A New Achievable Ergodic Secrecy Rate Region 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*—We give a new achievable ergodic secrecy rate region for the two-user fading multiple access wiretap channel. Our scheme creates a vector channel between the two transmitters and the intended receiver that has full-rank and creates another vector channel between the two transmitters and the eavesdropper whose rank is 1. In this sense, our scheme removes interference from the main receiver multiple access channel by introducing an extra dimension in this channel, while sustaining the interference in the eavesdropper multiple access channel by keeping the rank of this channel equal to one. We show that the secrecy sum rate achieved by our scheme scales with SNR. In particular, we show that a total number of $1/2$ secure degrees of freedom is achievable for the two users. Moreover, we compare our scheme with the Gaussian signaling scheme with cooperative jamming which improves significantly over the plain Gaussian signaling scheme. Our proposed scheme outperforms Gaussian signaling schemes (with or without cooperative jamming) at high signal-to-noise ratios (SNR). In particular, we show that Gaussian signaling schemes with or without cooperative jamming achieve zero secure degrees of freedom, while our proposed scheme achieves $1/2$ total secure degrees of freedom.**

I. Introduction

The notion of information theoretic secrecy was first introduced by Shannon in his seminal work [1]. Applying the notion of information theoretic secrecy to channel models with single transmitter, single receiver, and single eavesdropper (wiretapper) was pioneered by Wyner [2], Csiszar and Korner [3], and Leung-Yan-Cheong and Hellman [4]. Wyner [2], 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 [3], 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 [4], 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 Gaussian multiple access wiretap (MAC-WT) was introduced by [5]. In MAC-WT, multiple users wish to have secure communication with a single legitimate receiver, in the presence of an external eavesdropper. In [5] and [6], achievable secrecy rate regions were proposed for the Gaussian MAC-WT based on Gaussian signaling. Moreover, reference [6] goes further than plain Gaussian signaling and introduces a technique (on top of Gaussian signaling) in which a transmitter whose channel to the eavesdropper is stronger than its channel to the main receiver jams the eavesdropper and consequently helps increase the achievable secrecy rate of the other transmitter. This technique is known as cooperative jamming. Cooperative jamming can be interpreted as a channel prefixing technique, where specific choices are made for the auxiliary random variables [7]. In addition, cooperative jamming is the first practical example of channel prefixing in a multi-user wiretap channel that showed substantial improvement over plain Gaussian signaling. There have been other works that considered Gaussian signaling in achieving secrecy rates for the Gaussian MAC-WT, e.g., reference [8] 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.

A common notable disadvantage of these Gaussian signaling based schemes is that the secrecy rates that they achieve do not scale with the signal-to-noise ratios (SNR) of the users. In other words, the total number of secure degrees of freedom (DoF) achieved for the MAC-WT using these schemes is zero. This observation has a significant implication in light of recent results on the secure DoF of Gaussian interference networks, e.g., in [9], [10], [11], and [12]. These works showed that it is possible to achieve positive secure DoF for some classes of Gaussian interference channels that contain the Gaussian MAC-WT as a special case. In particular, in each of [9] and [10], it was shown that positive secure DoF is achievable for a class of vector Gaussian interference channels, e.g., time-varying interference channels where channel state information is known non-causally, which implies that positive secure DoF is achievable for the vector Gaussian MAC-WT. In [11] and [12], it was shown that through structured coding (e.g. lattice coding), it is possible to achieve positive secure DoF for a class

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

of scalar Gaussian channels with interference, that contains the Gaussian MAC-WT as a special case. These observations led to the conclusion that Gaussian signaling (with or without channel prefixing) is sub-optimal for the Gaussian MAC-WT.

Fading Gaussian MAC-WT was first considered in [13]. In [13], the authors have extended their Gaussian signaling and cooperative jamming based schemes which were originally proposed in [5] and [6] to the fading model of the MAC-WT. Using these schemes, they gave achievable ergodic secrecy rates for the fading MAC-WT. As intuition may suggest, as in the non-fading setting, these achievable ergodic secrecy rates do not scale with the average SNRs. In this paper, we propose a new achievable scheme for the fading Gaussian MAC-WT. Our achievable scheme is based on code repetition with proper scaling of transmitted signals. In particular, 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 decode both messages. Consequently, we obtain a new achievable secrecy rate region for the two-user fading MAC-WT. In addition, we show that the resulting secrecy rates scale with SNR. Specifically, the achievable secrecy sum rate scales as $1/2\log(SNR)$. Moreover, we show that the secrecy rates achieved through Gaussian signaling with cooperative jamming in fading MAC-WT do not scale with SNR. The significance of these results is that, they show 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 a recent work [14], Nazer *et. al.* showed that in a fading interference channel, given that the channel state information of all the links of the interference channel is available at all the nodes, each transmitter may repeat its symbols over two *carefully chosen* time instants, so that interference is perfectly canceled at each receiver. Hence, the resulting individual rates scale as $1/2\log(SNR)$. Thus, the rate reduction by a factor of $1/2$ comes with the benefit of perfect interference cancelation. In this paper, we briefly discuss the extension of the ergodic interference alignment concept to a secrecy context and we introduce a new technique which we call *ergodic secret alignment*. Using this technique, we introduce another achievable secrecy rate region for the two-user fading MAC-WT in which the achievable secrecy rates also scale with SNR as $1/2\log(SNR)$. The difference between *scaling-based* alignment discussed above and *opportunistic* alignment inspired by [14] is that, in the first case, we repeat the symbol in two *consecutive* time instances, and use scaling to achieve alignment irrespective of the channel states nature provides in these two consecutive time instances, while in the second case, we wait for the favorable channel states, where nature provides alignment for free.

II. System Model

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

$$Y_i = h_{1i}X_{1i} + h_{2i}X_{2i} + N_i \tag{1}$$

$$Z_i = g_{1i}X_{1i} + g_{2i}X_{2i} + N_i' \tag{2}$$

where, for $k = 1, 2$, X_{ki} is the input signal at the ith symbol at transmitter k, h_{ki} is the channel coefficient between transmitter k and the intended receiver at the ith symbol, g_{ki} is the channel coefficient between transmitter k and the eavesdropper at the ith symbol. 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 $\sigma_{h_k}^2$ and $\sigma_{g_k}^2$, respectively. Hence, $|h_k|^2$ and $|g_k|^2$ are exponentially distributed with mean $\sigma_{h_k}^2$ and $\sigma_{g_k}^2$, respectively. Moreover, we assume that all the channel coefficients are known to all the nodes in a causal fashion. In (1), (2), N_i and N_i' are the Gaussian noises in the ith symbol at the intended receiver and the eavesdropper, respectively. $\{N_i\}_{i=1}^{2n}$ and $\{N_i'\}_{i=1}^{2n}$ are i.i.d. circularly symmetric complex Gaussian random variables with zero-mean and unit-variance. Moreover, we have the following average power constraints

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

where $\bar{P}_k$ is the average power of user k.

III. Scaling Based Alignment

In this section, we propose 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)-(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

$$Y_o = h_{1o}X_1 + h_{2o}X_2 + N_o \quad (4)$$
$$Y_e = h_{1e}X_1 + h_{2e}X_2 + N_e \quad (5)$$

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

$$Z_o = g_{1o}X_1 + g_{2o}X_2 + N'_o \quad (6)$$
$$Z_e = g_{1e}X_1 + g_{2e}X_2 + N'_e \quad (7)$$

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 the ith time instant, the first user multiplies its channel input with g_{2i}, the channel gain of the second user to the eavesdropper, and the second user multiplies its channel input with g_{1i}, the channel gain of the first user to the eavesdropper. Hence the main receiver MAC can be described as

$$Y_o = h_{1o}g_{2o}X_1 + h_{2o}g_{1o}X_2 + N_o \quad (8)$$
$$Y_e = h_{1e}g_{2e}X_1 + h_{2e}g_{1e}X_2 + N_e \quad (9)$$

and the eavesdropper MAC can be described as

$$Z_o = g_{1o}g_{2o}X_1 + g_{1o}g_{2o}X_2 + N'_o \quad (10)$$
$$Z_e = g_{1e}g_{2e}X_1 + g_{2e}g_{2e}X_2 + N'_e \quad (11)$$

It is clear from (8)-(9) that the space of the received signal (without noise, i.e., high SNR) of the main receiver over the two consecutive time instants is two-dimensional 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 (10)-(11) 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 two-dimensional space, while they *align* the interfering signals at the eavesdropper in a one-dimensional space. As we will show in the next section, these properties play the central role in achieving secrecy rates that scale with SNR. Finally, we note that, due to signal scaling at the transmitters, the average power constraints become

$$E\left[\left(|g_{2o}|^2 + |g_{2e}|^2\right) P_1\right] \leq \bar{P}_1 \quad (12)$$
$$E\left[\left(|g_{1o}|^2 + |g_{1e}|^2\right) P_2\right] \leq \bar{P}_2 \quad (13)$$

where P_1 and P_2, which are functions of the channel gains, are the instantaneous powers of users 1 and 2, respectively, while $\bar{P}_1$ and $\bar{P}_2$ are average power constraints.

IV. 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 is given by the convex hull of all rate pairs (R_1, R_2) satisfying [5], [6], and [7]

$$R_1 \leq \left[I(U_1; Y|U_2) - I(U_1; Z)\right]^+ \quad (14)$$
$$R_2 \leq \left[I(U_2; Y|U_1) - I(U_2; Z)\right]^+ \quad (15)$$
$$R_1 + R_2 \leq \left[I(U_1, U_2; Y) - I(U_1, U_2; Z)\right]^+ \quad (16)$$

where the joint distribution $p(x_1, x_2, u_1, u_2, y, z)$ factors as $p(u_1)p(x_1|u_1)p(u_2)p(x_2|u_2)p(y, z|x_1, x_2)$, where $(.)^+$ denotes the positivity operator, i.e., $(x)^+ = \max(0, x)$.

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 [5] are obtained by choosing $X_1 = U_1$ and $X_2 = U_2$, i.e., no channel prefixing, and by choosing X_1 and X_2 to be Gaussian with full power. On the other hand, cooperative jamming based achievable rates proposed in [6] are obtained by choosing $X_1 = U_1 + V_1$ and $X_2 = U_2 + V_2$, and then by choosing 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 yield the following achievable rate region for the Gaussian MAC-WT [6]

$$R_1 \leq \left[\log\left(1 + \frac{|h_1|^2 P_1}{1 + |h_1|^2 Q_1 + |h_2|^2 Q_2}\right) - \log\left(1 + \frac{|g_1|^2 P_1}{1 + |g_1|^2 Q_1 + |g_2|^2 (P_2 + Q_2)}\right)\right]^+ \quad (17)$$

$$R_2 \leq \left[\log\left(1 + \frac{|h_2|^2 P_2}{1 + |h_1|^2 Q_1 + |h_2|^2 Q_2}\right) - \log\left(1 + \frac{|g_2|^2 P_2}{1 + |g_1|^2 (P_1 + Q_1) + |g_2|^2 Q_2}\right)\right]^+ \quad (18)$$

$$R_1 + R_2 \leq \left[\log\left(1 + \frac{|h_1|^2 P_1 + |h_2|^2 P_2}{1 + |h_1|^2 Q_1 + |h_2|^2 Q_2}\right) - \log\left(1 + \frac{|g_1|^2 P_1 + |g_2|^2 P_2}{1 + |g_1|^2 Q_1 + |g_2|^2 Q_2}\right)\right]^+ \quad (19)$$

where the powers of the signals must satisfy

$$P_k + Q_k \leq \bar{P}_k, \quad k = 1, 2 \quad (20)$$

where for $k = 1, 2$, 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 cooperative jamming for the fading MAC-WT can be expressed similarly by simply including expectations

over fading channel states [13]

$$R_1 \leq E_{\mathbf{h},\mathbf{g}}\Bigg\{ \log\left(1+\frac{|h_1|^2P_1}{1+|h_1|^2Q_1+|h_2|^2Q_2}\right) - \log\left(1+\frac{|g_1|^2P_1}{1+|g_1|^2Q_1+|g_2|^2(P_2+Q_2)}\right)\Bigg\} \tag{21}$$

$$R_2 \leq E_{\mathbf{h},\mathbf{g}}\Bigg\{ \log\left(1+\frac{|h_2|^2P_2}{1+|h_1|^2Q_1+|h_2|^2Q_2}\right) - \log\left(1+\frac{|g_2|^2P_2}{1+|g_1|^2(P_1+Q_1)+|g_2|^2Q_2}\right)\Bigg\} \tag{22}$$

$$R_1+R_2 \leq E_{\mathbf{h},\mathbf{g}}\Bigg\{ \log\left(1+\frac{|h_1|^2P_1+|h_2|^2P_2}{1+|h_1|^2Q_1+|h_2|^2Q_2}\right) - \log\left(1+\frac{|g_1|^2P_1+|g_2|^2P_2}{1+|g_1|^2Q_1+|g_2|^2Q_2}\right)\Bigg\} \tag{23}$$

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

$$E\left[P_k+Q_k\right] \leq \bar{P}_k, \quad k=1,2 \tag{24}$$

where $\bar{P}_k$ are average power constraints.

V. A New Achievable Secrecy Rate Region

Here we evaluate the secrecy rate region achievable by the *scaling based alignment* scheme proposed in Section III. Given the vector channels (8)-(9) and (10)-(11) created by the scheme we proposed, the following secrecy rates are achievable [5], [6] and [7]

$$R_1 \leq \frac{1}{2}[I(X_1;Y_o,Y_e|X_2,\mathbf{h},\mathbf{g}) - I(X_1;Z_o,Z_e|\mathbf{h},\mathbf{g})]^+ \tag{25}$$

$$R_2 \leq \frac{1}{2}[I(X_2;Y_o,Y_e|X_1,\mathbf{h},\mathbf{g}) - I(X_2;Z_o,Z_e|\mathbf{h},\mathbf{g})]^+ \tag{26}$$

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

These rates follow from (14)-(16) 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 $1/2$ 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 as our main result.

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

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

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

$$R_1+R_2 \leq \frac{1}{2}E_{\mathbf{h},\mathbf{g}}\Bigg\{ \log\Bigg(1+\left(|h_{1o}g_{2o}|^2+|h_{1e}g_{2e}|^2\right)P_1 + \left(|h_{2o}g_{1o}|^2+|h_{2e}g_{1e}|^2\right)P_2 + |h_{1e}h_{2o}g_{1o}g_{2e}-h_{1o}h_{2e}g_{1e}g_{2o}|^2P_1P_2\Bigg) - \log\left(1+\left(|g_{1o}g_{2o}|^2+|g_{1e}g_{2e}|^2\right)(P_1+P_2)\right)\Bigg\} \tag{30}$$

where $\mathbf{h} = [h_{1o} \ h_{1e} \ h_{2o} \ h_{2e}]^T$, $\mathbf{g} = [g_{1o} \ g_{1e} \ g_{2o} \ g_{2e}]^T$, and P_1, P_2, which are functions of $\mathbf{h}_o = [h_{1o} \ h_{2o}]^T$ and $\mathbf{g}_o = [g_{1o} \ g_{2o}]^T$, are the power allocation policies of users 1 and 2, respectively, that satisfy

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

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

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

VI. Degrees of Freedom

In this section, we show that the secrecy sum rate achieved by our scheme scales with SNR as $1/2\log(SNR)$ and that the secrecy sum rate achieved by the cooperative jamming scheme given in [13] does not scale with SNR. What we give here are rigorous proofs for intuitive results. Since by looking at (30), 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[1], 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 $1/2\log(P)$. In the same way, by considering the secrecy sum rate achieved by the cooperative jamming scheme given in (23), then by referring to the power allocation policies given in [13], one can also roughly claim that for all channel states, as the available average power goes to infinity, the overall expression converges to a constant.

We start by the DoF analysis of our scheme. For simplicity, we assume that $\bar{P}_1 = \bar{P}_2 = P$. We make the following choices

[1]There will be channel states where the difference inside the expectation in (30) will be negative. These can be handled by expressing this expectation as a nested expectation (see (64)) and by shutting down the transmit power at channel states where the inner expectation is negative.

for the power allocation policies P_1 and P_2. 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) and (32). Hence, the secrecy sum rate achieved using our scheme can be written as

$$R_s = \frac{1}{2}E_{\mathbf{h},\mathbf{g}}\Big\{ \log\left(1 + u_1(\mathbf{h},\mathbf{g})P + u_2(\mathbf{h},\mathbf{g})P^2\right) - \log\left(1 + u_3(\mathbf{g})P\right)\Big\} \tag{33}$$

where

$$u_1(\mathbf{h},\mathbf{g}) = \frac{1}{2\sigma_{g_2}^2}(|h_{1o}g_{2o}|^2 + |h_{1e}g_{2e}|^2) + \frac{1}{2\sigma_{g_1}^2}(|h_{2o}g_{1o}|^2 + |h_{2e}g_{1e}|^2) \tag{34}$$

$$u_2(\mathbf{h},\mathbf{g}) = \frac{1}{4\sigma_{g_1}^2\sigma_{g_2}^2}|h_{1e}h_{2o}g_{1o}g_{2e} - h_{1o}h_{2e}g_{1e}g_{2o}|^2 \tag{35}$$

$$u_3(\mathbf{g}) = \frac{\sigma_{g_1}^2 + \sigma_{g_2}^2}{2\sigma_{g_1}^2\sigma_{g_2}^2}(|g_{1o}g_{2o}|^2 + |g_{1e}g_{2e}|^2) \tag{36}$$

The achievable total number of secure DoF, η, is defined as

$$\eta \triangleq \lim_{P\to\infty}\frac{R_s}{\log(P)} \tag{37}$$

We assume that all channel gains are drawn from continuous bounded distributions. We also assume that all channel gains have finite variances. Now, we show that, for the two-user fading MAC-WT, a total number of secure DoF of $\eta = 1/2$ is achievable.

Towards this end, it suffices to show that the order of the limit and the expectation can be reversed. To do this, we make use of Lebesgue dominated convergence theorem. First, we define

$$f_P(\mathbf{h},\mathbf{g}) = \frac{1}{\log(P)}\Big[\log\left(1 + u_1(\mathbf{h},\mathbf{g})P + u_2(\mathbf{h},\mathbf{g})P^2\right) - \log\left(1 + u_3(\mathbf{g})P\right)\Big] \tag{38}$$

Hence, the total achievable secure DoF is given by

$$\eta = \frac{1}{2}\lim_{P\to\infty} E_{\mathbf{h},\mathbf{g}}[f_P(\mathbf{h},\mathbf{g})] \tag{39}$$

Now, we claim that for $P \geq 2$, $|f_P(\mathbf{h},\mathbf{g})|$ is upper bounded by $\psi(\mathbf{h},\mathbf{g})$ where

$$\psi(\mathbf{h},\mathbf{g}) = 4 + 2\left(\log(1+\frac{1}{\sigma_{g_1}^2}) + \log(1+\frac{1}{\sigma_{g_2}^2})\right) + \log\left(1 + \frac{\sigma_{g_1}^2+\sigma_{g_2}^2}{\sigma_{g_1}^2\sigma_{g_2}^2}\right) + 3\left(\sum_{k=1}^{2}\log(1+|h_{ko}|^2) + \sum_{k=1}^{2}\log(1+|h_{ke}|^2)\right) + 4\left(\sum_{k=1}^{2}\log(1+|g_{ko}|^2) + \sum_{k=1}^{2}\log(1+|g_{ke}|^2)\right) \tag{40}$$

Assuming that this claim is true, using the fact that all channel gains have finite variances together with Jensen's inequality, we have

$$E_{\mathbf{h},\mathbf{g}}[\psi(\mathbf{h},\mathbf{g})] < \infty \tag{41}$$

Thus, by the dominated convergence theorem, we have

$$\lim_{P\to\infty} E_{\mathbf{h},\mathbf{g}}[f_P(\mathbf{h},\mathbf{g})] = E_{\mathbf{h},\mathbf{g}}[\lim_{P\to\infty} f_P(\mathbf{h},\mathbf{g})] = 1 \tag{42}$$

Hence, $\eta = 1/2$.

Thus, it remains to prove that the claim is true. To do this, observe, for $P \geq 2$, we have

$$\begin{aligned}
&|f_P(\mathbf{h},\mathbf{g})| \\
&\leq \frac{1}{\log(P)}\Bigg[\log\Big(1 + \frac{1}{\sigma_{g_2}^2}\left(|h_{1o}g_{2o}|^2 + |h_{1e}g_{2e}|^2\right)P \\
&\quad + \frac{1}{\sigma_{g_1}^2}\left(|h_{2o}g_{1o}|^2 + |h_{2e}g_{1e}|^2\right)P \\
&\quad + \frac{1}{\sigma_{g_1}^2\sigma_{g_2}^2}\left(|h_{1e}h_{2o}g_{1o}g_{2e}|^2 + |h_{1o}h_{2e}g_{1e}g_{2o}|^2\right)P^2 \\
&\quad + \frac{1}{\sigma_{g_1}^2\sigma_{g_2}^2}|h_{1o}h_{2o}h_{1e}h_{2e}g_{1o}g_{2o}g_{1e}g_{2e}|P^2\Big) \\
&\quad + \log\left(1 + \frac{\sigma_{g_1}^2+\sigma_{g_2}^2}{\sigma_{g_1}^2\sigma_{g_2}^2}\left(|g_{1o}g_{2o}|^2 + |g_{1e}g_{2e}|^2\right)P\right)\Bigg] \qquad (43)\\
&\leq \frac{1}{\log(P)}\Bigg[3\log(P) \\
&\quad + \log\Big(1 + \frac{1}{\sigma_{g_2}^2}\left(|h_{1o}g_{2o}|^2 + |h_{1e}g_{2e}|^2\right) \\
&\quad + \frac{1}{\sigma_{g_1}^2}\left(|h_{2o}g_{1o}|^2 + |h_{2e}g_{1e}|^2\right) \\
&\quad + \frac{1}{\sigma_{g_1}^2\sigma_{g_2}^2}\left(|h_{1e}h_{2o}g_{1o}g_{2e}|^2 + |h_{1o}h_{2e}g_{1e}g_{2o}|^2\right) \\
&\quad + \frac{1}{\sigma_{g_1}^2\sigma_{g_2}^2}\left(|h_{1o}h_{2o}h_{1e}h_{2e}g_{1o}g_{2o}g_{1e}g_{2e}|\right)\Big) \\
&\quad + \log\left(1 + \frac{\sigma_{g_1}^2+\sigma_{g_2}^2}{\sigma_{g_1}^2\sigma_{g_2}^2}\left(|g_{1o}g_{2o}|^2 + |g_{1e}g_{2e}|^2\right)\right)\Bigg] \qquad (44)\\
&\leq 3 + 2\left(\log\left(1+\frac{1}{\sigma_{g_1}^2}\right) + \log\left(1+\frac{1}{\sigma_{g_2}^2}\right)\right) \\
&\quad + \log\left(1 + \frac{\sigma_{g_1}^2+\sigma_{g_2}^2}{\sigma_{g_1}^2\sigma_{g_2}^2}\right) \\
&\quad + \log\left(1 + |h_{1o}g_{2o}|^2 + |h_{1e}g_{2e}|^2\right) \\
&\quad + \log\left(1 + |h_{2o}g_{1o}|^2 + |h_{2e}g_{1e}|^2\right) \\
&\quad + \log\left(1 + |h_{1e}h_{2o}g_{1o}g_{2e}|^2 + |h_{1o}h_{2e}g_{1e}g_{2o}|^2\right) \\
&\quad + \log\left(1 + |h_{1o}h_{2o}h_{1e}h_{2e}g_{1o}g_{2o}g_{1e}g_{2e}|\right) \qquad (45)
\end{aligned}$$

where (43) follows from the triangle inequality, (44) follows from the fact that $\log(1 + xP) \leq \log(P) + \log(1 + x)$ if $P \geq 1$, (45) follows from the fact that $\log(1 + x + y) \leq \log(1 + x) + \log(1 + y)$ and

$\log(1+xy) \leq \log(1+x)+\log(1+y)$ if x and y are non-negative and the fact that $\log(P) \geq 1$ if $P \geq 2$. Continuing from (45), we develop the following upper bound on $|f_P(\mathbf{h},\mathbf{g})|$, where we obtain a square for the term in the last logarithm,

$$\begin{aligned}
&\leq 4 + 2\left(\log\left(1+\frac{1}{\sigma_{g_1}^2}\right)+\log\left(1+\frac{1}{\sigma_{g_2}^2}\right)\right) \\
&\quad + \log\left(1+\frac{\sigma_{g_1}^2+\sigma_{g_2}^2}{\sigma_{g_1}^2\sigma_{g_2}^2}\right) \\
&\quad + \log\left(1+|h_{1o}g_{2o}|^2+|h_{1e}g_{2e}|^2\right) \\
&\quad + \log\left(1+|h_{2o}g_{1o}|^2+|h_{2e}g_{1e}|^2\right)\big) \\
&\quad + \log\left(1+|h_{1e}h_{2o}g_{1o}g_{2e}|^2+|h_{1o}h_{2e}g_{1e}g_{2o}|^2\right) \\
&\quad + \log\left(1+|h_{1o}h_{2o}h_{1e}h_{2e}g_{1o}g_{2o}g_{1e}g_{2e}|^2\right) \qquad (46) \\
&\leq \psi(\mathbf{h},\mathbf{g}) \qquad (47)
\end{aligned}$$

where (46) follows from the fact that $\log(1+x) \leq 1+\log(1+x^2)$ if x is non-negative, and finally (47) follows again from the fact that $\log(1+x+y) \leq \log(1+x)+\log(1+y)$ and $\log(1+xy) \leq \log(1+x)+\log(1+y)$ if x and y are non-negative.

Next, we consider the secrecy sum rate achieved by Gaussian signaling with cooperative jamming [13] in the fading MAC-WT and show that such achievable rate does not scale with SNR. In other words, we show that the total number of secure DoF achieved is zero. We start with the secrecy sum rate given by the right hand side of (23). For simplicity, we assume symmetric average power constraints in (24), i.e., $E[P_1+Q_1] \leq P$ and $E[P_2+Q_2] \leq P$. According to the optimal power allocation policy described in [13], 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 optimal power allocation after eliminating the case of $|h_1| \leq |g_1|$ and $|h_2| \leq |g_2|$ when no transmission is possible.

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

$$R_s(\mathbf{h},\mathbf{g}) = \log\left(\frac{1+|h_1|^2P_1+|h_2|^2P_2}{1+|g_1|^2P_1+|g_2|^2P_2}\right) \qquad (48)$$

Hence, using the fact that

$$\frac{x+y}{z+t} \leq \frac{x}{z}+\frac{y}{t} \quad \text{if } x,y,z,t>0 \qquad (49)$$

we can give the following upper bound for $R_s(\mathbf{h},\mathbf{g})$:

$$\begin{aligned}
R_s(\mathbf{h},\mathbf{g}) &\leq \log\left(1+\frac{|h_1|^2}{|g_1|^2}+\frac{|h_2|^2}{|g_2|^2}\right) \qquad (50) \\
&\leq \log\left(1+\frac{|h_1|^2}{|g_1|^2}\right)+\log\left(1+\frac{|h_2|^2}{|g_2|^2}\right) \qquad (51)
\end{aligned}$$

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

$$\begin{aligned}
R_s(\mathbf{h},\mathbf{g}) &= \log\left(\frac{1+|h_1|^2P_1+|h_2|^2Q_2}{1+|g_1|^2P_1+|g_2|^2Q_2}\right) \\
&\quad + \log\left(\frac{1+|g_2|^2Q_2}{1+|h_2|^2Q_2}\right) \qquad (52)
\end{aligned}$$

Hence, using (49), $R_s(\mathbf{h},\mathbf{g})$ can be upper bounded as

$$R_s(\mathbf{h},\mathbf{g}) \leq 1+\log\left(1+\frac{|h_1|^2}{|g_1|^2}\right)+\log\left(1+\frac{|g_2|^2}{|h_2|^2}\right) \qquad (53)$$

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

$$\begin{aligned}
R_s(\mathbf{h},\mathbf{g}) &= \log\left(\frac{1+|h_1|^2Q_1+|h_2|^2P_2}{1+|g_1|^2Q_1+|g_2|^2P_2}\right) \\
&\quad + \log\left(\frac{1+|g_1|^2Q_1}{1+|h_1|^2Q_1}\right) \qquad (54)
\end{aligned}$$

As in the previous case, $R_s(\mathbf{h},\mathbf{g})$ can be upper bounded as

$$R_s(\mathbf{h},\mathbf{g}) \leq 1+\log\left(1+\frac{|h_2|^2}{|g_2|^2}\right)+\log\left(1+\frac{|g_1|^2}{|h_1|^2}\right) \qquad (55)$$

Now, since the instantaneous sum rate is zero outside $\mathcal{D}_1 \cup \mathcal{D}_2 \cup \mathcal{D}_3$, then from (51), (53), and (55), the ergodic secrecy sum rate, R_s, can be upper bounded as follows

$$\begin{aligned}
R_s \leq &\int_{\mathcal{D}_1}\left(\log\left(1+\frac{|h_1|^2}{|g_1|^2}\right)+\log\left(1+\frac{|h_2|^2}{|g_2|^2}\right)\right)d\mathbf{F} \\
&+\int_{\mathcal{D}_2}\left(1+\log\left(1+\frac{|h_1|^2}{|g_1|^2}\right)+\log\left(1+\frac{|g_2|^2}{|h_2|^2}\right)\right)d\mathbf{F} \\
&+\int_{\mathcal{D}_3}\left(1+\log\left(1+\frac{|h_2|^2}{|g_2|^2}\right)+\log\left(1+\frac{|g_1|^2}{|h_1|^2}\right)\right)d\mathbf{F} \qquad (56)
\end{aligned}$$

where

$$d\mathbf{F} = \prod_{k=1}^{2} f(|h_k|^2)f(|g_k|^2)d|h_k|^2d|g_k|^2 \qquad (57)$$

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 above expression is finite. Hence, we have $R_s < \infty$, and that R_s is bounded from above by a constant. Thus, from the definition of the achievable secure DoF, η, we have

$$\eta = \lim_{P\to\infty}\frac{R_s}{\log(P)} = 0 \qquad (58)$$

So far, we have proposed a scaling based alignment scheme, and showed that it scales with SNR and achieves a total secure DoF of $1/2$. A direct consequence of this result is the sub-optimality of Gaussian signaling (with or without cooperative jamming) in the fading MAC-WT. After we have devised this

achievable scheme, the ergodic interference alignment scheme of Nazer *et. al.* [14] inspired us to propose an improved achievable scheme. In the next section, we briefly discuss this scheme which we call *ergodic secret alignment*. The new ingredient in this scheme is to perform repetition coding at *carefully chosen* time instances as opposed to two *consecutive* time instances as we have done in Section III. A detailed derivation and analysis of this scheme can be found in [15].

VII. Ergodic Secret Alignment

In the scaling based alignment scheme in Section III, 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 fact, we can show that [15], 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 $[g_1 \ g_2]^T$. 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. On the other hand, this choice makes the vector MAC between the two transmitters and the eavesdropper equivalent to a single scalar MAC. Using this technique, we obtain another achievable secrecy rate region for the fading MAC-WT which is given by the following theorem [15].

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

$$R_1 \leq \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \Big\{ \log\left(1 + 2|h_1|^2 P_1\right) - \log\left(1 + \frac{2|g_1|^2 P_1}{1 + 2|g_2|^2 P_2}\right) \Big\} \tag{59}$$

$$R_2 \leq \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \Big\{ \log\left(1 + 2|h_2|^2 P_2\right) - \log\left(1 + \frac{2|g_2|^2 P_2}{1 + 2|g_1|^2 P_1}\right) \Big\} \tag{60}$$

$$R_1 + R_2 \leq \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \Big\{ \log\left(1 + 2|h_1|^2 P_1\right) + \log\left(1 + 2|h_2|^2 P_2\right) - \log\left(1 + 2(|g_1|^2 P_1 + |g_2|^2 P_2)\right) \Big\} \tag{61}$$

where $\mathbf{h} = [h_1 \ h_2]^T$, $\mathbf{g} = [g_1 \ g_2]^T$, and P_1 and P_2, which are functions of $\mathbf{h}$ and $\mathbf{g}$, are the power allocation policies of users 1 and 2, respectively, that satisfy

$$E[P_1] \leq \bar{P}_1 \tag{62}$$

$$E[P_2] \leq \bar{P}_2 \tag{63}$$

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

Clearly, the achievable sum secrecy rate given above scales with the SNR as $1/2\log(SNR)$. This can be shown by following the same lines of the derivation in the previous section. Moreover, the average power constraints in the above theorem are indeed easier to handle than those in (31)-(32). In [15], we derive the optimum power allocations for maximizing the secrecy sum rate given in Theorem 2.

VIII. Numerical Results

In this section, we verify by simulation that the secrecy sum rate achieved by the scaling based alignment (SBA) scheme given in Section III and the ergodic secret alignment (ESA) scheme given in Section VII scale with SNR, while the secrecy sum rate achieved by the Gaussian signaling with cooperative jamming (GS/CJ) scheme given in [13] does not scale with SNR. We also verify that the secrecy sum rate achievable by the ESA scheme is greater than the one achievable by the SBA scheme for all SNR values.

In our 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

$$R_s = \frac{1}{2} E_{\mathbf{h}_o,\mathbf{g}_o} \Bigg\{ E_{\mathbf{h}_e,\mathbf{g}_e} \Bigg[\log\Bigg(1 + \left(|h_{1o}g_{2o}|^2 + |h_{1e}g_{2e}|^2\right) P_1 + \left(|h_{2o}g_{1o}|^2 + |h_{2e}g_{1e}|^2\right) P_2 + |h_{1e}h_{2o}g_{1o}g_{2e} - h_{1o}h_{2e}g_{1e}g_{2o}|^2 P_1 P_2 \Bigg) - \log\left(1 + \left(|g_{1o}g_{2o}|^2 + |g_{1e}g_{2e}|^2\right)(P_1 + P_2)\right) \Bigg] \Bigg\} \tag{64}$$

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 $\mathbf{g}_o$. Secondly, 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 (61), that the achievable secrecy sum rate is

$$R_s = \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \Big\{ \log\left(1 + 2|h_1|^2 P_1\right) + \log\left(1 + 2|h_2|^2 P_2\right) - \log\left(1 + 2(|g_1|^2 P_1 + |g_2|^2 P_2)\right) \Big\} \tag{65}$$

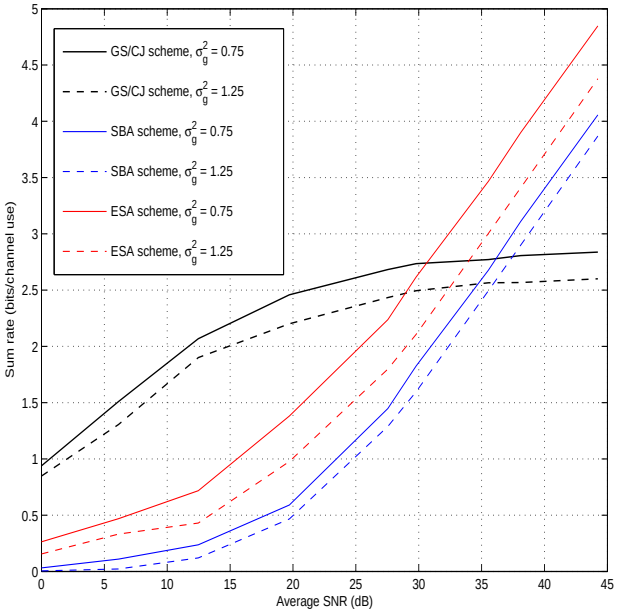

Fig. 1. Achievable secrecy sum rates of the Gaussian signaling with cooperative jamming scheme (GS/CJ scheme), the scaling based alignment scheme (SBA scheme) and the ergodic secret alignment scheme (ESA scheme) as function of the SNR for two different values of mean eavesdropper channel gain, σ_g^2.

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 optimal power allocation scheme described in [13].

In Figure 1, the secrecy sum rate of each of the three schemes is plotted versus the average SNR which is defined 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 be their common value.

IX. Conclusions

In this paper, we proposed two new achievable schemes for the fading multiple access wiretap channel. Our first scheme, the scaling based alignment (SBA) scheme, lets the interfering signals at the main receiver live in a two-dimensional space, while it aligns the interfering signals at the eavesdropper in a one-dimensional space. We obtained the secrecy rate region achieved by this scheme. These secrecy rates scale with SNR. In particular, we showed that the secrecy sum rate achieved by this scheme scales with SNR as $1/2\log(SNR)$, i.e., a total of $1/2$ secure DoF is achievable with this scheme in the two-user fading MAC-WT. We also showed that the secrecy sum rate achieved by the Gaussian signaling with cooperative jamming scheme does not scale with SNR, i.e., achievable secure DoF is zero. As a direct consequence, we showed the sub-optimality of Gaussian signaling (with or without cooperative jamming) in the fading MAC-WT.

Our second scheme, the ergodic secret alignment (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 gave the secrecy rate region achieved by this scheme and showed that, as in the scaling based alignment scheme, the secrecy sum rate achieved by the ergodic secret alignment scheme scales with SNR as $1/2\log(SNR)$.

Finally, we presented simulation results for the secrecy sum rates achieved by our proposed schemes and by the Gaussian signaling with cooperative jamming scheme. The simulation results illustrated that our schemes yield secrecy sum rates that scale with SNR, while the secrecy sum rate achieved by cooperative jamming does not scale with SNR. We note that the secrecy rates achievable by our schemes can be further improved by appropriate power control. While the rate expressions achieved with the scaling based alignment scheme seem complicated, the rate expressions achieved with the ergodic secret alignment scheme are more amenable for optimization of power allocations. We optimize the powers with respect to channel states in [15].

References

[1] C. E. Shannon. Communication theory of secrecy systems. *Bell Systems Technical Journal, vol. 28, pp. 656-715.*, 1949.

[2] A. D. Wyner. The wire-tap channel. *Bell Systems Technical Journal, vol. 54, no. 8, pp. 1355-1387*, January 1975.

[3] I. Csiszar and J. Korner. Broadcast channels with confidential messages. *IEEE Trans. on Inf. Theory, 24(3), pp. 339- 348*, May 1978.

[4] S. Leung-Yan-Cheong and M. E. Hellman. The gaussian wire-tap channel. *IEEE Trans. on Inf. Theory, 24(4), pp. 451-456*, July 1978.

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

[6] 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), pp. 2735-2751*, June 2008.

[7] 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. To appear.

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

[9] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor. Interference alignment for secrecy. *Submitted to IEEE Trans. on Inf. Theory*, October 2008.

[10] T. Gou and S. A. Jafar. On the secure degrees of freedom of wireless X networks. *In 46th Annual Allerton Conference on Communication, Control and Computing, UIUC, IL, pp. 826-833*, September 2008.

[11] X. He and A. Yener. Secure degrees of freedom for Gaussian channels with interference: Structured codes outperform Gaussian signaling. *In IEEE Globecom 2009*. Also available at [arXiv:0905.2638].

[12] X. He and A. Yener. K-user interference channels: Achievable secrecy rate and degrees of freedom. *In IEEE ITW'09, Volos*, June 2009.

[13] E. Tekin and A. Yener. Secrecy sum-rates for the multiple-access wire-tap channel with ergodic block fading. *In 45th Annual Allerton Conference, UIUC, IL, pp. 856-863*, September 2007.

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

[15] R. Bassily and S. Ulukus. Ergodic secret alignment. To be submitted.