Secure Rates in Multiband Broadcast Channels with Combating Jammers

Karim Banawan[1], Sennur Ulukus[1], Peng Wang[2], and Brian Henz[2]

[1]Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742
[2]US Army Research Laboratory, Aberdeen Proving Ground, MD 21005

Abstract—We consider the broadcast channel with confidential messages (BCCM) over N parallel Gaussian channels. The transmitter aims at maximizing the sum-rate. The system has two combating jammers, each aiming to enhance the secure rate to one receiver only, while hurting the other receiver by sending Gaussian jamming signals. We cast the problem as an extensive-form game and derive the optimal jamming policy. We show that the jamming strategy is a form of generalized water-filling, and provide theoretical insights on the optimal solution. We provide simulation results to show the convergence of the rate and power allocations, and study the effect of increasing the available power of the transmitter and/or the jammers.

I. INTRODUCTION

The broadcast channel with confidential messages (BCCM) [1] is a multi-user extension of the wiretap channel [2], where a transmitter wishes to communicate two independent messages to two receivers. Each message should be conveyed reliably to one of the receivers, while being kept secure from the other receiver. [3] extends this model to include a deaf helper. The helper increases the secure rate by sending cooperative jamming signals. [3] studies the asymptotic rates of this system at high SNR and derives the secure degrees of freedom using structured signals and real interference alignment.

Although [3] uses jamming to increase the secure rates, jamming can be used in a malicious way to disrupt communication. [4] formulates this problem as a two-person zero-sum game with mutual information as the payoff function, and shows that a saddle point exists for the Gaussian channel, when the jammer and the transmitter use full-power Gaussian inputs. [5] extends the problem to a multi-user setting, and obtains a generalized water-filling algorithm for power allocation of the users and the jammer. [6] considers the multiband jamming problem, formulates the problem as a Markovian system, and calculates the steady state rate according to a fixed frequency-hopping policy. [7] considers the multiband jamming problem under a minimum rate constraint on each accessed channel.

The majority of works on physical layer security studies the case of a passive eavesdropper which overhears the communication and aims to decode the confidential message without altering the transmitted signal itself, with a few exceptions: [8] studies the problem of a half-duplex active eavesdropper that can switch between jamming and eavesdropping, [9] uses the secrecy rate as the payoff function for the zero-sum game between the transmitter and the half-duplex eavesdropper, [10] considers a wiretap channel with a deaf relay that assists the eavesdropper by using pure relaying and/or sending interference, [11] considers the case where the jammer eavesdrops on the channel and uses the information obtained to perform correlated jamming, and [12] studies the adversarial interference channel using a payoff function that is a combination of secure and leakage rates.

We consider a multiband BCCM with two external jammers. The transmitter sends two messages to two receivers reliably and securely with the largest possible sum-rate. The jammers are *combating* in the sense that each jammer aims at increasing the secure rate of one of the receivers only, while hurting the other receiver by sending jamming signals. The jammers' strategies are restricted to Gaussian signals under average jamming-power constraints. Each jammer chooses a power allocation strategy over the channels in order to maximize the difference in secure rates between its own receiver and the other receiver. We formulate the problem as an extensive-form game [13], where the players (communication nodes) respond to the actions of the others to maximize the payoff function. The payoff for the transmitter is the secure sum-rate, while the payoff for the jammers is the difference in secure rates. We consider two cases: *concurrent jamming*, when the two jammers jam at the same time using the last reported jamming strategies, and *sequential jamming*, when one of the jammers acts after acquiring the knowledge of the other jammer.

In this paper, we derive the optimal strategies for the transmitter and the jammers. The problem of the transmitter is a parallel Gaussian BCCM problem [14]. The power allocation problem for the jammers has a generalized water-filling form. We develop theoretical properties of the optimal solution including: the conditions of switching jamming off in a specific channel, monotonicity of the rates, and the factors controlling the jamming power assignment. We use the convex-concave method [15] to approximate the optimization problem into an iterative convex program. We provide simulation results that show the convergence of the rates, power allocation, and the effects of power constraints of the nodes.

II. SYSTEM MODEL

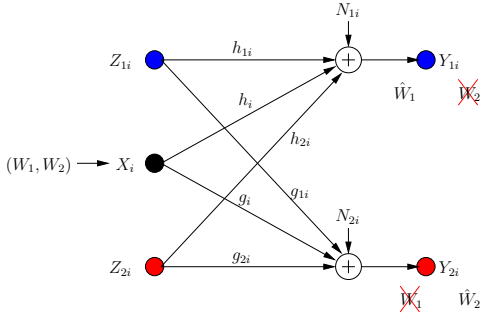We consider a two-user BCCM operating over N frequency bands (see Fig. 1). The transmitter has two messages

Fig. 1. BCCM with combating jammers.

(W_1, W_2). The message W_l is required to be decoded at the lth receiver, while being kept secure from the other receiver. The transmitter encodes (W_1, W_2) into the codewords $(X_1^n[k], X_2^n[k], \ldots, X_N^n[k])$, where $X_i^n[k]$ is the n-length channel input for the ith frequency band in the kth encoding frame. Under the power constraint $\sum_{i=1}^N \mathbb{E}[X_i[k]^2] \leq P$, where P is the power budget of the transmitter, the encoding satisfies the following reliability and security requirements:

$$\mathbb{P}(\hat{W}_1 \neq W_1) \leq \epsilon, \quad \frac{1}{n} I(W_1; Y_2^n) \leq \epsilon \qquad (1)$$

$$\mathbb{P}(\hat{W}_2 \neq W_2) \leq \epsilon, \quad \frac{1}{n} I(W_2; Y_1^n) \leq \epsilon \qquad (2)$$

where $\hat{W}_l$ is the estimate of W_l at the lth receiver. The system includes two jammers with independent channel inputs Z_1, Z_2. Each jammer aims to help one user only. Each jammer hurts the other user by sending jamming signals. We assume that jammer strategies are restricted to Gaussian jamming signals under jamming power constraints $\sum_{i=1}^N \mathbb{E}[Z_{li}[k]^2] \leq J_l$, where J_l is the jamming power of the lth jammer. Jammer l aims at maximizing the difference in secure rates:

$$\max \quad R_l - R_m \qquad (3)$$

where $l \neq m, l, m = 1, 2$. The transmitter aims at maximizing the sum-rate of the overall system:

$$\max \quad R_1 + R_2 \qquad (4)$$

We formulate the problem as an extensive-form game over the encoding frames [13]. We consider two scenarios: *concurrent jamming*, in which the jammers respond to the transmitter's encoding over the odd encoding frames, while the transmitter changes its signalling in the even encoding frames. The other scenario is *sequential jamming*, in which jammer 1 responds to the transmitter encoding at frame $k+1$, then jammer 2 responds to jammer 1 at frame $k+2$, then the transmitter changes its encoding at frame $k+3$. Each node maintains its signalling until its next turn. The channels are static, and frequency selective. The received signals at the kth frame over the ith frequency band are:

$$Y_{1i}[k] = h_i X_i[k] + \sum_{l=1}^{2} h_{li} Z_{li}[k] + N_{1i}[k] \qquad (5)$$

$$Y_{2i}[k] = g_i X_i[k] + \sum_{l=1}^{2} g_{li} Z_{li}[k] + N_{2i}[k] \qquad (6)$$

where h_i, g_i are the channel gains from the transmitter to receiver $1, 2$, respectively, in the ith channel. h_{li}, g_{li} are the channel gains from the lth jammer to receiver $1, 2$, respectively, and $N_{1i}[k], N_{2i}[k]$ are i.i.d. Gaussian noise $\mathcal{N}(0, 1)$.

III. ACHIEVABLE SCHEME

A. Transmitter Side Problem

The effect of jammers is to increase the noise floor at both receivers by introducing Gaussian jamming. This changes the effective channel gains. Denote $\tilde{h}_i, \tilde{g}_i$ as the effective channel gain to receiver 1, 2, respectively, after jamming is applied:

$$\tilde{h}_i = \frac{h_i}{\sqrt{h_{1i}^2 j_{1i} + h_{2i}^2 j_{2i} + 1}}, \quad \tilde{g}_i = \frac{g_i}{\sqrt{g_{1i}^2 j_{1i} + g_{2i}^2 j_{2i} + 1}} \qquad (7)$$

where j_{1i}, j_{2i} are the jamming powers in the ith channel. Note that initially $Z_{li}[0] = 0$, $l = 1, 2$, hence $\tilde{h}_i = h_i, \tilde{g}_i = g_i$. The problem is equivalent to the parallel Gaussian BCCM in [14]. Let $\mathcal{S}_1 = \{i : |\tilde{h}_i| > |\tilde{g}_i|\}$ denote the channels in which user 1 is stronger and $\mathcal{S}_2 = \{i : |\tilde{g}_i| > |\tilde{h}_i|\}$ denote the channels in which user 2 is stronger. The transmitter sends W_1 over $\mathcal{S}_1$ and W_2 over $\mathcal{S}_2$ using a Gaussian wiretap code. By performing water-filling over the channels, the following rate pairs are achievable [14]:

$$R_1 \leq \frac{1}{2} \sum_{i \in \mathcal{S}_1} \left[\log(1 + p_{1i} \tilde{h}_i^2) - \log(1 + p_{1i} \tilde{g}_i^2) \right] \qquad (8)$$

$$R_2 \leq \frac{1}{2} \sum_{i \in \mathcal{S}_2} \left[\log(1 + p_{2i} \tilde{g}_i^2) - \log(1 + p_{2i} \tilde{h}_i^2) \right] \qquad (9)$$

where $\{p_{li}\}_{i \in \mathcal{S}_l}, l = 1, 2$, are related as:

$$p_{1i} = \frac{1}{2} \left[-\frac{1}{\tilde{h}_i^2} - \frac{1}{\tilde{g}_i^2} + \sqrt{\alpha_i^2 - \frac{2P}{\lambda_1} \alpha_i} \right]^+ \qquad (10)$$

$$p_{2i} = \frac{1}{2} \left[-\frac{1}{\tilde{h}_i^2} - \frac{1}{\tilde{g}_i^2} + \sqrt{\alpha_i^2 + \frac{2P}{\lambda_2} \alpha_i} \right]^+ \qquad (11)$$

where $\alpha_i = \frac{1}{\tilde{h}_i^2} - \frac{1}{\tilde{g}_i^2}$, $[x]^+ = \max(x, 0)$ and λ_1, λ_2 are chosen such that for some $\gamma \in [0, 1]$

$$\sum_{i \in \mathcal{S}_1} p_{1i} = \gamma P, \qquad \sum_{i \in \mathcal{S}_2} p_{2i} = (1 - \gamma)P \qquad (12)$$

B. Jammers' Side Problem

The jammers assign power over channels to maximize the rate difference as in (3) in response to the transmitter. Define $p_i = p_{li}$, if $i \in \mathcal{S}_l, l = 1, 2$. Let $\sigma_{1i}^2, \sigma_{2i}^2$ be the observed noise levels by jammer 1 at receiver 1, 2, respectively:

$$\sigma_{1i}^2 = 1 + h_{2i}^2 j_{2i}, \quad \sigma_{2i}^2 = 1 + g_{2i}^2 j_{2i} \qquad (13)$$

where j_{2i} is the last reported jamming power of jammer 2 in channel i. This is true for concurrent and sequential scenarios. Let $\tilde{\sigma}_{1i}^2, \tilde{\sigma}_{2i}^2$ to be the observed noise level by jammer 2, i.e.,

$$\tilde{\sigma}_{1i}^2 = 1 + h_{1i}^2 j_{1i}, \quad \tilde{\sigma}_{2i}^2 = 1 + g_{1i}^2 j_{1i} \qquad (14)$$

where j_{1i} is the last reported jamming power of jammer 1 in channel i. Note that for the sequential scenario j_{1i} is the actual jamming power produced by jammer 1. However, this is not true for the concurrent setting, because jammer 1 is changing its encoding in the same time. We concentrate on the problem of the first jammer without loss of generality. Define $s_{li}(j_{1i})$ to be the signal to jamming ratio (SJNR) of the ith channel at receiver l as observed by jammer 1

$$s_{1i} = \frac{h_i^2 p_i}{h_{1i}^2 j_{1i} + \sigma_{1i}^2}, \quad s_{2i} = \frac{g_i^2 p_i}{g_{1i}^2 j_{1i} + \sigma_{2i}^2} \quad (15)$$

Jammer 1 chooses a power allocation strategy $\{j_{1i}\}_{i=1}^N$ to solve the following optimization problem

$$\max_{j_{1i}} \quad \sum_{i \in \mathcal{S}_1} \frac{1}{2} \left[\log\left(1 + s_{1i}(j_{1i})\right) - \log\left(1 + s_{2i}(j_{1i})\right) \right]^+$$
$$- \sum_{i \in \mathcal{S}_2} \frac{1}{2} \left[\log\left(1 + s_{2i}(j_{1i})\right) - \log\left(1 + s_{1i}(j_{1i})\right) \right]^+$$

$$\text{s.t.} \quad j_{1i} \geq 0, \quad \forall i, \qquad \sum_{i=1}^N j_{1i} \leq J_1 \quad (16)$$

We note that in (16), $[.]^+$ can be dropped $\forall i \in \mathcal{S}_1$ because providing no jamming $j_{1i} = 0$, $\forall i \in \mathcal{S}_1$ is a feasible jamming policy, and it achieves non-negative rates since $|h_i| > |g_i|$, $\forall i \in \mathcal{S}_1$. Meanwhile, this enlarges the feasible set for jamming channels in $\mathcal{S}_2$ which cannot increase the rate of user 2. Now, since $-[x]^+ = -\max(x, 0) = \min(-x, 0) = [-x]^-$, the objective function of (16) can be written as

$$\sum_{i \in \mathcal{S}_1} \frac{1}{2} \left[\log\left(1 + s_{1i}(j_{1i})\right) - \log\left(1 + s_{2i}(j_{1i})\right) \right]$$
$$+ \sum_{i \in \mathcal{S}_2} \frac{1}{2} \left[\log\left(1 + s_{1i}(j_{1i})\right) - \log\left(1 + s_{2i}(j_{1i})\right) \right]^- \quad (17)$$

Since $\mathcal{S}_1 \cap \mathcal{S}_2 = \emptyset$ and $\mathcal{S}_1 \cup \mathcal{S}_2 = \{1, 2, \cdots, N\}$, we write (16) in the hypograph form as:

$$\max_{j_{1i}, t_i} \quad \sum_{i=1}^N t_i$$
$$\text{s.t.} \quad t_i \leq 0, \, i \in \mathcal{S}_2, \quad t_i \geq 0, \, i \in \mathcal{S}_1$$
$$\log\left(1 + s_{1i}(j_{1i})\right) - \log\left(1 + s_{2i}(j_{1i})\right) \geq 2t_i, \quad \forall i$$
$$j_{1i} \geq 0, \forall i, \quad \sum_{i=1}^N j_{1i} \leq J_1 \quad (18)$$

IV. OPTIMALITY CONDITIONS

Lemma 1 *If the transmitter provides strictly positive rate for user 2 over channel $i \in \mathcal{S}_2$, then the rate of channel i is monotonically decreasing in j_{1i}.*

Proof: Consider the rate on channel i

$$f(j_i) = \log\left(1 + \frac{h_i^2 p_i}{\sigma_{1i}^2 + h_{1i}^2 j_i}\right) - \log\left(1 + \frac{g_i^2 p_i}{\sigma_{2i}^2 + g_{1i}^2 j_i}\right) \quad (19)$$

This function characterizes the rate of user 1 if $i \in \mathcal{S}_1$ and the negative of the rate of user 2 if $i \in \mathcal{S}_2$. To prove monotonicity,

it suffices to show that the derivative $f'(j_i) > 0$. A sufficient condition of ensuring that is

$$\frac{h_{1i}^2}{\sigma_{1i}^2 + h_{1i}^2 j_i + h_i^2 p_i} > \frac{g_{1i}^2}{\sigma_{2i}^2 + g_{1i}^2 j_i + g_i^2 p_i} \quad (20)$$

$$\text{and} \quad \frac{h_{1i}^2}{\sigma_{1i}^2 + h_{1i}^2 j_i} < \frac{g_{1i}^2}{\sigma_{2i}^2 + g_{1i}^2 j_i} \quad (21)$$

Let $j_i = j_i^0 + \Delta_j$, where j_i^0 is the jamming power in the previous encoding frame. Define $z_{1i} = 1 + \sigma_{1i}^2 + h_{1i}^2 j_i^0$ to be the noise level at receiver 1 as observed by the transmitter after jamming is applied and similarly at receiver 2, $z_{2i} = 1 + \sigma_{2i}^2 + g_{1i}^2 j_i^0$. We can write (20) as

$$\frac{h_{1i}^2}{z_{1i} + h_{1i}^2 \Delta_j + h_i^2 p_i} > \frac{g_{1i}^2}{z_{2i} + g_{1i}^2 \Delta_j + g_i^2 p_i} \quad (22)$$

$$\text{and} \quad \frac{h_{1i}^2}{z_{1i} + h_{1i}^2 \Delta_j} < \frac{g_{1i}^2}{z_{2i} + g_{1i}^2 \Delta_j} \quad (23)$$

From (23), $\frac{h_{1i}^2}{z_{1i}} < \frac{g_{1i}^2}{z_{2i}}$, and from the first condition, we have

$$h_{1i}^2(z_{2i} + g_i^2 p_i) > g_{1i}^2(z_{1i} + h_i^2 p_i) \quad (24)$$

$$\frac{h_{1i}^2}{z_{1i}}\left(1 + \frac{g_i^2 p_i}{z_{2i}}\right) > \frac{g_{1i}^2}{z_{2i}}\left(1 + \frac{h_i^2 p_i}{z_{1i}}\right) \quad (25)$$

$$\frac{(1 + \tilde{g}_i^2 p_i)}{(1 + \tilde{h}_i^2 p_i)} > \frac{\frac{g_{1i}^2}{z_{2i}}}{\frac{h_{1i}^2}{z_{1i}}} > 1 \quad (26)$$

i.e., $R_{2i} > 0$. (26) follows from $\frac{h_{1i}^2}{z_{1i}} < \frac{g_{1i}^2}{z_{2i}}$. $\blacksquare$

Lemma 2 *The jamming power constraint is satisfied with equality if there exists a channel $i \in \mathcal{S}_2$ that has strictly positive rate for user 2.*

Proof: Suppose the jammer power constraint is not satisfied with equality in the optimal solution, i.e., $J_1 - \sum_{i=1}^N j_{1i}^* = \delta > 0$. From Lemma 1, the existence of channel $m \in \mathcal{S}_2$ is a sufficient condition for ensuring that the rate of user 2 on channel m is monotone decreasing in j_{1i}. Consequently, let $j_{1m} = j_{1m}^* + \delta$ which is feasible. In this case, the rate of user 2 is strictly smaller, hence $R_1 - R_2$ is strictly increased, which is a contradiction. $\blacksquare$

Lemma 3 *Jammer 1 does not jam channel i if $R_{1i} < R_{1i}^0$ or $R_{2i} > R_{2i}^0$, where R_{li}, R_{li}^0 are the rate of user l over channel i with and without applying jamming, respectively.*

Proof: Suppose in the optimal solution $R_{1i} < R_{1i}^0$ for some $i \in \mathcal{S}_1$. First, if there exists $m \in \mathcal{S}_2$ such that it has positive rate, then by Lemma 2, we can switch the jamming off, i.e., $j_{1i} = 0$ and move all this power to channel m, i.e., $j_{1m} = j_{1m}^* + j_{1i}^*$, which is feasible. In this case, we strictly decrease R_{2m} and increase R_{1i}, hence, the objective function increases which is a contradiction. If all channels of user 2 have zero rate, then switching off this channel forces the rate over this channel to be R_{1i}^0, which is strictly better. The same argument follows for $R_{2i} > R_{2i}^0$. $\blacksquare$

Lemma 4 *A sufficient condition for jammer 1 not to jam channel i is*

$$R_{1i}^0 \leq \frac{1}{2}\left[\log\left(\frac{h_i^2 h_{1i}^2}{g_i^2 g_{1i}^2}\right) + \log\left(\frac{\sigma_{2i}^2}{\sigma_{1i}^2}\right)\right], \quad \forall i \in \mathcal{S}_1 \quad (27)$$

$$or \ R_{2i}^0 \geq \frac{1}{2}\left[\log\left(\frac{g_i^2 g_{1i}^2}{h_i^2 h_{1i}^2}\right) + \log\left(\frac{\sigma_{1i}^2}{\sigma_{2i}^2}\right)\right], \quad \forall i \in \mathcal{S}_2 \quad (28)$$

Proof: Consider first that $i \in \mathcal{S}_1$. From Lemma 3, jammer 1 does not jam channel i if $R_{1i}^0 > R_{1i}$, which implies

$$\log\left(1 + \frac{h_i^2 p_i}{\sigma_{1i}^2}\right) - \log\left(1 + \frac{g_i^2 p_i}{\sigma_{2i}^2}\right)$$
$$> \log\left(1 + \frac{h_i^2 p_i}{\sigma_{1i}^2 + h_{1i}^2 j_{1i}}\right) - \log\left(1 + \frac{g_i^2 p_i}{\sigma_{2i}^2 + g_{1i}^2 j_{1i}}\right) \quad (29)$$
$$\frac{\sigma_{2i}^2(\sigma_{1i}^2 + h_i^2 p_i)}{\sigma_{1i}^2(\sigma_{2i}^2 + g_i^2 p_i)} > \frac{(\sigma_{2i}^2 + g_{1i}^2 j_{1i})(\sigma_{1i}^2 + h_i^2 p_i + h_{1i}^2 j_{1i})}{(\sigma_{1i}^2 + h_{1i}^2 j_{1i})(\sigma_{2i}^2 + g_i^2 p_i + g_{1i}^2 j_{1i})} \quad (30)$$

Simplifying (30), the rate of user 1 on channel i is worse than switching jamming off if the jamming power satisfies

$$j_{1i} > \frac{\frac{g_i^2 g_{1i}^2}{\sigma_{2i}^2}\left(1 + \frac{h_i^2 p_i}{\sigma_{1i}^2}\right) - \frac{h_i^2 h_{1i}^2}{\sigma_{1i}^2}\left(1 + \frac{g_i^2 p_i}{\sigma_{2i}^2}\right)}{g_{1i}^2 h_{1i}^2\left(\frac{h_i^2}{\sigma_{1i}^2} - \frac{g_i^2}{\sigma_{2i}^2}\right)} \quad (31)$$

Since $\forall i \in \mathcal{S}_1$, $\frac{h_i^2}{\sigma_{1i}^2} > \frac{g_i^2}{\sigma_{2i}^2}$, if the numerator is less than or equal to zero, any positive jamming power in channel i strictly decreases R_{1i}. Thus, the condition of not jamming is,

$$\frac{g_i^2 g_{1i}^2}{\sigma_{2i}^2}\left(1 + \frac{h_i^2 p_i}{\sigma_{1i}^2}\right) - \frac{h_i^2 h_{1i}^2}{\sigma_{1i}^2}\left(1 + \frac{g_i^2 p_i}{\sigma_{2i}^2}\right) \leq 0 \quad (32)$$

$$\frac{1}{2}\log\frac{\left(1 + \frac{h_i^2 p_i}{\sigma_{1i}^2}\right)}{\left(1 + \frac{g_i^2 p_i}{\sigma_{2i}^2}\right)} \leq \frac{1}{2}\log\left(\frac{h_i^2 h_{1i}^2}{g_i^2 g_{1i}^2} \cdot \frac{\sigma_{2i}^2}{\sigma_{1i}^2}\right) \quad (33)$$

A similar condition can be obtained for $i \in \mathcal{S}_2$. ∎

Lemma 5 $\log\left(1 + s_{1i}(j_{1i})\right) - \log\left(1 + s_{2i}(j_{1i})\right) \geq 2t_i$ *constraint is satisfied with equality in all cases. In particular, if $t_i = 0$, then $j_{1i} = \frac{\sigma_{1i}^2 g_i^2 - \sigma_{2i}^2 h_i^2}{h_i^2 g_{1i}^2 - g_i^2 h_{1i}^2}$.*

Proof: Consider first $i \in \mathcal{S}_1$, suppose in the optimal solution we have $\log\left(1 + s_{1i}(j_{1i}^*)\right) - \log\left(1 + s_{2i}(j_{1i}^*)\right) > 2t_i^*$, then increasing t_i to match the constraint with equality is feasible, and the objective function strictly increases, which is a contradiction. The same argument holds for $i \in \mathcal{S}_2$ if $\log\left(1 + s_{1i}(j_{1i}^*)\right) - \log\left(1 + s_{2i}(j_{1i}^*)\right) \leq 0$. It remains to show the case $\log\left(1 + s_{1i}(j_{1i}^*)\right) - \log\left(1 + s_{2i}(j_{1i}^*)\right) > 0$, $i \in \mathcal{S}_2$. If the rate of user 2 is positive before jamming, then by continuity of the rate function, there exists a feasible jamming power $\tilde{j}_{1i} \leq \tilde{j}_{1i}^*$ policy that drives user 2's rate to zero. This power is given by equating $R_{2i} = 0$, hence $\tilde{j}_{1i} = \frac{\sigma_{1i}^2 g_i^2 - \sigma_{2i}^2 h_i^2}{h_i^2 g_{1i}^2 - g_i^2 h_{1i}^2}$. Using this policy cannot decrease the objective function due to the monotonicity. Note that if rate of user 2 is zero, then this channel carries no power and hence $t_i^* = 0$. ∎

Theorem 1 *The optimal jamming strategy for jammer 1 is a generalized water-filling: the jammer does not jam the ith*

channel if $\frac{g_{1i}^2}{\sigma_{2i}^2}r_{2i} - \frac{h_{1i}^2}{\sigma_{1i}^2}r_{1i} \leq 2\lambda$, where $r_{1i} = \frac{h_i^2 p_i}{\sigma_{1i}^2 + h_i^2 p_i}, r_{2i} = \frac{g_i^2 p_i}{\sigma_{2i}^2 + g_i^2 p_i}$. Otherwise, the jammer chooses j_{1i} such that

$$\frac{j_{1i}}{q_{2i}s_{2i} - q_{1i}s_{1i}} = \frac{1}{2\lambda} \quad (34)$$

where λ is chosen such that $\sum_{l=1}^N j_{1i} = J_1$, s_{li} is given in (15), and $q_{1i} = \frac{h_{1i}^2 j_{1i}}{\sigma_{1i}^2 + h_i^2 p_i + h_{1i}^2 j_{1i}}, q_{2i} = \frac{g_{1i}^2 j_{li}}{\sigma_{2i}^2 + g_i^2 p_i + g_{1i}^2 j_{1i}}$.

Proof: The Lagrangian of the problem in (18) is:

$$\mathcal{L} = -\sum_{i=1}^N t_i + \sum_{i \in \mathcal{S}_1} \nu_i t_i - \sum_{i \in \mathcal{S}_2} \nu_i t_i + \lambda\left(\sum_{l=1}^N j_{1i} - J_1\right)$$
$$+ \sum_{i=1}^N \theta_i\left[2t_i - \log\left(1 + \frac{g_i^2 p_i}{g_{1i}^2 j_{1i} + \sigma_{2i}^2}\right)\right.$$
$$\left. - \log\left(1 + \frac{h_i^2 p_i}{h_{1i}^2 j_{1i} + \sigma_{1i}^2}\right)\right] - \sum_{l=1}^N \mu_i j_{1i} \quad (35)$$

The KKT optimality conditions are:

$$2\theta_i - \nu_i = 1, \quad \forall i \in \mathcal{S}_1 \quad (36)$$
$$2\theta_i + \nu_i = 1, \quad \forall i \in \mathcal{S}_2 \quad (37)$$

$$\theta_i\left[\frac{g_{1i}^2}{\sigma_{2i}^2 + g_{1i}^2 j_{1i} + g_i^2 p_i} - \frac{g_{1i}^2}{\sigma_{2i}^2 + g_{1i}^2 j_{1i}} - \frac{h_{1i}^2}{\sigma_{1i}^2 + h_{1i}^2 j_{1i} + h_i^2 p_i}\right.$$
$$\left. + \frac{h_{1i}^2}{\sigma_{1i}^2 + h_{1i}^2 j_{1i}}\right] + \lambda - \mu_i = 0 \quad (38)$$

If $t_i \neq 0$, then $\nu_i = 0$ and therefore $\theta_i = 1/2$. The first part of the theorem, which is concerned with the conditions of not jamming the ith channel, i.e., $j_{1i} = 0$ and since $\mu_i \geq 0$, then

$$\frac{g_{1i}^2}{\sigma_{2i}^2 + g_i^2 p_i} - \frac{g_{1i}^2}{\sigma_{2i}^2} - \frac{h_{1i}^2}{\sigma_{1i}^2 + h_i^2 p_i} - \frac{h_{1i}^2}{\sigma_{1i}^2} + 2\lambda = 2\mu_i \geq 0 \quad (39)$$

which implies

$$\frac{g_{1i}^2}{\sigma_{2i}^2}\left(\frac{g_i^2 p_i}{\sigma_{2i}^2 + g_i^2 p_i}\right) - \frac{h_{1i}^2}{\sigma_{1i}^2}\left(\frac{h_i^2 p_i}{\sigma_{1i}^2 + h_i^2 p_i}\right) \leq 2\lambda \quad (40)$$

Now, we derive the power allocation for the jammer for the case $j_{li} > 0$, and hence $\mu_i = 0$. From (38), we have

$$\frac{g_{1i}^2 j_{1i}}{\sigma_{2i}^2 + g_{1i}^2 j_{1i} + g_i^2 p_i} \cdot \frac{g_i^2 p_i}{\sigma_{2i}^2 + g_{1i}^2 j_{1i}}$$
$$- \frac{h_{1i}^2 j_{1i}}{\sigma_{1i}^2 + h_{1i}^2 j_{1i} + h_i^2 p_i} \cdot \frac{h_i^2 p_i}{\sigma_{1i}^2 + h_{1i}^2 j_{1i}} = 2\lambda j_{1i} \quad (41)$$
$$q_{2i}s_{2i} - q_{1i}s_{1i} = 2\lambda j_{1i} \quad (42)$$

which is the water-filling algorithm in (34). ∎

V. Numerical Results

A. Convex-Concave Method

We use the convex-concave method [15] to solve problem (16) numerically. We replace the convex terms ($-\log$ terms) by their first-order approximations around some feasible point.
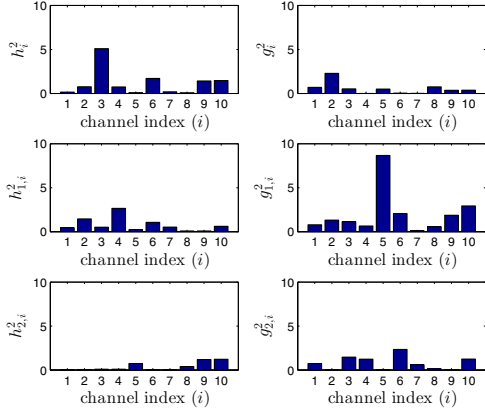
Fig. 2. Channel gains.

Fig. 3. Power allocation policy for the transmitter and the two jammers.

Hence, the problem is relaxed to maximization of a concave function, which can be solved efficiently. By updating the point of expansion by the optimal solution of the resultant convex optimization problem iteratively, we converge to a locally-optimal solution. The objective function of jammer 1 is:

$$\sum_{i \in \mathcal{S}_1} f(j_{1i}) + \sum_{i \in \mathcal{S}_2} \min(f(j_{1i}), 0) \tag{43}$$

where $f(j_{1i})$ is the rate in (19), which is approximated as:

$$
\begin{aligned}
&f(j_{1i}) \\
&\approx \log(\sigma_{1i}^2 + h_{1i}^2 j_{1i} + h_i^2 p_i) + \log(\sigma_{2i}^2 + g_{1i}^2 j_{1i}) \\
&\quad - \log\left(\sigma_{1i}^2 + h_{1i}^2 j_i^{(\kappa)}\right) - \log\left(\sigma_{2i}^2 + g_{1i}^2 j_i^{(\kappa)} + g_i^2 p_i\right) \\
&\quad - \left(\frac{h_{1i}^2}{\sigma_{1i}^2 + h_{1i}^2 j_i^{(\kappa)}} + \frac{g_{1i}^2}{\sigma_{2i}^2 + g_i^2 p_i + g_{1i}^2 j_i^{(\kappa)}}\right)(j_{1i} - j_i^{(\kappa)})
\end{aligned} \tag{44}
$$

where $j_i^{(\kappa)}, \kappa = 1, 2, \cdots$ is the point we approximate around at iteration κ. The approximated objective is a concave function, since it is the difference between a concave function and an affine function. We update $j_i^{(\kappa)} = j_{1i}^{*(\kappa-1)}$.

B. Simulation Results

In all simulations, we use fixed channel gains (Fig. 2) with $N = 10$. We assume that the transmitter and the jammers are involved in an extensive-form game of $T = 10$ rounds each.

1) Power Allocation Results: We assume that $P = J_1 = J_2 = 10$ and concurrent jamming. Fig. 3 shows the power allocation of the transmitter and the two jammers. The colored bars represent the value at each encoding frame. $\mathcal{S}_1 = \{3, 4, 6, 7, 9, 10\}$. We note that the transmitter performs water-filling over effective noise level of $\left|\frac{1}{h_i^2} - \frac{1}{g_i^2}\right|$. We note that jammer 1 jams channel 9, which belongs to $\mathcal{S}_1$ because $g_{1i}^2 > h_{1i}^2$ enough such that it can boost the SJNR difference, and achieve a higher secure rate. We note that $R_{1i}^0 \leq \frac{1}{2}\left[\log\left(\frac{h_i^2 h_{1i}^2}{g_i^2 g_{1i}^2}\right) + \log\left(\frac{\sigma_{2i}^2}{\sigma_{1i}^2}\right)\right]$ for channels $\{4, 6, 7\}$, which implies that if jammer 1 does not jam these channels, they have higher rates, and this conforms with Fig. 3. Jammer
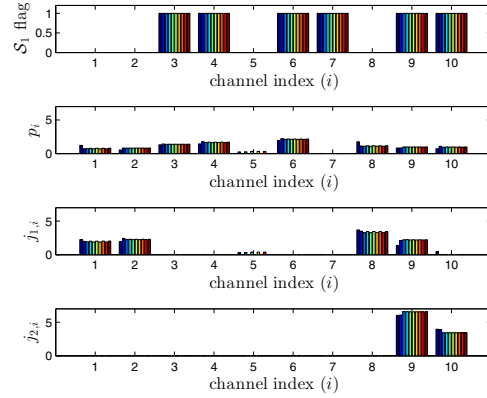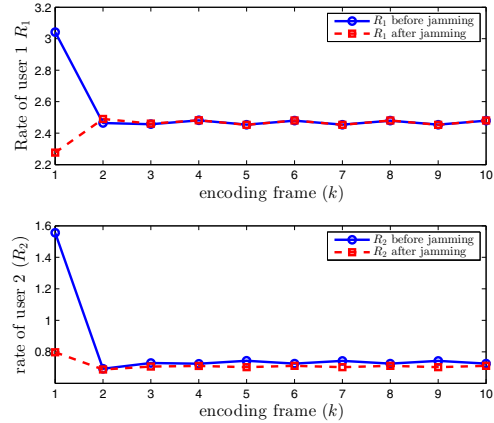

Fig. 4. Rates of user 1 and 2.

1 jams all channels of user 2 whenever they are active, e.g., channel 5. We observe that jammer 2 confines its power to channels $\{9, 10\}$, since in channels $\{3, 4, 6, 7\}$, the jamming channel g_{2i}^2 is much stronger than h_{2i}^2. Hence, if jammer 2 jams in these channels, it hurts receiver 2 even more. This is the opposite for channel 9. We observe that the elements of the transmitter/jammer power allocation vector either converge to an equilibrium state, or oscillate between two power levels, which results in oscillating rates. Finally, all power constraints for the transmitter and jammers are met with equality.

In Fig. 4, we show the evolution of rates between the encoding frames. We note that for user 1, the rates before and after the jamming coincide starting from frame $k = 3$. That implies that the effect of jammer 2 is almost negligible on user 1 when jammer 2 plays the equilibrium strategy. However, this is not the case for the rate of user 2, because on channel 8, which carries most of the rate of user 2, the optimal jamming policy of user 1 oscillates and hence leads to significant oscillations on the resultant rate.

2) Effect of Changing Transmitter and Jammer Power Constraints: In the sequel, we plot the average of the rates over the 10 game rounds, i.e., $\bar{R}_l = \frac{1}{T}\sum_{t=1}^{T}\sum_{i=1}^{N} R_{li}(t)$, where
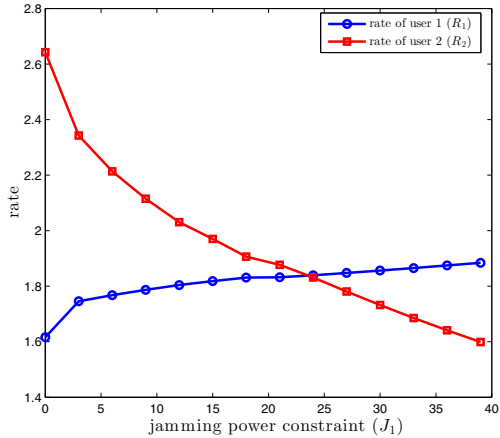
Fig. 5. Effect of changing the jamming power constraint (J_1) with $J_2 = 0$.

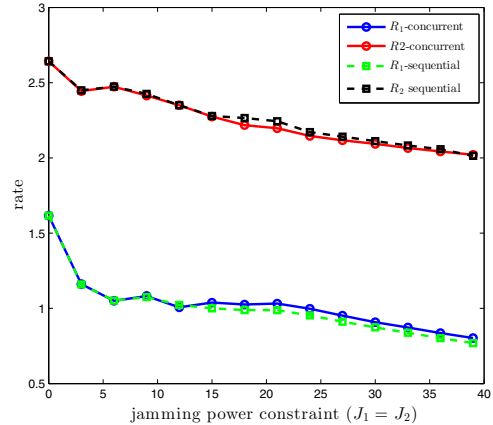

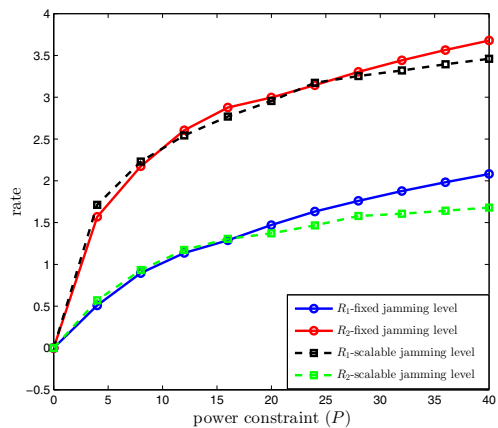Fig. 6. Effect of changing both jamming powers, $J_1 = J_2$.

Fig. 7. Effect of changing the transmitter power constraint. Fixed jamming corresponds to $J_1 = J_2 = 10$, and scalable jamming corresponds to $P = J_1 = J_2$.

$R_{li}(t)$ is the rate of the lth user on the ith channel on the tth round. Fig. 5 shows the effect of changing the power constraint of jammer 1 only, when the second jammer is switched off. We note that as J_1 increases, the rate of user 1 increases, while the rate of user 2 decreases. That is because jammer 1 acts as a helper for user 1 and a malicious jammer for user 2. We note that although both users have zero secure degrees of freedom, user 1 has non-zero rate in the limit in contrast to user 2.

In Fig. 6, we show the effect of increasing the available jamming power for both jammers, i.e., $J_1 = J_2 = J$, while keeping the power constraint of the transmitter fixed at 10. We note that for both concurrent and sequential jamming, as the jamming power increases, the rates of the two users decrease monotonically to zero, i.e., the malicious behaviour of the two jammers preclude any secure rates as $J \to \infty$. In the case of sequential jamming, jammer 2 has relative advantage over jammer 1, since it knows the exact jamming power vector of jammer 1, and hence it can hurt user 1 more than the concurrent case. Therefore, Fig. 6 shows a slight increase for the rate of user 2 and slight decrease for the rate user 1. Finally, Fig. 7 shows the effect of increasing the transmitter power constraint. Two cases are considered: first, when the jammers have fixed power $J_1 = J_2 = 10$ and the second, when the jamming power scales with the power constraint, i.e., $P = J_1 = J_2$. We note that in both cases, the rates monotonically increase in P. However, when the jamming power also scales with P, this enhancement is much slower.

References

[1] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates. Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions. *IEEE Trans. on Info. Theory*, 54(6):2493–2507, Jun. 2008.

[2] A. Wyner. The wire-tap channel. *The Bell System Tech. Jour.*, 54(8):1355–1387, Jan. 1975.

[3] J. Xie and S. Ulukus. Secure degrees of freedom of one-hop wireless networks. *IEEE Trans. on Info. Theory*, 60(6):3359–3378, Jun. 2014.

[4] R. J. McEliece. Communication in the presence of jamming-an information-theoretic approach. In *Secure Digital Communications*, pages 127–166. Springer, 1983.

[5] R. H. Gohary, Y. Huang, Z.-Q. Luo, and J.-S. Pang. A generalized iterative water-filling algorithm for distributed power control in the presence of a jammer. *IEEE Trans. on Signal Processing*, 57(7):2660–2674, Jul. 2009.

[6] P. Wang and B. Henz. Performance analysis of jammed single-hop wireless networks. In *IEEE MILCOM*, Nov. 2013.

[7] K. Banawan, S. Ulukus, P. Wang, and B. Henz. Multiband jamming strategies with minimum rate constraints. In *IEEE WCNC*, Apr. 2016.

[8] G. Amariucai and S. Wei. Half-duplex active eavesdropping in fast-fading channels: A block-markov Wyner secrecy encoding scheme. *IEEE Trans. on Info. Theory*, 58(7):4660–4677, Jul. 2012.

[9] A. Mukherjee and A. Swindlehurst. Jamming games in the MIMO wiretap channel with an active eavesdropper. *IEEE Trans. on Signal Processing*, 61(1):82–91, Jan. 2013.

[10] M. Yuksel, X. Liu, and E. Erkip. A secure communication game with a relay helping the eavesdropper. *IEEE Trans. on Info. Forensics and Security*, 6(3):818–830, Sep. 2011.

[11] S. Shafiee and S. Ulukus. Mutual information games in multiuser channels with correlated jamming. *IEEE Trans. on Info. Theory*, 55(10):4598–4607, Oct. 2009.

[12] J. Xie and S. Ulukus. Secrecy games on the one-sided interference channel. In *IEEE ISIT*, Jul. 2011.

[13] S. Tadelis. *Game Theory: An Introduction*. 2013.

[14] E. Ekrem and S. Ulukus. Ergodic secrecy capacity region of the fading broadcast channel. In *IEEE ICC*, Jun. 2009.

[15] T. Lipp and S. Boyd. Variations and extension of the convex-concave procedure. *Optimization and Engineering*, Nov. 2015.