Outer Bounds on the Secrecy Rate of the 2-User Symmetric Deterministic Interference Channel with Transmitter Cooperation

Parthajit Mohapatra

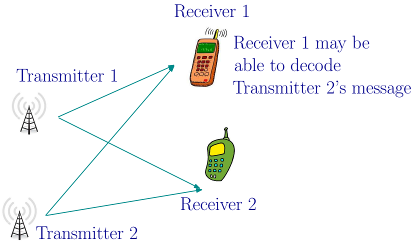
26th Oct. 2013

Outline

- Motivation
- Deterministic model
- System model and problem statement
- Outer bounds
- Summary

Motivation

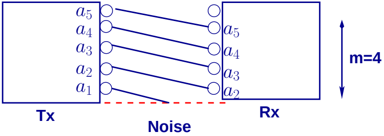
- Interference in wireless network
  - Limits the communication rate
  - Allows users to eavesdrop other user's signal
- Is it possible
  - Support high throughput
  - Ensure secrecy



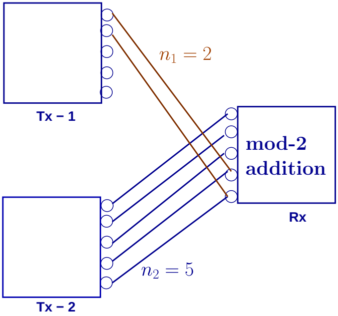
- Cooperation between users: both the gains simultaneously?

Deterministic model

- Good approximation of Gaussian wireless network at high SNR
- Gives insights into achievable schemes and outer bounds
- Noise: truncation



- Interference/superposition of signals: mod-2 addition



Point-to-point system

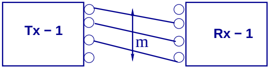
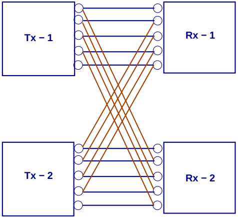


Figure: Point to point system

- Achievable rate: $R = m$



1. Ideal rate: $R = m$ (interference free rate)

Interference channel

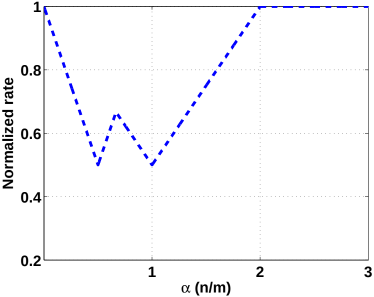


Figure: Capacity of symmetric linear deterministic IC

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

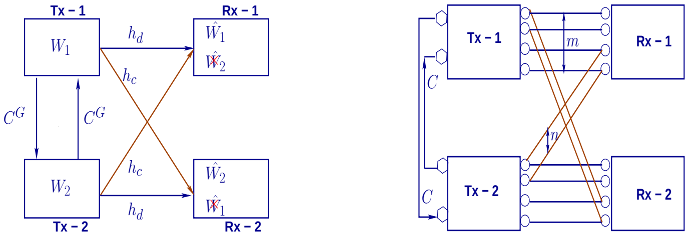
How to compensate for the loss

1. Feed back
2. Cooperation
3. Answer is positive in case of IC

Problem statement

- Possible to obtain such gain, when secrecy is an issue
- Role of limited transmitter cooperation in a 2-user symmetric linear deterministic interference channel (SLDIC)
  - Interference management
  - Secrecy
- From information theoretic view
- Focus: outer bounds

System model



(a) (b)

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

- $m \triangleq \left(\lfloor \log |h_d|^2 \rfloor\right)^+$ and $n \triangleq \left(\lfloor \log |h_c|^2 \rfloor\right)^+$
- $C \triangleq \lfloor C^G \rfloor$
- $\alpha \triangleq \frac{n}{m}$

- Encoding: $\mathbf{x}^i = f(W_i, W_i^r, v_{ij})$
- Decoding: solving the set of linear equation
- Cooperative links: lossless but of finite capacity
- Perfect secrecy

$$I(W_i; \mathbf{y}_j) = 0,\ \ (i \neq j) \quad \Leftrightarrow \quad H(W_i) = H(W_i/\mathbf{y}_j)$$

- Transmitters completely trust each other

Fano's inequality[1]

- Relates probability of error of a code to the uncertainty measure

Let $W \in \{1, 2, \ldots, 2^{tR}\}$ and $P_e = P(W \neq \hat{W})$, then we have

$$\begin{aligned} H(W|Y) &\leq H(P_e, 1 - P_e) + P_e \log(2^{tR} - 1), \\ &\leq 1 + P_e tR \end{aligned}$$

[1] 1952, Unpublished work

When $\alpha = 1$

- Output: $\mathbf{y}_1 = \mathbf{y}_2 = \mathbf{x}_1 \oplus \mathbf{x}_2$
  - $R = 0$

- Basis for outer bound
  - Reliable transmission requirement (Fano's inequality)

$$H(W_1|\mathbf{y}_1^t) \leq 1 + P_e^{(t)} t R_1 \leq t\epsilon_1$$

  - Secrecy constraint

$$I(W_1; \mathbf{y}_2^t) = 0$$

$$
\begin{aligned}
tR_1 &= H(W_1),\\
&= I(W_1;\mathbf{y}_1^t) + H(W_1|\mathbf{y}_1^t),\\
&\le I(W_1;\mathbf{y}_1^t) + t\epsilon_1,\\
&= I(W_1;\mathbf{y}_2^t) + t\epsilon_1, \qquad\qquad (\because \mathbf{y}_1 = \mathbf{y}_2),
\end{aligned}
$$

or $R_1 = 0$

- Irrespective of C, $R = 0$

When $\alpha \geq 2$ and $C = 0$

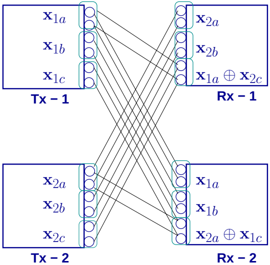


Figure: Splitting of the encoded message: $m = 3$ and $n = 6$

- Side information to receiver 1: $\mathbf{y}_{2a}^t = (\mathbf{x}_{1a}^t, \mathbf{x}_{1b}^t)$
- Helps to bound the rate by $I(W_1; \mathbf{y}_1^t | \mathbf{y}_{2a}^t)$

Proof outline

- Using Fano's inequality

$$
\begin{aligned}
tR_1 &\le I(W_1; \mathbf{y}_1^t) + t\epsilon_1, \\
&\le I(W_1; \mathbf{y}_1^t, \mathbf{y}_{2a}^t) + t\epsilon_1, \\
&= I(W_1; \mathbf{y}_{2a}^t) + I(W_1; \mathbf{y}_1^t | \mathbf{y}_{2a}^t) + t\epsilon_1.
\end{aligned}
$$

- From the secrecy constraint at receiver 2:

$$
\begin{aligned}
& I(W_1; \mathbf{y}_2^t) = 0, \\
\text{or } & I(W_1; \mathbf{y}_{2a}^t, \mathbf{y}_{2b}^t) = 0, \text{ where } \mathbf{y}_{2b}^t = \mathbf{x}_{2a}^t \oplus \mathbf{x}_{1c}^t, \\
\text{or } & I(W_1; \mathbf{y}_{2a}^t) + I(W_1; \mathbf{y}_{2b}^t | \mathbf{y}_{2a}^t) = 0 \\
\text{or } & I(W_1; \mathbf{y}_{2a}^t) = 0
\end{aligned}
$$

$$
\begin{aligned}
&tR_1 \\
&\leq I(W_1; \mathbf{y}_1^t | \mathbf{y}_{2a}^t) + t\epsilon_1, \\
&= H(\mathbf{y}_1^t | \mathbf{y}_{2a}^t) - H(\mathbf{y}_1^t | \mathbf{y}_{2a}^t, W_1) + t\epsilon_1, \\
&= H(\mathbf{x}_{2a}^t, \mathbf{x}_{2b}^t, \mathbf{x}_{1a}^t \oplus \mathbf{x}_{2c}^t | \mathbf{x}_{1a}^t, \mathbf{x}_{1b}^t) \\
&\qquad\qquad - H(\mathbf{x}_{2a}^t, \mathbf{x}_{2b}^t, \mathbf{x}_{1a}^t \oplus \mathbf{x}_{2c}^t | \mathbf{x}_{1a}^t, \mathbf{x}_{1b}^t, W_1) + t\epsilon_1, \\
&= H(\mathbf{x}_2^t | \mathbf{x}_{1a}^t, \mathbf{x}_{1b}^t) - H(\mathbf{x}_2^t | \mathbf{x}_{1a}^t, \mathbf{x}_{1b}^t, W_1) + t\epsilon_1,
\end{aligned}
$$

or $R_1 = 0$.

When $\alpha \geq 2$ and $C > 0$

- The encoded messages are no longer independent

$$I(\mathbf{x}_1^t; \mathbf{x}_2^t) \neq 0$$

Given the cooperating signals, the encoded messages and messages at two transmitters are independent[a], i.e.,

$$(W_1, \mathbf{x}_1^t) - (\mathbf{v}_{12}^t, \mathbf{v}_{21}^t) - (W_2, \mathbf{x}_2^t)$$

[a] F. Willems, The discrete memoryless multiple access channel with partially cooperating encoders, TIT, 1983

- $I(\mathbf{x}_1^t; \mathbf{x}_2^t | \mathbf{v}_{12}^t, \mathbf{v}_{21}^t) = 0$

Proof outline: with cooperation

$$
\begin{aligned}
& tR_1 \\
& = H(\mathbf{x}_2^t|\mathbf{x}_{1a}^t, \mathbf{x}_{1b}^t) - H(\mathbf{x}_2^t|\mathbf{x}_{1a}^t, \mathbf{x}_{1b}^t, W_1) + t\epsilon_1, \\
& \leq H(\mathbf{v}_{12}^t, \mathbf{v}_{21}^t, \mathbf{x}_2^t|\mathbf{x}_{1a}^t, \mathbf{x}_{1b}^t) - H(\mathbf{x}_2^t|\mathbf{v}_{12}^t, \mathbf{v}_{21}^t, \mathbf{x}_{1a}^t, \mathbf{x}_{1b}^t, W_1) \\
& \qquad\qquad + t\epsilon_1, \\
& \leq H(\mathbf{v}_{12}^t, \mathbf{v}_{21}^t) + H(\mathbf{x}_2^t|\mathbf{v}_{12}^t, \mathbf{v}_{21}^t, \mathbf{x}_{1a}^t, \mathbf{x}_{1b}^t) \\
& \qquad\qquad - H(\mathbf{x}_2^t|\mathbf{v}_{12}^t, \mathbf{v}_{21}^t, \mathbf{x}_{1a}^t, \mathbf{x}_{1b}^t, W_1) + t\epsilon_1,
\end{aligned}
$$

or $R_1 \leq 2C$

Theorem

In the moderate interference regime ($\frac{2}{3} < \alpha < 1$), the symmetric rate of the 2-user SLDIC with rate limited cooperation and secrecy constraints at the receivers is upper bounded as:

$$R \leq \frac{1}{3}\left[2C + 3m - 2n\right]$$

1. $\mathbf{y}_2^t$ is provided as side information to receiver 1
2. Encoded message is split into two parts
    1. Causes interference to the unintended receiver
    2. Does not cause interference to the unintended receiver

Theorem

When $(\alpha > 1)$*, the symmetric rate of the 2-user SLDIC with limited rate cooperation and secrecy constraints at the receivers is upper bounded as*

$$R \leq \frac{1}{3}\left[2C + n\right]$$

1. Proof is similar to that for the moderate interference regime

Theorem

In the high interference regime ($1 < \alpha < 2$), *the symmetric rate of the 2-user SLDIC with secrecy constraints at the receivers is upper bounded as*

$$R \leq 2C + 2m - n$$

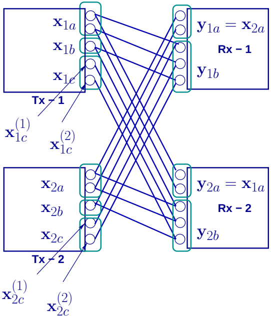


Figure: Splitting of message: $m = 3$ and $n = 5$

Moderate interference regime ($\frac{2}{3} < \alpha < 1$)

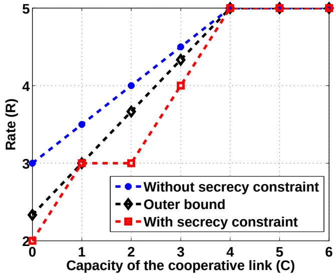


Figure: SLDIC with $m = 5$ and $n = 4$

Very high interference regime ($\alpha \geq 2$)

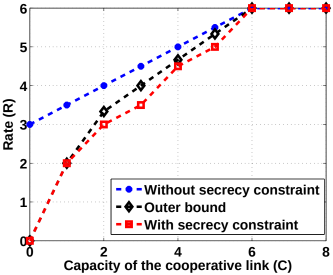


Figure: SLDIC with $m = 3$ and $n = 6$

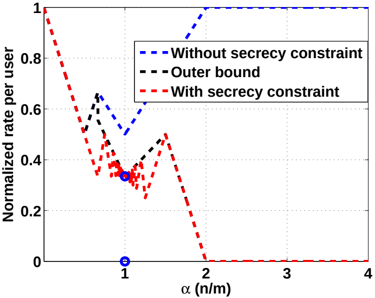


Figure: Normalized rate: $C = 0$

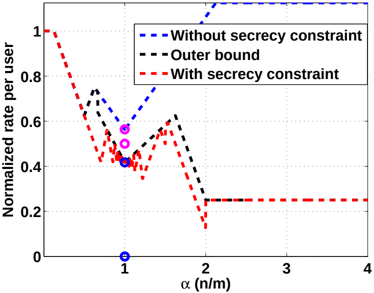


Figure: Normalized rate: $C = 50$

Summary

- When $C < n$: loss in the achievable rate due to the secrecy constraint at the receivers
- When $C = 0$: gives outer bound on the secrecy rate for the SLDIC without cooperation
- When $\alpha \geq 2$: sharing random bits through the cooperative link can achieve the optimal secrecy rate, when m is even (odd) and $0 < C \leq \frac{m}{2}$ $(0 < C \leq \frac{m+1}{2})$
- When $\alpha \geq 2$: not possible to achieve nonzero secrecy rate
- When $C = 0$ and $\frac{1}{2} < \alpha < \frac{2}{3}$: need to derive a tighter outer bound