Ergodic Secret Alignment

Raef Bassily, *Student Member, IEEE*, and Sennur Ulukus, *Member, IEEE*

***Abstract*—In this paper, we introduce two new achievable schemes for the fading multiple access wiretap channel (MAC-WT). In the model that we consider, we assume that perfect knowledge of the state of all channels is available at all the nodes in a causal fashion. Our schemes use this knowledge together with the time-varying nature of the channel model to align the interference from different users at the eavesdropper perfectly in a one-dimensional space while creating a higher dimensionality space for the interfering signals at the legitimate receiver, hence allowing for better chance of recovery. While we achieve this alignment through signal scaling at the transmitters in our first scheme (scaling-based alignment), we let nature provide this alignment through the ergodicity of the channel coefficients in the second scheme [ergodic secret alignment (ESA)] [1], [2]. For each scheme, we obtain the resulting achievable secrecy rate region. We show that the secrecy rates achieved by both schemes in the two-user fading MAC-WT scale with signal-to-noise ratio (SNR) as $\frac{1}{2}\log(\mathrm{SNR})$. Hence, we show the suboptimality of the independent identically distributed (i.i.d.) Gaussian signaling-based schemes with and without cooperative jamming by showing that the secrecy rates achieved using i.i.d. Gaussian signaling with cooperative jamming do not scale with SNR. In addition, we introduce an improved version of our ESA scheme where we incorporate cooperative jamming to achieve higher secrecy rates. Moreover, we derive the necessary optimality conditions for the power control policy that maximizes the secrecy sum rate achievable by our ESA scheme when used solely and with cooperative jamming. Finally, we discuss the extension of the proposed schemes to the case where there are more than two users and show that, for the K-user fading MAC-WT, each of the two schemes achieves secrecy sum rate that scales with SNR as $\frac{K-1}{K}\log(\mathrm{SNR})$.**

***Index Terms*—Ergodic alignment, fading Gaussian multiple access channel, information theoretic secrecy.**

I. Introduction

THE notion of information theoretic secrecy was first introduced by Shannon in his seminal work [3]. Applying the notion of information theoretic secrecy to channel models with single transmitter, single receiver, and single eavesdropper (wiretapper) was pioneered by Wyner [4], Csiszar and Korner [5], and Leung-Yan-Cheong and Hellman [6]. Wyner [4] introduced the wiretap channel where it is assumed that the received signal by the eavesdropper is a degraded version of the signal received by the legitimate receiver. For his model, Wyner established the secrecy capacity region, which is defined as the region of all simultaneously achievable rates and equivocation rates. In [5], the secrecy capacity region was established for the general case where the eavesdropper's channel is not necessarily a degraded version of the main receiver's channel. In particular, it was shown that to achieve the secrecy capacity region of the single user wiretap channel, channel prefixing may be necessary. In channel prefixing, an auxiliary random variable serves as the input of an artificially created prefix channel, whose output is used as the input to the original wiretap channel. In [6], the authors showed that, through plain Gaussian signaling alone, i.e., without channel prefixing, one can achieve the secrecy capacity of the Gaussian wiretap channel.

The multiple access wiretap channel (MAC-WT) was introduced in [7]. In MAC-WT, multiple users wish to have secure communication with a single receiver, in the presence of a passive eavesdropper. Tekin and Yener [7], [8] focus on the Gaussian MAC-WT and provide achievable schemes based on Gaussian signaling. They go further than plain Gaussian signaling and introduce a technique (on top of Gaussian signaling) that uses the power of a non-transmitting node in jamming the eavesdropper. This technique is called *cooperative jamming (CJ)*. CJ is indeed a channel prefixing technique where specific choices are made for the auxiliary random variables [9]. In addition, CJ is the first significant application of channel prefixing in a multiuser Gaussian wiretap channel that improves over plain Gaussian signaling. More recently, [10] showed that for a certain class of Gaussian MAC-WT, one can achieve through Gaussian signaling a secrecy rate region that is within 0.5 bits of the secrecy capacity region. Consequently, there has been some expectation that secrecy capacity may be obtained for Gaussian MAC-WT through independent identically distributed (i.i.d.) Gaussian signaling, potentially with Gaussian channel prefixing.

However, a notable shortcoming of these Gaussian signaling based achievable schemes is that rates obtained using them do not scale with the signal-to-noise ratio (SNR). In other words, the total number of degrees of freedom (DoF) for the MAC-WT achieved using these schemes is zero. This observation led to the belief that these schemes, and hence Gaussian signaling (with or without channel prefixing), may be suboptimal. This belief is made certain as a direct consequence of the results on the secure DoF of Gaussian interference networks that were obtained in several papers, e.g., in [11]–[15]. The schemes in each of [11] and [12] mainly relied on the *interference alignment* technique proposed by Cadambe and Jafar for the K-user interference channel in their pioneering work [16]. In the original interference alignment technique, the input data stream from each

Manuscript received October 25, 2010; revised July 09, 2011; accepted September 08, 2011. Date of current version February 29, 2012. This work was supported by the National Science Foundation under Grants CCF 04-47613, CCF 05-14846, CNS 07-16311, CCF 07-29127, and CCF 09-64645. The material in this paper was presented in part at the 47th Annual Allerton Conference on Communications, Control, and Computing, Monticello, IL, Sep. 2009 and the 2010 IEEE International Conference on Communications.

The authors are with the Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742 USA (e-mail: bassily@umd.edu; ulukus@umd.edu).

Communicated by S. A. Jafar, Associate Editor for Communications.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2011.2174613

user is mapped using a *precoding* matrix to a longer sequence (almost twice the original length in the asymptotic sense) and then sent over the channel. Hence, the observed signal space at each receiver is of *almost* twice the size (i.e., dimensionality) of the space of the original data. By carefully designing the precoding matrices at the transmitters, the observed signal space at each receiver could be partitioned into two almost equal subspaces, one of which is meant for the desired signal and the other acts as a waste basket for the interfering signals from other users. Consequently, it was shown that one can achieve $\frac{1}{2}$ DoF per user in the K-user interference channel using this technique. Inspired by this technique in the secrecy context, it was shown in [11] and [12] that positive secure DoF is achievable for a class of vector Gaussian interference channels. In fact, this result is also valid for time-varying channels with only causal knowledge of channel state information which, in turn, implies that positive secure DoF is achievable for the vector Gaussian MAC-WT in general. In [13] and [14], it was shown that through structured coding (e.g., lattice coding), it is possible to achieve positive DoF for a class of scalar (i.e., nontime-varying) Gaussian channels with interference that contains the Gaussian MAC-WT. More recently, in [15], both the Gaussian multiple-input multiple-output (MIMO) MAC-WT and the Gaussian scalar MAC-WT have been considered. For the K-user Gaussian MIMO MAC-WT model, [15] provides an algorithm which is inspired by the original interference alignment technique [16] to separate the received signals at the legitimate receiver and at the same time align them in a low-dimensional subspace in the signal space observed by the eavesdropper. For the K-user Gaussian scalar MAC-WT, [15] proposes an achievable secure coding scheme to achieve positive secure DoF. Namely, the proposed scheme achieves total secure DoF of $\frac{K-1}{K}$ for almost all channel gains. This is done by incorporating the new alignment technique known as real interference alignment that was first proposed in [17] that performs on a single real line and exploits the properties of real numbers to align interference in time-invariant channels.

Fading Gaussian MAC-WT was first considered in [18] where the Gaussian signaling and CJ schemes which were originally proposed in [7] and [8] are extended to the fading MAC-WT. Using these schemes, [18] gave achievable ergodic sum secrecy rates for the fading MAC-WT. Similar to the nonfading setting, these achievable ergodic secrecy rates do not scale with the average SNRs. In this paper, we propose two new achievable schemes for the fading Gaussian MAC-WT. Our first achievable scheme, the scaling based alignment (SBA) scheme, is based on code repetition with proper scaling of transmitted signals. We first consider the two-user fading MAC-WT. The generalization of this scheme to the case of more than two users is presented subsequently. In particular, for the two-user fading MAC-WT, transmitters repeat their symbols in two *consecutive* symbol instants. Transmitters further scale their transmit signals with the goal of creating a full-rank channel matrix at the main receiver and a unit-rank channel matrix at the eavesdropper, in every two consecutive time instants. These coordinated actions create a two-dimensional space for the signal received by the legitimate receiver, while sustaining the interference in a single-dimensional space at the eavesdropper. In other words, code repetition with proper scaling of the transmit signals at each transmitter *aligns* the received signals at the eavesdropper perfectly making it difficult for the eavesdropper to decode both messages. Consequently, we obtain a new achievable secrecy rate region for the two-user fading MAC-WT. In fact, it might be useful here to compare our SBA scheme with the technique used in [15] for the Gaussian MIMO MAC-WT. In the model considered here, we could create parallel MAC channels to each of the legitimate receiver and the eavesdropper by symbol repetition and exploiting the time-varying nature of fading channels and hence by proper scaling (precoding), one can almost surely create a full-dimensional space for the received signal at the legitimate receiver and one-dimensional space for the received signal at the eavesdropper. On the other hand, in [15], the existence of multiple spatial dimensions are already imposed by the model itself (Gaussian MIMO MAC-WT) and hence the precoding technique used in [15] for this model achieves secure DoF that eventually depends on the channel gain matrices from the transmitters to the legitimate receiver and the eavesdropper.

In another recent work [19], it was shown that in a fading interference channel, by code repetition over *properly chosen* time instants, one can perfectly cancel interference at each receiver so that the resulting individual rates scale as $\frac{1}{2}\log(\mathrm{SNR})$. Thus, the rate reduction by a factor of $\frac{1}{2}$ comes with the benefit of perfect interference cancellation. In this paper, we extend the ergodic interference alignment concept to a secrecy context and propose another achievable scheme which we call ergodic secret alignment (ESA). We first consider the two-user fading MAC-WT and generalize this scheme to the case of more than two users subsequently. In the SBA scheme, code repetition is done over two consecutive time instants, while in the ESA scheme, we carefully choose the time instants over which we do code repetition such that the received signals are aligned favorably at the legitimate receiver while they are aligned unfavorably at the eavesdropper. In particular, given some time instant with the vector of the main receiver channel coefficients and the vector of the eavesdropper channel coefficients given by $\mathbf{h} = [h_1\ h_2]^T$ and $\mathbf{g} = [g_1\ g_2]^T$, respectively, if X_1 and X_2 are the symbols transmitted in this time instant by users 1 and 2, respectively, our objective, roughly speaking, is to determine the channel gains we should wait for to transmit X_1 and X_2 again. In this paper, we show that, in order to maximize achievable secrecy rates, we should wait for a time instant in which the main receiver channel coefficients are $[h_1 - h_2]^T$ and the eavesdropper channel coefficients are $[g_1\ g_2]^T$. Consequently, we obtain another achievable secrecy rate region for the two-user fading MAC-WT.

For both proposed schemes, we show that the resulting secrecy rates scale with SNR. Specifically, the achievable secrecy sum rate scales as $\frac{1}{2}\log(\mathrm{SNR})$. Moreover, we show that the secrecy rates achieved through i.i.d. Gaussian signaling with CJ in fading MAC-WT do not scale with SNR. The significance of these results is that, they show that indeed neither plain i.i.d. Gaussian signaling nor i.i.d. Gaussian signaling with CJ is optimal for the fading MAC-WT, and that, for high SNRs, one can achieve higher secrecy rates by aligning interference perfectly in the eavesdropper MAC while reducing, or canceling, interference at the main receiver MAC using some coordinated actions at both transmitters that involve code repetition, i.e., a form of time-correlated (non-i.i.d.) signaling.

In fact, the achievable rate region using the second scheme, the ESA scheme, involves two significant improvements over the one achieved by the SBA scheme when the channel coefficients are circularly symmetric complex Gaussian random variables. First, the expressions for achievable rates by the SBA scheme involve products of the squared magnitudes of the channel coefficients. The squared magnitudes of the channel coefficients are exponential random variables and hence multiplying them together gives a random variable that takes small values with higher probability than the original exponential random variables would take these values. This in effect reduces the achievable rates by the SBA scheme. On the other hand, the achievable secrecy rates by the ESA scheme do not have this drawback. In other words, by code repetition, the SBA scheme creates two (not perfectly) correlated MAC channels to the main receiver and two perfectly correlated MAC channels to the eavesdropper, while the ESA scheme creates an orthogonal MAC channel to the main receiver and two perfectly correlated MAC channels to the eavesdropper. This fact leads to higher achievable secrecy rates by the ESA scheme. The second improvement of the ESA scheme with respect to the SBA scheme is that the average power constraints associated with the ESA scheme do not involve any channel coefficients, whereas those associated with the SBA scheme involve the gains of the eavesdropper channel which, in turn, result in inefficient use of transmit powers. However, it is noteworthy that SBA scheme holds one practical advantage over the ESA scheme that actually does not appear in the achievable rates by the two schemes. Namely, in the SBA scheme, we do not wait for favorable channel conditions for alignment since repetition is done over consecutive time slots. On the other hand, in the ESA scheme, one should wait for the proper channel conditions before repetition takes place. The waiting time required to match up the channel states is an important performance factor for the ESA scheme in practice.

In addition, we introduce an improved version of our second scheme in which we use CJ on top of the ESA scheme to achieve higher secrecy rates. Moreover, since the rate expressions achieved by the ESA scheme (with and without CJ) and their associated average power constraints are simpler than their counterparts in the SBA scheme, we derive the necessary conditions on the optimal power allocations that maximize the sum secrecy rate achieved by the ESA scheme when used alone and when used together with CJ. Since the achievable secrecy sum rate, in general, is not a concave function in the power allocation policy, the solution of such optimization problem may not be unique. Hence, we obtain a power allocation policy that satisfies the necessary (but not necessarily sufficient) Karush–Kuhn–Tucker (KKT) conditions of optimality.

We provide numerical examples that illustrate the scaling of the sum rates achieved by the proposed schemes with SNR and the saturation of the secrecy sum rate achieved by the i.i.d. Gaussian signaling scheme with CJ. We also give numerical examples for the secrecy sum rates achieved by the ESA scheme with and without CJ when power control is used.

Finally, we discuss the extension of the SBA and the ESA schemes to the case of K-user fading MAC-WT channel for $K \geq 2$. We show that each of the two schemes achieves a total of $\frac{K-1}{K}$ secure DoF which is the same total secure DoF shown in [15] to be achievable for the K-user Gaussian scalar MAC-WT for almost all channel gains using the real interference alignment technique.

II. System Model

We consider the two-user fading multiple access channel with an external eavesdropper. Transmitter k chooses a message W_k from a set of equally likely messages $\mathcal{W}_k = \{1, \ldots, 2^{2nR_k}\}$, $k = 1, 2$. Every transmitter encodes its message into a codeword of length $2n$ symbols. The channel output at the intended receiver and the eavesdropper at the symbol interval t are given by

$$Y_t = h_{1t}X_{1t} + h_{2t}X_{2t} + N_t \tag{1}$$

$$Z_t = g_{1t}X_{1t} + g_{2t}X_{2t} + N'_t \tag{2}$$

where, for $k = 1, 2$, X_{kt} is the input signal at transmitter k at channel use t, h_{kt}, g_{kt} are the channel coefficients at channel use t between transmitter k and the intended receiver and the eavesdropper, respectively. We assume a fast fading scenario where the channel coefficients randomly vary from one symbol to another in i.i.d. fashion. Also, we assume the independence of all channel coefficients h_{kt} and g_{kt} for all k, t. Each of the channel coefficients is a circularly symmetric complex Gaussian random variable with zero-mean. The variances of h_{kt} and g_{kt} are $\sigma^2_{h_k}$ and $\sigma^2_{g_k}$, respectively, for all t. Hence, $|h_{kt}|^2$ and $|g_{kt}|^2$ are exponentially distributed random variables with mean $\sigma^2_{h_k}$ and $\sigma^2_{g_k}$, respectively. Moreover, we assume that all the channel coefficients are known to all the nodes in a causal fashion. In (1)–(2), N_t and N'_t are the independent Gaussian noises at the intended receiver and the eavesdropper, respectively, and are i.i.d. (in time) circularly symmetric complex Gaussian random variables with zero-mean and unit-variance. For the rest of this paper, we will drop the time index t for notational convenience unless it is clearly stated otherwise. We have the usual average power constraints

$$E[|X_k|^2] \leq \bar{P}_k, \quad k = 1, 2. \tag{3}$$

A $(2^{2nR_1}, 2^{2nR_2}, 2n)$ code for this channel consists of two encoders φ_k, $k = 1, 2$ which maps a message $W_k \in \mathcal{W}_k$ to a sequence of complex numbers X_k^{2n}, and a decoder ψ which maps the received sequence at the main receiver Y^{2n} and the channel state sequences h_1^{2n}, h_2^{2n}, g_1^{2n}, g_2^{2n} to an estimate of the message pair $(\hat{W}_1, \hat{W}_2) \in \mathcal{W}_1 \times \mathcal{W}_2$. The probability of error is $P_e^{2n} = \Pr\left((\hat{W}_1, \hat{W}_2) \neq (W_1, W_2)\right)$. A rate pair (R_1, R_2) is said to be achievable with perfect secrecy if there is a $(2^{2nR_1}, 2^{2nR_2}, 2n)$ code satisfying $\lim_{n\to\infty} P_e^{2n} = 0$ and $\lim_{n\to\infty} \frac{1}{2n} I\left(W_1, W_2; Z^{2n} | h_1^{2n}, h_2^{2n}, g_1^{2n}, g_2^{2n}\right) = 0$.

III. Previously Known Results

Here, we summarize previously known results that are relevant to our development. For the general discrete-time memoryless MAC-WT, the best known achievable secrecy rate region [7]–[9] is given by the convex hull of all rate pairs (R_1, R_2) satisfying

$$R_1 \leq I(V_1; Y|V_2) - I(V_1; Z) \tag{4}$$

$$R_2 \leq I(V_2; Y|V_1) - I(V_2; Z) \tag{5}$$

$$R_1 + R_2 \leq I(V_1, V_2; Y) - I(V_1, V_2; Z) \tag{6}$$

where the distribution $p(x_1, x_2, v_1, v_2, y, z)$ factors as $p(v_1)p(x_1|v_1)p(v_2)p(x_2|v_2)p(y, z|x_1, x_2)$.

Known secrecy rate regions for the Gaussian MAC-WT can be obtained from these expressions by appropriate selections for the involved random variables. For instance, the Gaussian signaling-based achievable rates proposed in [7] are obtained by choosing $X_1 = V_1$ and $X_2 = V_2$, i.e., no channel prefixing, and by choosing X_1 and X_2 to be Gaussian with full power. On the other hand, CJ-based achievable rates proposed in [8] are obtained by choosing $X_1 = V_1 + T_1$ and $X_2 = V_2 + T_2$, and then by choosing V_1, V_2, T_1, T_2 to be independent Gaussian random variables [9]. Namely, for $k = 1, 2$, V_k and T_k are Gaussian random variables with zero mean and variances P_k and Q_k, respectively. Here, V_1 and V_2 carry messages, while T_1 and T_2 are jamming signals. The powers of (V_1, T_1) and (V_2, T_2) should be chosen to satisfy the power constraints of users 1 and 2, respectively. These selections yield the following achievable rate region for the Gaussian MAC-WT [8]:

$$R_1 \leq \log\left(1 + \frac{|h_1|^2 P_1}{1 + |h_1|^2 Q_1 + |h_2|^2 Q_2}\right) - \log\left(1 + \frac{|g_1|^2 P_1}{1 + |g_1|^2 Q_1 + |g_2|^2 (P_2 + Q_2)}\right) \tag{7}$$

$$R_2 \leq \log\left(1 + \frac{|h_2|^2 P_2}{1 + |h_1|^2 Q_1 + |h_2|^2 Q_2}\right) - \log\left(1 + \frac{|g_2|^2 P_2}{1 + |g_1|^2 (P_1 + Q_1) + |g_2|^2 Q_2}\right) \tag{8}$$

$$R_1 + R_2 \leq \log\left(1 + \frac{|h_1|^2 P_1 + |h_2|^2 P_2}{1 + |h_1|^2 Q_1 + |h_2|^2 Q_2}\right) - \log\left(1 + \frac{|g_1|^2 P_1 + |g_2|^2 P_2}{1 + |g_1|^2 Q_1 + |g_2|^2 Q_2}\right) \tag{9}$$

where the powers of the signals must satisfy

$$P_k + Q_k \leq \bar{P}_k, \quad k = 1, 2 \tag{10}$$

where P_k and Q_k are the transmission and jamming powers, respectively, of user k.

The ergodic secrecy rate region achieved by Gaussian signaling and CJ for the fading MAC-WT can be expressed similarly by simply including expectations over fading channel states [18]

$$R_1 \leq E_{\mathbf{h},\mathbf{g}}\left\{ \log\left(1 + \frac{|h_1|^2 P_1}{1 + |h_1|^2 Q_1 + |h_2|^2 Q_2}\right) - \log\left(1 + \frac{|g_1|^2 P_1}{1 + |g_1|^2 Q_1 + |g_2|^2 (P_2 + Q_2)}\right) \right\} \tag{11}$$

$$R_2 \leq E_{\mathbf{h},\mathbf{g}}\left\{ \log\left(1 + \frac{|h_2|^2 P_2}{1 + |h_1|^2 Q_1 + |h_2|^2 Q_2}\right) - \log\left(1 + \frac{|g_2|^2 P_2}{1 + |g_1|^2 (P_1 + Q_1) + |g_2|^2 Q_2}\right) \right\} \tag{12}$$

$$R_1 + R_2 \leq E_{\mathbf{h},\mathbf{g}}\left\{ \log\left(1 + \frac{|h_1|^2 P_1 + |h_2|^2 P_2}{1 + |h_1|^2 Q_1 + |h_2|^2 Q_2}\right) - \log\left(1 + \frac{|g_1|^2 P_1 + |g_2|^2 P_2}{1 + |g_1|^2 Q_1 + |g_2|^2 Q_2}\right) \right\} \tag{13}$$

where $\mathbf{h} = [h_1 \ h_2]^T$, $\mathbf{g} = [g_1 \ g_2]^T$, and the instantaneous powers P_k and Q_k, which are both functions of $\mathbf{h}$ and $\mathbf{g}$, satisfy

$$E[P_k + Q_k] \leq \bar{P}_k, \ k = 1, 2 \tag{14}$$

IV. Scaling Based Alignment (SBA)

In this section, we introduce a new achievable scheme for the fading MAC-WT. Our achievable scheme is based on code repetition with proper scaling of the signals transmitted by each transmitter. This is done as follows. For the channel described in (1) and (2), we use a repetition code such that each transmitter repeats its channel input symbol twice over two *consecutive* time instants. Due to code repetition, we may regard each of the MACs to the main receiver and to the eavesdropper as a vector MAC composed of two parallel scalar MACs, one for the *odd* time instants and the other for the *even* time instants. Consequently, we may describe the main receiver MAC channel by the following pair of equations:

$$Y_o = h_{1o} X_1 + h_{2o} X_2 + N_o \tag{15}$$

$$Y_e = h_{1e} X_1 + h_{2e} X_2 + N_e \tag{16}$$

where, for $k = 1, 2$, h_{ko}, h_{ke} are the coefficients of the kth main receiver channel in odd and even time instants, Y_o, Y_e and N_o, N_e are the received signal and the noise at the main receiver in odd and even time instants. In the same way, we may describe the eavesdropper MAC channel by the following pair of equations:

$$Z_o = g_{1o} X_1 + g_{2o} X_2 + N'_o \tag{17}$$

$$Z_e = g_{1e} X_1 + g_{2e} X_2 + N'_e \tag{18}$$

where for $k = 1, 2$, g_{ko}, g_{ke} are the coefficients of the kth eavesdropper channel in odd and even time instants, Z_o, Z_e and N_o, N_e are the received signal and the noise at the eavesdropper in odd and even time instants.

Since all the channel gains are known to all nodes in a causal fashion, the two transmitters use this knowledge as follows. In every symbol instant, each transmitter scales its transmit signal with the gain of the other transmitter's channel to the eavesdropper. That is, in every symbol duration, the first user multiplies its channel input with g_2, the channel gain of the second user to the eavesdropper, and the second user multiplies its channel input with g_1, the channel gain of the first user to the eavesdropper. Hence the main receiver MAC can be described as

$$Y_o = h_{1o} g_{2o} X_1 + h_{2o} g_{1o} X_2 + N_o \tag{19}$$

$$Y_e = h_{1e} g_{2e} X_1 + h_{2e} g_{1e} X_2 + N_e \tag{20}$$

and the eavesdropper MAC can be described as

$$Z_o = g_{1o} g_{2o} X_1 + g_{1o} g_{2o} X_2 + N'_o \tag{21}$$

$$Z_e = g_{1e}g_{2e}X_1 + g_{1e}g_{2e}X_2 + N\prime_e. \tag{22}$$

It is clear from (19) and (20) that the space of the received signal (without noise, i.e., high SNR) of the main receiver over the two consecutive time instants is 2-D almost surely. In other words, the channel matrix of the main receiver vector MAC is full-rank almost surely. This is due to the fact that the channel coefficients are drawn from continuous bounded distributions. On the other hand, it is clear from (21) and (22) that the channel matrix of the eavesdropper vector MAC is unit-rank. That is, the two ingredients of our scheme, i.e., code repetition and signal scaling, let the interfering signals at the main receiver live in a 2-D space, while they *align* the interfering signals at the eavesdropper in a 1-D space. As we will show in the Section VI, these properties play a central role in achieving secrecy rates that scale with SNR.

Let $\mathbf{h}_o = (h_{1o}, h_{2o})$ and $\mathbf{h}_e = (h_{1e}, h_{2e})$. We define $\mathbf{g}_o$ and $\mathbf{g}_e$ in the same way. For $k = 1, 2$, we define the power allocation policy of transmitter k as a mapping $P_k : \mathbb{C}^4 \to \mathbb{R}_+$ which maps $(\mathbf{h}_o, \mathbf{g}_o)$ to a nonnegative real number $P_k(\mathbf{h}_o, \mathbf{g}_o)$ which is the power of transmitter k in the odd time slot for which the values of channel gains are $(\mathbf{h}_o, \mathbf{g}_o)$. Note that due to symbol repetition, P_k is a function of $(\mathbf{h}_o, \mathbf{g}_o)$ only and does not depend on $(\mathbf{h}_e, \mathbf{g}_e)$. To simplify notation, we will use P_k to denote $P_k(\mathbf{h}_o, \mathbf{g}_o)$ since this dependence on channel gains is implicitly understood. We note that, due to signal scaling at the transmitters, the average power constraints become

$$E\left[\left(|g_{2o}|^2 + |g_{2e}|^2\right) P_1\right] \le \bar{P}_1 \tag{23}$$
$$E\left[\left(|g_{1o}|^2 + |g_{1e}|^2\right) P_2\right] \le \bar{P}_2. \tag{24}$$

Now, we evaluate the secrecy rate region achievable by our SBA scheme. Given the vector channels (19), (20) and (21), (22), the following secrecy rates are achievable [7]–[9]:

$$R_1 \le \frac{1}{2}\left[I(X_1; Y_o, Y_e | X_2, \mathbf{h}, \mathbf{g}) - I(X_1; Z_o, Z_e | \mathbf{h}, \mathbf{g})\right] \tag{25}$$
$$R_2 \le \frac{1}{2}\left[I(X_2; Y_o, Y_e | X_1, \mathbf{h}, \mathbf{g}) - I(X_2; Z_o, Z_e | \mathbf{h}, \mathbf{g})\right] \tag{26}$$
$$R_1 + R_2 \le \frac{1}{2}\left[I(X_1, X_2; Y_o, Y_e | \mathbf{h}, \mathbf{g}) - I(X_1, X_2; Z_o, Z_e | \mathbf{h}, \mathbf{g})\right] \tag{27}$$

where $\mathbf{h} = (\mathbf{h}_o, \mathbf{h}_e)$ and $\mathbf{g} = (\mathbf{g}_o, \mathbf{g}_e)$. These expressions for achievable rates follow from (4)–(6) by treating channel states as outputs at the receivers, and noting the independence of channel inputs and channel states. We note that the factor of $\frac{1}{2}$ on the right-hand sides of (25)–(27) is due to repetition coding. Now, by computing (25)–(27) with Gaussian signals, we obtain the secrecy rate region given in the following theorem.

Theorem 1: For the two-user fading MAC-WT, the rate region given by all rate pairs (R_1, R_2) satisfying constraints (28)–(30), shown at the bottom of the page, is achievable with perfect secrecy where P_1, P_2 are the power allocation policies (as defined above) of users 1 and 2, respectively, that satisfy

$$E\left[\left(|g_{2o}|^2 + |g_{2e}|^2\right) P_1\right] \le \bar{P}_1 \tag{31}$$
$$E\left[\left(|g_{1o}|^2 + |g_{1e}|^2\right) P_2\right] \le \bar{P}_2 \tag{32}$$

where $\bar{P}_1$ and $\bar{P}_2$ are the average power constraints.

V. Ergodic Secret Alignment (ESA)

After we have devised the SBA scheme, the ergodic interference alignment scheme of Nazer *et al.* [19] inspired us to propose an improved achievable scheme. In this section, we discuss this scheme which we call ESA. The new ingredient in this scheme is to perform repetition coding at two *carefully chosen* time instances as opposed to two *consecutive* time instances as we have done in Section IV.

For the MAC-WT described by (1) and (2), we use a repetition code in a way similar to the one in [19]. The simple idea of the scheme is that we repeat each code symbol in the time instant that holds certain channel conditions relative to the those conditions in the time instant where this code symbol is first transmitted. Namely, given a time instant with the main receiver channel state vector $\mathbf{h} = [h_1\ h_2]^T$ and the eavesdropper channel state vector $\mathbf{g} = [g_1\ g_2]^T$, where the symbols X_1 and X_2 are first transmitted by the two transmitters, we will solve for the channel states $\tilde{\mathbf{h}} = [\tilde{h}_1\ \tilde{h}_2]^T$ and $\tilde{\mathbf{g}} = [\tilde{g}_1\ \tilde{g}_2]^T$, where these symbols should be repeated again, such that the resulting secrecy rates achieved by Gaussian signaling are maximized.

The aforementioned description is an intuitive description that gives the idea of the scheme which is based on the concept of ergodic interference alignment introduced in [19]. A rigorous description and proof follow the arguments in [19]. In particular, the idea of the proof [19] is first to quantize the channel coefficients and deal with the quantized coefficients rather than dealing with the original coefficients defined over

$$R_1 \le \frac{1}{2} E_{\mathbf{h},\mathbf{g}}\left\{\log\left(1 + (|h_{1o}g_{2o}|^2 + |h_{1e}g_{2e}|^2)P_1\right) - \log\left(1 + \frac{(|g_{1o}g_{2o}|^2 + |g_{1e}g_{2e}|^2)P_1}{1 + (|g_{1o}g_{2o}|^2 + |g_{1e}g_{2e}|^2)P_2}\right)\right\} \tag{28}$$

$$R_2 \le \frac{1}{2} E_{\mathbf{h},\mathbf{g}}\left\{\log\left(1 + (|h_{2o}g_{1o}|^2 + |h_{2e}g_{1e}|^2)P_2\right) - \log\left(1 + \frac{(|g_{1o}g_{2o}|^2 + |g_{1e}g_{2e}|^2)P_2}{1 + (|g_{1o}g_{2o}|^2 + |g_{1e}g_{2e}|^2)P_1}\right)\right\} \tag{29}$$

$$R_1 + R_2 \le \frac{1}{2} E_{\mathbf{h},\mathbf{g}}\Bigg\{\log\Big(1 + \left(|h_{1o}g_{2o}|^2 + |h_{1e}g_{2e}|^2\right) P_1 + \left(|h_{2o}g_{1o}|^2 + |h_{2e}g_{1e}|^2\right) P_2 + |h_{1e}h_{2o}g_{1o}g_{2e} - h_{1o}h_{2e}g_{1e}g_{2o}|^2 P_1 P_2\Big) - \log\left(1 + \left(|g_{1o}g_{2o}|^2 + |g_{1e}g_{2e}|^2\right)(P_1 + P_2)\right)\Bigg\} \tag{30}$$

the whole complex plane. Then, one can show that those quantized channel coefficients of the same type (distribution) could be paired with another set of quantized channel coefficients of a *symmetric* type. Consequently, one can derive the achievable rate when such pairing between symmetric types is employed. Finally, using the continuity of the achievable rate as a function in channel coefficients, one can argue that by decreasing the quantization bin size, one can approach the desired rate for the original channel (with complex coefficients) in the limit. The detailed proof is found in [19].

Due to code repetition, we may regard each of the MACs to the main receiver and to the eavesdropper as a vector MAC composed of two parallel scalar MACs, one for each one of the two time instants over which the same code symbols X_1 and X_2 are transmitted. Consequently, we may describe the main receiver MAC channel by the following pair of equations:

$$Y_1 = h_1 X_1 + h_2 X_2 + N_1 \tag{33}$$
$$Y_2 = \tilde{h}_1 X_1 + \tilde{h}_2 X_2 + N_2 \tag{34}$$

where Y_1, Y_2 and N_1, N_2 are the received symbols and the noise at the main receiver in the two time instants of code repetition. In the same way, we may describe the eavesdropper MAC channel by the following pair of equations:

$$Z_1 = g_1 X_1 + g_2 X_2 + N_1' \tag{35}$$
$$Z_2 = \tilde{g}_1 X_1 + \tilde{g}_2 X_2 + N_2' \tag{36}$$

where Z_1, Z_2 and N_1', N_2' are the received symbols and the noise at the eavesdropper in the two time instants of code repetition. For $k = 1, 2$, we define the power allocation policy P_k of transmitter k in a way similar to the way it was defined in the SBA scheme. Namely, it is defined as a mapping $P_k : \mathbb{C}^4 \to \mathbb{R}_+$ which maps the values of the channel gains $(\mathbf{h}, \mathbf{g})$ to a nonnegative real number $P_k(\mathbf{h}, \mathbf{g})$ which is the power of transmitter k when the channel gains take the values $(\mathbf{h}, \mathbf{g})$. Again, to simplify notation, we will use P_k to denote $P_k(\mathbf{h}, \mathbf{g})$ since this dependence on channel gains is implicitly understood.

In the next theorem, we give another achievable secrecy rate region for the two-user fading MAC-WT. The achievable region is obtained using (25)–(27) and replacing (Y_o, Y_e) and (Z_o, Z_e) with (Y_1, Y_2) and (Z_1, Z_2), respectively, and evaluating these expressions with Gaussian signals, and by choosing optimal $\tilde{\mathbf{h}} = (\tilde{h}_1, \tilde{h}_2)$ and $\tilde{\mathbf{g}} = (\tilde{g}_1, \tilde{g}_2)$ to maximize the achievable rates. As we will show shortly as a result of Theorem 2, the optimal selection of $\tilde{\mathbf{h}}$ and $\tilde{\mathbf{g}}$ will yield an *orthogonal* MAC to the main receiver and a *scalar* MAC to the eavesdropper. In writing the achievable rate expressions, we will again account for code repetition by multiplying achievable rates by a factor of $\frac{1}{2}$.

Theorem 2: For the two-user fading MAC-WT, the rate region given by all rate pairs (R_1, R_2) satisfying the following constraints is achievable with perfect secrecy:

$$R_1 \le \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \left\{ \log\left(1+2|h_1|^2 P_1\right) - \log\left(1 + \frac{2|g_1|^2 P_1}{1+2|g_2|^2 P_2}\right) \right\} \tag{37}$$

$$R_2 \le \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \left\{ \log\left(1+2|h_2|^2 P_2\right) - \log\left(1 + \frac{2|g_2|^2 P_2}{1+2|g_1|^2 P_1}\right) \right\} \tag{38}$$

$$R_1 + R_2 \le \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \left\{ \log\left(1+2|h_1|^2 P_1\right) + \log\left(1+2|h_2|^2 P_2\right) - \log\left(1 + 2(|g_1|^2 P_1 + |g_2|^2 P_2)\right) \right\} \tag{39}$$

where P_1 and P_2 are the power allocation policies of users 1 and 2, respectively, and are both functions of $\mathbf{h}$ and $\mathbf{g}$ in general (as defined previously). In addition, they satisfy the average power constraints

$$E[P_1] \le \bar{P}_1 \tag{40}$$
$$E[P_2] \le \bar{P}_2. \tag{41}$$

Proof: First, consider the two vector MACs given by (33)–(36). Observe that as in [19], $\tilde{\mathbf{h}}$ must be chosen such that it has the same distribution as $\mathbf{h}$ and $\tilde{\mathbf{g}}$ must be chosen such that it has the same distribution as $\mathbf{g}$. The reason for this can be understood from the idea of the proof in [19] discussed earlier in this section. Indeed, in the quantized channel, in order for the pairing between channel coefficients at two different instants to be possible, the values of the channel coefficients at the two time instants must occur with the same probability. That is why we require that $\tilde{\mathbf{h}}$ and $\tilde{\mathbf{g}}$ to have the same distributions as $\mathbf{h}$ and $\mathbf{g}$, respectively. Now, since $\mathbf{h} \sim \mathcal{CN}(\mathbf{0}, \mathbf{B}_h)$ and $\mathbf{g} \sim \mathcal{CN}(\mathbf{0}, \mathbf{B}_g)$ where $\mathbf{B}_h = \mathrm{diag}(\sigma^2_{h_1}, \sigma^2_{h_2})$ and $\mathbf{B}_g = \mathrm{diag}(\sigma^2_{g_1}, \sigma^2_{g_2})$, then in order to achieve the requirement above, it follows from the symmetry property of the complex Gaussian distribution that the channel realizations $\mathbf{h}$ and $\mathbf{g}$ must be paired with the channel realizations $\tilde{\mathbf{h}}$ and $\tilde{\mathbf{g}}$, respectively, that are related as $\tilde{\mathbf{h}} = \mathbf{U}\mathbf{h}$ and $\tilde{\mathbf{g}} = \mathbf{V}\mathbf{g}$ for some unitary matrices $\mathbf{U}$ and $\mathbf{V}$ (rotations in $\mathbb{C}^2$). Furthermore, for such rotations to preserve the variances of the individual components of $\mathbf{h}$ (i.e., $\sigma^2_{h_1}, \sigma^2_{h_2}$) and of $\mathbf{g}$ (i.e., $\sigma^2_{g_1}, \sigma^2_{g_2}$), we must have $\mathbf{U} = \mathrm{diag}(\exp(j\theta_1), \exp(j\theta_2))$ and $\mathbf{V} = \mathrm{diag}(\exp(j\omega_1), \exp(j\omega_2))$ for some θ_1, θ_2, ω_1, $\omega_2 \in [0, 2\pi)$. Then, it follows that (33)–(36) can be written as

$$Y_1 = h_1 X_1 + h_2 X_2 + N_1 \tag{42}$$
$$Y_2 = h_1 e^{j\theta_1} X_1 + h_2 e^{j\theta_2} X_2 + N_2 \tag{43}$$
$$Z_1 = g_1 X_1 + g_2 X_2 + N_1' \tag{44}$$
$$Z_2 = g_1 e^{j\omega_1} X_1 + g_2 e^{j\omega_2} X_2 + N_2'. \tag{45}$$

Using (25)–(27) and replacing (Y_o, Y_e) and (Z_o, Z_e) with (Y_1, Y_2) and (Z_1, Z_2), respectively, and computing these achievable rates with Gaussian signals, we get (46)–(48), shown at the bottom of the next page, where $\theta = \theta_2 - \theta_1$ and $\omega = \omega_2 - \omega_1$.

Hence, the largest achievable secrecy rate region (46)–(48) is attained by choosing $\theta = \pi$ and $\omega = 0$. This can be achieved by choosing $\theta_1 = 0$ and $\theta_2 = \pi$ and by choosing $\omega_1 = \omega_2 = 0$. Consequently, we have $\tilde{\mathbf{h}} = [h_1 \; -h_2]^T$ and $\tilde{\mathbf{g}} = [g_1 \; g_2]^T$. By substituting these values of θ and ω in (46)–(48), we obtain the region given by (37)–(39). ∎

Therefore, when using the ESA technique, the best choice for $\tilde{h}_1$ and $\tilde{h}_2$ is such that $\tilde{\mathbf{h}}$ is orthogonal to $\mathbf{h}$ and that $\|\tilde{\mathbf{h}}\| = \|\mathbf{h}\|$, and the best choice for $\tilde{g}_1$ and $\tilde{g}_2$ is such that $\tilde{\mathbf{g}}$ and $\mathbf{g}$ are linearly dependent and that $\|\tilde{\mathbf{g}}\| = \|\mathbf{g}\|$, i.e., $\tilde{\mathbf{g}} = \mathbf{g}$. This choice makes

the vector MAC between the two transmitters and the main receiver equivalent to an orthogonal MAC, i.e., two independent single-user fading channels, one from each transmitter to the main receiver. This equivalent main receiver MAC channel can be expressed as

$$\bar{Y}_1 = 2h_1X_1 + \bar{N}_1 \tag{49}$$
$$\bar{Y}_2 = 2h_2X_2 + \bar{N}_2 \tag{50}$$

where $\bar{Y}_1 = Y_1 + Y_2$, $\bar{Y}_2 = Y_1 - Y_2$, $\bar{N}_1 = N_1 + N_2$, and $\bar{N}_2 = N_1 - N_2$. Note that $\bar{N}_1$ and $\bar{N}_2$ are independent. On the other hand, this choice makes the vector MAC between the two transmitters and the eavesdropper equivalent to a single scalar MAC. This equivalent eavesdropper MAC channel can be expressed as

$$\bar{Z}_1 = 2g_1X_1 + 2g_2X_2 + \bar{N}_1' \tag{51}$$
$$\bar{Z}_2 = \bar{N}_2' \tag{52}$$

where $\bar{Z}_1 = Z_1 + Z_2$, $\bar{Z}_2 = Z_1 - Z_2$, $\bar{N}_1' = N_1' + N_2'$, and $\bar{N}_2' = N_1' - N_2'$. Note again that $\bar{N}_1$ and $\bar{N}_2$ are independent. Note that, here, the second component of the eavesdropper's vector MAC is useless for her (i.e., leaks no further information than the first component) as it contains only noise. This selection of the repetition channel state yields a most favorable setting for the main receiver and a least favorable setting for the eavesdropper.

VI. Degrees of Freedom (DoF)

In this section, we show that the secrecy sum rates achieved by our schemes scale with SNR as $\frac{1}{2}\log(\mathrm{SNR})$ and that the secrecy sum rate achieved by the CJ scheme given in [18] does not scale with SNR. What we give here are rigorous proofs for intuitive results. Since by looking at (30) and (39), one can note that, if we assume that $\bar{P}_1 = \bar{P}_2 = P$, then if we take $P_1 = P_2 = P$, as P becomes large, roughly speaking, in (30) the first term inside the expectation grows as $\log(P^2)$ while the second term grows as $\log(P)$ and hence the overall expression grows as $\frac{1}{2}\log(P)$; and similarly, in (39), all three terms inside the expectation grow as $\log(P)$ and hence the overall expression grows as $\frac{1}{2}\log(P)$. In the same way, by considering the secrecy sum rate achieved by the CJ scheme given in (13), then by referring to the power allocation policies given in [18], one can also roughly say that for all channel states, as the available average power goes to infinity, the overall expression converges to a constant.

For simplicity, we assume symmetric average power constraints for all schemes, i.e., we set $\bar{P}_1 = \bar{P}_2 = P$ in (31)–(32), (40)–(41), and (14). We also assume that all channel gains are drawn from continuous bounded distributions and that all channel gains have finite variances. Let R_s be the achievable secrecy sum rate, then the total number of achievable secure DoF, η, is defined as

$$\eta \stackrel{\triangle}{=} \lim_{P\to\infty} \frac{R_s}{\log(P)} \tag{53}$$

We start by the DoF analysis of our proposed schemes, i.e., the SBA scheme and the ESA scheme, where we show that the sum secrecy rates obtained by these schemes achieve $\frac{1}{2}$ secure DoF, then we provide a rigorous proof for the fact that the scheme of [18] which is based on i.i.d. Gaussian signaling with CJ achieves a secrecy sum rate that does not scale with SNR, i.e., achieves zero secure DoF.

A. Secure DoF With the SBA Scheme

We make the following choices for the power allocation policies P_1 and P_2 of the SBA scheme. We set $P_1 = \frac{1}{2\sigma_{g_2}^2}P$, $P_2 = \frac{1}{2\sigma_{g_1}^2}P$. It can be verified that these choices satisfy the power constraints (31)–(32). Denoting the expression inside the expectation in (30) by $f_P(\mathbf{h},\mathbf{g})$, the secrecy sum rate achieved using the SBA scheme can be written as

$$R_s = \frac{1}{2}E_{\mathbf{h},\mathbf{g}}\left\{f_P(\mathbf{h},\mathbf{g})\right\}. \tag{54}$$

Hence, the total achievable secure DoF is given by

$$\eta = \frac{1}{2}\lim_{P\to\infty} E_{\mathbf{h},\mathbf{g}}\left[\frac{f_P(\mathbf{h},\mathbf{g})}{\log(P)}\right]. \tag{55}$$

Now, we show that, for the two-user fading MAC-WT, a total number of secure DoF $\eta = \frac{1}{2}$ is achievable with the SBA scheme. Toward this end, it suffices to show that the order of the limit and the expectation in (55) can be reversed. To do this, we make use of Lebesgue dominated convergence theorem. Now, we note that for large enough P, $\frac{f_P(\mathbf{h},\mathbf{g})}{\log(P)}$ is upper bounded by $\psi(\mathbf{h},\mathbf{g})$ given by (56), shown at the bottom of the next page.

$$R_1 \le \frac{1}{2}E_{\mathbf{h},\mathbf{g}}\left\{\log\left(1+2|h_1|^2P_1\right) - \log\left(1+\frac{2|g_1|^2P_1 + 2(1-\cos(\omega))|g_1|^2|g_2|^2P_1P_2}{1+2|g_2|^2P_2}\right)\right\} \tag{46}$$

$$R_2 \le \frac{1}{2}E_{\mathbf{h},\mathbf{g}}\left\{\log\left(1+2|h_2|^2P_2\right) - \log\left(1+\frac{2|g_2|^2P_2 + 2(1-\cos(\omega))|g_1|^2|g_2|^2P_1P_2}{1+2|g_1|^2P_1}\right)\right\} \tag{47}$$

$$\begin{aligned} R_1+R_2 \le \frac{1}{2}E_{\mathbf{h},\mathbf{g}}\Big\{ &\log(1+2|h_1|^2P_1+2|h_2|^2P_2+2(1-\cos(\theta))|h_1|^2|h_2|^2P_1P_2) \\ &- \log(1+2|g_1|^2P_1+2|g_2|^2P_2+2(1-\cos(\omega))|g_1|^2|g_2|^2P_1P_2)\Big\} \end{aligned} \tag{48}$$

Hence, using the fact that all channel gains have finite variances together with Jensen's inequality, we have

$$E_{\mathbf{h},\mathbf{g}}\left[\psi(\mathbf{h},\mathbf{g})\right] < \infty \tag{57}$$

Thus, by the dominated convergence theorem, we have

$$\lim_{P\to\infty} E_{\mathbf{h},\mathbf{g}}\left[\frac{f_P(\mathbf{h},\mathbf{g})}{\log(P)}\right] = E_{\mathbf{h},\mathbf{g}}\left[\lim_{P\to\infty}\frac{f_P(\mathbf{h},\mathbf{g})}{\log(P)}\right] = 1. \tag{58}$$

Hence, from (55), we have $\eta = \frac{1}{2}$.

B. Secure DoF With the ESA Scheme

We show that the ESA scheme achieves $\eta = \frac{1}{2}$ secure DoF in the two-user fading MAC-WT. Here, we also use a constant power allocation policy for the ESA scheme where we set $P_1 = P_2 = P$ for all channel states. Clearly, this constant policy satisfies the average power constraints (40)–(41). Denoting the expression inside the expectation in (39) by $\tilde{f}_P(\mathbf{h},\mathbf{g})$, the achievable secrecy sum rate, R_s is given by

$$R_s = \frac{1}{2}E_{\mathbf{h},\mathbf{g}}\left\{\tilde{f}_P(\mathbf{h},\mathbf{g})\right\}. \tag{59}$$

Hence, the total achievable secure DoF is given by

$$\eta = \frac{1}{2}\lim_{P\to\infty} E_{\mathbf{h},\mathbf{g}}\left[\frac{\tilde{f}_P(\mathbf{h},\mathbf{g})}{\log(P)}\right]. \tag{60}$$

We note that for large enough P, $\frac{\tilde{f}_P(\mathbf{h},\mathbf{g})}{\log(P)} \leq \tilde{\psi}(\mathbf{h},\mathbf{g})$ where

$$\begin{aligned}\tilde{\psi}(\mathbf{h},\mathbf{g}) = {} & 6 + \log\left(1+2|h_1|^2\right) + \log\left(1+2|h_2|^2\right) \\ & + \log\left(1+2\left(|g_1|^2+|g_2|^2\right)\right).\end{aligned} \tag{61}$$

Again, using the fact that all channel gains have finite variances together with Jensen's inequality, we have

$$E_{\mathbf{h},\mathbf{g}}\left[\tilde{\psi}(\mathbf{h},\mathbf{g})\right] < \infty. \tag{62}$$

Then, by the dominated convergence theorem, we have

$$\lim_{P\to\infty} E_{\mathbf{h},\mathbf{g}}\left[\frac{\tilde{f}_P(\mathbf{h},\mathbf{g})}{\log(P)}\right] = E_{\mathbf{h},\mathbf{g}}\left[\lim_{P\to\infty}\frac{\tilde{f}_P(\mathbf{h},\mathbf{g})}{\log(P)}\right] = 1. \tag{63}$$

Hence, from (60), we have $\eta = \frac{1}{2}$.

C. Secure DoF With i.i.d. Gaussian Signaling With CJ

We consider the secrecy sum rate achieved by Gaussian signaling with CJ [18] in the fading MAC-WT and show that this achievable rate does not scale with SNR. We start with the secrecy sum rate given by the right-hand side of (13). According to the optimal power allocation policy described in [18], for $k = 1, 2$, we cannot have $P_k > 0$ and $Q_k > 0$ simultaneously. Moreover, no transmission occurs when $|h_1| \leq |g_1|$ and $|h_2| \leq |g_2|$. Consequently, according to the relative values of the channel gains $(|h_1|, |h_2|, |g_1|, |g_2|)$, there are three different cases left for the instantaneous secrecy sum rate achieved using the optimum power allocation where we omitted the case where $|h_1| \leq |g_1|$ and $|h_2| \leq |g_2|$ since no transmission is allowed.

Case 1: $(\mathbf{h},\mathbf{g}) \in \mathcal{D}_1$ where $\mathcal{D}_1 = \left\{(\mathbf{h},\mathbf{g}) : |h_1| > |g_1|, |h_2| > |g_2|\right\}$. Consequently, $Q_1 = Q_2 = 0$. Thus, the instantaneous secrecy sum rate, $R_s(\mathbf{h},\mathbf{g})$, can be written as

$$R_s(\mathbf{h},\mathbf{g}) = \log\left(\frac{1+|h_1|^2P_1+|h_2|^2P_2}{1+|g_1|^2P_1+|g_2|^2P_2}\right). \tag{64}$$

We can upper bound $R_s(\mathbf{h},\mathbf{g})$ as

$$\begin{aligned}R_s(\mathbf{h},\mathbf{g}) &\leq \log\left(1+\frac{|h_1|^2}{|g_1|^2}+\frac{|h_2|^2}{|g_2|^2}\right) \\ &\leq \log\left(1+\frac{|h_1|^2}{|g_1|^2}\right)+\log\left(1+\frac{|h_2|^2}{|g_2|^2}\right).\end{aligned} \tag{65}$$

Case 2: $(\mathbf{h},\mathbf{g}) \in \mathcal{D}_2$ where $\mathcal{D}_2 = \left\{(\mathbf{h},\mathbf{g}) : |h_1| > |g_1|, |h_2| < |g_2|\right\}$. Consequently, $Q_1 = P_2 = 0$. Thus, the instantaneous secrecy sum rate, $R_s(\mathbf{h},\mathbf{g})$, can be written as

$$\begin{aligned}R_s(\mathbf{h},\mathbf{g}) = {} & \log\left(\frac{1+|h_1|^2P_1+|h_2|^2Q_2}{1+|g_1|^2P_1+|g_2|^2Q_2}\right) \\ & +\log\left(\frac{1+|g_2|^2Q_2}{1+|h_2|^2Q_2}\right).\end{aligned} \tag{66}$$

We can upper bound $R_s(\mathbf{h},\mathbf{g})$ as

$$R_s(\mathbf{h},\mathbf{g}) \leq 1+\log\left(1+\frac{|h_1|^2}{|g_1|^2}\right)+\log\left(1+\frac{|g_2|^2}{|h_2|^2}\right). \tag{67}$$

Case 3: $(\mathbf{h},\mathbf{g}) \in \mathcal{D}_3$ where $\mathcal{D}_3 = \left\{(\mathbf{h},\mathbf{g}) : |h_1| < |g_1|, |h_2| > |g_2|\right\}$. Consequently, $P_1 = Q_2 = 0$. Thus, the instantaneous secrecy sum rate, $R_s(\mathbf{h},\mathbf{g})$, can be written as

$$\begin{aligned}R_s(\mathbf{h},\mathbf{g}) = {} & \log\left(\frac{1+|h_1|^2Q_1+|h_2|^2P_2}{1+|g_1|^2Q_1+|g_2|^2P_2}\right) \\ & +\log\left(\frac{1+|g_1|^2Q_1}{1+|h_1|^2Q_1}\right).\end{aligned} \tag{68}$$

We can upper bound $R_s(\mathbf{h},\mathbf{g})$ as

$$R_s(\mathbf{h},\mathbf{g}) \leq 1+\log\left(1+\frac{|h_2|^2}{|g_2|^2}\right)+\log\left(1+\frac{|g_1|^2}{|h_1|^2}\right). \tag{69}$$

$$\begin{aligned}\psi(\mathbf{h},\mathbf{g}) = {} & 4+2\left(\log\left(1+\frac{1}{\sigma_{g_1}^2}\right)+\log\left(1+\frac{1}{\sigma_{g_2}^2}\right)\right)+\log\left(1+\frac{\sigma_{g_1}^2+\sigma_{g_2}^2}{\sigma_{g_1}^2\sigma_{g_2}^2}\right)+3\left(\sum_{k=1}^{2}\log(1+|h_{ko}|^2)+\sum_{k=1}^{2}\log(1+|h_{ke}|^2)\right) \\ & +4\left(\sum_{k=1}^{2}\log(1+|g_{ko}|^2)+\sum_{k=1}^{2}\log(1+|g_{ke}|^2)\right)\end{aligned} \tag{56}$$

Now, since the instantaneous sum rate is zero outside $\mathcal{D}_1 \cup \mathcal{D}_2 \cup \mathcal{D}_3$, then from (65), (67), and (69), the ergodic secrecy sum rate, R_s, can be upper bounded as follows:

$$\begin{aligned} R_s \le & \int_{\mathcal{D}_1} \left(\log\left(1+\frac{|h_1|^2}{|g_1|^2}\right) + \log\left(1+\frac{|h_2|^2}{|g_2|^2}\right)\right) d\mathbf{F} \\ & + \int_{\mathcal{D}_2} \left(1+\log\left(1+\frac{|h_1|^2}{|g_1|^2}\right) + \log\left(1+\frac{|g_2|^2}{|h_2|^2}\right)\right) d\mathbf{F} \\ & + \int_{\mathcal{D}_3} \left(1+\log\left(1+\frac{|h_2|^2}{|g_2|^2}\right) + \log\left(1+\frac{|g_1|^2}{|h_1|^2}\right)\right) d\mathbf{F} \end{aligned} \tag{70}$$

where

$$d\mathbf{F} = \prod_{k=1}^{2} f(|h_k|^2) f(|g_k|^2) d|h_k|^2 d|g_k|^2 \tag{71}$$

where for $k = 1, 2$, $f(|h_k|^2)$ and $f(|g_k|^2)$ are the density functions of $|h_k|^2$ and $|g_k|^2$, respectively. Now, since $E[|h_k|^2] < \infty$, $E[|g_k|^2] < \infty$ for $k = 1, 2$, $|\int_0^1 \log(x)dx| = \log(e) < \infty$, $|\int_0^1 \log(1+x)dx| = 2 - \log(e) < \infty$, and $f(|h_k|^2)$, $f(|g_k|^2)$ are continuous and bounded for $k = 1, 2$, it follows that each of the three integrals in the aforementioned expression is finite. Hence, we have $R_s < \infty$, and that R_s is bounded from above by a constant. Thus, from definition (53) of the achievable secure DoF, η, we have

$$\eta = \lim_{P\to\infty} \frac{R_s}{\log(P)} = 0. \tag{72}$$

VII. ESA Scheme With CJ

The result given in Theorem 2 can be strengthened by adding the technique of CJ to the ESA scheme of Section V. We refer to the resulting scheme as ESA/CJ. This is done through Gaussian channel prefixing as discussed in Section III. In particular, we choose the channel inputs in (33)–(36) to be $X_1 = V_1 + T_1$ and $X_2 = V_2 + T_2$, and then choose V_1, V_2, T_1, T_2 to be independent Gaussian random variables. Namely, for $k = 1, 2$, V_k and T_k are Gaussian random variables with zero mean and variances P_k and Q_k, respectively. Here, V_1 and V_2 carry messages, while T_1 and T_2 are jamming signals. The powers of (V_1, T_1) and (V_2, T_2) should be chosen to satisfy the average power constraints of users 1 and 2, respectively. After these selections are made, the transmitters repeat their channel inputs X_1 and X_2 over two time instants in the same way described in the ESA scheme of Section V. In particular, when transmitters 1 and 2 repeat X_1 and X_2, they repeat their selections of (V_1, T_1) and (V_2, T_2), respectively. Accordingly, the ESA scheme yield the achievable rate region given by (73)–(75), shown at the bottom of the page, where, for $k = 1, 2$, P_k and Q_k are the transmission and jamming power allocation policies, respectively, of user k, and are both functions of $\mathbf{h}$ and $\mathbf{g}$ in general. In addition, they satisfy the average power constraints

$$E[P_k + Q_k] \le \bar{P}_k,\ k = 1, 2. \tag{76}$$

This achievable rate region, through an appropriate power control strategy (see Section IX), can be made strictly larger than the region given in Theorem 2.

VIII. Maximizing Secrecy Sum Rate of the ESA Scheme

In this section, we consider the problem of maximizing the secrecy sum rate achieved by the ESA scheme as a function of the power allocations P_1 and P_2 of users 1 and 2, respectively. We define $\alpha_k \triangleq 2|h_k|^2$ and $\beta_k \triangleq 2|g_k|^2$. Then, we define $\alpha \triangleq [\alpha_1 \quad \alpha_2]^T$ and $\beta \triangleq [\beta_1 \quad \beta_2]^T$. The achievable secrecy sum rate is given by

$$\begin{aligned} R_s = \frac{1}{2} E_{\alpha,\beta} \Big\{ & \log(1+\alpha_1 P_1) + \log(1+\alpha_2 P_2) \\ & - \log(1+\beta_1 P_1 + \beta_2 P_2) \Big\}. \end{aligned} \tag{77}$$

We can write the optimization problem as

$$\begin{aligned} \max\ & \frac{1}{2} E_{\alpha,\beta} \Big\{ \log(1+\alpha_1 P_1) + \log(1+\alpha_2 P_2) \\ & - \log(1+\beta_1 P_1 + \beta_2 P_2) \Big\} && (78) \\ \text{s.t.}\quad & E_{\alpha,\beta}[P_k(\alpha,\beta)] \le \bar{P}_k, \quad k = 1, 2 && (79) \\ & P_k(\alpha,\beta) \ge 0, \quad k = 1, 2, \quad \forall \alpha, \beta. && (80) \end{aligned}$$

The necessary KKT optimality conditions are

$$\frac{\alpha_1}{1+\alpha_1 P_1} - \frac{\beta_1}{1+\beta_1 P_1 + \beta_2 P_2} - (\lambda_1 - \mu_1) = 0 \tag{81}$$

$$\frac{\alpha_2}{1+\alpha_2 P_2} - \frac{\beta_2}{1+\beta_1 P_1 + \beta_2 P_2} - (\lambda_2 - \mu_2) = 0 \tag{82}$$

for some $\lambda_k, \mu_k \ge 0$, $k = 1, 2$. It should be noted here that (81) and (82) are only necessary conditions for the optimal power allocations P_1 and P_2 since the objective function, i.e., the achievable secrecy sum rate, is not concave in (P_1, P_2) in general.

$$R_1 \le \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \left\{ \log\left(1+\frac{2|h_1|^2 P_1}{1+2|h_1|^2 Q_1}\right) - \log\left(1+\frac{2|g_1|^2 P_1}{1+2|g_1|^2 Q_1 + 2|g_2|^2 (P_2+Q_2)}\right) \right\} \tag{73}$$

$$R_2 \le \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \left\{ \log\left(1+\frac{2|h_2|^2 P_2}{1+2|h_2|^2 Q_2}\right) - \log\left(1+\frac{2|g_2|^2 P_2}{1+2|g_1|^2 (P_1+Q_1) + 2|g_2|^2 Q_2}\right) \right\} \tag{74}$$

$$R_1 + R_2 \le \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \left\{ \log\left(1+\frac{2|h_1|^2 P_1}{1+2|h_1|^2 Q_1}\right) + \log\left(1+\frac{2|h_2|^2 P_2}{1+2|h_2|^2 Q_2}\right) - \log\left(1+\frac{2(|g_1|^2 P_1 + |g_2|^2 P_2)}{1+2(|g_1|^2 Q_1 + |g_2|^2 Q_2)}\right) \right\} \tag{75}$$

For each channel state, we distinguish between three nonzero forms that the solution (P_1, P_2) of (81) and (82) may take. First, if $P_1 > 0$ and $P_2 > 0$, then $\mu_1 = \mu_2 = 0$. Hence, (P_1, P_2) is the positive common root of the following two quadratic equations:

$$\alpha_1 (1 + \beta_2 P_2) - \beta_1 = \lambda_1 (1 + \alpha_1 P_1)(1 + \beta_1 P_1 + \beta_2 P_2) \tag{83}$$

$$\alpha_2 (1 + \beta_1 P_1) - \beta_2 = \lambda_2 (1 + \alpha_2 P_2)(1 + \beta_1 P_1 + \beta_2 P_2). \tag{84}$$

Since it is hard to find a simple closed-form solution for the above system of equations, we solve this system numerically and obtain the positive common root (P_1, P_2). Secondly, if $P_1 > 0$ and $P_2 = 0$, then $\mu_1 = 0$. Hence, from (81), P_1 is given by

$$P_1 = \frac{1}{2}\left(\sqrt{\left(\frac{1}{\beta_1} - \frac{1}{\alpha_1}\right)^2 + \frac{4}{\lambda_1}\left(\frac{1}{\beta_1} - \frac{1}{\alpha_1}\right)} - \left(\frac{1}{\beta_1} + \frac{1}{\alpha_1}\right)\right). \tag{85}$$

Third, if $P_1 = 0$ and $P_2 > 0$, then $\mu_2 = 0$. Hence, from (82), P_2 is given by

$$P_2 = \frac{1}{2}\left(\sqrt{\left(\frac{1}{\beta_2} - \frac{1}{\alpha_2}\right)^2 + \frac{4}{\lambda_2}\left(\frac{1}{\beta_2} - \frac{1}{\alpha_2}\right)} - \left(\frac{1}{\beta_2} + \frac{1}{\alpha_2}\right)\right). \tag{86}$$

From conditions (81) and (82), we can derive the following necessary and sufficient conditions for the positivity of the optimal power allocation policies:

$$P_1 > 0, \quad \text{if and only if} \quad \alpha_1 - \frac{\beta_1}{(1 + \beta_2 P_2)} > \lambda_1 \tag{87}$$

$$P_2 > 0, \quad \text{if and only if} \quad \alpha_2 - \frac{\beta_2}{(1 + \beta_1 P_1)} > \lambda_2. \tag{88}$$

Consequently, according to conditions (87) and (88), we can divide the set of all possible channel states into 7 partitions such that in each partition the solution (P_1, P_2) will either have one of the three forms stated above or will be zero. Hence, the power allocation policy (P_1, P_2) that satisfies (81), (82) and (79), (80) can be fully described in 7 different cases of the channel gains. The details of such cases are given in Appendix A.

IX. Maximizing Secrecy Sum Rate of the ESA/CJ Scheme

In this section, we consider the problem of maximizing the achievable secrecy sum rate as a function in the power allocation policies P_1 and P_2 when CJ technique is used on top of the ESA scheme. Again, we define $\alpha_k \triangleq 2|h_k|^2$ and $\beta_k \triangleq 2|g_k|^2$. Then, we define $\alpha \triangleq [\alpha_1 \quad \alpha_2]^T$ and $\beta \triangleq [\beta_1 \quad \beta_2]^T$. In this case, the optimization problem is described by (89)–(91), shown at the bottom of the page.

We first show that, at any fading state, splitting a user's power into transmission and jamming is suboptimal, i.e., an optimum power allocation policy must not have $P_k > 0$ and $Q_k > 0$ simultaneously. We note that whether we split powers or not does not affect the first three terms of the objective function since we can always convert jamming power of user k into transmission power of the same user and vice versa while keeping the sum $P_k + Q_k$ fixed. Hence, we consider the last three terms of the sum rate. For convenience, we define

$$S = \log(1 + \beta_1 Q_1 + \beta_2 Q_2) - \log(1 + \alpha_1 Q_1) - \log(1 + \alpha_2 Q_2). \tag{92}$$

Consider, without loss of generality, the power allocation for user 1. We assume that P_1^*, Q_1^* is the optimum power allocation for user 1. We observe that the sign of

$$\frac{\partial S}{\partial Q_1} = \frac{\beta_1}{1 + \beta_1 Q_1 + \beta_2 Q_2} - \frac{\alpha_1}{1 + \alpha_1 Q_1} \tag{93}$$

does not depend on Q_1. Consider a power allocation $P_1 = P_1^* - \varepsilon$, $Q_1 = Q_1^* + \varepsilon$. Hence, we have $P_1 + Q_1 = P_1^* + Q_1^*$ and the first three terms in the expression of the achievable sum rate do not change. On the other hand, if (93) is positive, any positive ε results in an increase in the achievable sum rate and jamming with the same sum power is better. While, if (93) is negative, then any negative ε results in an increase in the achievable sum rate and transmitting with the same sum power is better. If (93) is zero, then the sum rate does not depend on Q_1 and we can set it to zero, i.e., use the sum power in transmitting. Therefore, the optimum power allocation will have either $P_k > 0$ or $Q_k > 0$, but not both.

Suppose that P_1, P_2, Q_1, and Q_2 are the optimal power allocations. Then, the necessary KKT conditions satisfy (94)–(97), shown at the bottom of the next page, for some $\lambda_k, \mu_k, \nu_k \geq 0$, $k = 1, 2$. As in Section VIII, we note that (94)–(97) are only necessary conditions for the optimal power allocations P_1, P_2, Q_1, and Q_2 since the objective function, i.e., the achievable secrecy sum rate, is not concave in (P_1, P_2, Q_1, Q_2) in general. Therefore, we give power control policies P_1, P_2, Q_1, and Q_2 that satisfy these necessary conditions. That is, we obtain one fixed point (P_1, P_2, Q_1, Q_2) of the Lagrangian such that (P_1, P_2, Q_1, Q_2) satisfies the constraints (90)–(91). The power

$$\max \quad \frac{1}{2} E_{\alpha,\beta}\Big\{ \log(1 + \alpha_1(P_1 + Q_1)) + \log(1 + \alpha_2(P_2 + Q_2)) - \log(1 + \beta_1(P_1 + Q_1) + \beta_2(P_2 + Q_2)) + \log(1 + \beta_1 Q_1 + \beta_2 Q_2) - \log(1 + \alpha_1 Q_1) - \log(1 + \alpha_2 Q_2) \Big\} \tag{89}$$

$$\text{s.t.} \quad E_{\alpha,\beta}[P_k(\alpha,\beta) + Q_k(\alpha,\beta)] \leq \bar{P}_k, \quad k = 1, 2 \tag{90}$$

$$P_k(\alpha,\beta), Q_k(\alpha,\beta) \geq 0, \quad k = 1, 2, \ \forall \alpha, \beta \tag{91}$$

allocation policy (P_1, P_2, Q_1, Q_2) that satisfies (94)–(97) and (90)–(91) is described in detail in Appendix B.

X. Numerical Results

In this section, we present some simple simulation results. We also plot the sum secrecy rate achieved using our SBA and ESA schemes, as well as the i.i.d. Gaussian signaling with cooperative jamming (GS/CJ) scheme in [18]. First, the secrecy sum rates achieved by the SBA and the ESA schemes scale with SNR. Hence, these rates exceed the one achieved by the GS/CJ scheme for high SNR. Second, the secrecy sum rate achieved by the ESA scheme is larger than the one achieved by the SBA scheme for all SNR.

In our first set of simulations, we use a rudimentary power allocation policy for our SBA and ESA schemes. For the SBA scheme, we first note, from (30), that the secrecy sum rate achieved can be expressed as a nested expectation as in (98), shown at the bottom of the page, where $\mathbf{h}_o = [h_{1o}\ h_{2o}]^T$, $\mathbf{h}_e = [h_{1e}\ h_{2e}]^T$, $\mathbf{g}_o = [g_{1o}\ g_{2o}]^T$, and $\mathbf{g}_e = [g_{1e}\ g_{2e}]^T$. For those channel gains $\mathbf{h}_o, \mathbf{g}_o$ for which the inner expectation with respect to $\mathbf{h}_e, \mathbf{g}_e$ is negative, we set $P_1 = P_2 = 0$. Otherwise, we set $P_1 = \frac{1}{2\sigma_g^2}\bar{P}_1$ and $P_2 = \frac{1}{2\sigma_g^2}\bar{P}_2$. Note that turning off the powers for some values of the channel gains $\mathbf{h}_o, \mathbf{g}_o$ is possible since P_1 and P_2 are functions of $\mathbf{h}_o$ and $\mathbf{g}_o$. Second, note that, if a power allocation satisfies the average power constraints, then the modified power allocation where the powers are turned off at some channel states, also satisfies the power constraints. For the ESA scheme, we first note, from (39), that the achievable secrecy sum rate is

$$R_s = \frac{1}{2}E_{\mathbf{h},\mathbf{g}}\Big\{\log\left(1+2|h_1|^2P_1\right)+\log\left(1+2|h_2|^2P_2\right) - \log\left(1+2(|g_1|^2P_1+|g_2|^2P_2)\right)\Big\}. \quad (99)$$

In this case, we set $P_1 = P_2 = 0$ for those values of channel gains for which the difference inside the expectation is negative. Otherwise, we set $P_1 = \bar{P}_1$ and $P_2 = \bar{P}_2$. Again, turning the powers off does not violate power constraints for a power allocation scheme which already satisfies the power constraints. For the GS/CJ scheme, we use the power allocation scheme described in [18].

In Fig. 1, the secrecy sum rate achieved by each of the three schemes is plotted versus the average SNR that we define as $\frac{1}{2}(\bar{P}_1+\bar{P}_2)$. In all simulations, we set $\sigma_{h_1}^2 = \sigma_{h_2}^2 = 1.0$, we also take $\sigma_{g_1}^2 = \sigma_{g_2}^2 = 0.75$. Clearly, the secrecy sum rate achieved by the GS/CJ scheme saturates as we increase the SNR while the secrecy sum rate achieved by the SBA and the ESA schemes grows unboundedly with the SNR. One can also notice, as discussed earlier, that the secrecy sum rate achieved by the ESA scheme is larger than the one achieved by the SBA scheme which is due to the fact that the ESA scheme creates two totally uncorrelated parallel MAC channels (i.e., orthogonal MAC) between the transmitters and the main receiver.

Next, in Fig. 2, we plot secrecy sum rates achievable with constant power allocation together with secrecy sum rates achievable with power control for the ESA scheme with and without CJ. It is clear here that the secrecy sum rate achieved by the ESA/CJ scheme (with power control) is larger than the rate achieved when the ESA scheme is used solely without CJ (with or without power control). One may also note that, for low SNR, the GS/CJ scheme still gives better rates than those achieved by all the proposed schemes which is due to the factor of $\frac{1}{2}$ in the rates achieved by the proposed schemes due to code repetition.

XI. SBA and ESA Schemes for the K-user Fading MAC-WT Channel

Let $\mathcal{K} \triangleq \{1,\ldots,K\}$. We consider the K-user MAC-WT for which the channel outputs at the intended receiver and the eavesdropper are given by

$$Y = \sum_{k\in\mathcal{K}} h_k X_k + N \quad (100)$$

$$\frac{\alpha_1}{1+\alpha_1(P_1+Q_1)} - \frac{\beta_1}{1+\beta_1(P_1+Q_1)+\beta_2(P_2+Q_2)} - (\lambda_1-\mu_1) = 0 \quad (94)$$

$$\frac{\alpha_2}{1+\alpha_2(P_2+Q_2)} - \frac{\beta_2}{1+\beta_1(P_1+Q_1)+\beta_2(P_2+Q_2)} - (\lambda_2-\mu_2) = 0 \quad (95)$$

$$\frac{\alpha_1}{1+\alpha_1(P_1+Q_1)} - \frac{\beta_1}{1+\beta_1(P_1+Q_1)+\beta_2(P_2+Q_2)} + \frac{\beta_1}{1+\beta_1Q_1+\beta_2Q_2} - \frac{\alpha_1}{1+\alpha_1Q_1} - (\lambda_1-\nu_1) = 0 \quad (96)$$

$$\frac{\alpha_2}{1+\alpha_2(P_2+Q_2)} - \frac{\beta_2}{1+\beta_1(P_1+Q_1)+\beta_2(P_2+Q_2)} + \frac{\beta_2}{1+\beta_1Q_1+\beta_2Q_2} - \frac{\alpha_2}{1+\alpha_2Q_2} - (\lambda_2-\nu_2) = 0 \quad (97)$$

$$R_s = \frac{1}{2}E_{\mathbf{h}_o,\mathbf{g}_o}\Bigg\{E_{\mathbf{h}_e,\mathbf{g}_e}\Big[\log\left(1+\left(|h_{1o}g_{2o}|^2+|h_{1e}g_{2e}|^2\right)P_1+\left(|h_{2o}g_{1o}|^2+|h_{2e}g_{1e}|^2\right)P_2+|h_{1e}h_{2o}g_{1o}g_{2e}-h_{1o}h_{2e}g_{1e}g_{2o}|^2P_1P_2\right) - \log\left(1+\left(|g_{1o}g_{2o}|^2+|g_{1e}g_{2e}|^2\right)(P_1+P_2)\right)\Big]\Bigg\} \quad (98)$$

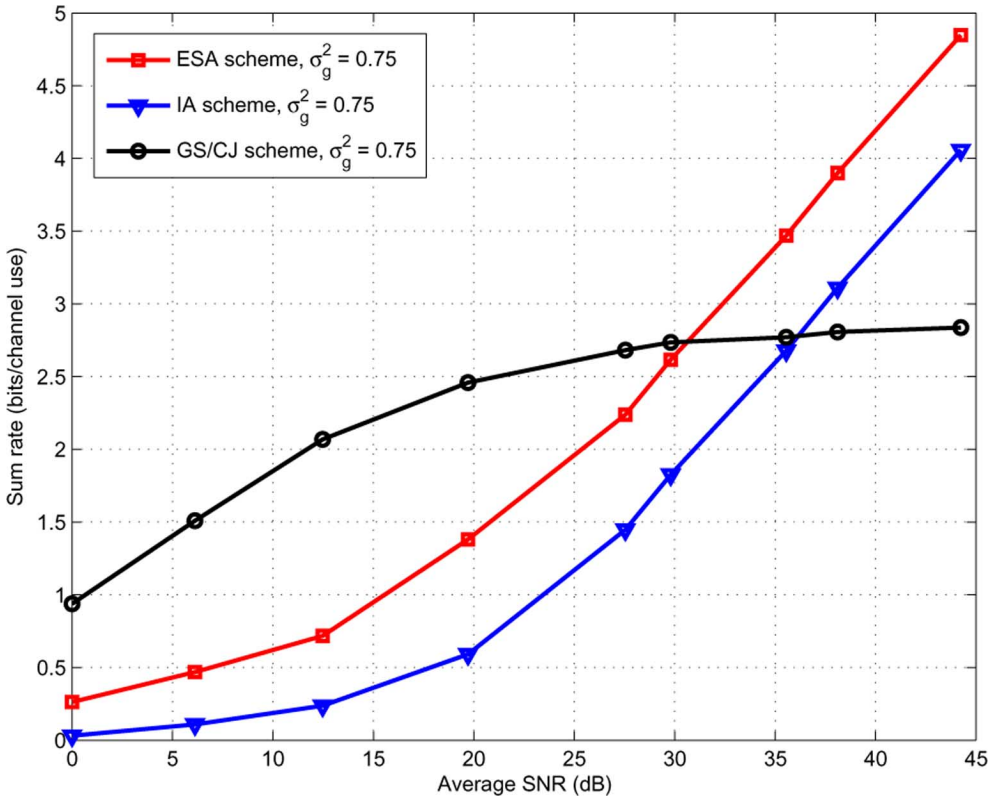

Fig. 1. Achievable secrecy sum rates of the SBA scheme of this paper, the ESA scheme of this paper, and the i.i.d. GS/CJ scheme of [18], as function of the SNR for two different values of mean eavesdropper channel gain, σ_g^2.

$$Z = \sum_{k\in\mathcal{K}} g_k X_k + N' \tag{101}$$

where, for $k \in \mathcal{K}$, h_k, g_k, X_k, N, N' are as defined in Section II. The average power constraints are given by

$$E[|X_k|^2] \le \bar{P}_k, \quad k \in \mathcal{K}. \tag{102}$$

A. SBA Scheme

Here, we use a repetition code in which each transmitter repeats its channel input symbol over K consecutive time instants. Moreover, in every time instant, $\forall k \in \mathcal{K}$, transmitter k multiplies its channel input by $\prod_{i\in\mathcal{K}\setminus\{k\}} g_i$. Thus, over K consecutive time instants, the channel outputs at the main receiver and the eavesdropper are given by

$$Y_j = \sum_{k\in\mathcal{K}} h_{kj} \prod_{i\in\mathcal{K}\setminus\{k\}} g_{ij} X_k + N_j, \quad 1 \le j \le K \tag{103}$$

$$Z_j = \prod_{i\in\mathcal{K}} g_{ij} \sum_{k\in\mathcal{K}} X_k + N'_j, \quad 1 \le j \le K \tag{104}$$

where Y_j and Z_j denote the observations at the jth time instant at each of the main receiver and the eavesdropper, respectively, h_{ij} and g_{ij} denote the channel coefficients at the jth time instant from the ith transmitter to the main receiver and the eavesdropper, respectively. Note that due to such scaling at the transmitters, the average power constraints become

$$E\left[\sum_{j=1}^{K} \prod_{i\in\mathcal{K}\setminus\{k\}} |g_{ij}|^2 P_k\right] \le \bar{P}_k, \ k \in \mathcal{K}. \tag{105}$$

It is clear from (103) and (104) that the observed signal space (without noise, i.e., at high SNR) of the main receiver over the K consecutive time instants is K-dimensional almost surely whereas that of the eavesdropper is 1-D. Indeed, one can express (103) and (104) as

$$\mathbf{Y} = \mathbf{H}\mathbf{X} + \mathbf{N} \tag{106}$$

$$\mathbf{Z} = \mathbf{G}\mathbf{X} + \mathbf{N}' \tag{107}$$

where $\mathbf{X} = [X_1, \ldots, X_K]^T$, $\mathbf{Y} = [Y_1, \ldots, Y_K]^T$, $\mathbf{Z} = [Z_1, \ldots, Z_K]^T$, $\mathbf{H}$ is $K \times K$ full-rank matrix of effective channel gains from the transmitters to the main receiver, and $\mathbf{G}$ is $K \times K$ unit-rank matrix of effective channel gains from the transmitters to the eavesdropper, where the elements at the jth row and the kth column of $\mathbf{H}$ and $\mathbf{G}$ are given, respectively, by

$$H_{jk} = h_{kj} \prod_{i\in\mathcal{K}\setminus\{k\}} g_{ij} \tag{108}$$

$$G_{jk} = \prod_{i\in\mathcal{K}} g_{ij}. \tag{109}$$

Hence, the achievable secrecy sum rate is given by

$$R_s = \frac{1}{K} E_{\mathbf{H},\mathbf{G}}\Big\{ \log\left(\det\left(\mathbf{I} + \mathbf{H}\mathbf{S}\mathbf{H}^*\right)\right) - \log\left(\det\left(\mathbf{I} + \mathbf{G}\mathbf{S}\mathbf{G}^*\right)\right) \Big\} \tag{110}$$

where $\mathbf{S} \triangleq \mathrm{Cov}(\mathbf{X}) = \mathrm{diag}\,(P_1, \ldots, P_K)$ and $\mathbf{A}^*$ denotes the conjugate transpose of the matrix $\mathbf{A}$.

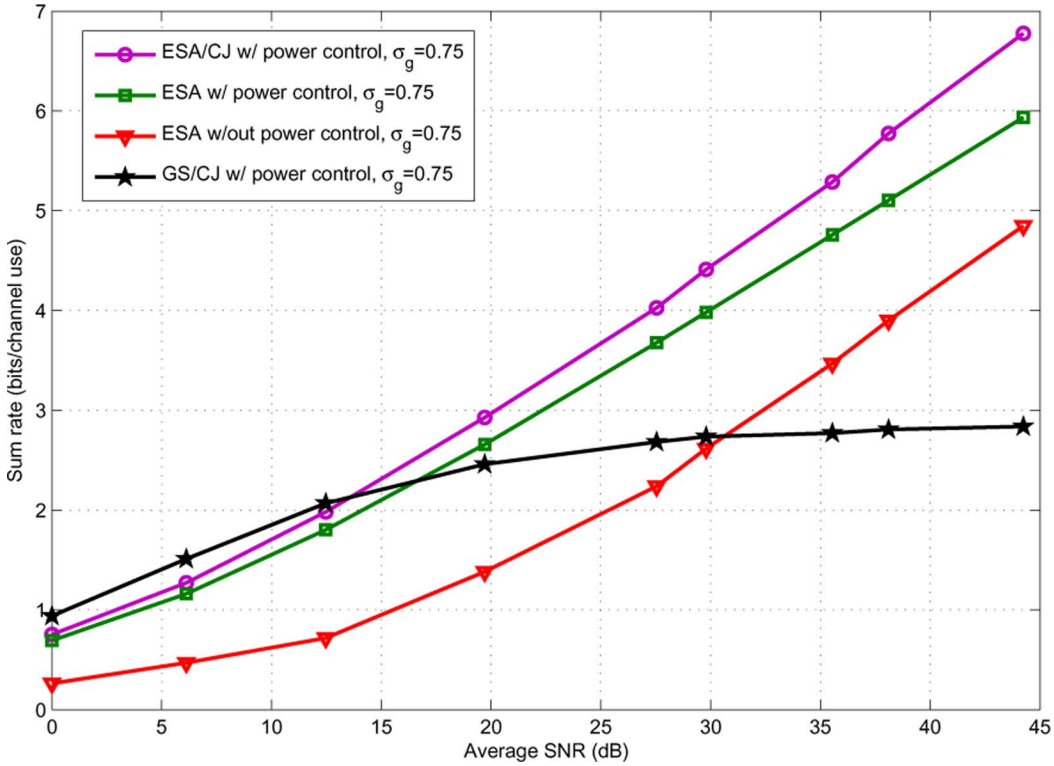

Fig. 2. Achievable secrecy sum rates for the ESA scheme of this paper, with and without power control, the ESA with cooperative jamming scheme (ESA/CJ scheme) of this paper with power control, and the i.i.d. GS/CJ scheme of [18], as function of the SNR for two different values of mean eavesdropper channel gain, σ_g^2.

In fact, the system given in (106) is equivalent to $K \times K$ MIMO channel with independent signaling across the antennas. Since $\mathbf{H}$ is full-rank, such MIMO channel possesses exactly K DoF. On the other hand, the system given in (107) is equivalent to $K \times K$ MIMO channel with independent signaling across the antennas and since $\mathbf{G}$ is unit-rank, such MIMO channel possesses exactly 1 DoF. Therefore, while deriving the total secure DoF achieved by the SBA scheme, conditioned on $\mathbf{H}$ and $\mathbf{G}$, the first term inside the expectation above yields K DoF whereas the second term inside the expectation yields 1 DoF. Thus, the total achievable secure DoF is $\eta = \frac{K-1}{K}$.

B. ESA Scheme

In order to extend the ESA scheme to the case of more than two users, i.e., K-user fading MAC-WT channel with $K \geq 2$, we use a repetition code, where each code symbol is repeated K times over K channel uses. However, unlike the SBA scheme, repetition is done over channel uses that hold certain conditions relative to those conditions in the channel use where this code symbol is first transmitted. For $1 \leq \ell \leq K$, let

$$\mathbf{h}_\ell \stackrel{\triangle}{=} [h_{1\ell}, \ldots, h_{K\ell}]^T \tag{111}$$

$$\mathbf{g}_\ell \stackrel{\triangle}{=} [g_{1\ell}, \ldots, g_{K\ell}]^T \tag{112}$$

where $h_{k\ell}$ and $g_{k\ell}$ denote the channel coefficients at the ℓth channel use from the kth transmitter to the main receiver and the eavesdropper, respectively. Following the same steps given in Section V, one can easily verify that the optimal repetition channel use $\ell, 2 \leq \ell \leq K$ (relative to the channel use where the first copy of the symbol is transmitted) must be chosen such that

$$\mathbf{h}_\ell = \mathbf{U}_\ell \mathbf{h}_1 \tag{113}$$

$$\mathbf{g}_\ell = \mathbf{g}_1 \tag{114}$$

where

$$\mathbf{U}_\ell \stackrel{\triangle}{=} \text{diag}\left(1, e^{j\frac{2\pi}{K}(\ell-1)}, \ldots, e^{j\frac{2\pi}{K}(\ell-1)(K-1)}\right) \tag{115}$$

where $j = \sqrt{-1}$. Note that, as explained in Section V, the above argument is based on the proof of the ergodic interference alignment technique given in [19]. The main idea is to quantize the channel coefficients and then group the sets of coefficients of symmetric types together. That is indeed tantamount to grouping $\{\mathbf{h}_\ell,\ \mathbf{g}_\ell : 1 \leq \ell \leq K\}$ together. Note that indeed this is possible due to the circular symmetry of the distribution of the channel coefficients. Then, using the continuity of the achievable rate as a function in channel coefficients, by decreasing the quantization bin size, one can approach the desired rate in the limit.

According to the selection given by (113) and (114), one can describe the main receiver and the eavesdropper MAC channels over such K channel uses by

$$Y_\ell = \mathbf{h}_1^T \mathbf{U}_\ell \mathbf{X} + N_\ell \tag{116}$$

$$Z_\ell = \mathbf{g}_1^T \mathbf{X} + N'_\ell \tag{117}$$

for $\ell = 1, \ldots, K$, where Y_ℓ and Z_ℓ are the observations at channel use ℓ at the main receiver and the eavesdropper, re-

spectively, N_ℓ and N'_ℓ are the noise values at channel use ℓ at the main receiver and the eavesdropper, respectively, and $\mathbf{X} = [X_1, \ldots, X_K]$ where X_k, $k \in \mathcal{K}$ is the channel input of transmitter k.

Using similar argument to the one in Section V, it is easy to see that the system in (116) is equivalent to an orthogonal K-user MAC channel where each component of such orthogonal MAC channel has unit-variance noise and channel gain $\sqrt{K}h_{k1}$, $k \in \mathcal{K}$, whereas the system in (117) is equivalent to 1-D MAC channel with unit-variance noise and channel gains $\sqrt{K}g_{k1}$, $k \in \mathcal{K}$. Hence, the achievable secrecy sum rate is given by

$$R_s = \frac{1}{K} E_{\mathbf{h}_1, \mathbf{g}_1} \left\{ \sum_{k \in \mathcal{K}} \log\left(1 + K|h_{k1}|^2 P_k\right) - \log\left(1 + K \sum_{k \in \mathcal{K}} |g_{k1}|^2 P_k\right) \right\}. \quad (118)$$

Therefore, by using the same approach of Section VI-B, one can easily verify that the total secure DoF achievable by the ESA scheme in the K-user fading MAC-WT channel is indeed $\eta = \frac{K-1}{K}$.

XII. Conclusion

In this paper, we proposed two new achievable schemes for the fading MAC-WT. Our first scheme, the SBA scheme, lets the interfering signals at the main receiver live in a 2-D space, while it aligns the interfering signals at the eavesdropper in a 1-D space. We obtained the secrecy rate region achieved by this scheme. We showed that the secrecy rates achieved by this scheme scale with SNR as $\frac{1}{2}\log(\mathrm{SNR})$, i.e., a total of $\frac{1}{2}$ secure DoF is achievable in the two-user fading MAC-WT. We also showed that the secrecy sum rate achieved by the i.i.d. Gaussian signaling with CJ scheme does not scale with SNR, i.e., the achievable secure DoF is zero. As a direct consequence, we showed the suboptimality of the i.i.d. Gaussian signaling based schemes with or without CJ in the fading MAC-WT.

Our second scheme, the ESA scheme, is inspired by the ergodic interference alignment technique. In this scheme, each transmitter repeats its symbols over carefully chosen time instants such that the interfering signals from the transmitters are aligned favorably at the main receiver while they are aligned unfavorably at the eavesdropper. We obtained the secrecy rate region achieved by this scheme and showed that, as in the SBA scheme, the secrecy sum rate achieved by the ESA scheme scales with SNR as $\frac{1}{2}\log(\mathrm{SNR})$. In addition, we introduced an improved version of our ESA scheme where CJ is used as an additional ingredient to achieve higher secrecy rates. Moreover, since the rate expressions achieved with the SBA scheme seem complicated, while the rate expressions achieved with the two versions of the ESA scheme (with and without CJ) are more amenable for optimization of power allocations, we derived the necessary conditions for the optimal power allocation that maximizes the secrecy sum rate achieved by the ESA scheme when used solely and when used with cooperative jamming. Finally, we discussed the extension of our schemes to the case of more than two users and showed that, for the K-user fading MAC-WT, our schemes achieve secrecy rates that scale with SNR as $\frac{K-1}{K}\log(\mathrm{SNR})$.

Appendix A
Power Control for the ESA Scheme

Here, we discuss the cases of the power allocation policy of Section VIII.

1) $\alpha_1 \le \lambda_1, \alpha_2 - \beta_2 \le \lambda_2$ or $\alpha_1 - \beta_1 \le \lambda_1, \alpha_2 \le \lambda_2$. In this case, $P_1 = P_2 = 0$. To prove this, suppose without loss of generality that $\alpha_1 \le \lambda_1$, $\alpha_2 - \beta_2 \le \lambda_2$. We note that $\alpha_1 \le \lambda_1$ implies that $\alpha_1 - \frac{\beta_1}{(1+\beta_2 P_2)} \le \lambda_1$ which, using (87), implies that $P_1 = 0$. Hence, from (88), we must also have $P_2 = 0$. In the same way, we can show that when $\alpha_1 - \beta_1 \le \lambda_1$, $\alpha_2 \le \lambda_2$, we also must have $P_1 = P_2 = 0$.
2) $\alpha_1 \le \lambda_1$, $\alpha_2 - \beta_2 > \lambda_2$. In this case, $P_1 = 0$ and $P_2 > 0$ where P_2 is given by (86). As in the previous case, $\alpha_1 \le \lambda_1$, using (87), implies that $P_1 = 0$. Hence, from (88), we must have $P_2 > 0$.
3) $\alpha_1 - \beta_1 > \lambda_1$, $\alpha_2 \le \lambda_2$. In this case, $P_1 > 0$ and $P_2 = 0$ where P_1 is given by (85). This case is the same as the previous one with roles of users 1 and 2 interchanged.
4) $\lambda_1 < \alpha_1 \le \lambda_1 + \beta_1$, $\lambda_2 < \alpha_2 \le \lambda_2 + \beta_2$. In this case, the solution (P_1, P_2) may not be unique. Namely, we either have $P_1 > 0$ and $P_2 > 0$, or we have $P_1 = P_2 = 0$. This is due to the following facts. It is easy to see that $P_1 = P_2 = 0$ satisfies $\alpha_1 - \frac{\beta_1}{(1+\beta_2 P_2)} \le \lambda_1$ and $\alpha_2 - \frac{\beta_2}{(1+\beta_1 P_1)} \le \lambda_2$, i.e., satisfies conditions (87) and (88). It is also easy to see that we can find positive P_1 and P_2 such that $\alpha_1 - \frac{\beta_1}{(1+\beta_2 P_2)} > \lambda_1$ and $\alpha_2 - \frac{\beta_2}{(1+\beta_1 P_1)} > \lambda_2$, i.e., there exist positive P_1 and P_2 that satisfy (87) and (88). Hence, the solution (P_1, P_2) may not be unique. It remains to show that we cannot have $P_1 > 0$, $P_2 = 0$ or $P_1 = 0$, $P_2 > 0$. Suppose without loss of generality that $P_1 > 0$, $P_2 = 0$. Hence, we have $\alpha_1 - \frac{\beta_1}{(1+\beta_2 P_2)} = \alpha_1 - \beta_1 \le \lambda_1$ which implies that $P_1 = 0$ which is a contradiction. Thus, we cannot have $P_1 > 0$, $P_2 = 0$. In the same way, it can be shown that we cannot have $P_1 = 0$, $P_2 > 0$. Hence, we obtain our power allocation policy for this case as follows. We examine the solution of (83) and (84), if it yields a real and nonnegative solution (P_1, P_2)[1], then we take it as our solution (P_1, P_2) for this case. Otherwise, we set $P_1 = P_2 = 0$.
5) $\lambda_1 < \alpha_1 \le \lambda_1 + \beta_1$, $\alpha_2 - \beta_2 > \lambda_2$. In this case, we must have $P_2 > 0$. However, we either have $P_1 > 0$ or $P_1 = 0$. This can be shown as follows. We note that $\alpha_2 - \beta_2 > \lambda_2$ implies that $\alpha_2 - \frac{\beta_2}{(1+\beta_1 P_1)} > \lambda_2$ for any $P_1 \ge 0$. Hence, by (88), we must have $P_2 > 0$. However, we either have $P_1 > 0$ or $P_1 = 0$ depending on whether the value of P_2 satisfies $\alpha_1 - \frac{\beta_1}{(1+\beta_2 P_2)} > \lambda_1$ or not. We obtain our power allocation policies as follows. We first solve (83) and (84), if this yields a real and nonnegative solution (P_1, P_2), then we take it to be the power allocation values for this case. Otherwise, we set $P_1 = 0$ and P_2 is obtained from (86).
6) $\alpha_1 - \beta_1 > \lambda_1$, $\lambda_2 < \alpha_2 \le \lambda_2 + \beta_2$. By the symmetry between this case and the previous case, we must have $P_1 > 0$ while we either have $P_2 > 0$ or $P_2 = 0$. We obtain our power allocation policies in a fashion similar to that of case 4 and case 5. In particular, we first solve (83) and (84), if this yields a real and nonnegative solution (P_1, P_2), then

[1]Note that there is at most one such common root for these two quadratic equations.

we take it to be the power allocation values for this case. Otherwise, we set $P_2 = 0$ and P_1 is obtained from (85).

7) $\alpha_1 - \beta_1 > \lambda_1, \alpha_2 - \beta_2 > \lambda_2$. Here, we must have $P_1 > 0$ and $P_2 > 0$. This is due to the fact that $\alpha_1 - \beta_1 > \lambda_1$ and $\alpha_2 - \beta_2 > \lambda_2$ imply that $\alpha_1 - \frac{\beta_1}{(1+\beta_2 P_2)} > \lambda_1$ and $\alpha_2 - \frac{\beta_2}{(1+\beta_1 P_1)} > \lambda_2$, respectively. Hence, from (87) and (88), we must have $P_1 > 0$ and $P_2 > 0$. The values of P_1 and P_2 are given by the positive common root (P_1, P_2) of (83) and (84) which, in this case, have only one positive common root.

Appendix B
Power Control for the ESA/CJ Scheme

Here, we discuss the power allocation policy of Section IX. For each channel state, since splitting power between transmission and jamming is suboptimal, we can distinguish between five nonzero forms that the solution (P_1, P_2, Q_1, Q_2) of (94)–(97) may take. First, if $P_1 > 0, P_2 > 0$ and $Q_1 = Q_2 = 0$, then $\mu_1 = \mu_2 = 0$. Hence, from (94) and (95), we conclude that (P_1, P_2) is the positive common root of (83) and (84) which are found in Section VIII and are rewritten here:

$$\alpha_1 (1 + \beta_2 P_2) - \beta_1 = \lambda_1 (1 + \alpha_1 P_1)(1 + \beta_1 P_1 + \beta_2 P_2) \tag{119}$$

$$\alpha_2 (1 + \beta_1 P_1) - \beta_2 = \lambda_2 (1 + \alpha_2 P_2)(1 + \beta_1 P_1 + \beta_2 P_2). \tag{120}$$

This root can be obtained through numerical solution. Second, if $P_1 > 0, Q_2 > 0$ and $P_2 = Q_1 = 0$, then $\mu_1 = \nu_2 = 0$. Hence, from (94) and (96), we conclude that (P_1, Q_2) is the positive common root of

$$\alpha_1 (1 + \beta_2 Q_2) - \beta_1 = \lambda_1 (1 + \alpha_1 P_1)(1 + \beta_1 P_1 + \beta_2 Q_2) \tag{121}$$

$$\beta_2 \beta_1 P_1 = \lambda_2 (1 + \beta_2 Q_2)(1 + \beta_1 P_1 + \beta_2 Q_2) \tag{122}$$

which can also be obtained through numerical solution. Third, if $P_2 > 0, Q_1 > 0$ and $P_1 = Q_2 = 0$, then $\mu_2 = \nu_1 = 0$. Hence, from (95) and (97), we conclude that (P_2, Q_1) is the positive common root of

$$\alpha_2 (1 + \beta_1 Q_1) - \beta_2 = \lambda_2 (1 + \alpha_2 P_2)(1 + \beta_1 Q_1 + \beta_2 P_2) \tag{123}$$

$$\beta_1 \beta_2 P_2 = \lambda_1 (1 + \beta_1 Q_1)(1 + \beta_1 Q_1 + \beta_2 P_2) \tag{124}$$

which again can be obtained through numerical solution. The fourth nonzero form of (P_1, P_2, Q_1, Q_2) is when $P_1 > 0$ and $P_2 = Q_1 = Q_2 = 0$, then $\mu_1 = 0$. Hence, from (94), P_1 is given by (85) which is found in Section VIII and will be repeated here for convenience:

$$P_1 = \frac{1}{2}\left(\sqrt{\left(\frac{1}{\beta_1} - \frac{1}{\alpha_1}\right)^2 + \frac{4}{\lambda_1}\left(\frac{1}{\beta_1} - \frac{1}{\alpha_1}\right)} - \left(\frac{1}{\beta_1} + \frac{1}{\alpha_1}\right)\right). \tag{125}$$

The last nonzero form of (P_1, P_2, Q_1, Q_2) is when $P_2 > 0$ and $P_1 = Q_1 = Q_2 = 0$, then $\mu_2 = 0$. Hence, from (95), P_2 is given by (86) in Section VIII and is given here again:

$$P_2 = \frac{1}{2}\left(\sqrt{\left(\frac{1}{\beta_2} - \frac{1}{\alpha_2}\right)^2 + \frac{4}{\lambda_2}\left(\frac{1}{\beta_2} - \frac{1}{\alpha_2}\right)} - \left(\frac{1}{\beta_2} + \frac{1}{\alpha_2}\right)\right). \tag{126}$$

We obtain the following sufficient conditions on zero jamming powers Q_1 and Q_2. By subtracting (96) from (94) and subtracting (97) from (95), we get

$$\frac{\alpha_1}{1 + \alpha_1 Q_1} - \frac{\beta_1}{1 + \beta_1 Q_1 + \beta_2 Q_2} + \mu_1 - \nu_1 = 0 \tag{127}$$

$$\frac{\alpha_2}{1 + \alpha_2 Q_2} - \frac{\beta_2}{1 + \beta_1 Q_1 + \beta_2 Q_2} + \mu_2 - \nu_2 = 0 \tag{128}$$

which, by using the fact that the two users cannot be jamming together, give the following conditions:

$$Q_1 = 0, \quad \text{if} \quad \alpha_1 > \beta_1 \tag{129}$$

$$Q_2 = 0, \quad \text{if} \quad \alpha_2 > \beta_2. \tag{130}$$

Moreover, we obtain necessary and sufficient conditions for the positivity of power allocations in the possible transmission/jamming scenarios in each channel state. First, when no user jams, i.e., $Q_1 = Q_2 = 0$, then from (94) and (95), we obtain the necessary and sufficient conditions (87) of Section VIII which we repeat here for convenience:

$$P_1 > 0, \quad \text{if and only if} \quad \alpha_1 - \frac{\beta_1}{(1 + \beta_2 P_2)} > \lambda_1 \tag{131}$$

$$P_2 > 0, \quad \text{if and only if} \quad \alpha_2 - \frac{\beta_2}{(1 + \beta_1 P_1)} > \lambda_2. \tag{132}$$

Second, when user 1 does not jam and user 2 does not transmit, i.e., $Q_1 = P_2 = 0$, then from (94) and (96), we can easily derive the following necessary and sufficient conditions for the positivity of the transmission power P_1 of user 1 and the jamming power Q_2 of user 2:

$$P_1 > 0, \quad \text{if and only if} \quad \alpha_1 - \frac{\beta_1}{(1 + \beta_2 Q_2)} > \lambda_1 \tag{133}$$

$$Q_2 > 0, \quad \text{if and only if} \quad \beta_2 - \frac{\beta_2}{(1 + \beta_1 P_1)} > \lambda_2. \tag{134}$$

Third, when user 1 does not transmit and user 2 does not jam, i.e., $P_1 = Q_2 = 0$, then from (95) and (97), we can similarly derive the following necessary and sufficient conditions for the

positivity of the transmission power P_2 of user 2 and the jamming power Q_1 of user 1:

$$P_2 > 0, \quad \text{if and only if} \quad \alpha_2 - \frac{\beta_2}{(1+\beta_1 Q_1)} > \lambda_2 \tag{135}$$

$$Q_1 > 0, \quad \text{if and only if} \quad \beta_1 - \frac{\beta_1}{(1+\beta_2 P_2)} > \lambda_1. \tag{136}$$

Using conditions (129)–(136) given previously, the power allocation policy (P_1, P_2, Q_1, Q_2) that satisfies (94)–(97) and (90) and (91) can be fully described through the following cases of the channel gains.

1) $\alpha_1 > \beta_1, \alpha_2 > \beta_2$. In this case, we must have $Q_1 = Q_2 = 0$. This follows directly from (129) and (130). Hence, this case reduces to one of the 7 cases given in Section VIII depending on the relative values of the channel gains and the values of λ_1 and λ_2. We can obtain the power allocations P_1 and P_2 in the same way described in Section VIII.
2) $\alpha_1 > \beta_1$, $\alpha_2 < \beta_2$. In this case, we must have $P_2 = Q_1 = 0$. This can be shown as follows. From (129), we must have $Q_1 = 0$. Suppose $P_2 > 0$. Hence, $\mu_2 = 0$. Since dividing power among transmission and jamming is suboptimal, then we must have $Q_2 = 0$. Since $Q_1 = 0$, then (128) implies $\bar{h}_2 - \bar{g}_2 \geq 0$ which is a contradiction. Therefore, $P_2 = 0$. The power allocations P_1 and Q_2 are obtained from one of the following subcases:
   a) $\alpha_1 \leq \lambda_1$ or $\alpha_1 - \beta_1 \leq \lambda_1, \beta_2 \leq \lambda_2$. We have $P_1 = Q_2 = 0$. To see this, note that $\alpha_1 \leq \lambda_1$ implies that $\alpha_1 - \frac{\beta_1}{(1+\beta_2 Q_2)} \leq \lambda_1$. Hence, using (133), we must have $P_1 = 0$ and thus $Q_2 = 0$ since we cannot have a jamming user when the other user is not transmitting. On the other hand, if $\beta_2 \leq \lambda_2$, then it follows from (134) that $Q_2 = 0$. Hence, the fact that $\alpha_1 - \beta_1 \leq \lambda_1$ together with (133) implies that $P_1 = 0$.
   b) $\alpha_1 - \beta_1 > \lambda_1, \beta_2 \leq \lambda_2$. We have $Q_2 = 0$ and $P_1 > 0$ where P_1 is given by (125). This can be shown to be true as follows. Since $\beta_2 \leq \lambda_2$, then, using (134), we must have $Q_2 = 0$. Hence, from (133) and the fact that $\alpha_1 - \beta_1 > \lambda_1$ in this case, we must have $P_1 > 0$.
   c) $\lambda_1 < \alpha_1 \leq \lambda_1 + \beta_1, \beta_2 > \lambda_2$. In this case, the solution (P_1, Q_2) may not be unique. Namely, we either have $P_1 > 0$ and $Q_2 > 0$, or we have $P_1 = Q_2 = 0$. This is due to the following facts. It is easy to see that $P_1 = Q_2 = 0$ satisfies $\alpha_1 - \frac{\beta_1}{(1+\beta_2 Q_2)} \leq \lambda_1$ and $\beta_2 - \frac{\beta_2}{(1+\beta_1 P_1)} \leq \lambda_2$, i.e., conditions (133) and (134). It is also easy to see that we can find positive P_1 and Q_2 that satisfy $\alpha_1 - \frac{\beta_1}{(1+\beta_2 Q_2)} > \lambda_1$ and $\beta_2 - \frac{\beta_2}{(1+\beta_1 P_1)} > \lambda_2$, i.e., conditions (133) and (134). Hence, the solution (P_1, Q_2) may not be unique. It remains to show that we cannot have $P_1 > 0, Q_2 = 0$. Suppose that $P_1 > 0$ and $Q_2 = 0$. Hence, we have $\alpha_1 - \frac{\beta_1}{(1+\beta_2 Q_2)} = \alpha_1 - \beta_1 \leq \lambda_1$ which, by (133), implies that $P_1 = 0$ which is a contradiction. Thus, we cannot have $P_1 > 0$ and $Q_2 = 0$. We obtain our power allocation policies for this case as follows. We examine the solution of (121) and (122), if it yields a real and nonnegative solution (P_1, Q_2), then we take it as our solution (P_1, Q_2) for this case. Otherwise, we set $P_1 = Q_2 = 0$.
   d) $\alpha_1 - \beta_1 > \lambda_1, \beta_2 > \lambda_2$. Here, we must have $P_1 > 0$. However, we either have $Q_2 > 0$ or $Q_2 = 0$, i.e., the solution may not be unique. To see this, we note that $\alpha_1 - \beta_1 > \lambda_1$ implies that $\alpha_1 - \frac{\beta_1}{(1+\beta_2 Q_2)} > \lambda_2$ for any $Q_2 \geq 0$. Hence, by (133), we must have $P_1 > 0$. However, we either have $Q_2 > 0$ or $Q_2 = 0$ depending on whether the value of P_1 satisfies $\beta_2 - \frac{\beta_2}{(1+\beta_1 P_1)} > \lambda_1$ or not. We obtain our power allocation policy as follows. We first solve (121) and (122), if this yields a real and nonnegative solution (P_1, Q_2), then we take it to be the power allocation values for this case. Otherwise, we set $Q_2 = 0$ and P_1 is obtained from (125).
3) $\alpha_1 < \beta_1, \alpha_2 > \beta_2$. From the symmetry between this case and the previous case, the power allocation roles can be obtained in this case by interchanging the power allocation roles of users 1 and 2 in the previous case. In particular, we must have $P_1 = Q_2 = 0$. The power allocations P_2 and Q_1 are given by one of the following subcases:
   a) $\alpha_2 \leq \lambda_2$ or $\beta_1 \leq \lambda_1, \alpha_2 - \beta_2 \leq \lambda_2$. We have $P_2 = Q_1 = 0$.
   b) $\beta_1 \leq \lambda_1, \alpha_2 - \beta_2 > \lambda_2$. We have $Q_1 = 0$ and $P_2 > 0$ where P_2 is given by (126).
   c) $\beta_1 > \lambda_1$, $\lambda_2 < \alpha_2 \leq \lambda_2 + \beta_2$. In this case, the solution (P_2, Q_1) may not be unique as we either have $P_2 > 0$ and $Q_1 > 0$, or have $P_1 = Q_2 = 0$. Therefore, we obtain our power allocation policy for this case by numerically solving (123) and (124), if we have a real and nonnegative solution (P_2, Q_1), then we take it as to be the power allocation values for this case. Otherwise, we set $P_2 = Q_1 = 0$.
   d) $\beta_1 > \lambda_1, \alpha_2 - \beta_2 > \lambda_2$. Here, we must have $P_2 > 0$. However, we either have $Q_1 > 0$ or $Q_1 = 0$, i.e., the solution may not be unique. We obtain our power allocation policy as follows. We first solve (123) and (124), if this yields a real and nonnegative solution (P_2, Q_1), then we take it to be the power allocation values for this case. Otherwise, we set $Q_1 = 0$ and P_2 is obtained from (126).
4) $\alpha_1 < \beta_1, \alpha_2 < \beta_2$ In this case, we have $P_2 = Q_1 = 0$ or $P_1 = Q_2 = 0$. In order to see this, suppose $P_1 > 0$ and $P_2 > 0$. Hence, $\mu_1 = \mu_2 = 0$. Since splitting a user's power into transmit and jamming powers is suboptimal, then we must have $Q_1 = Q_2 = 0$. Thus, from (127) and (128), we have $\bar{h}_1 \geq \bar{g}_1$ and $\bar{h}_2 \geq \bar{g}_2$ which is a contradiction. Therefore, we must have either $P_1 = 0$ or $P_2 = 0$. The power allocation policy (P_1, P_2, Q_1, Q_2) is given in the following four sub-cases of channel states:
   a) ($\alpha_1 \leq \lambda_1$ or $\beta_2 \leq \lambda_2$) and ($\alpha_2 \leq \lambda_2$ or $\beta_1 \leq \lambda_1$). In this case, we have $P_1 = P_2 = Q_1 = Q_2 = 0$. To see this, first, suppose that $P_2 = Q_1 = 0$. We note that if $\alpha_1 \leq \lambda_1$ then $\alpha_1 - \frac{\beta_1}{(1+\beta_2 Q_2)} \leq \lambda_1$. Hence, using (133), we must have $P_1 = 0$ and thus $Q_2 = 0$ since we cannot have a jamming user when the other user is not transmitting. On the other hand, if $\beta_2 \leq \lambda_2$, then it follows from (134) that $Q_2 = 0$. Hence, the fact that $\alpha_1 < \beta_1$ together with (133) implies that $P_1 = 0$.

Next, suppose that $P_1 = Q_2 = 0$. Using the fact that $\alpha_2 \leq \lambda_2$ or $\beta_1 \leq \lambda_1$ together with conditions (135) and (136), we can show that $P_2 = Q_1 = 0$. Therefore, in this case, we must have $P_1 = P_2 = Q_1 = Q_2 = 0$.

b) ($\alpha_2 \leq \lambda_2$ or $\beta_1 \leq \lambda_1$) and ($\alpha_1 > \lambda_1, \beta_2 > \lambda_2$). We have $P_2 = Q_1 = 0$. The solution (P_1, Q_2) may not be unique. In particular, we may have $P_1 > 0$, $Q_2 > 0$ or have $P_1 = Q_2 = 0$. To see this, consider the following argument. Using the fact that $\alpha_2 \leq \lambda_2$ or $\beta_1 \leq \lambda_1$, then, as shown in case $4(a)$, we conclude that we must have $P_2 = Q_1 = 0$. Now, we consider the power allocation policy (P_1, Q_2). We note that $P_1 = Q_2 = 0$ satisfies conditions (133) and (134). On the other hand, we can find positive P_1 and Q_2 that satisfy (133) and (133). Hence, the solution (P_1, Q_2) may not be unique as we may have $P_1 = Q_2 = 0$ or $P_1 > 0$, $Q_2 > 0$. It remains to show that we cannot have $P_1 > 0$, $Q_2 = 0$. Suppose that $P_1 > 0$ and $Q_2 = 0$. Hence, we have $\alpha_1 - \frac{\beta_1}{(1+\beta_2 Q_2)} = \alpha_1 - \beta_1 < 0 < \lambda_1$ which, by (133), implies that $P_1 = 0$ which is a contradiction. Thus, we cannot have $P_1 > 0$ and $Q_2 = 0$. Our power allocations P_1 and Q_2 are obtained for this case as follows. We solve (121) and (122). If the solution gives a real and nonnegative common root (P_1, Q_2), we take it as our power allocation values for P_1 and Q_2. Otherwise, we set $P_1 = Q_2 = 0$.

c) ($\alpha_1 \leq \lambda_1$ or $\beta_2 \leq \lambda_2$) and ($\alpha_2 > \lambda_2, \beta_1 > \lambda_1$). By the symmetry between this case and case $4(b)$, we have $P_1 = Q_2 = 0$. Again, in this case, the solution (P_2, Q_1) may not be unique. In particular, we may have $P_2 > 0$, $Q_1 > 0$ or have $P_2 = Q_1 = 0$. In fact, the power allocation policy in this case, can be obtained from case $4(b)$ by interchanging the roles of users 1 and 2. Our power allocations P_2 and Q_1 are obtained as follows in this case. We solve (123) and (124). If the solution gives a real and nonnegative common root (P_2, Q_1), we take it as our power allocation values for P_2 and Q_1. Otherwise, we set $P_2 = Q_1 = 0$.

d) ($\alpha_1 > \lambda_1, \beta_2 > \lambda_2$) and ($\alpha_2 > \lambda_2, \beta_1 > \lambda_1$). Here, again the solution (P_1, P_2, Q_1, Q_2) is not unique as we may either have $P_1 > 0$, $Q_2 > 0$, $P_2 = Q_1 = 0$, or $P_2 > 0$, $Q_1 > 0$, $P_1 = Q_2 = 0$, or $P_1 = P_2 = Q_1 = Q_2 = 0$. To see this, first, suppose that $P_2 = Q_1 = 0$ and consider the power allocation policy (P_1, Q_2). As in case $4(b)$, we can show that the solution (P_1, Q_2) may not be unique as we may have $P_1 = Q_2 = 0$ or $P_1 > 0$, $Q_2 > 0$. However, as shown in case $4(b)$, we cannot have $P_1 > 0$, $Q_2 = 0$. Next, suppose that $P_1 = Q_2 = 0$ and consider the power allocation policy (P_2, Q_1). As in case $4(c)$, we can show that the solution (P_2, Q_1) may not be unique as we may have $P_2 = Q_1 = 0$ or $P_2 > 0$, $Q_1 > 0$. However, we cannot have $P_2 > 0, Q_1 = 0$. We obtain our allocation policy (P_1, P_2, Q_1, Q_2) as follows. Let us denote the solution of (121) and (122) together by *solution*A and denote the solution of (123) and (124) together by *solution*B.

i) If solution A yields a real nonnegative (P_1, Q_2) while solution B does not yield real nonnegative (P_2, Q_1), then we take (P_1, Q_2) to be the power allocation values for users 1 and 2, respectively, and set $P_2 = Q_1 = 0$.

ii) If solution B yields a real nonnegative (P_2, Q_1) while solution A does not yield real nonnegative (P_1, Q_2), then we take (P_2, Q_1) to be the power allocation values for users 2 and 1, respectively, and set $P_1 = Q_2 = 0$.

iii) If neither solution A nor solution B gives real nonnegative common root, then we set $P_1 = P_2 = Q_1 = Q_2 = 0$.

iv) If both solutions A and B yield a real nonnegative common root, then we either choose the root given by solution A, i.e., (P_1, Q_2), and set $P_2 = Q_1 = 0$, or choose the root given by solution B, i.e., (P_2, Q_1), and set $P_1 = Q_2 = 0$. We make the choice that maximizes the achievable *instantaneous* secrecy sum rate.

REFERENCES

[1] R. Bassily and S. Ulukus, "A new achievable ergodic secrecy rate region for the fading multiple access wiretap channel," presented at the presented at the 47th Annu. Allerton Conf. Commun., Control Comput., Monticello, IL, Sep. 2009.

[2] R. Bassily and S. Ulukus, "Ergodic secret alignment for the fading multiple access wiretap channel," in *IEEE Int. Conf. Commun.*, Cape Town, South Africa, May 2010, pp. 1–5.

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

[4] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

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

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

[7] E. Tekin and A. Yener, "The Gaussian multiple access wiretap channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5747–5755, Dec. 2008.

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

[9] E. Ekrem and S. Ulukus, "Cooperative secrecy in wireless communications," in *Securing Wireless Communications at the Physical Layer*, W. Trappe and R. Liu, Eds. New York: Springer-Verlag, 2009.

[10] E. Ekrem and S. Ulukus, "On the secrecy of multiple access wiretap channel," in *Proc. 46th Annu. Allerton Conf. Commun., Control Comput.*, Sep. 2008, pp. 1014–1021.

[11] O. O. Koyluoglu, H. E. Gamal, L. Lai, and H. V. Poor, "Interference alignment for secrecy," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3323–3332, Jun. 2011.

[12] T. Gou and S. A. Jafar, "On the secure degrees of freedom of wireless X networks," in *Proc. 46th Annu. Allerton Conf. Commun., Control Comput.*, IL, Sep. 2008, pp. 826–833.

[13] X. He and A. Yener, "Secure degrees of freedom for Gaussian channels with interference: Structured codes outperform Gaussian signaling," in *Proc. IEEE Global Telecommun. Conf.*, 2009, pp. 1–6, [arXiv:0905.2638].

[14] X. He and A. Yener, "K-user interference channels: Achievable secrecy rate and degrees of freedom," in *Proc. IEEE Int. Theory Workshop Netw. Inf. Theory*, Jun. 2009, pp. 336–340.

[15] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "On the secure degrees of freedom of the multiple access channel," in *IEEE Int. Symp. Inf. Theory*, Austin, TX, Jun. 2010, pp. 1420–1427, [arXiv:1003.0729].

[16] V. R. Cadambe and S. A. Jafar, "Interference alignment and degrees of freedom of the K-user interference channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3425–3441, Aug. 2008.

[17] A. S. Motahari, S. O. Gharan, and A. K. Khandani, "Real interference alignment with real numbers," *IEEE Trans. Inf. Theory*, pp. 1–30, Aug. 2009 [Online]. Available: http://arxiv.org/abs/0908.1208v2

[18] E. Tekin and A. Yener, "Secrecy sum-rates for the multiple-access wire-tap channel with ergodic block fading," in *Proc. 45th Annu. Allerton Conf. Commun., Control Comput.*, Sep. 2007, pp. 856–863.

[19] B. Nazer, M. Gastpar, S. A. Jafar, and S. Vishwanath, "Ergodic interference alignment," in *Proc. IEEE Int. Symp. Inf. Theory*, Seoul, Korea, Jun. 2009, pp. 1769–1773.

Raef Bassily (S'11) received the B.S. degree in electrical and computer engineering and the M.S. degree in engineering mathematics from Cairo University, Giza, Egypt, in 2003 and 2006, respectively. Currently, he is working toward the Ph.D. degree in the department of electrical and computer engineering at the University of Maryland, College Park.

His research interests include information theory, wireless communications, and cryptography.

Sennur Ulukus (M'98) is a Professor of Electrical and Computer Engineering at the University of Maryland at College Park, where she also holds a joint appointment with the Institute for Systems Research (ISR). Prior to joining UMD, she was a Senior Technical Staff Member at AT&T Labs-Research. She received her Ph.D. degree in Electrical and Computer Engineering from Wireless Information Network Laboratory (WINLAB), Rutgers University, and B.S. and M.S. degrees in Electrical and Electronics Engineering from Bilkent University. Her research interests are in wireless communication theory and networking, network information theory for wireless communications, signal processing for wireless communications, information-theoretic physical-layer security, and energy-harvesting communications.

Dr. Ulukus received the 2003 IEEE Marconi Prize Paper Award in Wireless Communications, the 2005 NSF CAREER Award, and the 2010–2011 ISR Outstanding Systems Engineering Faculty Award. She served as an Associate Editor for the IEEE Transactions on Information Theory between 2007–2010, as an Associate Editor for the IEEE Transactions on Communications between 2003–2007, as a Guest Editor for the Journal of Communications and Networks for the special issue on energy harvesting in wireless networks, as a Guest Editor for the IEEE Transactions on Information Theory for the special issue on interference networks, as a Guest Editor for the IEEE Journal on Selected Areas in Communications for the special issue on multiuser detection for advanced communication systems and networks. She served as the TPC co-chair of the Communication Theory Symposium at the 2007 IEEE Global Telecommunications Conference, the Medium Access Control (MAC) Track at the 2008 IEEE Wireless Communications and Networking Conference, the Wireless Communications Symposium at the 2010 IEEE International Conference on Communications, the 2011 Communication Theory Workshop, the Physical-Layer Security Workshop at the 2011 IEEE International Conference on Communications, the Physical-Layer Security Workshop at the 2011 IEEE Global Telecommunications Conference. She was the Secretary of the IEEE Communication Theory Technical Committee (CTTC) in 2007–2009.