The Role of Limited Transmitter Cooperation in Interference Channel with Secret Messages

Parthajit Mohapatra

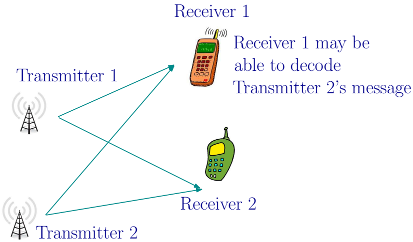
15^{th} Feb. 2014

Outline

- Motivation
- System model and problem statement
- Contributions
- Inner bounds
- Results and discussion

Motivation

- Interference in wireless network
  - Limits the communication rate
  - Allows users to eavesdrop other user's signal
- Is it possible
  - Support high throughput
  - Ensure secrecy
- Cooperation between users: both the gains simultaneously?



Effects of Cooperation on Achievable rate

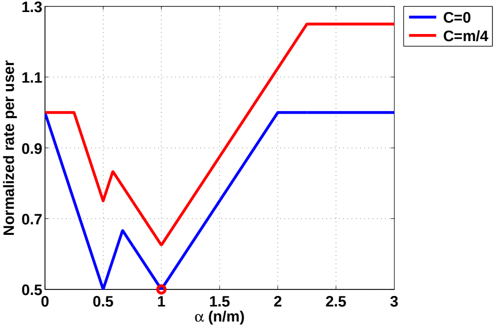


Figure: Capacity of symmetric linear deterministic IC[1]

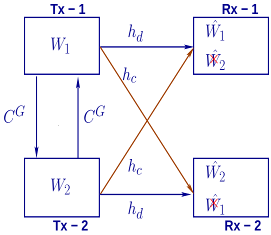
- α: coupling between the signal and interference
- Loss in rate: isolation between the Tx/Rx

[1] I. Wang and D. Tse, Interference mitigation through limited transmitter cooperation, TIT, May 2011

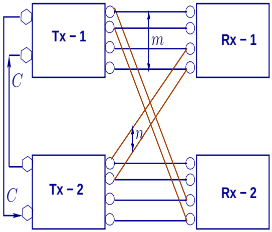
Problem statement

- Role of limited transmitter cooperation in a 2-user interference channel
  - Interference management
  - Secrecy
- From information theoretic view

System model



(a)



(b)

Figure: (a) Gaussian symmetric IC, and (b) Symmetric linear deterministic IC, with transmitter cooperation.

- $m \triangleq (\lfloor \log |h_d|^2 \rfloor)^+$ and $n \triangleq (\lfloor \log |h_c|^2 \rfloor)^+$
- $C \triangleq \lfloor C^G \rfloor$

Contributions

- Outer bounds: SLDIC
  - Partitioning the encoded message or output based on α
  - Side information to receivers
- Outer bounds: GSIC
  - Non trivial to extend the bounds developed for the deterministic case
  - Difficulty lies in partitioning of the encoded message/output
  - Finding the analogous quantity for the Gaussian case

- Achievable scheme: SLDIC
  - Interference cancelation
  - Relaying of other user's data bits
  - Time sharing
  - Random bits transmission
- When $\alpha \geq 2$: sharing of data bits, random bits or both depending on the value of C

- Achievable scheme: GSIC
  - Stochastic encoding
  - Marton's based coding scheme
  - Transmission of dummy information by one of the user
  - Time-sharing
- Weak/Moderate interference regime: Dummy information is treated as noise
- High/very high interference: Tries to decode the dummy information

Achievable scheme: Weak/Moderate intf. regime

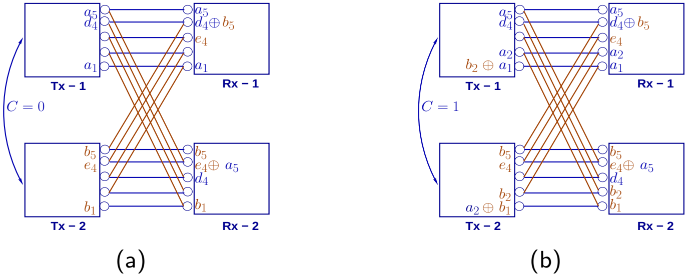


Figure: When (a) $C = 0$ and (b) $C = 1$.

- Not possible to extend the scheme directly to the Gaussian case

Achievable scheme contd.

- Split the message into two parts
  - Non-cooperative private (w_{pi}): Stochastic encoding
  - Cooperative private (w_{cpi}): Marton's based coding scheme
    - Interference caused by the non-intended cooperative private part is completely canceled at the non-intended receiver
  - Transmitter 2 sends dummy information

Encoding: Non-cooperative private message

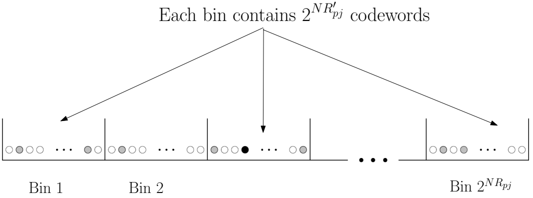
- Stochastic encoder: matrix of conditional probability

$$\sum_{x_{pj,i}} f_{pj}(x_{pj,i}|w_{pj}) = 1, \qquad \forall i = 1, 2, \ldots, N,$$

- Transmitter j ($j = 1, 2$) generates $2^{N(R_{pj}+R'_{pj})}$ i.i.d. sequences of length N at random according to

$$P(\mathbf{x}_{pj}^N) = \prod_{i=1}^{N} P(x_{pj,i})$$

- Grouping of codewords

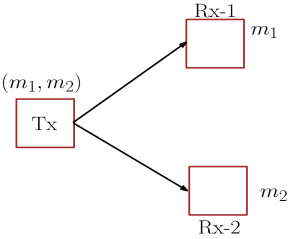


- For transmission of w_{pj}
  - w_{pj}: selects the bin
  - w'_{pj}: selects the codeword
- Dummy message
  - Transmitter 2 generates $2^{NR_{d2}}$ i.i.d. sequences of length N
  - Grouping of codewords: $2^{NR'_{d2}}$ bins and each bin containing $2^{NR''_{d2}}$ codewords
  - Codeword sent: $\mathbf{x}_{d2}^{N}(w'_{d2}, w''_{d2})$

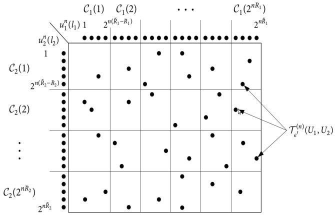
Marton's coding scheme

- For each message $m_j (j = 1, 2)$: generate sub-codebook $C_j(m_j)$ consisting of independently generated u_j^N sequences
- For each message pair: find (u_1^N, u_2^N) in the product sub-codebook $C_1(m_1) \times C_2(m_2)$
- Requirement to succeed (Mutual covering lemma)

$$(\widetilde{R_1} - R_1) + (\widetilde{R_2} - R_2) > I(U_1; U_2)$$



(a) BC Model



(b) Marton's coding scheme

Marton's coding scheme contd.

- Allows U_1 and U_2 to be arbitrarily correlated
- Achieves the following secrecy rate

$$\begin{aligned} R_1 &< I(U_1; Y_1) \\ R_2 &< I(U_2; Y_2) \\ R_1 + R_2 &< I(U_1; Y_1) + I(U_2; Y_2) - I(U_1; U_2) \end{aligned}$$

- In this work: we choose U_1 and U_2 to be independent

$$I(U_1; U_2) = 0$$

Encoding for cooperative private part of the message

- Generate the cooperative private vector codeword $\mathbf{x}_{cp}^N(w_{cp1}, w_{cp2})$ based on Marton's coding scheme according to

$$P(\mathbf{x}_{cp}^N, \mathbf{u}_1^N, \mathbf{u}_2^N) = \prod_{i=1}^{N} P(\mathbf{x}_{cp,i}, u_{1,i}, u_{2,i})$$

- $\mathbf{u}_1^N(\widetilde{w}_{cp1})$ and $\mathbf{u}_2^N(\widetilde{w}_{cp2})$: auxiliary codewords
- Transmit codewords:
  - $\mathbf{x}_1^N(w_{cp1}, w_{cp2}, w_{p1}, w'_{p1}) = \underline{\mathbf{x}}_{cp}^N[1] + \mathbf{x}_{p1}^N$
  - $\mathbf{x}_2^N(w_{cp1}, w_{cp2}, w_{p2}, w'_{p2}, w'_{d2}, w''_{d2}) = \underline{\mathbf{x}}_{cp}^N[2] + \mathbf{x}_{p1}^N + \mathbf{x}_{d2}^N$

- Decoding: receiver j looks for a unique message tuple such that

$$(\mathbf{y}_j^N, \mathbf{u}_j^N(\hat{\tilde{w}}_{cpj}), \mathbf{x}_{pj}^N(\hat{w}_{pj}, \hat{w}'_{pj})) \in T_\epsilon^{(N)}$$

- Choice of codebook parameters for ensuring secrecy
  - Non-cooperative private message at transmitter 1
    - $R'_{p1} = I(\mathbf{x}_{p1}; \mathbf{y}_2 | \mathbf{x}_{p2}, \mathbf{u}_2)$
    - $R'_{d2} = I(\mathbf{x}_{d2}; \mathbf{y}_2 | \mathbf{x}_{p1}, \mathbf{x}_{p2}, \mathbf{u}_2)$
  - Non-cooperative private message at transmitter 2
    - $R'_{p2} = I(\mathbf{x}_{p2}; \mathbf{y}_1 | \mathbf{x}_{p1}, \mathbf{u}_1)$
    - $R''_{d2} = I(\mathbf{x}_{d2}; \mathbf{y}_1 | \mathbf{x}_{p1}, \mathbf{x}_{p2}, \mathbf{u}_1)$

Choice of $\mathbf{u}_1$ and $\mathbf{u}_2$

- Chosen such that interference caused by the unintended cooperative private part is canceled
- Advantage
  - Eliminates interference
  - Ensures secrecy for the cooperative part

$$\underline{\mathbf{x}}_{cp} = \mathbf{w}_{1z}\underline{v}_{1z} + \mathbf{w}_{2z}\underline{v}_{2z},$$
$$\mathbf{u}_1 = [h_d \quad h_c]\,\underline{v}_{1z}\mathbf{w}_{1z}, \text{ and } \mathbf{u}_2 = [h_c \quad h_d]\,\underline{v}_{2z}\mathbf{w}_{2z}$$

where

- $\underline{v}_{1z} \triangleq [h_d \qquad -h_c]^T$
- $\underline{v}_{2z} \triangleq [-h_c \qquad h_d]^T$
- $\mathbf{w}_{1z}$ and $\mathbf{w}_{2z}$: independent Gaussian with variance σ_{1z}^2 and σ_{2z}^2, respectively

Output at receiver 1

$$\underline{\mathbf{x}}_{cp} = \mathbf{w}_{1z} \begin{bmatrix} h_d \\ -h_c \end{bmatrix} + \mathbf{w}_{2z} \begin{bmatrix} -h_c \\ h_d \end{bmatrix}$$

- Encoded message at transmitter 1

$$\begin{aligned} \mathbf{x}_1 &= \underline{\mathbf{x}}_{cp}[1] + x_{p1} \\ &= h_d \mathbf{w}_{1z} - h_c \mathbf{w}_{2z} + x_{p1} \end{aligned}$$

- Encoded message at transmitter 2

$$\begin{aligned} \mathbf{x}_2 &= \underline{\mathbf{x}}_{cp}[2] + x_{p2} + x_{d2} \\ &= h_d \mathbf{w}_{2z} - h_c \mathbf{w}_{1z} + x_{p2} + x_{d2} \end{aligned}$$

- Output at receiver 1

$$\begin{aligned} y_1 &= h_d x_1 + h_c x_2 + z_1 \\ &= \underbrace{(h_d^2 - h_c^2) w_{1z}}_{u_1} + h_d x_{p1} + h_c x_{p2} + h_c x_{d2} + z_1 \end{aligned}$$

Achievable Secrecy Rate: Weak/Moderate Intf. Regime

- Achievable scheme
  - Transmitter 1: sends non-cooperative private and cooperative private message
  - Transmitter 2: sends non-cooperative private and cooperative private message along with dummy message
  - Separate decoding: treats the dummy message as noise

Theorem

In the weak/moderate interference regime, the following rate is achievable for the GSIC with limited-rate transmitter cooperation and secrecy constraints at the receivers:

$$R_1 + R'_{p1} \leq I(\mathbf{u}_1, \mathbf{x}_{p1}; \mathbf{y}_1)$$
$$R_1 + R'_{p1} \leq I(\mathbf{x}_{p1}; \mathbf{y}_1 | \mathbf{u}_1) + \min\{C, I(\mathbf{u}_1; \mathbf{y}_1 | \mathbf{x}_{p1})\}$$

where $R'_{p1} = I(\mathbf{x}_{p1}; \mathbf{y}_2 | \mathbf{x}_{p2}, \mathbf{u}_2)$

Corollary

Using the proposed achievable scheme and time-sharing between transmitters, following symmetric secrecy rate is achievable:

$$R_s = \frac{1}{2}\left[R_i^*(1) + R_i^*(2)\right], \qquad \textit{where } i = 1, 2$$

$$R_1(1) \leq \begin{cases} 0.5\log\left(1 + \frac{\sigma_u^2 + h_d^2 P_{p1}}{1 + h_c^2 P_{d2} + h_c^2 P_{p2}}\right) - R'_{p1}, \\ 0.5\log\left(1 + \frac{h_d^2 P_{p1}}{1 + h_c^2 P_{d2} + h_c^2 P_{p2}}\right) \\ \qquad + \min\left\{C, 0.5\log\left(1 + \frac{\sigma_u^2}{1 + h_c^2 P_{d2} + h_c^2 P_{p2}}\right)\right\} - R'_{p1} \end{cases}$$

where $R'_{p1} = 0.5\log\left(1 + \frac{h_c^2 P_{p1}}{1 + h_d^2 P_{d2}}\right)$, $\sigma_u^2 \triangleq (h_d^2 - h_c^2)^2 \sigma_z^2$, $\sigma_z^2 \triangleq \frac{\theta_1}{\theta_1 + \theta_2} \frac{P_1}{h_d^2 + h_c^2}$, $P_{p1} \triangleq \frac{\theta_2}{\theta_1 + \theta_2} P_1$, $P_i \triangleq \beta P$ $(i = 1, 2)$ *and* $0 \leq (\theta_i, \beta) \leq 1$.

Achievable Secrecy Rate: High/Very High Intf. Regime

- Achievable scheme
  - Transmitter 1: sends non-cooperative private and cooperative private message
  - Transmitter 2: sends cooperative private and dummy message
  - Dummy message: transmitter chooses the codeword randomly
- Dummy message: not possible to ensure secrecy for the non-cooperative message
- Decoding:
  - Receiver 1: $(\mathbf{y}_1^N, \mathbf{u}_1^N(\hat{\hat{w}}_{cp1}), \mathbf{x}_{p1}^N(\hat{w}_{p1}, \hat{w}'_{p1}), \mathbf{x}_{d2}^N(\hat{w}_{d2})) \in T_\epsilon^N$
  - Receiver 2: $(\mathbf{y}_2^N, \mathbf{u}_2^N(\hat{\hat{w}}_{cp2})) \in T_\epsilon^N$

Theorem

In the high/very high interference regime, the following rate is achievable for the GSIC

$$\begin{aligned}
R_1 + R'_{p1} &\leq I(\mathbf{u}_1, \mathbf{x}_{p1}; \mathbf{y}_1 | \mathbf{x}_{d2}) \\
R_1 + R'_{p1} &\leq I(\mathbf{x}_{p1}; \mathbf{y}_1 | \mathbf{u}_1, \mathbf{x}_{d2}) + \min\{I(\mathbf{u}_1; \mathbf{y}_1 | \mathbf{x}_{p1}, \mathbf{x}_{d2}), C\} \\
R_1 + R'_{p1} + R_{d2} &\leq \min[I(\mathbf{u}_1, \mathbf{x}_{p1}, \mathbf{x}_{d2}; \mathbf{y}_1), I(\mathbf{x}_{p1}, \mathbf{x}_{d2}; \mathbf{y}_1 | \mathbf{u}_1) \\
&\qquad + \min\{I(\mathbf{u}_1; \mathbf{y}_1 | \mathbf{x}_{p1}, \mathbf{x}_{d2}), C\}] \\
R_1 + R'_{p1} + R_{d2} &\leq I(\mathbf{x}_{p1}; \mathbf{y}_1 | \mathbf{u}_1, \mathbf{x}_{d2}) + I(\mathbf{u}_1, \mathbf{x}_{d2}; \mathbf{y}_1 | \mathbf{x}_{p1}) \\
R_1 + R'_{p1} + 2R_{d2} &\leq I(\mathbf{x}_{p1}, \mathbf{x}_{d2}; \mathbf{y}_1 | \mathbf{u}_1) + I(\mathbf{u}_1, \mathbf{x}_{d2}; \mathbf{y}_1 | \mathbf{x}_{p1}) \\
R_2 &\leq \min\{I(\mathbf{u}_2; \mathbf{y}_2), C\} \\
R_{d2} &\leq I(\mathbf{x}_{d2}; \mathbf{y}_1 | \mathbf{u}_1, \mathbf{x}_{p1})
\end{aligned}$$

where $R_1 \triangleq R_{p1} + R_{cp1}$, $R_2 \triangleq R_{cp2}$ *and* R'_{p1} *and* R_{d2} *are set as* $I(\mathbf{x}_{p1}; \mathbf{y}_2 | \mathbf{u}_2)$ *and* $I(\mathbf{x}_{d2}; \mathbf{y}_2 | \mathbf{x}_{p1}, \mathbf{u}_2)$*, respectively.*

Outer bounds

- Outer bounds: using the intuition gained from deterministic model

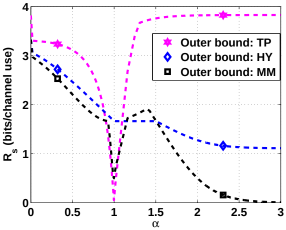


Figure: GSIC with $C = 0$, $P = 100$ and $h_d = 1$.

- In the legend
  - HY: X. He and A. Yener, *A new outer bound for the Gaussian interference channel with confidential messages,* CISS 2009
  - TP: X. Tang, R. Liu, P. Spasojevic, and H. Poor, *Interference assisted secret communication*, TIT 2011

Comparison among different schemes

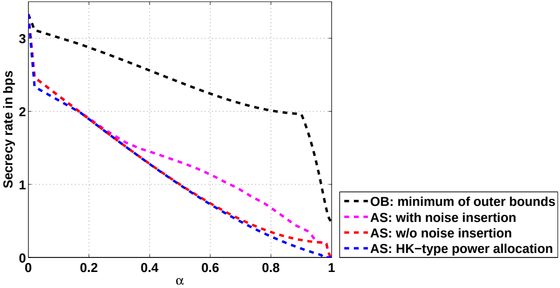
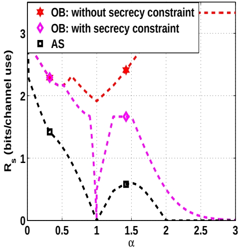
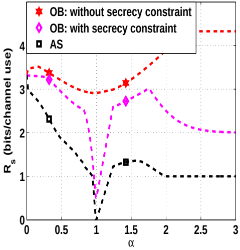


Figure: Achievable secrecy rate and outer bound: $P = 20$dB, C=0.2

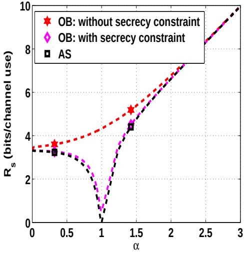
Rate against α



(a)



(b)



(c)

Figure: GSIC with $P = 100$, $h_d = 1$: (a) $C = 0$, (b) $C = 1$ and (c) $C = 10$.

Equivocation computation

- Need to show: $H(W_{p1}|\mathbf{y}_2^N) \geq N\left[R_{p1} - \epsilon_s\right]$

$$\begin{aligned} H(W_{p1}|\mathbf{y}_2^N) &\geq H(W_{p1}|\mathbf{y}_2^N, \mathbf{x}_{p2}^N, \mathbf{u}_2^N, W''_{d2}), \\ &\geq N\left[R_{p1} + R'_{p1} + R'_{d2}\right] - I(\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N; \mathbf{y}_2^N|\mathbf{u}_2^N, \mathbf{x}_{p2}^N) \\ &\qquad - H(\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N|\mathbf{y}_2^N, \mathbf{u}_2^N, \mathbf{x}_{p2}^N, W_{p1}, W''_{d2}) \end{aligned}$$

- It can be shown:
  $I(\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N; \mathbf{y}_2^N|\mathbf{u}_2^N, \mathbf{x}_{p2}^N) \leq NI(\mathbf{x}_{p1}, \mathbf{x}_{d2}; \mathbf{y}_2|\mathbf{u}_2, \mathbf{x}_{p2}) + N\epsilon'$

- $H(\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N | \mathbf{y}_2^N, \mathbf{u}_2^N, \mathbf{x}_{p2}^N, W_{p1}, W''_{d2}) \leq N\delta_1$ provided

$$R'_{P1} \leq I(\mathbf{x}_{p1}; \mathbf{y}_2 | \mathbf{x}_{d2}, \mathbf{u}_2, \mathbf{x}_{p2})$$
$$R'_{d2} \leq I(\mathbf{x}_{d2}; \mathbf{y}_2 | \mathbf{x}_{p1}, \mathbf{u}_2, \mathbf{x}_{p2})$$
$$R'_{p1} + R'_{d2} \leq I(\mathbf{x}_{p1}, \mathbf{x}_{d2}; \mathbf{y}_2 | \mathbf{u}_2, \mathbf{x}_{p2})$$

- Equivocation becomes

$$H(W_{p1} | \mathbf{y}_2^N) \geq N \left[R_{p1} + R'_{p1} + R'_{d2} - I(\mathbf{x}_{p1}, \mathbf{x}_{d2}; \mathbf{y}_2 | \mathbf{u}_2, \mathbf{x}_{p2}) - \epsilon_1 \right]$$

- Choose $R'_{p1} + R'_{d2} = I(\mathbf{x}_{p1}, \mathbf{x}_{d2}; \mathbf{y}_2 | \mathbf{u}_2, \mathbf{x}_{p2})$ for ensuring secrecy
- Hence, $R'_{p1} = I(\mathbf{x}_{p1}; \mathbf{y}_2 | \mathbf{x}_{p2}, \mathbf{u}_2)$ and $R'_{d2} = I(\mathbf{x}_{d2}; \mathbf{y}_2 | \mathbf{x}_{p1}, \mathbf{x}_{p2}, \mathbf{u}_2)$