Ergodic Secret Alignment for the Fading Multiple Access Wiretap Channel

Raef Bassily Sennur Ulukus
Department of Electrical and Computer Engineering
University of Maryland, College Park, MD 20742
bassily@umd.edu *ulukus@umd.edu*

***Abstract*—In this paper, we provide a new achievable ergodic secrecy rate region for the multiple access wiretap channel in fading. Our achievable scheme is based on repeating each symbol at two fading instances, as in the original ergodic interference alignment technique of Nazer *et. al.* We choose the channel states where the symbols are repeated in such a way that the received signals are aligned favorably at the legitimate receiver, while they are aligned unfavorably at the eavesdropper. We show that our new scheme outperforms plain Gaussian signaling and Gaussian signaling with Gaussian channel prefixing, i.e., cooperative jamming, in high signal-to-noise ratios (SNR). In particular, we show that, while Gaussian signaling with or without channel prefixing yields zero secure degrees of freedom, our new achievable scheme provides a total of 1/2 secure degrees of freedom in a two-user multiple access channel in fading.**

I. Introduction

The multiple access wiretap channel (MAC-WT) was introduced in [1]. In MAC-WT, multiple users wish to have secure communication with a single receiver, in the presence of a passive eavesdropper. References [1] and [2] focus on the Gaussian MAC-WT, and provide achievable schemes based on Gaussian signaling. Reference [2] goes further than plain Gaussian signaling and introduces 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. Cooperative jamming is indeed a channel prefixing technique where specific choices are made for the auxiliary random variables [3]. In addition, cooperative jamming is the first significant application of channel prefixing in a multi-user Gaussian wiretap channel that improves over plain Gaussian signaling. More recently, reference [4] 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 can be obtained for Gaussian MAC-WT through 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 [5], [6], [7], and [8]. In particular, in each of [5] and [6], it was shown that positive secure DoF is achievable for a class of vector Gaussian interference channels (i.e., time-varying channels where channel state information is known non-causally) which in turn implies that positive secure DoF is achievable for the vector Gaussian MAC-WT. In [7] and [8], 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., non-time-varying) Gaussian channels with interference that contains the Gaussian MAC-WT.

Fading MAC-WT was first considered in [9], where Gaussian signaling and cooperative jamming based achievable schemes were presented. As in the non-fading setting, these schemes provide achievable secrecy rates which do not scale with the average SNRs. In [10], we proposed a new achievable scheme for fading MAC-WT. Our achievable scheme in [10] is based on code repetition with proper scaling of transmitted signals. In particular, in [10], 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 at the eavesdropper. In [10], we showed that the resulting secrecy rates scale with SNR. Specifically, the achievable secrecy sum rate scales as $\frac{1}{2}\log(SNR)$. The significance of this result is that, it showed that indeed neither plain Gaussian signaling nor Gaussian signaling with cooperative jamming is optimal for the fading MAC-WT, and that, for high SNRs, one can achieve higher secrecy rates by code repetition and signal scaling at the transmitters.

In another recent work [11], 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 $\frac{1}{2}\log(SNR)$. Thus, the rate reduction by a factor of $\frac{1}{2}$ comes with the benefit of perfect interference cancellation. In this

This work was supported by NSF Grants CCF 04-47613, CCF 05-14846, CNS 07-16311 and CCF 07-29127.

paper, we extend the ergodic interference alignment concept to a secrecy context and we call the resulting technique *ergodic secret alignment*. Using this technique, we introduce a new achievable secrecy rate region for the two-user fading MAC-WT. In [10], code repetition is done over two consecutive time instants, while here 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, let X_1 and X_2 be 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 $[g_1 \ g_2]^T$. Using this technique, we obtain a new achievable secrecy rate region for the fading MAC-WT. We show that, as in the case of [10], the achievable rates in this paper scale as $\frac{1}{2}\log(SNR)$ as well.

The achievable rate region in this paper involves two significant improvements over the one in [10]. In order to see those, we note the achievable sum secrecy rates found in this paper and in [10]: The achievable sum secrecy rate found in this paper is given in (9), and the achievable sum secrecy rate found in [10] is given in [10, eqn. (30)]. For circularly symmetric complex Gaussian channel coefficients, the squared magnitudes of the channel coefficients are exponential random variables and hence multiplying them will intuitively make the small values of their product occur with higher probability and the large values occur with lower probability. This in effect reduces the expectation in [10, eqn. (30)] and hence yields lower rates than the one in (9) in this paper. The second improvement of the technique here with respect to [10] is that the average power constraints associated with the achievable rate region, i.e., those in (10) in this paper, do not involve any channel coefficients whereas those in [10], i.e., [10, eqns. (31)-(32)], involve the gains of the eavesdropper channel which in turn result in inefficient use of transmit powers.

Moreover, we introduce an improved version of our scheme in which we use cooperative jamming on top of the ergodic secret alignment scheme to achieve higher secrecy rates. In [12], we derive the optimum power control strategies that maximize secrecy sum rates achievable by our scheme with and without cooperative jamming. Due to space limitations here, we are unable to provide the derivation of the optimum power control policies and refer to [12] for details. Instead, we present simple simulation results here, which show the improvements cooperative jamming and power control provide.

II. System Model and Problem Formulation

We consider the two-user fading multiple access channel with an external eavesdropper. The channel output at the intended receiver and the eavesdropper are given by

$$Y = h_1X_1 + h_2X_2 + N \tag{1}$$

$$Z = g_1X_1 + g_2X_2 + N' \tag{2}$$

where, for $k = 1,2$, X_k is the input signal at transmitter k, h_k is the channel coefficient between transmitter k and the intended receiver, g_k is the channel coefficient between transmitter k and the eavesdropper. 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_1, h_2, g_1, and g_2 at every symbol instant. At any instant of time, each of the channel coefficients is a circularly symmetric complex Gaussian random variable with zero-mean. The variances of h_k and g_k are $\sigma^2_{h_k}$ and $\sigma^2_{g_k}$, respectively. Hence, $|h_k|^2$ and $|g_k|^2$ are exponentially distributed 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 and N' are the 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. Moreover, we have the usual average power constraints $E[|X_k|^2] \leq \bar{P}_k$, for $k = 1,2$.

For this channel, we use a repetition code in a way similar to the one in [11]. Indeed, we repeat each code symbol in the time instant that holds certain channel conditions relative to 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.

Now, 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

$$Y_1 = h_1X_1 + h_2X_2 + N_1 \tag{3}$$

$$Y_2 = \tilde{h}_1X_1 + \tilde{h}_2X_2 + N_2 \tag{4}$$

where Y_1, Y_2 and N_1, N_2 are the received signals 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

$$Z_1 = g_1X_1 + g_2X_2 + N'_1 \tag{5}$$

$$Z_2 = \tilde{g}_1X_1 + \tilde{g}_2X_2 + N'_2 \tag{6}$$

where Z_1, Z_2 and N'_1, N'_2 are the received signals and the noise at the eavesdropper in the two time instants of code repetition.

In the next section, we will write achievable secrecy rates for the vector channels (3)-(4) and (5)-(6), using Gaussian signaling, and determine the best choices for repetition instants $\tilde{\mathbf{h}}$ and $\tilde{\mathbf{g}}$. In writing the achievable rate expressions, we will account for code repetition by multiplying achievable rates by a factor of $\frac{1}{2}$.

III. Main Result

The main result of this paper is given in the following theorem which gives a new achievable secrecy rate region for the two-user fading MAC-WT. The achievable region is obtained due to a scheme that uses the standard Gaussian signaling as in [1] and [2] and on top of such standard signaling, we use two extra ingredients that yield secrecy rates that scale with SNR. The first ingredient is code repetition which creates a system of two parallel scalar MACs for both the main receiver and the eavesdropper. The second ingredient is the ergodic secret alignment technique that chooses the repetition instants in such a way that the parallel MAC to the main receiver is the most favorable from the main transmitter-receiver pair's point of view, and the parallel MAC to the eavesdropper is the least favorable from the eavesdropper's point of view. As we will show shortly as a result of Theorem 1, this optimal selection will yield an *orthogonal* MAC to the main receiver and a *scalar* MAC to the eavesdropper.

Theorem 1: 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

$$R_1 \leq \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \Big\{ \log\left(1 + 2|h_1|^2 P_1\right) - \log\left(1 + \frac{2|g_1|^2 P_1}{1 + 2|g_2|^2 P_2}\right) \Big\} \tag{7}$$

$$R_2 \leq \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \Big\{ \log\left(1 + 2|h_2|^2 P_2\right) - \log\left(1 + \frac{2|g_2|^2 P_2}{1 + 2|g_1|^2 P_1}\right) \Big\} \tag{8}$$

$$R_1 + R_2 \leq \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \Big\{ \log\left(1 + 2|h_1|^2 P_1\right) + \log\left(1 + 2|h_2|^2 P_2\right) - \log\left(1 + 2(|g_1|^2 P_1 + |g_2|^2 P_2)\right) \Big\} \tag{9}$$

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. In addition, they satisfy the average power constraints

$$E[P_1] \leq \bar{P}_1, \qquad E[P_2] \leq \bar{P}_2 \tag{10}$$

Next, we give the proof of this theorem.

Proof: First, consider the two vector MACs given by (3)-(6). Observe that as in [11], $\tilde{\mathbf{h}}$ 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 $\mathbf{g}$. Since $\mathbf{h} \sim \mathcal{CN}(\mathbf{0}, \mathbf{B}_h)$ and $\mathbf{g} \sim \mathcal{CN}(\mathbf{0}, \mathbf{B}_g)$ where $\mathbf{B}_h = \text{diag}(\sigma_{h_1}^2, \sigma_{h_2}^2)$ and $\mathbf{B}_g = \text{diag}(\sigma_{g_1}^2, \sigma_{g_2}^2)$, then $\tilde{\mathbf{h}}$ and $\tilde{\mathbf{g}}$ must be in the form $\tilde{\mathbf{h}} = \mathbf{U}\mathbf{h}$ and $\tilde{\mathbf{g}} = \mathbf{V}\mathbf{g}$, where the unitary matrices $\mathbf{U}$ and $\mathbf{V}$ must further be of the form: $\mathbf{U} = \text{diag}(\exp(j\theta_1), \exp(j\theta_2))$ and $\mathbf{V} = \text{diag}(\exp(j\omega_1), \exp(j\omega_2))$ for some $\theta_1, \theta_2, \omega_1, \omega_2 \in [0, 2\pi)$. Then, it follows that (3)-(6) can be written as

$$Y_1 = h_1 X_1 + h_2 X_2 + N_1 \tag{11}$$

$$Y_2 = h_1 e^{j\theta_1} X_1 + h_2 e^{j\theta_2} X_2 + N_2 \tag{12}$$

$$Z_1 = g_1 X_1 + g_2 X_2 + N_1' \tag{13}$$

$$Z_2 = g_1 e^{j\omega_1} X_1 + g_2 e^{j\omega_2} X_2 + N_2' \tag{14}$$

As in [1], [2] and [10], the following rate pairs are achievable with perfect secrecy for the two-user fading MAC-WT described by (11)-(14),

$$R_1 \leq \frac{1}{2}[I(X_1; Y_1, Y_2 | X_2, \mathbf{h}, \mathbf{g}) - I(X_1; Z_1, Z_2 | \mathbf{h}, \mathbf{g})] \tag{15}$$

$$R_2 \leq \frac{1}{2}[I(X_2; Y_1, Y_2 | X_1, \mathbf{h}, \mathbf{g}) - I(X_2; Z_1, Z_2 | \mathbf{h}, \mathbf{g})] \tag{16}$$

$$R_1 + R_2 \leq \frac{1}{2}[I(X_1, X_2; Y_1, Y_2 | \mathbf{h}, \mathbf{g}) - I(X_1, X_2; Z_1, Z_2 | \mathbf{h}, \mathbf{g})] \tag{17}$$

where the factor of $\frac{1}{2}$ on the right hand sides of (15)-(17) is due to repetition coding. Now, by computing (15)-(17) with Gaussian signals, we get

$$R_1 \leq \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \Big\{ \log\left(1 + 2|h_1|^2 P_1\right) - \log\left(1 + \frac{2|g_1|^2 P_1 + 2(1 - \cos(\omega))|g_1|^2 |g_2|^2 P_1 P_2}{1 + 2|g_2|^2 P_2}\right) \Big\} \tag{18}$$

$$R_2 \leq \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \Big\{ \log\left(1 + 2|h_2|^2 P_2\right) - \log\left(1 + \frac{2|g_2|^2 P_2 + 2(1 - \cos(\omega))|g_1|^2 |g_2|^2 P_1 P_2}{1 + 2|g_1|^2 P_1}\right) \Big\} \tag{19}$$

$$R_1 + R_2 \leq \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \Big\{ \log(1 + 2|h_1|^2 P_1 + 2|h_2|^2 P_2 + 2(1 - \cos(\theta))|h_1|^2 |h_2|^2 P_1 P_2) - \log(1 + 2|g_1|^2 P_1 + 2|g_2|^2 P_2 + 2(1 - \cos(\omega))|g_1|^2 |g_2|^2 P_1 P_2) \Big\} \tag{20}$$

where $\theta = \theta_2 - \theta_1$ and $\omega = \omega_2 - \omega_1$.

Hence, the largest achievable secrecy rate region (18)-(20) 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 (18)-(20), we obtain the region given by (7)-(9). ■

Therefore, when using the ergodic secret alignment 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

$$\bar{Y}_1 = 2h_1X_1 + \bar{N}_1 \tag{21}$$

$$\bar{Y}_2 = 2h_2X_2 + \bar{N}_2 \tag{22}$$

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

$$\bar{Z}_1 = 2g_1X_1 + 2g_2X_2 + \bar{N}_1' \tag{23}$$

$$\bar{Z}_2 = \bar{N}_2' \tag{24}$$

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.

Intuitively, the achievable secrecy rates given above in Theorem 1, scale with SNR as $\frac{1}{2}\log(SNR)$. This can be observed from the achievable rates in (7)-(9), by using constant (channel independent) powers for both users and by letting the powers go to infinity and taking limits. This leads to the conclusion that the ergodic secret alignment scheme introduced here achieves a total of $\frac{1}{2}$ secure DoF in the fading MAC-WT as in [10]. However, the rates achieved here are larger as will be illustrated in the numerical results section.

IV. Improving Rates with Cooperative Jamming

The previous result can be strengthened by adding the technique of cooperative jamming to our proposed scheme. This is done through Gaussian channel prefixing as in [3] and [10] where we set the channel inputs $X_1 = U_1 + V_1$ and $X_2 = U_2 + V_2$, and then choose U_1, U_2, V_1, V_2 to be independent Gaussian random variables. Here, U_1 and U_2 carry messages, while V_1 and V_2 are jamming signals. The powers of (U_1, V_1) and (U_2, V_2) should be chosen to satisfy the power constraints of users 1 and 2, respectively. These selections when made in our ergodic secret alignment scheme yield the following achievable rate region which, through appropriate power control strategy [12], can be made strictly larger than the region given in Theorem 1,

$$\begin{aligned} R_1 \leq \frac{1}{2}E_{\mathbf{h},\mathbf{g}}\Big\{ &\log\left(1 + \frac{2|h_1|^2P_1}{1 + 2|h_1|^2Q_1}\right) \\ &- \log\left(1 + \frac{2|g_1|^2P_1}{1 + 2|g_1|^2Q_1 + 2|g_2|^2(P_2 + Q_2)}\right)\Big\} \end{aligned} \tag{25}$$

$$\begin{aligned} R_2 \leq \frac{1}{2}E_{\mathbf{h},\mathbf{g}}\Big\{ &\log\left(1 + \frac{2|h_2|^2P_2}{1 + 2|h_2|^2Q_2}\right) \\ &- \log\left(1 + \frac{2|g_2|^2P_2}{1 + 2|g_1|^2(P_1 + Q_1) + 2|g_2|^2Q_2}\right)\Big\} \end{aligned} \tag{26}$$

$$\begin{aligned} R_1 + R_2 \leq \frac{1}{2}E_{\mathbf{h},\mathbf{g}}\Big\{ &\log\left(1 + \frac{2|h_1|^2P_1}{1 + 2|h_1|^2Q_1}\right) \\ &+ \log\left(1 + \frac{2|h_2|^2P_2}{1 + 2|h_2|^2Q_2}\right) \\ &- \log\left(1 + \frac{2(|g_1|^2P_1 + |g_2|^2P_2)}{1 + 2(|g_1|^2Q_1 + |g_2|^2Q_2)}\right)\Big\} \end{aligned} \tag{27}$$

where, for $k = 1, 2$, P_k and Q_k are the transmission and jamming powers, respectively, of user k, and are both functions of $\mathbf{h}$ and $\mathbf{g}$ in general. In addition, they satisfy the average power constraints

$$E[P_1 + Q_1] \leq \bar{P}_1, \qquad E[P_2 + Q_2] \leq \bar{P}_2 \tag{28}$$

V. Further Improvements with Power Control

We obtain the optimal power allocation policies that maximize the achievable secrecy sum rates by our scheme when used solely and with cooperative jamming. We solve for the optimum power values, as a function of the channel states, in (9) when no cooperative jamming is used. When cooperative jamming is used on top of our scheme, we solve for the optimum power values, as a function of the channel states, in (27). The derivation of the optimum power allocation scheme is omitted here due to space limitations and can be found in [12]. A notable feature in the power control strategies derived in [12] is that we may have a transmitting user (i.e., optimum non-zero power) even though the gain of the channel from this user to the receiver is close to (or even less than) the gain of the channel from the user to the eavesdropper. Moreover, when cooperative jamming is used, we show in [12] that, for any channel state, splitting a user's power between transmission and jamming is suboptimal. In addition, when cooperative jamming is used we show in [12] that when $|h_1| < |g_1|$ and $|h_2| > |g_2|$, user 1 must jam, i.e., $Q_1 > 0$ and user 2 must transmit, i.e., $P_2 > 0$. In this case, the jamming user can significantly boost the achievable secrecy sum rate. We have a similar situation when $|h_1| > |g_1|$ and $|h_2| < |g_2|$ where in this case the roles of users 1 and 2 must be interchanged.

VI. Numerical Results

In this section, we present some simple simulation results. We also plot the sum secrecy rate achieved using the cooperative jamming technique in [9]. It was shown in [10] that the scheme based on cooperative jamming with Gaussian signaling is suboptimal since it achieves a secrecy sum rate that does not scale with SNR as compared to the scheme in [10] that is based on scaling based interference alignment. Here we plot the three secrecy sum rates together to illustrate the following facts. First, the secrecy sum rate achieved in this paper scales with SNR. Hence, it exceeds the one based on cooperative jamming on top of Gaussian signaling for high SNR. Second, the secrecy sum rate achieved in this paper is larger than the one in [10] for all SNR.

In our simulations, we first use a rudimentary power allocation policy for the scheme described in this paper similar to the one in [10]. Namely, we set $P_1 = \bar{P}_1$ and $P_2 = \bar{P}_2$ for all channel states. For the scheme in [10], we use the

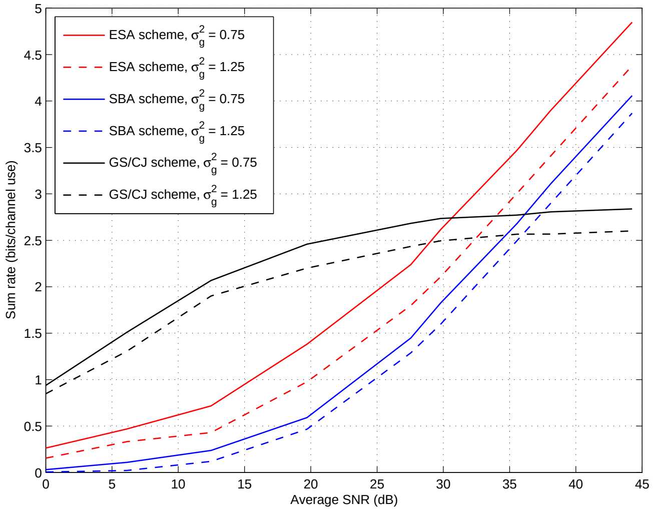

Fig. 1. Achievable secrecy sum rates of the ergodic secret alignment scheme (ESA scheme) of this paper, the scaling based alignment scheme (SBA scheme) of [10], and the Gaussian signaling with cooperative jamming scheme (GS/CJ scheme) of [9], as function of the SNR for two different values of mean eavesdropper channel gain, σ_g^2.

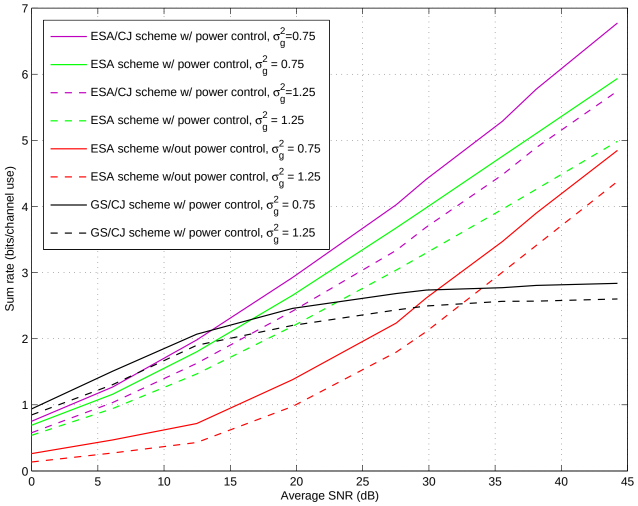

Fig. 2. Achievable secrecy sum rates for the ergodic secret alignment scheme (ESA scheme) of this paper, with and without optimum power control, the ergodic secret alignment with cooperative jamming scheme (ESA/CJ scheme) of this paper with optimum power control, and the Gaussian signaling with cooperative jamming scheme (GS/CJ scheme) of [9], as function of the SNR for two different values of mean eavesdropper channel gain, σ_g^2.

simple power allocation policy described in [10] which is also a constant power allocation scheme, however, since each transmitter scales its transmit signal with the channel gain of the other transmitter to the eavesdropper, the constant power in [10] is not necessarily equal to the average power. For the cooperative jamming scheme, we use the optimal power allocation policy described in [9].

In Figure 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 $\sigma_{g_1}^2 = \sigma_{g_2}^2$ and we let σ_g^2 denote their common value. Next, in Figure 2, we plot secrecy sum rates achievable with constant power allocation together with secrecy sum rates achievable with optimum power allocation for the ergodic secret alignment scheme with and without cooperative jamming.

VII. Conclusions

In this paper, we proposed a new achievable secrecy scheme for the two-user fading MAC-WT based on the ergodic interference alignment technique. This new scheme resulted in a new achievable secrecy rate region. We showed that the best choice of the main receiver and eavesdropper channel state vectors that the transmitters must wait for to repeat a code symbol makes the two parallel MAC channels between the two transmitters and the main receiver equivalent to an orthogonal MAC, while this choice of channel state vectors makes the two parallel MAC channels between the two transmitters and the eavesdropper equivalent to a single scalar MAC. We showed that the secrecy sum rate achieved using the technique described in this paper scales with SNR and is larger than the secrecy sum rate achieved using the techniques in [9] and [10]. We introduced an improved version of our scheme where cooperative jamming is used to achieve higher secrecy rates. Finally, we presented simulation results of achievable secrecy sum rates with optimum power allocation.

References

[1] E. Tekin and A. Yener. The Gaussian multiple access wiretap channel. *IEEE Trans. on Inf. Theory, 54(12):5747-5755*, December 2008.

[2] E. Tekin and A. Yener. The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming. *IEEE Trans. on Inf. Theory, 54(6):2735-2751*, June 2008.

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

[4] E. Ekrem and S. Ulukus. On the secrecy of multiple access wiretap channel. *46th Annual Allerton Conference on Communication, Control and Computing*, September 2008.

[5] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor. Interference alignment for secrecy. *IEEE Trans. on Inf. Theory*, October 2008. Submitted. Also available at [arXiv:0810.1187].

[6] T. Gou and S. A. Jafar. On the secure degrees of freedom of wireless X networks. *46th Annual Allerton Conference on Communication, Control and Computing*, September 2008.

[7] X. He and A. Yener. Secure degrees of freedom for Gaussian channels with interference: Structured codes outperform Gaussian signaling. *IEEE Globecom*, March 2009.

[8] X. He and A. Yener. K-user interference channels: Achievable secrecy rate and degrees of freedom. *IEEE Information Theory Workshop, Volos, Greece*, June 2009.

[9] E. Tekin and A. Yener. Secrecy sum-rates for the multiple-access wiretap channel with ergodic block fading. *45th Annual Allerton Conference on Communication, Control and Computing*, September 2007.

[10] R. Bassily and S. Ulukus. A new achievable secrecy rate region for the fading multiple access wiretap channel. *47th Annual Allerton Conference on Communication, Control, and Computing*, September 2009.

[11] B. Nazer, M. Gastpar, S. A. Jafar, and S. Vishwanath. Ergodic interference alignment. *In IEEE International Symposium on Information Theory, Seoul, Korea*, June 2009.

[12] R. Bassily and S. Ulukus. Ergodic secret alignment. To be submitted for journal publication.