

Problem Statement

- The Gaussian MIMO multi-receiver wiretap channel:

$$\mathbf{Y}_k = \mathbf{H}_k \mathbf{X} + \mathbf{N}_k, \quad k = 1, \dots, K$$

$$\mathbf{Z} = \mathbf{H}_Z \mathbf{X} + \mathbf{N}_Z$$

where $\{\mathbf{N}_k\}_{k=1}^K, \mathbf{N}_Z$ are Gaussian random vectors with covariance matrices $\{\Sigma_k\}_{k=1}^K, \Sigma_Z$, respectively.

- The channel input \mathbf{X} is subject to a covariance constraint $E[\mathbf{X}\mathbf{X}^T] \preceq \mathbf{S}$.
- Secrecy is imposed by the following conditions

$$\lim_{n \rightarrow \infty} I(S(W); \mathbf{Z}^n) = 0, \quad \forall S(W)$$

where $S(W)$ denotes any subset of $\{W_1, \dots, W_K\}$.

- What is the **secrecy capacity region**?

Main Result

- Given the covariance matrices $\{\mathbf{K}_k\}_{k=1}^K$ such that $\sum_{k=1}^K \mathbf{K}_k \preceq \mathbf{S}$, we define the following rates

$$R_k^{\text{DPC}}(\pi, \{\mathbf{K}_k\}_{k=1}^K) = \frac{1}{2} \log \frac{|\mathbf{H}_k(\sum_{i=1}^k \mathbf{K}_{\pi(i)}) \mathbf{H}_k^T + \Sigma_{\pi(k)}|}{|\mathbf{H}_k(\sum_{i=1}^{k-1} \mathbf{K}_{\pi(i)}) \mathbf{H}_k^T + \Sigma_{\pi(k)}|} - \frac{1}{2} \log \frac{|\mathbf{H}_Z(\sum_{i=1}^k \mathbf{K}_{\pi(i)}) \mathbf{H}_Z^T + \Sigma_Z|}{|\mathbf{H}_Z(\sum_{i=1}^{k-1} \mathbf{K}_{\pi(i)}) \mathbf{H}_Z^T + \Sigma_Z|}$$

for $k = 1, \dots, K$, where $\pi(\cdot)$ is a one-to-one permutation on $\{1, \dots, K\}$.

- We define the following region:

$$\mathcal{R}^{\text{DPC}}(\pi, \mathbf{S}) = \bigcup \left\{ (R_1, \dots, R_K) : R_k = R_{k, \pi(k)}^{\text{DPC}}(\pi, \{\mathbf{K}_k\}_{k=1}^K) \right\}$$

where the union is over all positive semi-definite matrices $\{\mathbf{K}_k\}_{k=1}^K$ that satisfy $\sum_{k=1}^K \mathbf{K}_k \preceq \mathbf{S}$.

- Main result:

Theorem 1 The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel is given by the convex closure of the following union

$$\bigcup_{\pi \in \Pi} \mathcal{R}^{\text{DPC}}(\pi, \mathbf{S})$$

where Π is the set of all possible one-to-one permutations on $\{1, \dots, K\}$.

- Dirty-paper coding** with **stochastic encoding** is capacity-achieving.

An Outlook for the Proof

- We identify two sub-classes of our channel model:

– The **degraded** channel:

$$\mathbf{H}_k = \mathbf{I}, \quad k = 1, \dots, K, \text{ and } \mathbf{H}_Z = \mathbf{I}$$

$$\mathbf{0} \prec \Sigma_1 \preceq \dots \preceq \Sigma_K \preceq \Sigma_Z, \text{ i.e., we have the Markov chain}$$

$$\mathbf{X} \rightarrow \mathbf{Y}_1 \rightarrow \dots \rightarrow \mathbf{Y}_K \rightarrow \mathbf{Z}$$

– The **aligned** channel:

$$\mathbf{H}_k = \mathbf{I}, \quad k = 1, \dots, K, \text{ and } \mathbf{H}_Z = \mathbf{I}$$

• No order among noise covariance matrices

- Proof consists of three steps:

– We first find the secrecy capacity region for the **degraded** case

– Secondly, we obtain the secrecy capacity region for the **aligned** case

– We use **channel enhancement** and the capacity result for the **degraded** case

– Finally, we establish the secrecy capacity region of the general case by using some limiting argument with the capacity result for the **aligned** case

- Main contribution is the way we solve the **degraded** case, which will be outlined here!

The Degraded Multi-receiver Wiretap Channel

- Superposition coding** with **stochastic encoding** is optimal for the **degraded** multi-receiver wiretap channel

- In particular, the secrecy capacity region of the **degraded** multi-receiver wiretap channel is given as follows

Theorem 2 The secrecy capacity region of the **degraded** multi-receiver wiretap channel is given by the union of the rate tuples (R_1, \dots, R_K) satisfying

$$R_k \leq I(U_k; Y_k | U_{k+1}, Z), \quad k = 1, \dots, K$$

where $U_1 = X, U_{K+1} = \emptyset$, and the union is over all probability distributions of the form

$$p(u_k) p(u_{k-1} | u_k) \dots p(u_2 | u_3) p(x | u_2)$$

- We now evaluate this region for the **degraded Gaussian** MIMO multi-receiver wiretap channel, i.e., find the optimal joint distribution for (X, U_2, \dots, U_K) :

– Jointly Gaussian (X, U_2, \dots, U_K) is optimal.

The Degraded Gaussian MIMO Multi-receiver Wiretap Channel

- The secrecy capacity region of the **degraded Gaussian** MIMO multi-receiver wiretap channel is given as follows

Theorem 3 The secrecy capacity region of the **degraded Gaussian** MIMO multi-receiver wiretap channel is given by the union of the rate tuples R_1, \dots, R_K satisfying

$$R_k \leq \frac{1}{2} \log \frac{|\sum_{i=1}^k \mathbf{K}_i + \Sigma_k|}{|\sum_{i=1}^{k-1} \mathbf{K}_i + \Sigma_k|} - \frac{1}{2} \log \frac{|\sum_{i=1}^k \mathbf{K}_i + \Sigma_Z|}{|\sum_{i=1}^{k-1} \mathbf{K}_i + \Sigma_Z|}, \quad k = 1, \dots, K$$

where the union is over all positive semi-definite matrices $\{\mathbf{K}_k\}_{k=1}^K$ that satisfy $\sum_{k=1}^K \mathbf{K}_k \preceq \mathbf{S}$.

- Achievability of this region is immediate from Theorem 2:

– Jointly Gaussian $(\mathbf{X}, U_2, \dots, U_K)$ exhausts this region

Background for Proof of Theorem 3

- The worst additive noise lemma

Lemma 1 Let \mathbf{N} be a Gaussian random vector with covariance matrix Σ , and \mathbf{K}_X be a positive semi-definite matrix. Consider the following optimization problem,

$$\min_{p(\mathbf{X})} I(\mathbf{N}; \mathbf{N} + \mathbf{X}) \quad \text{s.t. } \text{Cov}(\mathbf{X}) = \mathbf{K}_X$$

where \mathbf{X} and \mathbf{N} are independent. A Gaussian \mathbf{X} is the minimizer of this optimization problem.

- A new extremal inequality:

Theorem 4 Let \mathbf{U}, \mathbf{X} be arbitrarily correlated random vectors which are independent of $\mathbf{N}_1, \mathbf{N}_2, \mathbf{N}_Z$, where $\mathbf{N}_1, \mathbf{N}_2, \mathbf{N}_Z$ are zero-mean Gaussian random vectors with covariance matrices $\mathbf{0} \prec \Sigma_1 \preceq \Sigma_2 \preceq \Sigma_Z$, respectively. Moreover, assume that the second moment of \mathbf{X} is constrained as $E[\mathbf{X}\mathbf{X}^T] \preceq \mathbf{S}$ where $\mathbf{S} \succeq \mathbf{0}$. Then, for any admissible (\mathbf{U}, \mathbf{X}) pair, there exists a matrix \mathbf{K}^* such that $\mathbf{0} \preceq \mathbf{K}^* \preceq \mathbf{S}$, and

$$h(\mathbf{X} + \mathbf{N}_Z | \mathbf{U}) - h(\mathbf{X} + \mathbf{N}_2 | \mathbf{U}) = \frac{1}{2} \log \frac{|\mathbf{K}^* + \Sigma_Z|}{|\mathbf{K}^* + \Sigma_2|}$$

$$h(\mathbf{X} + \mathbf{N}_Z | \mathbf{U}) - h(\mathbf{X} + \mathbf{N}_1 | \mathbf{U}) \geq \frac{1}{2} \log \frac{|\mathbf{K}^* + \Sigma_Z|}{|\mathbf{K}^* + \Sigma_1|}$$

- Proof of Theorem 4 can be found in our journal.

The desired bound on R_2

- We first use Theorem 2:

$$R_2 \leq I(U_2; \mathbf{Y}_2) - I(U_2; \mathbf{Z})$$

$$= [I(\mathbf{X}; \mathbf{Y}_2) - I(\mathbf{X}; \mathbf{Z})] - [I(\mathbf{X}; \mathbf{Y}_2 | U_2) - I(\mathbf{X}; \mathbf{Z} | U_2)] \quad (1)$$

where the equality is due to the chain rule and the Markov chain $U_2 \rightarrow \mathbf{X} \rightarrow (\mathbf{Y}_2, \mathbf{Z})$.

- The expression in the first bracket of (2) is

$$I(\mathbf{X}; \mathbf{Y}_2) - I(\mathbf{X}; \mathbf{Z}) = h(\mathbf{Y}_2) - h(\mathbf{Z}) - \frac{1}{2} \log \frac{|\Sigma_Z|}{|\Sigma_Z|} \quad (3)$$

- The difference of differential entropies in (3) is maximized by a Gaussian \mathbf{X} as shown

$$h(\mathbf{Y}_2) - h(\mathbf{Z}) = h(\mathbf{Y}_2) - h(\mathbf{Y}_2 + \tilde{\mathbf{N}}_2) = -I(\tilde{\mathbf{N}}_2; \mathbf{Y}_2 + \tilde{\mathbf{N}}_2) \leq \max_{\mathbf{0} \preceq \tilde{\Sigma}_2 \preceq \mathbf{S}} \frac{1}{2} \log \frac{|\mathbf{K} + \Sigma_Z|}{|\mathbf{K} + \Sigma_Z|} \quad (4)$$

$$= \frac{1}{2} \log \frac{|\mathbf{S} + \Sigma_Z|}{|\mathbf{S} + \Sigma_Z|} \quad (5)$$

where $\tilde{\mathbf{N}}_2$ is Gaussian with covariance matrix $\Sigma_Z - \Sigma_2$, and independent of \mathbf{X}, \mathbf{N}_2 . Inequality in (4) comes from Lemma 1.

- Plugging (5) into (3) yields

$$I(\mathbf{X}; \mathbf{Y}_2) - I(\mathbf{X}; \mathbf{Z}) \leq \frac{1}{2} \log \frac{|\mathbf{S} + \Sigma_Z|}{|\Sigma_Z|} - \frac{1}{2} \log \frac{|\mathbf{S} + \Sigma_Z|}{|\Sigma_Z|} \quad (6)$$

- We now consider the expression in the second bracket of (2) by using Theorem 4.

- According to Theorem 4, for any admissible (U_2, \mathbf{X}) , there exists a \mathbf{K}^* such that

$$h(\mathbf{X} + \mathbf{N}_Z | U_2) - h(\mathbf{X} + \mathbf{N}_2 | U_2) = \frac{1}{2} \log \frac{|\mathbf{K}^* + \Sigma_Z|}{|\mathbf{K}^* + \Sigma_2|} \quad (7)$$

which is equivalent to

$$I(\mathbf{X}; \mathbf{Z} | U_2) - I(\mathbf{X}; \mathbf{Y}_2 | U_2) = \frac{1}{2} \log \frac{|\mathbf{K}^* + \Sigma_Z|}{|\Sigma_Z|} - \frac{1}{2} \log \frac{|\mathbf{K}^* + \Sigma_2|}{|\Sigma_2|} \quad (8)$$

- Thus, using (6) and (8) in (2), we get

$$R_2 \leq \frac{1}{2} \log \frac{|\mathbf{S} + \Sigma_Z|}{|\mathbf{K}^* + \Sigma_2|} - \frac{1}{2} \log \frac{|\mathbf{S} + \Sigma_Z|}{|\mathbf{K}^* + \Sigma_2|} \quad (9)$$

which is the desired bound on R_2 given in Theorem 3.

The desired bound on R_1

- We use Theorem 2 again:

$$R_1 \leq I(\mathbf{X}; \mathbf{Y}_1 | U_2) - I(\mathbf{X}; \mathbf{Z} | U_2) = h(\mathbf{Y}_1 | U_2) - h(\mathbf{Z} | U_2) - \frac{1}{2} \log \frac{|\Sigma_Z|}{|\Sigma_Z|} \quad (10)$$

- We next bound the difference of conditional differential entropies in (10) by using Theorem 4.

- Theorem 4 states that for any admissible (U_2, \mathbf{X}) , there exists a matrix \mathbf{K}^* such that it satisfies (7) and also

$$h(\mathbf{Z} | U_2) - h(\mathbf{Y}_1 | U_2) \geq \frac{1}{2} \log \frac{|\mathbf{K}^* + \Sigma_Z|}{|\mathbf{K}^* + \Sigma_1|} \quad (11)$$

- Thus, using (11) in (10), we get

$$R_1 \leq \frac{1}{2} \log \frac{|\mathbf{K}^* + \Sigma_1|}{|\Sigma_1|} - \frac{1}{2} \log \frac{|\mathbf{K}^* + \Sigma_Z|}{|\Sigma_Z|} \quad (12)$$

which is the desired bound on R_1 given in Theorem 3