Secrecy in Interference Channel with Source Cooperation: A Deterministic View

P. Mohapatra

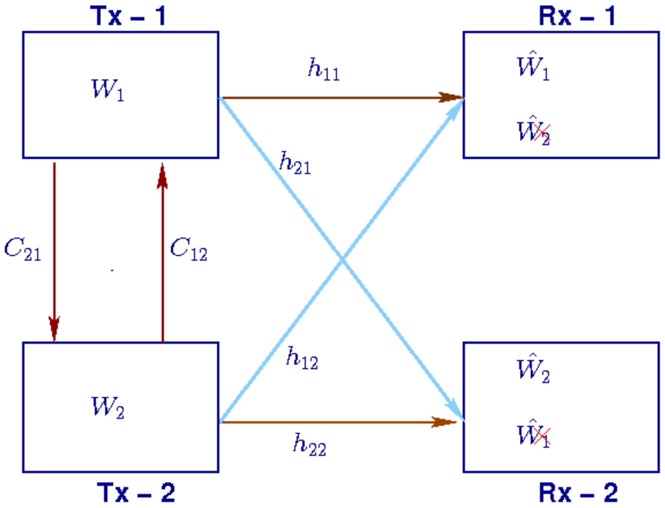
Dept. of ECE, Indian Institute of Science
Bangalore

13th October 2012

Motivation

- Open nature of wireless medium: users can eavesdrop other user message
- Different users have subscribed to different contents
- e.g.: cellular network
- Users can cooperate
- How cooperation and interference affect the secrecy capacity?

Interference channel with source cooperation



Problem statement

- To investigate the effects of user cooperation on secrecy of interference channel (IC)
- In general, solving such problem is hard!
- e.g.: Capacity of 2-user Gaussian IC (GIC) still remains an elusive problem
- Analogous model: deterministic model
- Translate the ideas from deterministic model to Gaussian model
- More optimistic to go for approximate capacity (secure DOF/GDOF) characterization

System model

- Symmetric GIC
- Cooperative links: lossless but of finite capacity
- Global CSI at every nodes
- Transmitters completely trust each other

Notion of secrecy

- Perfect secrecy

$$I(W_i; Y_j) = 0, \;\; i \neq j$$

- Strong secrecy

$$\lim_{n \to \infty} I(W_i; Y_j^n) = 0, \;\; i \neq j$$

- Weak secrecy

$$\lim_{n \to \infty} \frac{1}{n} I(W_i; Y_j^n) = 0, \;\; i \neq j$$

- Symmetric secrecy capacity: largest secrecy rate that can be achieved by any coding scheme

Recap on deterministic model

- Introduced by Avestimehr, Diggavi and David Tse for relay network[1]
- We will consider it for
  1. Point-to-Point AWGN channel
  2. Two-user Interference channel

[1] Wireless Network Information Flow: A Deterministic Approach, Trans. IT, April, 2011

Modeling of Point-to-Point Link

Real scalar Gaussian model:

$$y = hx + z, \;\; z \sim N(0,1)$$

Assumptions:

- Avg. power constraint at the Transmitter: $E[|x|^2] \leq 1$
- The transmit power and noise power are normalized to 1

Channel gain is related to SNR as: $|h| = \sqrt{\text{SNR}}$

The capacity of this channel is:

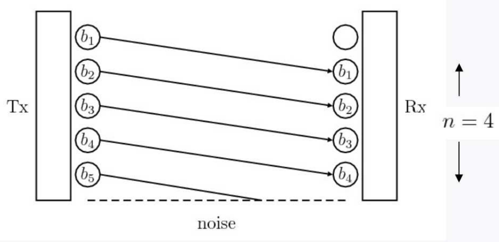
$$C_{\text{AWGN}} = \frac{1}{2}\log(1 + SNR).$$

- Assume h, x and z: positive real numbers
- x has peak power constraint of 1

The received signal in binary form is

$$\begin{aligned} y &= hx + z = \sqrt{SNR}x + z \\ &= 2^{\frac{1}{2}\log SNR} \sum_{i=1}^{\infty} x(i) 2^{-i} + \sum_{i=-\infty}^{\infty} z(i) 2^{-i} \\ &= 2^{\frac{1}{2}\log SNR} \sum_{i=1}^{\infty} x(i) 2^{-i} + \sum_{i=1}^{\infty} z(i) 2^{-i} \\ &\approx \underbrace{2^n \sum_{i=1}^{n} x(i) 2^{-i}}_{\text{n-most significant bits}} + \underbrace{\sum_{i=1}^{\infty} [x(i+n) + z(i)]\, 2^{-i}}_{\text{Mixed with noise}}, \end{aligned}$$

$$\text{where } n = \left\lceil \frac{1}{2} \log \text{SNR} \right\rceil^{+}$$



- Transmitting signal: a sequence of bits at different signal levels
- Highest signal level = MSB and Lowest signal level = LSB
- Noise: modeled by truncation

IC: Deterministic model

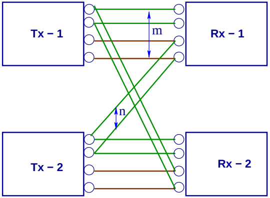
- System model

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

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

where $\mathbf{x}_i$: binary input vector of length $q = \max(m, n)$

$$D = \begin{bmatrix} 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \\ & \vdots & \vdots & \vdots & \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix}$$



IC with source cooperation: Deterministic model

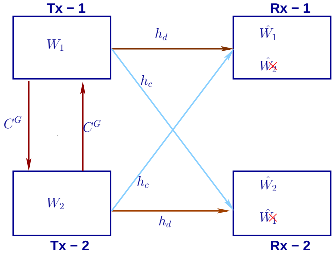


Figure: Symmetric GIC with source cooperation

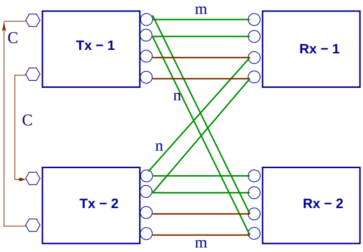


Figure: Deterministic Equivalence

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

Class of channel: weak/moderate interference case $(m > n)$

- Type of links
  - Type V
  - Type VI
  - Type VII
  - Type VIII
- Class of channel
  - Class A: Type V, VI and VII
  - Class B: Type V and VII
  - Class C: Type V, VII and VIII

Class B

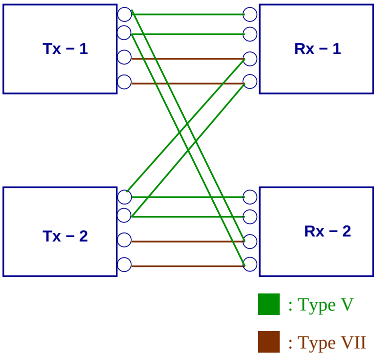


Figure: Deterministic IC: $m = 4$, and $n = 2$

- For class B: $m = 2n$
- Number of Type V links: $T_5 = n$
- Number of Type VII links: $T_7 = n$

Achievable scheme for Class B

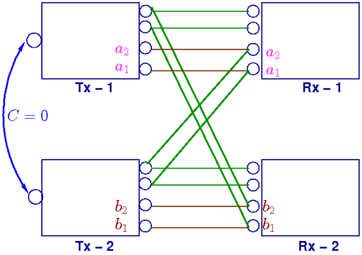


Figure: Deterministic IC: $m = 4, n = 2$ and $C = 0$

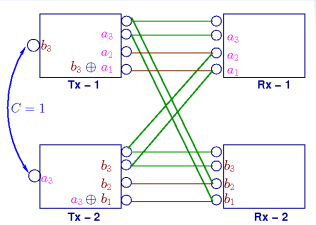


Figure: Deterministic IC: $m = 4, n = 2$ and $C = 1$

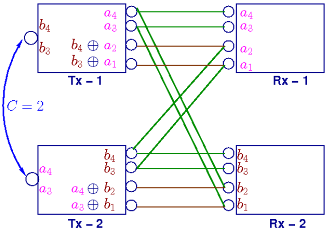


Figure: Deterministic IC: $m = 4, n = 2$ and $C = 2$

Achievable scheme: Class B

- When $C \leq n$
  - Transmit in Type VII links from 1 to $\min(n, C)$ as :

$$a_{m-n+i} \oplus b_i$$

  - If $n - \min(n, C) > 0$, then transmit in the remaining Type VII links

$$b_{\min(n,C)+i}, \qquad i = 1 \text{ to } n - \min(n, C)$$

  - If $\min(n, C) > 0$, then transmit in the Type V links

$$b_{m-n+i}, \qquad i = 1 \text{ to } \min(n, C)$$

- Secrecy capacity

$$C_S = n + \min(m - n, C)$$

- If $C > n$, then discard the excess $C - n$ bits!

Class A

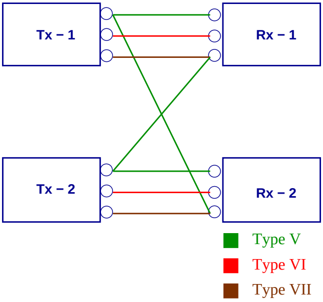


Figure: DIC: $m = 3$, and $n = 1$

- For class B: $m > 2n$
- Number of Type V links: $T_5 = m$
- Number of Type VII links: $T_7 = m$
- Number of Type VI links: $T_6 = m - 2n$

- Use the same achievable scheme as described for the Class B channel
- Transmit the data bits as it is on the Type VI links
- Secrecy capacity

$$
\begin{aligned}
C_S &= n + \min(m - n, C) + T_6 \\
&= m - n + \min(m - n, C)
\end{aligned}
$$

Class C

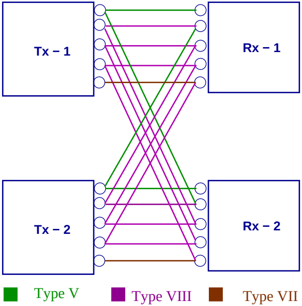


Figure: Deterministic IC: $m = 5$, and $n = 4$

- For Class C: $m < 2n$
- Number of Type VIII links: $T_8 = 2n - m$
- Number of Type V links: $T_5 = m - n$
- Number of Type VI links: $T_7 = m - n$

$T_8 > T_5 + T_7$ and $m < 2n$

- Type V and VII links do not interfere with each other
- At least $T_5 + T_7$ bits can be transmitted
- How many bits can be transmitted on the Type VIII links?
- Number of levels available for transmission on Type VIII links

$$r = T_8 - (T_5 + T_7)$$

- Transmitted bits get shifted by an amount of $m - n$ at the unintended Rx

Transmission on Type VIII links

- No. of bits that can be sent consecutively on Type VIII links: $B = m - n$
- No. of such consecutive levels: $B' = \lfloor \frac{r}{B} \rfloor$
- No. of consecutive levels that can be used for transmission

$$S = \begin{cases} \frac{B'}{2} & \text{if } B' \text{ is even} \\ \frac{B'+1}{2} & \text{if } B' \text{ is odd} \end{cases}$$

- Total number of bits sent on the consecutive level: SB
- No. of consecutive levels no bits transmitted: $S' = \lfloor \frac{r-SB}{B} \rfloor$
- No. of nonconsecutive levels: $u = r\%B$
- If $S' = S$ and $u \neq 0$, then these remaining u levels can be used for signal transmission
- If $S' \neq S$ and $u \neq 0$, then these remaining u levels can not be used for transmission

Achievable scheme: Class C

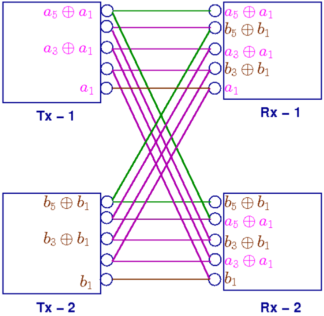
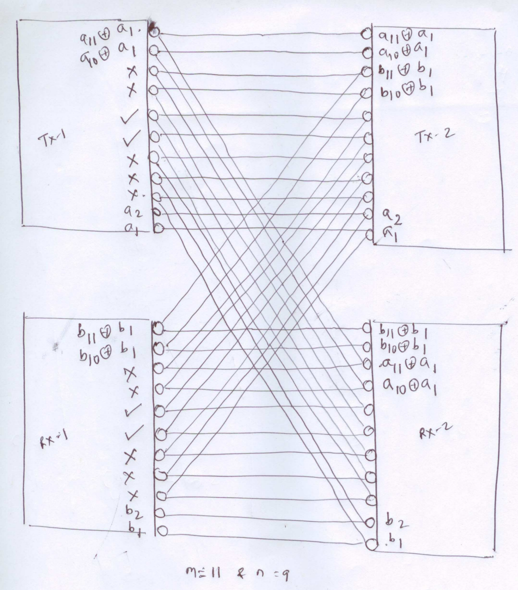
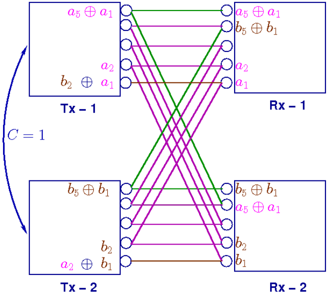
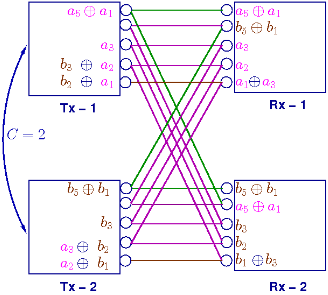


Figure: Deterministic IC: $m = 5, n = 4$ and $C = 0$

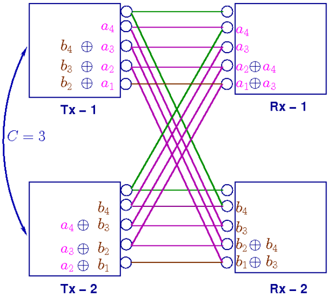

Tx-1
Tx-2
Rx-1
Rx-2
a11 ⊕ a1
a10 ⊕ a1
b11 ⊕ b1
b10 ⊕ b1
a2
a1
b2
b1
m=11 & n=9

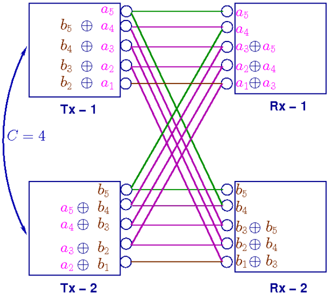


$a_5 \oplus a_1$
a_2
$b_2 \oplus a_1$
Tx – 1
$C = 1$
$b_5 \oplus b_1$
b_2
$a_2 \oplus b_1$
Tx – 2
$a_5 \oplus a_1$
$b_5 \oplus b_1$
a_2
a_1
Rx – 1
$b_5 \oplus b_1$
$a_5 \oplus a_1$
b_2
b_1
Rx – 2

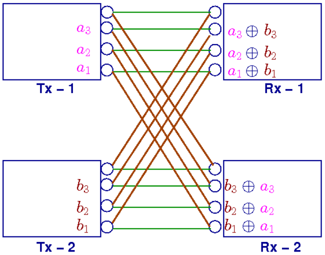


$a_5 \oplus a_1$
a_3
$b_3 \oplus a_2$
$b_2 \oplus a_1$
Tx – 1
$C = 2$
$b_5 \oplus b_1$
b_3
$a_3 \oplus b_2$
$a_2 \oplus b_1$
Tx – 2
$a_5 \oplus a_1$
$b_5 \oplus b_1$
a_3
a_2
$a_1 \oplus a_3$
Rx – 1
$b_5 \oplus b_1$
$a_5 \oplus a_1$
b_3
b_2
$b_1 \oplus b_3$
Rx – 2


a_4
$b_4 \oplus a_3$
$b_3 \oplus a_2$
$b_2 \oplus a_1$
Tx – 1
a_4
a_3
$a_2 \oplus a_4$
$a_1 \oplus a_3$
Rx – 1
$C = 3$
b_4
$a_4 \oplus b_3$
$a_3 \oplus b_2$
$a_2 \oplus b_1$
Tx – 2
b_4
b_3
$b_2 \oplus b_4$
$b_1 \oplus b_3$
Rx – 2


a_5
$b_5 \oplus a_4$
$b_4 \oplus a_3$
$b_3 \oplus a_2$
$b_2 \oplus a_1$
Tx – 1
a_5
a_4
$a_3 \oplus a_5$
$a_2 \oplus a_4$
$a_1 \oplus a_3$
Rx – 1
$C = 4$
b_5
$a_5 \oplus b_4$
$a_4 \oplus b_3$
$a_3 \oplus b_2$
$a_2 \oplus b_1$
Tx – 2
b_5
b_4
$b_3 \oplus b_5$
$b_2 \oplus b_4$
$b_1 \oplus b_3$
Rx – 2

Interference as strong as signal ($m = n$)

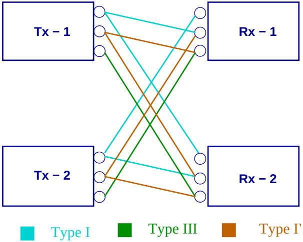


- $y_1 = y_2 = x_1 \oplus x_2$
- $C_S = 0$

High interference case: $m < n$

- Different type of links
  - Type I
  - Type II
  - Type III
  - Type IV
- Type of channel
  - Class 1
  - Class 2
  - Class 3

Class 3 channel



- For Class 3: $n < 2m$
- Number of Type VIII links: $T_4 = 2m - n$
- Number of Type V links: $T_5 = n - m$
- Number of Type VI links: $T_7 = n - m$

Achievable scheme: Class 3

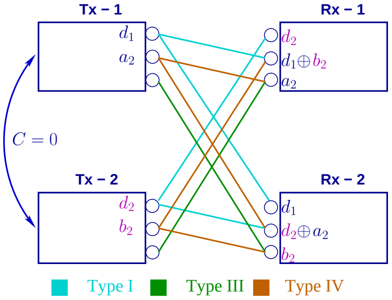


Figure: DIC: $m = 2, n = 3$ and $C = 0$

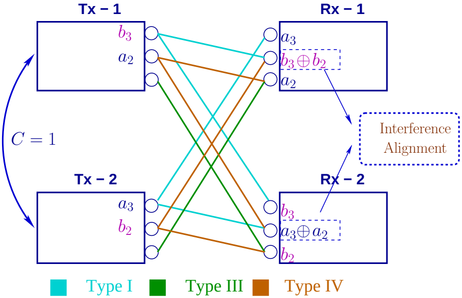


Figure: DIC: $m = 2, n = 3$ and $C = 1$

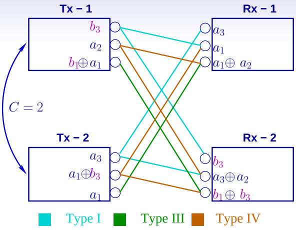


Figure: DIC: $m = 2, n = 3$ and $C = 2$ (First round)

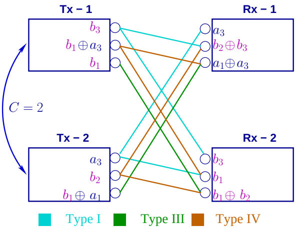


Figure: DIC: $m = 2, n = 3$ and $C = 2$ (Second round)

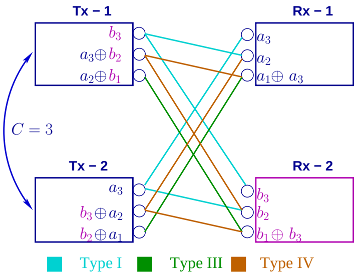


Figure: Deterministic IC: $m = 2, n = 3$ and $C = 3$

Some observations

- When $C = n$, it is possible to achieve $\max(m, n)$
- For Class A and B (weak/moderate intf. regime): scheme is optimal
- For Class C: not optimal always
- For Class 3 (high intf. regime): scheme is optimal when $C \geq 1$
- For Class 1 and 2: When $C = 0$, $C_S = 0$

Future work

- Outer bounds: DIC with source cooperation
- Use the insights obtained from DIC to derive inner/outer bounds for the GIC
- Is secrecy in DIC equivalent to secrecy in GIC?
- Is it possible to achieve the maximum possible rate (without secrecy constraint) as in DIC?
- $C_{\mathrm{DIC}} \subseteq C^{S}_{\mathrm{DIC}}$?
- What if, the users can not be trusted?