Optimal Trade-off Between Transmission Rate and Secrecy Rate in Gaussian MISO Wiretap Channels

Tobias J. Oechtering

joint work with Phuong Le Cao

WSA 2017 - Berlin

OVERVIEW

STATE OF THE ART

- Physical-layer secrecy has received much attention recently
- Wiretap channel - notable works:

  Wyner (1975) - **one of the pioneer studies**
  Csiszár and Körner (1978) - **extended to non-degraded case**
  Leung-Yan-Cheong and Hellman (1978)- **SISO Gaussian wiretap channel**
  F. Oggier *et al.* (2008), A. Khisti *et al.* (2010), J. Li *et al.* (2010), Q. Shi *et al.* (2012), Q. Li *et al.* (2013) - **MISO and MIMO wiretap channel with a sum power constraint**

- Per-antenna power constraints

  M. Vu (2011), Z. Pi (2012) - **point-to-point MISO/MIMO**
  W. Yu *et al.* (2007), S. Shi *et al.* (2008) - **multi-user MIMO**

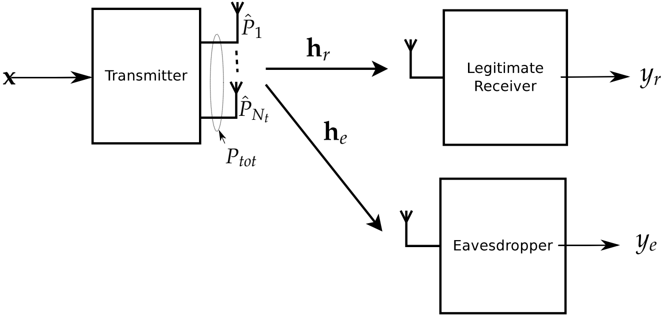
- Joint sum and per-antenna power constraints

  P. Cao *et al.* (2016,2017) - **point-to-point MISO/MIMO**

➔ **Wiretap channels with joint sum and per-antenna power constraints have not been considered yet.**

➔ **We are not aware that the optimal trade-off between communication rate and secrecy rate of a wiretap channel has been studied**

MISO WIRETAP CHANNEL



Power constraints

$$\mathcal{S}(\hat{\mathbf{p}}) := \{\mathbf{Q} \succeq 0 : \mathrm{tr}(\mathbf{Q}) \leq P_{tot}, \mathbf{e}_k^T \mathbf{Q} \mathbf{e}_k \leq \hat{P}_k, \forall k \in \mathcal{I}\},$$

where $\hat{\mathbf{p}} = [P_{tot}, \hat{P}_1, \ldots, \hat{P}_{N_t}], \mathcal{I} := \{1, \ldots, N_t\}$.

* **Sum power constraint only** is consider when the per-antenna power constraints are never active, i.e., $P_{tot} < \min_k\{\hat{P}_k\}$
* **Per-antenna power constraints only** is considered when the sum power constraint is never active, i.e., $P_{tot} > \sum_{i=1}^{N_t} \hat{P}_k$
* **Joint sum and per-antenna power constraints** are considered when the power relations satisfy $\min_k(\hat{P}_k) \leq P_{tot} \leq \sum_{i=1}^{N_t} \hat{P}_k$, i.e., both sum and per-antenna power constraints can be active

TRADE-OFF BETWEEN TRANSMISSION RATE AND SECRECY RATE

- Capacity and Secrecy capacity

$$C(\hat{\mathbf{p}}) = \max_{\mathbf{Q}\in\mathcal{S}(\hat{\mathbf{p}})} C(\mathbf{Q}) \text{ and } C_s(\hat{\mathbf{p}}) = \max_{\mathbf{Q}\in\mathcal{S}(\hat{\mathbf{p}})} C_s(\mathbf{Q})$$

where $C_s(\mathbf{Q}) = C(\mathbf{Q}) - C_e(\mathbf{Q}), C(\mathbf{Q}) = \log(1 + \mathbf{h}_r^H\mathbf{Q}\mathbf{h}_r), C_e(\mathbf{Q}) = \log(1 + \mathbf{h}_e^H\mathbf{Q}\mathbf{h}_e)$.

A necessary and sufficient condition for a positive secrecy rate of a Gaussian MISO wiretap channel, i.e., $C_s(\mathbf{Q}) > 0$, is that $\mathbf{h}_r\mathbf{h}_r^H$ - $\mathbf{h}_e\mathbf{h}_e^H \in \mathbb{C}^{N_t\times N_t}$ has to have a positive eigenvalue.

- Rate region describing the trade-off between transmission rate and secrecy rate with a given set of power constraints

$$\mathcal{R}_{MISO}(\hat{\mathbf{p}}) = \{[R, R_s] : 0 \le R_s \le R \le C(\mathbf{Q}), R_s \le C_s(\mathbf{Q}), \mathbf{Q} \in \mathcal{S}(\hat{\mathbf{p}})\}$$

$\mathcal{R}_{MISO}(\hat{\mathbf{p}})$ **is not necessarily a convex set sin** R_s **is non-convex**.

- If we allow time-sharing between rate pairs, the convex hull of the rate region is denoted by

$$\mathcal{C}_{MISO}(\hat{\mathbf{p}}) = \mathrm{Conv}\{[R, R_s] : 0 \le R_s \le R \le C(\mathbf{Q}), R_s \le C_s(\mathbf{Q}), \mathbf{Q} \in \mathcal{S}(\hat{\mathbf{p}})\}.$$

BOUNDARY OF RATE REGION

- The region $\mathcal{R}_{MISO}(\hat{\mathbf{p}})$ can be characterized by the set of all weighted rate sum optimal rate pairs.

- The weighted rate sum for a given weight vector $\mathbf{w} = [w_1, w_2] \in \mathbb{R}^2_+$ with $w_1 + w_2 = 1$

$$R_{\sum}(\mathbf{Q}, \mathbf{w}) := w_1 C(\mathbf{Q}) + w_2 C_s(\mathbf{Q}), \tag{1}$$

or equivalently

$$R_{\sum}(\mathbf{Q}, \mathbf{w}) = C(\mathbf{Q}) - w_2 C_e(\mathbf{Q}). \tag{2}$$

Find optimal transmit strategy **Q** with weights $w_1, w_2 \neq 0$

OPTIMIZATION PROBLEM

Optimization Problem

$$\begin{aligned} \text{maximize} \quad & R_{\sum}(\mathbf{Q}, \mathbf{w}) \\ \text{s.t.} \quad & \mathbf{Q} \in \mathcal{S}(\hat{\mathbf{p}}). \end{aligned}$$

Overall Solution

Our solution

- Alternating problem formulation
- Find optimal transmit strategy for a given $t \in [0, \ldots, 2^{C_s(\hat{\mathbf{p}})}]$.

  If we compute the optimal transmit strategy for all possible t, we obtain a parametrization of the boundary without time-sharing
- Find the best value of t

How to approach the solution?

Alternative problem formulation

Lemma 1 [JPKR'11, Scalar case]

Consider the function $f(D) = -DE + \log(D) + 1$ where $D, E \in \mathbb{R}, E > 0$. Then,

$$\max_{D>0} f(D) = \log(E^{-1}),$$

with the optimum value $D^* = E^{-1}$.

[3] J. Jose, N. Prasad, M. Khojastepour, and S. Rangarajan, "On robust weighted-sum rate maximixation in MIMO interference networks," in *IEEE International Conference on Communications (ICC)*, 2011.

Alternative problem formulation

Alternative optimization problem

$$R_{\sum}(\hat{\mathbf{p}}) = \max_{\mathbf{Q}\in\mathcal{S}(\hat{\mathbf{p}})} \log(1+\mathbf{h}_r^H\mathbf{Q}\mathbf{h}_r) - w_2\log(1+\mathbf{h}_e^H\mathbf{Q}\mathbf{h}_e)$$

$$= \max_{\mathbf{Q}\in\mathcal{S}(\hat{\mathbf{p}})} \{\min_{D_r>0}(D_r(1+\mathbf{h}_r^H\mathbf{Q}\mathbf{h}_r) - \log(D_r) - 1)$$

$$+ w_2 \max_{D_e>0}(-D_e(1+\mathbf{h}_e^H\mathbf{Q}\mathbf{h}_e) + \log(D_e) + 1)\}$$

Optimization to obtain optimal transmit strategy for a given t

$$\mathbf{Q}_{opt}(\hat{\mathbf{p}}, t) = \arg\max_{\mathbf{Q}\in\mathcal{S}(\hat{\mathbf{p}})} \mathbf{h}_r^H\mathbf{Q}\mathbf{h}_r - t\mathbf{h}_e^H\mathbf{Q}\mathbf{h}_e.$$

where $t = w_2\frac{D_e}{D_r}$.

PARAMETRIZATION OF THE BOUNDARY OF RATE REGION

Boundary of rate region

It is sufficient for the boundary of the rate region $\mathcal{R}_{MISO}(\hat{\mathbf{p}})$ to consider

$$0 \leq t \leq 2^{C_s(\hat{\mathbf{p}})},$$

where $C_s(\hat{\mathbf{p}})$ is the secrecy capacity.

Rate region corresponds to a set of power constraints $\mathcal{S}(\hat{\mathbf{p}})$

$$\begin{aligned}\mathcal{R}_{MISO}(\hat{\mathbf{p}}) =& \{[R, R_s] : 0 \leq R_s \leq R \leq C(\mathbf{Q}(\hat{\mathbf{p}}, t)),\\ & R_s \leq C_s(\mathbf{Q}(\hat{\mathbf{p}}, t)), t \in [0, 2^{C_s(\hat{\mathbf{p}})}]\}.\end{aligned}$$

- Sum power constraint, $\mathcal{S}(\hat{\mathbf{p}}) \rightarrow \mathcal{S}_{SPC}$
- Per-antenna power constraints, $\mathcal{S}(\hat{\mathbf{p}}) \rightarrow \mathcal{S}_{PAPC}$
- Joint sum and per-antenna power constraints, $\mathcal{S}(\hat{\mathbf{p}}) \rightarrow \mathcal{S}_{JSPC}$

Optimal transmit strategy for a given t

WITH SUM POWER CONSTRAINT

Problem:

$$\mathbf{Q}_{SPC}(t) = \arg\max_{\mathbf{Q}\in\mathcal{S}_{SPC}} \mathbf{h}_r^H\mathbf{Q}\mathbf{h}_r - t\mathbf{h}_e^H\mathbf{Q}\mathbf{h}_e.$$

Solution:

Closed-form solution

The closed-form expression for the optimal transmit strategy is given by

$$\mathbf{Q}_{SPC}(t) = P_{tot}\mathbf{v}\mathbf{v}^H$$

where $\mathbf{v}$ is the eigenvector associated with the largest eigenvalue of $\mathbf{h}_r\mathbf{h}_r^H - t\mathbf{h}_e\mathbf{h}_e^H$ for a given t.

Optimal transmit strategy for a given t

WITH PER-ANTENNA POWER CONSTRAINT

Problem:

$$\mathbf{Q}_{PAPC}(t) = \arg \max_{\mathbf{Q} \in \mathcal{S}_{PAPC}} \mathbf{h}_r^H \mathbf{Q} \mathbf{h}_r - t \mathbf{h}_e^H \mathbf{Q} \mathbf{h}_e.$$

Solution:

Diagonal elements

The optimal transmit strategy $\mathbf{Q}_{PAPC}(t)$ has diagonal elements $q_{kk} = \hat{P}_k$, $\forall k \in \mathcal{I}$.

Off-diagonal elements

We consider a relaxed optimization problem involving a 2×2 principal minors of $\mathbf{Q}_{PAPC}(t)$. The optimal transmit strategy $\mathbf{Q}_{PAPC-R}(t)$ of a relaxed optimization problem has off-diagonal elements

$$q_{kl}(t) = \frac{h_{rk}^* h_{rl} - t h_{ek}^* h_{el}}{|h_{rk}^* h_{rl} - t h_{ek}^* h_{el}|} \sqrt{\hat{P}_k \hat{P}_l}$$

with $k, l \in \mathcal{I}; k \neq l$.

Optimal transmit strategy for a given t

WITH PER-ANTENNA POWER CONSTRAINT

- If $\mathbf{Q}_{PAPC-R}(t) \succeq 0$, then $\mathbf{Q}_{PAPC}(t) = \mathbf{Q}_{PAPC-R}(t)$
- If there are only two transmit antennas, then $\mathbf{Q}_{PAPC}(t) = \mathbf{Q}_{PAPC-R}(t)$
- $\mathbf{Q}_{PAPC-R}(t)$ has rank one solution
- The numerical experiments show that the results of diagonal and off-diagonal elements hold for $N_t > 2$

OPTIMAL TRANSMIT STRATEGY FOR A GIVEN t

WITH JOINT SUM AND PER-ANTENNA POWER CONSTRAINTS

Problem:

$$\mathbf{Q}_{JSPC}(t) = \arg\max_{\mathbf{Q}\in\mathcal{S}_{JSPC}} \mathbf{h}_r^H \mathbf{Q} \mathbf{h}_r - t\mathbf{h}_e^H \mathbf{Q} \mathbf{h}_e$$

Solution:

Property

The optimal solution for the MISO wiretap channel with joint sum and per-antenna power constraints problem can be achieved when the transmit strategy uses full power P_{tot}, i.e., $\mathrm{tr}(\mathbf{Q}_{JSPC}(t)) = P_{tot}$.

Optimal transmit strategy for a given t

With joint sum and per-antenna power constraints

Solution (cont.):

Optimal transmit strategy (special case with two transmit antennas only)

Let $\mathbf{Q}_{SPC}(t)$ be the optimal transmit strategy under the sum power constraint only. Let $\mathcal{P} := \{k \in \mathcal{I} : \mathbf{e}_k^T \mathbf{Q}_{SPC}(t)\mathbf{e}_k > \hat{P}_k\}$ where $\mathcal{I} := \{1, 2\}$. Then, for the optimization problem with joint sum and per-antenna power constraints, we have

- If $\mathcal{P} = \emptyset$, $\mathbf{Q}_{JSPC}(t) = \mathbf{Q}_{SPC}(t)$
- Otherwise $\mathbf{Q}_{JSPC}(t)$ has diagonal elements

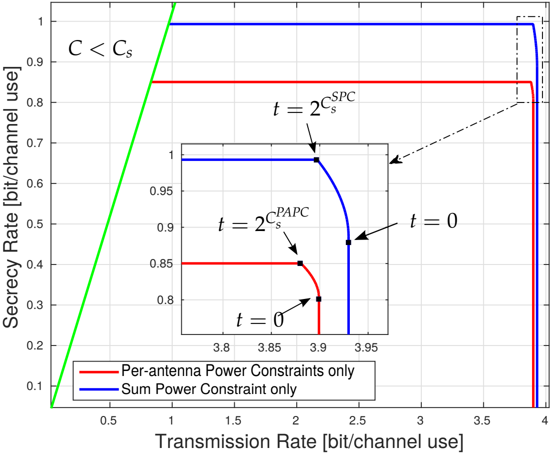
$$\begin{cases} \mathbf{e}_k^T \mathbf{Q}_{JSPC}(t)\mathbf{e}_k = \hat{P}_k, \\ \mathbf{e}_l^T \mathbf{Q}_{JSPC}(t)\mathbf{e}_l = P_{tot} - \hat{P}_k, \end{cases}$$

and off-diagonal elements

$$q_{kl}^{\star}(t) = \frac{h_{rk}^* h_{rl} - t h_{ek}^* h_{el}}{|h_{rk}^* h_{rl} - t h_{ek}^* h_{el}|} \sqrt{\hat{P}_k (P_{tot} - \hat{P}_k)},$$

with $k \in \mathcal{P}$, $l \neq k$.

OPTIMAL RATE REGION



Optimal regions between the transmission rates and the secrecy rate with sum power constraint only $P_{tot} = 14$ and per-antenna power constraints only $\hat{P}_1 = 6$ and $\hat{P}_2 = 8$

Summary and conclusions

- Trade-off between transmission rate and secrecy rate considering different power constraint settings
- Capacity region is characterized from the optimal rate pairs using a parametrization of the rate region
- Beam-forming is the optimal solution for the optimization problem with a sum power constraint only
- Under per-antenna power constraints only, the diagonal elements of the covariance matrix are set to be equals maximal individual transmit power on every antennas
- The optimal transmit strategy with joint sum and per-antenna power constraints is achieved when full sum transmit power is used. The transmit power is set equal to the maximal per-antenna transmit power if an optimal power allocation of the sum power constraint only solution exceeds a per-antenna power constraint.

Q & A