Secrecy in Broadcast Channel with Combating Helpers and Interference Channel with Selfish 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 investigate the secure degrees of freedom (s.d.o.f.) of two new channel models: broadcast channel with combating helpers and interference channel with selfish users. 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. The goal of introducing these channel models is to investigate various malicious interactions that arise in networks, including active adversaries. 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.**

I. Introduction

Information-theoretic security for discrete memoryless interference and broadcast channels with confidential messages are studied in [1]. The broadcast channel with confidential messages (BCCM) consists of a transmitter and two receivers. The transmitter has two messages, each directed to one of the receivers and needs to be kept secure from the other receiver. The secure degrees of freedom (s.d.o.f.) of Gaussian BCCM is zero for each user [2]. However, with an altruistic system helper, each user in the BCCM can have an s.d.o.f. of $1/2$ [2]. The interference channel with confidential messages (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. With an altruistic system helper, each user in the ICCM can have an s.d.o.f. of $1/2$. 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 this work, we investigate these models in the case of selfish and malicious behaviour, where the users/helpers do not perform the system-wide-optimal altruistic behaviour 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 [1], [2] and are a step forward in studying channel models with active adversaries. We use asymptotic analysis in terms of s.d.o.f. to study the effects of these malicious behaviours. We choose the BCCM and ICCM channel models because of their *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.

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 [2]. 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 [3], 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 [4] in a recursive way. We prove that under this stringent objective function and recursive real interference alignment, the malicious behaviours 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 [2], 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 the optimal strategy in [2] 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 [2]. 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. The presented schemes are only achievable; new converses are needed.

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

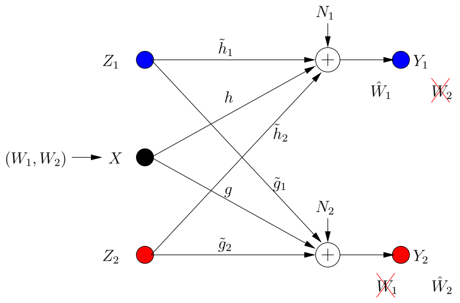

Fig. 1. BCCM with combating helpers.

II. BCCM with Combating Helpers

A. 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 $R_i = \frac{1}{n} \log |\mathcal{W}_i|$. 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 $\hat{W}_i$ 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 Fig. 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.

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:

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

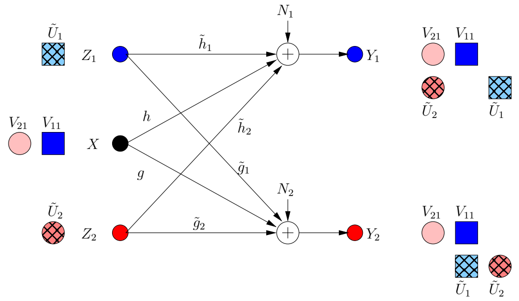

Fig. 2. BCCM frame $k = 1$. Pink circle and blue square denote user signals, and the hatched circles/squares denote corresponding helper jamming signals.

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

We use recursive real interference alignment as 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.

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 [2], 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, hence 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 Fig. 2. Hence $d_i(1) = 1/3$ for each user as we show formally in Section II-C (instead of $d_i = 1/2$ in BCCM with coordinating helpers).

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,

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

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

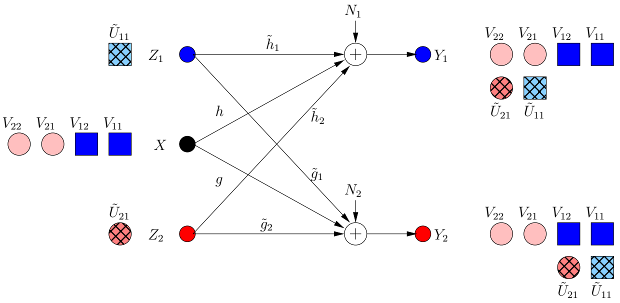
$\tilde U_{11}$
Z_1
$\tilde h_1$
N_1
Y_1
V_{22} V_{21} V_{12} V_{11}
$\tilde U_{21}$ $\tilde U_{11}$
V_{22} V_{21} V_{12} V_{11}
X
h
$\tilde h_2$
g
$\tilde g_1$
N_2
$\tilde U_{21}$
Z_2
$\tilde g_2$
Y_2
V_{22} V_{21} V_{12} V_{11}
$\tilde U_{21}$ $\tilde U_{11}$

Fig. 3. BCCM frame $k = 2$.

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

$$\begin{aligned} Y_1[1] =& \alpha_1 h V_{11} + \frac{\alpha_2 h^2 \tilde g_2}{\tilde h_2 g} V_{12} + \frac{\alpha_1 g \tilde h_1}{\tilde g_1}(V_{22} + \tilde U_{11}) \\ &+ \alpha_2 h (V_{21} + \tilde U_{21}) + N_1 \qquad (13) \\ Y_2[1] =& \alpha_2 g V_{21} + \frac{\alpha_1 g^2 \tilde h_1}{\tilde g_1 h} V_{22} + \frac{\alpha_2 h \tilde g_2}{\tilde h_2}(V_{12} + \tilde U_{12}) \\ &+ \alpha_1 g (V_{11} + \tilde U_{11}) + N_2 \qquad (14) \end{aligned}$$

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

3) For Frame $k = 3$: Now, each helper minimizes the s.d.o.f. of the other user by sending 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,

$$Z_1[3] = Z_1[1] + \frac{\alpha_2 h}{\tilde h_1} \tilde U_{12}, \quad Z_2[3] = Z_2[1] + \frac{\alpha_1 g}{\tilde g_2} \tilde U_{22} \quad (15)$$

Consequently, the received signals are,

$$Y_1[3] = Y_1[2] + \alpha_2 h \tilde U_{12} + \frac{\alpha_1 \tilde h_2 g}{\tilde g_2} \tilde U_{22} \qquad (16)$$

$$Y_2[3] = Y_2[2] + \alpha_1 g \tilde U_{22} + \frac{\alpha_2 \tilde g_2 h}{\tilde h_1} \tilde U_{12} \qquad (17)$$

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 Fig. 4. Note that, neither of the helpers can hold back its original jamming signal (i.e., each helper should append its previous signalling with new jamming signals), because if not, its previous message-carrying signals are compromised.

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).

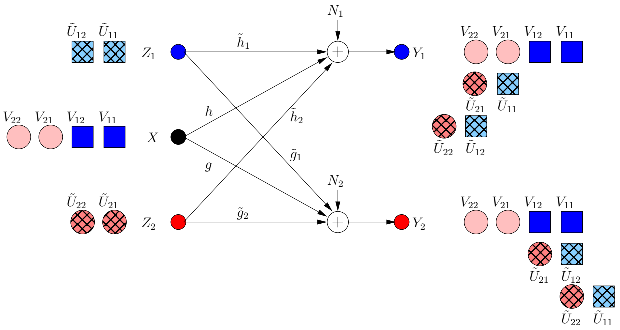
$\tilde U_{12}$ $\tilde U_{11}$
Z_1
$\tilde h_1$
N_1
Y_1
V_{22} V_{21} V_{12} V_{11}
$\tilde U_{21}$ $\tilde U_{11}$
$\tilde U_{22}$ $\tilde U_{12}$
V_{22} V_{21} V_{12} V_{11}
X
h
$\tilde h_2$
$\tilde g_1$
g
N_2
$\tilde U_{22}$ $\tilde U_{21}$
Z_2
$\tilde g_2$
Y_2
V_{22} V_{21} V_{12} V_{11}
$\tilde U_{21}$ $\tilde U_{12}$
$\tilde U_{22}$ $\tilde U_{11}$

Fig. 4. BCCM frame $k = 3$.

C. 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*

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

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: We give only a sketch of a proof here due to space limitations. At every encoding frame, the transmitter transmits PAM signals with parameters $Q_k = P^{\frac{1-\delta}{2(L_k+\delta)}}$ and $a_k = \gamma P^{\frac{1}{2}} / Q_k$. This satisfies the power constraint and ensures that the probability of error goes to zero as $P \to \infty$. From [1], the following rates are achievable for the BCCM,

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

By techniques similar to [2], we calculate $I(\mathbf{V}_1[k]; Y_1[k]) \geq \frac{J_k(1-\delta)}{L_k+\delta} \left(\frac{1}{2} \log P\right) + o(\log P)$, while the leakage rate is upper bounded by $o(\log P)$, as every message-carrying signal is protected by CJ signal. Taking limits concludes the proof. ■

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,*

$$d_i(k) = \begin{cases} 1/2, & k \text{ even} \\ \frac{k+1}{2k+4} \to 1/2, & k \text{ odd} \end{cases} \qquad (20)$$

I.e., the combating behaviour 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 (20). 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, transmitter can always add extra 2 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

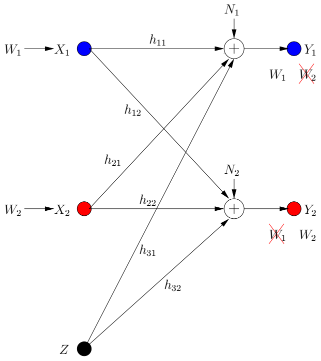

Fig. 5. ICCM with selfish users.

the transmitter uses the extra irrational dimension produced by jamming in odd frames in its favor, hence it adds one extra dimension corresponding to the new message-carrying signal. This results in the following simultaneous equations,

$$\frac{J_{k-2}}{L_{k-2}} = \frac{k-1}{2k}, \quad \frac{J_{k-1}}{L_{k-1}} = \frac{J_{k-2}+1}{L_{k-2}+1} = \frac{1}{2} \tag{21}$$

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 extra jamming component aligned with 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 $1/2$. ■

III. ICCM with Selfish Users

A. 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 Fig. 5 is given by,

$$Y_1[k] = h_{11}X_1[k] + h_{21}X_2[k] + h_{31}Z[k] + N_1[k] \tag{22}$$
$$Y_2[k] = h_{12}X_1[k] + h_{22}X_2[k] + h_{32}Z[k] + N_2[k] \tag{23}$$

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

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,

$$\max \quad d_i(k) - d_j(k) \tag{24}$$

where $i \neq j$, $i,j \in \{1,2\}$. The role of the users here is *less stringent* than 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 side of any of the users and maximizes the sum s.d.o.f. of the system,

$$\max \quad d_i(k) + d_j(k) \tag{25}$$

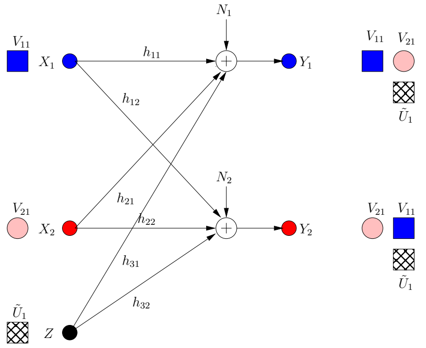

Fig. 6. ICCM frame $k = 0$. Pink circle and blue square denote user signals, and the hatched squares denote jamming signals.

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

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

1) For Frame $k = 0$: All nodes perform the optimal *selfless* strategy as in [2]. The transmitted signals are,

$$X_1[0] = \frac{h_{32}}{h_{12}}V_{11}, \quad X_2[0] = \frac{h_{31}}{h_{21}}V_{21}, \quad Z[0] = \tilde{U}_1 \tag{26}$$

The received signals at both receivers are (as in Fig. 6),

$$Y_1[0] = \frac{h_{32}h_{11}}{h_{12}}V_{11} + h_{31}(V_{21} + \tilde{U}_1) + N_1 \tag{27}$$
$$Y_2[0] = \frac{h_{31}h_{22}}{h_{21}}V_{21} + h_{32}(V_{11} + \tilde{U}_1) + N_2 \tag{28}$$

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

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 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,

$$X_1[1] = X_1[0] + \frac{h_{31}h_{22}}{h_{12}h_{21}}U_{11} \tag{29}$$
$$X_2[1] = X_2[0] + \frac{h_{32}h_{11}}{h_{12}h_{21}}U_{21} \tag{30}$$

Hence, the received signals in this case are,

$$\begin{aligned} Y_1[1] =& \frac{h_{32}h_{11}}{h_{12}}(V_{11} + U_{21}) + h_{31}(V_{21} + \tilde{U}_1) \\ &+ \frac{h_{31}h_{22}h_{11}}{h_{12}h_{21}}U_{11} + N_1 \end{aligned} \tag{31}$$
$$\begin{aligned} Y_2[1] =& \frac{h_{31}h_{22}}{h_{21}}(V_{21} + U_{11}) + h_{32}(V_{11} + \tilde{U}_1) \\ &+ \frac{h_{32}h_{12}h_{22}}{h_{12}h_{21}}U_{11} + N_2 \end{aligned} \tag{32}$$

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

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 individual user. Since the s.d.o.f. of

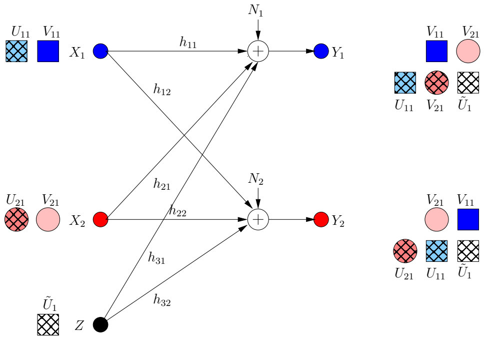

Fig. 7. ICCM frame $k = 1$.

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 extra jamming component in a new irrational dimension, which allows each user to produce extra secure signal. Thus,

$$X_1[2] = X_1[1] + \frac{\alpha_1 h_{32}}{h_{12}} V_{12} + \frac{h_{32} h_{11} h_{22}}{h_{12}^2 h_{21}} V_{13} \tag{33}$$

$$X_2[2] = X_2[1] + \frac{\alpha_1 h_{31}}{h_{21}} V_{22} + \frac{h_{31} h_{22} h_{11}}{h_{21}^2 h_{12}} V_{23} \tag{34}$$

$$Z[2] = Z[1] + \alpha_1 \tilde{U}_2 \tag{35}$$

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

$$\begin{aligned} Y_1[2] =& Y_1[1] + \alpha_1 h_{31}(V_{22} + \tilde{U}_2) + \frac{h_{31} h_{22} h_{11}}{h_{21} h_{12}} V_{23} \\ &+ \frac{\alpha_1 h_{32} h_{11}}{h_{12}} V_{12} + \frac{h_{32} h_{11}^2 h_{22}}{h_{12}^2 h_{21}} V_{13} \end{aligned} \tag{36}$$

$$\begin{aligned} Y_2[2] =& Y_2[1] + \alpha_1 h_{32}(V_{12} + \tilde{U}_2) + \frac{h_{32} h_{11} h_{22}}{h_{12} h_{21}} V_{13} \\ &+ \frac{\alpha_1 h_{31} h_{22}}{h_{21}} V_{22} + \frac{h_{31} h_{22} h_{11}}{h_{21}^2 h_{12}} V_{23} \end{aligned} \tag{37}$$

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

4) For General kth Frame: The s.d.o.f. differs 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 extra jamming signal from the system helper to protect more signals.

C. 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*

$$d_i(k) = \begin{cases} 0, & k \text{ odd} \\ \frac{2}{k+4} \to 0, & k \text{ even} \end{cases} \tag{38}$$

I.e., selfishness eventually precludes secure communication.

Proof: From [1], 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 extra jamming component allowing protection of one extra signals. Then, $J_k = \frac{k}{2} + 1 = \frac{k+2}{2}$.

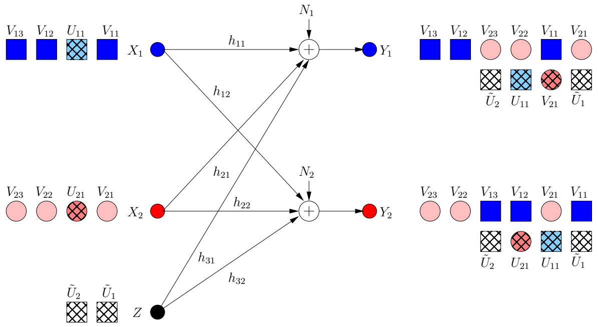

Fig. 8. ICCM frame $k = 2$.

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 (38) is true, then, $d_i(k-2) = \frac{2}{k+2}$. Then, from 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

$$d_i(k) = \frac{J_k}{L_k} = \frac{J_k}{L_{k-2} + 2J_k} = \frac{2}{k+4} \tag{39}$$

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

IV. Conclusion and Discussion

We introduced two new channel models as extensions of BCCM and ICCM to study the effects of selfishness and malicious behaviour on secrecy in networks. We derived achievable s.d.o.f. for both systems. The models are different but 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, transmitter in BCCM can send useful signals, but 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. The presented schemes are only achievable, new role-based converse arguments are needed.

References

[1] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates. Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions. *IEEE Trans. on Info. Theory*, 54(6):2493–2507, June 2008.

[2] 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.

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

[4] A. S. Motahari, S. O. Gharan, M.-A. Maddah-Ali, and A. K. Khandani. Real interference alignment: Exploiting the potential of single antenna systems. *IEEE Trans. on Info. Theory*, 60(8):4799–4810, August 2014.