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 straightforwardly 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 ≠ j. If we treat the real and and imaginary streams of transmitter i’s complex signals as two transmitters: i1, i2, then the symbol i1 should be protected from that of i2 at the receiver side. However, the information of i1 received at i2 is not a leakage because this corresponds to the scenario where 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 matrix. 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, \ldots, h_M\} is m if there exists a set of real numbers \{H_1, \ldots, H_m\} such that each h_i can be represented as a rational combination of H_j’s, h_i = \alpha_{i1}H_1, \ldots, \alpha_{im}H_m where \alpha_{ik} \in \mathbb{Q} for all k = 1, \ldots, m, where \mathbb{Q} is the set of rational numbers. In particular, \{h_1, \ldots, h_M\} are rationally independent.
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

\[ d_{\text{min}} > \frac{\kappa G_0}{\max(Q_0, Q_1)^{1+\epsilon}} \]

where \( \kappa, \epsilon \) are constants. The corresponding error probability is upper bounded by

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

The variable \( \sigma^2 \) 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

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

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

\[ D^{cs} = \lim_{P \to \infty} \frac{R_{s1} + R_{s2}}{\log_2 P}. \]

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

\[ D^{rs} = \lim_{P \to \infty} \frac{R_{r1} + R_{r2}}{2 \log_2 P}. \]

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

\[ y_i = h_{ii} x_i + h_{ij} x_j + n_i \]

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 \( v_i \).

\[ x_i = u_i + \frac{h_{ij}}{h_{ii}} v_i. \]

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

\[ y_i = h_{ii} u_i + h_{ij} (u_j + v_i) + \frac{h_{ij} h_{ji}}{h_{ii}} v_j + n_i. \]

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 \( \{h_{ii}, h_{ij}, h_{ij} h_{ji}\} \) 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 \( u_j \) is retrieved in 1/3 of real dimension and thus a total of \( D^{rs} = 2/3 \) is achieved.
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. The desired symbol is in a subspace of dimension 1/2. The leakage information can be upper bounded in the following

\[
I(u_2; y_1) < I(u_2; u_2 + v_1) \leq \log_2(4Q) - \log_2(2Q) = 1.
\]

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

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

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
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, the channel coefficients and transmit symbols at the relay. The channel coefficients and transmit symbols are the corresponding phase angles. The equivalent channel by $\tilde{G}_i = |g_i|\tilde{J}_{\phi_{g_i}}$, $\tilde{h}_{ik} = |h_{ik}|\tilde{J}_{\phi_{h_{ik}}}$, where $\tilde{J}_{\phi}$ is a rotation matrix [19]. $J(\theta) = \begin{bmatrix} \cos(\theta); \sin(\theta); \sin(\theta); \cos(\theta) \end{bmatrix}$.

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

With a layer-1 relay, the relay matrix $\tilde{R}$ is given as

$$\tilde{R} = \begin{bmatrix} |r|J(\phi_r) \end{bmatrix}$$

where $|r|$ and $\phi_r$ are the magnitude and phase angles of the complex relay amplification scalar. We perform the same information leakage neutralization as in (9). $\tilde{G}_2 R F_1 + H_{g1} = 0_n$, by setting $|r| = \frac{|g_{21}|}{|g_{22}|}$ and $\phi_r = \phi_{g2} - \phi_{f1} = \phi_{g2}$. With the above specified relay matrix $\tilde{R}$, denote the equivalent channel by $H_{ij} = H_{ij} + G_{i} R F_{j}$. We choose the beamforming matrix to be $P_1 = H_{ii}^{-1}$. The input-output relationship becomes

$$y_1 = x_1 + \tilde{H}_{12} \tilde{H}_{22}^{-1} x_2 + G_{1} R n_r + n_1$$

$$y_2 = x_2 + G_{2} R n_r + n_2$$

(18)

Denote the matrix product $\tilde{H} = \tilde{H}_{12} \tilde{H}_{22}$, $\tilde{n}_i = G_{i} R n_r + n_i$ and the corresponding $(i,j)$-th element $[\cdot]_{(i,j)}$. Let the transmit signals be

$$x_1 = \begin{bmatrix} u_{11}, u_{12} + a \frac{[\tilde{H}]_{(2,1)}}{[\tilde{H}]_{(1,1)}} v_1 + a \frac{[\tilde{H}]_{(2,2)}}{[\tilde{H}]_{(1,2)}} v_2 \end{bmatrix}^T$$

(19)

$$x_2 = \begin{bmatrix} a u_{21}, a u_{22} \end{bmatrix}^T$$

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

$$y_{i1} = u_{11} + a(u_{21} + u_{22}) + [\tilde{n}_i]_{(1)}$$

$$y_{i2} = u_{12} + a \frac{[\tilde{H}]_{(2,1)}}{[\tilde{H}]_{(1,1)}} (u_{21} + v_1)$$

$$+ a \frac{[\tilde{H}]_{(2,2)}}{[\tilde{H}]_{(1,2)}} (u_{22} + v_2) + [\tilde{n}_i]_{(2)}$$

(20)

As shown in Figure 5, all the desired signals $u_{ij}$ are secure. 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 $\tilde{R} \in \mathbb{R}^{2 \times 2}$. This allows the relay to scale and rotate the real and imaginary part of the input signal differently. We choose the relay matrix $\tilde{R}$ such that the imaginary dimension from transmitter one to receiver

1Due 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.
two and the real dimension from transmitter two to receiver one are neutralized,

\[
\begin{pmatrix}
\mathbf{H}_{21} & \mathbf{H}_{12}
\end{pmatrix}_{(2,:)} = 0_{1\times2},
\begin{pmatrix}
\mathbf{H}_{21} & \mathbf{H}_{12}
\end{pmatrix}_{(1,:)} = 0_{1\times2},
\] (21)

Equivalently, we have

\[
\begin{pmatrix}
\mathbf{H}_{21} & \mathbf{G}_2 \mathbf{R} \mathbf{F}_1 & \mathbf{H}_{12} & \mathbf{G}_1 \mathbf{R} \mathbf{F}_2
\end{pmatrix}_{(2,:)} = 0_{1\times2},
\begin{pmatrix}
\mathbf{H}_{21} & \mathbf{G}_2 \mathbf{R} \mathbf{F}_1 & \mathbf{H}_{12} & \mathbf{G}_1 \mathbf{R} \mathbf{F}_2
\end{pmatrix}_{(1,:)} = 0_{1\times2}.
\] (22)

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

\[
\text{vec}(\mathbf{R}) = - 
\begin{pmatrix}
\mathbf{F}_1^T \otimes \mathbf{G}_2 & \mathbf{F}_2^T \otimes \mathbf{G}_1
\end{pmatrix}_{(2,:)}^{-1}
\begin{pmatrix}
\text{vec}(\mathbf{H}_{21})_{(2,:)}
\text{vec}(\mathbf{H}_{12})_{(1,:)}
\end{pmatrix}.
\]

Denote the equivalent second channel from source 2 to destination 1 as \(q_2^T\), and the first channel from source 1 to destination 2 as \(q_2^T\). The input-output equation in (17) becomes

\[
y_1 = \mathbf{P}_1 x_1 + \begin{pmatrix} 0_{1\times2} & q_1^T \end{pmatrix} \mathbf{H}_{22}^{-1} \mathbf{P}_2 x_2 + \mathbf{G}_1 \mathbf{R} \mathbf{n}_r + n_1,
\]

\[
y_2 = \begin{pmatrix} q_1^T \end{pmatrix} \mathbf{H}_{11}^{-1} \mathbf{P}_1 x_1 + \mathbf{P}_2 x_2 + \mathbf{G}_2 \mathbf{R} \mathbf{n}_r + n_2.
\]

To simplify the notation, we denote \(q_2^T = q_2^T \mathbf{H}_{22}^{-1}\). We observe that at destination one, the desired signal \(x_1\) 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 \(y_1\) as \(y_{11}\) and \(y_{12}\). Now, we choose \(\mathbf{P}_1 = \mathbf{I}_2\) and

\[
x_1 = \begin{pmatrix}
\frac{b x_{11}}{q_{21}(1)} & \frac{b x_{12}}{q_{21}(2)}
\end{pmatrix}^T, x_2 = \begin{pmatrix}
\frac{a x_{21}}{q_{12}(1)} & \frac{a x_{22}}{q_{12}(2)}
\end{pmatrix}^T.
\]

The received signal at destination one is given by

\[
y_{11} = \frac{b x_{11}}{q_{21}(1)} + [n_1]_{(1)},
\]

\[
y_{12} = x_{12} + a(x_{21} + x_{22}) + [n_1]_{(2)}.
\] (23)

The received signal at destination two can be written similarly and is omitted here. As shown in Figure 6, transmitter \(i\) only transmits desired symbols \(u_{1i}, u_{2i}\). 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 \(D^{s} = 1\) 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


