Secure Degrees of Freedom of the Interference Channel with No Eavesdropper CSI

Pritam Mukherjee Sennur Ulukus
Department of Electrical and Computer Engineering
University of Maryland, College Park, MD 20742
pritamm@umd.edu *ulukus@umd.edu*

***Abstract*—We consider the K-user interference channel with an external eavesdropper, with no eavesdropper's channel state information at the transmitters (CSIT). We determine the exact sum secure degrees of freedom (s.d.o.f.) for this channel by providing a new alignment based achievable scheme and a matching converse. Our results show that the lack of eavesdropper's CSIT does not have a significant impact on the optimal s.d.o.f. of the interference channel with an external eavesdropper, especially when the number of users is large.**

I. Introduction

We consider the K-user interference channel with an external eavesdropper, where K transmitters wish to send independent messages to their respective receivers in the presence of an external eavesdropper; see Fig. 1. The messages need to be kept secure from the external eavesdropper. We consider the case where all the channel gains to the legitimate receivers are known at each transmitter, but no eavesdropper channel state information (CSI) is available at any of the transmitters. This models a practically relevant case, where the legitimate receivers feed back the CSI to the legitimate transmitters, but the passive eavesdropper does not report any CSI back, though she may be measuring and using it for her own purposes.

The capacity of the interference channel, even without security constraints, remains an open problem. In the absence of exact capacity regions, the degrees of freedom (d.o.f.) of the interference channel at high signal-to-noise (SNR) regimes has been studied in the literature. Reference [1] establishes the optimal sum d.o.f. of the K-user interference channel without any security constraints to be $\frac{K}{2}$. With an external eavesdropper whose CSIT is available, references [2], [3] determine the optimal sum secure degrees of freedom (s.d.o.f.) of the K-user interference channel to be $\frac{K(K-1)}{2K-1}$. In this paper, we focus on the case when no eavesdropper's CSIT is available and establish the optimal sum s.d.o.f. to be $\frac{K-1}{2}$ in this case.

To that end, we provide an achievable scheme based on asymptotic real interference alignment [4], [5]. We consider the case of fixed channel gains in this paper. Our work can be extended to the case of fading channel gains using a scheme based on vector space alignment [1], that achieves the same optimal sum s.d.o.f. of $\frac{K-1}{2}$; we omit the scheme here due to space constraints, see [6]. An interesting aspect of our proposed scheme is that it provides confidentiality of the messages not only from the external eavesdropper but also from the unintended legitimate receivers. Thus, our scheme achieves the optimal sum s.d.o.f. for the K-user interference channel with both confidential messages and an external eavesdropper, with no eavesdropper CSIT.

This work was supported by NSF Grants CNS 13-14733, CCF 14-22111 and CCF 14-22129.

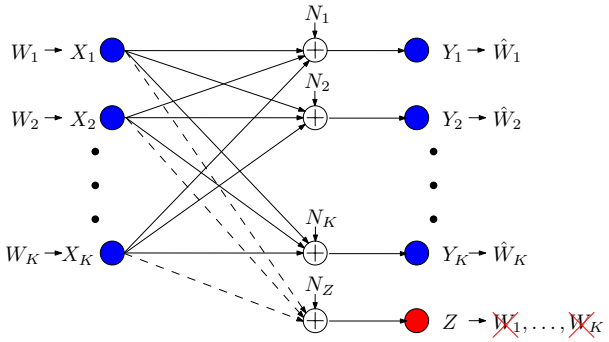

Fig. 1. K-user interference channel with an external eavesdropper.

To prove the converse, we combine techniques from [3] and [7]. We exploit a key result in [7] that the output entropy at a receiver whose CSIT is not available is at least as large as the output entropy at a receiver whose CSIT is available, even when the transmitters cooperate and transmit correlated signals. Intuitively, this is true since no alignment of signals is possible at the receiver whose CSIT is unavailable. Using this insight along with the techniques of [3], we establish the optimal sum s.d.o.f. to be $\frac{K-1}{2}$ for our model.

Related work: The K-user interference channel with an external eavesdropper is studied in [8]. When the eavesdropper's CSIT is available, [8] proposes a scheme that achieves sum s.d.o.f. of $\frac{K-1}{2}$. The optimal s.d.o.f. in this case, however, is established in [3] to be $\frac{K(K-1)}{2K-1}$, using cooperative jamming signals along with interference alignment techniques. When the eavesdropper's CSIT is not available, reference [8] proposes a scheme that achieves a sum s.d.o.f. of $\frac{K-2}{2}$. In this paper, we show that this is suboptimal and establish the optimal s.d.o.f. to be $\frac{K-1}{2}$.

The impact of no eavesdropper CSIT has been investigated for other channel models as well. For the wiretap channel with K helpers and no eavesdropper CSIT, reference [9] shows that the optimal s.d.o.f. is $\frac{K}{K+1}$, which coincides with the optimal s.d.o.f. with full eavesdropper's CSIT [10]. Thus, there is no loss of s.d.o.f. in this case due to unavailability of the

eavesdropper's CSIT. For the K-user multiple access wiretap channel, reference [11] shows that when the eavesdropper's CSIT is not available, the optimal sum s.d.o.f. decreases from $\frac{K(K-1)}{K(K-1)+1}$ [10] to $\frac{K-1}{K}$, and the K-user multiple access wiretap channel reduces to a wiretap channel with $K-1$ helpers. For the interference channel with an external eavesdropper too, we see that the optimal sum s.d.o.f. decreases from $\frac{K(K-1)}{2K-1}$ [3], to $\frac{K-1}{2}$, when the eavesdropper's CSIT is not available. It can be verified that the loss in s.d.o.f. is at most $\frac{1}{4}$. Thus, when K is large, the loss in s.d.o.f. is small compared to the optimal sum s.d.o.f. with eavesdropper CSIT.

II. System Model

The input output relations for the K-user interference channel with an external eavesdropper, Fig. 1, are

$$Y_i = \sum_{j=1}^{K} h_{ji} X_j + N_i, \quad i = 1, \ldots, K \tag{1}$$

$$Z = \sum_{j=1}^{K} g_j X_j + N_Z \tag{2}$$

where Y_i is the channel output of receiver i, Z is the channel output at the eavesdropper, X_j is the channel input of transmitter j, h_{ji} is the channel gain from transmitter j to receiver i, g_j is the channel gain from transmitter j to the eavesdropper, and $\{N_1, \ldots, N_K, N_Z\}$ are mutually independent zero-mean unit-variance white Gaussian noise random variables. The channel gains h_{ji}s and g_is are assumed to be drawn from an arbitrary but fixed continuous distribution with bounded support. The channel gains to the eavesdropper, g_is are not known at any of the transmitters. All channel inputs satisfy average power constraints $E[X_i^2] \leq P$, for $i = 1, \ldots, K$.

Transmitter i wishes to send a message W_i, chosen uniformly from a set $\mathcal{W}_i$, to receiver i. The messages $W_1, \ldots, W_K$ are mutually independent. A secure rate tuple $(R_1, \ldots, R_K)$, with $R_i = \frac{\log |\mathcal{W}_i|}{n}$ is achievable if there exists a sequence of codes which satisfy the reliability constraints at the legitimate receivers, namely, $\Pr[W_i \neq \hat{W}_i] \leq \epsilon_n$, for $i = 1, \ldots, K$, and the security condition

$$\frac{1}{n} I(W_1^K; Z^n) \leq \epsilon_n \tag{3}$$

where $\epsilon_n \to 0$, as $n \to \infty$. An s.d.o.f. tuple $(d_1, \ldots, d_K)$ is said to be achievable if a rate tuple $(R_1, \ldots, R_K)$ is achievable with $d_i = \lim_{P \to \infty} \frac{R_i}{\frac{1}{2} \log P}$. The sum s.d.o.f. d_s is the largest achievable $\sum_{i=1}^{K} d_i$.

III. Main Results and Discussion

The main result of this paper is the determination of the exact sum s.d.o.f. of the K-user interference channel with an external eavesdropper, when no eavesdropper CSI is available at the transmitters. We present the main result of this paper in the following theorem.

Theorem 1 *For the K-user interference channel with an external eavesdropper and no eavesdropper CSI at the transmitters, the optimal sum s.d.o.f. d_s is given by,*

$$d_s = \frac{K-1}{2} \tag{4}$$

for almost all channel gains.

We present the converse proof for Theorem 1 in Section IV, and an achievable scheme in Section V. Let us now highlight a few interesting aspects of our result.

First, we consider the cost of security against an external eavesdropper. Without any security constraints, in the absence of the external eavesdropper, the optimal sum d.o.f. is $\frac{K}{2}$, [1]. Thus, from Theorem 1, the introduction of an external eavesdropper whose CSI is not available at the transmitters decreases the sum d.o.f. by $\frac{1}{2}$. It is interesting to note that the loss does not depend on the number of users.

Next, we consider the loss of s.d.o.f. due to lack of the eavesdropper's CSIT. With full eavesdropper's CSIT, the optimal s.d.o.f. is $\frac{K(K-1)}{2K-1}$. In the absence of the eavesdropper's CSIT, the optimal s.d.o.f. reduces to $\frac{K-1}{2}$. It can be shown that the s.d.o.f. loss is bounded by $\frac{1}{4}$, which implies that as a percentage of the optimal s.d.o.f. with eavesdropper CSIT, the loss in s.d.o.f. is small, especially as the number of users increases.

IV. Proof of the Converse

To prove the converse, we combine techniques from [3], [10] and [7]. Here, we use $\mathbf{X}_i$ to denote the collection of all channel inputs $\{X_i(t),\ t = 1, \ldots, n\}$ of transmitter i. Similarly, we use $\mathbf{Y}_i$ and $\mathbf{Z}$ to denote the channel outputs at legitimate receiver i and the eavesdropper, respectively, over n channel uses. We further define $\mathbf{X}_1^K$ as the collection of all channel inputs from all of the transmitters, i.e., $\{\mathbf{X}_i,\ i = 1, \ldots, K\}$. Finally, for a fixed j, we define $\mathbf{X}_{-j} \stackrel{\Delta}{=} \{\mathbf{X}_i,\ i \neq j,\ i = 1, \ldots, K\}$. We divide the proof into three steps.

1) Deterministic channel model: We consider the deterministic channel given as,

$$Y_i(t) = \sum_{j=1}^{K} \lfloor h_{ji}(t) X_j(t) \rfloor \tag{5}$$

$$Z(t) = \sum_{j=1}^{K} \lfloor g_j(t) X_j(t) \rfloor \tag{6}$$

for $i = 1, \ldots, K$, with the constraint that

$$X_j(t) \in \left\{0, 1, \ldots, \left\lfloor \sqrt{P} \right\rfloor \right\} \tag{7}$$

We show that there is no loss of s.d.o.f. in considering the channel in (5)-(6) instead of the one in (1)-(2) by proving that given any codeword tuple $(\mathbf{X}_1^G, \ldots, \mathbf{X}_K^G)$ for the original channel of (1)-(2), we can construct a codeword tuple $(\mathbf{X}_1^D, \ldots, \mathbf{X}_K^D)$ with $X_i^D(t) = \left\lfloor X_i^G(t) \right\rfloor \bmod \lfloor \sqrt{P} \rfloor$, for the deterministic channel of (5)-(6), that achieves an s.d.o.f. no smaller than the s.d.o.f. achieved by $(\mathbf{X}_1^G, \ldots, \mathbf{X}_K^G)$

on the original channel. For $i = 1, \ldots, K$, define $Y_i^G(t) \triangleq \sum_{j=1}^{K} h_{ji}(t) X_j^G(t) + N_1(t)$ and $Y_i^D(t) \triangleq \sum_{j=1}^{K} \lfloor h_{ji}(t) X_j^D(t) \rfloor$. Defining Z^G and Z^D similarly, it suffices to show that

$$I(W_i; \mathbf{Y}_i^G) \leq I(W_i; \mathbf{Y}_i^D) + no(\log P) \tag{8}$$

$$I(W_1^K; \mathbf{Z}^D) \leq I(W_1^K; \mathbf{Z}^G) + no(\log P) \tag{9}$$

for every $i = 1, \ldots, K$. The proof of (8) follows along similar lines as the proof presented in [7] and is omitted here. To prove (9), we define $\bar{Z}(t) \triangleq \sum_{i=1}^{K} \lfloor g_i(t) \lfloor X_i^G(t) \rfloor \rfloor$, $\hat{Z}(t) \triangleq \bar{Z}(t) - Z^D(t)$, and $\tilde{Z}(t) \triangleq \lfloor Z^G(t) \rfloor - \bar{Z}(t) - \lfloor N_Z(t) \rfloor$. Then,

$$I(W_1^K; \mathbf{Z}^D) \leq I(W_1^K; \mathbf{Z}^D, \mathbf{Z}^G, \bar{\mathbf{Z}}) \tag{10}$$

$$\leq I(W_1^K; \mathbf{Z}^G) + H(\bar{\mathbf{Z}}|\mathbf{Z}^G) + H(\mathbf{Z}^D|\bar{\mathbf{Z}}) \tag{11}$$

$$\leq I(W_1^K; \mathbf{Z}^G) + H(\bar{\mathbf{Z}}|\lfloor \mathbf{Z}^G \rfloor) + H(\hat{\mathbf{Z}}) \tag{12}$$

$$\leq I(W_1^K; \mathbf{Z}^G) + no(\log P) \tag{13}$$

where $\lfloor \mathbf{Z}^G \rfloor = \left(\lfloor Z^G(1) \rfloor, \ldots, \lfloor Z^G(n) \rfloor \right)$. Here, (13) follows since $H(\hat{Z}(t)) \leq o(\log P)$ following the steps of the proof in [7, Appendix A.2]. In addition, $H(\bar{\mathbf{Z}}|\lfloor \mathbf{Z}^G \rfloor) \leq no(\log P)$, using [12, Lemma E.1, Appendix E]; see [6] for details.

Therefore, the s.d.o.f. of the deterministic channel in (5)-(6) with integer channel inputs as described in (7) is no smaller than the s.d.o.f. of the original channel in (1)-(2). Consequently, any upper bound (e.g., converse) developed for the s.d.o.f. of (5)-(6) will serve as an upper bound for the s.d.o.f. of (1)-(2). Thus, we will consider this deterministic channel in the remaining part of the converse.

2) An upper bound on the sum rate: We begin as in the secrecy penalty lemma in [10], i.e., [10, Lemma 1]. Note that, unlike [10, Lemma 1], channel inputs are integer here:

$$n \sum_{i=1}^{K} R_i \leq I(W_1^K; \mathbf{Y}_1^K) - I(W_1^K; \mathbf{Z}) + n\epsilon \tag{14}$$

$$\leq I(W_1^K; \mathbf{Y}_1^K|\mathbf{Z}) + n\epsilon \tag{15}$$

$$\leq H(\mathbf{Y}_1^K|\mathbf{Z}) + n\epsilon \tag{16}$$

$$= H(\mathbf{Y}_1^K, \mathbf{Z}) - H(\mathbf{Z}) + n\epsilon \tag{17}$$

$$\leq H(\mathbf{X}_1^K, \mathbf{Y}_1^K, \mathbf{Z}) - H(\mathbf{Z}) + n\epsilon \tag{18}$$

$$= H(\mathbf{X}_1^K) - H(\mathbf{Z}) + n\epsilon \tag{19}$$

$$\leq \sum_{k=1}^{K} H(\mathbf{X}_k) - H(\mathbf{Z}) + n\epsilon \tag{20}$$

where (19) follows since $H(\mathbf{Y}_1^K, \mathbf{Z}|\mathbf{X}_1^K) = 0$.

Also, to ensure decodability at the legitimate receiver, we use the role of a helper lemma in [10], i.e., [10, Lemma 2],

$$nR_i \leq I(\mathbf{X}_i; \mathbf{Y}_i) + n\epsilon' \tag{21}$$

$$= H(\mathbf{Y}_i) - H(\mathbf{Y}_i|\mathbf{X}_i) + n\epsilon' \tag{22}$$

$$\leq H(\mathbf{Y}_i) - H(\mathbf{X}_j) + n\epsilon' + nc \tag{23}$$

for any $j \neq i$, and (23) holds under a mild technical condition on the common distribution F of the channel gains: $\int_{-\infty}^{\infty} \log\left(1 + \frac{1}{|h|}\right) dF(h) \leq c$ for some $c \in \mathbb{R}$; see [6]. Using (23) and (20), we obtain,

$$2n \sum_{i=1}^{K} R_i \leq \sum_{k=1}^{K} H(\mathbf{Y}_k) - H(\mathbf{Z}) \tag{24}$$

$$\leq (K-1)\frac{n}{2} \log P + (H(\mathbf{Y}_K) - H(\mathbf{Z})) + n\epsilon'' \tag{25}$$

where $\epsilon'' = o(\log P)$. Dividing by n and letting $n \to \infty$,

$$2 \sum_{i=1}^{K} R_i \leq (K-1)\frac{1}{2} \log P + \lim_{n\to\infty} \frac{1}{n} \left(H(\mathbf{Y}_K) - H(\mathbf{Z})\right) + \epsilon'' \tag{26}$$

Now dividing by $\frac{1}{2} \log P$ and taking $P \to \infty$,

$$\sum_{i=1}^{K} d_i \leq \frac{K-1}{2} + \frac{1}{2} \lim_{P\to\infty} \lim_{n\to\infty} \frac{H(\mathbf{Y}_K) - H(\mathbf{Z})}{\frac{n}{2} \log P} \tag{27}$$

3) Bounding the difference of entropies: Now, we enhance the system by relaxing the condition that channel inputs from different transmitters are mutually independent, and think of the K single antenna terminals as a single transmitter with K antennas. Thus, we wish to maximize $H(\mathbf{Y}_K) - H(\mathbf{Z})$, where $\mathbf{Y}_K$ and $\mathbf{Z}$ are two single antenna receiver outputs, under the constraint that the channel gains to $\mathbf{Z}$ are unknown at the transmitter. This brings us to the K-user MISO broadcast channel setting of [7]. We know from [7, eqns. (75)-(103)] that even without any security or decodability constraints, the difference of entropies, $H(\mathbf{Y}_K) - H(\mathbf{Z})$ cannot be larger than $no(\log P)$, if the channel gains to the second receiver is unknown. Thus,

$$H(\mathbf{Y}_K) - H(\mathbf{Z}) \leq o(\log P) \tag{28}$$

Using (28) in (27), we have

$$\sum_{i=1}^{K} d_i \leq \frac{K-1}{2} \tag{29}$$

This completes the converse proof of Theorem 1.

V. An Achievable Scheme

For the sake of clarity of exposition, here, we present the achievable scheme for the special case of $K = 3$ instead of the general K-user scheme [6]. We use the technique of asymptotic real interference alignment introduced in [5]. Fig. 2 shows the desired signal alignment at the receivers and the eavesdropper. In the figure, the boxes labeled by V denote the message symbols, while the hatched boxes labeled with U denote artificial noise symbols. It is clear from Fig. 2 that 2 out of 6 *signal dimensions* are buried in the artificial noise. Thus, heuristically, the s.d.o.f. for each legitimate user pair is $\frac{2}{6} = \frac{1}{3}$, and the sum s.d.o.f. is, therefore, $3 \times \frac{1}{3} = 1$, as expected from our optimal sum s.d.o.f. expression $\frac{K-1}{2} = \frac{3-1}{2} = 1$. Let us now present the scheme in more detail.

Let m be a large integer. Also, let c_1, c_2, c_3 and c_4 be real constants drawn from a fixed continuous distribution with bounded support independently of each other and of all

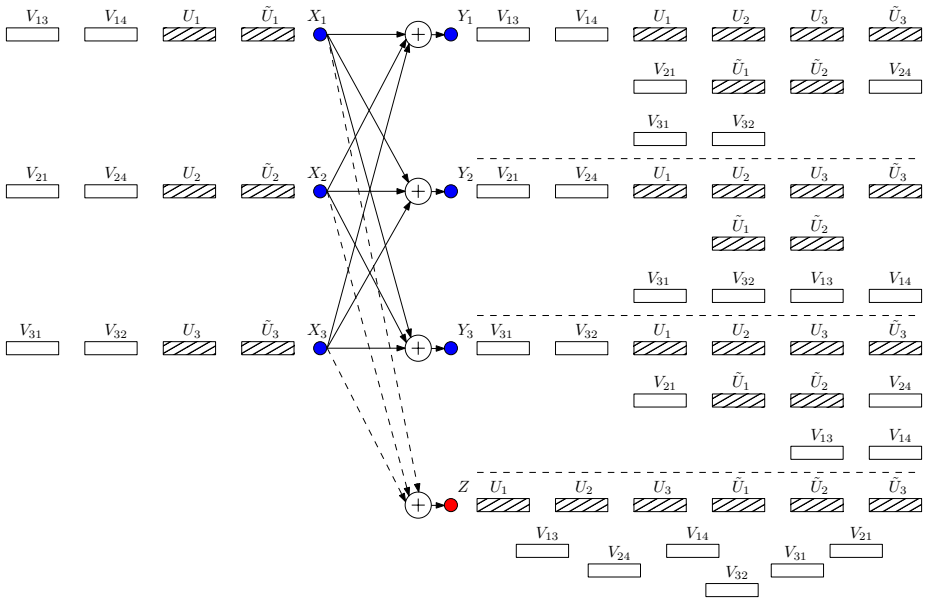

Fig. 2. Alignment for the interference channel for $K = 3$.

the channel gains. This ensures that the c_is are *rationally independent* of each other and of the channel gains almost surely. Now, we define four sets T_i, $i = 1, \ldots, 4$, as follows:

$$T_1 \triangleq \Big\{ h_{11}^{r_{11}} h_{12}^{r_{12}} h_{13}^{r_{13}} h_{21}^{r_{21}} h_{31}^{r_{31}} h_{32}^{r_{32}} h_{23}^{r_{23}} c_1^s : r_{jk}, s \in \{1, \ldots, m\} \Big\} \quad (30)$$

$$T_2 \triangleq \Big\{ h_{21}^{r_{21}} h_{22}^{r_{22}} h_{23}^{r_{23}} \left(\frac{h_{12}}{h_{11}}\right)^{r_{12}} \left(\frac{h_{13}}{h_{11}}\right)^{r_{13}} h_{31}^{r_{31}} h_{32}^{r_{32}} c_2^s : r_{jk}, s \in \{1, \ldots, m\} \Big\} \quad (31)$$

$$T_3 \triangleq \Big\{ h_{31}^{r_{31}} h_{32}^{r_{32}} h_{33}^{r_{33}} \left(\frac{h_{21}}{h_{22}}\right)^{r_{21}} \left(\frac{h_{23}}{h_{22}}\right)^{r_{23}} h_{12}^{r_{12}} h_{13}^{r_{13}} c_3^s : r_{jk}, s \in \{1, \ldots, m\} \Big\} \quad (32)$$

$$T_4 \triangleq \Big\{ h_{31}^{r_{31}} h_{32}^{r_{32}} h_{33}^{r_{33}} h_{21}^{r_{21}} h_{12}^{r_{12}} h_{13}^{r_{13}} h_{23}^{r_{23}} c_4^s : r_{jk}, s \in \{1, \ldots, m\} \Big\} \quad (33)$$

Let M_i be the cardinality of the set T_i. Note that all the M_is are same, which we denote by M:

$$M \triangleq m^8 \quad (34)$$

We subdivide each message W_i into 2 independent sub-messages $V_{ij}, j = 1, \ldots, 4, j \neq i, i+1$. For each transmitter i, let $\mathbf{p}_{ij}$ be the vector containing all the elements of T_j, for $j \neq i, i+1$. For any given (i, j) with $j \neq i, i+1$, $\mathbf{p}_{ij}$ represents the dimension along which message V_{ij} is sent. Further, at each transmitter i, let $\mathbf{q}_i$ and $\tilde{\mathbf{q}}_i$ be vectors containing all the elements in sets T_i and $\beta_i T_{i+1}$, respectively, where $\beta_i = \frac{1}{h_{ii}}$ for $i = 1, 2$ and $\beta_3 = 1$. The vectors $\mathbf{q}_i$ and $\tilde{\mathbf{q}}_i$ represent dimensions along which artificial noise symbols U_i and $\tilde{U}_i$, respectively, are sent. We define a $4M$ dimensional vector $\mathbf{b}_i$ by stacking the $\mathbf{p}_{ij}$s, $\mathbf{q}_i$ and $\tilde{\mathbf{q}}_i$ as

$$\mathbf{b}_i^T = \begin{bmatrix} \mathbf{p}_{i1}^T \cdots \mathbf{p}_{i(i-1)}^T & \mathbf{p}_{i(i+2)}^T \cdots \mathbf{p}_{i4}^T & \mathbf{q}_i^T & \tilde{\mathbf{q}}_i^T \end{bmatrix} \quad (35)$$

The transmitter encodes V_{ij} using an M dimensional vector $\mathbf{v}_{ij}$, and the cooperative jamming signals U_i and $\tilde{U}_i$ using M dimensional vectors $\mathbf{u}_i$ and $\tilde{\mathbf{u}}_i$, respectively. Each element of $\mathbf{v}_{ij}$, $\mathbf{u}_i$ and $\tilde{\mathbf{u}}_i$ are drawn uniformly in an i.i.d. fashion from the PAM constellation $C(a, Q) \triangleq a\{-Q, -Q+1, \ldots, Q-1, Q\}$, where Q is a positive integer and a is a real number, whose values will be specified later. Let

$$\mathbf{a}_i^T = \begin{bmatrix} \mathbf{v}_{i1}^T \cdots \mathbf{v}_{i(i-1)}^T & \mathbf{v}_{i(i+2)}^T \cdots \mathbf{v}_{i4}^T & \mathbf{u}_i^T & \tilde{\mathbf{u}}_i^T \end{bmatrix} \quad (36)$$

The channel input of transmitter i is then given by

$$x_i = \mathbf{a}_i^T \mathbf{b} \quad (37)$$

Let us now analyze the structure of the received signals at the receivers. For example, consider receiver 1. The desired signals at receiver 1, $\mathbf{v}_{13}$ and $\mathbf{v}_{14}$ arrive along dimensions $h_{11}T_3$ and $h_{11}T_4$, respectively. Since only T_i (and not $T_j, j \neq i$) contains c_i, these dimensions are rationally independent. Thus, they appear along different columns in Fig. 2. The artificial noise symbols $\mathbf{u}_1$, $\mathbf{u}_2$, $\mathbf{u}_3$ and $\tilde{\mathbf{u}}_3$ arrive along dimensions $h_{11}T_1$, $h_{21}T_2$, $h_{31}T_3$ and $h_{31}T_4$, respectively. Again they are all rationally separate and thus, appear along different columns in Fig. 2. Further, they are all separate from the dimensions of the desired signals, because T_3 and T_4 do not contain h_{11}, while T_1 and T_2 do not contain either c_3 or c_4. On the other hand, the unintended signals $\mathbf{v}_{21}$ and $\mathbf{v}_{31}$ arrive along $h_{21}T_1$ and $h_{31}T_1$, and since T_1 contains powers of h_{21} and h_{31}, they align with the artificial noise $\mathbf{u}_1$ in $\tilde{T}_1$, where,

$$\tilde{T}_1 \triangleq \Big\{ h_{11}^{r_{11}} h_{12}^{r_{12}} h_{13}^{r_{13}} h_{21}^{r_{21}} h_{31}^{r_{31}} h_{32}^{r_{32}} h_{23}^{r_{23}} c_1^s : r_{jk}, s \in \{1, \ldots, m+1\} \Big\} \quad (38)$$

We define $\tilde{T}_2$, $\tilde{T}_3$ and $\tilde{T}_4$ similarly. We note that the unintended signals $\mathbf{v}_{32}$ and $\mathbf{v}_{24}$ arrive along $h_{31}T_2$ and $h_{21}T_4$ and thus, align with $\mathbf{u}_2$ and $\tilde{\mathbf{u}}_3$, respectively, in $\tilde{T}_2$ and $\tilde{T}_4$. Thus, they appear in the same column in Fig. 2. Finally, the artificial noise symbols $\tilde{\mathbf{u}}_1$ and $\tilde{\mathbf{u}}_2$ align with $\mathbf{u}_2$ and $\mathbf{u}_3$, respectively. A similar analysis is true for receivers 2 and 3 also.

At the eavesdropper, there is no alignment, since the channel gains of the eavesdropper are not known at the transmitters. The artificial noise symbols all arrive along different dimensions at the eavesdropper, exhausting its decoding capability.

We note that the interference at each receiver is confined to the dimensions $\tilde{T}_1$, $\tilde{T}_2$, $\tilde{T}_3$ and $\tilde{T}_4$. Further, these dimensions are separate from the dimensions occupied by the desired signals at each receiver. Thus, the set

$$S = \left(\bigcup_{j \neq i, i+1} h_{ii} T_j \right) \bigcup \left(\bigcup_{j=1}^{4} \tilde{T}_j \right) \tag{39}$$

has cardinality $M_S = 2m^8 + 4(m+1)^8$. Intuitively, out of these M_S dimensions, $2m^8$ dimensions carry the desired signals. Thus, the s.d.o.f. of each legitimate user pair is $\frac{2m^8}{2m^8+4(m+1)^8}$ which approaches $\frac{1}{3}$ as $m \to \infty$. Thus, the sum s.d.o.f. is 1. Further, note that the unintended messages at each receiver are buried in artificial noise, see Fig. 2. Thus, our scheme provides confidentiality of messages from unintended legitimate receivers as well.

More formally, since we have only one eavesdropper, we use [3, Theorem 2] and observe that the rate

$$R_i = I(V_i; Y_i) - I(V_i; Z | V_{-i}) \tag{40}$$

is achievable, where V_i is an auxiliary random variable satisfying $V_i \to X_i \to Y, Z$, and V_{-i} denotes the collection $\{V_j, j \neq i\}$. First, we can upper bound the probability of error at each receiver. Let $V_i \triangleq \left(\mathbf{v}_{i1} \dots \mathbf{v}_{i(i-1)} \quad \mathbf{v}_{i(i+2)} \dots \mathbf{v}_{i4} \right)$. Then, for any $\delta > 0$, there exists a positive constant γ, which is independent of P, such that if we choose $Q = P^{\frac{1-\delta}{2(M_S+\delta)}}$ and $a = \frac{\gamma P^{\frac{1}{2}}}{Q}$, then for almost all channel gains the average power constraint is satisfied and the probability of error is bounded by

$$\Pr(V_i \neq \hat{V}_i) \leq \exp\left(-\eta_{\gamma_i} P^{\delta}\right) \tag{41}$$

where η_{γ_i} is a positive constant which is independent of P and $\hat{V}_i$ is the estimate for V_i obtained by choosing the closest point in the constellation based on observation Y_i.

By Fano's inequality and the Markov chain $V_i \to Y_i \to \hat{V}_i$,

$$I(V_i; Y_i) \geq \frac{2M(1-\delta)}{M_S + \delta} \left(\frac{1}{2} \log P \right) + o(\log P) \tag{42}$$

where $o(\cdot)$ is the little-o function, and M is defined in (34).

Next, letting $U \triangleq \{\mathbf{u}_i, \tilde{\mathbf{u}}_i, i = 1, \dots, 3\}$, we bound the second term in (40) as,

$$\begin{aligned} I(V_i; Z | V_{-i}) =& I(V_i, U; Z | V_{-i}) - I(U; Z | V_1^3) && (43) \\ =& h(Z) - h(Z | U, V_1^3) - H(U | V_1^3) \\ &+ H(U | Z, V_1^3) && (44) \\ \leq& \frac{1}{2} \log P - H(U) + o(\log P) && (45) \\ =& \frac{1}{2} \log P - \frac{(1-\delta)6M}{2(M_S+\delta)} \log P + o(\log P) && (46) \end{aligned}$$

where (45) follows from the fact that U and V_1^3 are independent, and since given V_1^3 and Z, U can be decoded as the $\mathbf{u}_i$s and $\tilde{\mathbf{u}}_i$s occupy independent rational dimensions at the eavesdropper. Now, combining (42) and (46), we have,

$$R_i \geq \frac{(1-\delta)8M - M_S - \delta}{M_S + \delta} \left(\frac{1}{2} \log P \right) + o(\log P) \tag{47}$$

By choosing δ small enough and choosing m large enough, we can make R_i arbitrarily close to $\frac{1}{3}$. Thus, the sum s.d.o.f. of 1 is achievable with $K = 3$ users.

VI. Conclusion

We determined the exact sum s.d.o.f. of the interference channel with an external eavesdropper when there is no eavesdropper CSIT. We proposed a new achievable scheme based on real interference alignment that not only provides security against the external eavesdropper, but also against other unintended legitimate receivers as well. We also provided a matching converse. Our results showed that the lack of eavesdropper's CSIT does not decrease the sum s.d.o.f. significantly, especially when the number of users is large.

References

[1] V. R. Cadambe and S. A. Jafar. Interference alignment and degrees of freedom of the K-user interference channel. *IEEE Transactions on Information Theory*, 54(8):3425–3441, Aug. 2008.

[2] J. Xie and S. Ulukus. Unified secure DoF analysis of K-user Gaussian interference channels. In *IEEE ISIT*, Jul. 2013.

[3] J. Xie and S. Ulukus. Secure degrees of freedom of K-user Gaussian interference channels: A unified view. *IEEE Transactions on Information Theory*, 61(5):2647–2661, May 2015.

[4] A. S. Motahari, S. Oveis-Gharan, and A. K. Khandani. Real interference alignment with real numbers. *IEEE Transactions on Information Theory*, submitted Aug. 2009. Also available at [arXiv:0908.1208].

[5] A. S. Motahari, S. Oveis-Gharan, M. A. Maddah-Ali, and A. K. Khandani. Real interference alignment: Exploiting the potential of single antenna systems. *IEEE Transactions on Information Theory*, 60(8):4799–4810, Aug. 2014.

[6] P. Mukherjee, J. Xie, and S. Ulukus. Secure degrees of freedom of one-hop wireless networks with no eavesdropper CSIT. *IEEE Transactions on Information Theory*, submitted Jun. 2015. Also available at [arXiv:1506.06114].

[7] A. G. Davoodi and S. A. Jafar. Aligned image sets under channel uncertainty: Settling a conjecture by Lapidoth, Shamai and Wigger on the collapse of degrees of freedom under finite precision CSIT. Available at [arXiv:1403.1541].

[8] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor. Interference alignment for secrecy. *IEEE Transactions on Information Theory*, 57(6):3323–3332, Jun. 2011.

[9] J. Xie and S. Ulukus. Secure degrees of freedom of the Gaussian wiretap channel with helpers and no eavesdropper CSI: Blind cooperative jamming. In *CISS*, Mar. 2013.

[10] J. Xie and S. Ulukus. Secure degrees of freedom of one-hop wireless networks. *IEEE Transactions on Information Theory*, 60(6):3359–3378, Jun. 2014.

[11] P. Mukherjee and S. Ulukus. Secure degrees of freedom of the multiple access wiretap channel with no eavesdropper CSI. In *IEEE ISIT*, Jul. 2015.

[12] A. S. Avestimehr, S. N. Diggavi, and D. Tse. Wireless network information flow: A deterministic approach. *IEEE Transactions on Information Theory*, 57(4):1872–1905, Apr. 2011.