Secure Degrees of Freedom of the Multiple Access Wiretap 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 Gaussian multiple access wiretap channel (MAC-WT), where no eavesdropper channel state information (CSI) is available at the transmitters. We show that the exact sum secure degrees of freedom (s.d.o.f.) of this channel model is $\frac{K-1}{K}$. This result shows that, under the condition of no eavesdropper CSI, the MAC-WT acts like a single-transmitter $K-1$ helper wiretap channel. We further show that, when a subset of the transmitters have eavesdropper CSI, then higher sum s.d.o.f. can be achieved, and the system can be operated as a MAC-WT for the users with eavesdropper CSI, with the remaining users acting as helpers. In particular, if m of the K transmitters have eavesdropper CSI, we show that $\frac{m(K-1)}{m(K-1)+1}$ sum s.d.o.f. can be achieved, showing the benefits of having the eavesdropper CSI at the transmitters.**

I. Introduction

We consider the K-user Gaussian multiple access wiretap channel (MAC-WT), where K transmitters wish to have secure communication with a legitimate receiver in the presence of an external eavesdropper; see Fig. 1. We consider a fading channel, where no eavesdropper channel state information (CSI) is available at the transmitters, while each transmitter knows all of the channel gains to the legitimate receivers. This models a practically relevant case, where the legitimate receiver feeds back the CSI to the legitimate transmitters, but the passive eavesdropper does not report any CSI back, while she may be measuring it to use for her own purposes.

The Gaussian MAC-WT channel is introduced in [1], [2], which provide achievable rates using Gaussian signalling and introduce the technique of cooperative jamming to improve these rates. Reference [3] provides outer bounds and identifies cases where these outer bounds are within 0.5 bits per channel use of the rates achievable by Gaussian signalling. The secrecy capacity region of the Gaussian MAC-WT is still unknown. In the absence of an exact secrecy capacity region, recent work focused on identifying secure degrees of freedom (s.d.o.f.) region for this network, which determines the pre-log of achievable secrecy rates at high signal-to-noise ratio (SNR). The achievable rates in [1]–[3] yield zero s.d.o.f.

Reference [4] proposes scaling-based and ergodic alignment techniques to achieve a sum s.d.o.f. of $\frac{K-1}{K}$ for the K-user MAC-WT; thus, showing that an alignment based scheme strictly outperforms i.i.d. Gaussian signaling with or without cooperative jamming at high SNR. Recently, reference [5]

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

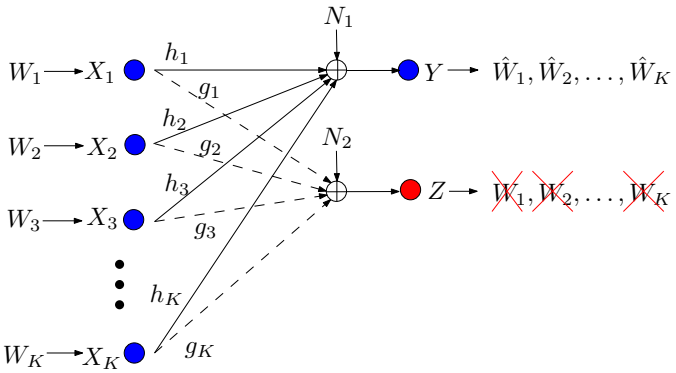

Fig. 1. K-user MAC-WT channel.

shows that the exact sum s.d.o.f. of the K-user MAC-WT is $\frac{K(K-1)}{K(K-1)+1}$. The achievable scheme in [5] is based on real interference alignment [6], channel prefixing via cooperative jamming, and structured signalling. Reference [5] also provides a matching converse via secrecy penalty and role of a helper lemmas. Finally, the exact s.d.o.f. *region* of the K-user MAC-WT is determined in [7].

All of the references mentioned above assume the availability of perfect CSI to all receivers at all transmitters. In this paper, we consider the practically more relevant case where the transmitters have only their own CSI to the legitimate receiver, but no CSI to the eavesdropper. Intuitively, the absence of the CSI of the eavesdropper links at the transmitters may prohibit achieving a desired form of alignment, and may reduce the s.d.o.f. There are examples in the literature in favor of and against this intuition. For instance, in the two-user multiple-input single-output (MISO) broadcast channel with confidential messages (BCCM) with two antennas at the transmitter, if the CSI to both receivers is known, the sum s.d.o.f. is 2, which is achieved by zero-forcing. However, if only one of the CSIs is known, the sum s.d.o.f. is 1, which is achieved by zero-forcing only in one of the directions, which is also the upper bound from the recent converse in [8]. On the other hand, for the case of a wiretap channel with M-helpers, the optimal s.d.o.f. is $\frac{M}{M+1}$ whether the transmitters have the full CSI [5] or no CSI [9] of the eavesdropper channel.

In this paper, our goal is to determine the exact s.d.o.f. of the K-user MAC-WT channel with no eavesdropper CSI, and uncover if there are any s.d.o.f. losses due to lack of eavesdropper CSI. We first note that, we can treat the K-user

MAC-WT as a wiretap channel with $K-1$ helpers, and achieve the $K-1$ helper channel s.d.o.f. Such a scheme achieves $\frac{K-1}{K}$ sum s.d.o.f., which is the optimal s.d.o.f. of the wiretap channel with $K-1$ helpers and no eavesdropper CSI [9]. We develop a converse to show that $\frac{K-1}{K}$ is indeed the largest sum s.d.o.f. that can be achieved in the K-user MAC-WT with no eavesdropper CSI. We note that, with eavesdropper CSI at the transmitters, the optimal sum s.d.o.f. of the K-user MAC-WT channel is $\frac{K(K-1)}{K(K-1)+1}$, which is strictly larger than $\frac{K-1}{K}$. This implies that while with perfect eavesdropper CSI MAC-WT enjoys a larger sum s.d.o.f. than the corresponding helper wiretap channel, with no eavesdropper CSI the MAC-WT reduces to a helper wiretap channel.

Next, we consider the case where a subset of the transmitters have eavesdropper CSI. We show that when m of the K transmitters in the MAC-WT have eavesdropper CSI, a sum s.d.o.f. of $\frac{m(K-1)}{m(K-1)+1}$ is achievable, which is strictly larger than $\frac{K-1}{K}$ when $m>1$. This shows that, even when a portion of the transmitters have eavesdropper CSI, the sum s.d.o.f. of the system can be improved. Finally, our results in this paper together with [9] provide insight into the price we pay when eavesdropper CSI is not available at the transmitters in wiretap networks: while there is no price to be paid in a helper wiretap network, where there is one message to be protected from an eavesdropper [9]; there is significant price to be paid in a MAC-WT network, where there are multiple messages to be protected from an eavesdropper.

II. System Model

The K-user MAC-WT, see Fig. 1, is described by,

$$Y(t)=\sum_{i=1}^{K} h_i(t)X_i(t)+N_1(t) \tag{1}$$

$$Z(t)=\sum_{i=1}^{K} g_i(t)X_i(t)+N_2(t) \tag{2}$$

where $X_i(t)$ denotes the ith user's channel input, $Y(t)$ denotes the legitimate receiver's channel output, and $Z(t)$ denotes the eavesdropper's channel output, at time t. In addition, $N_1(t)$ and $N_2(t)$ are white Gaussian noise variables with zero-mean and unit-variance. Here, $h_i(t)$ and $g_i(t)$ are the channel gains of user i to the legitimate receiver and the eavesdropper, respectively, and they are drawn from an arbitrary but fixed continuous distribution with bounded support in an i.i.d. fashion. The $g_i(t)$s are not known at any of the transmitters. We assume full CSI at the receivers, that is, both receivers know all of the channel gains over n channel uses. All channel inputs satisfy the average power constraint $E[X_i(t)^2]\leq P,\ i=1,\ldots,K$.

Let $\Omega=\{(h_i(t),g_i(t)),\ i=1,\ldots,K,\ t=1,\ldots,n\}$ denote the collection of all channel gains in n channel uses. The ith user transmits message W_i which is uniformly distributed in $\mathcal{W}_i$. 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 receiver, namely, $\Pr[W_i\neq\hat{W}_i]\leq\epsilon_n$, for $i=1,\ldots,K$, and the secrecy constraint, namely,

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

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 $\sum_{i=1}^{K}d_i$.

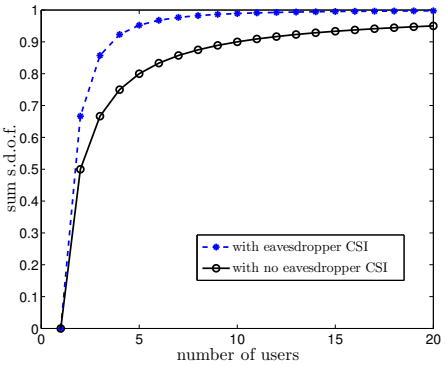

Fig. 2. Loss of s.d.o.f. due to lack of eavesdropper CSI.

III. Main Results

The main result of this paper is the determination of the exact s.d.o.f. region of the MAC-WT channel with no eavesdropper CSI at the transmitters. We first state the sum s.d.o.f. of this channel in the following theorem.

Theorem 1 *For the K-user MAC-WT with no eavesdropper CSI at the transmitters, the optimal sum s.d.o.f. d_s is given by,*

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

We prove Theorem 1 in Section IV. The entire s.d.o.f. region follows from Theorem 1, as stated in the following corollary.

Corollary 1 *The s.d.o.f. region of the K-user MAC-WT with no eavesdropper CSI at the transmitters is given by,*

$$d_i\geq 0,\ i=1,\ldots,K,\quad \textit{and}\quad \sum_{i=1}^{K}d_i\leq\frac{K-1}{K} \tag{5}$$

The proof of Corollary 1 follows directly from the achievability proof of Theorem 1. In particular, the achievable scheme in Theorem 1 treats the K-user MAC-WT as a $K-1$ helper wiretap channel for each user, and achieves the corner points $d_i=\frac{K-1}{K}$ and $d_j=0$ for $j\neq i$, and then time-shares between them. Therefore, given the sum s.d.o.f. upper bound in Theorem 1, and that each corner point with s.d.o.f. of $\frac{K-1}{K}$ for a single user is achievable, the region in Corollary 1 follows.

Fig. 2 shows the optimal sum s.d.o.f. in the presence and absence of eavesdropper CSI at the transmitters for the MAC-WT. The sum s.d.o.f. decreases from $\frac{K(K-1)}{K(K-1)+1}$ to $\frac{K-1}{K}$ when the eavesdropper's CSIT is unavailable. Indeed, in the absence

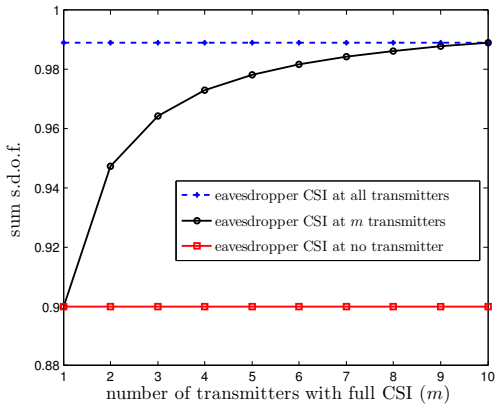

Fig. 3. S.d.o.f. versus the number of users with eavesdropper CSI for $K = 10$.

of eavesdropper CSI, the MAC-WT reduces to a $K-1$ helper channel whose s.d.o.f. is $\frac{K-1}{K}$ with [5] or without [9] eavesdropper CSIT. As K increases, the optimal sum s.d.o.f. approaches 1 as $\sim \frac{1}{K^2}$ with eavesdropper's CSIT but only as $\sim \frac{1}{K}$ without eavesdropper's CSIT.

Next, we consider the intermediate case where some of the transmitters have eavesdropper CSI, and state our achievable s.d.o.f. in the following theorem.

Theorem 2 *In the K-user MAC-WT, where $m \leq K$ transmitters have eavesdropper CSI, and the remaining $K-m$ transmitters have no eavesdropper CSI, the following sum s.d.o.f. is achievable,*

$$d_s = \frac{m(K-1)}{m(K-1)+1} \tag{6}$$

We present the proof of Theorem 2 in Section V. In Fig. 3, we show the achievable sum s.d.o.f. with respect to the number of transmitters, m, which have eavesdropper CSI.

IV. Proof of Theorem 1

A. Achievable Scheme

We first note that it is sufficient to show the achieveability of the s.d.o.f. tuple $(d_1, d_2, \ldots, d_K) = \left(\frac{K-1}{K}, 0, \ldots, 0\right)$. The achievable scheme presented here treats the MAC-WT as a wiretap channel with $K-1$ helpers. It is already known from [9] that the optimal s.d.o.f. of the helper wiretap channel is $\frac{K-1}{K}$. Reference [9] provides an achievable scheme for static (non-time-varying) channels. Here, we provide an achievable scheme for fading (time-varying) channels.

In this scheme, the transmitter (without loss of generality the first transmitter) sends $K-1$ symbols, $\mathbf{V} = \{V_1, \ldots, V_{K-1}\}$ securely to the legitimate receiver in K time slots. Fig. 4 shows the alignment of these signals with the artificial noise for $K = 3$. This is done as follows:

At time $t = 1$, the ith transmitter sends a scaled artificial noise symbol U_i,

$$X_i(1) = \frac{1}{h_i(1)} U_i, \quad i = 1, \ldots, K \tag{7}$$

The channel outputs at time $t = 1$ are,

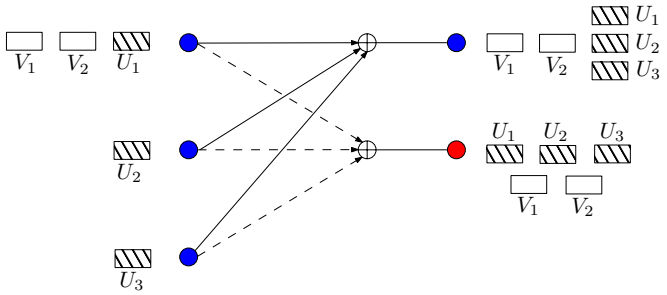

Fig. 4. Alignment of signals when $K = 3$.

$$Y(1) = \sum_{i=1}^{K} U_i \tag{8}$$

$$Z(1) = \sum_{i=1}^{K} \frac{g_i(1)}{h_i(1)} U_i \tag{9}$$

where we neglected the additive Gaussian noise at high SNR.

At times $t = 2, \ldots, K$, the first transmitter sends,

$$X_1(t) = \frac{1}{h_1(t)} \left(V_{t-1} + U_1\right), \quad t = 2, \ldots, K \tag{10}$$

and the ith transmitter, $i = 2, \ldots, K$, sends,

$$X_i(t) = \frac{1}{h_i(t)} U_i, \quad t = 2, \ldots, K \tag{11}$$

The channel outputs at times $t = 2, \ldots, K$ are,

$$Y(t) = V_{t-1} + \sum_{i=1}^{K} U_i \tag{12}$$

$$Z(t) = \frac{g_1(t)}{h_1(t)} V_{t-1} + \sum_{i=1}^{K} \frac{g_i(t)}{h_i(t)} U_i \tag{13}$$

This ensures that the artificial noise symbols align at the legitimate receiver in every time slot. Since, the eavesdropper CSI is unavailable, no alignment is possible at the eavesdropper.

At the end of the K slots, the legitimate receiver recovers $V_t = Y(t+1) - Y(1)$ for $t = 1, \ldots, K-1$ within noise variance. Let $\mathbf{Y} = \{Y(t),\ t = 1, \ldots, K\}$. Then,

$$I(\mathbf{V}; \mathbf{Y}) = (K-1)\frac{1}{2} \log P + o(\log P) \tag{14}$$

We also have,

$$I(\mathbf{V}; \mathbf{Z}) = h(\mathbf{Z}) - h(\mathbf{Z}|\mathbf{V}) \tag{15}$$

$$\leq \frac{K}{2} \log P - \frac{K}{2} \log P + o(\log P) \tag{16}$$

$$= o(\log P) \tag{17}$$

where $\mathbf{Z}$ is defined similar to $\mathbf{Y}$. This means that the leakage to the eavesdropper does not scale with $\log P$. Now consider the vector wiretap channel from $\mathbf{V}$ to $\mathbf{Y}$ and $\mathbf{Z}$, by treating the K slots in the scheme above as one channel use. A single-letter expression for an achievable secure rate for this vector channel is given by [10],

$$R_1 = I(\mathbf{V}; \mathbf{Y}) - I(\mathbf{V}; \mathbf{Z}) \tag{18}$$

$$=(K-1)\frac{1}{2}\log P + o(\log P) \tag{19}$$

Since each channel use of this vector channel uses K actual channel uses, the achievable rate for the actual channel is,

$$R_1 = \frac{(K-1)}{K}\frac{1}{2}\log P + o(\log P) \tag{20}$$

Thus, the achievable s.d.o.f. of this scheme is,

$$d_1 = \frac{K-1}{K} \tag{21}$$

This completes the proof of the achievability of Theorem 1.

B. Converse Proof

We combine techniques from [5] and [8] to prove the converse. 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 $\mathbf{Y}$ and $\mathbf{Z}$ to denote the channel outputs at the legitimate receiver 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 use $\mathbf{X}_{-j}$ to denote all channel inputs from all transmitters except transmitter j, i.e., $\{\mathbf{X}_i,\ i\neq j,\ i=1\ldots,K\}$. We divide the proof into three steps.

1) Deterministic channel model: We show that there is no loss of s.d.o.f. in considering the integer-input integer-output deterministic channel in (22)-(23) instead of the one in (1)-(2),

$$Y(t) = \sum_{i=1}^{K} \lfloor h_i(t)X_i(t)\rfloor \tag{22}$$

$$Z(t) = \sum_{i=1}^{K} \lfloor g_i(t)X_i(t)\rfloor \tag{23}$$

with the constraint that

$$X_i(t) \in \left\{0,1,\ldots,\left\lfloor\sqrt{P}\right\rfloor\right\} \tag{24}$$

Following the proof provided in [8], we note that this channel transformation does not reduce the d.o.f. without secrecy constraints. We only need to show that the deterministic eavesdropper channel in (23) leaks no more information to the eavesdropper than the original eavesdropper channel in (2) from an s.d.o.f. perspective. Consider an integer codeword $\tilde{\mathbf{X}}$ for the deterministic eavesdropper channel in (23). Since $\tilde{\mathbf{X}}$ satisfies the per symbol power constraint of (24), it satisfies the average power constraint of the original channel in (2). The channel output when $\tilde{X}$ is the input of (2), is

$$\tilde{Z}(t) = \sum_{i=1}^{K} g_i(t)\tilde{X}_i(t) + N_2(t) \tag{25}$$

We have,

$$\begin{aligned} I(W_1^K;\mathbf{Z}) \leq& I(W_1^K;\tilde{\mathbf{Z}},\mathbf{Z}) && (26)\\ =& I(W_1^K;\tilde{\mathbf{Z}}) + I(W_1^K;\mathbf{Z}|\tilde{\mathbf{Z}}) && (27)\\ \leq& I(W_1^K;\tilde{\mathbf{Z}}) + H(\mathbf{Z}|\tilde{\mathbf{Z}}) && (28)\\ \leq& I(W_1^K;\tilde{\mathbf{Z}}) + no(\log P) && (29)\end{aligned}$$

where (29) follows since $H(\mathbf{Z}|\tilde{\mathbf{Z}}) \leq no(\log P)$, which can be shown similarly as in [11, Lemma 7.2]. Intuitively, this holds since $\sum_{i=1}^{K} g_i(t)\tilde{X}_i(t) - \sum_{i=1}^{K}\lfloor g_i(t)\tilde{X}_i(t)\rfloor \leq K$ and the power of N_2 does not scale with P. Therefore, the s.d.o.f. of the deterministic channel in (22)-(23) with integer channel inputs as described in (24) is no smaller than the s.d.o.f. of the original channel in (1)-(2). Consequently, any converse developed for the s.d.o.f. of (22)-(23) 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.

Since both receivers know Ω, it appears in the conditioning in every entropy and mutual information term below. We keep this in mind, but drop it for the sake of notational simplicity.

2) An upper bound on the sum rate: We begin as in the secrecy penalty lemma in [5], i.e., [5, Lemma 1]. Note that, unlike [5, Lemma 1], channel inputs are integer here:

$$\begin{aligned} n\sum_{i=1}^{K} R_i \leq& I(W_1^K;\mathbf{Y}|\mathbf{Z}) + n\epsilon && (30)\\ \leq& I(\mathbf{X}_1^K;\mathbf{Y}|\mathbf{Z}) + n\epsilon && (31)\\ \leq& H(\mathbf{Y}|\mathbf{Z}) + n\epsilon && (32)\\ =& H(\mathbf{Y},\mathbf{Z}) - H(\mathbf{Z}) + n\epsilon && (33)\\ \leq& H(\mathbf{X}_1^K,\mathbf{Y},\mathbf{Z}) - H(\mathbf{Z}) + n\epsilon && (34)\\ =& H(\mathbf{X}_1^K) - H(\mathbf{Z}) + n\epsilon && (35)\\ \leq& \sum_{k=1}^{K} H(\mathbf{X}_k) - H(\mathbf{Z}) + n\epsilon && (36)\end{aligned}$$

where (35) follows since $H(\mathbf{Y},\mathbf{Z}|\mathbf{X}_1^K) = 0$ for the channel in (22)-(23). To ensure decodability at the legitimate receiver, we use the role of a helper lemma in [5], i.e., [5, Lemma 2],

$$\begin{aligned} n\sum_{i\neq j} R_i \leq& I(W_{-j};\mathbf{Y}) + n\epsilon' && (37)\\ \leq& I(\mathbf{X}_{-j};\mathbf{Y}) + n\epsilon' && (38)\\ =& H(\mathbf{Y}) - H(\mathbf{Y}|\mathbf{X}_{-j}) + n\epsilon' && (39)\\ =& H(\mathbf{Y}) - H(\mathbf{X}_j) + n\epsilon' && (40)\end{aligned}$$

Eliminating $H(\mathbf{X}_j)$s using (36) and (40), we get,

$$\begin{aligned} Kn\sum_{i=1}^{K} R_i \leq& KH(\mathbf{Y}) - H(\mathbf{Z}) + n\epsilon + nK\epsilon' && (41)\\ \leq& (K-1)\frac{n}{2}\log P + (H(\mathbf{Y}) - H(\mathbf{Z})) + n\epsilon'' && (42)\end{aligned}$$

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

$$\begin{aligned} K\sum_{i=1}^{K} R_i \leq& (K-1)\frac{1}{2}\log P + \epsilon'' \\ &+ \lim_{n\to\infty}\frac{1}{n}\left(H(\mathbf{Y}) - H(\mathbf{Z})\right) && (43)\end{aligned}$$

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

$$\sum_{i=1}^{K} d_i \leq \frac{K-1}{K} + \frac{1}{K}\lim_{P\to\infty}\lim_{n\to\infty}\frac{(H(\mathbf{Y}) - H(\mathbf{Z}))}{\frac{n}{2}\log P} \tag{44}$$

3) Bounding the difference of entropies: We now upper bound the difference of entropies $H(\mathbf{Y})-H(\mathbf{Z})$ in (44) as:

$$H(\mathbf{Y})-H(\mathbf{Z}) \leq \sup_{\{\mathbf{X}_i\}:\mathbf{X}_i \perp\!\!\!\perp \mathbf{X}_j} H(\mathbf{Y})-H(\mathbf{Z}) \quad (45)$$

$$\leq \sup_{\{\mathbf{X}_i\}} H(\mathbf{Y})-H(\mathbf{Z}) \quad (46)$$

where $X \perp\!\!\!\perp Y$ is used to denote that X and Y are statistically independent and (46) follows from (45) by relaxing the condition of independence in (45). Since the $\mathbf{X}_i$s in (46) may be arbitrarily correlated, we can think of the K single antenna terminals as a single transmitter with K antennas. Thus, we wish to maximize $H(\mathbf{Y})-H(\mathbf{Z})$, where $\mathbf{Y}$ 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 [8]. We know from [8, eqns. (75)-(103)] that even without any security or decodability constraints, the difference of entropies, $H(\mathbf{Y})-H(\mathbf{Z})$ cannot be larger than $no(\log P)$, if the channel gains to the second receiver are unknown. Thus,

$$H(\mathbf{Y})-H(\mathbf{Z}) \leq no(\log P) \quad (47)$$

Using (47) in (44), we have

$$\sum_{i=1}^{K} d_i \leq \frac{K-1}{K} \quad (48)$$

This completes the converse proof of Theorem 1.

V. Proof of Theorem 2

We construct a scheme that achieves the desired sum s.d.o.f. Without loss of generality, assume that the first m transmitters have eavesdropper CSI, while the remaining transmitters have no eavesdropper CSI. We provide a scheme to achieve the rate tuple $(d_1,\ldots,d_m,d_{m+1},\ldots,d_K) = \left(\frac{K-1}{m(K-1)+1},\ldots,\frac{K-1}{m(K-1)+1},0,\ldots,0\right)$, thus, achieving the required sum s.d.o.f. of $\frac{m(K-1)}{m(K-1)+1}$. For each $i=1,\ldots,m$, transmitter i sends $\mathbf{V}_i=\{V_{ij},, j\neq i, j=1,\ldots,K\}$ symbols in $m(K-1)+1$ time slots. Let $\mathbf{V}=\{\mathbf{V}_i, i=1,\ldots,K\}$. Fig. 5 illustrates the alignment of the signals at the end of the scheme when $K=3$ and $m=2$. The scheme is as follows:

At time $t\in\{1,\ldots,m(K-1)+1\}$, transmitter i sends,

$$X_i(t)=\begin{cases}\sum_{j=1,j\neq i}^{K}\frac{g_j(t)}{h_j(t)g_i(t)}V_{ij}+\frac{1}{h_i(t)}U_i, & 1\leq i\leq m\\ \frac{1}{h_i(t)}U_i, & m+1\leq i\leq K\end{cases} \quad (49)$$

where U_i is an artificial noise symbol. This ensures that the noise symbols U_i all align at the legitimate receiver. On the other hand, the artificial noise symbol from the jth transmitter U_j protects all the messages V_{ij} for every i, at the eavesdropper. The channel outputs are given by,

$$Y(t)=\sum_{i=1}^{m}\sum_{j\neq i}\frac{h_i(t)g_j(t)}{h_j(t)g_i(t)}V_{ij}+\sum_{i=1}^{K}U_i \quad (50)$$

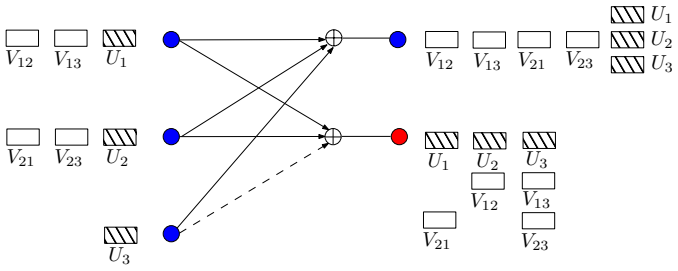

Fig. 5. Alignment of signals when $K=3$ and $m=2$.

$$Z(t)=\sum_{i=1}^{K}\frac{g_i(t)}{h_i(t)}\left(U_i+\sum_{j=1,j\neq i}^{m}V_{ji}\right) \quad (51)$$

After the $m(K-1)+1$ time slots, the legitimate receiver ends up with $m(K-1)+1$ linearly independent equations with $m(K-1)+1$ variables: $\sum_{i=1}^{K}U_i$ and the $m(K-1)$ variables $\{V_{ij}\}$. Thus, it can decode all the $m(K-1)$ message symbols V_{ij} within noise variance. Therefore, defining $\mathbf{Y}$ and $\mathbf{Z}$ similarly as in Section IV-A, we have that $I(\mathbf{V};\mathbf{Y}) = m(K-1)\frac{1}{2}\log P+o(\log P)$. In addition, each $V_{ji}, i\neq j$ is aligned with the artificial noise U_i at the eavesdropper; thus, $I(\mathbf{V};\mathbf{Z})\leq o(\log P)$, concluding the proof of Theorem 2.

VI. Conclusions

We considered the K-user MAC-WT with no eavesdropper CSI and determined its s.d.o.f. region. We showed that in the absence of eavesdropper CSI, the optimal sum s.d.o.f. of the K-user MAC-WT is $\frac{K-1}{K}$, which can be achieved by treating it as a wiretap channel with $K-1$ helpers. In addition, we provided a scheme that achieves a sum s.d.o.f. of $\frac{m(K-1)}{m(K-1)+1}$ when m of the K transmitters have eavesdropper CSI.

References

[1] E. Tekin and A. Yener. The Gaussian multiple access wire-tap channel. *IEEE Trans. Inf. theory*, 54(12):5747–5755, Dec. 2008.

[2] 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, Jun. 2008.

[3] E. Ekrem and S. Ulukus. On the secrecy of multiple access wiretap channel. In *Allerton Conference*, Sept. 2008.

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

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

[6] 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 Trans. Inf. Theory*, 60(8):4799–4810, Aug. 2014.

[7] J. Xie and S. Ulukus. Secure degrees of freedom region of the Gaussian multiple access wiretap channel. In *Asilomar Conference*, Nov. 2013.

[8] 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].

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

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