Secrecy in the 2-User Symmetric Interference Channel with Transmitter Cooperation: Deterministic View

P. Mohapatra

9^{th} March 2013

Outline

- Motivation
- Problem statement
- Achievable scheme
    1. Weak interference regime
    2. Moderate interference regime
    3. Very high interference regime (for a specific case)
- Summary
- Outer bound (if time permits)

Motivation

- Interference in wireless network
  - Limits the communication rate
  - Allows users to eavesdrop other user's signal
- Secrecy: important concern in wireless network
  - Cellular network
  - Support high throughput and secure its transmissions
- Is it possible to get both the benefits?
- Answer these questions using information theoretic approach

Problem statement

- Users are not completely isolated (e.g.: base stations)
- Users can cooperate
- Effectiveness of limited transmitter cooperation in a 2-user symmetric linear deterministic interference channel
    - Interference management
    - Secrecy

Why deterministic model

- Good approximation of Gaussian model at high SNR
- Give insights into achievable schemes and outer bounds
- Not feasible in deterministic model: may not be feasible in Gaussian case

Deterministic model

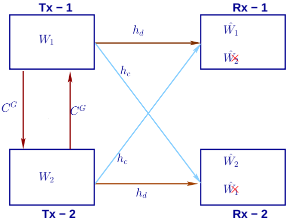


Figure: Symmetric GIC

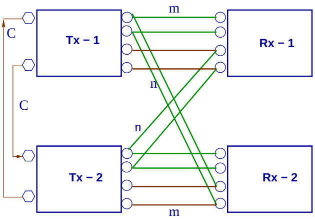


Figure: SLDIC

- $m \triangleq (\lfloor \log |h_d|^2 \rfloor)^+$, $n \triangleq (\lfloor \log |h_c|^2 \rfloor)^+$ and $C \triangleq \lfloor C^G \rfloor$
- $\alpha \triangleq \frac{n}{m}$
- a_i and b_i: data bits of transmitter 1 and 2
- d_i and e_i: random bits of transmitter 1 and 2
- Data bits and random bits: Bern $\left(\frac{1}{2}\right)$

System model

- Input-output equation

$$\mathbf{y}_1 = \mathbf{D}^{q-m}\mathbf{x}_1 \oplus \mathbf{D}^{q-n}\mathbf{x}_2; \;\; \mathbf{y}_2 = \mathbf{D}^{q-m}\mathbf{x}_2 \oplus \mathbf{D}^{q-n}\mathbf{x}_1$$

  - $\mathbf{x}_i$ and $\mathbf{y}_i$: binary vectors of length $q \triangleq \max\{m, n\}$
  - $\mathbf{D}$: $q \times q$ downshift matrix with elements

$$d_{j,k} = \begin{cases} 1 & \text{if } 2 \leq j = k+1 \leq q \\ 0 & \text{otherwise} \end{cases}$$

- Encoding: $\mathbf{x}_i = f(W_i, W_i^r, v_{ij})$
- Decoding: solving the set of linear equation
- Receiver does not require the knowledge of the random bits

System model

- Cooperative links: lossless but of finite capacity
- Perfect secrecy
  - $I(W_i; \mathbf{y}_j) = 0, \;\; (i \neq j) \Leftrightarrow H(W_i) = H(W_i / \mathbf{y}_j)$
- Transmitters completely trust each other

Weak interference regime ($0 \leq \alpha \leq \frac{2}{3}$)

- Achievable scheme
  - Interference cancelation
  - Uncoded bit transmission

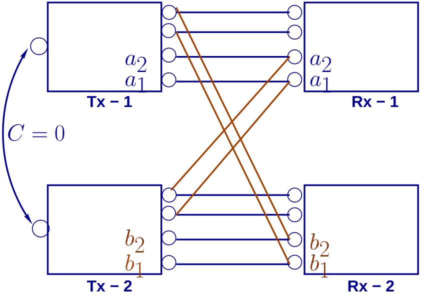


Figure: SLDIC with $m = 4$, $n = 2$ and $C = 0$: $R_S = 2$

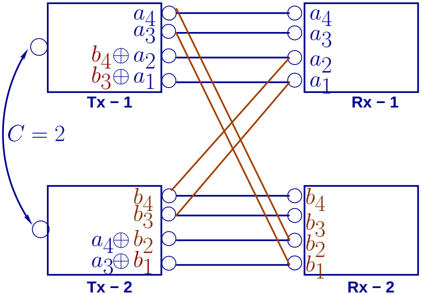


Figure: SLDIC with $m = 4$, $n = 2$ and $C = 4$: $R_S = 4$

Encoding scheme

- Encoding for message of transmitter 1

$$\mathbf{x}_1 = \begin{bmatrix} \mathbf{0}_{(m-(r+C))^+\times 1} \\ \mathbf{a}_{(r+C)\times 1} \end{bmatrix} \oplus \begin{bmatrix} \mathbf{0}_{(m-C)\times 1} \\ \mathbf{b}^c_{C\times 1} \end{bmatrix}$$

where $\mathbf{a} \triangleq [a_{r+C}, a_{r+C-1}, \ldots, a_1]^T$,
$\mathbf{b}^c \triangleq [b_{r+C}, b_{r+C-1}, \ldots, b_{r+1}]^T$ and $r \triangleq m - n$

- Achievable rate

$$R_S = \underbrace{m-n}_{\text{uncoded transmission}} + \underbrace{\min\{n, C\}}_{\text{interference cancelation}}$$

Result

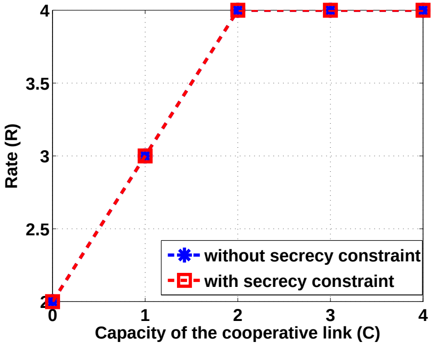


Figure: Achievable rate of the SLDIC with $m = 4$ and $n = 2$

- When $0 \leq \alpha \leq \frac{1}{2}$, one obtains secrecy for free

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

- Achievable scheme
  - Interference cancelation
  - Random bit transmission

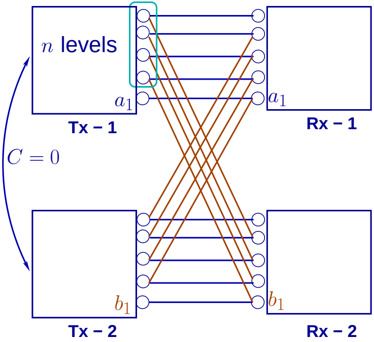


Figure: SLDIC with $m = 5$, $n = 4$ and $C = 0$

- Possible to transmit at least $m - n$ bits securely

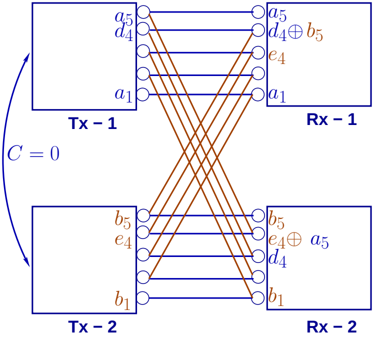


Figure: SLDIC with $m = 5$, $n = 4$ and $C = 0$: $R_S = 2$

- Possible to transmit in the upper levels: random bits transmission

With cooperation

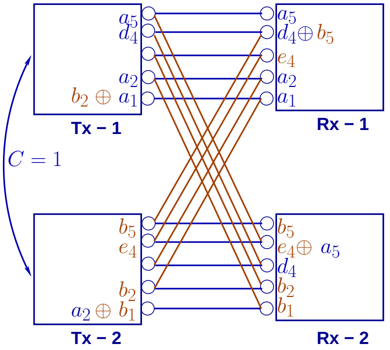
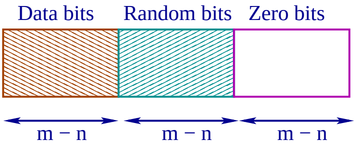


Figure: SLDIC with $m = 5$, $n = 4$ and $C = 1$: $R_S = 3$

- Uses combination of interference cancelation and random bit transmission
- Need to determine the number of data bits that can be transmitted with the help of random bit transmission

Encoding scheme

- Data transmission with the help of random bits transmission



- $B \triangleq \left\lfloor \frac{g}{3(m-n)} \right\rfloor$ and $t \triangleq g\%\{3(m-n)\}$, where $g \triangleq \{n-(r_2+C)\}^+$

- $q \triangleq \min\{(t-r_2)^+, r_2\}$: number of data bits that can be securely sent on the remaining t levels

Encoding scheme

- Encoding of transmitter 1 message when $q = 0$

$$\mathbf{x}_1 = \begin{bmatrix} \mathbf{0}_{(m-(r_2+C))^+\times 1} \\ \mathbf{a}_{(r_2+C)\times 1} \end{bmatrix} \oplus \begin{bmatrix} \mathbf{0}_{(m-C)\times 1} \\ \mathbf{b}^c_{C\times 1} \end{bmatrix} \oplus \begin{bmatrix} \mathbf{a}^u_{p\times 1} \\ \mathbf{0}_{p'\times 1} \end{bmatrix}$$

$$\begin{aligned} \mathbf{a}^u &\triangleq [\mathbf{u}_1, \mathbf{d}_2, \mathbf{z}_3, \dots, \mathbf{u}_{3B-2}, \mathbf{d}_{3B-1}, \mathbf{z}_{3B},]^T, \\ \mathbf{u}_l &\triangleq \left[a_{m-(l-1)r_2}, a_{m-(l-1)r_2-1}, \dots, a_{m-lr_2+1}\right], \\ \mathbf{d}_l &\triangleq \left[d_{m-(l-1)r_2}, d_{m-(l-1)r_2-1}, \dots, d_{m-lr_2+1}\right], \end{aligned}$$

$\mathbf{z}_l$ is a zero vector of size $1 \times r_2$, $p \triangleq 3B(m-n)$

- Achievable rate

$$R_S = m - n + \underbrace{B(m-n) + q}_{\text{random bits transmission}} + \min\{n, C\}$$

Result

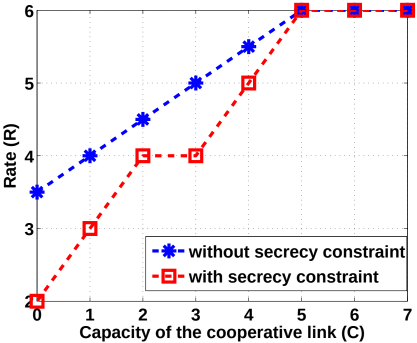


Figure: Achievable rate of the SLDIC with $m = 6$ and $n = 5$

- Gap may be due to the secrecy constraint

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

- Scheme for $\alpha = 2$ and even valued m
- Achievable scheme
  - Relaying of the other user's data bits
  - Time sharing
  - Techniques used in the moderate interference regime
- Involves sharing of random bits/data bits or both

Achievable scheme

- When $C = 0$
  - Not possible to achieve perfect secrecy
  - We will look at the outer bound (if time permits)
- When $0 < C \leq \frac{m}{2}$
  - Only random bit sharing
- When $\frac{m}{2} < C < \frac{3m}{2}$
  - Data bits and random bits sharing
- When $\frac{3m}{2} \leq C \leq n$
  - Data bits sharing

When $0 < C \leq \frac{m}{2}$: $m = 2$, $n = 4$ and $C = 1$

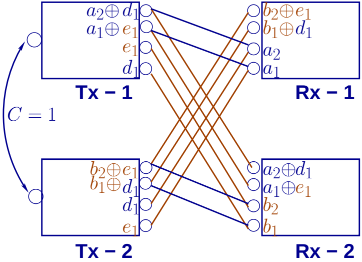


Figure: With random bits sharing

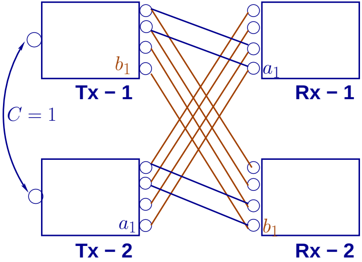
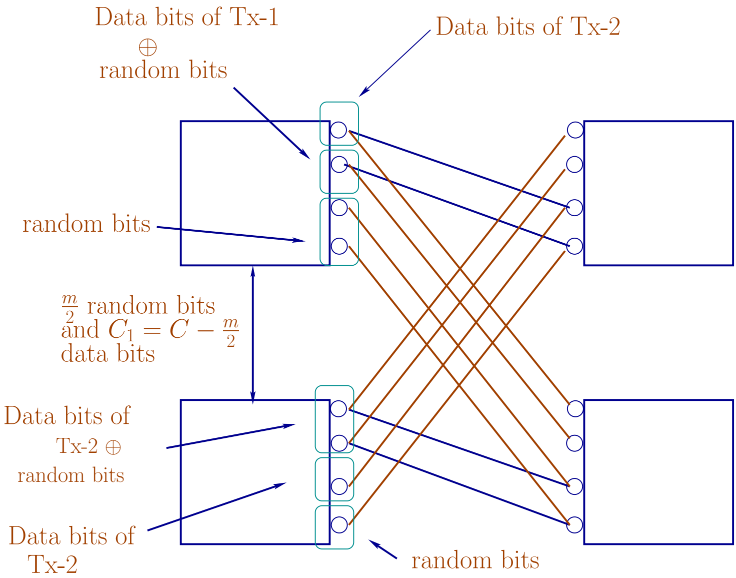


Figure: With data bits sharing

When $\frac{m}{2} < C < \frac{3m}{2}$: $m = 2$, $n = 4$ and $C = 2$



$m = 2$, $n = 4$ and $C = 2$

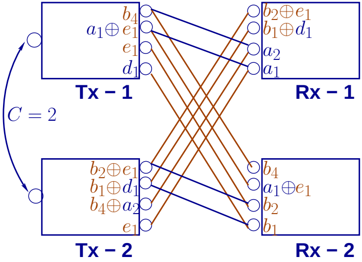


Figure: First time slot

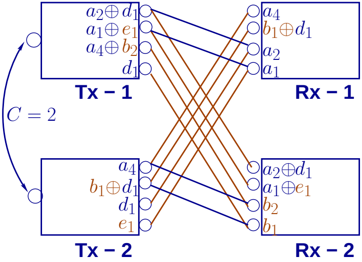


Figure: Second time slot

- Achieves: $R_S = 2.5$

Result

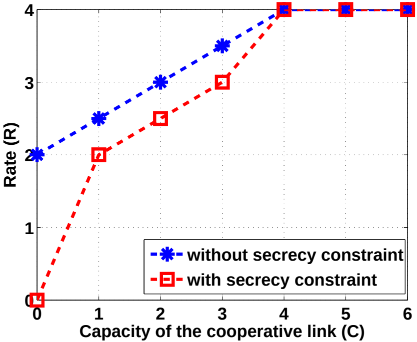


Figure: Achievable rate of the SLDIC with $m = 2$ and $n = 4$

- Possible to achieve non-zero secrecy rate with cooperation

Summary

- When $0 \leq \alpha \leq \frac{1}{2}$: secrecy comes for free
- When $C = n$ and $\alpha \neq 1$: the proposed scheme achieves the maximum possible rate of $\max\{m, n\}$
- In all the interference regimes, the proposed scheme always achieves nonzero secrecy rate with cooperation, except for the $\alpha = 1$ case
- Very high interference regime $\alpha \geq 2$: sharing random bits, data bits or both found to be useful

Outer bound ($\alpha = 1$)

- Based on: Fano's inequality and secrecy constraints

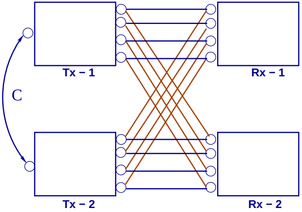
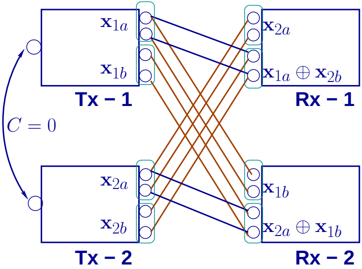


Figure: SLDIC with $m = n = 4$

- $\mathbf{y}_1 = \mathbf{y}_2 = \mathbf{x}_1 \oplus \mathbf{x}_2$
- Bound on R_1

$$
\begin{aligned}
nR_1 &\leq I(W_1; \mathbf{y}_1^n) + n\epsilon_n \\
&= I(W_1; \mathbf{y}_2^n) + n\epsilon_n \\
\text{or } R_1 &= 0
\end{aligned}
$$

$\alpha = 2$



$$\mathbf{y}_{1a} = \mathbf{x}_{2a} \qquad \mathbf{y}_{1b} = \mathbf{x}_{1a} \oplus \mathbf{x}_{2b}$$

$$\mathbf{y}_{2a} = \mathbf{x}_{1a} \qquad \mathbf{y}_{2b} = \mathbf{x}_{2a} \oplus \mathbf{x}_{1b}$$

Outline of the proof

$$\begin{aligned}
nR_1 &\leq I(W_1, \mathbf{y}_1^n) + n\epsilon \\
&= I(W_1, \mathbf{y}_1^n) - I(W_1, \mathbf{y}_2^n) + n\epsilon \\
&= I(W_1, \mathbf{y}_1^n, \mathbf{x}_2^n) - I(W_1, \mathbf{y}_2^n) + n\epsilon \\
&= I(W_1, \mathbf{y}_{1a}^n, \mathbf{y}_{1b}^n | \mathbf{x}_2^n) - I(W_1, \mathbf{y}_{2a}^n, \mathbf{y}_{2b}^n) + n\epsilon \\
&= H(\mathbf{x}_{1a}^n) - H(\mathbf{x}_{1a}^n | W_1) - I(W_1; \mathbf{y}_{2a}^n) - I(W_1; \mathbf{y}_{2b}^n | \mathbf{y}_{2a}^n) + n\epsilon \\
&\leq I(W_1; \mathbf{x}_{1a}^n) - I(W_1; \mathbf{x}_{1a}^n) + n\epsilon \\
\text{or } R_1 &= 0
\end{aligned}$$