Secure Degrees of Freedom on Widely Linear Instantaneous Relay-Assisted Interference Channel

Zuleita Ho and Eduard Jorswieck
Institut für Nachrichtentechnik
Fakultät Elektro- und Informationstechnik
Technische Universität Dresden
{zuleita.ho, eduard.jorswieck}@tu-dresden.de

***Abstract*— The number of secure data streams a relay-assisted interference channel can support has been an intriguing problem. The problem is not solved even for a fundamental scenario with a single antenna at each transmitter, receiver and relay. In this paper, we study the achievable secure degrees of freedom of instantaneous relay-assisted interference channels with real and complex coefficients. The study of secure degrees of freedom with complex coefficients is not a trivial multiuser extension of the scenarios with real channel coefficients as in the case for the degrees of freedom, due to secrecy constraints. We tackle this challenge by jointly designing the improper transmit signals and widely-linear relay processing strategies.**

***Index Terms*— instantaneous relay channel; widely linear; secure degrees of freedom; interference neutralization; information leakage neutralization; real interference alignment**

I. Introduction

The number of secure data streams supported in a wireless system using purely physical layer security techniques - as an ever increasingly popular topic - provides additional protection to conventional cryptographic techniques. There are several well-studied approaches to improve physical layer security, e.g., artificial noise from helpers or from built-in source signals [1], lattice code [2], interference alignment with secrecy precoding [3] and neutralization [4]. In a single-antenna relay-assisted interference channel with confidential messages, we propose to apply the combination of interference neutralization (by choosing the relay strategy smartly) and *real interference alignment* [5], [6] which combines transmit symbol constellation design and artificial noise transmission.

A. Non-trivial secure degrees of freedom in complex channel

The term *real interference alignment* is due to the application of Khintchine-Groshev theorem of Diophantine approximation in number theory on the estimation of integers (desired symbols) from real numbers (received signals). An assumption of real channel coefficients are conventionally assumed. If the degrees of freedom (DoF) is considered, the scenarios of complex channel coefficients can be straight-forwardly extended from that of real channel coefficients. As the real and imaginary parts of all transmitter-receiver pairs can be paired up and the complex system is equivalent to a real system with double the number of transmitter-receiver pairs. However, this is not the case if secure degrees of freedom (sDoF) is considered. When sDoF is concerned, each transmitter i's signal should be protected from being eavesdropped by receiver j, for $i \neq j$. If we treat the real and and imaginary streams of transmitter i's complex signals as two transmitters: i_1, i_2, then the symbol i_1 should be protected from that of i_2 at the receiver side. However, the information of i_1 received at i_2 is not a *leakage* because this corresponds to the scenario when the imaginary part of the received signal of i contains part of the real part of the transmit signal of i. Hence, the extension of sDoF in complex channel from the real channel is not trivial.

To achieve the desired complex sDoF, we observe that (i) the transmit signals are improper signals, in our case pulse amplitude modulation (PAM) and with different constellation size in the real and imaginary part of the signals; (ii) widely-linear processing should be applied at the relay. Improper signals have essential applications in wireless communications including a wide range of modulation techniques such as binary phase shift keying (BPSK), amplitude shift keying (ASK) and Gaussian minimum-shift keying (GMSK). The term *improper* describes statistical properties of complex signals. In particular, improper signals are complex signals that have (i) different power in the real and imaginary parts (I/Q imbalance) and/or (ii) correlation between the real and imaginary parts. Widely-linear processing are signal processing techniques that take into consideration the complete second order statistics of the signal, both the covariance and the pseudo-covariance [7]. It is shown to achieve a smaller MSE in various systems than conventional linear minimum MSE filter [8], [9] and is incorporated into various standards including GSM [10], [11] and 3GPP [12]. While most works on widely-linear techniques [13] and references therein are applied on receive processing, recently it is adopted in transmit filter design for performance enhancement [14], [15]. Here, it is applied at the relay design to enhance sDoF of the system.

B. Preliminary

***Definition** 1 ([5]):* The rational dimension of a set of real numbers $\{h_1, \dots h_M\}$ is m if there exists a set of real numbers $\{H_1, \dots H_m\}$ such that each h_i can be represented as a rational combination of H_j's, $h_i = \alpha_{i1}H_1, \dots, \alpha_{im}H_{im}$ where $\alpha_{ik} \in \mathbb{Q}$ for all $k = 1, \dots, m$, where $\mathbb{Q}$ is the set of rational numbers. In particular, $\{h_1, \dots, h_M\}$ are rationally

This work has been performed in the framework of the European research project DIWINE, which is partly funded by the European Union under its FP7 ICT Objective 1.1 - The Network of the Future. This work is partly supported in part by the German Research Foundation (DFG) in the Collaborative Research Center 912 "Highly Adaptive Energy-Efficient Computing".

independent if the rational dimension is M, i.e., none of the numbers can be represented as a rational combination of other numbers.

***Lemma** 1 ([5], [6]): Lower bound of minimum distance using the Khintchine-Groshev theorem:* If a received constellation of the following form

$$y = G_0 x + G_1 I + n$$

and the desired signal x and interference I are integers in a PAM constellation set $[-Q_0, Q_0]$ and $[-Q_1, Q_1]$ respectively, then by the Khintchine-Groshev theorem, the minimum distance between the received constellation points undergoing hard decoding is lower bounded by

$$d_{min} > \frac{\kappa G_0}{\max(Q_0, Q_1)^{1+\epsilon}} \tag{1}$$

where κ, ϵ are constants. The corresponding error probability is upper bounded by

$$P_e < \exp\left(-\frac{(\kappa G_0)^2}{8\sigma^2 \max(Q_0, Q_1)^{2(1+\epsilon)}}\right). \tag{2}$$

The variable σ^2 defines the variance of the noise signal n.

II. System Model

We assume two transmitters where each transmitter aims to transmit a secure message to its target receiver and is interested in eavesdropping the message from the other user. These two transmitters are assisted by a single-antenna relay. We assume that the point-to-point links in the interference channel are assisted by inherit layer-1 relays (simple repeaters), such as in LTE systems. These repeaters are only capable of amplify-and-forward and not able to adapt its forwarding strategies. A smart relay is introduced to the system. The equivalent network can be modeled as an instantaneous relay interference channel (IRIC) in which the signals from the transmitters through the smart relay and through the layer-1 relays arrive at the receivers at the same time [16], [17], see Figure 4.

Denote the complex channel gain from transmitter i, $i = 1, 2$, to relay as f_i and the complex channel from relay to receiver i as g_i. The complex transmit symbol from transmitter i is denoted as x_i with transmit power constraint P. The relay received signal is $y_r = \sum_{k=1}^{2} f_k x_k + n_r$ where the noise n_r is a circular Gaussian noise with identity matrix as covariance. The received signal at receiver i is given by

$$y_i = \sum_{k=1}^{2} (g_i r f_k + h_{ik}) x_k + g_i r n_r + n_i. \tag{3}$$

Denote the achievable secrecy rate of transmitter-receiver pair i as R_{si} and R_{rsi} in systems with complex and real channel coefficients respectively. The sum secure degrees-of-freedom (sDoF) of a system with complex channel coefficients is given by

$$D^{cs} = \lim_{P\to\infty} \frac{R_{s1} + R_{s2}}{\log_2 P}. \tag{4}$$

In the case when the channel coefficients are real numbers, the achievable sum sDoF is then given by

$$D^{rs} = \lim_{P\to\infty} \frac{R_{rs1} + R_{rs2}}{\frac{1}{2}\log_2 P}. \tag{5}$$

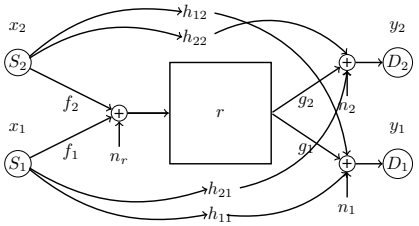

Fig. 1. A system model for a layer-1 relay-assisted single-user system.

The idea of real interference alignment is conventionally applied to scenarios in which the channel coefficients are real numbers. In the following we briefly review the known results of sDoF on real IC. Then we apply the real interference alignment technique to compute an achievable sDoF on real IRIC. We then extend the sDoF results to the scenarios with complex coefficients. We show that the achievable sDoF in channels with complex coefficients with a layer-1 relay is only 2/3 whereas the proposed widely linear relay can achieve 1 sDoF.

A. sDoF of real IC with confidential messages, $D^{rs} = 2/3$

We review briefly the sDoF results on two-user IC with confidential messages with the application of real interference alignment [6]. The received signal of receiver i, $i = 1, 2$, is given by

$$y_i = h_{ii} x_i + h_{ij} x_j + n_i \tag{6}$$

where $j = 1, 2, j \neq i$ and the channel coefficients h_{ij} are real. The transmitters transmit signals that are a weighted sum of a data symbol u_i and a noise symbol v_i,

$$x_i = u_i + \frac{h_{ij}}{h_{ii}} v_i. \tag{7}$$

The symbols u_1, u_2, v_1, v_2 are all integer symbols chosen from the constellation set $[-Q, Q]$. Note that the noise symbol v_i is used to protect the data from transmitter j, u_j, from being eavesdropped by receiver i. This can be applied in the scenarios where the transmitters are trusted and cooperate to prevent malicious receivers from eavesdropping. The received signal y_i can be written as

$$y_i = h_{ii} u_i + h_{ij}(u_j + v_i) + \frac{h_{ij} h_{ji}}{h_{jj}} v_j + n_i. \tag{8}$$

The symbols u_j and v_i are *aligned* at receiver i because the sum of integers are also an integer and thus a valid constellation point. At high SNR, the noise is dominated and the received signal $y_i - n_i$ is a linear sum of three integer symbols weighted by real channel coefficients. From Definition 1, the rational dimension of $\{h_{ii}, h_{ij}, \frac{h_{ij}h_{ji}}{h_{jj}}\}$ is three, as shown in Figure 2. It can be shown that the leakage signal u_j is masked by noise signal v_i at receiver i, in a subspace of dimension $1/3$. Its data signal u_i is retrieved in $1/3$ of real dimension and thus a total of $D^{rs} = 2/3$ is achieved.

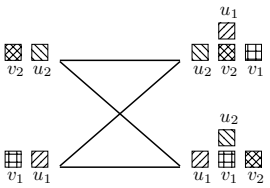

Fig. 2. The sDoF $D^{rs} = 2/3$ of an interference channel with real coefficients with confidential messages is achievable [6]. At receiver i, the desired symbol u_i is in a subspace of dimension $1/3$ whereas the leakage symbol u_j aligns with noise symbol v_i in a subspace of dimension $1/3$ and the noise symbol v_j spans a dimension of $1/3$.

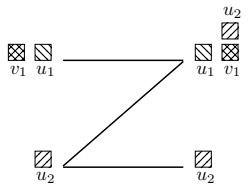

Fig. 3. The sDoF $D^{rs} = 1$ of a layer-1 relay assisted interference channel with real coefficients with confidential messages is achievable. The layer-1 relay neutralizes a leakage link and converts the interference relay channel to an equivalent Z channel. Transmitter two enjoys a leakage free channel whereas the leakage symbol u_2 aligns with noise symbol v_1 at receiver one in a subspace of dimension $1/2$. The desired symbol is in a subspace of dimension $1/2$.

B. sDoF of real IRIC, $D^{rs} = 1$

Motivated by the result described in previous subsection, we propose the following novel sDoF achievable scheme for the real IRIC. In particular, the relay instead of performing cooperative jamming, is chosen to neutralize one leakage link. Without loss of generality, we choose the relay amplification scalar r such that the information leakage from transmitter one to receiver two is neutralized. The interference channel reduces to a Z channel by setting the equivalent channel from transmitter one to receiver two to zero:

$$g_2 r f_1 + h_{21} = 0. \tag{9}$$

Or equivalently, $r = -\frac{h_{21}}{g_2 f_1}$. Hence, the channel input-output equation becomes

$$\begin{aligned} y_1 &= z_{11}x_1 + z_{12}x_2 + n_1, \\ y_2 &= z_{22}x_2 + n_2 \end{aligned} \tag{10}$$

where $z_{11} = h_{11} - \frac{h_{21}g_1}{g_2}$, $z_{12} = h_{12} - \frac{h_{21}g_1 f_2}{g_2 f_1}$ and $z_{22} = h_{22} - \frac{h_{21}f_2}{f_1}$. Here we apply the idea of real interference alignment [5]. The transmit signal x_1 is a linear sum of a desired signal u_1 and a noise symbol v_1 whereas x_2 consists of only the desired signal u_2. All signals u_1, v_1, u_2 are integers in constellation set $[-Q, Q]$. The value of the constant Q is chosen such that the constellation size scales with the transmit power P; consequently the minimum distance of the constellation points at the receiver scales with P; thus the decoding error probability converges to zero when P goes to infinity. Let

$$x_1 = A\left(u_1 + \frac{z_{12}}{z_{11}}v_1\right), \qquad x_2 = Au_2. \tag{11}$$

The scalar A is chosen to satisfy the transmit power constraints at the transmitters. The input-output relation becomes

$$\begin{aligned} y_1 &= A\left(z_{11}u_1 + z_{12}(u_2 + v_1)\right) + n_1, \\ y_2 &= Az_{22}u_2 + n_2. \end{aligned} \tag{12}$$

The noise signal v_1 aligns with the information leakage u_2 in the sense that the sum of signals $u_2 + v_1$ is also an a valid constellation point in a constellation $[-2Q, 2Q]$ with enlarged cardinality. The alignment scheme is shown in Figure 3.

1) Proof of achievablility of sDoF: Due to space limitation, we can only provide the key steps in the following. From Definition 1 we see that $\{z_{11}, z_{12}\}$ are rationally independent except for a subset of channel coefficients of probability zero. t can be shown that the following secrecy rates are achievable:

$$\begin{aligned} R_{rs1} &= I(u_1; y_1) \\ R_{rs2} &= I(u_2; y_2) - I(u_2; y_1|u_1). \end{aligned} \tag{13}$$

We choose the constellation of u_1, u_2, v_1 in (12) to be $Q = \lfloor \gamma P^{\frac{1-\epsilon}{2(2+\epsilon)}} \rfloor$ and the power normalization factor $A = P^{1/2}/Q$. From Lemma 1, the error probability of decoding u_1 at receiver one goes to zero when $P \to \infty$. The desired mutual information can be lower bounded using the above error probability lower bound [6],

$$I(u_1; y_1) \quad > \frac{1-\epsilon}{2(2+\epsilon)}\left(1 - \exp\left(-\kappa' P^{\epsilon}\right)\right)\left(\log_2 P + \tau_1\right) - 1 \tag{14}$$

for some constant τ_1. Thus, we see that the achievable sDoF of transmitter-receiver pair one is given by

$$D_{rs1} = \lim_{P\to\infty} \frac{I(u_1; y_1)}{0.5 \log_2 P} > \frac{1}{2}. \tag{15}$$

Now we compute the achievable sDoF of transmitter-receiver pair two. Note that there is no interference at receiver two. Similar to the argument above, we obtain

$$I(u_2; y_2) > \frac{1-\epsilon}{2(2+\epsilon)}\left(1 - \exp\left(-\kappa_2 P^{\epsilon'}\right)\right)\left(\log_2 P + \tau_2\right) - 1$$

for some positive constants $\epsilon', \kappa_2, \tau_2$. The leakage information can be upper bounded in the following

$$I(u_2; y_1|u_1) < I(u_2; u_2 + v_1) \quad \leq \log_2(4Q) - \log_2(2Q) = 1.$$

Hence, the achievable sDoF of transmitter-receiver pair two is given by

$$D_{rs2} = \lim_{P\to\infty} \frac{I(u_2; y_2) - I(u_2; y_1|u_1)}{0.5 \log_2 P} > \frac{1}{2}. \tag{16}$$

The sDoF of transmitter-receiver pair two is only 1/2 despite the fact that it enjoys an interference free AWGN channel. The reason is that the constellation size of u_2 chosen for secrecy alignment at receiver one is smaller than what it can be for the AWGN link alone. If the constellation size for u_2 is chosen to be too large, the noise signal v_1 cannot completely mask it and the data is no longer secure. The total sDoF achievable is thus $D^{rs} = 1$. An instantaneous relay increases the sDoF of the system by $1/3$. This result draws parallels with the sDoF achievability scheme for an

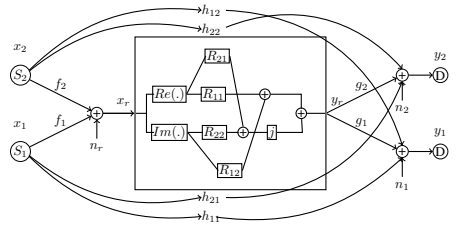

Fig. 4. A system model for the proposed optimum relay design for improper source signals. The value R_{ij} is the (i,j)-th element of the relay matrix $\mathbf{R}$.

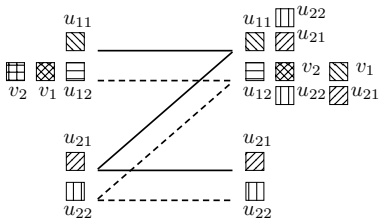

Fig. 5. The complex sDoF $D^{cs} = 2/3$ of a layer-1 relay assisted interference channel with real coefficients with confidential messages is achievable. The layer-1 relay neutralizes a leakage link and converts the interference relay channel to an equivalent Z channel. Transmitter two enjoys a leakage free channel. The complex channel is treated as a two-by-two real systems and each transmitter i is able to securely transmit two real symbols u_{i1}, u_{i2} with each in a subspace of dimension $1/3$.

two-user interference channel with one helper [6] who sends artificial noise to confuse eavesdroppers. On the other hand, the instantaneous relay here is responsible for neutralizing a leakage link, ensuring zero leakage without the assumption of a wiretap code [18]. In the following, we investigate how to extend the above results when the channel coefficients are complex numbers.

III. WIDELY LINEAR RELAY PROCESSING

In this section, we extend the results above to scenarios with complex channel coefficients. First we compute the achievable sDoF of the complex IC assisted with a layer-1 relay. Then we show that it is possible to improve the achievable sDoF by applying widely linear relay processing at the relay. The channel coefficients and transmit symbols in (3) are assumed to be complex. We denote the covariance matrix of $\mathbf{x}_i = [\mathrm{Re}(x_i), \mathrm{Im}(x_i)]^{\mathrm{T}}$ as $\mathbf{Q}_i = \tilde{\mathbf{P}}_i \tilde{\mathbf{P}}_i^{\mathrm{H}}$. If x_i is circular, then $\mathbf{Q}_i$ is a scaled identity matrix. To facilitate the demonstration, we write $\mathbf{x}_i = \tilde{\mathbf{P}}_i \, \mathbf{s}_i$ where $\mathbf{s}_i$ has zero mean and identity covariance matrix and $\tilde{\mathbf{P}}_i$ is treated as a precoding matrix over the real-valued domain. The equivalent real-valued representation to (3) is written as

$$\mathbf{y}_i = \sum_{k=1}^{2} \left(\mathbf{G}_i \, \mathbf{R} \, \mathbf{F}_k + \mathbf{H}_{ik} \right) \tilde{\mathbf{P}}_k \, \mathbf{x}_k + \mathbf{G}_i \, \mathbf{R} \, \mathbf{n}_r + \mathbf{n}_i \, . \quad (17)$$

which is shown in Figure 4. Denote $|g_i|, |f_k|, |h_{ik}|$ as the magnitudes of the channel realization g_i, f_k, h_{ik} and $\phi_{g_i}, \phi_{f_k}, \phi_{h_{ik}}$ are the corresponding phase angles. The real-valued channel matrices $\mathbf{F}_k$, $\mathbf{G}_i$ and $\mathbf{H}_{ik}$ are written as, $\mathbf{F}_k = |f_k| \, \mathbf{J}_{\phi_{f_k}}$, $\mathbf{G}_i = |g_i| \, \mathbf{J}_{\phi_{g_i}}$ and $\mathbf{H}_{ik} = |h_{ik}| \, \mathbf{J}_{\phi_{h_{ik}}}$, where $\mathbf{J}(.)$ is a rotation matrix [19], $\mathbf{J}(\theta) = [\cos(\theta), -\sin(\theta); \sin(\theta), \cos(\theta)]$.

A. sDoF of complex IC with a layer-1 relay, $D^{cs} = 2/3$

With a layer-1 relay, the relay matrix $\mathbf{R}$ is given as $\mathbf{R} = |r| \, \mathbf{J}(\phi_r)$ where $|r|$ and ϕ_r are the magnitude and phase angles of the complex relay amplification scalar. We perform the same information leakage neutralization as in (9), $\mathbf{G}_2 \, \mathbf{R} \, \mathbf{F}_1 + \mathbf{H}_{21} = \mathbf{0}_2$, by setting $|r| = \frac{|h_{21}|}{|g_2||f_1|}$ and $\phi_r = \phi_{h_{21}} - \phi_{f_1} - \phi_{g_2}$. With the above specified relay matrix $\mathbf{R}$, denote the equivalent channel by $\bar{\mathbf{H}}_{ij} = \mathbf{H}_{ij} + \mathbf{G}_i \, \mathbf{R} \, \mathbf{F}_j$. We choose the beamforming matrix to be $\tilde{\mathbf{P}}_i = \bar{\mathbf{H}}_{ii}^{-1}$. The input-output relationship becomes

$$\begin{aligned} \mathbf{y}_1 &= \mathbf{x}_1 + \bar{\mathbf{H}}_{12} \bar{\mathbf{H}}_{22}^{-1} \, \mathbf{x}_2 + \mathbf{G}_1 \, \mathbf{R} \, \mathbf{n}_r + \mathbf{n}_1 \\ \mathbf{y}_2 &= \mathbf{x}_2 + \mathbf{G}_2 \, \mathbf{R} \, \mathbf{n}_r + \mathbf{n}_2 \, . \end{aligned} \quad (18)$$

Denote the matrix product $\tilde{\mathbf{H}} = \bar{\mathbf{H}}_{12} \, \mathbf{H}_{22}$, $\tilde{\mathbf{n}}_i = \mathbf{G}_i \, \mathbf{R} \, \mathbf{n}_r + \mathbf{n}_i$ and the corresponding (i,j)-th element $[.]_{(i,j)}$. Let the transmit signals to be

$$\begin{aligned} \mathbf{x}_1 &= \left[u_{11}, u_{12} + \frac{a[\tilde{\mathbf{H}}]_{(2,1)}}{[\tilde{\mathbf{H}}]_{(1,1)}} v_1 + \frac{a[\tilde{\mathbf{H}}]_{(2,2)}}{[\tilde{\mathbf{H}}]_{(1,2)}} v_2 \right]^{\mathrm{T}} \\ \mathbf{x}_2 &= \left[\frac{a u_{21}}{[\tilde{\mathbf{H}}]_{(1,1)}}, \frac{a u_{22}}{[\tilde{\mathbf{H}}]_{(1,2)}} \right]^{\mathrm{T}} \end{aligned} \quad (19)$$

for a real scalar a. Receiver i decodes the signal from real y_{i1} and complex domain y_{i2} separately.

$$\begin{aligned} y_{11} &= u_{11} + a(u_{21} + u_{22}) + [\tilde{\mathbf{n}}_1]_{(1)} \, , \\ y_{12} &= u_{12} + \frac{a[\tilde{\mathbf{H}}]_{(2,1)}}{[\tilde{\mathbf{H}}]_{(1,1)}} \left(u_{21} + v_1 \right) \\ &\quad + \frac{a[\tilde{\mathbf{H}}]_{(2,2)}}{[\tilde{\mathbf{H}}]_{(1,2)}} \left(u_{22} + v_2 \right) + [\tilde{\mathbf{n}}_1]_{(2)} \, , \\ y_{21} &= \frac{a u_{21}}{[\tilde{\mathbf{H}}]_{(1,1)}} + [\tilde{\mathbf{n}}_2]_{(1)} \, , \\ y_{22} &= \frac{a u_{22}}{[\tilde{\mathbf{H}}]_{(1,2)}} + [\tilde{\mathbf{n}}_2]_{(2)} \, . \end{aligned} \quad (20)$$

As shown in Figure 5, all the desired signals u_{ij} are secure[1]. The detailed proof follows the steps in Section II-B and is omitted here due to space limit. At receiver one, the desired signal u_{12} is a subspace of dimension $1/3$ whereas the leakage symbol u_{21} is protected by alignment with v_1 and u_{22} is protected by v_2, each in a subspace of dimension $1/3$. This means that the dimensions of all desired signals u_{ij} are $1/3$ and a total of $D^{cs} = 2/3$ is achieved.

B. sDoF of a complex IC with a widely linear relay, $D^{cs} = 1$

With widely linear relay processing, the relay matrix is written in real-valued domain as $\mathbf{R} \in \mathbb{R}^{2\times 2}$. This allows the relay to scale and rotate the real and imaginary part of the input signal differently. We choose the relay matrix $\mathbf{R}$ such that the imaginary dimension from transmitter one to receiver

[1]Due to the statistical independence of u_{12} and u_{22}, the alignment of them is no different from aligning a secret message with an artificial noise message. Hence a joint decoding of u_{12}, u_{22} does not improve performance of the eavesdropper.

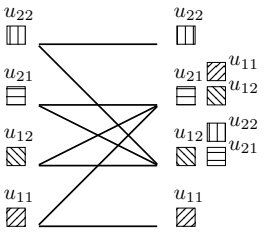

Fig. 6. The complex sDoF $D^{cs} = 1$ of a widely-linear relay assisted interference channel with real coefficients with confidential messages is achievable. The widely-linear relay neutralizes half of a leakage link for each receiver. Each transmitter i transmits with improper signaling and is able to securely transmit two real symbols u_{i1}, u_{i2} with each in a subspace of dimension $1/2$.

two and the real dimension from transmitter two to receiver one are neutralized,

$$\left[\bar{\mathbf{H}}_{21}\right]_{(2,:)} = \mathbf{0}_{1\times 2},\ \left[\bar{\mathbf{H}}_{12}\right]_{(1,:)} = \mathbf{0}_{1\times 2}, \tag{21}$$

Equivalently, we have

$$\begin{aligned} \left[\mathbf{H}_{21}\right]_{(2,:)} + \left[\mathbf{G}_2\,\mathbf{R}\,\mathbf{F}_1\right]_{(2,:)} &= \mathbf{0}_{1\times 2}, \\ \left[\mathbf{H}_{12}\right]_{(1,:)} + \left[\mathbf{G}_1\,\mathbf{R}\,\mathbf{F}_2\right]_{(1,:)} &= \mathbf{0}_{1\times 2}\,. \end{aligned} \tag{22}$$

Vectorize both sides and combine both criteria, we see that the relay matrix satisfies

$$\mathrm{vec}(\mathbf{R}) = -\begin{bmatrix} \mathbf{F}_1^{\mathrm{T}} \otimes \left[\mathbf{G}_2\right]_{(2,:)} \\ \mathbf{F}_2^{\mathrm{T}} \otimes \left[\mathbf{G}_1\right]_{(1,:)} \end{bmatrix}^{-1} \begin{bmatrix} \mathrm{vec}\left(\left[\mathbf{H}_{21}\right]_{(2,:)}\right) \\ \mathrm{vec}\left(\left[\mathbf{H}_{12}\right]_{(1,:)}\right) \end{bmatrix}.$$

Denote the equivalent second channel from source 2 to destination 1 as $\mathbf{q}_{12}^{\mathrm{T}}$ and the first channel from source 1 to destination 2 as $\mathbf{q}_{21}^{\mathrm{T}}$. The input-output equation in (17) becomes

$$\begin{aligned} \mathbf{y}_1 &= \mathbf{P}_1\,\mathbf{x}_1 + \left[\mathbf{0}_{1\times 2}; \mathbf{q}_{12}^{\mathrm{T}}\right]\bar{\mathbf{H}}_{22}^{-1}\,\mathbf{P}_2\,\mathbf{x}_2 + \mathbf{G}_1\,\mathbf{R}\,\mathbf{n}_r + \mathbf{n}_1, \\ \mathbf{y}_2 &= \left[\mathbf{q}_{21}^{\mathrm{T}}; \mathbf{0}_{1\times 2}\right]\bar{\mathbf{H}}_{11}^{-1}\,\mathbf{P}_1\,\mathbf{x}_1 + \mathbf{P}_2\,\mathbf{x}_2 + \mathbf{G}_2\,\mathbf{R}\,\mathbf{n}_r + \mathbf{n}_2\,. \end{aligned}$$

To simplify the notation, we denote $\tilde{q}_{12}^{\mathrm{T}} = \mathbf{q}_{12}^{\mathrm{T}}\bar{\mathbf{H}}_{22}^{-1}$. We observe that at destination one, the desired signal $\mathbf{x}_1$ is spread over both channels whereas the information leakage arrives only at the second channel. We write the first and second element of the received signal $\mathbf{y}_1$ as y_{11} and y_{12}. Now, we choose $\mathbf{P}_i = \mathbf{I}_2$ and

$$\mathbf{x}_1 = \left[\frac{bx_{11}}{\left[\tilde{\mathbf{q}}_{21}\right]_{(1)}}, \frac{bx_{12}}{\left[\tilde{\mathbf{q}}_{21}\right]_{(2)}}\right]^{\mathrm{T}},\ \mathbf{x}_2 = \left[\frac{ax_{21}}{\left[\tilde{\mathbf{q}}_{12}\right]_{(1)}}, \frac{ax_{22}}{\left[\tilde{\mathbf{q}}_{12}\right]_{(2)}}\right]^{\mathrm{T}}.$$

The received signal at destination one is given by

$$\begin{aligned} y_{11} &= \frac{bx_{11}}{\left[\tilde{\mathbf{q}}_{21}\right]_{(1)}} + \left[\tilde{\mathbf{n}}_1\right]_{(1)} \\ y_{12} &= x_{12} + a(x_{21} + x_{22}) + \left[\tilde{\mathbf{n}}_1\right]_{(2)}\,. \end{aligned} \tag{23}$$

The received signal at destination two can be written similarly and thus is omitted here. As shown in Figure 6, transmitter i only transmits desired symbols u_{i1}, u_{i2}. The receivers decode the desired symbol in each domain. The leakage symbol is protected by the unwanted symbol in that domain. We see that each desired symbol is in a subspace of dimension $1/2$ and a total of $D^{cs} = 1$ is achieved. The detailed proof follows the steps in Section II-B and is omitted here due to space limit.

We have shown above an achievability scheme of sDoF on complex IRIC. The advantages of the proposed scheme is three-fold. First, it is an sDoF achievability scheme on complex IRIC which is novel. Second, the proposed scheme with widely linear relay achieves 1/3 higher sDoF than that of layer-1 relay. Third, the proposed scheme is of higher power efficiency over those on real channels as all the transmit power here is spent on desired symbols and no power on noise symbols.

REFERENCES

[1] J. Huang and A. L. Swindlehurst, "Cooperative Jamming for Secure Communications in MIMO Relay Networks," *IEEE Transaction on Signal Processing*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[2] X. He and A. Yener, "Providing Secrecy With Structured Codes : Tools and Applications to Two-User Gaussian Channels," *preprint, available at http://arXiv:0907.5388v1*, 2009.

[3] O. O. Koyluoglu, H. El Gamal, L.-F. Lai, and H. V. Poor, "Interference Alignment for Secrecy," *IEEE Transactions on Information Theory*, vol. 57, no. 6, pp. 3323– 3332, 2011.

[4] Z. K.-M. Ho, E. Jorswieck, and S. Gerbracht, "Information Leakage Neutralization for the Relay-Assisted Multi-Carrier Interference Channel," *preprint, available at http://tnt.wcms-file2.tu-dresden.de/BibtexDbMng/upload/ZG12.pdf*, 2012.

[5] Abolfazl Seyed Motahari, Shahab Oveis Gharan, Mohammad-Ali Maddah-Ali, and Amir Keyvan Khandani, "Real Interference Alignment: Exploiting the Potential of Single Antenna Systems," Aug. 2009.

[6] J. Xie and S. Ulukus, "Secure Degrees of Freedom of One-hop Wireless," *preprint, available at http://arXiv:1209.5370v1*, pp. 1–44, 2012.

[7] P. Chevalier and B. Picinbono, "Widely Linear Estimation with complex data," *IEEE Transaction on Signal Processing*, vol. 43, pp. 2030– 2033, 1995.

[8] W. H. Gerstacker, R. Schober, and A. Lampe, "Receivers with Widely Linear Processing for Frequency-Selective Channels," *IEEE Transactions on Communications*, vol. 51, pp. 1512 – 1523, 2003.

[9] P. Chevalier and F. Dupuy, "Widely Linear Alamouti Receiver for the Reception of Real-Valued Constellations Corrupted by Interferences - The Alamouti-SAIC/MAIC Concept," *IEEE Transactions on Signal Processing*, vol. 59, no. 7, pp. 3339–3354, July 2011.

[10] D. Astely, M. Kristensson, and B. Ottersten, "Receiver and Method for Rejecting Cochannel Interference, Patent no. EP1301997B1," 2005.

[11] R. Meyer, W. H. Gerstacker, R. Schober, and J. B. Huber, "A Single Antenna Interference Cancellation Algorithm for Increased GSM Capacity," *IEEE Transactions on Wireless Communications*, vol. 5, no. 7, pp. 1616– 1621, 2006.

[12] "MUROS Uplink Receiver Performance," *3GPP TSG Geran Tdoc GP-090114, ST-NXP Wireless France, Com-Research, GERAN no. 41*, 2009.

[13] T. Adali, P. J. Schreier, and L. L. Scharf, "Complex-Valued Signal Processing: The Proper Way To Deal With Impropriety," *IEEE Transactions on Signal Processing*, vol. 59, no. 11, pp. 5101–5125, 2011.

[14] Z. K.-M. Ho and E. Jorswieck, "Improper Gaussian Signaling On The Two-User SISO Interference Channel," *IEEE Transactions on Wireless Communications*, vol. 11, no. 9, pp. 3194 – 3203, 2011.

[15] Y. Zeng, C. M. Yetis, E. Gunawan, Y. L. Guan, and R. Zhang, "Improving achievable rate for the two-user SISO interference channel with improper Gaussian signaling," in *IEEE Asilomar Conference on Signals, Systems and Computers, 2012. (Invited)*.

[16] A. El Gamal and N. Hassanpour, "Relay-without-Delay," in *Proceedings of International Symposium on Information Theory*, 2005, vol. 1, pp. 1078–1080.

[17] Z. K.-M. Ho and E. Jorswieck, "Instantaneous Relaying: Optimal Strategies and Interference Neutralization," *IEEE Transactions on Signal Processing*, vol. 60, no. 12, pp. 6655 – 6668, Dec. 2012.

[18] M. Bloch and J. Barros, *Physical Layer Security From Information Theory to Security Engineering*, Cambridge University Press, 2011.

[19] G. A. F. Seber, *A Matrix Handbook For Statisticians*, John Wiley & Sons, Inc., Dec. 2008.