Secure Degrees of Freedom of the Gaussian Multiple Access Wiretap Channel

Jianwei Xie Sennur Ulukus
Department of Electrical and Computer Engineering
University of Maryland, College Park, MD 20742
xiejw@umd.edu *ulukus@umd.edu*

***Abstract*—We show that the sum secure degrees of freedom (d.o.f.) of the K-user Gaussian multiple access (MAC) wiretap channel is $\frac{K(K-1)}{K(K-1)+1}$. Our achievability is based on real interference alignment and structured cooperative jamming. Each user divides its message into $K-1$ sub-messages, and sends a linear combination of signals carrying these sub-messages together with a structured cooperative jamming signal. All cooperative jamming signals are aligned in a single dimension at the legitimate receiver allowing for reliable decoding of the message carrying signals by the legitimate receiver. Each cooperative jamming signal is aligned with $K-1$ message signals at the eavesdropper limiting the information leakage rate to the eavesdropper. We provide a matching converse establishing the *exact* sum secure d.o.f. of the Gaussian MAC wiretap channel as $\frac{K(K-1)}{K(K-1)+1}$.**

I. Introduction

Security of communication was first considered by Shannon in [1], where a legitimate pair wishes to have secure communication in the presence of an eavesdropper over a noiseless channel, leading to the necessity of secure keys and the one-time-pad encryption method, in that model. Wyner introduced the noisy wiretap channel, and demonstrated that secure communication can be attained by stochastic encoding without using any keys, if the eavesdropper is degraded with respect to the legitimate receiver [2]. Csiszar and Korner generalized his result to arbitrary, not necessarily degraded, wiretap channels, and showed that secure communication is still possible, even when the eavesdropper is not degraded [3]. Csiszar and Korner introduced channel prefixing and rate splitting into the achievable scheme in addition to Wyner's stochastic encoding. Leung-Yan-Cheong and Hellman obtained the capacity-equivocation region of the Gaussian wiretap channel [4], which is degraded. They showed that a Gaussian input signal is optimum, and in particular, secrecy capacity equals the difference of the capacities of the legitimate and eavesdropping links in this case. This line of research has been subsequently extended to many multi-user settings. In this paper, we focus on the multiple access (MAC) wiretap channel.

The Gaussian MAC wiretap channel, where multiple legitimate users wish to have secure communication with a single legitimate receiver over a Gaussian MAC in the presence of an eavesdropper (see Fig. 1), was introduced in [5], and further studied in [6]–[13]. Reference [5] extended Wyner's stochastic encoding to a degraded Gaussian MAC wiretap channel,

This work was supported by NSF Grants CNS 09-64632, CCF 09-64645, CCF 10-18185 and CNS 11-47811.

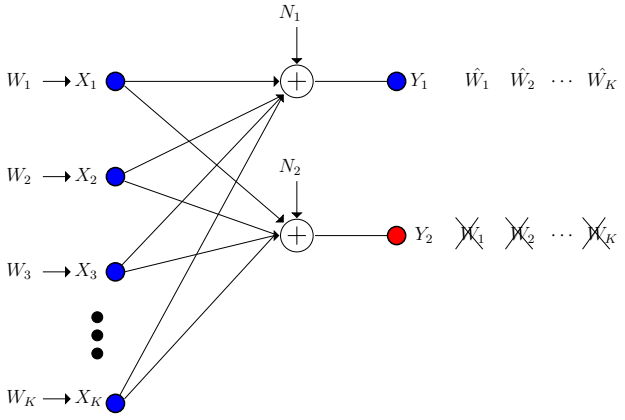

Fig. 1. K-user multiple access wiretap channel.

and reported achievable secrecy rates with Gaussian channel inputs. Reference [6] proposed the technique of cooperative jamming where some of the users cease message transmission, and transmit independent and identically distributed (i.i.d.) Gaussian noise to improve the sum secrecy rate. Cooperative jamming can further be interpreted as a form of channel prefixing, in which the channel input is a random function of the message carrying signal [10], [13], where at one extreme, the channel input does not carry any information signal as in [6]. Reference [9] showed that for certain weak-eavesdropper Gaussian MAC wiretap channels, achievable schemes based on Gaussian signalling with no channel prefixing can get within 0.5 bits of the secrecy capacity region. The secrecy capacity region of the Gaussian MAC wiretap channel is still unknown. In the absence of an exact secrecy capacity region, [11]–[13] studied the secure degrees of freedom (d.o.f.) of the MAC wiretap channel.

For the K-user Gaussian MAC wiretap channel, the best known achievable sum secure d.o.f is $\frac{K-1}{K}$ [12] which gives $\frac{1}{2}$ for $K=2$. Since the individual secrecy rate is a lower bound for the sum secrecy rate, the individual secure d.o.f. capacity result of $\frac{K-1}{K}$ in [14] for the wiretap channel with helpers can be interpreted as an achievable sum secure d.o.f. for the MAC wiretap channel. In addition, for $K=2$, the individual secure d.o.f. of $\frac{1}{2}$ achieved in [11], [15] for a wiretap channel with a helper (for the class of algebraic irrational channel gains) can also be understood as an achievable sum secure d.o.f. for the two-user MAC wiretap channel. These results can be summarized as follows: References [11], [14], [15]

achieve positive secure d.o.f. via cooperative jamming, i.e., forcing all but one user transmit cooperative jamming signals to confuse the eavesdropper. It is known that i.i.d. Gaussian cooperative jamming signals result in zero secure d.o.f. for the MAC wiretap channel [13]; and [11], [14], [15] achieved positive secure d.o.f. by using structured cooperative jamming. While i.i.d. Gaussian cooperative jamming signals maximally jam the eavesdropper, they also maximally hurt the legitimate receiver's decoding capability. Structured cooperative jamming signals in [11], [14], [15] strike a better balance between these two end-effects, i.e., by hurting the eavesdropper sufficiently, and not hurting the legitimate receiver as much. In addition, [12] achieved positive sum secure d.o.f. without using any cooperative jamming signals, but by using structured message signals from all legitimate transmitters, and by aligning them carefully at the legitimate receiver and the eavesdropper via real interference alignment [16].

In this paper, we show that the exact sum secure d.o.f. of the K-user Gaussian MAC wiretap channel is $\frac{K(K-1)}{K(K-1)+1}$ which gives $\frac{2}{3}$ for $K=2$. Our achievability is based on real interference alignment and structured cooperative jamming. Each legitimate transmitter divides its message into $K-1$ sub-messages. Each transmitter sends a sum of signals carrying each one of these sub-messages together with a cooperative jamming signal. Both message carrying signals and cooperative jamming signals are structured: they come from the same discrete alphabet. These signals are sent in such a way that all of the cooperative jamming signals are aligned in a single dimension at the legitimate receiver, allowing for the reliable decodability of the message carrying signals. In addition, each one of the cooperative jamming signals is aligned with $K-1$ message carrying signals at the eavesdropper, limiting the information leakage rate to the eavesdropper; that is, each cooperative jamming signal protects $K-1$ sub-messages. This achievable scheme is illustrated in Fig. 2 for $K=3$.

A major difference of our achievable scheme from the existing achievable schemes, that enables us to reach the sum secure d.o.f. capacity, is that each user sends both message carrying signals and a structured cooperative jamming signal. Further, all of the signals are carefully aligned at the two receivers, and the individual powers of the signals are carefully chosen. The addition of a cooperative jamming signal to message carrying signals at each transmitter can be interpreted as channel prefixing. Therefore, our achievable scheme combines: channel prefixing, structured signalling, structured cooperative jamming, and interference alignment. Our converse is a generalization of our converse in [14]. We first show that the sum secrecy rate is upper bounded by the sum of differential entropies of all channel inputs except the one eliminated by the eavesdropper's observation. We next develop a direct relationship between each user's channel input and the sum rate of all users except this user, for the decodability at the legitimate receiver. This gives us a matching converse and establishes the exact sum secure d.o.f. of the K-user Gaussian MAC wiretap channel as $\frac{K(K-1)}{K(K-1)+1}$.

II. System Model, Definitions and the Result

The K-user Gaussian MAC wiretap channel (see Fig. 1) is defined by,

$$Y_1 = \sum_{i=1}^{K} h_i X_i + N_1 \tag{1}$$

$$Y_2 = \sum_{i=1}^{K} g_i X_i + N_2 \tag{2}$$

where h_i and g_i are the channel gains of user i to the legitimate receiver and the eavesdropper, respectively, and N_1 and N_2 are independent Gaussian random variables with zero-mean and unit-variance. Each transmitter i has a message W_i intended for the legitimate receiver, whose channel output is Y_1. For each i, message W_i is uniformly and independently chosen from set $\mathcal{W}_i$. The rate of message i is $R_i \triangleq \frac{1}{n}\log|\mathcal{W}_i|$. Transmitter i uses a stochastic function $f_i : \mathcal{W}_i \to \mathbf{X}_i$ where the n-length vector $\mathbf{X}_i \triangleq X_i^n$ denotes the ith user's channel input in n channel uses. All messages are needed to be kept secret from the eavesdropper, whose channel output is Y_2.

A secrecy rate tuple $(R_1, R_2, \ldots, R_K)$ is said to be achievable if for any $\epsilon > 0$ there exist n-length codes such that the legitimate receiver can decode the messages reliably, i.e., the probability of decoding error is less than ϵ

$$\Pr\left[(W_1,\ldots,W_K) \neq (\hat{W}_1,\ldots,\hat{W}_K)\right] \leq \epsilon \tag{3}$$

and the messages are kept information-theoretically secure against the eavesdropper

$$\frac{1}{n}H(W_1, W_2, \ldots, W_K|\mathbf{Y}_2) \geq \frac{1}{n}H(W_1, W_2, \ldots, W_K) - \epsilon \tag{4}$$

where $\hat{W}_1, \ldots, \hat{W}_K$ are the estimates of the messages based on observation $\mathbf{Y}_1$, where $\mathbf{Y}_1 \triangleq Y_1^n$ and $\mathbf{Y}_2 \triangleq Y_2^n$. This definition implies the secrecy for any subset of the messages, including individual messages, i.e., for any $\mathbf{S} \subset \{1,\ldots,K\}$:

$$\begin{aligned}
\frac{1}{n}H(W_{\mathbf{S}}|\mathbf{Y}_2) &= \frac{1}{n}H(W_{\mathbf{S}}, W_{\mathbf{S}^c}|\mathbf{Y}_2) - \frac{1}{n}H(W_{\mathbf{S}^c}|\mathbf{Y}_2, W_{\mathbf{S}}) \\
&\geq \frac{1}{n}H(W_{\mathbf{S}}, W_{\mathbf{S}^c}|\mathbf{Y}_2) - \frac{1}{n}H(W_{\mathbf{S}^c}|W_{\mathbf{S}}) \\
&\geq \frac{1}{n}H(W_{\mathbf{S}}, W_{\mathbf{S}^c}) - \epsilon - \frac{1}{n}H(W_{\mathbf{S}^c}|W_{\mathbf{S}}) \\
&\geq \frac{1}{n}H(W_{\mathbf{S}}) - \epsilon
\end{aligned} \tag{5}$$

The sum secure d.o.f. is defined as

$$D_{s,\Sigma} \triangleq \lim_{P\to\infty} \sup \frac{\sum_{i=1}^{K} R_i}{\frac{1}{2}\log P} \tag{6}$$

where the supremum is over all achievable secrecy rate tuples $(R_1,\ldots,R_K)$. The main result of this paper is stated in the following theorem.

Theorem 1 *The sum secure d.o.f. of the K-user Gaussian MAC wiretap channel is $\frac{K(K-1)}{K(K-1)+1}$ for almost all channel gains.*

III. Converse

We start with the sum rate:

$$
\begin{aligned}
n\sum_{i=1}^{K} R_i &= \sum_{i=1}^{K} H(W_i) = H(W_1^K) && (7)\\
&\le I(W_1^K;\mathbf{Y}_1) - I(W_1^K;\mathbf{Y}_2) + nc_1 && (8)\\
&\le I(W_1^K;\mathbf{Y}_1,\mathbf{Y}_2) - I(W_1^K;\mathbf{Y}_2) + nc_1 && (9)\\
&= I(W_1^K;\mathbf{Y}_1|\mathbf{Y}_2) + nc_1 && (10)\\
&\le I(\mathbf{X}_1^K;\mathbf{Y}_1|\mathbf{Y}_2) + nc_1 && (11)\\
&= h(\mathbf{Y}_1|\mathbf{Y}_2) - h(\mathbf{Y}_1|\mathbf{Y}_2,\mathbf{X}_1^K) + nc_1 && (12)\\
&= h(\mathbf{Y}_1|\mathbf{Y}_2) - h(\mathbf{N}_1|\mathbf{Y}_2,\mathbf{X}_1^K) + nc_1 && (13)\\
&\le h(\mathbf{Y}_1|\mathbf{Y}_2) + nc_2 && (14)\\
&= h(\mathbf{Y}_1,\mathbf{Y}_2) - h(\mathbf{Y}_2) + nc_2 && (15)\\
&= h(\tilde{\mathbf{X}}_1,\tilde{\mathbf{X}}_2,\ldots,\tilde{\mathbf{X}}_K,\mathbf{Y}_1,\mathbf{Y}_2)\\
&\quad - h(\tilde{\mathbf{X}}_1,\tilde{\mathbf{X}}_2,\ldots,\tilde{\mathbf{X}}_K|\mathbf{Y}_1,\mathbf{Y}_2)\\
&\quad - h(\mathbf{Y}_2) + nc_2 && (16)
\end{aligned}
$$

where $W_1^K \triangleq \{W_1,\ldots,W_K\}$ and $\mathbf{X}_1^K \triangleq \{\mathbf{X}_1,\ldots,\mathbf{X}_K\}$. All $\{c_i : i \ge 0\}$ in this paper are constants independent of P.

In (16), we introduce random vectors $\tilde{\mathbf{X}}_j = \mathbf{X}_j + \tilde{\mathbf{N}}_j$, for $j = 1,\ldots,K$, where $\tilde{\mathbf{N}}_j$ is an i.i.d. sequence of Gaussian random variable $\tilde{N}_j$ which is zero-mean and of variance $\sigma_j^2 < \min(1/h_j^2, 1/g_j^2)$. All $\{\tilde{N}_j\}_{j=1}^K$ are mutually independent, and are independent of all other random variables. Essentially, $\tilde{\mathbf{X}}_j$ is a slightly noised version of the channel input $\mathbf{X}_j$. Let us also define $\tilde{\mathbf{X}}_1^K \triangleq \{\tilde{\mathbf{X}}_1,\ldots,\tilde{\mathbf{X}}_K\}$ and $\tilde{\mathbf{N}}_1^K \triangleq \{\tilde{\mathbf{N}}_1,\ldots,\tilde{\mathbf{N}}_K\}$ for convenience. Continuing from (16), we have

$$
\begin{aligned}
n\sum_{i=1}^{K} R_i &\le h(\tilde{\mathbf{X}}_1^K,\mathbf{Y}_1,\mathbf{Y}_2) - h(\tilde{\mathbf{X}}_1^K|\mathbf{Y}_1,\mathbf{Y}_2)\\
&\quad - h(\mathbf{Y}_2) + nc_2 && (17)\\
&\le h(\tilde{\mathbf{X}}_1^K,\mathbf{Y}_1,\mathbf{Y}_2) - h(\tilde{\mathbf{X}}_1^K|\mathbf{Y}_1,\mathbf{Y}_2,\mathbf{X}_1^K)\\
&\quad - h(\mathbf{Y}_2) + nc_2 && (18)\\
&= h(\tilde{\mathbf{X}}_1^K,\mathbf{Y}_1,\mathbf{Y}_2) - h(\tilde{\mathbf{N}}_1^K|\mathbf{Y}_1,\mathbf{Y}_2,\mathbf{X}_1^K)\\
&\quad - h(\mathbf{Y}_2) + nc_2 && (19)\\
&\le h(\tilde{\mathbf{X}}_1^K,\mathbf{Y}_1,\mathbf{Y}_2) - h(\mathbf{Y}_2) + nc_3 && (20)\\
&= h(\tilde{\mathbf{X}}_1^K) + h(\mathbf{Y}_1,\mathbf{Y}_2|\tilde{\mathbf{X}}_1^K) - h(\mathbf{Y}_2) + nc_3 && (21)\\
&\le h(\tilde{\mathbf{X}}_1^K) - h(\mathbf{Y}_2) + nc_4 && (22)\\
&= \sum_{j=1}^{K} h(\tilde{\mathbf{X}}_j) - h(\mathbf{Y}_2) + nc_5 && (23)\\
&\le \sum_{j=2}^{K} h(\tilde{\mathbf{X}}_j) + nc_6 && (24)
\end{aligned}
$$

where (22) is due to $h(\mathbf{Y}_1,\mathbf{Y}_2|\tilde{\mathbf{X}}_1^K) \le nc_7$, which will be proved formally in the sequel, and (24) is due to

$$h(\tilde{\mathbf{X}}_1) \le h(g_1\mathbf{X}_1 + \mathbf{N}_2) + nc_8 \le h(\mathbf{Y}_2) + nc_8 \qquad (25)$$

which is due to the differential entropy version of [17, Problem 2.14]. We now show $h(\mathbf{Y}_1,\mathbf{Y}_2|\tilde{\mathbf{X}}_1^K) \le nc_7$ formally. The intuition behind this is that, given all (slightly noisy versions of) the channel inputs, (at high SNR) the channel outputs can be reconstructed. Formally, we have

$$
\begin{aligned}
&h(\mathbf{Y}_1,\mathbf{Y}_2|\tilde{\mathbf{X}}_1^K)\\
&\quad\le h(\mathbf{Y}_1|\tilde{\mathbf{X}}_1^K) + h(\mathbf{Y}_2|\tilde{\mathbf{X}}_1^K) && (26)\\
&\quad= h\left(\sum_{i=1}^{K} h_i(\tilde{\mathbf{X}}_i - \tilde{\mathbf{N}}_i) + \mathbf{N}_1 \middle| \tilde{\mathbf{X}}_1^K\right)\\
&\qquad + h\left(\sum_{i=1}^{K} g_i(\tilde{\mathbf{X}}_i - \tilde{\mathbf{N}}_i) + \mathbf{N}_2 \middle| \tilde{\mathbf{X}}_1^K\right) && (27)\\
&\quad= h\left(-\sum_{i=1}^{K} h_i\tilde{\mathbf{N}}_i + \mathbf{N}_1 \middle| \tilde{\mathbf{X}}_1^K\right)\\
&\qquad + h\left(-\sum_{i=1}^{K} g_i\tilde{\mathbf{N}}_i + \mathbf{N}_2 \middle| \tilde{\mathbf{X}}_1^K\right) && (28)\\
&\quad\le h\left(-\sum_{i=1}^{K} h_i\tilde{\mathbf{N}}_i + \mathbf{N}_1\right) + h\left(-\sum_{i=1}^{K} g_i\tilde{\mathbf{N}}_i + \mathbf{N}_2\right) && (29)\\
&\quad\triangleq nc_7 && (30)
\end{aligned}
$$

On the other hand, similar to [14, Lemma 2], we can develop an upper bound for each $h(\tilde{\mathbf{X}}_j)$ to further upper bound (24)

$$
\begin{aligned}
n\sum_{i\ne j} R_i &= \sum_{i\ne j} H(W_i) = H(W_{\ne j}) && (31)\\
&\le I(W_{\ne j};\mathbf{Y}_1) + nc_9 && (32)\\
&\le I\left(\sum_{i\ne j} h_i\mathbf{X}_i;\mathbf{Y}_1\right) + nc_9 && (33)\\
&= h\left(\mathbf{Y}_1\right) - h\left(\mathbf{Y}_1\middle|\sum_{i\ne j} h_i\mathbf{X}_i\right) + nc_9 && (34)\\
&= h\left(\mathbf{Y}_1\right) - h\left(h_j\mathbf{X}_j + \mathbf{N}_1\right) + nc_9 && (35)\\
&\le h(\mathbf{Y}_1) - h(\tilde{\mathbf{X}}_j) + nc_{10} && (36)
\end{aligned}
$$

where $W_{\ne j} \triangleq \{W_i\}_{i=1}^K \backslash \{W_j\}$ which satisfies the Markov chain $W_{\ne j} \to \mathbf{X}_{\ne j} \to \sum_{i\ne j} h_i\mathbf{X}_i \to \mathbf{Y}_1$. Therefore, for each j, we have

$$h(\tilde{\mathbf{X}}_j) \le h(\mathbf{Y}_1) - n\sum_{i\ne j} R_i + nc_{10} \qquad (37)$$

which is an upper bound on the differential entropy of $\tilde{\mathbf{X}}_j$ for the decodability of $W_{\ne j}$ at the legitimate receiver.

Now, continuing from (24) and incorporating (37), we have

$$
\begin{aligned}
n\sum_{i=1}^{K} R_i &\le \sum_{j=2}^{K} h(\tilde{\mathbf{X}}_j) + nc_6 && (38)\\
&\le \sum_{j=2}^{K}\left(h(\mathbf{Y}_1) - n\sum_{i\ne j} R_i\right) + nc_{11} && (39)
\end{aligned}
$$

which is equivalent to

$$nR_1 + (K-1)\sum_{j=1}^{K} nR_j \leq (K-1)h(\mathbf{Y}_1) + nc_{11} \quad (40)$$

We then apply this upper bounding technique for a different i by eliminating a different $h(\tilde{\mathbf{X}}_i)$ each time in the same way that we have eliminated $h(\tilde{\mathbf{X}}_1)$ in (24) and (25), and obtain K upper bounds in total as:

$$nR_i + (K-1)\sum_{j=1}^{K} nR_j \leq (K-1)h(\mathbf{Y}_1) + nc_{12} \quad (41)$$

for all $i = 1, \ldots, K$. Then, by summing (41) for all i, we obtain

$$[K(K-1)+1]\sum_{j=1}^{K} nR_j \leq K(K-1)h(\mathbf{Y}_1) + nc_{13} \quad (42)$$

$$\leq K(K-1)\frac{n}{2}\log P + nc_{14} \quad (43)$$

which gives us the desired upper bound

$$D_{s,\Sigma} \leq \frac{K(K-1)}{K(K-1)+1} \quad (44)$$

concluding the converse part of the theorem.

IV. Achievable Scheme

Each transmitter i divides its message into $K-1$ mutually independent sub-messages. Each transmitter sends a linear combination of signals that carry these sub-messages together with a cooperative jamming signal. The messages are sent in such a way that all of the cooperative jamming signals are aligned in a single dimension at the legitimate receiver, occupying the smallest possible space at the legitimate receiver, and hence allowing for the reliable decodability of the message carrying signals. In addition, each cooperative jamming signal is aligned with $K-1$ message carrying signals at the eavesdropper to limit the information leakage rate to the eavesdropper. This scheme is illustrated in Fig. 2 for $K = 3$.

More specifically, we use a total of K^2 mutually independent random variables

$$V_{i,j}, \quad i,j \in \{1,\ldots,K\}, j \neq i \quad (45)$$

$$U_k, \quad k \in \{1,\ldots,K\} \quad (46)$$

where $\{V_{i,j}\}_{j\neq i}$ denote the message carrying signals and U_i denotes the cooperative jamming signal sent from transmitter i. In particular, $V_{i,j}$ carries the jth sub-message of transmitter i. Each of these random variables is uniformly and independently drawn from the same discrete constellation $C(a,Q)$,

$$C(a,Q) = a\{-Q, -Q+1, \ldots, Q-1, Q\} \quad (47)$$

where a and Q will be specified later. We choose the input signal of transmitter i, for $i = 1,\ldots,K$, as

$$X_i = \sum_{j=1, j\neq i}^{K} \frac{g_j}{g_i h_j} V_{i,j} + \frac{1}{h_i} U_i \quad (48)$$

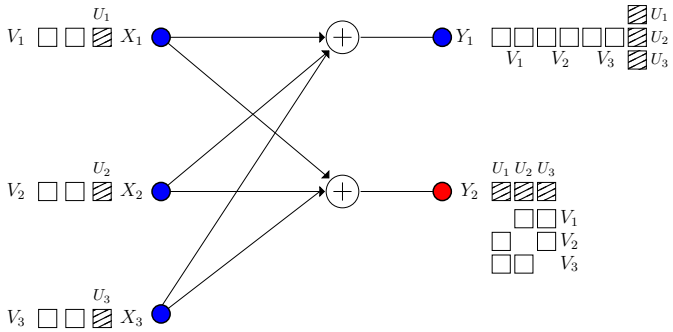

Fig. 2. Illustration of interference alignment for the K-user MAC wiretap channel. Here, $K = 3$ and we define $V_i \triangleq \{V_{i,j} : j \neq i\}$ for $i = 1, 2, 3$.

With these input selections, observations of the receivers are

$$Y_1 = \sum_{i=1}^{K}\sum_{j=1, j\neq i}^{K} \frac{g_j h_i}{g_i h_j} V_{i,j} + \left[\sum_{k=1}^{K} U_k\right] + N_1 \quad (49)$$

and

$$Y_2 = \sum_{i=1}^{K}\sum_{j=1, j\neq i}^{K} \frac{g_j}{h_j} V_{i,j} + \sum_{j=1}^{K} \frac{g_j}{h_j} U_j + N_2 \quad (50)$$

$$= \sum_{j=1}^{K} \frac{g_j}{h_j}\left[U_j + \sum_{i=1, i\neq j}^{K} V_{i,j}\right] + N_2 \quad (51)$$

where the terms inside brackets in (49) and (51) are *aligned*.

By [12, Theorem 1], we can achieve the following sum secrecy rate

$$\sup \sum_{i=1}^{K} R_i \geq I(\mathbf{V}; Y_1) - I(\mathbf{V}; Y_2) \quad (52)$$

where $\mathbf{V} \triangleq \{V_{i,j} : i,j \in \{1,\ldots,K\}, j \neq i\}$.

Now, we first use Fano's inequality to bound the first term in (52). Note that the *space* observed at receiver 1 consists of $(2Q+1)^{K(K-1)}(2KQ+1)$ points in $K(K-1)+1$ *dimensions*, and the sub-signal in each dimension is drawn from a constellation of $C(a, KQ)$. Here, we use the property that $C(a,Q) \subset C(a,KQ)$. By using Khintchine-Groshev theorem of Diophantine approximation [16], we can bound the minimum distance d_{min} between the points in receiver 1's space, i.e., for any $\delta > 0$, there exists a constant k_δ such that

$$d_{min} \geq \frac{k_\delta a}{(KQ)^{K(K-1)+\delta}} \quad (53)$$

for almost all rationally independent factors in Y_1 except for a set of Lebesgue measure zero. Then, we can upper bound the probability of decoding error of such a PAM scheme by considering the additive Gaussian noise at receiver 1 as,

$$\Pr\left[\mathbf{V} \neq \hat{\mathbf{V}}\right] \leq \exp\left(-\frac{d_{min}^2}{8}\right) \quad (54)$$

$$\leq \exp\left(-\frac{a^2 k_\delta^2}{8(KQ)^{2(K(K-1)+\delta)}}\right) \quad (55)$$

where $\hat{\mathbf{V}}$ is the estimate of $\mathbf{V}$ by choosing the closest point

in the constellation based on observation Y_1. For any $\delta > 0$, if we choose $Q = P^{\frac{1-\delta}{2(K(K-1)+1+\delta)}}$ and $a = \gamma P^{\frac{1}{2}}/Q$, where γ is a constant independent of P, then

$$\Pr\left[\mathbf{V} \neq \hat{\mathbf{V}}\right] \leq \exp\left(-\frac{k_\delta^2 \gamma^2 K^2 P}{8(KQ)^{2(K(K-1)+\delta)+2}}\right) \tag{56}$$

$$= \exp\left(-\frac{k_\delta^2 \gamma^2 K^2 P^\delta}{8K^{2(K(K-1)+\delta)}}\right) \tag{57}$$

and we can have $\Pr\left[\mathbf{V} \neq \hat{\mathbf{V}}\right] \to 0$ as $P \to \infty$. To satisfy the power constraint at the transmitters, we can simply choose

$$\gamma \leq \min_i \frac{1}{\sqrt{\sum_{j=1, j\neq i}^{K} \left(\frac{g_j}{g_i h_j}\right)^2 + \left(\frac{1}{h_i}\right)^2}} \tag{58}$$

By Fano's inequality and the Markov chain $\mathbf{V} \to Y_1 \to \hat{\mathbf{V}}$, we know that

$$H(\mathbf{V}|Y_1) \leq H(\mathbf{V}|\hat{\mathbf{V}}) \tag{59}$$

$$\leq 1 + \exp\left(-\frac{k_\delta^2 \gamma^2 K^2 P^\delta}{8K^{2(K(K-1)+1+\delta)}}\right) \log(2Q+1)^{K(K-1)} \tag{60}$$

$$= o(\log P) \tag{61}$$

where $o(\cdot)$ is the little-o function. This means that

$$I(\mathbf{V}; Y_1) = H(\mathbf{V}) - H(\mathbf{V}|Y_1) \tag{62}$$

$$= \log(2Q+1)^{K(K-1)} - H(\mathbf{V}|Y_1) \tag{63}$$

$$\geq \log(2Q+1)^{K(K-1)} - o(\log P) \tag{64}$$

On the other hand, we can bound the second term in (52) as

$$I(\mathbf{V}; Y_2) \leq I\left(\mathbf{V}; \sum_{j=1}^{K} \frac{g_j}{h_j}\left[U_j + \sum_{i=1, i\neq j}^{K} V_{i,j}\right]\right) \tag{65}$$

$$= H\left(\sum_{j=1}^{K} \frac{g_j}{h_j}\left[U_j + \sum_{i=1, i\neq j}^{K} V_{i,j}\right]\right) - H\left(\sum_{j=1}^{K} \frac{g_j}{h_j}\left[U_j + \sum_{i=1, i\neq j}^{K} V_{i,j}\right] \middle| \mathbf{V}\right) \tag{66}$$

$$= H\left(\sum_{j=1}^{K} \frac{g_j}{h_j}\left[U_j + \sum_{i=1, i\neq j}^{K} V_{i,j}\right]\right) - H\left(\sum_{j=1}^{K} \frac{g_j}{h_j} U_j\right) \tag{67}$$

$$\leq K \log \frac{2KQ+1}{2Q+1} \tag{68}$$

$$\leq K \log K \tag{69}$$

$$= o(\log P) \tag{70}$$

where (68) is due to the fact that entropy is maximized by the uniform distribution which takes values over a set of cardinality $(2KQ+1)^K$.

Combining (64) and (70), we obtain

$$\sup \sum_{i=1}^{K} R_i \geq I(\mathbf{V}; Y_1) - I(\mathbf{V}; Y_2) \tag{71}$$

$$\geq \log(2Q+1)^{K(K-1)} - o(\log P) \tag{72}$$

$$= \frac{K(K-1)(1-\delta)}{K(K-1)+1+\delta}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{73}$$

By choosing δ arbitrarily small, we can achieve the sum secure d.o.f. of $\frac{K(K-1)}{K(K-1)+1}$ for almost all channel gains.

V. Conclusions

In this paper, we obtained the exact sum secure d.o.f. of the K-user Gaussian MAC wiretap channel. Our achievability combines channel prefixing, structured signalling, structured cooperative jamming and real interference alignment. We align message carrying signals and cooperative jamming signals in a desired manner at the legitimate receiver and the eavesdropper to achieve the largest sum secure d.o.f. Our matching converse is based on directly relating the channel input of each user to the sum rate of the remaining users at the legitimate receiver.

References

[1] C. E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656–715, October 1949.

[2] A. D. Wyner. The wiretap channel. *Bell Syst. Tech. J.*, 54(8):1355–1387, January 1975.

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

[4] S. K. Leung-Yan-Cheong and M. E. Hellman. Gaussian wiretap channel. *IEEE Trans. Inf. Theory*, 24(4):451–456, July 1978.

[5] E. Tekin, S. Serbetli, and A. Yener. On secure signaling for the Gaussian multiple access wire-tap channel. In *39th Asilomar Conf. Signals, Systems and Computers*, November 2005.

[6] E. Tekin and A. Yener. Achievable rates for the general Gaussian multiple access wire-tap channel with collective secrecy. In *44th Annual Allerton Conf. Commun., Contr. and Comput.*, September 2006.

[7] E. Tekin and A. Yener. The Gaussian multiple access wire-tap channel. *IEEE Trans. Inf. Theory*, 54(12):5747–5755, December 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*, 54(6):2735–2751, June 2008.

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

[10] 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.

[11] X. He and A. Yener. Providing secrecy with structured codes: Tools and applications to two-user Gaussian channels. *IEEE Trans. Inf. Theory*, submitted July 2009. Also available at [arXiv:0907.5388].

[12] G. Bagherikaram, A. S. Motahari, and A. K. Khandani. On the secure degrees-of-freedom of the multiple-access-channel. *IEEE Trans. Inf. Theory*, submitted March 2010. Also available at [arXiv:1003.0729].

[13] R. Bassily and S. Ulukus. Ergodic secret alignment. *IEEE Trans. Inf. Theory*, 58(3):1594–1611, March 2012.

[14] J. Xie and S. Ulukus. Secure degrees of freedom of the Gaussian wiretap channel with helpers. In *50th Annual Allerton Conference on Communication, Control and Computing*, Monticello, IL, October 2012.

[15] X. He. *Cooperation and information theoretic security in wireless networks*. Ph.D. dissertation, Pennsylvania State University, 2010.

[16] A. S. Motahari, S. Oveis-Gharan, and A. K. Khandani. Real interference alignment with real numbers. *IEEE Trans. Inf. Theory*, submitted August 2009. Also available at [arXiv:0908.1208].

[17] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. Wiley-Interscience, second edition, 2006.