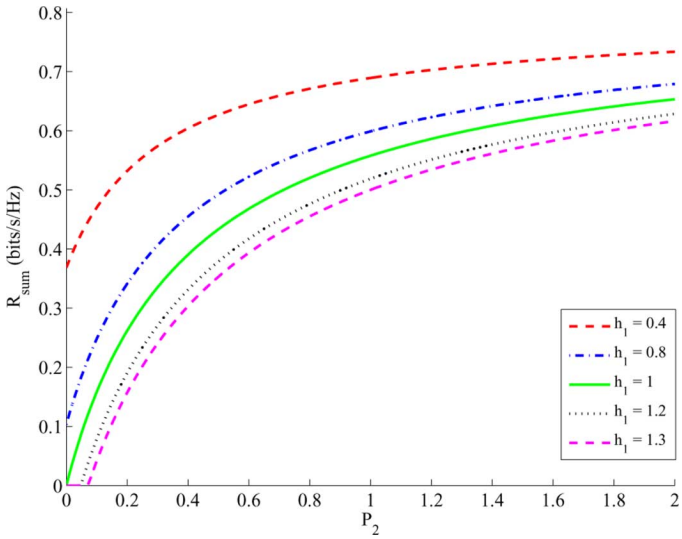

Fig. 9. GTW-WT cooperative jamming secrecy sum rate as a function of P_2 with different h_1 for $\bar{P}_1 = \bar{P}_2 = 2$ and $h_2 = 4.2$.

than the GGMAC-WT, and offers more protection to "weak" users. In addition, TDMA does not enlarge the achievable region for GTW-WT since superposition coding always allows users to achieve their single-user secrecy rates for any transmit power.

Let us have a closer look at the secrecy advantage of the two-way channel over the MAC with two users. For the GGMAC-WT with $K = 2$, the achievable maximum secrecy sum rate $R_1^s + R_2^s$ is limited by the channel parameters. It was shown in [39] that for the degraded case $h \leq 1$, the secrecy sum capacity $C_{\mathcal{K}}^{\mathrm{M}}(\mathbf{P}) - C_{\mathcal{K}}^{\mathrm{W}}(\mathbf{P})$ is an increasing function of the total sum power $\bar{P}_\Sigma = \bar{P}_1 + \bar{P}_2$. However, it is limited since $C_{\mathcal{K}}^{\mathrm{M}}(\mathbf{P}) - C_{\mathcal{K}}^{\mathrm{W}}(\mathbf{P}) \to -\frac{1}{2}\log h$ as $\bar{P}_\Sigma \to \infty$. For the general case, where $\bar{P}_1, \bar{P}_2 \to \infty$, Theorem 3 implies that the sum rate is maximized when only user 1 transmits (assuming $h_2 > h_1$), and is bounded similarly by $-\frac{1}{2}\log h_1$. On the other hand, for the GTW-WT, unlike the GGMAC-WT, it is possible to increase the secrecy capacity by increasing the transmit powers. This mainly stems from the fact that the users now have the extra advantage over the eavesdropper that they know their own transmitted codewords. In effect, each user helps encrypt the other user's transmission. To see this more clearly, consider the symmetric case where $\alpha_1 = \alpha_2 = h_1 = h_2 = 1$ and $\bar{P}_1 = \bar{P}_2 = \bar{P}$, which makes all users receive a similarly noisy version of the same sum message. The only disadvantage the eavesdropper has is that he does not know any of the codewords whereas user k knows $\mathbf{X}_k$. In this case, $R_1^s + R_2^s \leq \frac{1}{2}\log\left(1 + \bar{P}^2/(1+2\bar{P})\right)$ is achievable, and this rate approaches $\frac{1}{2}\log(\frac{1}{2}\bar{P})$ as $\bar{P} \gg 1$. Thus, it is possible to achieve a secrecy rate increase at the same rate as the increase in channel capacity.

Next, we examine the secrecy sum-rate maximizing power allocations and optimum powers for the cooperative jamming scheme. Figs. 7 and 8 show the achievable secrecy rate improvement for the cooperative jamming scheme for various channel parameters for the GGMAC-WT with $K = 2$. The plots are the secrecy rates for user 1 when user 2 is jamming with a given power, which correspond to user 1's single-user secrecy *capacity* [12], since only one user is transmitting. When $h_1 \geq 1$, the secrecy capacity is seen to be zero, unless user 2 has enough power to *convert* user 1's restandardized channel gain to less than 1. For the GTW-WT, it is always optimal for user 2 to jam as long as it enables user 1 to transmit, as seen in Fig. 9. The results show, as expected, that secrecy is achievable for both users so long as we can keep the eavesdropper from single-user decoding the transmitted codewords by treating the remaining user as noise.

Since the coding schemes considered here assume knowledge of eavesdropper's channel gains, applications are limited. One practical application could be securing of a physically protected area such as inside a building, when the eavesdropper is known to be outside. In such a case, we can design for the worst case scenario. An example is given in Fig. 10 for the GGMAC-WT, where we assume a simple path-loss model and fixed locations for two transmitters (T) and one receiver (R) at the center. We

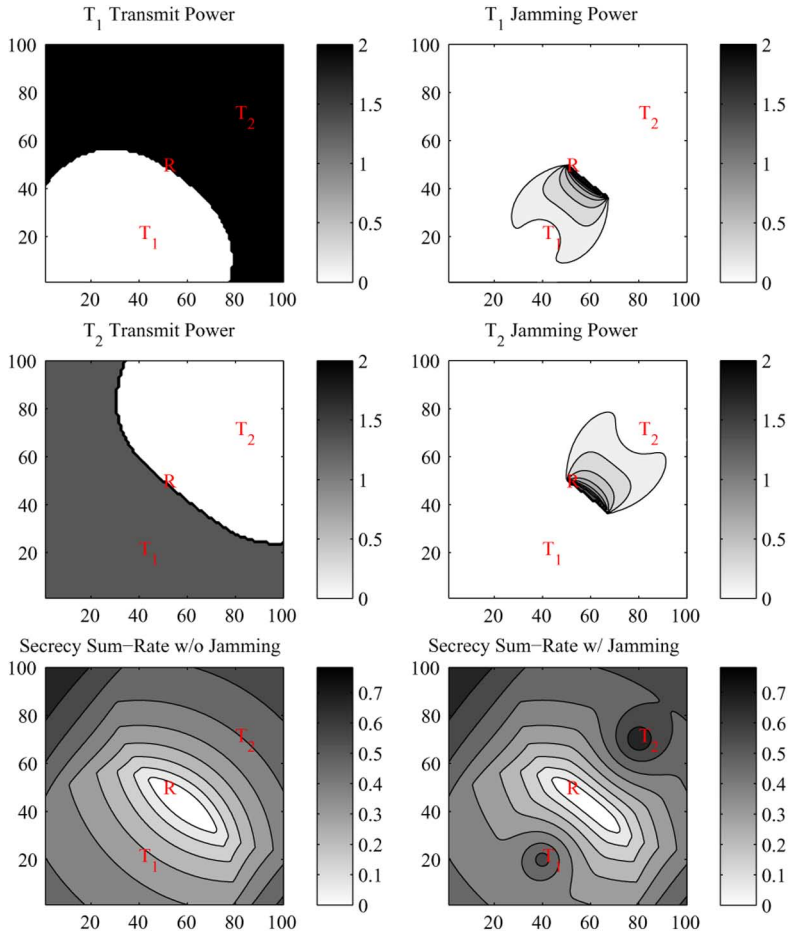

Fig. 10. GGMAC-WT cooperative jamming example—darker shades correspond to higher values.

examine the transmit/jam powers for this area when the eavesdropper is known to be at (x, y) using a fixed path-loss model for the channel gains, and plot the transmit/jam powers and the achieved secrecy sum rates as a function of the eavesdropper location. It is readily seen that when the eavesdropper is close to the BS, the secrecy sum rate falls to zero. Also, when the eavesdropper is in the vicinity of a transmitter, that transmitter cannot transmit in secrecy. However, in this case, the transmitter can jam the eavesdropper effectively and allow the other transmitter to transmit and/or increase its secrecy rate with little jamming power. The situation for the GTW-WT is similar and is shown in Fig. 11. In this case, jamming is more useful as compared to the GGMAC-WT, and we see that it is possible to provide secrecy for a much larger area where the eavesdropper is located, as the jamming signal does not hurt the intended receiver.

VII. Conclusion and Future Work

In this paper, we have considered the Gaussian multiple-access and two-way channels in the presence of an external eavesdropper who receives the transmitted signals through a multiple-access channel, and provided achievable secrecy rates. We have shown that the multiple-access nature of the channels considered can be utilized to improve the secrecy of the system. In particular, we have shown that the total extra randomness is what matters mainly concerning the eavesdropper, rather than the individual randomness in the codes. As such, it may be possible for users whose single-user wiretap capacity are zero, to communicate with nonzero secrecy rate, as long as it is possible to put the eavesdropper at an *overall disadvantage*. This is even clearer for two-way channels, where even though the eavesdropper's channel gain may be better than a terminal's, the extra knowledge of its own codeword by that terminal enables communication in perfect secrecy as long as the eavesdropper's received signal is not strong enough to allow single-user decoding.

We found achievable secrecy rate regions for the GGMAC-WT and the GTW-WT. We also showed that for the GGMAC-WT the secrecy sum rate is maximized when only users with "strong" channels to the intended receiver as opposed to the eavesdropper transmit, and they do so using all their available power. For the GTW-WT, the sum rate is maximized when both terminals transmit with maximum power as long as the eavesdropper's channel is not good enough to decode them using single-user decoding.

Finally, we proposed a scheme termed *cooperative jamming*, where a disadvantaged user may help improve the secrecy rate by jamming the eavesdropper. We found the optimum power allocations for the transmitting and jamming users, and we showed that significant rate gains may be achieved, especially when the eavesdropper has much higher SNR than the receivers

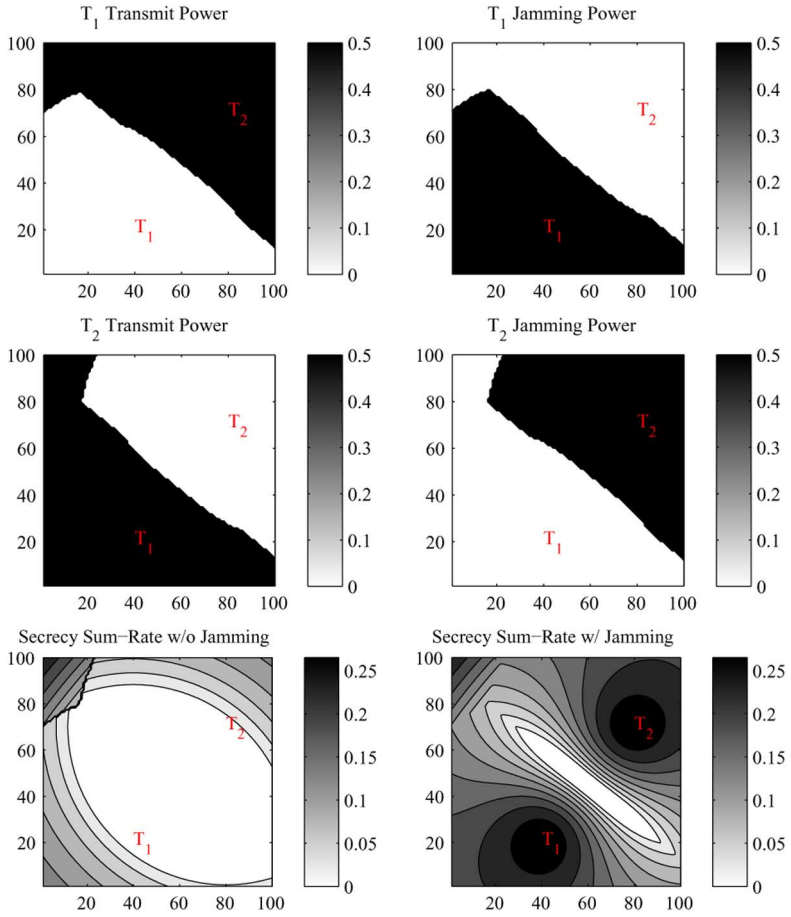

Fig. 11. GTW-WT cooperative jamming example—darker shades correspond to higher values.

and normal secret communications is not possible. The gains can be significant for both the GGMAC-WT and the GTW-WT. This cooperative behavior is useful when the maximum secrecy sum rate is of interest. We have also contrasted the secrecy rates of the two channels we considered, noting the benefit of the two-way channels where the fact that each receiver has perfect knowledge of its transmitted signal brings an advantage with each user effectively encrypting the communications of the other user.

In this paper, we only presented achievable secrecy rates for the GGMAC-WT and the GTW-WT. The secrecy capacity region for these channels are still open problems. In [45], we also found an upper bound for the secrecy sum rate of the GGMAC-WT and noted that the achievable secrecy sum rate and the upper bound we found only coincide for the degraded case, so that we have the secrecy sum capacity for the degraded GMAC-WT. Even though there is a gap between the achievable secrecy sum rates and upper bounds, cooperative jamming was shown in [45] to give a secrecy sum rate that is close to the upper bound in general.

Finally, we note that the results provided are of mainly theoretical interest, since as of yet there are no currently known practical codes for multiple-access wiretap channels unlike the single-user case where in some cases practical codes have been shown to be useful for the wiretap channel [46], [47]. Furthermore, accurate estimates of the eavesdropper channel parameters are required for code design for wiretap channels where the channel model is quasi-static, as in our models considered in this paper.

REFERENCES

[1] R. Ahlswede, "Multi-way communication channels," in *Proc. 2nd. Int. Symp. Inf. Theory*, Tsahkadsor, Armenian S.S.R., 1971, pp. 23–52.
[2] H. Liao, "Multiple access channels," Ph.D. dissertation, Dept. Electr. Engr., Univ. Hawaii, Honolulu, HI, 1972.
[3] C. E. Shannon, "Two-way communication channels," in *Proc. 4th Berkeley Symp. Math. Statist. Probab.*, 1961, vol. 1, pp. 611–644.
[4] G. Dueck, "The capacity region of the two-way channel can exceed the inner bound," *Inf. Control*, no. 40, pp. 258–266, 1979.
[5] T. S. Han, "A general coding scheme for the two-way channel," *IEEE Trans. Inf. Theory*, vol. IT-30, no. 1, pp. 35–44, Jan. 1984.
[6] R. Ahlswede, "The capacity region of a channel with two senders and two receivers," *Ann. Probab.*, vol. 2, no. 5, pp. 805–814, 1974.
[7] H. Sato, "Two-user communication channels," *IEEE Trans. Inf. Theory*, vol. IT-23, no. 3, pp. 295–304, May 1977.
[8] A. El Gamal and T. Cover, "Multiple user information theory," *Proc. IEEE*, vol. 68, no. 12, pp. 1466–1483, Dec. 1980.
[9] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, 1949.
[10] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, 1975.
[11] 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.
[12] 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.

[13] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.
[14] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Lecture Notes in Computer Science*. Berlin, Germany: Springer-Verlag, 2000, vol. 1807, pp. 351–368.
[15] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.
[16] 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.
[17] 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.
[18] 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.
[19] 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.
[20] U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels—Part II: The simulatability condition," *IEEE Trans. Inform. Theory*, vol. 49, no. 4, pp. 832–838, Apr. 2003.
[21] 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.
[22] 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.
[23] 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.
[24] 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.
[25] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3047–3061, Dec. 2004.
[26] 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.
[27] 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.
[28] Y. Oohama, "Coding for relay channels with confidential messages," in *Proc. IEEE Inf. Theory Workshop*, 2001, pp. 87–89.
[29] 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.
[30] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security—Part I: Theoretical aspects," *IEEE Trans. Inf. Theory*, accepted for publication.
[31] Y. Liang and V. Poor, "Secure communication over fading channels," in *Proc. Allerton Conf. Commun. Control Comput.*, Monticello, IL, Sep. 27–29, 2006.
[32] 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.
[33] 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.
[34] Y. Liang and V. Poor, "Generalized multiple access channels with confidential messages," *IEEE Trans. Inf. Theory*, accepted for publication.
[35] 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.
[36] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, submitted for publication.
[37] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Trans. Inf. Theory*, submitted for publication.
[38] E. Tekin, S. Şerbetli, and A. Yener, "On secure signaling for the Gaussian multiple access wire-tap channel," in *Proc. Asilomar Conf. Signal Syst. Comput.*, Asilomar, CA, Nov. 1, 2005, pp. 1747–1751.
[39] 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.
[40] E. Tekin and A. Yener, "The Gaussian multiple-access wire-tap channel," *IEEE Trans. Inf. Theory* [Online]. Available: http://arxiv.org/format/cs.IT/0605028, submitted for publication
[41] 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.
[42] E. Tekin and A. Yener, "Achievable rates for two-way wire-tap channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Nice, France, Jun. 24–29, 2007.
[43] A. B. Carleial, "Interference channels," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 1, pp. 60–70, Jan. 1978.
[44] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York: Wiley, 1991.
[45] E. Tekin and A. Yener, "Secrecy sum-rates for the multiple-access wire-tap channel with ergodic block fading," in *Proc. Allerton Conf. Commun. Control Comput.*, Monticello, IL, Sep. 26–28, 2007.
[46] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.
[47] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security—Part II: Practical implementation," *IEEE Trans. Inf. Theory*, accepted for publication.