Secure Degrees of Freedom Region 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*— [1] showed that the sum secure degrees of freedom (s.d.o.f.) of the K-user Gaussian multiple access (MAC) wiretap channel is $\frac{K(K-1)}{K(K-1)+1}$. In this paper, we determine the entire s.d.o.f. *region* of the K-user Gaussian MAC wiretap channel. The converse follows from a middle step in the converse of [1]. The achievability follows from exploring the polytope structure of the converse region, determining its extreme points, and then showing that each extreme point can be achieved by an m-user MAC wiretap channel with $K-m$ helpers, i.e., by setting $K-m$ users' secure rates to zero and utilizing them as pure (structured) cooperative jammers. A byproduct of our result is that the sum s.d.o.f. is achieved *only at one corner point* of the s.d.o.f. region.**

I. Introduction

Wyner introduced the noisy wiretap channel, and demonstrated that secure communication can be attained by stochastic encoding/decoding between a legitimate pair in the presence of an eavesdropper, 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]. Leung-Yan-Cheong and Hellman obtained the capacity-equivocation region of the Gaussian wiretap channel [4], which is degraded. 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 [1], [6]–[13]. The secrecy capacity region of the Gaussian MAC wiretap channel is still unknown. In the absence of an exact secrecy capacity region, [1], [11]–[13] studied the secure degrees of freedom (s.d.o.f.) of the MAC wiretap channel, where the s.d.o.f. represents the pre-log of the secure rates at the high signal-to-noise ratio (SNR) regime.

Previously, [11] achieved strictly positive s.d.o.f. for the Gaussian MAC wiretap channel using nested lattice codes. Reference [12] achieved a sum s.d.o.f. of $\frac{K-1}{K}$ (which gives $\frac{1}{2}$ for the $K=2$ user case) by employing structured message signals from all legitimate transmitters, and by aligning them carefully at the legitimate receiver and the eavesdropper via real interference alignment [14]. Reference [13] achieved the same $\frac{1}{2}$ sum s.d.o.f. for the two-user ergodic Gaussian MAC wiretap channel by using scaling-based and ergodic alignment schemes. In addition, for $K=2$, the individual s.d.o.f. of $\frac{1}{2}$ achieved in [11], [15], [16] for a wiretap channel with a helper can also be understood as an achievable sum s.d.o.f. for the two-user MAC wiretap channel. Recently, [1] showed that the *exact* sum s.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 $K=2$. The achievability in [1] is based on real interference alignment, structured cooperative jamming, and channel prefixing. The converse in [1] is a generalization of the converse in [16] to the case of multiple legitimate transmitters.

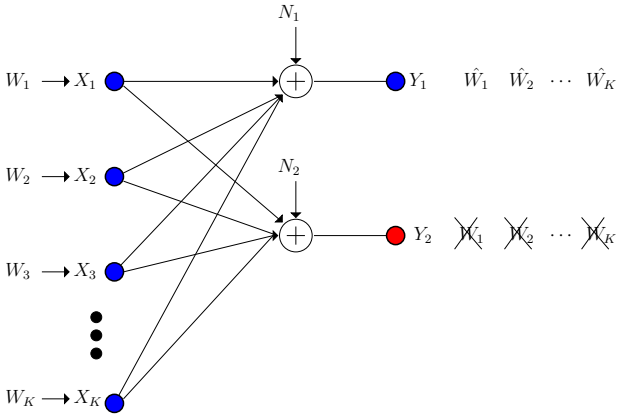

Fig. 1. K-user multiple access wiretap channel.

While the sum s.d.o.f. of the K-user MAC wiretap channel is known due to [1], the s.d.o.f. *region* has been unknown; in this paper, we determine the *exact* s.d.o.f. region of the K-user MAC wiretap channel by providing a converse and an achievability for the entire region. The converse surprisingly comes from a middle step in the converse proof of [1]. While [1] developed asymmetric upper bounds for the secure rates, since the sum s.d.o.f. was achieved by symmetric rates, [1] summed up the asymmetric upper bounds to get a symmetric upper bound to match the achievability; we revisit the converse proof in [1] and develop a converse for the entire region by keeping the developed asymmetric upper bounds.

The converse region for the secrecy problem has a general *polytope* structure, as opposed to the non-secrecy counterpart for the MAC which has a *polymatroid* structure. First, we determine the corner points of this converse (polytope) region,

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

whose convex hull gives the entire converse region. We then develop an achievable scheme for each corner point of the converse region. In particular, each corner point of the converse region is achieved by an m-user MAC wiretap channel with $K-m$ helpers, for $m=1,\ldots,K$, i.e., by setting $K-m$ users' secure rates to zero and utilizing them as pure (structured) cooperative jammers. A byproduct of our result in this paper is that the sum s.d.o.f. is achieved *only at one corner point* of the s.d.o.f. region, which is the symmetric-rate corner point.

II. System Model, Definitions and the Result

The K-user Gaussian MAC wiretap channel (see Fig. 1) is:

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

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

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 $(R_1,\ldots,R_K)$ 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

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

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 $\mathbf{Y}_2 \triangleq Y_2^n$.

The s.d.o.f. region is defined as:

$$D_s(K) = \Big\{(d_1,\ldots,d_K)^T : (R_1,\ldots,R_K) \text{ is achievable and } d_i \triangleq \lim_{P\to\infty}\frac{R_i}{\frac{1}{2}\log P},\ i=1,\ldots,K\Big\} \tag{5}$$

where T is the transpose. The sum s.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 sum s.d.o.f. of the K-user Gaussian MAC wiretap channel is characterized in the following theorem.

Theorem 1 ([1, Theorem 1]) *The sum s.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.*

In this paper, we characterize the s.d.o.f. region of the K-user Gaussian MAC wiretap channel in the following theorem.

Theorem 2 *The s.d.o.f. region $D_s(K)$ of the K-user Gaussian MAC wiretap channel is*

$$D_s(K) = \Big\{\mathbf{d} :\ d_i \geq 0,\ \mathbf{a}_i^T\mathbf{d} \leq 1,\ i \in \{1,\ldots,K\}\Big\} \tag{7}$$

for almost all channel gains, where $\mathbf{d} \triangleq (d_1,\ldots,d_K)^T$ and $\mathbf{a}_i$ is a $K\times 1$ column vector containing all 1's but one $\frac{K}{K-1}$ at the ith element, i.e., $a_{ii} = \frac{K}{K-1}$ and $a_{ij} = 1$ for $j \neq i$.

III. Converse

The converse simply follows from a key inequality in the proof in [1]. We reexamine equation (41) in [1]: $\forall i$,

$$nR_i + (K-1)\sum_{j=1}^{K} nR_j \leq (K-1)h(\mathbf{Y}_1) + nc_i \tag{8}$$

where all $\{c_i\}$ in this paper are constants independent of P.

Clearly, (8) is not symmetric. However, the lower bound derived in [1] was achieved by a symmetric scheme. Therefore, in [1], in order to obtain a matching upper bound, we summed up (8) for all i to obtain:

$$[K(K-1)+1]\sum_{j=1}^{K} nR_j \leq K(K-1)h(\mathbf{Y}_1) + nc' \tag{9}$$

$$\leq K(K-1)\frac{n}{2}\log P + nc'' \tag{10}$$

which provided the desired upper bound for the sum s.d.o.f.

$$D_{s,\Sigma} \leq \frac{K(K-1)}{K(K-1)+1} \tag{11}$$

which is the converse for Theorem 1.

In fact, (8) provides more information than what is needed for the sum s.d.o.f. only. In this paper, we start from (8)

$$nR_i + (K-1)\sum_{j=1}^{K} nR_j \leq (K-1)\left(\frac{n}{2}\log P\right) + nc_i \tag{12}$$

divide by $\frac{1}{2}\log P$ and take the limit $P\to\infty$ on both sides,

$$d_i + (K-1)\sum_{j=1}^{K} d_j \leq (K-1) \tag{13}$$

which is equivalent to $\frac{K}{K-1}d_i + \sum_{j=1,j\neq i}^{K} d_j \leq 1$, that is, $\mathbf{a}_i^T\mathbf{d} \leq 1$. This concludes the converse proof of Theorem 2.

IV. Polytope Structure and Extreme Points

To prove that the region $D_s(K)$ in (7) is tight, we first express it in terms of its *corner points*, i.e., *extreme points*, explicitly characterize all of its extreme points, and develop a scheme to achieve each of its extreme points.

Let $X \subseteq R^n$. The convex hull of X, $\mathrm{Co}(X)$, is the set of all convex combinations of the points in X: $\mathrm{Co}(X) \triangleq \{\sum_i \lambda_i \mathbf{x}_i \mid \mathbf{x}_i \in X,\ \sum_i \lambda_i = 1,\ \lambda_i \in R,\ \text{and } \lambda_i \geq 0,\ \forall i\}$. A set $P \subseteq R^n$ is a *polyhedron* if there is a system of finitely many inequalities $A\mathbf{x} \leq \mathbf{b}$ such that $P = \{\mathbf{x} \in R^n \mid A\mathbf{x} \leq \mathbf{b}\}$. A set $P \subseteq R^n$ is a *polytope* if there is a finite set $X \subseteq R^n$ such that $P = \mathrm{Co}(X)$. Then, we have the following theorem.

Theorem 3 ([17, Theorem 3.1.3]) *Let $P \subseteq R^n$. Then, P is a bounded polyhedron if only if P is a polytope.*

Therefore, the region in (7) is a polytope, which is a convex hull of some finite set X. By the properties of the convex hull of a finite set X, $D_s(K)$ is a bounded, closed, convex set. Since $D_s(K) \subset R^K$, $D_s(K)$ is a compact convex set. Next, we refer to the formal definition of a *corner (extreme) point*.

Definition 1 (Extreme point) *Let $C \subseteq R^n$. An $\mathbf{x} \in C$ is an extreme point if there are no $\mathbf{y}, \mathbf{z} \in C \setminus \{\mathbf{x}\}$ such that $\mathbf{x} = \lambda\mathbf{y} + (1-\lambda)\mathbf{z}$ for any $\lambda \in (0,1)$. Then, Ex(C) is the set of all extreme points of C.*

Theorem 4 (Minkowski, 1910. [17, Theorem 2.4.5]) *Let $C \subseteq R^n$ be a compact convex set. Then,*

$$C = Co(Ex(C)). \tag{14}$$

From Minkowski theorem, the polytope $D_s(K)$ in (7) is a convex hull of its extreme points. Then, in order to prove that $D_s(K)$ is tight, it suffices to prove that each extreme point of $D_s(K)$ is achievable. Then, from convexification through time-sharing, all points in $D_s(K)$ are achievable. It is clear that zero vector is an extreme point in $D_s(K)$ and is trivially achievable. The rest of the achievability proof focuses on non-zero extreme points.

Let $\mathbf{d} \in D_s(K)$ be a non-zero extreme point of $D_s(K)$. Then, $\mathbf{d}$ must be on the boundary, i.e., there exists a subset $S \subseteq \{1, \ldots, K\}$, $S \neq \phi$, such that

$$\mathbf{a}_i^T \cdot \mathbf{d} = 1, \qquad \forall i \in S \tag{15}$$

$$\mathbf{a}_j^T \cdot \mathbf{d} < 1, \qquad \forall j \in S^c \tag{16}$$

where S^c is the complement of S. We call the boundary condition satisfying (15) and (16) as the *boundary* S.

Lemma 1 *If the extreme point $\mathbf{d}$ is on boundary S, then the ith and the kth elements of $\mathbf{d}$ are the same for any $i, k \in S$,*

$$d_i = d_k \tag{17}$$

Proof: Let $i \neq k$. Since $i, k \in S$, by the definition of S,

$$\mathbf{a}_i^T \cdot \mathbf{d} = d_k + \frac{K}{K-1} d_i + \sum_{l \neq i,k} d_l = 1 \tag{18}$$

$$\mathbf{a}_k^T \cdot \mathbf{d} = d_i + \frac{K}{K-1} d_k + \sum_{l \neq i,k} d_l = 1 \tag{19}$$

which proves Lemma 1. ■

Lemma 2 *If the extreme point $\mathbf{d}$ is on boundary S, then $\forall j \in S^c$ (if exists), the jth element of $\mathbf{d}$ must be zero, i.e., $d_j = 0$.*

Proof: We prove this lemma by contradiction. Assume that $S^c \neq \phi$ and $\exists j \in S^c$ such that $d_j > 0$. By Lemma 1, let $\Delta \triangleq d_i, \forall i \in S$. It is easy to see that $\Delta > 0$; otherwise, if $\Delta = 0$, then $\mathbf{a}_j^T \cdot \mathbf{d} > 1$, which contradicts the fact that $j \in S^c$.

For convenience, denote by m the cardinality of the set S, i.e., $m \triangleq |S|$. We aim to construct two distinct points $\mathbf{y}, \mathbf{z} \in D_s(K)$ such that

$$\mathbf{d} = \lambda\mathbf{y} + (1-\lambda)\mathbf{z} \tag{20}$$

for some $\lambda \in (0,1)$.

Let $\epsilon_y > 0$ be a small positive number and $\mathbf{y}$ be

$$\mathbf{y} \triangleq \begin{cases} y_k = d_k - \frac{\epsilon_y}{\frac{K}{K-1}+(m-1)}, & \forall k \in S \\ y_k = d_k + \epsilon_y, & k = j \\ y_k = d_k, & \forall k \in S^c \setminus \{j\} \end{cases} \tag{21}$$

It is easy to check that $\forall i \in S$, $\mathbf{a}_i^T \cdot \mathbf{y} = 1$. For finitely many $k \in S^c$, we can always find a threshold ϵ_y' such that $\mathbf{a}_k^T \cdot \mathbf{y} < 1$ if $\epsilon_y' \geq \epsilon_y > 0$. In addition, let

$$\epsilon_y = \min\left\{\epsilon_y', \left[\frac{K}{K-1} + (m-1)\right]\Delta\right\} \tag{22}$$

Then, $y_i \geq 0, \forall i \in S$, i.e., $\mathbf{y} \in D_s(K)$.

Similarly, let $\epsilon_z > 0$ be a small positive number and $\mathbf{z}$ be

$$\mathbf{z} \triangleq \begin{cases} z_k = d_k + \frac{\epsilon_z}{\frac{K}{K-1}+(m-1)}, & \forall k \in S \\ z_k = d_k - \epsilon_z, & k = j \\ z_k = d_k, & \forall k \in S^c \setminus \{j\} \end{cases} \tag{23}$$

By the same argument, such $\epsilon_z > 0$ exists, by the assumption $d_j > 0$, and thereby $\mathbf{z} \in D_s(K)$.

Simply take $\epsilon_y = \epsilon_z$ as the minimum of (ϵ_y, ϵ_z) found above. Clearly, $\mathbf{y} \neq \mathbf{z}$, $\mathbf{y}, \mathbf{z} \in D_s(K) \setminus \{\mathbf{d}\}$, and $\mathbf{d} = \frac{1}{2}(\mathbf{y}+\mathbf{z})$, which contradicts Definition 1 of the extreme point $\mathbf{d}$. This implies $d_j = 0$ for all $j \in S^c$. ■

As a straightforward consequence of Lemmas 1 and 2, we have the following result.

Proposition 1 *For any extreme point $\mathbf{d} \in D_s(K)$, if*

$$S = \{i \mid \mathbf{a}_i^T \cdot \mathbf{d} = 1\}, \qquad m \triangleq |S| \tag{24}$$

then,

$$\mathbf{d} = \begin{cases} d_k = \Delta, & \forall k \in S \\ d_k = 0, & \forall k \in S^c \end{cases} \tag{25}$$

where

$$\Delta = \frac{K-1}{m(K-1)+1} \tag{26}$$

V. Achievability: m-user Gaussian MAC Wiretap Channel with $(K-m)$ Helpers

The previous section showed that the converse region is a polytope with extreme points which have m coordinates all equal to Δ given in (26), and the remaining $K-m$ coordinates

all equal to zero. In this section, we prove that each of these extreme points is achievable. Without loss of generality, we prove that the s.d.o.f. point of

$$\mathbf{d} = (\underbrace{\Delta, \ldots, \Delta}_{m \text{ item(s)}}, \underbrace{0, \ldots, 0}_{(K-m) \text{ item(s)}}) \tag{27}$$

is achievable for all $1 < m < K$ with Δ in (26). By symmetry, this proves the achievability of all extreme points. Note that $m = K$ is shown in [1], and $m = 1$ is shown in [16].

Theorem 5 *The extreme point $\mathbf{d} \in D_s(K)$ given in (27) is achieved by m-user Gaussian MAC wiretap channel with $K - m$ helpers for almost all channel gains.*

Proof: Consider the m-user Gaussian MAC wiretap channel with $K - m$ helpers where transmitter i, $i = 1, \ldots, m$, has confidential message W_i intended for the legitimate receiver and the remaining $K - m$ transmitters serve as independent helpers without messages of their own.

In order to achieve the extreme point $\mathbf{d}$ in (27), transmitter i, $i = 1, \ldots, m$, divides its message into $K - 1$ mutually independent sub-messages. Each transmitter sends a linear combination of signals that carry the sub-messages. In addition to message carrying signals, all transmitters also send cooperative jamming signals U_i, $i = 1, \ldots, K$, respectively. 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 at most $K - 1$ message carrying signals at the eavesdropper to limit the information leakage rate to the eavesdropper. An example of $K = 3$, $m = 2$, and $K - m = 1$ is given in Fig. 2.

More specifically, we use a total of $m(K-1)+K$ mutually independent random variables

$$V_{i,j}, \quad i \in \{1, \ldots, m\}, \ j \in \{1, \cdots, K\} \setminus \{i\} \tag{28}$$

$$U_k, \quad k \in \{1, \cdots, K\} \tag{29}$$

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 $C(a, Q)$,

$$C(a, Q) = a\{-Q, -Q+1, \ldots, Q-1, Q\} \tag{30}$$

where a and Q will be specified later. We choose the input signals of the transmitters as

$$X_i = \sum_{j=1, j \neq i}^{K} \frac{g_j}{h_j g_i} V_{ij} + \frac{1}{h_i} U_i, \qquad i \in \{1, \ldots, m\} \tag{31}$$

$$X_j = \frac{1}{h_j} U_j, \qquad j \in \{m+1, \ldots, K\} \tag{32}$$

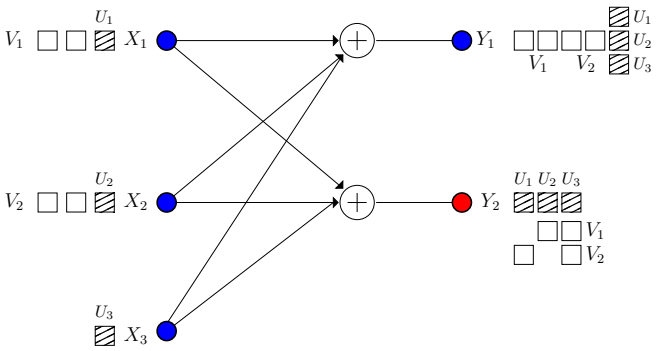

Fig. 2. Illustration of secure interference alignment for the s.d.o.f. triple $(2/5, 2/5, 0)$ for the two-user MAC wiretap channel with one helper; $K = 3$ and $m = 2$. Here, we define $V_i \triangleq \{V_{i,j} : j = 1, 2, 3, j \neq i\}$ for $i = 1, 2$.

With these input selections, observations of the receivers are

$$Y_1 = \left[\sum_{i=1}^{m} \sum_{j=1, j \neq i}^{K} \left(\frac{g_j h_i}{h_j g_i} V_{ij}\right)\right] + \left(\sum_{k=1}^{K} U_k\right) + N_1 \tag{33}$$

and

$$Y_2 = \sum_{j=1}^{K} \frac{g_j}{h_j} \left(U_j + \sum_{i=1, i \neq j}^{m} V_{ij}\right) + N_2 \tag{34}$$

where the terms inside the parentheses in (33) and (34) are *aligned*.

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

$$\sup \sum_{i=1}^{m} R_i \geq I(\mathbf{V}; Y_1) - I(\mathbf{V}; Y_2) \tag{35}$$

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

By similar steps to [1], for any $\delta > 0$, if we choose $Q = P^{\frac{1-\delta}{2 \times (m(K-1)+1+\delta)}}$ and $a = \gamma P^{\frac{1}{2}}/Q$, where γ is a constant independent of P to meet the average power constraint, then

$$\Pr\left[\mathbf{V} \neq \hat{\mathbf{V}}\right] \leq \exp\left(-\beta P^{\delta}\right) \tag{36}$$

for some constant $\beta > 0$ (independent of P), where $\hat{\mathbf{V}}$ is the estimate of $\mathbf{V}$ by choosing the closest point in the constellation based on observation Y_1. This means that we can have $\Pr[\mathbf{V} \neq \hat{\mathbf{V}}] \to 0$ as $P \to \infty$.

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

$$H(\mathbf{V}|Y_1) \leq H(\mathbf{V}|\hat{\mathbf{V}}) \tag{37}$$

$$\leq 1 + \exp\left(-\beta P^{\delta}\right) \log(2Q+1)^{m(K-1)} \tag{38}$$

$$= o(\log P) \tag{39}$$

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

$$I(\mathbf{V}; Y_1) = H(\mathbf{V}) - H(\mathbf{V}|Y_1) \tag{40}$$

$$= \log(2Q+1)^{m(K-1)} - H(\mathbf{V}|Y_1) \tag{41}$$

$$\geq \log(2Q+1)^{m(K-1)} - o(\log P) \tag{42}$$

On the other hand, we can bound the second term in (35) as

$$I(\mathbf{V};Y_2) \le I\left(\mathbf{V};Y_2-N_2\right) \tag{43}$$

$$= \sum_{j=1}^{K} H\left(U_j + \sum_{i=1,i\neq j}^{m} V_{ij}\right) - H\left(U_1,\ldots,U_K\right) \tag{44}$$

$$\le K\log\frac{2KQ+1}{2Q+1} \tag{45}$$

$$\le K\log K \tag{46}$$

$$= o(\log P) \tag{47}$$

where (45) is due to the fact that entropy of each $U_j + \sum_{i=1,i\neq j}^{m} V_{ij}$ is maximized by the uniform distribution which takes values over a set of cardinality $2KQ+1$.

Combining (42) and (47), we obtain

$$\sup\sum_{i=1}^{m} R_i \ge I(\mathbf{V};Y_1) - I(\mathbf{V};Y_2) \tag{48}$$

$$\ge \log(2Q+1)^{m(K-1)} - o(\log P) \tag{49}$$

$$= \frac{m(K-1)(1-\delta)}{m(K-1)+1+\delta}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{50}$$

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

$$\Bigg(\underbrace{\frac{(K-1)}{m(K-1)+1},\ldots,\frac{(K-1)}{m(K-1)+1}}_{m \text{ item(s)}},\ \underbrace{0,\ldots,0}_{K-m \text{ item(s)}}\Bigg) \tag{51}$$

is achievable by symmetry, which is (27). ■

VI. Example S.D.O.F Regions for $K = 2$ and 3

For $K=2$, the s.d.o.f. region in (7) becomes

$$D_s(2) = \left\{d_1,d_2\ge 0,\ 2d_1+d_2\le 1,\ d_1+2d_2\le 1\right\} \tag{52}$$

As shown in Fig. 3, in order to provide the achievability, it suffices to prove that the corner points $(\frac{1}{2},0),(0,\frac{1}{2})$, and $(\frac{1}{3},\frac{1}{3})$ are achievable. In fact the achievability of $(\frac{1}{2},0),(0,\frac{1}{2})$ was proved in [16] and the achievability of $(\frac{1}{3},\frac{1}{3})$ was proved in [1]. Note that $(\frac{1}{3},\frac{1}{3})$ is the only sum s.d.o.f. optimum point.

For $K=3$, the s.d.o.f. region in (7) becomes

$$D_s(3) = \Big\{d_1,d_2,d_3\ge 0,\quad 3d_1+2d_2+2d_3\le 2,\quad 2d_1+3d_2+2d_3\le 2,\quad 2d_1+2d_2+3d_3\le 2\Big\} \tag{53}$$

The extreme points (corner points) of this region are: $(2/3,0,0)$, $(0,2/3,0)$, $(0,0,2/3)$, $(2/5,2/5,0)$, $(2/5,0,2/5)$, $(0,2/5,2/5)$, $(2/7,2/7,2/7)$, which correspond to the maximum individual s.d.o.f. (see Gaussian wiretap channel with two helpers [16]), the maximum sum of pair of s.d.o.f. (see two-user Gaussian MAC wiretap channel with one helper, proved in Section V), and the maximum sum s.d.o.f. (see three-user Gaussian MAC wiretap channel [1]).

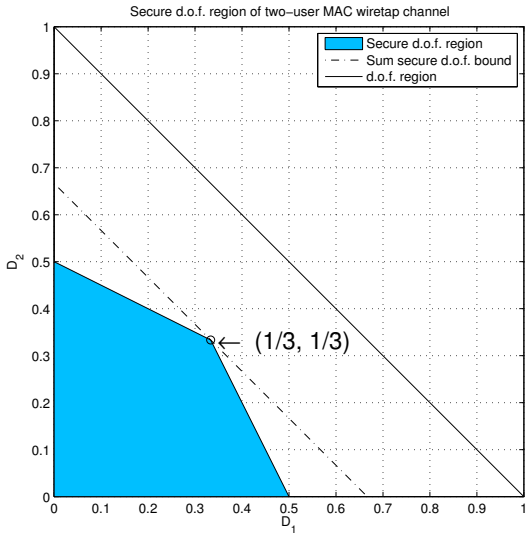

Fig. 3. The s.d.o.f. region of the $K=2$-user multiple access wiretap channel.

References

[1] J. Xie and S. Ulukus. Secure degrees of freedom of the Gaussian multiple access wiretap channel. In *IEEE International Symposium on Information Theory*, Istanbul, Turkey, July 2013.

[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] 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].

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

[16] 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.

[17] B. Grunbaum. *Convex Polytopes*. Springer, second edition, 2003.