Achievable Secrecy Rates in the Multiple Access Wiretap Channel with Deviating Users

Karim Banawan Sennur Ulukus
Department of Electrical and Computer Engineering
University of Maryland, College Park, MD 20742
kbanawan@umd.edu *ulukus@umd.edu*

***Abstract*—We consider the multiple access wiretap channel (MAC-WTC), where multiple legitimate users wish to have secure communication with a legitimate receiver in the presence of an eavesdropper. The exact secure degrees of freedom (s.d.o.f.) region of this channel is known. Achieving this region requires users to follow a certain protocol altruistically and transmit both message-carrying and cooperative jamming signals in an optimum manner. In this paper, we consider the case when a subset of users deviate from this optimum protocol. We consider two kinds of deviation: when some of the users stop transmitting cooperative jamming signals, and when a user starts sending intentional jamming signals. For the first scenario, we investigate possible responses of the remaining users to counteract such deviation. For the second scenario, we use an extensive-form game formulation for the interactions of the deviating and well-behaving users. We prove that a deviating user can drive the s.d.o.f. to zero; however, the remaining users can exploit its intentional jamming signals as cooperative jamming signals against the eavesdropper and achieve an optimum s.d.o.f.**

I. Introduction

In the multiple access wiretap channel (MAC-WTC), which is introduced in [1], [2], multiple legitimate users wish to have secure communication with a legitimate receiver in the presence of an eavesdropper. The secrecy capacity region of the MAC-WTC is still unknown, even in the simple Gaussian setting [1]–[7]. In the absence of exact secrecy rates, secure degrees of freedom (s.d.o.f.) provides a first order approximation to the secrecy rate by giving its scaling with $\frac{1}{2}\log P$. Recently, [6] and [7] determined the *exact* sum s.d.o.f. and the entire s.d.o.f. region, respectively, of the MAC-WTC.

The exact sum s.d.o.f. of a K-user MAC-WTC is $\frac{K(K-1)}{K(K-1)+1}$ [6]. The achievability of this sum s.d.o.f. requires all users to send signals in a certain optimum manner. The main tools in the achievability are: structured signalling, channel prefixing, cooperative jamming and interference alignment. An example optimum achievable scheme is shown in Fig. 1 for $K = 4$ users. Here each box shows a signal stream; message-carrying signals are shown by empty boxes and cooperative jamming signals are shown by hatched boxes. In the optimum scheme, each user sends $K-1$ streams of message-carrying signals and 1 stream of cooperative jamming signal. The signals are simultaneously aligned at the two receivers: at the eavesdropper all message-carrying signals are aligned with a cooperative jamming signal, which ensures that the information leakage to the eavesdropper is zero in the s.d.o.f. sense; at the legitimate receiver all cooperative jamming signals are aligned in a single dimension occupying the smallest space, thereby leaving the largest space for message-carrying signals. The total number of dimensions created at the legitimate receiver is $K(K-1)+1$ and 1 dimension is lost for the cooperative jamming signals, hence achieving a sum s.d.o.f. of $\frac{K(K-1)}{K(K-1)+1}$.

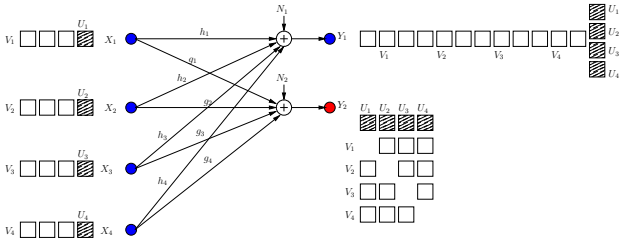

Fig. 1. Optimal achievable scheme for a $K = 4$ user MAC-WTC.

A careful look at the achievable scheme in Fig. 1 reveals that the cooperative jamming signal of each user protects parts of the message-carrying signals of the other users; and that no user can protect its own signals. This creates an interesting ecosystem where each user strictly depends on the rest of the users for its own security. The fact that a user's cooperative jamming transmission does not contribute to its own security, but at the same time uses up its own transmit power, may motivate some selfish users not to send cooperative jamming signals. In this paper, we investigate the effects of such (and worse) deviations from the optimum signalling scheme on the system s.d.o.f., and the actions that the rest of the users can take to compensate for such behavior.

We first consider the case where M out of K users deviate by not transmitting cooperative jamming signals. We start by evaluating the achievable sum s.d.o.f. when the remaining users do not change their original optimum strategies. We show that the sum s.d.o.f. of the system decreases, and deviating users do not benefit from their actions. Then, we consider two possible counter-strategies by the remaining users: In the first strategy, all users decrease their rates to ensure that all message-carrying signals are protected by the remaining cooperative jamming signals, and leakage s.d.o.f. is zero. We show that, interestingly, the individual s.d.o.f. of the deviating users increase, if the remaining users adopt this strategy. Hence, deviating users gain in this case, in the expense of

This work was supported by NSF Grants CNS 13-14733, CCF 14-22111, CCF 14-22129, and CNS 15-26608.

well-behaving users. In the second strategy, we allow the leakage s.d.o.f. to be non-zero, but constrain leakage in a single dimension. We show that, although the sum s.d.o.f. of the system is lower than the case of the first counter-strategy, this strategy decreases the individual s.d.o.f. of the deviating users and increases the s.d.o.f. of well-behaving users.

Next, we consider a more severe form of deviation. While so far we have considered M selfish users stopping to send cooperative jamming signals, next we consider one user turning malicious and sending intentional jamming signals. As this deviating user has infinite power, it can wipe out all communication, secure or otherwise, if it sends Gaussian signals. For the sake of a meaningful formulation, we restrict the strategy set of this deviating user to be of structured signalling and alignment type. Under this restriction, we formulate the problem as an extensive-form game [8]. We show that this deviating user can drive the s.d.o.f. of the system to zero. We then show that, interestingly, the remaining users can utilize these intentional (malicious) jamming signals to protect more message-carrying signals at the eavesdropper, achieving a sum s.d.o.f. of $\frac{(K-1)^2}{(K-1)^2+1}$. We prove that this sum s.d.o.f. matches the sum s.d.o.f. of a $K-1$ user MAC-WTC with 1 external altruistic helper, thereby, show that the system turns a malicious jammer into an altruistic helper, i.e., the deviating user benefits the system against its intensions.

II. System Model

The K-user Gaussian MAC-WTC is given by (see Fig. 1),

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

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

where Y_1, Y_2 are the channel outputs at the legitimate receiver and the eavesdropper, respectively, h_i, g_i are the channel gains from user i to the receiver and the eavesdropper, respectively. User i has a message W_i picked uniformly from the message set $\mathcal{W}_i$, with a rate $R_i = \frac{1}{n}\log|\mathcal{W}_i|$, and sends it in n channel uses using X_i^n reliably and securely, i.e.,

$$\mathbb{P}(\hat{W}_1^K \neq W_1^K) \leq \epsilon, \quad \frac{1}{n} I(W_1^K; Y_2^n) \leq \epsilon \tag{3}$$

where $W_1^K = (W_1, \ldots, W_K)$, and $\hat{W}_1^K = (\hat{W}_1, \ldots, \hat{W}_K)$ are the estimates of the messages at the legitimate receiver. The transmitters are subject to power constraints $\mathbb{E}[X_i^2] \leq P$. The sum s.d.o.f. is given by $d_s = \lim_{P\to\infty} \frac{\sum_{i=1}^{K} R_i}{\frac{1}{2}\log P}$.

In the second part of the paper, we consider a severe form of deviation where one user transmits intentional jamming signals. To distinguish that user and its jamming signal, we denote its channel input as Z, which also is subject to the power constraint $\mathbb{E}[Z^2] \leq P$, and we designate it as the Kth user without loss of generality, see Fig. 5. The malicious user and the remaining users respond to each other in multiple coding frames. The channel inputs/outputs for this model in

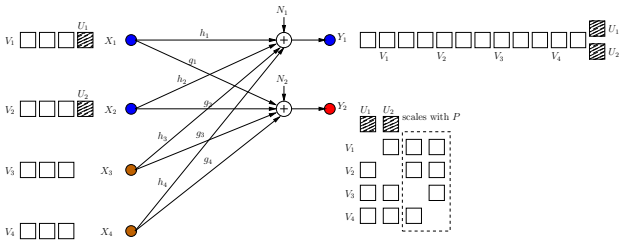

Fig. 2. The remaining users keep their originally optimum schemes.

frame k are:

$$Y_1[k] = \sum_{i=1}^{K-1} h_i X_i[k] + \tilde{h} Z[k] + N_1[k] \tag{4}$$

$$Y_2[k] = \sum_{i=1}^{K-1} g_i X_i[k] + \tilde{g} Z[k] + N_2[k] \tag{5}$$

where $\tilde{h}, \tilde{g}$ are the channel gains from the malicious user to the legitimate receiver and the eavesdropper, respectively.

III. S.d.o.f. When Remaining Users Do Not Respond

Consider that M users have deviated from the optimum strategy in [6] (see Fig. 1) by not sending cooperative jamming signals and that the remaining users have kept their originally optimum strategies, i.e., have not responded to the deviating users (see Fig. 2). That is, the user signals are [6],

$$X_i = \begin{cases} \sum_{j=1, j\neq i}^{K} \frac{g_j}{g_i h_j} V_{ij} + \frac{1}{h_i} U_i, & i = 1, \ldots, K-M \\ \sum_{j=1, j\neq i}^{K} \frac{g_j}{g_i h_j} V_{ij}, & i = K-M+1, \ldots, K \end{cases} \tag{6}$$

where V_{ij}, U_i are picked uniformly from PAM constellation set $C(a, Q)$ [6]. The constants a, Q are chosen as [6]

$$Q = P^{\frac{1-\delta}{2K(K-1)+1+\delta}}, \quad a = \gamma \frac{P^{1/2}}{Q} \tag{7}$$

Consequently, the received signals are (see Fig. 2),

$$Y_1 = \sum_{i=1}^{K} \sum_{j=1, j\neq i}^{K} \frac{g_j h_i}{g_j h_j} V_{ij} + \sum_{k=1}^{K-M} U_k + N_1 \tag{8}$$

$$Y_2 = \sum_{i=1}^{K} \sum_{j=1, j\neq i}^{K} \frac{g_j}{h_j} V_{ij} + \sum_{j=1}^{K-M} \frac{g_j}{h_j} U_j + N_2 \tag{9}$$

$$= \sum_{j=1}^{K-M} \frac{g_j}{h_j} \left(U_j + \sum_{i=1, i\neq j}^{K} V_{ij} \right) + \sum_{j=K-M+1}^{K} \sum_{i=1, i\neq j}^{K} \frac{g_j}{h_j} V_{ij} + N_2 \tag{10}$$

Let $\mathbf{V} = \{V_{ij} : i, j = 1, \ldots K, i \neq j\}$. From [5], [6], the following secure rates are achievable,

$$\sum_{i=1}^{K} R_i \geq I(\mathbf{V}; Y_1) - I(\mathbf{V}; Y_2) \tag{11}$$

For the first term $I(\mathbf{V}; Y_1)$: we note that the components of vector $\mathbf{V}$ are received in different rational dimensions, and

hence we have $(2Q+1)^{K(K-1)}$ separable constellation points, while the cooperative jamming signal components are aligned in the same rational dimension, i.e., $(2(K-M)Q+1)$ constellation points. From data processing and Fano's inequalities,

$$I(\mathbf{V};Y_1) \geq I(\mathbf{V};\hat{\mathbf{V}}) = H(\mathbf{V}) - H(\mathbf{V}|\hat{\mathbf{V}}) \tag{12}$$
$$\geq [1-\exp(\eta_\gamma P^\delta)]\log(2Q+1)^{K(K-1)} - 1 \tag{13}$$
$$= \frac{K(K-1)(1-\delta)}{K(K-1)+1+\delta}\cdot\frac{1}{2}\log P + o(\log P) \tag{14}$$

For the second term $I(\mathbf{V};Y_2)$: we note that we have $K-M$ dimensions, in which message-carrying signals are aligned with cooperative jamming signals, while M dimensions lack cooperative jamming signals, i.e., we have $(2KQ+1)^{K-M}\cdot(2(K-1)Q+1)^M$ constellation points. Hence,

$$I(\mathbf{V};Y_2) \leq H(Y_2-N_2) - H(Y_2-N_2|\mathbf{V}) \tag{15}$$
$$\leq \log(2KQ+1)^{K-M}(2(K-1)Q+1)^M) - \log(2Q+1)^{K-M} \tag{16}$$
$$= (K-M)\log\frac{2KQ+1}{2Q+1} + M\log(2(K-1)Q+1) \tag{17}$$
$$\leq (K-M)\log K + \frac{M(1-\delta)}{K(K-1)+1+\delta}\cdot\frac{1}{2}\log P + o(\log P) \tag{18}$$
$$= \frac{M(1-\delta)}{K(K-1)+1+\delta}\cdot\frac{1}{2}\log P + o(\log P) \tag{19}$$

Substituting (14) and (19) into (11), and taking the limit as $P\to\infty$, the achievable sum s.d.o.f. is,

$$d_s \geq \frac{K(K-1)-M}{K(K-1)+1} \tag{20}$$

That is, the sum s.d.o.f. decreases by $\frac{M}{K(K-1)+1}$ from the optimal in [6]. This affects all users, including the deviating users, hence they do not benefit from their deviation.

IV. S.D.O.F. When Remaining Users Respond

In this section, we consider two achievable schemes resulting from two different responses of the remaining users.

A. Reducing the Secure Rate for Zero Leakage Rate

In this achievable scheme, all users decrease their secure rates, i.e., decrease the number of message-carrying signal components to ensure that all of them are aligned with cooperative jamming signals. Specifically, the first $K-M$ users send $K-M-1$ message-carrying signals and 1 cooperative jamming signal, while the rest of the users, i.e., the deviating users, send $K-M$ message-carrying signals and no cooperative jamming signals, see Fig. 3. Note that the deviating users are motivated to decrease their message-carrying signals from $K-1$ to $K-M$, as otherwise, some of their message-carrying signals would not be protected. The transmitted signals are,

$$X_i = \begin{cases} \sum_{j=1,j\neq i}^{K-M}\frac{g_j}{g_i h_j}V_{ij} + \frac{1}{h_i}U_i, & i=1,\ldots,K-M \\ \sum_{j=1}^{K-M}\frac{g_j}{g_i h_j}V_{ij}, & i=K-M+1,\ldots,K \end{cases} \tag{21}$$

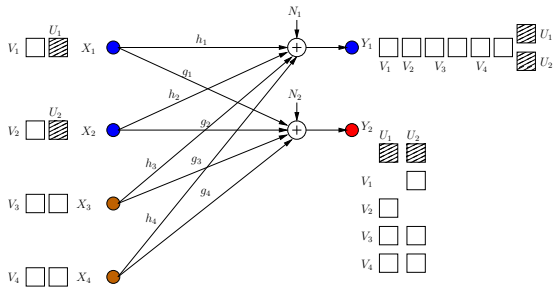

Fig. 3. All users reduce rates to have zero leakage s.d.o.f.

Consequently, the received signals are (see Fig. 3),

$$Y_1 = \sum_{i=1}^{K-M}\sum_{j=1,j\neq i}^{K-M}\frac{g_j h_i}{g_j h_j}V_{ij} + \sum_{i=K-M+1}^{K}\sum_{j=1}^{K-M}\frac{g_j h_i}{g_j h_j}V_{ij} + \sum_{k=1}^{K-M}U_k + N_1 \tag{22}$$

$$Y_2 = \sum_{i=1}^{K-M}\sum_{j=1,j\neq i}^{K-M}\frac{g_j}{h_j}V_{ij} + \sum_{i=K-M+1}^{K-M}\sum_{j=1}^{K-M}\frac{g_j}{h_j}V_{ij} + \sum_{j=1}^{K-M}\frac{g_j}{h_j}U_j + N_2 \tag{23}$$
$$= \sum_{j=1}^{K-M}\frac{g_j}{h_j}\left(U_j + \sum_{i=1,i\neq j}^{K-M}V_{ij} + \sum_{i=K-M+1}^{K}V_{ij}\right) + N_2 \tag{24}$$

Let $\mathbf{V} = \{V_{ij} : i=1,\ldots K, j=1,\ldots,K-M, i\neq j\}$. We evaluate the secrecy rates using (11), after choosing,

$$Q = P^{\frac{1-\delta}{2(K-M)(K-1)+1+\delta}}, \quad a = \gamma\frac{P^{1/2}}{Q} \tag{25}$$

The components of $\mathbf{V}$ are received in different dimensions, and hence we have $(2Q+1)^{(K-M)(K-M-1)+M(K-M)} = (2Q+1)^{(K-M)(K-1)}$ separable constellation points, while the cooperative jamming signals are aligned in the same dimension, i.e., $(2(K-M)Q+1)$ constellation points. Thus,

$$I(\mathbf{V};Y_1) \geq I(\mathbf{V};\hat{\mathbf{V}}) \tag{26}$$
$$= \frac{(K-M)(K-1)(1-\delta)}{(K-M)(K-1)+1+\delta}\cdot\frac{1}{2}\log P + o(\log P) \tag{27}$$

Since all message-carrying signals are jammed by cooperative jamming signals, we have $K-M$ dimensions with $(2KQ+1)^{(K-M)}$ overlapping constellation points. Thus,

$$I(\mathbf{V};Y_2) \leq H(Y_2-N_2) - H(Y_2-N_2|\mathbf{V}) \tag{28}$$
$$= H\left(\sum_{j=1}^{K-M}\frac{g_j}{h_j}\left(U_j + \sum_{i=1,i\neq j}^{K-M}V_{ij} + \sum_{i=K-M+1}^{K}V_{ij}\right)\right) - H\left(\sum_{j=1}^{K-M}\frac{g_j}{h_j}U_j\right) \tag{29}$$

$$=(K-M)\log\frac{2KQ+1}{2Q+1} \tag{30}$$

$$\leq(K-M)\log K \tag{31}$$

Substituting (27) and (31) into (11), and taking the limit as $P\to\infty$, the achievable sum s.d.o.f. is,

$$d_s \geq \frac{(K-M)(K-1)}{(K-M)(K-1)+1} \tag{32}$$

The resultant sum s.d.o.f. is less than the optimal in [6]. However, interestingly, the individual s.d.o.f. of each deviating user is $\frac{K-M}{(K-M)(K-1)+1}$, which is larger than its s.d.o.f. without deviation $\frac{K-1}{K(K-1)+1}$, so long as $M\leq K-1+\frac{1}{K}$, i.e., if at least one user sticks to the optimal strategy in [6].

B. Reducing the Leakage to a Single Dimension

In this achievable scheme, we allow one rational dimension to be leaked. This dimension is not secured by a cooperative jamming signal. This results in the ability of injecting an extra message-carrying signal component for each user. All these extra signals are aligned in the same rational dimension at the eavesdropper. The transmitted signals are (see Fig. 4),

$$X_i=\begin{cases}\sum_{j=1,j\neq i}^{K-M}\frac{g_j}{g_ih_j}V_{ij}+\frac{\alpha}{h_i}V_{i0}+\frac{1}{h_i}U_i, i=1,\ldots,K-M\\ \sum_{j=1}^{K-M}\frac{g_j}{g_ih_j}V_{ij}+\frac{\alpha}{h_i}V_{i0}, \quad i=K-M+1,\ldots,K\end{cases} \tag{33}$$

where α is rationally independent from all channel gains. The received signals are shown in Fig. 4. By similar steps, we have the following s.d.o.f. for this scheme,

$$d_s \geq \frac{(K-M)^2+M(K-M+1)-1}{(K-M)^2+M(K-M+1)+1} \tag{34}$$

Although the sum s.d.o.f. in this case is smaller than in (32), the individual s.d.o.f. of a well-behaving user is higher and a deviating user is lower than in (32).

V. Malicious Deviation: Intentional Jamming

In this section, we consider a more severe form of deviation, where a user (say the Kth user) sends intentional jamming signals. The deviating (malicious) user is restricted to use structured signals. In this section, we show that, when the malicious user acts, it can drive the sum s.d.o.f. to zero. However, when the remaining users respond, the sum s.d.o.f. is raised to $d_s=\frac{(K-1)^2}{(K-1)^2+1}$, which is the sum s.d.o.f. of a $K-1$ user MAC-WTC with an external altruistic helper.

A. When the Jammer Responds to the Users

In any encoding frame, each user sends its message-carrying signals V_{ij} on N rationally independent dimensions α_{ij} as,

$$X_i[k]=\sum_{j=1}^{N}\alpha_{ij}V_{ij} \tag{35}$$

Then, the jammer designs structured jamming signals $\tilde{U}_{ij}$ as a response to users' signals as,

$$Z[k]=\sum_{i=1}^{K-1}\sum_{j=1}^{N}\frac{\alpha_{ij}h_i}{\tilde{h}}\tilde{U}_{ij} \tag{36}$$

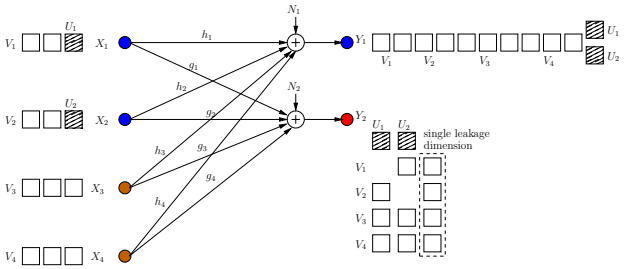

Fig. 4. All users reduce the leakage dimension to 1.

Consequently, the received signal at the legitimate receiver is,

$$Y_1[k]=\sum_{i=1}^{K-1}\sum_{j=1}^{N}h_i\alpha_{ij}(V_{ij}+\tilde{U}_{ij})+N_1[k] \tag{37}$$

Hence, each message-carrying signal is aligned with a jamming signal. Let $\mathbf{V}[k]=[V_{ij},i=1,\ldots,K-1,j=1,\ldots,N]^T$ to be vectorization of all secure signal components. Then, the secure rate is upper bounded as,

$$\sum_{i=1}^{K-1}R_i\leq I(\mathbf{V}[k];Y_1[k]-N_1[k]) \tag{38}$$

$$=\sum_{i=1}^{K-1}\sum_{j=1}^{N}H(V_{ij}+\tilde{U}_{ij})-H(\tilde{U}_{ij}) \tag{39}$$

$$\leq\sum_{i=1}^{K-1}\sum_{j=1}^{N}\log(4Q+1)-\log(2Q+1) \tag{40}$$

$$\leq N(K-1)=o(\log P) \tag{41}$$

Hence $d_s=0$, i.e., whenever the jammer knows the signalling scheme of the users, it nulls the communication by jamming.

B. When the Users Respond to the Jammer

Since structured jamming signalling suffices to jam the system, the jammer sends structured signals in N dimensions,

$$Z[k]=\sum_{j=1}^{N}\alpha_j\tilde{U}_j \tag{42}$$

Users make use of the generated jamming signals to hide extra secure signals from the eavesdropper. Users send,

$$X_i[k]=\sum_{j=1}^{N}\sum_{l=1,l\neq i}^{K-1}\frac{\alpha_j\tilde{h}g_l}{g_ih_i}V_{ijl}+\sum_{j=1}^{N}\frac{\alpha_j\tilde{g}}{g_i}V_{ij0}+\sum_{j=1}^{N}\frac{\alpha_j\tilde{h}}{h_i}U_{ij} \tag{43}$$

where V_{ijl},V_{ij0} are the message-carrying signals which are protected by cooperative jamming signals generated by other users, and the jamming signals generated by the malicious user, respectively. Then, the received signal at receiver 1 is,

$$Y_1[k]=\sum_{j=1}^{N}\left(\sum_{i=1}^{K-1}\sum_{l=1,l\neq i}^{K-1}\frac{\alpha_j\tilde{h}g_lh_i}{g_i}V_{ijl}+\sum_{i=1}^{K-1}\frac{\alpha_j\tilde{g}h_i}{g_i}V_{ij0}+\alpha_j\tilde{h}\left(\tilde{U}_j+\sum_{i=1}^{K-1}U_{ij}\right)\right)+N_1 \tag{44}$$

i.e., users' jamming signals use the same dimensions as the external jammer to inject extra cooperative jamming signals. The received signal at the eavesdropper is,

$$Y_2[k] = \sum_{i=1}^{K-1} g_i \left[\sum_{j=1}^{N} \sum_{l=1, l\neq i}^{K-1} \frac{\alpha_j \tilde{h} g_l}{g_i h_i} V_{ijl} + \sum_{j=1}^{N} \frac{\alpha_j \tilde{g}}{g_i} V_{ij0} + \sum_{j=1}^{N} \frac{\alpha_j \tilde{h}}{h_i} U_{ij} \right] + \tilde{g} \sum_{j=1}^{N} \alpha_j \tilde{U}_j + N_2 \quad (45)$$

$$= \sum_{j=1}^{N} \left[\alpha_j \tilde{g} \left(\sum_{i=1}^{K-1} V_{ij0} + \tilde{U}_j \right) + \sum_{l=1}^{K-1} \frac{\alpha_j \tilde{h} g_l}{h_l} \left(U_{ij} + \sum_{i=1, i\neq l}^{K-1} V_{lji} \right) \right] \quad (46)$$

i.e., all message-carrying signals are protected from the eavesdropper, as in Fig. 5, with $K = 4$, $N = 1$.

We note that the received signals at receiver Y_1 consists of $(2Q+1)^{N(K-1)(K-2)+N(K-1)}(2NKQ+1)$ constellation points in $N((K-1)^2+1)$ dimensions. Each user is transmitting using PAM constellation $C(a, Q)$. By choosing $Q = P^{\frac{1-\delta}{2N((K-1)^2+1)+\delta}}$ and $a = \gamma P^{\frac{1}{2}}/Q$, we have

$$I(\mathbf{V}; Y_1[k]) \geq \frac{N(K-1)^2(1-\delta)}{N((K-1)^2+1)+\delta} \left(\frac{1}{2} \log P \right) + o(\log P) \quad (47)$$

Further, since every message-carrying signal is protected by a cooperative jamming signal, $I(\mathbf{V}; Y_2[k]) \leq o(\log P)$. Thus, the achievable sum s.d.o.f. with one malicious jammer when users respond is $d_s(k) = \frac{(K-1)^2}{(K-1)^2+1}$. Finally, in the Appendix, we determine the sum s.d.o.f. of a K-user MAC-WTC with M external altruistic helpers, as a result on its own. We note that this $d_s(k)$ is in fact equal to the sum s.d.o.f. of a $K-1$ user MAC-WTC with 1 external helper, concluding that the users' action to the jammer is optimal, as they achieve the s.d.o.f. of the case of an altruistic helper with a malicious jammer.

APPENDIX
K-USER MAC-WTC WITH M EXTERNAL HELPERS

Theorem 1 *The s.d.o.f. of the K-user Gaussian MAC-WTC with M-external helpers is given by $d_s = \frac{K(K+M-1)}{K(K+M-1)+1}$.*

Proof: We give only a sketch of a proof here due to space limitations. For the achievability, each user sends $K+M-1$ message-carrying signals and one cooperative jamming signal to secure the other users. Each helper sends one cooperative jamming signal. The cooperative jamming signals are aligned in the same rational dimension at the receiver.

For the converse, we rely on the techniques in [6]. First, we have the following upper bound which represents the *secrecy penalty* due to the secrecy constraint on the eavesdropper,

$$n \sum_{i=1}^{K} R_i \leq \sum_{l=2}^{K} h(\tilde{\mathbf{X}}_l) + \sum_{j=1}^{M} h(\tilde{\mathbf{Z}}_j) + nc_1 \quad (48)$$

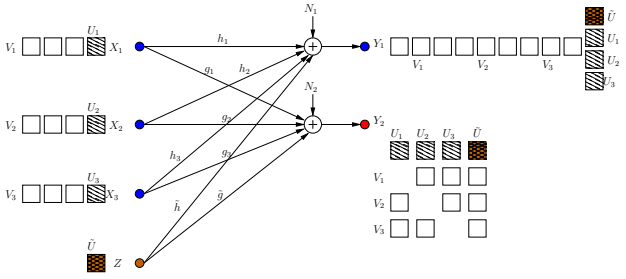

Fig. 5. A malicious jamming user: users' response.

where $\tilde{\mathbf{X}}_i, \tilde{\mathbf{Z}}_j$ are the perturbed inputs of user i and helper j, respectively. Next, we have the *role of the external helper(s)*,

$$\sum_{j=1}^{M} h(\tilde{\mathbf{Z}}_j) \leq Mh(\mathbf{Y}_1) - nM \sum_{i=1}^{K} R_i + nc_2 \quad (49)$$

By considering the rates of all users except one for the $K-1$ users, we have *role of the internal helper(s)*,

$$\sum_{l=2}^{K} h(\tilde{\mathbf{X}}_l) \leq (K-1)h(\mathbf{Y}_1) - n \sum_{l=2}^{K} \sum_{i\neq l} R_i + nc_3 \quad (50)$$

We substitute (49) and (50) in (48) to have,

$$n\big(R_1 + (M+K-1) \sum_{i=1}^{K} R_i\big) \leq (M+K-1)h(\mathbf{Y}_1) + nc_4 \quad (51)$$

We have written (48) by eliminating the first user's channel input, hence the summation starting at $i = 2$. This inequality holds when any other user's channel input is chosen. Writing (48) for all K users, and adding the K corresponding bounds,

$$n(K(K+M-1)+1) \sum_{i=1}^{K} R_i \leq K(K+M-1) \left(\frac{n}{2} \log P \right) + nc_5 \quad (52)$$

Taking the limit as $P \to \infty$, we have $d_s \leq \frac{K(K+M-1)}{K(K+M-1)+1}$. ■

Note that this result is related to the s.d.o.f. region result in [7] for the $K+M$ user MAC-WTC, when we focus on the hyperplane corresponding to zero s.d.o.f. for M of the users; these M users essentially serve as helpers.

REFERENCES

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

[2] E. Tekin and A. Yener. The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming. *IEEE Trans. on Info. Theory*, 54(6):2735–2751, June 2008.

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

[4] H. Ge, R. Xu, and R. A. Berry. Secure signaling games for Gaussian multiple access wiretap channels. In *IEEE ISIT*, June 2015.

[5] G. Bagherikaram, A. S. Motahari, and A. K. Khandani. On the secure DoF of the single-antenna MAC. In *IEEE ISIT*, June 2010.

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

[7] J. Xie and S. Ulukus. Secure degrees of freedom regions of multiple access and interference channels: The polytope structure. *IEEE Trans. on Info. Theory*, 62(4):2044–2069, April 2016.

[8] S. Tadelis. *Game Theory: An Introduction*. Princeton Univ. Press, 2013.