The Gaussian Interference Channel in the Presence of Malicious Jammers

ITA 2018

Fatemeh Hosseinigoki, Oliver Kosut
Arizona State University

Introduction

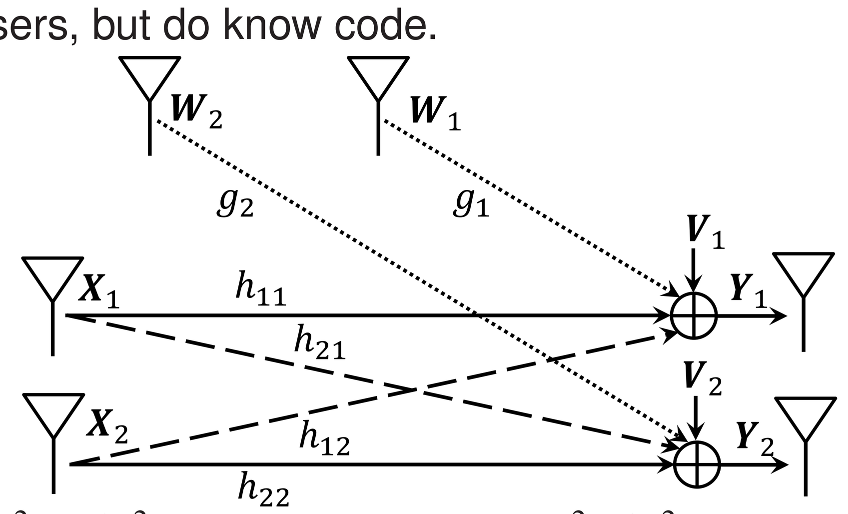
- The open nature of the wireless communication medium makes it inherently vulnerable to an active attack.
- How should a wireless communication system simultaneously handle: (i) interference, (ii) noise, and (iii) a malicious jammer.
- We characterize the capacity region of the two-user Gaussian interference channel (GIC) in the presence of intelligent jammers under input and state constraints.

Model for Gaussian Interference Channel with two Jammers

Received signals:

$$\mathbf{Y}_1 = h_{11}\mathbf{X}_1 + h_{12}\mathbf{X}_2 + g_1\mathbf{W}_1 + \mathbf{V}_1$$
$$\mathbf{Y}_2 = h_{21}\mathbf{X}_1 + h_{22}\mathbf{X}_2 + g_2\mathbf{W}_2 + \mathbf{V}_2$$

- $\mathbf{X}_1$ and $\mathbf{X}_2$ are n-length vectors representing the user's signal.
- $\mathbf{V}_i \sim \mathcal{N}(0,1)$ is AWGN independent of $\mathbf{X}_1$, $\mathbf{X}_2$, $\mathbf{W}_1$ and $\mathbf{W}_2$ (for $i=1,2$).
- $\mathbf{W}_1$ and $\mathbf{W}_2$ are the adversarial jammer signals.
- Jammers are independent of the users, but do know code.



Power Constraints

- $\|\mathbf{X}_2\|^2 \le nP_1$
- $\|\mathbf{W}_1\|^2 \le n\Lambda$
- $\|\mathbf{X}_2\|^2 \le nP_2$
- $\|\mathbf{W}_2\|^2 \le n\Lambda$

The power-to-noise ratios:

- $S_1 = h_{11}^2 P_1/\sigma^2$
- $I_1 = h_{12}^2 P_2/\sigma^2$
- $J_1 = g_1^2\Lambda/\sigma^2$
- $S_2 = h_{22}^2 P_2/\sigma^2$
- $I_2 = h_{21}^2 P_1/\sigma^2$
- $J_2 = g_2^2\Lambda/\sigma^2$

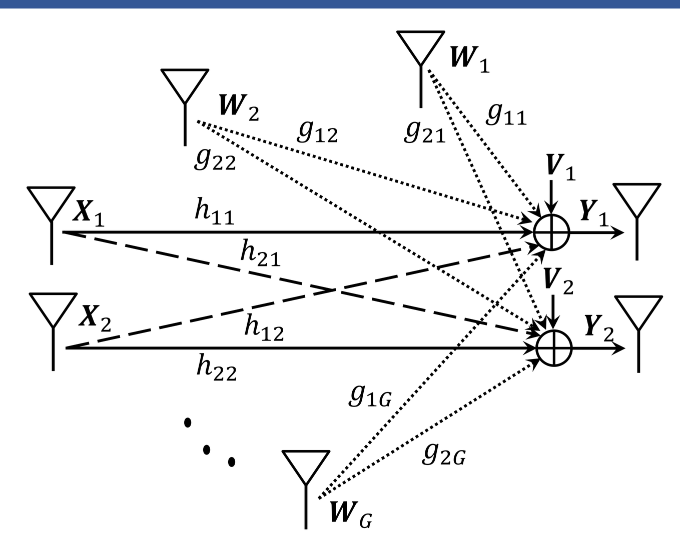
Assume: the transmitters and receivers know the SNR and INR, but they need not know the JNR.

Gaussian Interference Channel with Multiple Jammers

- Let C_G be the capacity region of a GIC with G jammers ($G \ge 1$).
- where $\|\mathbf{W}_i\|^2 \le n\Lambda$ for $i = 1,2,\ldots,G$.

Proposition 1. We have $C_G = C$ as long as

$$|g_{11}| + |g_{12}| + \ldots + |g_{1G}| = |g_1|$$
$$|g_{21}| + |g_{22}| + \ldots + |g_{2G}| = |g_2|$$



Outer and Inner Bounds for the GIC with No Jammer

For $(i,j) \in \{(1,2),(2,1)\}$:

The outer bound in [1]

$\mathscr{R}_o(S_1,S_2,I_1,I_2)$ is the set of (R_1,R_2) s.t.

$$R_i \le C(S_i)$$
$$R_i + R_j \le C\left(\frac{S_i}{1+I_j}\right) + C(I_j + S_j)$$
$$R_1 + R_2 \le C\left(\frac{S_1+I_1+I_1I_2}{1+I_2}\right) + C\left(\frac{S_2+I_2+I_1I_2}{1+I_1}\right)$$
$$2R_i + R_j \le C\left(\frac{S_i}{1+I_j}\right) + C(S_i+I_i) + C\left(\frac{S_j+I_j+I_iI_j}{1+I_i}\right)$$

The Han-Kobayashi inner bound [2]

$\mathscr{R}_i(S_1,S_2,I_1,I_2)$ is the set of (R_1,R_2) s.t.

$$R_i < C\left(\frac{S_i}{1+\alpha_j I_i}\right)$$
$$R_i + R_j < C\left(\frac{S_i+\bar{\alpha}_j I_i}{1+\alpha_j I_i}\right) + C\left(\frac{\alpha_j S_j}{1+\alpha_i I_j}\right)$$
$$R_1 + R_2 < C\left(\frac{\alpha_1 S_1 + \bar{\alpha}_2 I_1}{1+\alpha_2 I_1}\right) + C\left(\frac{\alpha_2 S_2 + \bar{\alpha}_1 I_2}{1+\alpha_1 I_2}\right)$$
$$2R_i + R_j < C\left(\frac{S_i+\bar{\alpha}_j I_i}{1+\alpha_j I_i}\right) + C\left(\frac{\alpha_i S_i}{1+\alpha_j I_i}\right) + C\left(\frac{\alpha_j S_j + \bar{\alpha}_i I_j}{1+\alpha_i I_j}\right)$$

- For some $\alpha_i \in [0,1]$, $\bar{\alpha}_i = 1-\alpha_i$ and $C(x) = \frac{1}{2}\log(1+x)$.
- In the Han-Kobayashi proof, encoder i divides the message m_i into private message m_{ip} and common message m_{ic} with power $\alpha_i P_i$ and $\bar{\alpha}_i P_i$ respectively.

Main Results

Define $S_i' = \frac{S_i}{1+J_i}$ and $I_i' = \frac{I_i}{1+J_i}$.

Theorem 1. [Outer Bound]

$$\begin{cases} C = 0, & \text{if } S_1 \le J_1 \text{ or } S_2 \le J_2 \\ C \subseteq \mathscr{R}_o(S_1', S_2', I_1', I_2'), & \text{otherwise} \end{cases}$$

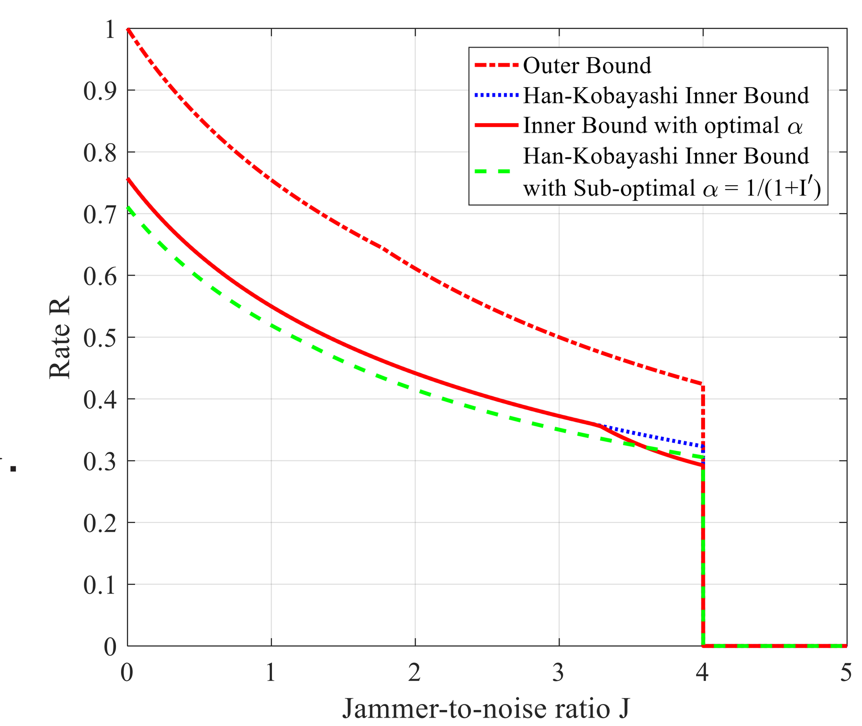
Theeorem 2. [Inner Bound]
Assume $S_i > J_i$ for $i = 1,2$. Let $\tilde{\mathscr{R}}_i(S_1',S_2',I_1',I_2')$ be the subset of rate pairs in $\mathscr{R}_i(S_1',S_2',I_1',I_2')$ achieved by $\alpha_i \in [0,1]$ satisfying

$$\alpha_i S_i + \bar{\alpha}_j I_i > J_i \text{ for } (i,j) = (1,2),(2,1).$$

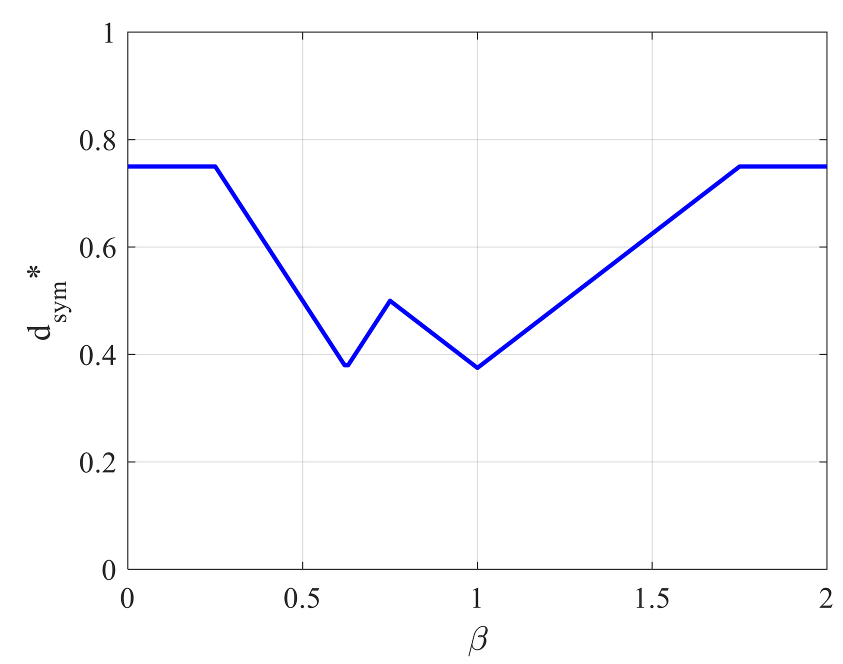
Then $\tilde{\mathscr{R}}_i(S_1',S_2',I_1',I_2') \subseteq C$.

Bounds on the Symmetric Capacity

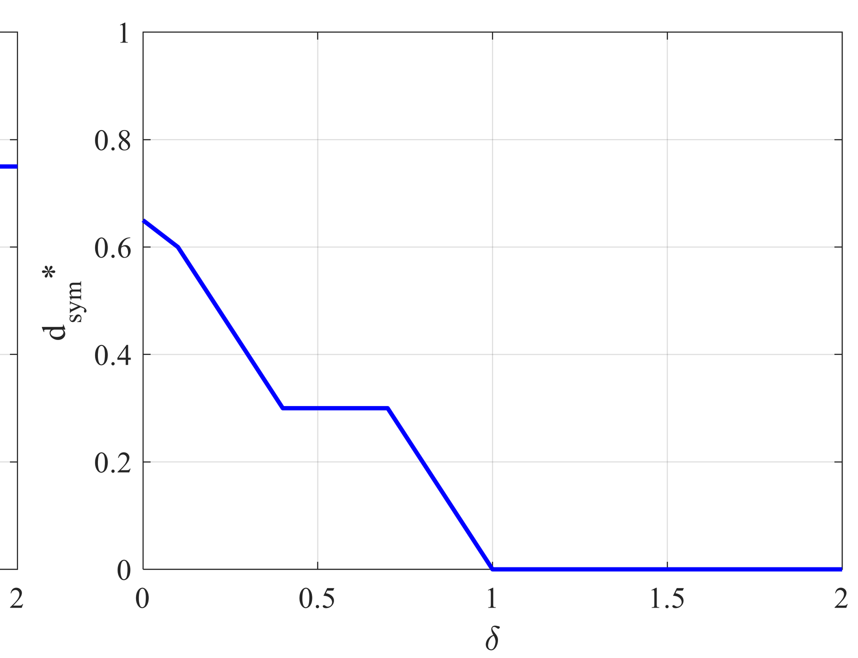
- $S_1 = S_2 = S = 4$, $I_1 = I_2 = I = 3$, $J_1 = J_2 = J \in [0,5]$, $R_1 = R_2 = R$.
- Optimal to choose $\alpha_1 = \alpha_2 = \alpha$ for inner bound.
- Define the symmetric capacity $C_{\text{sym}}(S,I,J) = \max\{R : (R,R) \in C\}$.
- $\mathscr{R}_i(S',S',I',I')$ is identical to our inner bound if $J < 3.2$.



Symmetric Degrees of Freedom (DoF)



$\delta = \frac{1}{4}$, $\beta \in [0,2]$



$\beta = 0.7$, $\delta \in [0,2]$

- The symmetric DoF

$$d^*_{\text{sym}}(\beta,\delta) = \lim_{S\to\infty} \frac{C_{\text{sym}}(S,I,J)}{C(S)}, \qquad \text{where } I = S^\beta \text{ and } J = S^\delta$$

- The symmetric DoF for GIC with Jammers

$$d^*_{\text{sym}}(\beta,\delta) = \min\left\{\max\{0,1-\delta\}, \max\{0,1-\beta,\beta-\delta\}, \max\left\{0, 1-\frac{\beta}{2}-\frac{\delta}{2}, \frac{\beta}{2}-\frac{\delta}{2}\right\}\right\}$$

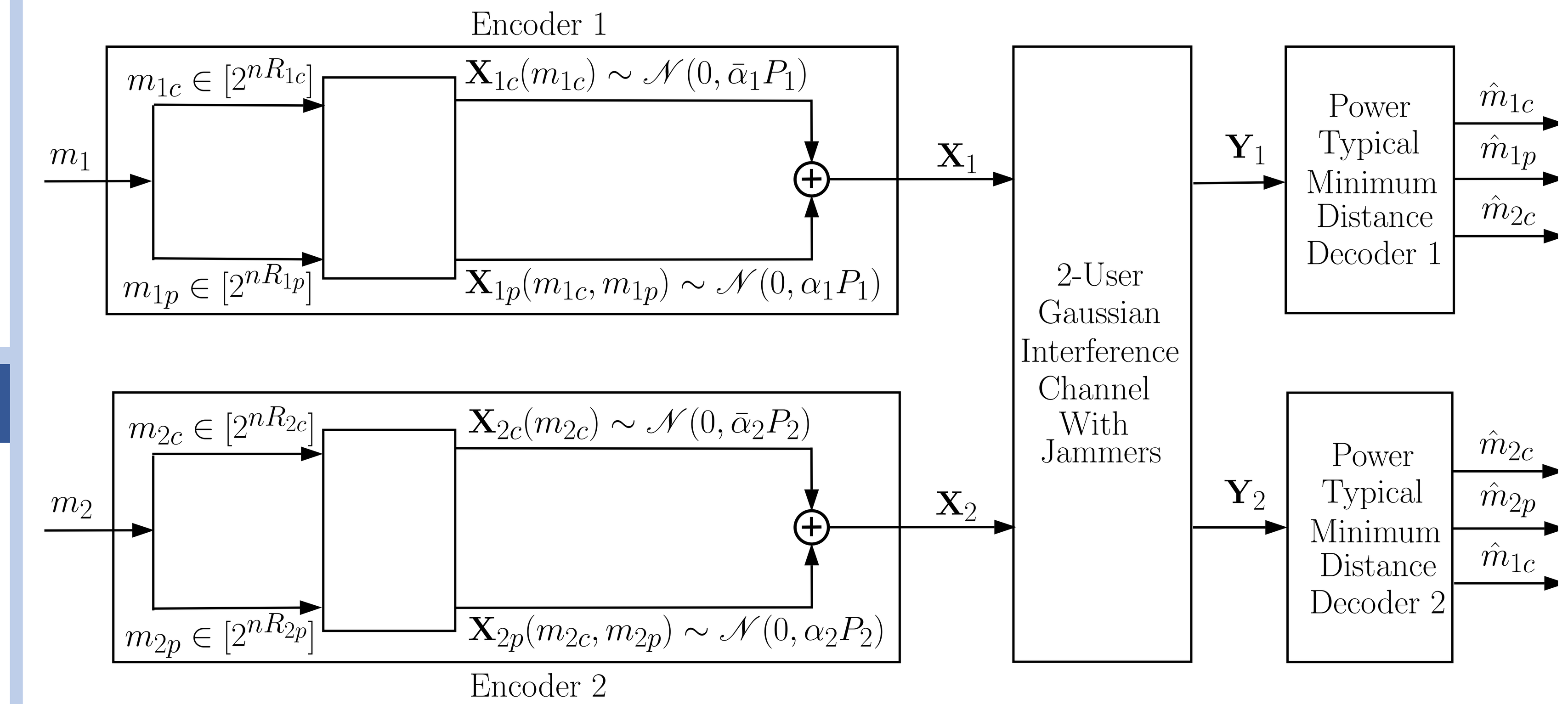
- **Note:** For a fixed $\delta = \log J/\log S$, the DoF exhibits the same "W" shape as it does with no jammer.

Proof of Outer Bound

- The jammers can transmit Gaussian noise with variance Λ, resulting in the noise power $\sigma^2 + g_i^2\Lambda$, and thus outer bound $\mathscr{R}_o(S_1',S_2',I_1',I_2')$.
- **Symmetrizing attack:** If $J_1 \ge S_1$, jammer 1 transmits $\mathbf{w}_1 = \mathbf{x}_1(\tilde{m}_1)h_{11}/g_1$.

Proof of Inner Bound

- Generalization of the Han-Kobayashi bound (rate splitting $R_i = R_{ic} + R_{ip}$).
- Fix $\alpha_1, \alpha_2 \in [0,1]$ and $\gamma > 0$:



Power Typical Minimum Distance Decoder:

- Define typical set $\mathcal{T}_\epsilon^{(n)}(X_1,\ldots,X_k)$ for Gaussian R.V. $X_1,\ldots,X_k$ as:

$$\mathcal{T}_\epsilon^{(n)}(X_1,\ldots,X_k) = \left\{(\mathbf{x}_1,\ldots,\mathbf{x}_k) : \mathbb{E}(X_iX_j) - \epsilon \le \frac{1}{n}\langle \mathbf{x}_i,\mathbf{x}_j\rangle \le \mathbb{E}(X_iX_j) + \epsilon \text{ for all } i,j \in [1:k]\right\}$$

- For receiver 1, let

$$\mathscr{S} = \left\{(m_{1c},m_{1p},m_{2c}) : (\mathbf{x}_{1c}(m_{1c}), \mathbf{x}_{1p}(m_{1c},m_{1p}), \mathbf{x}_{2c}(m_{2c}), \mathbf{y}_1) \in \bigcup \mathcal{T}_\epsilon^{(n)}(X_{1c},X_{1p},X_{2c},Y_1)\right\}$$

the union is over all joint Gaussian distributions $X_{1c}, X_{1p}, X_{2c}, Y_1$ s.t. $(X_{1c}, X_{1p}, X_{2c}, Y_1 - h_{11}X_{1c} - h_{11}X_{1p} - h_{12}X_{2c})$ are mutually independent.

- Given $\mathbf{y}_1$, decoder 1 finds

$$(\hat{m}_{1c},\hat{m}_{1p},\hat{m}_{2c}) = \underset{(m_{1c},m_{1p},m_{2c})\in\mathscr{S}}{\arg\min} \|\mathbf{y}_1 - h_{11}\mathbf{x}_{1c}(m_{1c}) - h_{11}\mathbf{x}_{1p}(m_{1c},m_{1p}) - h_{12}\mathbf{x}_{2c}(m_{2c})\|$$

Analysis of the probability of error: True messages $((M_{1c},M_{1p}),(M_{2c},M_{2p}))$. Let

$$\mathscr{U} = \{(m_{1c},m_{1p},m_{2c}) \in \mathscr{S} : \|\mathbf{Y}_1 - h_{11}\mathbf{x}_{1c}(m_{1c}) - h_{11}\mathbf{x}_{1p}(m_{1c},m_{1p}) - h_{12}\mathbf{x}_{2c}(m_{2c})\|^2 \le \|\mathbf{Y}_1 - h_{11}\mathbf{x}_{1c}(M_{1c}) - h_{11}\mathbf{x}_{1p}(M_{1c},M_{1p}) - h_{12}\mathbf{x}_{2c}(M_{2c})\|^2\}$$

- $\mathcal{E}_0 = \{(M_{1c},M_{1p},M_{2c}) \notin \mathscr{S}\} \to 0$ by LLN.
- $\mathcal{E}_1 = \{\exists \tilde{m}_{1p} \ne M_{1p} : (M_{1c},\tilde{m}_{1p},M_{2c}) \in \mathscr{U}\} \to 0$ by a generalized packing lemma using M_{1c} as common randomness if $R_{1p} < C\left(\frac{\alpha_1 S_1}{1+J_1+\alpha_2 I_1}\right)$
- $\mathcal{E}_2 = \{\exists \tilde{m}_{1c} \ne M_{1c}, \tilde{m}_{1p} : (\tilde{m}_{1c},\tilde{m}_{1p},M_{2c}) \in \mathscr{U}\} \to 0$ by generalized packing lemma if
$$\frac{J_1}{S_1} < 1, R_{1c} < C\left(\frac{\bar{\alpha}_1 S_1}{1+J_1+\alpha_2 I_1}\right), R_{1p} < C\left(\frac{\alpha_1 S_1}{1+J_1+\alpha_2 I_1}\right), R_{1c}+R_{1p} < C\left(\frac{S_1}{1+J_1+\alpha_2 I_1}\right)$$
- $\mathcal{E}_3 = \{\exists \tilde{m}_{1p} \ne M_{1p}, \tilde{m}_{2c} \ne M_{2c} : (M_{1c},\tilde{m}_{1p},\tilde{m}_{2c}) \in \mathscr{U}\} \to 0$ by generalized packing lemma if
$$\alpha_1 S_1 + \bar{\alpha}_2 I_1 > J_1, R_{2c} < C\left(\frac{\bar{\alpha}_2 I_1}{1+J_1+\alpha_2 I_1}\right), R_{1p} < C\left(\frac{\alpha_1 S_1}{1+J_1+\alpha_2 I_1}\right), R_{1p}+R_{2c} < C\left(\frac{(\alpha_1 S_1 + \bar{\alpha}_2 I_1)}{1+J_1+\alpha_2 I_1}\right)$$
- $\mathcal{E}_4 = \{\exists \tilde{m}_{1c} \ne M_{1c}, \tilde{m}_{1p}, \tilde{m}_{2c} \ne M_{2c} : (\tilde{m}_{1c},\tilde{m}_{1p},\tilde{m}_{2c}) \in \mathscr{U}\} \to 0$ by generalized packing lemma if all above and
$$S_1 + \bar{\alpha}_2 I_1 > J_1, R_{1c}+R_{2c} < C\left(\frac{(\bar{\alpha}_1 S_1 + \bar{\alpha}_2 I_1)}{1+J_1+\alpha_2 I_1}\right), R_{1c}+R_{1p}+R_{2c} < C\left(\frac{(S_1 + \bar{\alpha}_2 I_1)}{1+J_1+\alpha_2 I_1}\right)$$

References

[1] T. Han and K. Kobayashi, "A new achievable rate region for the interference channel," *Information Theory, IEEE Transactions on*, vol. 27, no. 1, pp. 49–60, Jan 1981.
[2] R. H. Etkin, D. N. C. Tse, and H. Wang, "Gaussian interference channel capacity to within one bit," *Information Theory, IEEE Transactions on*, vol. 54, no. 12, pp. 5534–5562, Dec 2008.

School of Electrical, Computer, and Energy Engineering — Arizona State University — Tempe, AZ
EMails: fhossei1@asu.edu, and okosut@asu.edu