entropy

MDPI

Article

Secure Degrees of Freedom in Networks with User Misbehavior

Karim Banawan [1] and Sennur Ulukus [2,*]

[1] Faculty of Engineering, Alexandria University, Alexandria 21544, Egypt; kbanawan@alexu.edu.eg
[2] Department of ECE, University of Maryland, College Park, MD 20742, USA
* Correspondence: ulukus@umd.edu; Tel.: +1-301-405-4909

Received: 18 July 2019; Accepted: 14 September 2019; Published: 26 September 2019

Abstract: We investigate the secure degrees of freedom (s.d.o.f.) of three new channel models: broadcast channel with combating helpers, interference channel with selfish users, and multiple access wiretap channel with deviating users. The goal of introducing these channel models is to investigate various malicious interactions that arise in networks, including active adversaries. That is in contrast with the common assumption in the literature that the users follow a certain protocol altruistically and transmit both message-carrying and cooperative jamming signals in an optimum manner. In the first model, over a classical broadcast channel with confidential messages (BCCM), there are two helpers, each associated with one of the receivers. In the second model, over a classical interference channel with confidential messages (ICCM), there is a helper and users are selfish. By casting each problem as an extensive-form game and applying recursive real interference alignment, we show that, for the first model, the combating intentions of the helpers are neutralized and the full s.d.o.f. is retained; for the second model, selfishness precludes secure communication and no s.d.o.f. is achieved. In the third model, 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. We consider the case when a subset of users deviate from the optimum protocol that attains the exact s.d.o.f. of this channel. 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.

Keywords: secure degrees of freedom; interference alignment; extensive-form games

1. Introduction

Physical layer security techniques allow secure transmission of information (in absolute sense) without the need for encryption keys [1]. Consequently, the problems of exchanging encryption keys across open wireless networks are mitigated. In the seminal work [2], Wyner showed that secure communication through a degraded wiretap channel is possible by exploiting the noisy nature of the channel. The problem was extended to general wiretap channel, which may not be necessarily degraded by Csiszar and Korner in [3]. The physical layer security framework was then extended to various multiuser settings such as: the multiple access wiretap channel (MAC-WTC) [4], broadcast channel with confidential messages (BCCM) [5–9], interference channel with confidential messages (ICCM) [5], multireceiver wiretap channels [10,11], and relay-eavesdropper channels [12]. In the

absence of exact secrecy rates, secure degrees of freedom (s.d.o.f.) provide a first order approximation to the secrecy rate by giving their scaling with $\frac{1}{2}\log P$, where P is the total average transmitted power. The s.d.o.f. have been considered in the literature in many multiuser channel models, such as helper wiretap channel [13,14], multiple-access wiretap channel [13,15–17], interference channel [13,17–22], X-channel [23,24], half-duplex relay channel [25], compound wiretap channel [26], diamond channel [27], MIMO wiretap Y channel [28], multiuser channel models under imperfect CSIT [29–33]. An investigation of the intercept probability in the presence of eavesdropping attack and interference can be found in [34].

In this work, we investigate extended versions of BCCM, ICCM, and MAC-WTC channel models. Information-theoretic security for discrete memoryless interference and broadcast channels with confidential messages were studied in [5]. BCCM consists of a transmitter and two receivers. The transmitter has two messages, each directed to one of the receivers and needing to be kept secure from the other receiver. The s.d.o.f. of Gaussian BCCM is zero for each user [13]. However, with an altruistic system helper, each user in the BCCM can have an s.d.o.f. of $1/2$ [13]. ICCM consists of two transmitters and two receivers. Each transmitter has a message that needs to be conveyed reliably to one of the receivers and needs to be kept secret from the other receiver. The s.d.o.f. of Gaussian ICCM is $1/3$ for each user [13]. With an altruistic system helper, each user in the ICCM can have an s.d.o.f. of $1/2$ [13]. In both of these systems, this eventual $1/2$ s.d.o.f. per user requires perfect coordination between the transmitters and the helper, even if that obliges the transmitters to jam their own receivers as in the case of ICCM.

In MAC-WTC, which was introduced in [4,35], 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 [4,13,15,17,35–37]. Recently, [13] and [17] 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 $\frac{K(K-1)}{K(K-1)+1}$ [13]. 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 signaling, channel prefixing, cooperative jamming, and interference alignment. 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 one dimension is lost for the cooperative jamming signals, hence achieving a sum s.d.o.f. of $\frac{K(K-1)}{K(K-1)+1}$.

All these works assume that all nodes are *altruistic* and follow a prescribed transmission policy in order to maximize the sum secure rate of the entire system. In this paper, we investigate BCCM, ICCM, and MAC-WTC channel models in the case of selfish and malicious behavior, where the users/helpers do not perform the system-wide-optimal altruistic behavior but apply a selfish strategy and/or take sides by aiming to help one user and potentially hurt the other. These new models are extensions of the ones studied in [4,5,13] and are a step forward in studying channel models with active adversaries. We use s.d.o.f. metric to quantify the effects of these malicious behaviors. For BCCM and ICCM channel models, we note a self-enforcing property: Even with the excessive capabilities of the helpers/users (infinite power and all-knowing entities), these capabilities are naturally restricted in these channel models due to the users'/helpers' interest in reliable communication to/with their own receivers. That is, no entity can use infinite powered Gaussian jamming signals which would wipe out the communication for everybody. This self-enforcing property necessitates users to apply selective jamming via interference alignment. This motivates studying such jamming techniques and analyzing their effect on the s.d.o.f. of the users. In addition, a careful look at the achievable scheme for the MAC-WTC in [13] 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 work, we investigate the effects of such (and worse) deviations from the optimum signaling scheme on the system s.d.o.f., and the actions that the rest of the users can take to compensate for such behavior.

In the first model, which is the *BCCM with combating helpers*, there are two helpers, where each helper takes the side of one of the receivers and at the same time aims to hurt the secure communication to the other receiver. The two helpers have contradicting objectives and hence are combating. Helpers in this model do not coordinate with the transmitter as in [13]. We use a stringent objective function for each helper: Each helper minimizes the s.d.o.f. of the other receiver, while not decreasing the s.d.o.f. of its own receiver by its action. We formulate the problem as an extensive-form game [38], which is a sequential strategic game, where every player (node) acts according to its information about the other nodes' actions in previous transmission frames. We investigate achievable schemes that use real interference alignment [39] in a recursive way. We prove that under this stringent objective function and recursive real interference alignment, the malicious behaviors of the two combating helpers are neutralized, and the s.d.o.f. for each user converges to the optimal s.d.o.f. of $1/2$ per user [13], as if both helpers are altruistic.

In the second model, which is the *ICCM with selfish users*, there is an external system helper. In this model, the users do not coordinate as in the optimal strategy in [13] instructs. The users are selfish and want to hurt the other receiver; each transmitter's goal is to maximize the difference of the s.d.o.f. between the two receivers. This permits each user to jam its own receiver if this hurts the other receiver more, making self-jamming more natural here than the optimum scheme in [13]. There is a neutral helper in this system which aims to maximize the s.d.o.f. of the system. Using the extensive-form game formulation and recursive real interference alignment, we show that the selfishness of the users precludes any secure communication and drives the s.d.o.f. of both users to zero, despite the existence of a mediating helper.

In the third model, which is the *MAC-WTC with deviating users*, 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 counterstrategies 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, in this case, the individual s.d.o.f. of the deviating users increase. Hence, deviating users gain at the expense of well-behaving users. In the second strategy, we allow the leakage s.d.o.f. to be nonzero but constrain leakage in a single dimension. We show that, although the sum s.d.o.f. of the system is lower than in the case of the first counterstrategy, 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 by considering 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 signaling and alignment type. Under this restriction, we formulate the problem as an extensive-form game [38]. 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 showing that the system turns a malicious jammer into an altruistic helper, i.e., the deviating user benefits the system against its intentions.

Organization: In Section 2 , we focus on the BCCM with combating helpers. In Section 3, we consider the ICCM with selfish users. Finally, in Section 4, we consider the MAC-WTC with deviating users. For each model, we first give the formal description of the channel model, then we present our proposed achievable schemes.

2. BCCM with Combating Helpers

2.1. System Model and Assumptions

In BCCM, the transmitter has two private messages W_1 and W_2 picked from the message sets $\mathcal{W}_1, \mathcal{W}_2$ uniformly with rates R_1, R_2, respectively, where $R_i = \frac{1}{n}\log|\mathcal{W}_i|$, where n is the length of the codeword. Each message W_i should be received reliably by the ith receiver, while being kept secure from the jth receiver, $i \neq j$:

$$\mathbb{P}(\hat{W}_1 \neq W_1) \leq \epsilon, \quad \mathbb{P}(\hat{W}_2 \neq W_2) \leq \epsilon \tag{1}$$

$$\frac{1}{n}I(W_2; Y_1^n) \leq \epsilon, \quad \frac{1}{n}I(W_1; Y_2^n) \leq \epsilon \tag{2}$$

where $I(X;Y)$ is the mutual information between the random variables, X and Y, and $\hat{W}_i$ is the estimate of W_i at the ith receiver. The s.d.o.f. d_i is defined as $d_i = \lim_{P\to\infty} \frac{R_i}{\frac{1}{2}\log P}$, where P is the transmitter power constraint $\mathbb{E}[X^2] \leq P$.

The system has two helpers with inputs Z_1 and Z_2, with the power constraints $\mathbb{E}[Z_i^2] \leq P$. Each helper assists secure transmission to *one* of the receivers. The input/output relations for the BCCM with combating helpers (see Figure 1) are:

$$Y_1[k] = hX[k] + \tilde{h}_1 Z_1[k] + \tilde{h}_2 Z_2[k] + N_1[k] \tag{3}$$

$$Y_2[k] = gX[k] + \tilde{g}_1 Z_1[k] + \tilde{g}_2 Z_2[k] + N_2[k] \tag{4}$$

where $Y_i[k]$ is the received signal at the ith receiver in the kth transmission frame, h, g are the channel gains from the transmitter to receivers 1, 2, respectively, and $\tilde{h}_i$, $\tilde{g}_i$ are the channel gains from helper i to receivers 1, 2, respectively.

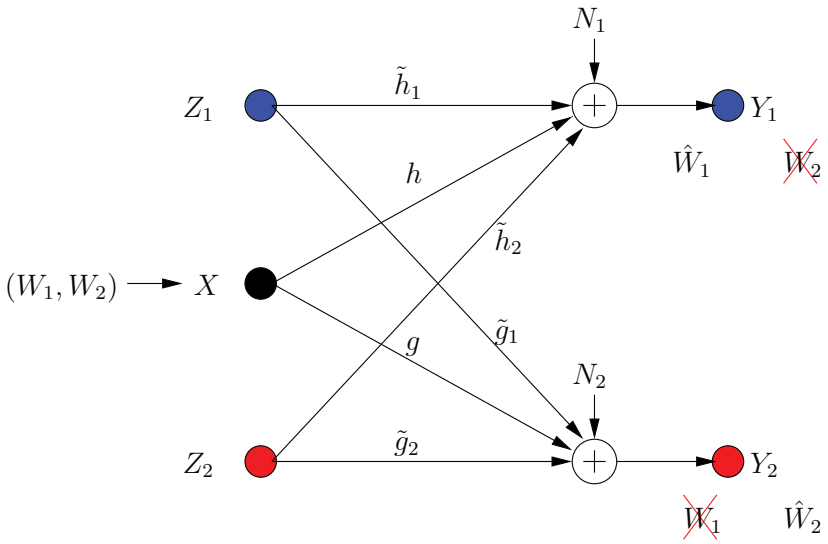

Figure 1. Broadcast channel with confidential messages (BCCM) with combating helpers.

The helpers are *combating* as they maximize the s.d.o.f. of one user only, while hurting the other user by sending jamming signals. The transmitter acts in even transmission frames, and helpers respond in odd frames. Each node has perfect channel state information (CSI) and knows the actions

of others at the end of every frame. We require that the action of a helper does not hurt its own receiver (in terms of s.d.o.f.) if no new jamming signals are produced by the other helper. Consequently, we formalize the role of the ith helper as:

$$\min \quad d_j(k) \qquad \text{s.t.} \quad d_i(k) = d_i(k-1) \tag{5}$$

where $i, j \in \{1, 2\}$, $i \neq j$ and $d_j(k)$ is the s.d.o.f. of the jth user in the kth transmission frame, where k is odd. On the other hand, the transmitter does not take the side of any of the users and maximizes the sum s.d.o.f. of the system, i.e., transmitter's role in even encoding frames is:

$$\max \quad d_1(k) + d_2(k) \tag{6}$$

2.2. Achievable Scheme: Recursive Real Interference Alignment as Extensive-Form Game

We use recursive real interference alignment as the achievable strategy for our model. At encoding frame k, all secure and jamming signals are picked from PAM constellation set $C(a_k, Q_k)$, where a_k is the minimum distance between any two points in the constellation and Q_k is the number of points.

2.2.1. For Frames $k = 0$, $k = 1$

Frames 0 and 1 are considered transient frames. For frame 0, the transmitter performs the optimal strategy in the presence of helpers [13] and sends two signal components V_{11}, V_{21} in two irrational dimensions:

$$X[0] = \alpha_1 V_{11} + \alpha_2 V_{21} \tag{7}$$

where α_1, α_2 are rationally independent scalars. These message-carrying signals are not secured. None of the helpers expects the other helper to jam its own receiver; thus, each helper needs to protect the message of its own receiver at the other receiver. Hence, at $k = 1$, the ith helper sends a structured jamming signal $\tilde{U}_{i1}$ in the irrational dimension where its message-carrying signal lies at the other receiver as:

$$Z_1[1] = \frac{\alpha_1 g}{\tilde{g}_1}\tilde{U}_{11}, \quad Z_2[1] = \frac{\alpha_2 h}{\tilde{h}_2}\tilde{U}_{21} \tag{8}$$

Then, the received signals are:

$$Y_1[1] = \alpha_1 h V_{11} + \frac{\alpha_1 g \tilde{h}_1}{\tilde{g}_1}\tilde{U}_{11} + \alpha_2 h(V_{21} + \tilde{U}_{21}) + N_1 \tag{9}$$

$$Y_2[1] = \alpha_2 g V_{21} + \frac{\alpha_2 h \tilde{g}_2}{\tilde{h}_2}\tilde{U}_{21} + \alpha_1 g(V_{11} + \tilde{U}_{11}) + N_2 \tag{10}$$

Although V_{11}, V_{21} are now secure, this results in a new irrational dimension at each receiver as in Figure 2. Hence, $d_i(1) = 1/3$ for each user as we show formally in Section 2.3 (instead of $d_i = 1/2$ in BCCM with coordinating helpers).

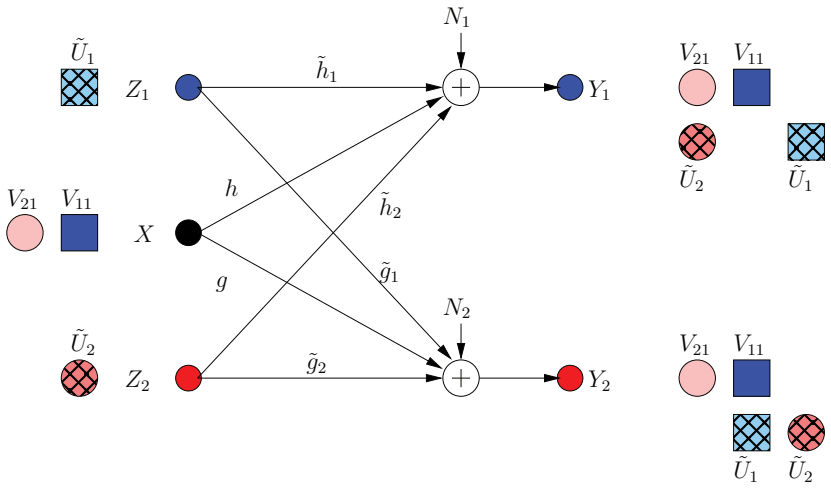

Figure 2. BCCM frame $k = 1$. Pink circle and blue square denote user signals, and the hatched circles/squares denote corresponding helper jamming signals.

2.2.2. For Frame $k = 2$

The transmitter knows that a new irrational dimension is generated within frame $k = 1$. The transmitter uses this dimension in its favor, as it can protect more message-carrying signals. It produces two new message-carrying signal components V_{12}, V_{22} to be aligned with the generated jamming dimensions in frame $k = 1$ as:

$$X[2] = \alpha_1 V_{11} + \alpha_2 V_{21} + \frac{\alpha_2 h \tilde{g}_2}{\tilde{h}_2 g} V_{12} + \frac{\alpha_1 g \tilde{h}_1}{\tilde{g}_1 h} V_{22} \tag{11}$$

$$= X[1] + \beta_1 V_{12} + \beta_2 V_{22} \tag{12}$$

That is, the transmitter appends its last frame transmission with two new signal components in rationally independent dimensions β_1, β_2 (see Figure 3). The received signals are:

$$Y_1[1] = \alpha_1 h V_{11} + \frac{\alpha_2 h^2 \tilde{g}_2}{\tilde{h}_2 g} V_{12} + \frac{\alpha_1 g \tilde{h}_1}{\tilde{g}_1} (V_{22} + \tilde{U}_{11}) + \alpha_2 h (V_{21} + \tilde{U}_{21}) + N_1 \tag{13}$$

$$Y_2[1] = \alpha_2 g V_{21} + \frac{\alpha_1 g^2 \tilde{h}_1}{\tilde{g}_1 h} V_{22} + \frac{\alpha_2 h \tilde{g}_2}{\tilde{h}_2} (V_{12} + \tilde{U}_{12}) + \alpha_1 g (V_{11} + \tilde{U}_{11}) + N_2 \tag{14}$$

Consequently, the system retains full s.d.o.f. ($d_i(2) = 1/2$).

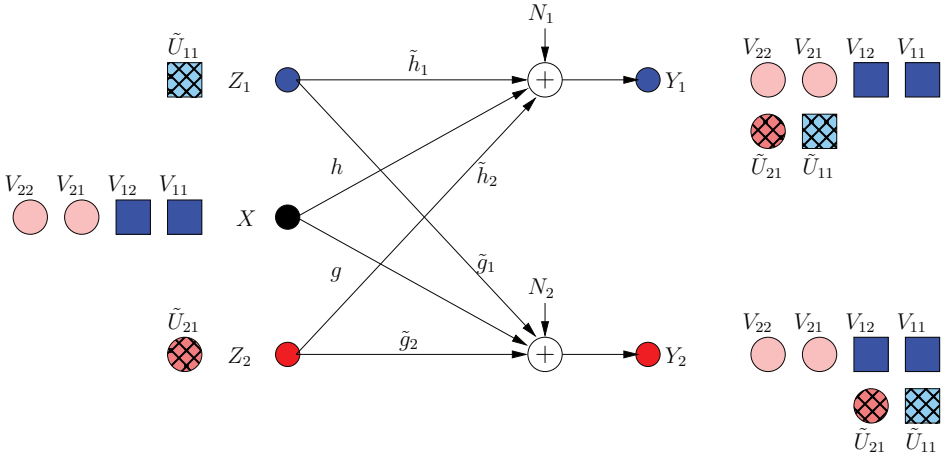

Figure 3. BCCM frame $k = 2$.

2.2.3. For Frame $k = 3$

Now, each helper minimizes the s.d.o.f. of the other user by sending a jamming signal. However, due to the strong constraint $d_i(3) = d_i(2)$, no helper jams the other receiver directly, as this would create a new jamming dimension at the side of its own receiver, decreasing its own s.d.o.f. Instead, it transmits a jamming signal which aligns with the already jammed dimension at its own receiver as:

$$Z_1[3] = Z_1[1] + \frac{\alpha_2 h}{\tilde{h}_1}\tilde{U}_{12}, \quad Z_2[3] = Z_2[1] + \frac{\alpha_1 g}{\tilde{g}_2}\tilde{U}_{22} \tag{15}$$

Consequently, the received signals are:

$$Y_1[3] = Y_1[2] + \alpha_2 h\tilde{U}_{12} + \frac{\alpha_1 \tilde{h}_2 g}{\tilde{g}_2}\tilde{U}_{22} \tag{16}$$

$$Y_2[3] = Y_2[2] + \alpha_1 g\tilde{U}_{22} + \frac{\alpha_2 \tilde{g}_2 h}{\tilde{h}_1}\tilde{U}_{12} \tag{17}$$

Since the $\alpha_2 h$ dimension is already jammed, the first helper does not create a new irrational dimension. Hence, it does not hurt its own receiver. However, it creates a new jamming dimension $\frac{\alpha_2 \tilde{g}_2 h}{\tilde{h}_1}$ at the second receiver, which decreases the resultant s.d.o.f. From the symmetry, the second helper applies the same strategy, and hence, the resulting s.d.o.f. is $d_i(3) = 2/5$ as in Figure 4. Note that neither of the helpers can hold back its original jamming signal (i.e., each helper should append its previous signaling with new jamming signals), because if not, its previous message-carrying signals are compromised.

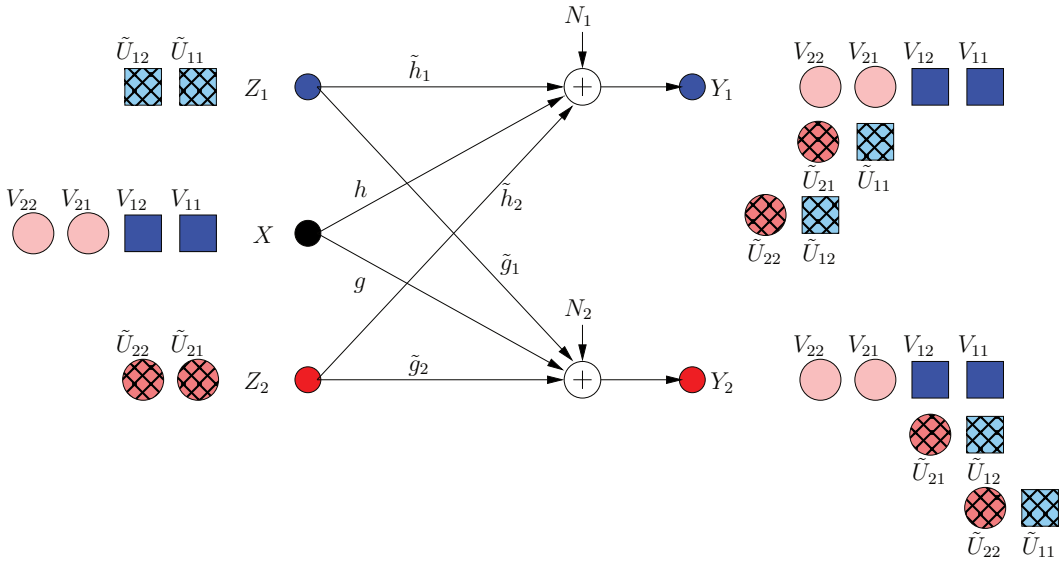

Figure 4. BCCM frame $k = 3$.

2.2.4. For General kth Frame

If k is odd, the helpers produce one extra jamming component aligned with the last generated jamming signal of the other helper. If k is even, the transmitter makes use of this jamming signal and provides two extra secure signals, achieving the maximum possible s.d.o.f. ($d_i(k) = 1/2$, k is even).

2.3. Calculation of the Secure Degrees of Freedom

To calculate the s.d.o.f., we need the following lemma.

Lemma 1. *If every message-carrying signal is protected by a cooperative jamming signal, then the s.d.o.f. is given by:*

$$d_i(k) = \frac{J_k}{L_k} \tag{18}$$

where J_k is the number of irrational dimensions needed to receive the message-carrying signal of user i at the kth frame $\mathbf{V}_i[k] = [V_{i1}, V_{i2}, \dots V_{iJ_k}]^T$ and L_k is the total number of irrational dimensions.

Proof. From [5], the following rate expression is achievable for the BCCM:

$$R_1[k] \geq I(\mathbf{V}_1[k]; Y_1[k]) - I(\mathbf{V}_1[k]; Y_2[k]|\mathbf{V}_2[k]) \tag{19}$$

Let L_k denote the total number of irrational dimensions used in the kth frame at receiver 1, and J_k denote the number of dimensions used to receive $\mathbf{V}_1[k]$ at receiver 1 (without loss of generality, due to symmetry). Then, by choosing $Q_k = P^{\frac{1-\delta}{2(L_k+\delta)}}$ and $a_k = \gamma P^{\frac{1}{2}}/Q_k$, the average power constraint is satisfied for all nodes, and the probability of error is upper bounded using the Khintchine–Groshev theorem of Diophantine approximation in number theory as in [39] as:

$$\mathbb{P}(\hat{\mathbf{V}}_i[k] \neq \mathbf{V}_i[k]) \leq \exp\left(-\eta_\gamma P^\delta\right) \tag{20}$$

where η_γ is constant that does not depend on P. Hence, the probability of error converges to zero as $P \to \infty$. Then, using Fano's inequality and the data processing inequality of $\mathbf{V}_i[k] \to Y_i[k] \to \hat{\mathbf{V}}_i[k]$, we lower bound $I(\mathbf{V}_i; Y_i[k])$ as follows:

$$\begin{aligned}
I(\mathbf{V}_i[k]; Y_i[k]) &= H(\mathbf{V}_i[k]) - H(\mathbf{V}_i[k]|Y_i[k]) && (21)\\
&\geq H(\mathbf{V}_i[k]) - H(\mathbf{V}_i[k]|\hat{\mathbf{V}}_i[k]) && (22)\\
&\geq [1 - \exp(-\eta_\gamma P^\delta)] \log(2Q+1)^{J_k} - 1 && (23)\\
&= \frac{J_k(1-\delta)}{L_k+\delta}\left(\frac{1}{2}\log P\right) + o(\log P) && (24)
\end{aligned}$$

Since we designed the coding scheme at each frame so that $\mathbf{V}_1[k]$ is completely hidden for some $\mathbf{U}_1[k]$, we can upper bound the second term as:

$$\begin{aligned}
I(\mathbf{V}_1[k]; Y_2[k]|\mathbf{V}_2[k]) &\leq I\left(\mathbf{V}_1[k]; \mathbf{A}[k](\mathbf{V}_1[k] + \mathbf{U}_1[k])\right) && (25)\\
&= H(\mathbf{V}_1[k] + \mathbf{U}_1[k]) - H(\mathbf{U}_1[k]) && (26)\\
&= \log(4Q+1)^{J_k} - \log(2Q+1)^{J_k} && (27)\\
&\leq J_k && (28)
\end{aligned}$$

where $\mathbf{A}[k]$ is a diagonal matrix which corresponds to the irrational-dimension gains. The last step follows from carefully designing the jamming vector $\mathbf{U}_1[k]$, so that it aligns with each component of $\mathbf{V}_1[k]$. By taking limit as $P \to \infty$, we have $d_i(k) = \frac{J_k}{L_k}$. □

Now, we are ready to formally calculate the resulting s.d.o.f. from the recursive real interference alignment in the following theorem.

Theorem 1. *For BCCM with combating helpers under the constraint of not decreasing the s.d.o.f. of their own receivers due to helper actions, the s.d.o.f. of each user evolves as:*

$$d_i(k) = \begin{cases} 1/2, & k \text{ even} \\ \frac{k+1}{2k+4} \to 1/2, & k \text{ odd} \end{cases} \tag{29}$$

i.e., the combating behavior is asymptotically neutralized.

Proof. Using Lemma 1, we have $d_i(k) = \frac{J_k}{L_k}$. We complete the proof by calculating the dimensions J_k, L_k. We prove this by induction on k. For the base step $k = 1$, we have $J_k = 1$ and $L_k = 3$ which conforms with (29). For $k = 2$, we have $J_k = 2$ and $L_k = 4$, and hence, $d_i(k) = 1/2$.

For the induction step, assume that k is odd and $d_i(k-2) = \frac{k-1}{2k}$. Then, in the $(k-1)$th frame, the transmitter can always add two extra message-carrying signals to have $d_i(k-1) = 1/2$. Thus, $J_{k-1} = J_{k-2} + 1$ and $L_{k-1} = L_{k-2} + 1$. This is because the transmitter uses the extra irrational dimension produced by jamming in odd frames in its favor, hence adding one extra dimension corresponding to the new message-carrying signal. This results in the following simultaneous equations:

$$\frac{J_{k-2}}{L_{k-2}} = \frac{k-1}{2k}, \quad \frac{J_{k-1}}{L_{k-1}} = \frac{J_{k-2}+1}{L_{k-2}+1} = \frac{1}{2} \tag{30}$$

Solving these two equations gives $L_{k-2} = k$ and $J_{k-2} = \frac{(k-1)}{2}$. Then, $L_{k-1} = k+1$ and $J_{k-1} = \frac{k+1}{2}$. In the next frame transmission, each helper produces an extra jamming component aligned with a already jammed dimension. This increases L_k by one at the other receiver without changing J_k. Consequently, $d_i(k) = \frac{J_k}{L_k} = \frac{\frac{k+1}{2}}{k+2} = \frac{k+1}{2k+4}$, which converges to $1/2$. □

3. ICCM with Selfish Users

3.1. System Model and Assumptions

In ICCM, each transmitter has a message W_i picked from the message set $\mathcal{W}_i$ uniformly with rate $R_i = \frac{1}{n} \log |\mathcal{W}_i|$ for $i \in \{1, 2\}$. Message W_i should be received reliably by the ith receiver, while being kept secure from the jth receiver, $i \neq j$. The system has an external helper with channel input Z. Inputs satisfy power constraints $\mathbb{E}[X_i^2] \leq P$ and $\mathbb{E}[Z^2] \leq P$. The ICCM model depicted in Figure 5 is given by:

$$Y_1[k] = h_{11}X_1[k] + h_{21}X_2[k] + h_{31}Z[k] + N_1[k] \tag{31}$$

$$Y_2[k] = h_{12}X_1[k] + h_{22}X_2[k] + h_{32}Z[k] + N_2[k] \tag{32}$$

where $Y_i[k]$ is the received signal at the ith receiver in the kth transmission frame, and h_{ij} is the channel gain from transmitter $i = 1, 2, 3$ (transmitter 3 is the helper) to receiver $j = 1, 2$.

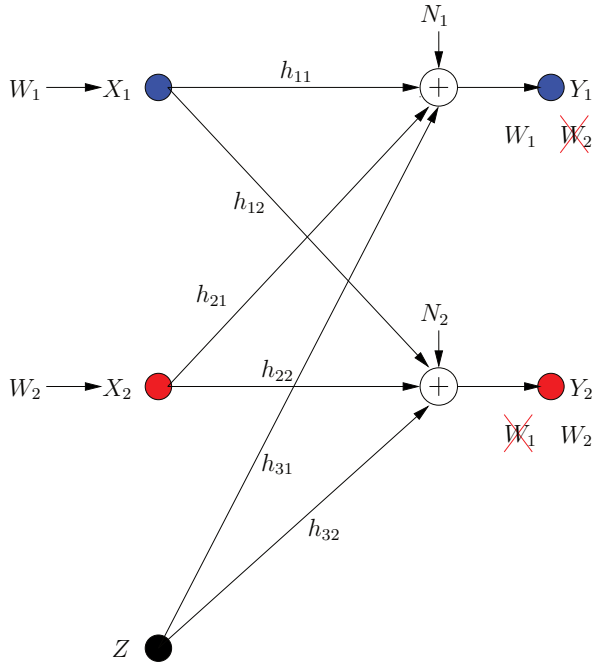

Figure 5. Interference channel with confidential messages (ICCM) with selfish users.

The users are *selfish* and malicious. User i maximizes the individual s.d.o.f. at receiver Y_i, while maximally hurting the second user. Formally, the ith user's role is:

$$\max \quad d_i(k) - d_j(k) \tag{33}$$

where $i \neq j$, $i, j \in \{1, 2\}$. The role of the users here is *less stringent* than in the BCCM model, since in the ICCM model, we allow the users to hurt their own receivers if they hurt the other receiver more. On the other hand, the system helper does not take the side of any of the users and maximizes the sum s.d.o.f. of the system:

$$\max \quad d_i(k) + d_j(k) \tag{34}$$

3.2. Achievable Scheme: Recursive Real Interference Alignment as Extensive Form Game

Similar to the BCCM, we propose using recursive interference alignment using the PAM constellation $C(a_k, Q_k)$.

3.2.1. For Frame $k = 0$

All nodes perform the optimal *selfless* strategy as in [13]. The transmitted signals are:

$$X_1[0] = \frac{h_{32}}{h_{12}} V_{11}, \quad X_2[0] = \frac{h_{31}}{h_{21}} V_{21}, \quad Z[0] = \tilde{U}_1 \tag{35}$$

The received signals at both receivers are (as in Figure 6):

$$Y_1[0] = \frac{h_{32}h_{11}}{h_{12}} V_{11} + h_{31}(V_{21} + \tilde{U}_1) + N_1 \tag{36}$$

$$Y_2[0] = \frac{h_{31}h_{22}}{h_{21}} V_{21} + h_{32}(V_{11} + \tilde{U}_1) + N_2 \tag{37}$$

which implies that the achievable s.d.o.f. $d_i(0) = 1/2$.

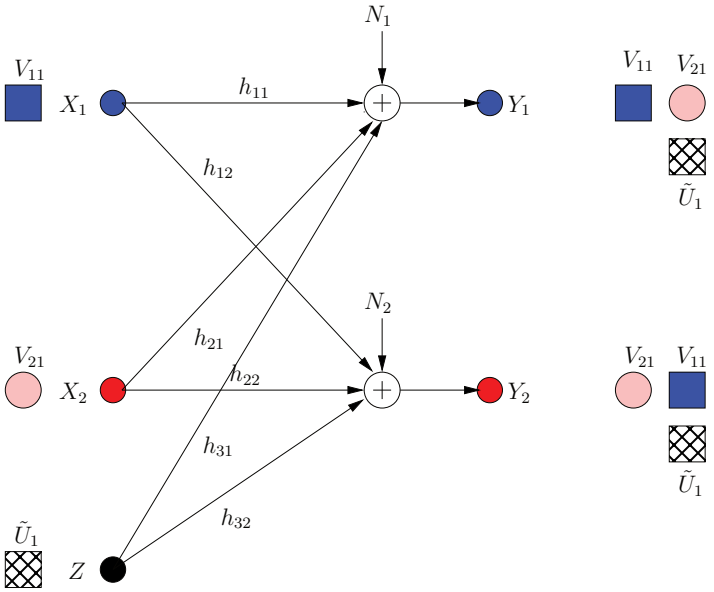

Figure 6. ICCM frame $k = 0$. Pink circle and blue square denote user signals, and the hatched squares denote jamming signals.

3.2.2. For Frame $k = 1$

User i maximizes $d_i(1) - d_j(1)$ assuming that user j keeps its strategy as in frame 0. Each user prefers to jam the other user directly, even if it results in partial decrease of its own s.d.o.f. (by creating an extra dimension at its receiver), since in this case, it can drive the s.d.o.f. of the other user to zero and maximize the s.d.o.f. difference. Thus:

$$X_1[1] = X_1[0] + \frac{h_{31}h_{22}}{h_{12}h_{21}}U_{11} \tag{38}$$

$$X_2[1] = X_2[0] + \frac{h_{32}h_{11}}{h_{12}h_{21}}U_{21} \tag{39}$$

Hence, the received signals in this case are:

$$Y_1[1] = \frac{h_{32}h_{11}}{h_{12}}(V_{11} + U_{21}) + h_{31}(V_{21} + \tilde{U}_1) + \frac{h_{31}h_{22}h_{11}}{h_{12}h_{21}}U_{11} + N_1 \tag{40}$$

$$Y_2[1] = \frac{h_{31}h_{22}}{h_{21}}(V_{21} + U_{11}) + h_{32}(V_{11} + \tilde{U}_1) + \frac{h_{32}h_{12}h_{22}}{h_{12}h_{21}}U_{11} + N_2 \tag{41}$$

which implies that all secure signals are jammed and communication is driven to zero s.d.o.f. as in Figure 7.

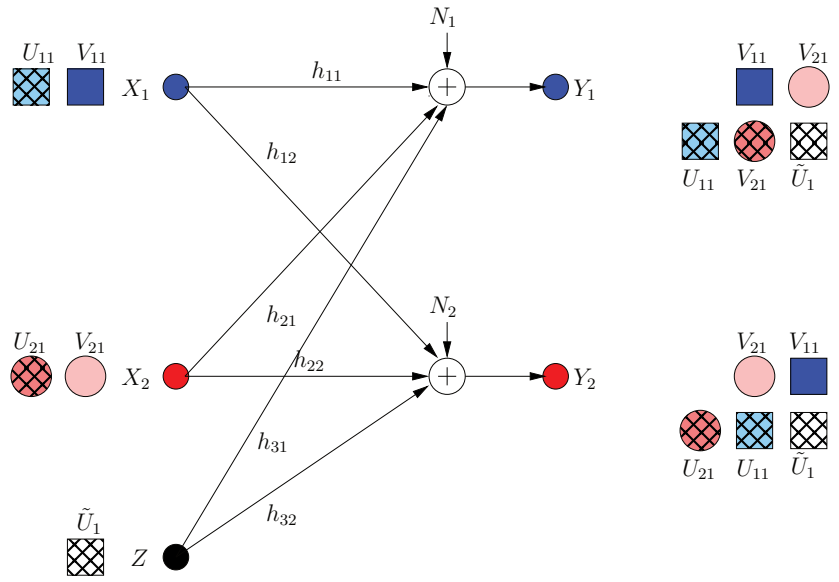

Figure 7. ICCM frame $k = 1$.

3.2.3. For Frame $k = 2$

Both users know that their communication links are jammed during frame $k = 1$. Therefore, the problem of maximizing the s.d.o.f. difference reduces to maximizing s.d.o.f. of each individual user, since the s.d.o.f. of the other user is zero. Each user benefits from the extra jamming dimension created by the other user to protect extra message-carrying component. Moreover, the helper produces an extra jamming component in a new irrational dimension, which allows each user to produce extra secure signal. Thus:

$$X_1[2] = X_1[1] + \frac{\alpha_1 h_{32}}{h_{12}} V_{12} + \frac{h_{32} h_{11} h_{22}}{h_{12}^2 h_{21}} V_{13} \tag{42}$$

$$X_2[2] = X_2[1] + \frac{\alpha_1 h_{31}}{h_{21}} V_{22} + \frac{h_{31} h_{22} h_{11}}{h_{21}^2 h_{12}} V_{23} \tag{43}$$

$$Z[2] = Z[1] + \alpha_1 \tilde{U}_2 \tag{44}$$

where α_1 is an irrational number independent from all channel gains. Hence, the received signals are:

$$Y_1[2] = Y_1[1] + \alpha_1 h_{31}(V_{22} + \tilde{U}_2) + \frac{h_{31} h_{22} h_{11}}{h_{21} h_{12}} V_{23} + \frac{\alpha_1 h_{32} h_{11}}{h_{12}} V_{12} + \frac{h_{32} h_{11}^2 h_{22}}{h_{12}^2 h_{21}} V_{13} \tag{45}$$

$$Y_2[2] = Y_2[1] + \alpha_1 h_{32}(V_{12} + \tilde{U}_2) + \frac{h_{32} h_{11} h_{22}}{h_{12} h_{21}} V_{13} + \frac{\alpha_1 h_{31} h_{22}}{h_{21}} V_{22} + \frac{h_{31} h_{22} h_{11}}{h_{21}^2 h_{12}} V_{23} \tag{46}$$

Consequently, $d_i(2) = 1/3$ as shown in Figure 8.

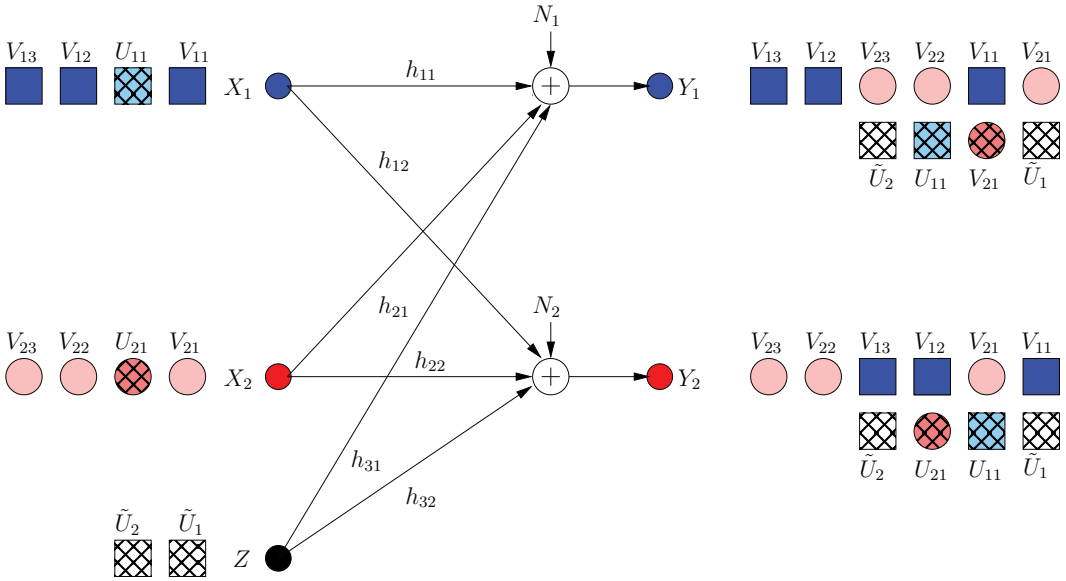

Figure 8. ICCM frame $k = 2$.

3.2.4. For General kth Frame

The s.d.o.f. differs based on whether k is odd/even. If k is odd, each user chooses to jam all dimensions of the other user's secure signals. This choice leads to $d_i(k) = 0$ for all odd frames. If k is even, each user takes advantage of the generated jamming by the other user plus the extra jamming signal from the system helper to protect more signals.

3.3. Calculation of the Secure Degrees of Freedom

Theorem 2. *For the ICCM with selfish users in the presence of a system helper, assuming that users maximize the s.d.o.f. difference for every transmission frame, the s.d.o.f. evolves as:*

$$d_i(k) = \begin{cases} 0, & k \text{ odd} \\ \frac{2}{k+4} \to 0, & k \text{ even} \end{cases} \tag{47}$$

i.e., selfishness eventually precludes secure communication.

Proof. From [5], the rates given in (19) are achievable for the ICCM. Then, from Lemma 1, we have $d_i(k) = \frac{J_k}{L_k}$. Next, we count $J_k = \frac{k+2}{2}$ when k is even. This follows by induction: For $k = 1$, the number

of secure dimensions is 1. Now, assume that the relation holds for any even $k-2$. Then, $J_{k-2} = \frac{k}{2}$. Then, since user i jams all secure dimensions of user j in frame $k-1$, it creates $\frac{k}{2}$ new dimensions. These dimensions are used by user i in frame k to protect $\frac{k}{2}$ new secure signals. The helper produces an extra jamming component, allowing protection of one extra signal. Then, $J_k = \frac{k}{2} + 1 = \frac{k+2}{2}$.

We use this result in proving s.d.o.f. by induction: For $k = 0$, $J_0 = 1$ and $L_0 = 2$, which leads to $d_i(0) = 1/2$. For $k = 1$, $J_1 = 0$ and $L_1 = 3$, which leads to $d_i(1) = 0$. Now, assume that k is even and expression (47) is true, then, $d_i(k-2) = \frac{2}{k+2}$. Then, from the above, we have $J_{k-2} = \frac{k}{2}$. Hence, $L_{k-2} = \frac{k(k+2)}{4}$. The total dimensions L_k at any receiver is increased over the $k-2$ frame by $2J_k$, since the increase is caused by the new secure dimensions J_k for the two users, which are symmetric. Therefore, the s.d.o.f. for even k is:

$$d_i(k) = \frac{J_k}{L_k} = \frac{J_k}{L_{k-2} + 2J_k} = \frac{2}{k+4} \tag{48}$$

If k is odd, users make s.d.o.f. zero, completing the proof. □

Remark 1. *Although the previous channel models are different, they have critical similarities: In both models, there is a central node, transmitter in BCCM, and helper in ICCM, which altruistically want to maximize the sum s.d.o.f.; however, the transmitter in BCCM can send useful signals, but the helper ICCM can only jam. In both models, there are two adversarial/selfish transmitters, helpers in BCCM, and users in ICCM; however, helpers in BCCM can only jam, but users in ICCM can send useful signals and/or jam. We observe that this difference in roles drives systems to opposite end results of full s.d.o.f. in BCCM and zero s.d.o.f. in ICCM.*

4. Multiple Access Wiretap Channel with Deviating Users

4.1. System Model and Assumptions

The K-user Gaussian MAC-WTC is given by (see Figure 9):

$$Y_1 = \sum_{i=1}^{K} h_i X_i + N_1 \tag{49}$$

$$Y_2 = \sum_{i=1}^{K} g_i X_i + N_2 \tag{50}$$

where Y_1, Y_2 are the channel outputs at the legitimate receiver and the eavesdropper, respectively, and 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.,

$$\mathbb{P}(\hat{W}_1^K \neq W_1^K) \leq \epsilon, \quad \frac{1}{n} I(W_1^K; Y_2^n) \leq \epsilon \tag{51}$$

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 section, 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 is also subject to the power constraint $\mathbb{E}[Z^2] \leq P$, and we designate it as the Kth user without loss of generality, see Figure 13. The malicious user and the remaining users respond to each other in multiple coding frames. The channel inputs/outputs for this model in frame k are:

$$Y_1[k] = \sum_{i=1}^{K-1} h_i X_i[k] + \tilde{h} Z[k] + N_1[k] \tag{52}$$

$$Y_2[k] = \sum_{i=1}^{K-1} g_i X_i[k] + \tilde{g} Z[k] + N_2[k] \tag{53}$$

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

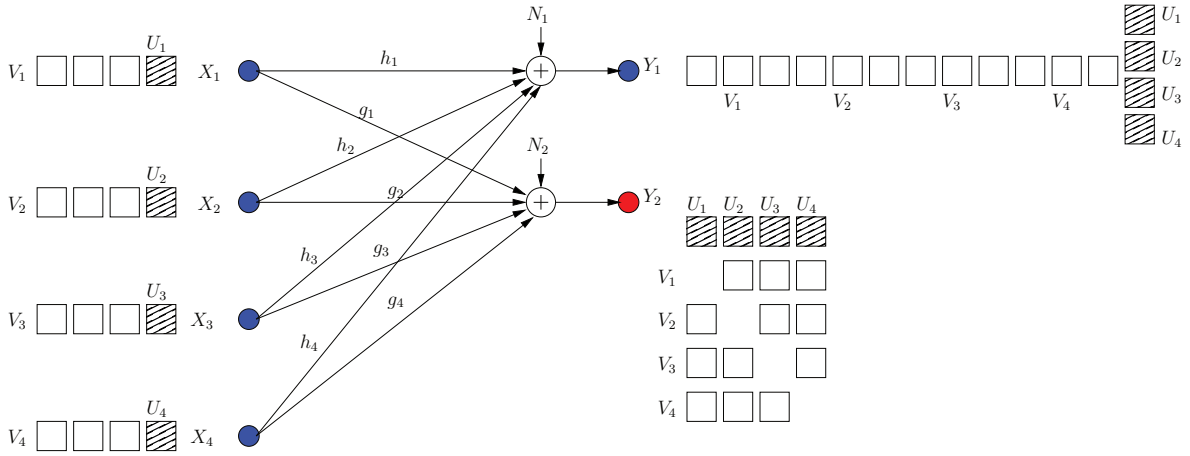

Figure 9. Optimal achievable scheme for a $K = 4$ user multiple access wiretap channel (MAC-WTC).

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

Consider that M users have deviated from the optimum strategy in [13] (see Figure 9) 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 Figure 10). That is, the user signals are [13]:

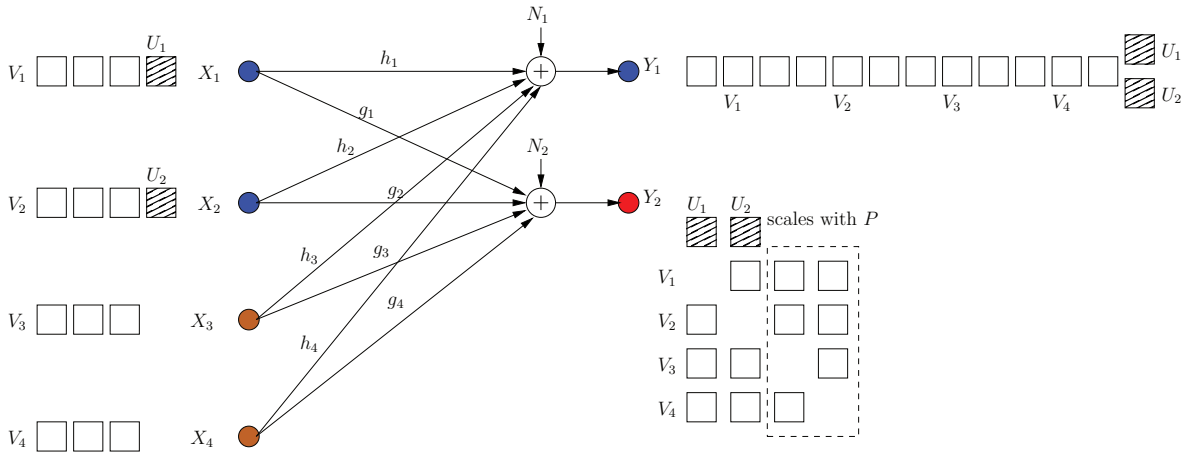

Figure 10. The remaining users keep their originally optimum schemes.

$$X_i = \begin{cases} \sum_{j=1, j\neq i}^{K} \frac{g_j}{g_i h_j} V_{ij} + \frac{1}{h_i} U_i, & i = 1, \ldots, K-M \\ \sum_{j=1, j\neq i}^{K} \frac{g_j}{g_i h_j} V_{ij}, & i = K-M+1, \ldots, K \end{cases} \tag{54}$$

where V_{ij}, U_i are picked uniformly from PAM constellation set $C(a, Q)$ [13]. The constants a, Q are chosen as [13]:

$$Q = P^{\frac{1-\delta}{2K(K-1)+1+\delta}}, \quad a = \gamma \frac{P^{1/2}}{Q} \tag{55}$$

Consequently, the received signals are (see Figure 10):

$$Y_1 = \sum_{i=1}^{K} \sum_{j=1, j\neq i}^{K} \frac{g_j h_i}{g_j h_j} V_{ij} + \sum_{k=1}^{K-M} U_k + N_1 \tag{56}$$

$$Y_2 = \sum_{i=1}^{K} \sum_{j=1, j\neq i}^{K} \frac{g_j}{h_j} V_{ij} + \sum_{j=1}^{K-M} \frac{g_j}{h_j} U_j + N_2 \tag{57}$$

$$= \sum_{j=1}^{K-M} \frac{g_j}{h_j} \left(U_j + \sum_{i=1, i\neq j}^{K} V_{ij} \right) + \sum_{j=K-M+1}^{K} \sum_{i=1, i\neq j}^{K} \frac{g_j}{h_j} V_{ij} + N_2 \tag{58}$$

Let $\mathbf{V} = \{V_{ij} : i, j = 1, \dots K, i \neq j\}$. From [13,15], the following secure rates are achievable:

$$\sum_{i=1}^{K} R_i \geq I(\mathbf{V}; Y_1) - I(\mathbf{V}; Y_2) \tag{59}$$

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:

$$I(\mathbf{V}; Y_1) \geq I(\mathbf{V}; \hat{\mathbf{V}}) = H(\mathbf{V}) - H(\mathbf{V}|\hat{\mathbf{V}}) \tag{60}$$

$$\geq [1 - \exp(\eta_\gamma P^\delta)] \log(2Q+1)^{K(K-1)} - 1 \tag{61}$$

$$= \frac{K(K-1)(1-\delta)}{K(K-1)+1+\delta} \cdot \frac{1}{2} \log P + o(\log P) \tag{62}$$

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:

$$I(\mathbf{V}; Y_2) \leq H(Y_2 - N_2) - H(Y_2 - N_2|\mathbf{V}) \tag{63}$$

$$\leq \log(2KQ+1)^{K-M}(2(K-1)Q+1)^M) - \log(2Q+1)^{K-M} \tag{64}$$

$$= (K-M) \log \frac{2KQ+1}{2Q+1} + M \log(2(K-1)Q+1) \tag{65}$$

$$\leq (K-M) \log K + \frac{M(1-\delta)}{K(K-1)+1+\delta} \cdot \frac{1}{2} \log P + o(\log P) \tag{66}$$

$$= \frac{M(1-\delta)}{K(K-1)+1+\delta} \cdot \frac{1}{2} \log P + o(\log P) \tag{67}$$

Substituting (62) and (67) into (59), and taking the limit as $P \to \infty$, the achievable sum s.d.o.f. is:

$$d_s \geq \frac{K(K-1) - M}{K(K-1)+1} \tag{68}$$

That is, the sum s.d.o.f. decreases by $\frac{M}{K(K-1)+1}$ from the optimal in [13]. This affects all users, including the deviating users; hence, they do not benefit from their deviation.

4.3. 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.

4.3.1. 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 Figure 11. 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:

$$X_i = \begin{cases} \sum_{j=1,j\neq i}^{K-M} \frac{g_j}{g_i h_j} V_{ij} + \frac{1}{h_i} U_i, & i = 1,\dots,K-M \\ \sum_{j=1}^{K-M} \frac{g_j}{g_i h_j} V_{ij}, & i = K-M+1,\dots,K \end{cases} \tag{69}$$

Consequently, the received signals are (see Figure 11):

$$Y_1 = \sum_{i=1}^{K-M} \sum_{j=1,j\neq i}^{K-M} \frac{g_j h_i}{g_j h_j} V_{ij} + \sum_{i=K-M+1}^{K} \sum_{j=1}^{K-M} \frac{g_j h_i}{g_j h_j} V_{ij} + \sum_{k=1}^{K-M} U_k + N_1 \tag{70}$$

$$Y_2 = \sum_{i=1}^{K-M} \sum_{j=1,j\neq i}^{K-M} \frac{g_j}{h_j} V_{ij} + \sum_{i=K-M+1}^{K-M} \sum_{j=1}^{K-M} \frac{g_j}{h_j} V_{ij} + \sum_{j=1}^{K-M} \frac{g_j}{h_j} U_j + N_2 \tag{71}$$

$$= \sum_{j=1}^{K-M} \frac{g_j}{h_j} \left(U_j + \sum_{i=1,i\neq j}^{K-M} V_{ij} + \sum_{i=K-M+1}^{K} V_{ij} \right) + N_2 \tag{72}$$

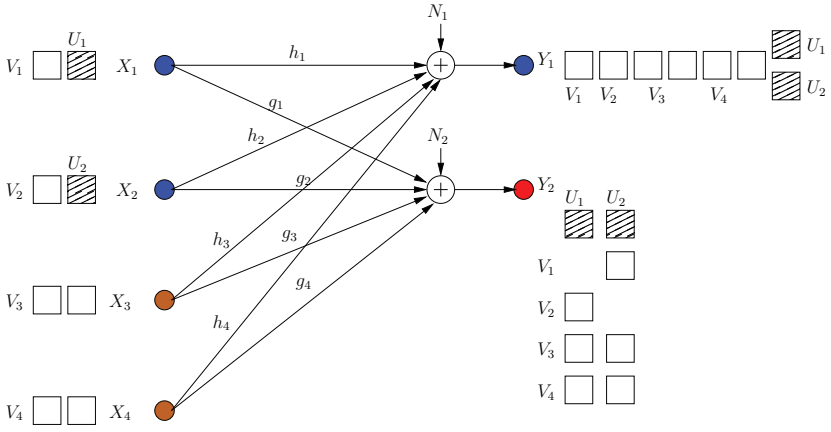

Figure 11. All users reduce rates to have zero leakage secure degrees of freedom (s.d.o.f.)

Let $\mathbf{V} = \{V_{ij} : i = 1,\dots K, j = 1,\dots,K-M, i \neq j\}$. We evaluate the secrecy rates using (59), after choosing:

$$Q = P^{\frac{1-\delta}{2(K-M)(K-1)+1+\delta}}, \quad a = \gamma \frac{P^{1/2}}{Q} \tag{73}$$

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:

$$I(\mathbf{V};Y_1) \geq I(\mathbf{V};\hat{\mathbf{V}}) \tag{74}$$

$$= \frac{(K-M)(K-1)(1-\delta)}{(K-M)(K-1)+1+\delta} \cdot \frac{1}{2}\log P + o(\log P) \tag{75}$$

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:

$$I(\mathbf{V};Y_2) \leq H(Y_2-N_2) - H(Y_2-N_2|\mathbf{V}) \tag{76}$$

$$= H\left(\sum_{j=1}^{K-M}\frac{g_j}{h_j}\left(U_j + \sum_{i=1,i\neq j}^{K-M} V_{ij} + \sum_{i=K-M+1}^{K} V_{ij}\right)\right) - H\left(\sum_{j=1}^{K-M}\frac{g_j}{h_j}U_j\right) \tag{77}$$

$$= (K-M)\log\frac{2KQ+1}{2Q+1} \tag{78}$$

$$\leq (K-M)\log K \tag{79}$$

Substituting (75) and (79) into (59), and taking the limit as $P\to\infty$, the achievable sum s.d.o.f. is:

$$d_s \geq \frac{(K-M)(K-1)}{(K-M)(K-1)+1} \tag{80}$$

The resultant sum s.d.o.f. is less than the optimal in [13]. 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 [13].

4.3.2. 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 Figure 12):

$$X_i = \begin{cases} \sum_{j=1,j\neq i}^{K-M}\frac{g_j}{g_i h_j}V_{ij} + \frac{\alpha}{h_i}V_{i0} + \frac{1}{h_i}U_i, i=1,\ldots,K-M \\ \sum_{j=1}^{K-M}\frac{g_j}{g_i h_j}V_{ij} + \frac{\alpha}{h_i}V_{i0}, \quad i=K-M+1,\ldots,K \end{cases} \tag{81}$$

where α is rationally independent from all channel gains. The received signals are shown in Figure 12. Through similar steps, we have the following s.d.o.f. for this scheme:

$$d_s \geq \frac{(K-M)^2 + M(K-M+1) - 1}{(K-M)^2 + M(K-M+1) + 1} \tag{82}$$

Although the sum s.d.o.f. in this case is smaller than in (80), the individual s.d.o.f. of a well-behaving user is higher and a deviating user is lower than in (80).

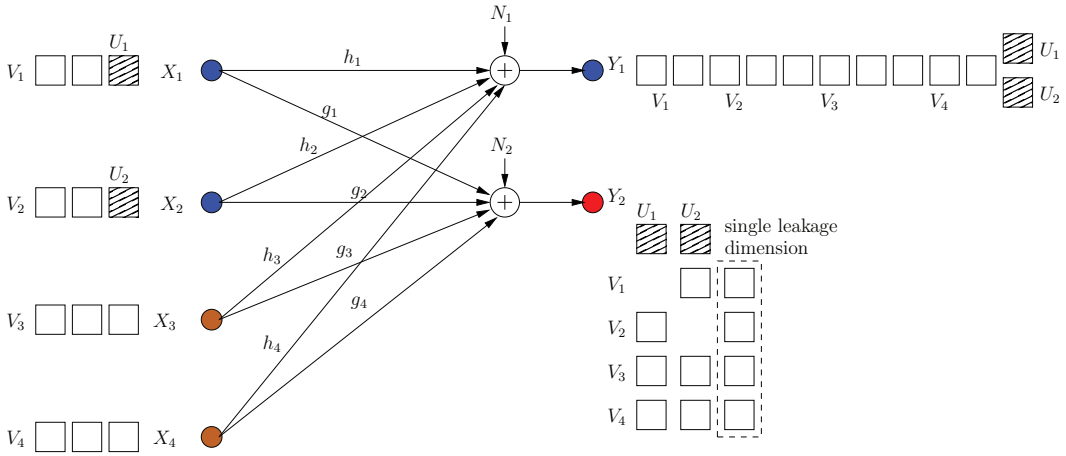

Figure 12. All users reduce the leakage dimension to 1.

4.4. 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 using 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.

4.4.1. 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:

$$X_i[k] = \sum_{j=1}^{N} \alpha_{ij} V_{ij} \tag{83}$$

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

$$Z[k] = \sum_{i=1}^{K-1} \sum_{j=1}^{N} \frac{\alpha_{ij} h_i}{\tilde{h}} \tilde{U}_{ij} \tag{84}$$

Consequently, the received signal at the legitimate receiver is:

$$Y_1[k] = \sum_{i=1}^{K-1} \sum_{j=1}^{N} h_i \alpha_{ij} (V_{ij} + \tilde{U}_{ij}) + N_1[k] \tag{85}$$

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 a vectorization of all secure signal components. Then, the secure rate is upper bounded as:

$$\sum_{i=1}^{K-1} R_i \leq I(\mathbf{V}[k]; Y_1[k] - N_1[k]) \tag{86}$$

$$= \sum_{i=1}^{K-1} \sum_{j=1}^{N} H(V_{ij} + \tilde{U}_{ij}) - H(\tilde{U}_{ij}) \tag{87}$$

$$\leq \sum_{i=1}^{K-1} \sum_{j=1}^{N} \log(4Q+1) - \log(2Q+1) \tag{88}$$

$$\leq N(K-1) = o(\log P) \tag{89}$$

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

4.4.2. When the Users Respond to the Jammer

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

$$Z[k] = \sum_{j=1}^{N} \alpha_j \tilde{U}_j \tag{90}$$

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

$$X_i[k] = \sum_{j=1}^{N} \sum_{l=1, l\neq i}^{K-1} \frac{\alpha_j \tilde{h} g_l}{g_i h_i} V_{ijl} + \sum_{j=1}^{N} \frac{\alpha_j \tilde{g}}{g_i} V_{ij0} + \sum_{j=1}^{N} \frac{\alpha_j \tilde{h}}{h_i} U_{ij} \tag{91}$$

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:

$$Y_1[k] = \sum_{j=1}^{N} \left(\sum_{i=1}^{K-1} \sum_{l=1, l\neq i}^{K-1} \frac{\alpha_j \tilde{h} g_l h_i}{g_i} V_{ijl} + \sum_{i=1}^{K-1} \frac{\alpha_j \tilde{g} h_i}{g_i} V_{ij0} + \alpha_j \tilde{h} \left(\tilde{U}_j + \sum_{i=1}^{K-1} U_{ij} \right) \right) + N_1 \tag{92}$$

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:

$$Y_2[k] = \sum_{i=1}^{K-1} g_i \left[\sum_{j=1}^{N} \sum_{l=1, l\neq i}^{K-1} \frac{\alpha_j \tilde{h} g_l}{g_i h_i} V_{ijl} + \sum_{j=1}^{N} \frac{\alpha_j \tilde{g}}{g_i} V_{ij0} + \sum_{j=1}^{N} \frac{\alpha_j \tilde{h}}{h_i} U_{ij} \right] + \tilde{g} \sum_{j=1}^{N} \alpha_j \tilde{U}_j + N_2 \tag{93}$$

$$= \sum_{j=1}^{N} \left[\alpha_j \tilde{g} \left(\sum_{i=1}^{K-1} V_{ij0} + \tilde{U}_j \right) + \sum_{l=1}^{K-1} \frac{\alpha_j \tilde{h} g_l}{h_l} \left(U_{ij} + \sum_{i=1, i\neq l}^{K-1} V_{lji} \right) \right] + N_2 \tag{94}$$

i.e., all message-carrying signals are protected from the eavesdropper, as in Figure 13, with $K = 4$, $N = 1$.

We note that the received signals at receiver Y_1 consist 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:

$$I(\mathbf{V}; Y_1[k]) \geq \frac{N(K-1)^2(1-\delta)}{N((K-1)^2+1)+\delta} \left(\frac{1}{2} \log P \right) + o(\log P) \tag{95}$$

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 A, 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 one 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.

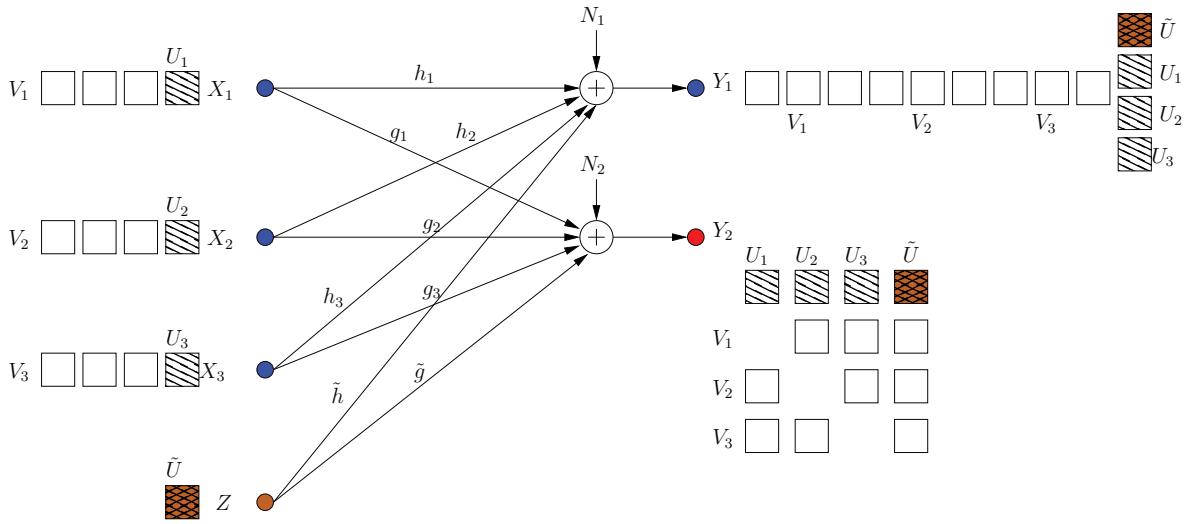

Figure 13. A malicious jamming user: users' response.

5. Conclusions

We introduced three new channel models, namely, BCCM with combating helpers, ICCM with selfish users, and MAC-WTC with deviating users. These new models aimed at studying the effects of selfishness and malicious behavior on the secure rate in networks. We investigated the achievable s.d.o.f. in these models. The presented schemes are only achievable; new role-based converse arguments are needed.

For the BCCM with combating helpers, we formulated the problem as an extensive-form game. We assumed that each helper wants to minimize the s.d.o.f. of the other receiver without sacrificing the s.d.o.f. of its receiver and analyzed schemes that employ recursive real interference alignment. In this case, we showed that the malicious behaviors of the combating helpers are neutralized and the s.d.o.f. of both users converge to $1/2$, as in the case of altruistic helpers.

For the ICCM with selfish users, we changed the objective function of the users to maximizing the difference of the s.d.o.f. between the two users. By similar analysis to BCCM, we showed that the selfishness precludes any secure communication, and the s.d.o.f. of two users converge to zero.

Finally, for the MAC-WTC with deviating users, we considered two types of deviation: First, in the case when some of the users stop transmitting cooperative jamming signals as required by the optimal scheme, we evaluated the corresponding s.d.o.f. and proposed counterstrategies to respond to the deviation. Second, we investigated an extreme form of deviation, where a user sends intentional jamming signals. We showed that although a deviating user can drive the sum s.d.o.f. to zero, the jamming signals can be exploited as cooperative jamming signals against the eavesdropper to achieve an optimum s.d.o.f.

Author Contributions: Conceptualization, K.B. and S.U.; Formal analysis, K.B. and S.U.; Investigation, K.B. and S.U.; Methodology, K.B. and S.U.; Validation, K.B. and S.U.; Visualization, K.B. and S.U.; Writing–original draft, K.B. and S.U.; Writing–review and editing, K.B. and S.U.

Funding: This work was supported by NSF Grants CNS 13-14733, CCF 14-22111, CCF 14-22129, and CNS 15-26608, and was presented in part at ISIT conference, Barcelona, Spain, July 2016.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. *K*-User MAC-WTC with *M* External Helpers

In this Appendix, we present the *exact* s.d.o.f. for a MAC-WTC with K users in the presence of M external helpers. In the context of user-misbehavior, the s.d.o.f. of this model serves as an upper bound for the MAC-WTC when the users respond to the intentional jamming when the number of

users is $K-1$ and the number of helpers is 1, i.e., we upper bound the s.d.o.f. in this case by replacing the jammer by an altruistic helper.

Theorem A1. *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. 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 [13]. The received signals at legitimate and eavesdropper receivers of the K-user Gaussian MAC with M external helpers are given by:

$$Y_1 = \sum_{i=1}^{K} h_i X_i + \sum_{j=1}^{M} \tilde{h}_j Z_j + N_1 \tag{A1}$$

$$Y_2 = \sum_{i=1}^{K} g_i X_i + \sum_{j=1}^{M} \tilde{g}_j Z_j + N_2 \tag{A2}$$

where h_i, g_i are the channel gains from the ith user to the legitimate receiver and the eavesdropper, respectively, and $\tilde{h}_j, \tilde{g}_j$ are channel gains from the jth helper to the legitimate receiver and the eavesdropper, respectively. X_i, Z_j are input signals from the ith user and the jth helper, respectively. We denote all n-lettered signals by bold vector notation, e.g., let X_i^n be expressed as $\mathbf{X}_i$.

First, we have the following upper bound which represents the *secrecy penalty* due to the secrecy constraint on the eavesdropper:

$$\begin{aligned}
n\sum_{i=1}^{K} R_i &= \sum_{i=1}^{K} H(W_i) && \text{(A3)}\\
&= H(W_1^K) && \text{(A4)}\\
&\leq I(W_1^K;\mathbf{Y}_1) + H(W_1^K|\mathbf{Y}_1) - I(W_1^K;\mathbf{Y}_2) + nc_1 && \text{(A5)}\\
&\leq I(W_1^K;\mathbf{Y}_1,\mathbf{Y}_2) - I(W_1^K;\mathbf{Y}_2) + nc_2 && \text{(A6)}\\
&= I(W_1^K;\mathbf{Y}_1|\mathbf{Y}_2) + nc_2 && \text{(A7)}\\
&\leq I(\mathbf{X}_1^K;\mathbf{Y}_1|\mathbf{Y}_2) + nc_2 && \text{(A8)}\\
&= h(\mathbf{Y}_1|\mathbf{Y}_2) - h(\mathbf{Y}_1|\mathbf{Y}_2,\mathbf{X}_1^K) + nc_2 && \text{(A9)}\\
&\leq h(\mathbf{Y}_1|\mathbf{Y}_2) - h(\mathbf{Y}_1|\mathbf{Y}_2,\mathbf{X}_1^K,\mathbf{Z}_1^M) + nc_2 && \text{(A10)}\\
&= h(\mathbf{Y}_1|\mathbf{Y}_2) - h(\mathbf{N}_1) + nc_2 && \text{(A11)}\\
&\leq h(\mathbf{Y}_1|\mathbf{Y}_2) + nc_3 && \text{(A12)}\\
&= h(\mathbf{Y}_1,\mathbf{Y}_2) - h(\mathbf{Y}_2) + nc_3 && \text{(A13)}
\end{aligned}$$

where $W_1^K = \{W_i\}_1^K$ corresponds to messages 1 through K, and similarly, $\mathbf{X}_1^K, \mathbf{Z}_1^M$ represent input signals 1 through K from the users and input signals 1 through M from the helpers, respectively. Inequality (A5) follows from applying the secrecy constraint, (A6) follows from Fano's inequality due to reliability requirements, and (A10) follows from conditioning over helpers' input signals. We define Gaussian-perturbed input signals for the users and the helpers to not deal with mixed probability

measures as $\tilde{\mathbf{X}}_i = \mathbf{X}_i + \tilde{\mathbf{N}}_i$, where $\tilde{N}_i$ is i.i.d. Gaussian noise with variance $\sigma_i^2 < \min\{\frac{1}{h_i^2}, \frac{1}{g_i^2}\}$ and similarly, for $\tilde{\mathbf{Z}}_i = \mathbf{Z}_i + \tilde{\mathbf{N}}_i$. We introduce these channel inputs in our bound as:

$$n\sum_{i=1}^{K} R_i \leq h(\tilde{\mathbf{X}}_1^K, \tilde{\mathbf{Z}}_1^M, \mathbf{Y}_1, \mathbf{Y}_2) - h(\tilde{\mathbf{X}}_1^K, \tilde{\mathbf{Z}}_1^M | \mathbf{Y}_1, \mathbf{Y}_2) - h(\mathbf{Y}_2) + nc_3 \tag{A14}$$

$$\leq h(\tilde{\mathbf{X}}_1^K, \tilde{\mathbf{Z}}_1^M, \mathbf{Y}_1, \mathbf{Y}_2) - h(\tilde{\mathbf{X}}_1^K, \tilde{\mathbf{Z}}_1^M | \mathbf{Y}_1, \mathbf{Y}_2, \mathbf{X}_1^K, \mathbf{Z}_1^M) - h(\mathbf{Y}_2) + nc_3 \tag{A15}$$

$$\leq \sum_{i=1}^{K} h(\tilde{\mathbf{X}}_i) + \sum_{j=1}^{M} h(\tilde{\mathbf{Z}}_j) - h(\mathbf{Y}_2) + nc_4 \tag{A16}$$

where (A16) follows from the fact that $\tilde{\mathbf{X}}_1^K, \tilde{\mathbf{Z}}_1^M$ are reconstructable up to finite variance Gaussian noise given $\mathbf{Y}_1, \mathbf{Y}_2, \mathbf{X}_1^K, \mathbf{Z}_1^M$ and applying the independence upper bound for the first term. The differential entropy of the received observations at the eavesdropper can be lower bounded as:

$$h(\mathbf{Y}_2) = h(g_j\tilde{\mathbf{X}}_j + \sum_{i=1, i\neq j} g_i\mathbf{X}_i + \sum_{l=1}^{M} \tilde{g}_l\tilde{\mathbf{Z}}_l + \grave{\mathbf{N}}_2) \tag{A17}$$

$$\geq h(g_j\tilde{\mathbf{X}}_j) \tag{A18}$$

$$= h(\tilde{\mathbf{X}}_j) + n\log|g_j| \tag{A19}$$

for some $j \in \{1, \ldots, K\}$. Consequently, we can write (A16) as the following upper bound which represents the secrecy penalty due to the secrecy constraint imposed on $\mathbf{Y}_2$

$$n\sum_{i=1}^{K} R_i \leq \sum_{i=2}^{K} h(\tilde{\mathbf{X}}_i) + \sum_{j=1}^{M} h(\tilde{\mathbf{Z}}_j) + nc_5 \tag{A20}$$

Next, we have the *role of the external helper(s)*, i.e., upper bounding the differential entropy of the external helpers to ensure decodability of all messages at the legitimate receiver. The sum rate is upper bounded as:

$$n\sum_{i=1}^{K} R_i = H(W_1^K) \tag{A21}$$

$$\leq I(W_1^K; \mathbf{Y}_1) + nc_6 \tag{A22}$$

$$\leq I(\sum_{i=1}^{K} h_i\mathbf{X}_i; \mathbf{Y}_1) + nc_6 \tag{A23}$$

$$= h(\mathbf{Y}_1) - h(\mathbf{Y}_1|\sum_{i=1}^{K} h_i\mathbf{X}_i) + nc_6 \tag{A24}$$

$$\leq h(\mathbf{Y}_1) - h(\mathbf{Y}_1|\sum_{i=1}^{K} h_i\mathbf{X}_i, \sum_{l\neq j} \tilde{h}_l\tilde{\mathbf{Z}}_l) + nc_6 \tag{A25}$$

$$= h(\mathbf{Y}_1) - h(\tilde{\mathbf{Z}}_j) + nc_7 \tag{A26}$$

where (A30) follows from Fano's inequality and (A31) follows from the data processing inequality. Therefore, we can upper bound the differential entropy of the jth external helper as:

$$h(\tilde{\mathbf{Z}}_j) \leq h(\mathbf{Y}_1) - n\sum_{i=1}^{K} R_i + nc_7 \tag{A27}$$

The above argument holds for every external helper, i.e., $\forall j \in \{1, \ldots, M\}$. By adding the corresponding upper bounds of the M helpers, we have the following role of the external helpers upper bound:

$$\sum_{j=1}^{M} h(\tilde{\mathbf{Z}}_j) \leq Mh(\mathbf{Y}_1) - nM \sum_{i=1}^{K} R_i + nc_8 \tag{A28}$$

Next, by considering the rates of all users except one for the $K-1$ users, we have the *role of the internal helper(s)*. Since each user affects the decodability of other users, by upper bounding the message entropy of all users except one, we can obtain an upper bound on the differential entropy of the signaling scheme employed by each user. Let $W_{\neq l}$ be all messages from all users except user l:

$$\begin{aligned}
n \sum_{i \neq l} R_i &= H(W_{\neq l}) && \text{(A29)}\\
&\leq I(W_{\neq l}; \mathbf{Y}_1) + nc_9 && \text{(A30)}\\
&\leq I(\sum_{i \neq l} h_i \mathbf{X}_i; \mathbf{Y}_1) + nc_9 && \text{(A31)}\\
&= h(\mathbf{Y}_1) - h(\mathbf{Y}_1 | \sum_{i \neq l} h_i \mathbf{X}_i) + nc_9 && \text{(A32)}\\
&\leq h(\mathbf{Y}_1) - h(\mathbf{Y}_1 | \sum_{i \neq l} h_i \mathbf{X}_i, \sum_{j=1}^{M} \tilde{h}_l \tilde{\mathbf{Z}}_l) + nc_9 && \text{(A33)}\\
&= h(\mathbf{Y}_1) - h(\tilde{\mathbf{X}}_l) + nc_9 && \text{(A34)}
\end{aligned}$$

Hence, we have the following upper bound on the differential entropy of each user:

$$h(\tilde{\mathbf{X}}_l) \leq h(\mathbf{Y}_1) - n \sum_{i \neq l}^{K} R_i + nc_9 \tag{A35}$$

Applying the above upper bound for the $K-1$ users starting from user 2 to user K, we have the following role of the users upper bound:

$$\sum_{j=2}^{K} h(\tilde{\mathbf{X}}_l) \leq (K-1)h(\mathbf{Y}_1) - n \sum_{l=2}^{K} \sum_{i \neq l} R_i \tag{A36}$$

Now, we combine all these bounds together. From the upper bounds (A28) and (A36), we substitute in (A20) to have:

$$n \sum_{i=1}^{K} R_i \leq (K-1)h(\mathbf{Y}_1) - n \sum_{l=2}^{K} \sum_{i \neq l} R_i + Mh(\mathbf{Y}_1) - nM \sum_{i=1}^{K} R_i + nc_{10} \tag{A37}$$

We rearrange and simplify (A37) as:

$$n(R_1 + (M+K-1) \sum_{i=1}^{K} R_i) \leq (M+K-1)h(\mathbf{Y}_1) + nc_{10} \tag{A38}$$

Noting that (A20) still holds for penalizing any of the users' rate, then by changing role of users and adding the K bounds, we have:

$$n\left(\sum_{i=1}^{K} R_i + K(K+M-1)\sum_{i=1}^{K} R_i\right) = n(K(K+M-1)+1)\sum_{i=1}^{K} R_i \tag{A39}$$

$$\leq K(K+M-1)h(\mathbf{Y}_1) + nc_{11} \tag{A40}$$

$$\leq K(K+M-1)\left(\frac{n}{2}\log P\right) + nc_{12} \tag{A41}$$

where we used the fact that Gaussian maximizes differential entropy under an average power constraint. By normalizing by $\frac{1}{2}\log P$ and taking limits as $P \to \infty$, we have the following upper bound on the sum s.d.o.f. for the $K-$user MAC with M external helpers as:

$$d_s \leq \frac{K(K+M-1)}{K(K+M-1)+1} \tag{A42}$$

concluding the proof of the theorem. □

Note that this result is related to the s.d.o.f. region result in [17] 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. Liang, Y.; Poor, H.V.; Shamai, S. Information theoretic security. *Found. Trends Commun. Inf. Theory* **2009**, *5*, 355–580. [CrossRef]
2. Wyner, A.D. The wire-tap channel. *Bell Labs Tech. J.* **1975**, *54*, 1355–1387. [CrossRef]
3. Csiszar, I.; Korner, J. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory* **1978**, *24*, 339–348. [CrossRef]
4. Tekin, E.; Yener, A. The Gaussian Multiple Access Wire-Tap Channel. *IEEE Trans. Inf. Theory* **2008**, *54*, 5747–5755. [CrossRef]
5. Liu, R.; Maric, I.; Spasojevic, P.; Yates, R.D. Discrete Memoryless Interference and Broadcast Channels With Confidential Messages: Secrecy Rate Regions. *IEEE Trans. Inf. Theory* **2008**, *54*, 2493–2507. [CrossRef]
6. Chong, H.F.; Liang, Y.C. Secrecy capacity region of a class of two-user Gaussian MIMO BC with degraded message sets. In Proceedings of the IEEE International Symposium on Information Theory, Istanbul, Turkey, 7–12 July 2013.
7. Liu, R.; Liu, T.; Poor, H.V.; Shamai, S. Multiple-Input Multiple-Output Gaussian Broadcast Channels With Confidential Messages. *IEEE Trans. Inf. Theory* **2010**, *56*, 4215–4227.
8. Khina, A.; Kochman, Y.; Khisti, A. The confidential MIMO broadcast capacity: A simple derivation. In Proceedings of the IEEE International Symposium on Information Theory, Hong Kong, China, 14–19 June 2015.
9. Goldfeld, Z.; Permuter, H. MIMO Gaussian Broadcast Channels with Common, Private and Confidential Messages. *arXiv* **2016**, arXiv:1608.06057.
10. Khisti, A.; Tchamkerten, A.; Wornell, G.W. Secure Broadcasting Over Fading Channels. *IEEE Trans. Inf. Theory* **2008**, *54*, 2453–2469. [CrossRef]
11. Ekrem, E.; Ulukus, S. The Secrecy Capacity Region of the Gaussian MIMO Multi-Receiver Wiretap Channel. *IEEE Trans. Inf. Theory* **2011**, *57*, 2083–2114. [CrossRef]
12. Lai, L.; Gamal, H.E. The Relay-Eavesdropper Channel: Cooperation for Secrecy. *IEEE Trans. Inf. Theory* **2008**, *54*, 4005–4019. [CrossRef]
13. Xie, J.; Ulukus, S. Secure Degrees of Freedom of One-Hop Wireless Networks. *IEEE Trans. Inf. Theory* **2014**, *60*, 3359–3378. [CrossRef]
14. Nafea, M.; Yener, A. Secure Degrees of Freedom for the MIMO Wire-Tap Channel With a Multi-Antenna Cooperative Jammer. *IEEE Trans. Inf. Theory* **2017**, *63*, 7420–7441. [CrossRef]

15. Bagherikaram, G.; Motahari, A.S.; Khandani, A.K. On the secure DoF of the single-antenna MAC. In Proceedings of the IEEE International Symposium on Information Theory, Austin, TX, USA, 13–18 June 2010.
16. He, X.; Khisti, A.; Yener, A. MIMO Multiple Access Channel With an Arbitrarily Varying Eavesdropper: Secrecy Degrees of Freedom. *IEEE Trans. Inf. Theory* **2013**, *59*, 4733–4745.
17. Xie, J.; Ulukus, S. Secure Degrees of Freedom Regions of Multiple Access and Interference Channels: The Polytope Structure. *IEEE Trans. Inf. Theory* **2016**, *62*, 2044–2069. [CrossRef]
18. Koyluoglu, O.O.; Gamal, H.E.; Lai, L.; Poor, H.V. On the secure degrees of freedom in the *K*-user Gaussian interference channel. In Proceedings of the IEEE International Symposium on Information Theory, Toronto, ON, Canada, 6–11 July 2008.
19. He, X.; Yener, A. *K*-user interference channels: Achievable secrecy rate and degrees of freedom. In Proceedings of the IEEE Information Theory Workshop on Networking and Information Theory, Volos, Greece, 10–12 June 2009.
20. He, X.; Yener, A. Secure Degrees of Freedom for Gaussian Channels with Interference: Structured Codes Outperform Gaussian Signaling. In Proceedings of the GLOBECOM IEEE Global Telecommunications Conference, Honolulu, HI, USA, 30 November–4 December 2009.
21. Xie, J.; Ulukus, S. Secure Degrees of Freedom of *K*-User Gaussian Interference Channels: A Unified View. *IEEE Trans. Inf. Theory* **2015**, *61*, 2647–2661. [CrossRef]
22. Banawan, K.; Ulukus, S. Secure Degrees of Freedom Region of Static and Time-Varying Gaussian MIMO Interference Channel. *IEEE Trans. Inf. Theory* **2019**, *65*, 444–461. [CrossRef]
23. Gou, T.; Jafar, S.A. On the secure degrees of freedom of wireless *X* networks. In Proceedings of the 46th Annual Allerton Conference on Communication, Control, and Computing, Urbana-Champaign, IL, USA, 23–26 September 2008.
24. Wang, Z.; Xiao, M.; Skoglund, M.; Poor, H.V. Secure Degrees of Freedom of Wireless *X* Networks Using Artificial Noise Alignment. *IEEE Trans. Commun.* **2015**, *63*, 2632–2646. [CrossRef]
25. Kim, T.T.; Poor, H.V. On the Secure Degrees of Freedom of Relaying With Half-Duplex Feedback. *IEEE Trans. Inf. Theory* **2011**, *57*, 291–302. [CrossRef]
26. Khisti, A. Interference Alignment for the Multiantenna Compound Wiretap Channel. *IEEE Trans. Inf. Theory* **2011**, *57*, 2976–2993. [CrossRef]
27. Lee, S.H.; Zhao, W.; Khisti, A. Secure Degrees of Freedom of the Gaussian Diamond-Wiretap Channel. *IEEE Trans. Inf. Theory* **2017**, *63*, 496–508. [CrossRef]
28. Fan, Y.; Liao, X.; Vasilakos, A.V. Physical Layer Security Based on Interference Alignment in *K*-User MIMO *Y* Wiretap Channels. *IEEE Access* **2017**, *5*, 5747–5759. [CrossRef]
29. Tandon, R.; Mohajer, S.; Poor, H.V.; Shamai, S. Degrees of Freedom Region of the MIMO Interference Channel With Output Feedback and Delayed CSIT. *IEEE Trans. Inf. Theory* **2013**, *59*, 1444–1457. [CrossRef]
30. Yang, S.; Kobayashi, M.; Piantanida, P.; Shamai, S. Secrecy Degrees of Freedom of MIMO Broadcast Channels With Delayed CSIT. *IEEE Trans. Inf. Theory* **2013**, *59*, 5244–5256. [CrossRef]
31. Zaidi, A.; Awan, Z.H.; Shamai, S.; Vandendorpe, L. Secure Degrees of Freedom of MIMO *X*-Channels With Output Feedback and Delayed CSIT. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 1760–1774. [CrossRef]
32. Mukherjee, P.; Xie, J.; Ulukus, S. Secure Degrees of Freedom of One-Hop Wireless Networks With No Eavesdropper CSIT. *IEEE Trans. Inf. Theory* **2017**, *63*, 1898–1922. [CrossRef]
33. Mukherjee, P.; Tandon, R.; Ulukus, S. Secure Degrees of Freedom Region of the Two-User MISO Broadcast Channel With Alternating CSIT. *IEEE Trans. Inf. Theory* **2017**, *63*, 3823–3853. [CrossRef]
34. Moualeu, J.M.; Hamouda, W.; Takawira, F. Intercept Probability Analysis of Wireless Networks in the Presence of Eavesdropping Attack With Co-Channel Interference. *IEEE Access* **2018**, *6*, 41490–41503. [CrossRef]
35. Tekin, E.; Yener, A. The General Gaussian Multiple-Access and Two-Way Wiretap Channels: Achievable Rates and Cooperative Jamming. *IEEE Trans. Inf. Theory* **2008**, *54*, 2735–2751. [CrossRef]
36. Ekrem, E.; Ulukus, S. On the secrecy of multiple access wiretap channel. In Proceedings of the 46th Annual Allerton Conference on Communication, Control, and Computing, Urbana-Champaign, IL, USA, 23–26 September 2008.
37. Ge, H.; Xu, R.; Berry, R.A. Secure signaling games for Gaussian multiple access wiretap channels. In Proceedings of the IEEE International Symposium on Information Theory, Hong Kong, China, 14–19 June 2015.

38. Tadelis, S. *Game Theory: An Introduction*; Princeton University Press: Princeton, NJ, USA, 2013.
39. Motahari, A.S.; Oveis-Gharan, S.; Maddah-Ali, M.A.; Khandani, A.K. Real Interference Alignment: Exploiting the Potential of Single Antenna Systems. *IEEE Trans. Inf. Theory* **2014**, *60*, 4799–4810. [CrossRef]