Forty-Fifth Annual Allerton Conference
Allerton House, UIUC, Illinois, USA
September 26-28, 2007

Secrecy Sum-Rates for the Multiple-Access Wire-Tap Channel with Ergodic Block Fading

Ender Tekin
Wireless Communications and Networking Laboratory
Electrical Engineering Department
The Pennsylvania State University
University Park, PA 16802
tekin@psu.edu

Aylin Yener
Wireless Communications and Networking Laboratory
Electrical Engineering Department
The Pennsylvania State University
University Park, PA 16802
yener@ee.psu.edu

***Abstract*—We consider a two-user multiple-access wiretap channel that undergoes ergodic block fading. In this scenario, there are two users are communicating with a base station in the presence of an eavesdropper, who has access to the communications through a multiple-access channel. We assume independent fading for each block, and that the fading process is ergodic. We also assume that the channel gains are measured accurately and are available to each transmitter and the eavesdropper in advance. We find the sum-rate maximizing power allocations for this case, and compare this to the instantaneous power control sum-rate. We also give a numerical solution when we incorporate cooperative jamming, where a user is allowed to use part of its power to jam the eavesdropper. In addition, we present an outer bound to the general multiple-access wire-tap channel, which is shown to be tight only for the degraded case.**

I. Introduction

Wyner, in [1], defined the *wire-tap channel*, where there is a wire-tapper who has access to a degraded version of the intended receiver's signal. He found the region of all possible rate/equivocation pairs, and the existence of a *secrecy capacity*, C_s, the rate up to which it is possible to transmit zero information to the wire-tapper. Reference [2] extended this result to Gaussian channels. Later, Csiszár and Körner, [3], generalized Wyner's results to channels satisfying some weaker conditions than degradedness.

Gaussian multiple-access wire-tap (GMAC-WT) channels are considered in [4]–[8], where transmitters communicate with an intended receiver in the presence of an external wire-tapper. In [5], [6], we considered the case where the wire-tapper gets a degraded version of the signal at the legitimate receiver, and found the secrecy-sum capacity for the *collective* set of constraints using Gaussian codebooks and stochastic encoders. In [7], the general (non-degraded) GMAC-WT was considered, and an achievable rate region for perfect secrecy with collective secrecy measures was found. In this work, we also present an outer bound to this result.

In [9], a Gaussian channel was presented where both the receiver and transmitter know the instantaneous channel gains. Given a long-term power constraint and a stationary ergodic distribution on the channel gains, it was shown that a water-filling power allocation over the fading states, where transmission stopped during deep-fades was capacity-optimal. Knopp and Humblet examined the multiple-access case and showed that it was optimal for a single-user to be transmitting with a water-filling power allocation at any given time, [10]. Single-user wire-tap channels were examined from this perspective in [11], [12]. It was shown that in this case, the optimal power allocation is not water-filling, but takes a more complicated form.

This paper examines achievable sum-rates for the block-fading Gaussian multiple-access wire-tap channel (GMAC-WT). For the GMAC-WT, the capacity region is not yet known, but an achievable rate was given in [5], [6] for the case where the eavesdropper is a degraded version of the intended receiver, and generalized in [7]. It was also shown in [5], [6], that this scheme achieved the sum-capacity for the degraded GMAC-WT. In this paper, we first give an outer bound to the sum-capacity of the general GMAC-WT, which is shown to correspond with the achievable rates only for the degraded case. We then find the sum-rate maximizing power allocation for the GMAC-WT and compare it with the sum-rate maximizing instantaneous power control solution found in [7], [8]. We then examine the case where we utilize cooperative jamming, which was proposed in [7]. For this case, we give partial solutions to the optimal power allocation for some cases, and show how to find a numerical solution for the remaining cases. We see that utilizing cooperative jamming allows us to achieve a secrecy-sum rate close to the outer bound.

II. System Model and Problem Statement

We consider $K = 2$ users communicating with a receiver in the presence of a eavesdropper. Transmitter $k = 1, 2$ chooses a message W_k from a set of equally likely messages $\mathcal{W}_k = \{1, \ldots, M_k\}$. The messages are encoded using $(2^{nR_k}, n)$ codes into $\{X_k^n(W_k)\}$, where $R_k = \frac{1}{n}\log_2 M_k$. The encoded messages $\{\mathbf{X}_k\} = \{X_k^n\}$ are then transmitted, and the intended receiver and the eavesdropper each get a copy $\mathbf{Y} = Y^n$ and $\mathbf{Z} = Z^n$. The receiver decodes $\mathbf{Y}$ to get an estimate of the transmitted messages, $\hat{\mathbf{W}}$. We would like to communicate with the receiver with arbitrarily low probability of error, while maintaining perfect secrecy of the transmitted messages. The signals at the intended receiver and the eavesdropper are given by

$$\mathbf{Y} = \sum_{k=1}^{K} \sqrt{h_k^{\mathrm{M}}}\mathbf{X}_k + \mathbf{N}_{\mathrm{M}} \quad (1)$$

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

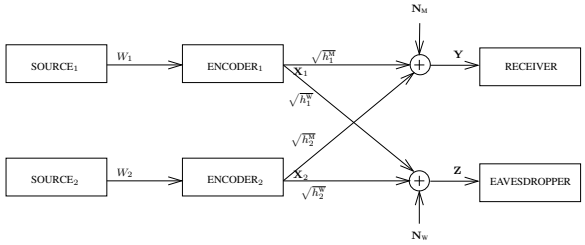

Fig. 1: Equivalent General Gaussian Multiple-Access Wire-Tap Channel (GGMAC-WT) system model.

where $\mathbf{N}_{\text{M}}, \mathbf{N}_{\text{W}}$ are the AWGN, and without loss of generality, we assume $\mathbf{N}_{\text{M}}, \mathbf{N}_{\text{W}} \sim \mathcal{N}(\mathbf{0}, \mathbf{I})$ and the following transmit power constraints:

$$\frac{1}{n}\sum_{i=1}^{n} X_{ki}^2 \leq \bar{P}_k, \ k = 1, 2 \tag{3}$$

We use the collective secrecy constraints defined in [4] to take into account the multi-access nature of the channel.

$$\Delta_{\mathcal{S}} \triangleq \frac{H(\mathbf{W}_{\mathcal{S}}|\mathbf{Z})}{H(\mathbf{W}_{\mathcal{S}})} \quad \forall \mathcal{S} \subseteq \mathcal{K} \triangleq \{1, \ldots, K\} \tag{4}$$

It was shown in [5] that guaranteeing the secrecy of all users is sufficient to guarantee the secrecy of all groups of users, i.e., $\frac{H(W_{\mathcal{S}}|\mathbf{Z})}{H(W_{\mathcal{S}})} \geq 1-\epsilon \Rightarrow \frac{H(W_{\mathcal{S}}|\mathbf{Z})}{H(W_{\mathcal{S}})} \geq 1-\epsilon$ for any $\mathcal{S} \subseteq \mathcal{K}$ of users.

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

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

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

$$\Delta_{\mathcal{S}} \geq 1 - \epsilon \quad \forall \mathcal{S} \subseteq \mathcal{K} = \{1, \ldots, K\} \tag{7}$$

where user k chooses one of M_k symbols to transmit according to the uniform distribution and P_e is the average probability of error.

III. Sum-Rates with Ergodic Fading

Theorem 1 (Achievable Rates): Let $\mathbf{h} = (h_1^{\text{M}}, h_2^{\text{M}}, h_1^{\text{W}}, h_2^{\text{W}})$ and $\mathrm{d}\mathbf{h} = \mathrm{d}h_1^{\text{M}}\mathrm{d}h_2^{\text{M}}\mathrm{d}h_1^{\text{W}}\mathrm{d}h_2^{\text{W}}$. Given a power control policy $\{P_k(\mathbf{h})\}_{k=1}^2$ satisfying

$$\int_0^\infty \int_0^\infty \int_0^\infty \int_0^\infty P_k(\mathbf{h}) p(\mathbf{h}) \mathrm{d}\mathbf{h} \leq \bar{P}_k \tag{8}$$

we can achieve the secrecy sum-rate

$$\frac{1}{2}\int_0^\infty \cdots \int \left[\log\left(\frac{\Phi^{\text{M}}}{\Phi^{\text{W}}}\right)\right]^+ p(\mathbf{h})\mathrm{d}\mathbf{h} \tag{9}$$

where $[x]^+ \triangleq \max x, 0$ and

$$\Phi^{\text{M}} = 1 + h_1^{\text{M}} P_1(\mathbf{h}) + h_2^{\text{M}} P_2(\mathbf{h}) \tag{10}$$

$$\Phi^{\text{W}} = 1 + h_1^{\text{W}} P_1(\mathbf{h}) + h_2^{\text{W}} P_2(\mathbf{h}) \tag{11}$$

The proof of this theorem is very similar to the proofs of the *Coding Theorem* in [9] and Theorem 1 in [12], and is therefore omitted. The only difference is that there are now 4 integrals to consider for the two-user scenario.

IV. Sum Rate Maximization

We are interested in finding the power allocation that will maximize the achievable sum-rate as described in Theorem 1. We can write the optimization problem as

$$\max_{P_1(\mathbf{h}), P_2(\mathbf{h})} \int_0^\infty \cdots \int \log\left(\frac{\Phi^{\text{M}}}{\Phi^{\text{W}}}\right) p(\mathbf{h})\mathrm{d}\mathbf{h} \tag{12}$$

$$\text{s.t.} \int_0^\infty \cdots \int P_k(\mathbf{h}) p(\mathbf{h})\mathrm{d}\mathbf{h} \leq \bar{P}_k, \quad k = 1, 2 \tag{13}$$

$$P_k(\mathbf{h}) \geq 0, \quad k = 1, 2 \tag{14}$$

We can then write the derivative of the Lagrangian as

$$\frac{\partial \mathcal{L}}{\partial P_k} = \frac{h_k^{\text{M}}}{\Phi^{\text{M}}} - \frac{h_k^{\text{W}}}{\Phi^{\text{W}}} - \lambda_k + \mu_k = 0, \quad k = 1, 2 \tag{15}$$

Note that we always have $1 + h_1^{\text{M}} P_1 + h_2^{\text{M}} P_2 \geq 1 + h_1^{\text{W}} P_1 + h_2^{\text{W}} P_2$ to have non-negative achievable rate. We can also see that the optimum powers will not violate this since we can just shut them down for these h_k values and achieve higher sum secrecy rate while obeying the power constraint. As a result, we can easily see that we have

$$\frac{\partial \mathcal{L}}{\partial P_k} = 0 \leq h_k^{\text{M}} - h_k^{\text{W}} - (\lambda_k - \mu_k)\Phi^{\text{M}}\Phi^{\text{W}}, \quad k = 1, 2 \tag{16}$$

$$\lambda_k - \mu_k \leq \frac{h_k^{\text{M}} - h_k^{\text{W}}}{\Phi^{\text{M}}\Phi^{\text{W}}} \leq h_k^{\text{M}} - h_k^{\text{W}} \tag{17}$$

and hence,

$$P_k = 0 \quad \text{if } h_k^{\text{M}} - h_k^{\text{W}} < \lambda_k \tag{18}$$

We are looking for the case when $P_k > 0$, i.e. assume $\mu_k = 0$. Consider user 1. We can write

$$\lambda_1 h_1^{\text{M}} h_1^{\text{W}} P_1^2 + \lambda_1 \bar{\theta}_1 P_1 + [\lambda_1 \psi_1 - \theta_1] = 0 \tag{19}$$

where we define

$$\theta_1 \triangleq h_1^{\text{M}}(1 + h_2^{\text{W}} P_2) - h_1^{\text{W}}(1 + h_2^{\text{M}} P_2) \tag{20}$$

$$\bar{\theta}_1 \triangleq h_1^{\text{M}}(1 + h_2^{\text{W}} P_2) + h_1^{\text{W}}(1 + h_2^{\text{M}} P_2) \tag{21}$$

$$\psi_1 \triangleq (1 + h_2^{\text{M}} P_2)(1 + h_2^{\text{W}} P_2) \tag{22}$$

Since we are only interested in the non-negative solution, we can write

$$P_1 = \frac{-\lambda_1\bar{\theta}_1 + \sqrt{\lambda_1^2\bar{\theta}_1^2 - 4\lambda_1^2 h_1^{\text{M}} h_1^{\text{W}} \psi_1 + 4\lambda_1 h_1^{\text{M}} h_1^{\text{W}} \theta_k}}{2\lambda_1 h_1^{\text{M}} h_1^{\text{W}}} \tag{23}$$

$$= \frac{-\lambda_1\bar{\theta}_1 + \sqrt{\lambda_1^2\theta_1^2 + 4\lambda_1 h_1^{\text{M}} h_1^{\text{W}} \theta_k}}{2\lambda_1 h_1^{\text{M}} h_1^{\text{W}}} \tag{24}$$

and proceeding similarly for user 2, we arrive at

$$P_k = \frac{-\lambda_k\bar{\theta}_k + \sqrt{\lambda_k^2\theta_k^2 + 4\lambda_k h_k^{\text{M}} h_k^{\text{W}} \theta_k}}{2\lambda_k h_k^{\text{M}} h_k^{\text{W}}}, \quad k = 1, 2 \tag{25}$$

where

$$\theta_2 \triangleq h_2^{\mathrm{M}}(1+h_1^{\mathrm{W}}P_1) - h_2^{\mathrm{W}}(1+h_1^{\mathrm{M}}P_1) \tag{26}$$

$$\bar{\theta}_2 \triangleq h_2^{\mathrm{M}}(1+h_1^{\mathrm{W}}P_1) + h_2^{\mathrm{W}}(1+h_1^{\mathrm{M}}P_1) \tag{27}$$

$$\psi_2 \triangleq (1+h_1^{\mathrm{M}}P_1)(1+h_1^{\mathrm{W}}P_1) \tag{28}$$

We note that if the optimum power for user k is positive,

$$\lambda_k^2\left(2h_k^{\mathrm{M}}h_k^{\mathrm{W}}P_k + \bar{\theta}_k\right)^2 = \lambda_k^2\theta_k^2 + 4\lambda_k h_k^{\mathrm{M}}h_k^{\mathrm{W}}\theta_k \tag{29}$$

$$\lambda_k(2h_k^{\mathrm{M}}\Phi^{\mathrm{W}})(2h_k^{\mathrm{W}}\Phi^{\mathrm{M}}) = 4h_k^{\mathrm{M}}h_k^{\mathrm{W}}\theta_k \tag{30}$$

$$\Psi \triangleq \Phi^{\mathrm{M}}\Phi^{\mathrm{W}} = \frac{\theta_k}{\lambda_k} \tag{31}$$

so that when both users have non-zero optimum power,

$$\frac{\theta_1}{\lambda_1} = \frac{\theta_2}{\lambda_2} = \Psi \tag{32}$$

Note that if $h_1^{\mathrm{W}} = h_2^{\mathrm{W}} = 0$, i.e. the no eavesdropper case, we would have $\theta_k = h_k^{\mathrm{M}}$ and this would simplify to

$$\frac{h_1^{\mathrm{M}}}{\lambda_1} = \frac{h_2^{\mathrm{M}}}{\lambda_2} \tag{33}$$

and since we have h_k^{M} drawn according to a continuous distribution, the probability of this event would be zero, implying that only one user should be transmitting, which is the solution found in [10]. However, in our case it is possible that the powers will satisfy this equality. We also easily verify from (31) that to have $P_k > 0$, we must have

$$\frac{\theta_k}{\psi_k} > \frac{\theta_k}{\Psi} = \lambda_k \tag{34}$$

Since $\Psi \geq \psi_k \geq 1$, $k = 1, 2$, if $\theta_k \leq 0$, we cannot have $P_k > 0$. We can also write the above result as:

$$P_1 > 0 \text{ iff } \frac{h_1^{\mathrm{M}}}{1+h_2^{\mathrm{M}}P_2} - \frac{h_1^{\mathrm{W}}}{1+h_2^{\mathrm{W}}P_2} > \lambda_1 \tag{35}$$

$$P_2 > 0 \text{ iff } \frac{h_2^{\mathrm{M}}}{1+h_1^{\mathrm{M}}P_1} - \frac{h_2^{\mathrm{W}}}{1+h_1^{\mathrm{W}}P_1} > \lambda_2 \tag{36}$$

WLOG, let $\frac{h_2^{\mathrm{M}}}{h_2^{\mathrm{W}}} < \frac{h_1^{\mathrm{M}}}{h_1^{\mathrm{W}}}$ and consider the four possibilities:

A. $h_1^M - h_1^W < \lambda_1$, $h_2^M - h_2^W < \lambda_2$

We showed earlier that $P_1 = P_2 = 0$.

B. $h_1^M - h_1^W \geq \lambda_1$, $h_2^M - h_2^W < \lambda_2$

We showed earlier that in this case $P_2 = 0$. Hence, we have $P_1 > 0$, and we can find P_1 from (25) which simplifies to:

$$P_1 = \frac{1}{2}\left[\sqrt{\left(\frac{\theta_1}{h_1^{\mathrm{M}}h_1^{\mathrm{W}}}\right)^2 + \frac{4}{\lambda_1}\frac{\theta_1}{h_1^{\mathrm{M}}h_1^{\mathrm{W}}}} - \frac{\bar{\theta}_1}{h_1^{\mathrm{M}}h_1^{\mathrm{W}}}\right] \tag{37}$$

$$= \frac{1}{2}\sqrt{\left(\frac{1}{h_1^{\mathrm{W}}} - \frac{1}{h_1^{\mathrm{M}}}\right)^2 + \frac{4}{\lambda_1}\left(\frac{1}{h_1^{\mathrm{W}}} - \frac{1}{h_1^{\mathrm{M}}}\right)} - \frac{1}{2}\left(\frac{1}{h_1^{\mathrm{W}}} + \frac{1}{h_1^{\mathrm{M}}}\right) \tag{38}$$

(38) is the solution given in [11], [12] for the single user case, also found by setting $h_2^{\mathrm{W}} = h_2^{\mathrm{M}} = 0$. This solution, as noted in [11], is not the standard water-filling solution. However, in the high SNR regime, in the sense that $\frac{1}{\lambda_1} \ll \frac{1}{h_1^{\mathrm{W}}} - \frac{1}{h_1^{\mathrm{M}}}$, we have

$$P_1 = \frac{1}{2}\left[\sqrt{\left(\frac{\theta_1}{h_1^{\mathrm{M}}h_1^{\mathrm{W}}}\right)^2 + \frac{4}{\lambda_1}\frac{\theta_1}{h_1^{\mathrm{M}}h_1^{\mathrm{W}}}} - \frac{\bar{\theta}_1}{h_1^{\mathrm{M}}h_1^{\mathrm{W}}}\right] \tag{39}$$

$$\approx \frac{1}{2}\left[\sqrt{\left(\frac{\theta_1}{h_1^{\mathrm{M}}h_1^{\mathrm{W}}}\right)^2 + \frac{4}{\lambda_1}\frac{\theta_1}{h_1^{\mathrm{M}}h_1^{\mathrm{W}}} + \frac{4}{\lambda_1^2}} - \frac{\bar{\theta}_1}{h_1^{\mathrm{M}}h_1^{\mathrm{W}}}\right] \tag{40}$$

$$= \frac{1}{2}\left[\frac{\theta_1}{h_1^{\mathrm{M}}h_1^{\mathrm{W}}} + \frac{2}{\lambda_1} - \frac{\bar{\theta}_1}{h_1^{\mathrm{M}}h_1^{\mathrm{W}}}\right] \tag{41}$$

$$= \frac{1}{\lambda_1} - \frac{1}{h_1^{\mathrm{M}}} \tag{42}$$

which is the well-known water-filling solution, [9]. Note that if $h_1^{\mathrm{W}} \to 0$, this is always true.

C. $h_1^M - h_1^W < \lambda_1$, $h_2^M - h_2^W \geq \lambda_2$

This can be treated the same way as the previous case. We have $P_1 = 0$, and

$$P_2 = \frac{1}{2}\left[\sqrt{\left(\frac{\theta_2}{h_2^{\mathrm{M}}h_2^{\mathrm{W}}}\right)^2 + \frac{4}{\lambda_2}\frac{\theta_2}{h_2^{\mathrm{M}}h_2^{\mathrm{W}}}} - \frac{\bar{\theta}_2}{h_2^{\mathrm{M}}h_2^{\mathrm{W}}}\right] \tag{43}$$

$$= \frac{1}{2}\sqrt{\left(\frac{1}{h_2^{\mathrm{W}}} - \frac{1}{h_2^{\mathrm{M}}}\right)^2 + \frac{4}{\lambda_2}\left(\frac{1}{h_2^{\mathrm{W}}} - \frac{1}{h_2^{\mathrm{M}}}\right)} - \frac{1}{2}\left(\frac{1}{h_2^{\mathrm{W}}} + \frac{1}{h_2^{\mathrm{M}}}\right) \tag{44}$$

D. $h_1^M - h_1^W \geq \lambda_1$, $h_2^M - h_2^W \geq \lambda_2$

In this case, it is easy to see that at least one user must be transmitting. We first examine the conditions and power allocations when both users should be transmitting:

We can write (32) as

$$\lambda_2[h_1^{\mathrm{M}}(1+h_2^{\mathrm{W}}P_2) - h_1^{\mathrm{W}}(1+h_2^{\mathrm{M}}P_2)] = \lambda_1[h_2^{\mathrm{M}}(1+h_1^{\mathrm{W}}P_1) - h_2^{\mathrm{W}}(1+h_1^{\mathrm{M}}P_1)] \tag{45}$$

which gives us

$$P_2 = \frac{\frac{\lambda_1}{\lambda_2}(h_2^{\mathrm{M}} - h_2^{\mathrm{W}}) - (h_1^{\mathrm{M}} - h_1^{\mathrm{W}})}{h_1^{\mathrm{M}}h_2^{\mathrm{W}} - h_2^{\mathrm{M}}h_1^{\mathrm{W}}} - \frac{\lambda_1}{\lambda_2}P_1 \tag{46}$$

$$P_1 = \frac{(h_2^{\mathrm{M}} - h_2^{\mathrm{W}}) - \frac{\lambda_2}{\lambda_1}(h_1^{\mathrm{M}} - h_1^{\mathrm{W}})}{h_1^{\mathrm{M}}h_2^{\mathrm{W}} - h_2^{\mathrm{M}}h_1^{\mathrm{W}}} - \frac{\lambda_2}{\lambda_1}P_2 \tag{47}$$

which can also be written as

$$\lambda_2 P_2 + \lambda_1 P_1 = \frac{\lambda_1(h_2^{\mathrm{M}} - h_2^{\mathrm{W}}) - \lambda_2(h_1^{\mathrm{M}} - h_1^{\mathrm{W}})}{h_1^{\mathrm{M}}h_2^{\mathrm{W}} - h_2^{\mathrm{M}}h_1^{\mathrm{W}}} \triangleq \Lambda \tag{48}$$

Note that we cannot have positive P_1, P_2 if

1) $h_1^{\mathrm{M}}h_2^{\mathrm{W}} - h_2^{\mathrm{M}}h_1^{\mathrm{W}} > 0$ and $\frac{h_1^{\mathrm{M}} - h_1^{\mathrm{W}}}{h_2^{\mathrm{M}} - h_2^{\mathrm{W}}} \geq \frac{\lambda_1}{\lambda_2}$.
2) $h_1^{\mathrm{M}}h_2^{\mathrm{W}} - h_2^{\mathrm{M}}h_1^{\mathrm{W}} < 0$ and $\frac{h_1^{\mathrm{M}} - h_1^{\mathrm{W}}}{h_2^{\mathrm{M}} - h_2^{\mathrm{W}}} \leq \frac{\lambda_1}{\lambda_2}$.

which means that our assumption that both users transmit is wrong, and only one user should actually be transmitting.

WLOG, assume $\frac{h_1^{\mathrm{M}}}{h_1^{\mathrm{W}}} \geq \frac{h_2^{\mathrm{M}}}{h_2^{\mathrm{W}}}$. Consider $\frac{h_1^{\mathrm{M}}-h_1^{\mathrm{W}}}{h_2^{\mathrm{M}}-h_2^{\mathrm{W}}} \geq \frac{\lambda_1}{\lambda_2}$. Assume user 2 is the transmitting user and user 1 is silent, i.e. $\frac{h_1^{\mathrm{M}}}{1+h_2^{\mathrm{M}}P_2} - \frac{h_1^{\mathrm{W}}}{1+h_2^{\mathrm{W}}P_2} \leq \lambda_1$ and $h_2^{\mathrm{M}} - h_2^{\mathrm{W}} > \lambda_2$. Then, we can write

$$h_1^{\mathrm{M}}(1+h_2^{\mathrm{W}}P_2) - h_1^{\mathrm{W}}(1+h_2^{\mathrm{M}}P_2) \leq \lambda_1(1+h_2^{\mathrm{M}}P_2)(1+h_2^{\mathrm{W}}P_2) \tag{49}$$

$$\frac{\theta_2}{\lambda_2} = \Psi \Rightarrow \frac{h_2^{\mathrm{M}} - h_2^{\mathrm{W}}}{\lambda_2} = (1+h_2^{\mathrm{M}}P_2)(1+h_2^{\mathrm{W}}P_2) \tag{50}$$

Combining the two, we get

$$\frac{h_2^{\mathrm{M}} - h_2^{\mathrm{W}}}{\lambda_2} \geq \frac{h_1^{\mathrm{M}}(1+h_2^{\mathrm{W}}P_2) - h_1^{\mathrm{W}}(1+h_2^{\mathrm{M}}P_2)}{\lambda_1} \geq \frac{h_1^{\mathrm{M}} - h_1^{\mathrm{W}}}{\lambda_1} \tag{51}$$

which violates the assumption that $\frac{h_1^{\mathrm{M}}-h_1^{\mathrm{W}}}{h_2^{\mathrm{M}}-h_2^{\mathrm{W}}} \geq \frac{\lambda_1}{\lambda_2}$. Thus, we see that only user 1 should be transmitting in this case.

We then consider the case $\frac{h_1^{\mathrm{M}}-h_1^{\mathrm{W}}}{h_2^{\mathrm{M}}-h_2^{\mathrm{W}}} < \frac{\lambda_1}{\lambda_2}$.

Substituting (47) into (31), after some algebra we can write

$$\begin{aligned}&(\lambda_1 h_2^{\mathrm{M}} - \lambda_2 h_1^{\mathrm{M}})[(h_1^{\mathrm{M}} - h_1^{\mathrm{W}}) + (h_1^{\mathrm{M}}h_2^{\mathrm{W}} - h_2^{\mathrm{M}}h_1^{\mathrm{W}})P_2] \\ &\quad \times (\lambda_1 h_2^{\mathrm{W}} - \lambda_2 h_1^{\mathrm{W}})[(h_1^{\mathrm{M}} - h_1^{\mathrm{W}}) + (h_1^{\mathrm{M}}h_2^{\mathrm{W}} - h_2^{\mathrm{M}}h_1^{\mathrm{W}})P_2] \\ &= \lambda_1(h_1^{\mathrm{M}}h_2^{\mathrm{W}} - h_2^{\mathrm{M}}h_1^{\mathrm{W}})^2[(h_1^{\mathrm{M}} - h_1^{\mathrm{W}}) + (h_1^{\mathrm{M}}h_2^{\mathrm{W}} - h_2^{\mathrm{M}}h_1^{\mathrm{W}})P_2]\end{aligned} \tag{52}$$

and since $(h_1^{\mathrm{M}} - h_1^{\mathrm{W}}) + (h_1^{\mathrm{M}}h_2^{\mathrm{W}} - h_2^{\mathrm{M}}h_1^{\mathrm{W}})P_2 > 0$, we get

$$\begin{aligned}&[(h_1^{\mathrm{M}} - h_1^{\mathrm{W}}) + (h_1^{\mathrm{M}}h_2^{\mathrm{W}} - h_2^{\mathrm{M}}h_1^{\mathrm{W}})P_2] \\ &\qquad = \frac{\lambda_1(h_1^{\mathrm{M}}h_2^{\mathrm{W}} - h_2^{\mathrm{M}}h_1^{\mathrm{W}})^2}{(\lambda_1 h_2^{\mathrm{M}} - \lambda_2 h_1^{\mathrm{M}})(\lambda_1 h_2^{\mathrm{W}} - \lambda_2 h_1^{\mathrm{W}})}\end{aligned} \tag{53}$$

which gives

$$P_2 = \frac{\lambda_1(h_1^{\mathrm{M}}h_2^{\mathrm{W}} - h_2^{\mathrm{M}}h_1^{\mathrm{W}})}{(\lambda_1 h_2^{\mathrm{M}} - \lambda_2 h_1^{\mathrm{M}})(\lambda_1 h_2^{\mathrm{W}} - \lambda_2 h_1^{\mathrm{W}})} - \frac{h_1^{\mathrm{M}} - h_1^{\mathrm{W}}}{h_1^{\mathrm{M}}h_2^{\mathrm{W}} - h_2^{\mathrm{M}}h_1^{\mathrm{W}}} \tag{54}$$

as we cannot have

$$P_2 = \frac{h_1^{\mathrm{W}} - h_1^{\mathrm{M}}}{h_1^{\mathrm{M}}h_2^{\mathrm{W}} - h_2^{\mathrm{M}}h_1^{\mathrm{W}}} < 0 \tag{55}$$

Similarly, substituting (46) into (31), we can write

$$\begin{aligned}&(\lambda_2 h_1^{\mathrm{M}} - \lambda_1 h_2^{\mathrm{M}})[(h_2^{\mathrm{M}} - h_2^{\mathrm{W}}) - (h_1^{\mathrm{M}}h_2^{\mathrm{W}} - h_2^{\mathrm{M}}h_1^{\mathrm{W}})P_1] \\ &\quad \times (\lambda_2 h_1^{\mathrm{W}} - \lambda_1 h_2^{\mathrm{W}})[(h_2^{\mathrm{M}} - h_2^{\mathrm{W}}) - (h_1^{\mathrm{M}}h_2^{\mathrm{W}} - h_2^{\mathrm{M}}h_1^{\mathrm{W}})P_1] \\ &= \lambda_2(h_1^{\mathrm{M}}h_2^{\mathrm{W}} - h_2^{\mathrm{M}}h_1^{\mathrm{W}})^2[(h_2^{\mathrm{M}} - h_2^{\mathrm{W}}) - (h_1^{\mathrm{M}}h_2^{\mathrm{W}} - h_2^{\mathrm{M}}h_1^{\mathrm{W}})P_1]\end{aligned} \tag{56}$$

giving us either

$$P_1 = \frac{h_2^{\mathrm{M}} - h_2^{\mathrm{W}}}{h_1^{\mathrm{M}}h_2^{\mathrm{W}} - h_2^{\mathrm{M}}h_1^{\mathrm{W}}} \tag{57}$$

or

$$P_1 = \frac{-\lambda_2(h_1^{\mathrm{M}}h_2^{\mathrm{W}} - h_2^{\mathrm{M}}h_1^{\mathrm{W}})}{(\lambda_1 h_2^{\mathrm{M}} - \lambda_2 h_1^{\mathrm{M}})(\lambda_1 h_2^{\mathrm{W}} - \lambda_2 h_1^{\mathrm{W}})} + \frac{h_2^{\mathrm{M}} - h_2^{\mathrm{W}}}{h_1^{\mathrm{M}}h_2^{\mathrm{W}} - h_2^{\mathrm{M}}h_1^{\mathrm{W}}} \tag{58}$$

where it is easily verified that (57) corresponds to (55) and does not satisfy (48). Thus, P_1 is given by (58).

We note that it will be optimal for both users to transmit iff

$$\frac{h_2^{\mathrm{M}} - h_2^{\mathrm{W}}}{\lambda_2} \geq \frac{(h_1^{\mathrm{M}}h_2^{\mathrm{W}} - h_1^{\mathrm{W}}h_2^{\mathrm{W}})^2}{(\lambda_1 h_2^{\mathrm{M}} - \lambda_2 h_1^{\mathrm{M}})(\lambda_1 h_2^{\mathrm{W}} - \lambda_2 h_1^{\mathrm{W}})} \geq \frac{h_1^{\mathrm{M}} - h_1^{\mathrm{W}}}{\lambda_1} \tag{59}$$

V. Sum Rate Maximization w/ Cooperative Jamming

We denote the transmission power of user k as P_k and jamming power of user k as Q_k. Then, the instantaneous sum-rate achievable is given by:

$$\begin{aligned}&\frac{1}{2}\log\left(\frac{1+h_1^{\mathrm{M}}(P_1+Q_1)+h_2^{\mathrm{M}}(P_2+Q_2)}{1+h_1^{\mathrm{M}}Q_1+h_2^{\mathrm{M}}Q_2}\right) \\ &\quad - \frac{1}{2}\log\left(\frac{1+h_1^{\mathrm{W}}(P_1+Q_1)+h_2^{\mathrm{W}}(P_2+Q_2)}{1+h_1^{\mathrm{W}}Q_1+h_2^{\mathrm{W}}Q_2}\right)\end{aligned} \tag{60}$$

We can write the optimization problem as

$$\max_{P_1(\mathbf{h}),P_2(\mathbf{h})} \int_0^\infty \cdots \int \log\left(\frac{\Phi^{\mathrm{M}}+\phi^{\mathrm{M}}-1}{\Phi^{\mathrm{W}}+\phi^{\mathrm{W}}-1}\cdot\frac{\phi^{\mathrm{W}}}{\phi^{\mathrm{M}}}\right) p(\mathbf{h})\mathrm{d}\mathbf{h} \tag{61}$$

$$\text{s.t.} \int_0^\infty \cdots \int \left(P_k(\mathbf{h}) + Q_k(\mathbf{h})\right) p(\mathbf{h})\mathrm{d}\mathbf{h} \leq \bar{P}_k, \quad k=1,2 \tag{62}$$

$$P_k(\mathbf{h}) \geq 0, \quad k=1,2 \tag{63}$$

$$Q_k(\mathbf{h}) \geq 0, \quad k=1,2 \tag{64}$$

where

$$\phi^{\mathrm{M}} = 1 + h_1^{\mathrm{M}}Q_1 + h_2^{\mathrm{M}}Q_2 \tag{65}$$

$$\phi^{\mathrm{W}} = 1 + h_1^{\mathrm{W}}Q_1 + h_2^{\mathrm{W}}Q_2 \tag{66}$$

and P_1, P_2, Q_1, Q_2 are functions of $\mathbf{h}$ even if this is not explicitly shown.

We first show that dividing power is suboptimal, i.e., the optimum power allocation should not have $P_k, Q_k > 0$. We prove this using contradiction. Assume the optimum power allocation is $\mathbf{P}^*, \mathbf{Q}^*$, and for user 1, $P_1^*, Q_1^* > 0$. Note

$$\frac{\partial \frac{\phi^{\mathrm{W}}}{\phi^{\mathrm{M}}}}{\partial Q_1} = \frac{h_1^{\mathrm{W}}\phi^{\mathrm{M}} - h_1^{\mathrm{M}}\phi^{\mathrm{W}}}{{\phi^{\mathrm{M}}}^2} \tag{67}$$

$$= \frac{h_1^{\mathrm{W}} - h_1^{\mathrm{M}} - (h_1^{\mathrm{M}}h_2^{\mathrm{W}} - h_2^{\mathrm{M}}h_1^{\mathrm{W}})\,Q_2}{{\phi^{\mathrm{M}}}^2} \tag{68}$$

the sign of which does not depend on Q_1. Consider a power allocation such that $P_1 = P_1^* - \pi$, $Q_1 = Q_1^* + \pi$. Then, $P_1 + Q_1 = P_1^* + Q_1^*$ and $\frac{\Phi^{\mathrm{M}}+\phi^{\mathrm{M}}-1}{\Phi^{\mathrm{W}}+\phi^{\mathrm{W}}-1}$ does not change. If (68) is positive, any $\pi > 0$ causes an increase in the achievable sum-rate, and jamming with the same sum power is better. If (68) is negative, then any $\pi < 0$ increases the sum-rate, and transmitting with the same sum power gives a higher rate. If this quantity is zero, the sum-rate does not depend on Q_2, and we can set it to 0. Thus, we see that the optimal allocation will have either $P_k > 0$ or $Q_k > 0$, but never both. Note that this also implies that we must have $\frac{\phi^{\mathrm{W}}}{\phi^{\mathrm{M}}} \geq 1$, or else a power allocation that gives the same sum power to transmission would achieve a higher rate.

We can then write the derivative of the Lagrangian with respect to the transmit power of user k as

$$\frac{\partial \mathcal{L}}{\partial P_k} = \frac{h_k^{\mathrm{M}}}{\Phi^{\mathrm{M}}+\phi^{\mathrm{M}}-1} - \frac{h_k^{\mathrm{W}}}{\Phi^{\mathrm{W}}+\phi^{\mathrm{W}}-1} - \lambda_k + \mu_k = 0 \tag{69}$$

Noting that we must have

$$\frac{\Phi^{\text{M}}+\phi^{\text{M}}-1}{\phi^{\text{M}}} \geq \frac{\Phi^{\text{W}}+\phi^{\text{W}}-1}{\phi^{\text{W}}} \tag{70}$$

to have a non-negative secrecy rate. We can then write

$$\lambda_k - \mu_k = \frac{h_k^{\text{M}}}{\Phi^{\text{M}}+\phi^{\text{M}}-1} - \frac{h_k^{\text{W}}}{\Phi^{\text{W}}+\phi^{\text{W}}-1} \tag{71}$$

$$\leq \frac{\frac{\phi^{\text{W}}}{\phi^{\text{M}}}h_k^{\text{M}}}{\Phi^{\text{W}}+\phi^{\text{W}}-1} - \frac{h_k^{\text{W}}}{\Phi^{\text{W}}+\phi^{\text{W}}-1} \tag{72}$$

$$\leq \frac{\phi^{\text{W}}h_k^{\text{M}} - \phi^{\text{M}}h_k^{\text{W}}}{\phi^{\text{M}}} \tag{73}$$

$$\leq \phi^{\text{W}}h_k^{\text{M}} - \phi^{\text{M}}h_k^{\text{W}} \tag{74}$$

and as a result, if $\phi^{\text{W}}h_k^{\text{M}} - \phi^{\text{M}}h_k^{\text{W}} < \lambda_k$, we must have $\mu_k > 0 \Rightarrow P_k = 0$. Now consider the jamming powers:

$$\frac{\partial \mathcal{L}}{\partial Q_k} = \frac{h_k^{\text{M}}}{\Phi^{\text{M}}+\phi^{\text{M}}-1} - \frac{h_k^{\text{W}}}{\Phi^{\text{W}}+\phi^{\text{W}}-1} - \frac{h_k^{\text{M}}}{\phi^{\text{M}}} + \frac{h_k^{\text{W}}}{\phi^{\text{W}}} - \lambda_k + \nu_k \tag{75}$$

Using (69) in (75), we get

$$-\frac{h_k^{\text{M}}}{\phi^{\text{M}}} + \frac{h_k^{\text{W}}}{\phi^{\text{W}}} + \nu_k = \mu_k \tag{76}$$

If a user is jamming, we must have $\nu_k = 0, \mu_k \geq 0$. Hence,

$$\frac{h_k^{\text{W}}}{\phi^{\text{W}}} \geq \frac{h_k^{\text{M}}}{\phi^{\text{M}}} \tag{77}$$

Since we should not have both users jamming at the same time (in which case the achievable rate is 0 and we should stop any transmission), this implies that for the jamming user,

$$\frac{h_k^{\text{W}}}{h_k^{\text{M}}} \geq \frac{1+h_k^{\text{W}}Q_k}{1+h_k^{\text{M}}Q_k} \Rightarrow h_k^{\text{W}} \geq h_k^{\text{M}} \tag{78}$$

Thus, if a user has $h_k^{\text{W}} > h_k^{\text{M}}$, then we necessarily have $\frac{h_k^{\text{W}}}{\phi^{\text{W}}} > \frac{h_k^{\text{M}}}{\phi^{\text{M}}}$ and as a result $\mu_k > 0$, indicating that user is not transmitting, as expected. If both users have $h_k^{\text{W}} \geq h_k^{\text{M}}$, no user transmits or jams. We see that

- A user will not be transmitting if $\phi^{\text{W}}h_k^{\text{M}} - \phi^{\text{M}}h_k^{\text{W}} < \lambda_k$.
- A user will not be jamming if $\phi^{\text{W}}h_k^{\text{M}} - \phi^{\text{M}}h_k^{\text{W}} > 0$ (or equivalently $h_k^{\text{M}} \geq h_k^{\text{W}}$.)

If, for both users we have $h_k^{\text{M}} \geq h_k^{\text{W}}$, neither user will be jamming, and we can find the solutions from Section IV.

We would like to find out when the solution takes the form if one user transmitting and the other jamming. Without loss of generality, assume $P_1 > 0, Q_2 > 0$, i.e. when user 1 is transmitting and user 2 is jamming. We can re-write (75) as:

$$h_2^{\text{W}}h_1^{\text{W}}P_1\phi^{\text{M}}(\Phi^{\text{M}}+\phi^{\text{M}}-1) - h_2^{\text{M}}h_1^{\text{M}}P_1\phi^{\text{W}}(\Phi^{\text{W}}+\phi^{\text{W}}-1) = \lambda_2\phi^{\text{M}}\phi^{\text{W}}(\Phi^{\text{M}}+\phi^{\text{M}}-1)(\Phi^{\text{W}}+\phi^{\text{W}}-1) \tag{79}$$

We then need to have the following two equations simultaneously satisfied:

$$\frac{h_1^{\text{M}}}{\Phi^{\text{M}}+\phi^{\text{M}}-1} - \frac{h_1^{\text{W}}}{\Phi^{\text{W}}+\phi^{\text{W}}-1} = \lambda_1 \tag{80}$$

$$\frac{h_2^{\text{W}}h_1^{\text{W}}/\phi^{\text{W}}}{\Phi^{\text{W}}+\phi^{\text{W}}-1} - \frac{h_2^{\text{M}}h_1^{\text{M}}/\phi^{\text{M}}}{\Phi^{\text{M}}+\phi^{\text{M}}-1} = \frac{\lambda_2}{P_1} \tag{81}$$

Although so far we have not been able to find a simple close-form expression for this case, we see that for a given jamming power Q_2, user 1's power is found from (25) with Q_2 instead of P_2. We note the following two observations for cooperative jamming:

1) Cooperative jamming effectively reduces the transmission threshold for the active user. Since $\phi^{\text{W}} \geq \phi^{\text{M}}$, we see that the condition to transmit is relaxed from $h_k^{\text{M}} - h_k^{\text{W}} \geq \lambda_k$ to $\frac{\phi^{\text{W}}}{\phi^{\text{M}}}h_k^{\text{M}} - h_k^{\text{W}} \geq \lambda_k$.
2) A user only jams if its main channel gain is lower than that of its eavesdropper channel gain.

VI. Sum-Capacity Upper Bound for MAC-WT

We find a bound for the sum-rate of the general K-user MAC-WT such that the received signal $\mathbf{Y}$ is conditionally independent of the wire-tapper signal $\mathbf{Z}$ given $\mathbf{X}_{\mathcal{K}}$, where $\mathbf{X}_{\mathcal{K}} = (\mathbf{X}_1, \ldots, \mathbf{X}_{\mathcal{K}})$ and the codewords are of length n. In other words, consider the joint distribution

$$p(x_1,..,x_K,y,z) = p(y|x_1,..,x_K)p(z|x_1,..,x_K)p(x_1,..,x_K)$$

where for the MAC-WT, $p(x_1,..,x_K) = \prod_{k=1}^{K} p(X_k)$.

We start with a strong secrecy constraint in the sense of [13]. Let $W_{\mathcal{S}} = \{W_k\}_{k\in\mathcal{S}}$ be the set of secret messages in the subset $\mathcal{S} \subseteq \mathcal{K}$ of users. For any $\epsilon > 0$

$$H(W_{\mathcal{K}}|\mathbf{Z}) \geq H(W_{\mathcal{K}}) - \epsilon \tag{82}$$

We will show that $H(W_{\mathcal{S}}|\mathbf{Z}) \geq H(W_{\mathcal{S}}) - \epsilon$ for any $\mathcal{S} \subseteq \mathcal{K}$. The proof is by contradiction. Assume otherwise, i.e. $H(W_{\mathcal{S}}|\mathbf{Z}) < H(W_{\mathcal{S}}) - \epsilon$:

$$H(W_{\mathcal{S}}) - \epsilon + H(W_{\mathcal{S}^c}|\mathbf{Z}) > H(W_{\mathcal{S}}|W_{\mathcal{S}^c},\mathbf{Z}) + H(W_{\mathcal{S}^c}|\mathbf{Z}) \tag{83}$$

$$= H(W_{\mathcal{K}}|\mathbf{Z}) \tag{84}$$

$$\geq H(W_{\mathcal{K}}) - \epsilon \tag{85}$$

$$= H(W_{\mathcal{S}}) + H(W_{\mathcal{S}^c}) - \epsilon \tag{86}$$

and hence, we must have

$$H(W_{\mathcal{S}^c}|\mathbf{Z}) > H(W_{\mathcal{S}^c}) \tag{87}$$

which is not possible. Hence, $H(W_{\mathcal{S}}|\mathbf{Z}) \geq H(W_{\mathcal{S}}) - \epsilon$. Then,

$$n\sum_{k\in\mathcal{K}} R_k^s = H(W_{\mathcal{K}}) \tag{88}$$

$$\leq H(W_{\mathcal{K}}|\mathbf{Z}) + \epsilon \tag{89}$$

$$\overset{(a)}{\leq} H(W_{\mathcal{K}}|\mathbf{Z}) + \epsilon + n\epsilon_n' - H(W_{\mathcal{K}}|\mathbf{Y},\mathbf{Z}) \tag{90}$$

$$= I(W_{\mathcal{K}};\mathbf{Y}|\mathbf{Z}) + n\epsilon_n \tag{91}$$

$$= \sum_{i=1}^{n} I(W_{\mathcal{K}};Y_i|\mathbf{Y}^{i-1},\mathbf{Z}) + n\epsilon_n \tag{92}$$

$$= \sum_{i=1}^{n} H(Y_i|\mathbf{Y}^{i-1},\mathbf{Z}) - \sum_{i=1}^{n} H(Y_i|W_{\mathcal{K}},\mathbf{Y}^{i-1},\mathbf{Z}) + n\epsilon_n \tag{93}$$

$$\overset{(b)}{\leq} \sum_{i=1}^{n} H(Y_i|Z_i) - \sum_{i=1}^{n} H(Y_i|W_{\mathcal{K}}, X_{\mathcal{K},i}, \mathbf{Y}^{i-1}, \mathbf{Z}) + n\epsilon_n \tag{94}$$

$$\overset{(c)}{=} \sum_{i=1}^{n} H(Y_i|Z_i) - \sum_{i=1}^{n} H(Y_i|X_{\mathcal{K},i}) + n\epsilon_n \tag{95}$$

$$\leq \sum_{i=1}^{n} H(Y_i|Z_i) - \sum_{i=1}^{n} H(Y_i|X_{\mathcal{K},i}, Z_i) + n\epsilon_n \tag{96}$$

$$= \sum_{i=1}^{n} I(X_{\mathcal{K},i}; Y_i|Z_i) + n\epsilon_n \tag{97}$$

$$\overset{(d)}{=} n\frac{1}{n}\sum_{i=1}^{n} I(X_{\mathcal{K},Q}; Y_Q|Z_Q, Q=i) + n\epsilon_n \tag{98}$$

$$= nI(X_{\mathcal{K},Q}; Y_Q|Z_Q, Q) + n\epsilon_n \tag{99}$$

$$= n\left(H(Y_Q|Z_Q, Q) - H(Y_Q|X_{\mathcal{K},Q}, Z_Q, Q) + \epsilon_n\right) \tag{100}$$

$$\overset{(e)}{\leq} n\left(H(Y_Q|Z_Q) - H(Y_Q|X_{\mathcal{K},Q}, Z_Q) + \epsilon_n\right) \tag{101}$$

$$= n\left(I(X_{\mathcal{K},Q}; Y_Q|Z_Q) + \epsilon_n\right) \tag{102}$$

where we get

- (a) from Fano's Inequality with $H(W_{\mathcal{K}}|\mathbf{Y}, \mathbf{Z}) < H(W_{\mathcal{K}}|\mathbf{Y}) < n\epsilon'_n$,
- (b) by removing conditioning, we have $H(Y_i|\mathbf{Y}^{i-1}, \mathbf{Z}) \leq H(Y_i|Z_i)$. Since conditioning reduces entropy, we have $H(Y_i|W_{\mathcal{K}}, \mathbf{Y}^{i-1}, \mathbf{Z}) \geq H(Y_i|W_{\mathcal{K}}, X_{\mathcal{K},i}, \mathbf{Y}^{i-1}, \mathbf{Z})$,
- (c) as $H(Y_i|W_{\mathcal{K}}, X_{\mathcal{K},i}, \mathbf{Y}^{i-1}, \mathbf{Z}) = H(Y_i|X_{\mathcal{K},i})$ since Y_i is independent of all else given $X_{\mathcal{K},i}$,
- (d) by introducing a new time-sharing variable Q uniformly distributed on $\{1, \ldots, n\}$,
- (e) since conditioning reduces entropy, and Y_Q is independent of all else given $X_{\mathcal{K},Q}$.

Thus, there exists random variables $X_{\mathcal{K}}$ with some joint distribution satisfying

$$\sum_{k\in\mathcal{K}} R_k^s \leq I(X_{\mathcal{K}}; Y|Z) + \epsilon_n \tag{103}$$

A. Gaussian MAC

We write the upper bound on the achievable secrecy sum-rate starting from (103),

$$\textstyle\sum_{k=1}^{K} R_k \overset{(a)}{\leq} \min_{p(N_1,N_2)} \max_{\prod_{k=1}^{K} p(X_k)} I(X_{\mathcal{K}}; Y|Z) \tag{104}$$

$$= \min_{p(N_1,N_2)} \max_{\prod_{k=1}^{K} p(X_k)} H(Y|Z) - H(Y|X_{\mathcal{K}}, Z) \tag{105}$$

$$\overset{(b)}{=} \min_{p(N_1,N_2)} \max_{\prod_{k=1}^{K} p(X_k)} H(Y|Z) - H(N_1|N_2) \tag{106}$$

$$\overset{(c)}{=} \min_{p(N_1,N_2)} \max_{\prod_{k=1}^{K} p(X_k)} H(Y - \xi Z|Z) - H(N_1|N_2) \tag{107}$$

$$\overset{(d)}{\leq} \min_{p(N_1,N_2)} \max_{\prod_{k=1}^{K} p(X_k)} H(Y - \xi Z) - H(N_1|N_2) \tag{108}$$

- (a) where we tighten the outer bound by considering all noise correlations. Since the capacity of this channel only depends on the marginal probabilities, its capacity should be equal to that of the least favorable noise.
- (b) Since we can write $H(Y|X_{\mathcal{K}}, Z) = H(N_1|X_{\mathcal{K}}, Z) = H(N_1|X_{\mathcal{K}}, Z, N_2) = H(N_1|N_2)$.
- (c) since translation does not change entropy. We will let ξ be the MMSE estimate of Y from Z. Then, $Y - \xi Z$ is the minimum mean squared error of this estimate.
- (d) by removing conditioning. This is satisfied with equality iff Y, Z are jointly Gaussian, making the error a Gaussian independent of Z. Since the marginals would then be Gaussian, and each of Y, Z are sums of random variables, all X_k must then also be Gaussian.

We proceed in a way similar to [14]. Taking Y, Z to be jointly Gaussian (with a specified covariance matrix), we write

$$Y = \xi Z + \eta \tag{109}$$

where $\eta \sim \mathcal{N}\left(0, \sigma_\eta^2\right)$ and

$$\xi = \frac{\sigma_{YZ}}{\sigma_Z^2} \tag{110}$$

$$\sigma_\eta^2 = \sigma_Y^2 - \xi^2\sigma_Z^2 = \frac{\sigma_Y^2\sigma_Z^2 - \sigma_{YZ}^2}{\sigma_Z^2} \tag{111}$$

Let

$$K_{N_1N_2} = \begin{bmatrix} 1 & \nu \\ \nu & 1 \end{bmatrix} \tag{112}$$

$$K_{YZ} = \begin{bmatrix} 1 + \sum_k h_k^{\mathrm{M}} P_k & \nu + \sum_k \sqrt{h_k^{\mathrm{M}} h_k^{\mathrm{W}}} P_k \\ \nu + \sum_k \sqrt{h_k^{\mathrm{M}} h_k^{\mathrm{W}}} P_k & 1 + \sum_k h_k^{\mathrm{W}} P_k \end{bmatrix} \tag{113}$$

We then have,

$$\sigma_\eta^2 = \frac{(1 + \sum_k h_k^{\mathrm{M}} P_k)(1 + \sum_k h_k^{\mathrm{W}} P_k)}{1 + \sum_k h_k^{\mathrm{W}} P_k} - \frac{\left(\nu + \sum_k \sqrt{h_k^{\mathrm{M}} h_k^{\mathrm{W}}} P_k\right)^2}{1 + \sum_k h_k^{\mathrm{W}} P_k} \tag{114}$$

and we can thus write from (108)

$$\sum_{k=1}^{K} R_k^s \leq \min_{\nu:\, |\nu|\leq 1} \max_{\mathbf{P}\leq\bar{\mathbf{P}}} \frac{1}{2}\log\left(\sigma_\eta^2\right) - \frac{1}{2}\log\left(1 - \nu^2\right) \tag{115}$$

$$= \min_{\nu:\, |\nu|\leq 1} \max_{P_k\leq\bar{P}_k, \forall k} \frac{1}{2}\log f(\mathbf{P}, \nu) \tag{116}$$

where

$$f(\mathbf{P}, \nu) \triangleq \frac{\sigma_\eta^2}{1 - \nu^2} \tag{117}$$

Since the logarithm is a monotonically increasing function, we can equally find the powers that

$$\min_{\nu:\, |\nu|\leq 1} \max_{P_k\leq\bar{P}_k, \forall k} f(\mathbf{P}, \nu) \tag{118}$$

We first maximize over the transmit powers:

$$\frac{\partial f}{\partial P_j} = \frac{\left[\sqrt{h_j^{\mathrm{M}}}\left(1 + \sum_k h_k^{\mathrm{W}} P_k\right) - \sqrt{h_j^{\mathrm{W}}}\left(\nu + \sum_k \sqrt{h_k^{\mathrm{M}} h_k^{\mathrm{W}}} P_k\right)\right]^2}{\left(1 - \nu^2\right)\left(1 + \sum_k h_k^{\mathrm{W}} P_k\right)^2} \tag{119}$$

and we see that for all $\nu, \mathbf{P}$, we have $\frac{\partial f(\mathbf{P},\nu)}{\partial P_j} \geq 0$. Thus, maximum powers always maximize $f(\mathbf{P}, \nu)$, regardless of ν.

Now optimizing over ν, we have

$$\frac{\partial f(\mathbf{P},\nu)}{\partial \nu} = \frac{-2\left(\sum_k \sqrt{h_k^{\mathrm{M}} h_k^{\mathrm{W}}} P_k\right)\left(\nu^2 - \zeta\nu + 1\right)}{(1-\nu^2)^2\left(1+\sum_k h_k^{\mathrm{W}} P_k\right)} \quad (120)$$

where

$$\zeta = \frac{\sum_k h_k^{\mathrm{M}} P_k + \sum_k h_k^{\mathrm{W}} P_k + \sum_k h_k^{\mathrm{M}} P_k \sum_k h_k^{\mathrm{W}} P_k}{\sum_k \sqrt{h_k^{\mathrm{M}} h_k^{\mathrm{W}}} P_k} - \sum_k \sqrt{h_k^{\mathrm{M}} h_k^{\mathrm{W}}} P_k \quad (121)$$

and we can find the possible optima as:

$$\nu_{1,2} = \frac{\zeta \pm \sqrt{\zeta^2 - 4}}{2} \quad (122)$$

It can be easily shown that $\zeta \geq 2$ and that we will always have $\nu_1\nu_2 = 1$, so only ν^* will satisfy the constraint $|\nu| \leq 1$. Also, we can easily verify that f is convex in ν for $|\nu| \leq 1$. Substituting into (116):

$$\sum_{k=1}^{K} R_k^s \leq \frac{1}{2}\log\left(1 + \frac{(\zeta - 2\nu^*)\left(\sum_k \sqrt{h_k^{\mathrm{M}} h_k^{\mathrm{W}}} P_k\right)}{1-\nu^{*2}}\right) - \frac{1}{2}\log\left(1 + \sum_k h_k^{\mathrm{W}} P_k\right)$$

Using the fact that $1 + \nu^{*2} = \zeta\nu^*$, we have

$$\frac{\zeta - 2\nu^*}{1-\nu^{*2}} = \frac{\zeta\nu^* - 2\nu^{*2}}{\nu^*(1-\nu^{*2})} = \frac{\nu^{*2} + 1 - 2\nu^{*2}}{\nu^*(1-\nu^{*2})} = \frac{1}{\nu^*} \quad (123)$$

and we also see that $0 < \nu^* \leq 1$. Hence we have,

Theorem 2:

$$\sum_{k=1}^{K} R_k^s \leq \frac{1}{2}\log\left(1 + \sum_k \frac{\sqrt{h_k^{\mathrm{M}} h_k^{\mathrm{W}}}}{\nu^*} P_k\right) - \frac{1}{2}\log\left(1 + \sum_k h_k^{\mathrm{W}} P_k\right) \quad (124)$$

where ν^* is the solution in (122) satisfying $0 < \nu^* \leq 1$.

Corollary 2.1: When the channel gains are standardized as in [6], [7], we have:

$$\sum_{k=1}^{K} R_k^s \leq \frac{1}{2}\log\left(1 + \sum_k \frac{\sqrt{h_k}}{\nu^*} P_k\right) - \frac{1}{2}\log\left(1 + \sum_k h_k P_k\right) \quad (125)$$

where ν^* is found from (122) with

$$\zeta = \frac{\sum_k P_k + \sum_k h_k P_k + \sum_k P_k \sum_k h_k P_k}{\sum_k \sqrt{h_k} P_k} - \sum_k \sqrt{h_k} P_k \quad (126)$$

For the degraded case, the standardized gains are $h_1 = \ldots = h_K = h$, and we can easily verify that $\zeta = \sqrt{h} + \frac{1}{\sqrt{h}}$, and hence $\nu_1 = \frac{1}{\sqrt{h}}$ and $\nu_2 = \sqrt{h}$, giving:

$$\sum_{k=1}^{K} R_k^s \leq \begin{cases} \frac{1}{2}\log\left(\frac{1+\sum_k P_k}{1+h\sum_k P_k}\right), & \text{if } h < 1 \Rightarrow \nu^* = \sqrt{h} \\ 0, & \text{if } h \geq 1 \Rightarrow \nu^* = \frac{1}{\sqrt{h}} \end{cases} \quad (127)$$

in accordance with [6]. Note that in general we have a gap of $\Gamma = I(X_{\mathcal{K}}; Y|Z) - [I(X_{\mathcal{K}}; Y) - I(X_{\mathcal{K}}; Z)] = I(X_{\mathcal{K}}; Z|Y)$ between the achievable secrecy sum-rate and the upper bound. This gap disappears as shown for the degraded case since $X_{\mathcal{K}} \to Y \to Z$ implies $I(X_{\mathcal{K}}; Z|Y) = 0$.

In Figures 2–3, we plot these achievable rates and the outer bound above as functions of the standardized channel gains when when $\bar{P}_1 = 10$, $\bar{P}_2 = 5$.

Similarly, we can extend this upper bound given in Theorem 2 to the ergodic fading scenario to get:

Theorem 3: With a power control policy $P_1(\mathbf{h}), P_2(\mathbf{h})$ as described in Theorem 1, the sum-rate obtainable is limited by

$$\int_0^{\infty} \cdots \int \frac{1}{2}\log\left(\frac{\bar{\Phi}^{\mathrm{M}}(\nu^*)}{\Phi^{\mathrm{W}}}\right) \quad (128)$$

where $\bar{\Phi}^{\mathrm{M}}(\nu) = 1 + \frac{\sqrt{h_1^{\mathrm{M}} h_1^{\mathrm{W}}}}{\nu} P_1(\mathbf{h}) + \frac{\sqrt{h_2^{\mathrm{M}} h_2^{\mathrm{W}}}}{\nu} P_2(\mathbf{h})$, and $\nu^*(\mathbf{h}, \mathbf{P}(\mathbf{h}))$ for a given $\mathbf{P}$ can be found from (122).

VII. Numerical Results

The secrecy sum-rate maximizing power allocation with fading is such that we use higher transmission powers when channel conditions are more favorable, i.e., high main channel gains, low eavesdropper channel gains, and cease transmission when channel conditions are unfavorable, i.e., the main channel gain is not better than the eavesdropper channel gain by a certain threshold. The power allocations in this case, however, do not have a simple water-filling interpretation as in the case without secrecy constraints. Yet, for really favorable channel conditions, the power allocation approximates the standard water-filling solution. With cooperative jamming, a user facing unfavorable channel conditions can jam the eavesdropper (with more power used for jamming when the eavesdropper channel is much stronger), and allow the other user to transmit by effectively lowering the threshold that the difference of that user's main and wiretapper channel gains must exceed.

We then examine an upper bound on the secrecy sum-rate for fixed channel gains. Comparing Figure 2 and Figure 3, we note that the outer bound given by Theorem 2 and the achievable region with cooperative jamming given in [7, Theorem 2] are loose when both users have good eavesdropper channel gains (high standardized channel gains). The bound is also somewhat loose when both standardized gains are very low. However, for the degraded case, when $h_1 = h_2$, we see that the outer and inner bounds coincide exactly, giving the sum-capacity found in [5].

We also considered independent Rayleigh fading for all channels where the power gains $h_1^{\mathrm{M}}, h_2^{\mathrm{M}}, h_1^{\mathrm{W}}, h_2^{\mathrm{W}}$ obey exponential distributions. Letting the mean gain for the main channels to be 1, we plot the achievable ergodic rates and outer bound in Figure 4 as a function of the mean eavesdropper channel gain. The dashed lines represent instantaneous power control, where we impose the same maximum power constraint on each fading block. The solid lines represent ergodic fading case, where we maintain a long-term average power constraint. The lines denoted by $\triangledown$ show achievable rates, the lines denoted

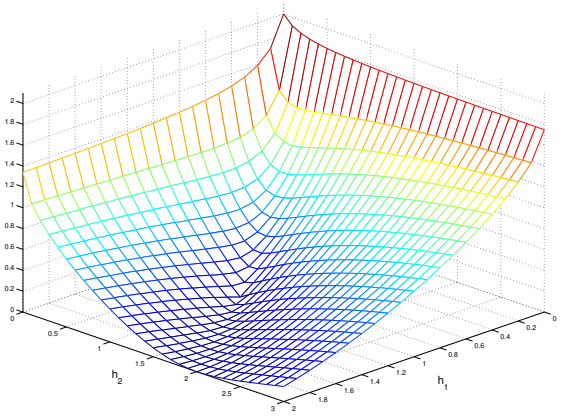

Fig. 2: Upper bound on the secrecy-sum rate as a function of standardized channel gains $h_k = h_k^{\mathrm{W}}/h_k^{\mathrm{M}}$.

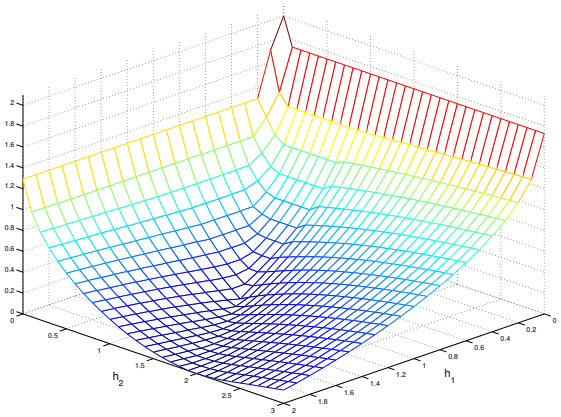

Fig. 3: Achievable secrecy sum rate w/ cooperative jamming as a function of standardized channel gains $h_k = h_k^{\mathrm{W}}/h_k^{\mathrm{M}}$.

by $*$ represent achievable rates with cooperative jamming, and the lines denoted by $\triangle$ show the outer bounds. We see that the outer bounds and achievable rates for both instantaneous and ergodic power control are close when the eavesdropper channel is weak, but drift apart as the eavesdropper channel gets stronger. Cooperative jamming improves the achievable secrecy sum-rate most when the eavesdropper channel is strong, as it is possible to more effectively jam the eavesdropper.

VIII. Conclusions

In this paper, we examined the block-fading Gaussian Multiple-Access Wire-Tap Channels (GMAC-WT). We provided achievable regions and outer bounds to the block-fading GMAC-WT. We gave the sum-rate optimizing power allocations for the GMAC-WT. We showed that the optimum power allocation does not have a simple water-filling interpretation as opposed to the standard GMAC. In addition, there are certain cases where unlike GMAC, it is optimal for both users to transmit. We then gave a solution when we incorporate cooperative jamming, and note that cooperative jamming is useful when one of the transmitters has a better eavesdropper channel than its main channel, and furthermore the other transmitter has a main channel that is better than its

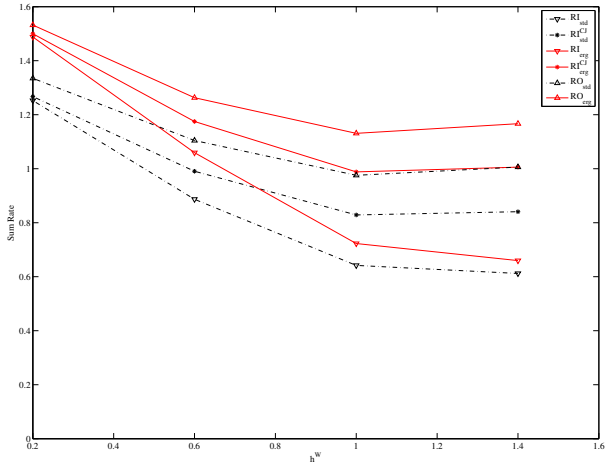

Fig. 4: Inner and outer bounds as a function of mean eavesdropper channel gain h_W.

eavesdropper channel by a certain margin that is lower than the non-jamming case. We gave numerical results showing the achievable rates and outer bounds in a Rayleigh fading setting, and showed that cooperative jamming provides a clear improvement in the achievable rates.

References

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

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

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

[4] E. Tekin, S. Şerbetli, and A. Yener, "On secure signaling for the Gaussian multiple access wire-tap channel," in *Proc. ASILOMAR Conf. Sig., Syst., Comp.*, Oct 2005.

[5] E. Tekin and A. Yener, "The Gaussian multiple-access wire-tap channel with collective secrecy constraints," in *Proc. IEEE Int. Symp. Inform. Theory (ISIT)*, Jul 2006.

[6] ——, "The Gaussian multiple-access wire-tap channel," *IEEE Trans. Inform. Theory*, submitted for publication, [Online.] Available: http://arxiv.org/format/cs.IT/0605028.

[7] ——, "Achievable rates for the general gaussian multiple access wire-tap channel with collective secrecy," in *Proc. Allerton Conf. Commun., Contr., Comput.*, Sep 2006, [Online.] Available: http://arxiv.org/abs/cs/0612088.

[8] ——, "The general Gaussian multiple-access and two-way wire-tap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inform. Theory*, submitted for publication November 2006, [Online.] Available: http://arxiv.org/abs/cs/0702112.

[9] A. J. Goldsmith and P. P. Varaiya, "Capacity of fading channels with channel side information," *IEEE Trans. Inform. Theory*, vol. 43, no. 6, pp. 1986–1997, Nov 1997.

[10] R. Knopp and P. A. Humblet, "Information capacity and power control in single-cell multiuser communications," in *IEEE Int. Conf. Comm.*, Seattle, WA, Jun 1995, pp. 331–335.

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

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

[13] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Proc. of EUROCRYPT 2000, Lecture Notes in Comp. Sci.*, vol. 1807. Springer-Verlag, 2000, pp. 351–368.

[14] M. Médard, "Capacity of correlated jamming channels," in *Allerton Conf. Commun., Contr., Comput.* Monticello, IL: University of Illinois at Urbana-Champaign, 1997, pp. 1043–1052.