MIMO Gaussian Wiretap Channels with Two Transmit Antennas: Optimal Precoding and Power Allocation

Mojtaba Vaezi
joint work with Wonjae Shin, H. Vincent Poor, and Jungwoo Lee

Department of Electrical Engineering
Princeton University

International Symposium on Information Theory
Aachen, Germany
June 28, 2017

PHY Security - Motivation

Wireless (broadcast medium) has inherent security vulnerabilities

- Wireless Security
  - Cryptographic protocols (e.g., transport layer)
  - Physical layer (PHY) security

PHY security: use physical medium and the transmitted signals to aid in providing security

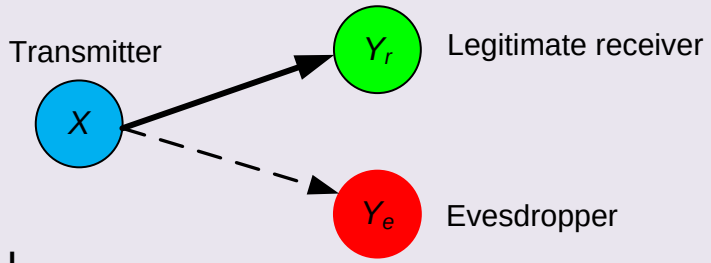
PHY Security - Motivation

Wireless (broadcast medium) has inherent security vulnerabilities

- Wireless Security
  - ☐ Cryptographic protocols (e.g., transport layer)
  - ☐ Physical layer (PHY) security

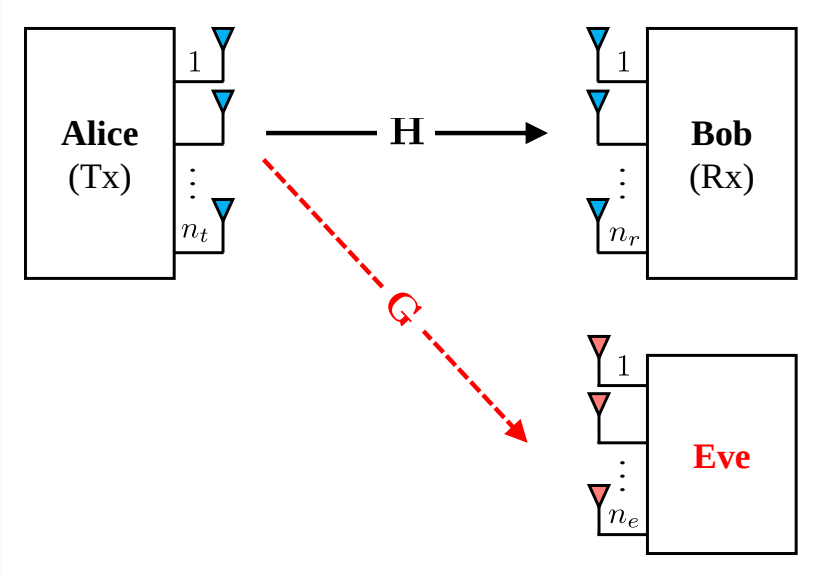
PHY security: use physical medium and the transmitted signals to aid in providing security

Key result ('degraded' wiretap channel [Wyner'75])



- Communication cab be both reliable and secure
  - Total (reliable) communication rate: $I(X;Y_r)$
  - Secure communication rate: $I(X;Y_r) - I(X;Y_e)$
- Secrecy is a plus rather than sacrificing communication rate

Channel Model

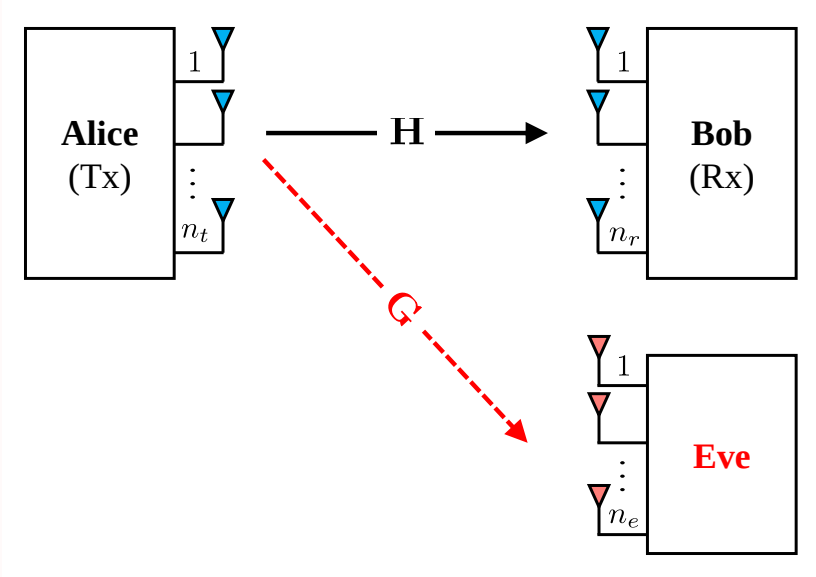


MIMO Gaussian wiretap channel

$$\mathbf{y}_r = \mathbf{H}\,\mathbf{x} + \mathbf{w}_r$$
$$\mathbf{y}_e = \mathbf{G}\,\mathbf{x} + \mathbf{w}_e$$

- $\mathbf{w}_r$ and $\mathbf{w}_e$ are i.i.d. Gaussian noise vectors
- $\mathrm{tr}(\mathbb{E}\{\mathbf{x}\mathbf{x}^t\}) = \mathrm{tr}(\mathbf{Q}) \leq P$ (average power constraint)

Channel Model



MIMO Gaussian wiretap channel

$$\mathbf{y}_r = \mathbf{H}\,\mathbf{x} + \mathbf{w}_r$$
$$\mathbf{y}_e = \mathbf{G}\,\mathbf{x} + \mathbf{w}_e$$

- $\mathbf{w}_r$ and $\mathbf{w}_e$ are i.i.d. Gaussian noise vectors
- $\mathrm{tr}(\mathbb{E}\{\mathbf{x}\mathbf{x}^t\}) = \mathrm{tr}(\mathbf{Q}) \le P$ (average power constraint)

Secrecy capacity [Khisti-Wornell'08] [Oggier-Hassibi'08]

$$\max_{\mathbf{Q}} \quad \frac{1}{2}\Big[\overbrace{\log\det(\mathbf{I}_{n_r} + \mathbf{H}\mathbf{Q}\mathbf{H}^t)}^{I(\mathbf{X};\mathbf{Y}_r)} - \overbrace{\log\det(\mathbf{I}_{n_e} + \mathbf{G}\mathbf{Q}\mathbf{G}^t)}^{I(\mathbf{X};\mathbf{Y}_e)}\Big] \qquad (1)$$
$$\text{s.t.} \quad \mathbf{Q} \succeq \mathbf{0}, \mathbf{Q} = \mathbf{Q}^t,\ \mathrm{tr}(\mathbf{Q}) \le P,$$

Closed-form Solution for $\mathbf{Q}$

This problem is still difficult as:

- Maximization over all admissible covariance matrices $\mathbf{Q}$
- This optimization problem is non-convex

Closed-form solution for the optimal $\mathbf{Q}$ is known only for

- MISO case ($n_r = 1$) [Khisti-Wornell'10]
- $n_t = n_r = 2$ and $n_e = 1$ [Shafiee-Liu-Ulukus'09]
- Strictly degraded channel ($\mathbf{H}^H\mathbf{H} \succ \mathbf{G}^H\mathbf{G}$) only if $P > P_0$

  [Loyka-Charalambous'16][Fakoorian-Swindlehurst'13]

Closed-form Solution for $\mathbf{Q}$

This problem is still difficult as:

- Maximization over all admissible covariance matrices $\mathbf{Q}$
- This optimization problem is non-convex

Closed-form solution for the optimal $\mathbf{Q}$ is known only for

- MISO case ($n_r = 1$) [Khisti-Wornell'10]
- $n_t = n_r = 2$ and $n_e = 1$ [Shafiee-Liu-Ulukus'09]
- Strictly degraded channel ($\mathbf{H}^H\mathbf{H} \succ \mathbf{G}^H\mathbf{G}$) only if $P > P_0$

  [Loyka-Charalambous'16][Fakoorian-Swindlehurst'13]

Questions

1. Can we find a closed-form solution for non-degraded case?
2. Is linear beamforming an optimal encoding strategy?

This Talk

We study MIMO Gaussian wiretap chancel with

- $n_t = 2$ and arbitrary n_r and n_e
- Channel state information is available at the transmitter and receiver
- **H** and **G** are real

Our contribution

- Linear beamforming is optimal for this channel
- A closed form solution for the power allocation
- A new approach to find the optimal input

Reformulating the Problem

since $\det(\mathbf{I}_m + \mathbf{AB}) = \det(\mathbf{I}_n + \mathbf{BA})$, we can write

$$\begin{aligned} C_s &= \max_{\mathbf{Q}} \frac{1}{2} \left[\log\det(\mathbf{I}_{n_r} + \mathbf{HQH}^t) - \log\det(\mathbf{I}_{n_e} + \mathbf{GQG}^t)\right] \\ &= \max_{\mathbf{Q}} \frac{1}{2} \log \frac{\det(\mathbf{I}_{n_t} + \mathbf{H}^t\mathbf{HQ})}{\det(\mathbf{I}_{n_t} + \mathbf{G}^t\mathbf{GQ})} \end{aligned} \tag{2}$$

- $\mathbf{H}^t\mathbf{H}$ and $\mathbf{G}^t\mathbf{G}$ are $n_t \times n_t$ symmetric matrices
- $\mathbf{Q} \in \mathbb{R}^{n_t \times n_t}$ is symmetric and can be *eigendecomposed* as

$$\mathbf{Q} = \mathbf{V}\mathbf{\Lambda}\mathbf{V}^t$$

- $\mathbf{V} \in \mathbb{R}^{n_t \times n_t}$ is an *orthogonal* matrix
- $\mathbf{\Lambda}$ is a diagonal matrix

Reformulating the Problem

Without loss of generality, for $n_t = 2$, let

$$\mathbf{V} = \begin{bmatrix} -\sin\theta & \cos\theta \\ \cos\theta & \sin\theta \end{bmatrix}, \quad \mathbf{\Lambda} = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}.$$

Further, assume

$$\mathbf{H}^t\mathbf{H} = \begin{bmatrix} h_1 & h_2 \\ h_2 & h_3 \end{bmatrix}, \quad \mathbf{G}^t\mathbf{G} = \begin{bmatrix} g_1 & g_2 \\ g_2 & g_3 \end{bmatrix}.$$

Then, the optimization problem in (2) is equivalent to

$$C_s = \max_{\lambda_1+\lambda_2 \le P} \frac{1}{2} \log \left(\frac{a_1 \sin 2\theta + b_1 \cos 2\theta + c_1}{a_2 \sin 2\theta + b_2 \cos 2\theta + c_2} \right), \quad (3)$$

in which a_1, b_1, c_1 and a_2, b_2, c_2 are functions of λ_1, λ_2 and channel coefficients.

We need to find θ, λ_1, λ_2. But, effectively, there are only two parameters to be designed.

Solving the New Problem

This problem can be solved in two steps:

1. Find θ: Using basic trigonometry we can show that optimal θ is obtained by

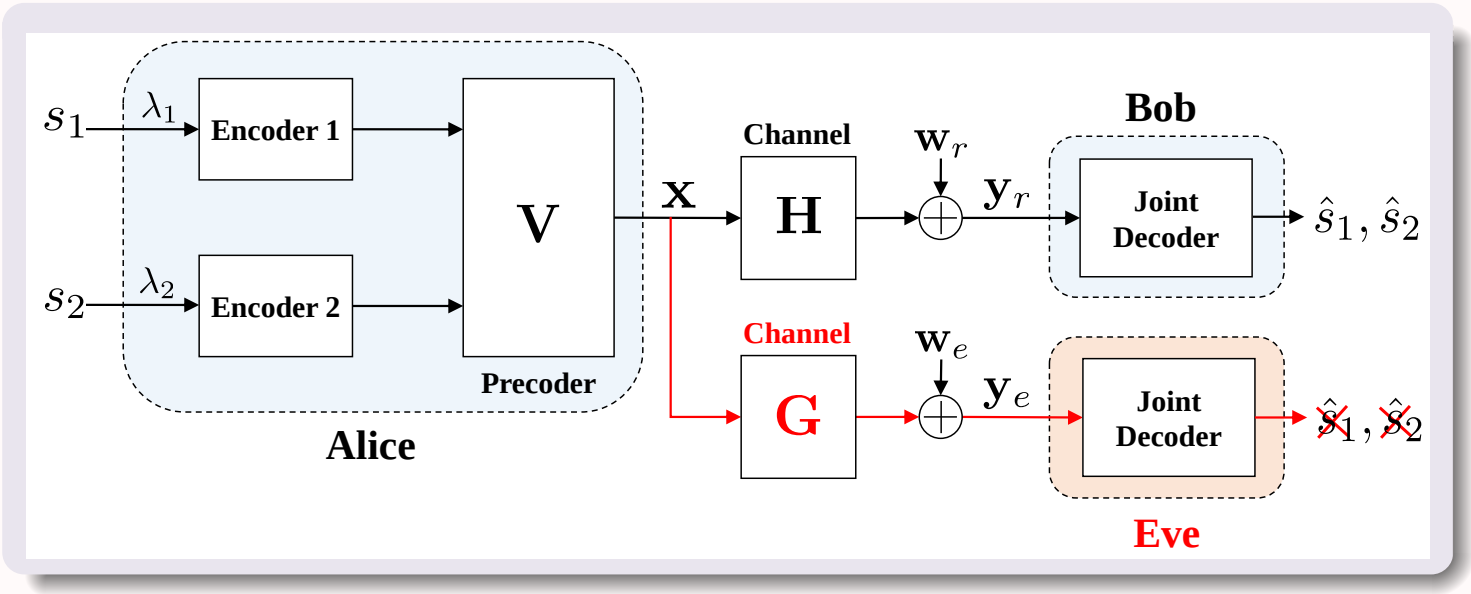
$$\theta = -\frac{1}{2}\arctan\frac{b}{a} + \frac{1}{2}\arcsin\frac{c}{\sqrt{a^2+b^2}} + \frac{\pi}{2},$$

in which $a = c_1 b_2 - c_2 b_1$, $b = a_1 c_2 - a_2 c_1$, and $c = a_1 b_2 - a_2 b_1$.

2. Find λ_1:
   - First, we show the constraint $\lambda_1 + \lambda_2 \leq P$ simplifies as $\lambda_1 + \lambda_2 = P$ except for the case $\mathbf{H}^H\mathbf{H} \preceq \mathbf{G}^H\mathbf{G}$ which has trivial solution.
   - Next, to find optimal λ_1 (or λ_2)
     - we can use linear search over $[0,\ P]$
     - we also have a closed form solution

Precoding and Power Allocation

Once the optimal $\mathbf{V}$, λ_1, and λ_2 are determined, very similar to the V-BLAST architecture



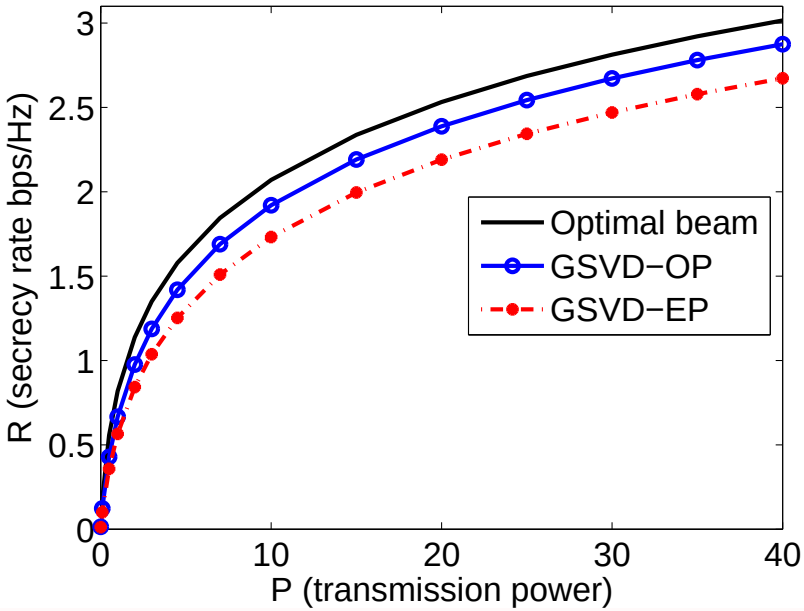
Intuition to the solution: design precoder to bring an effective channel advantage to legitimate user.

Special Cases

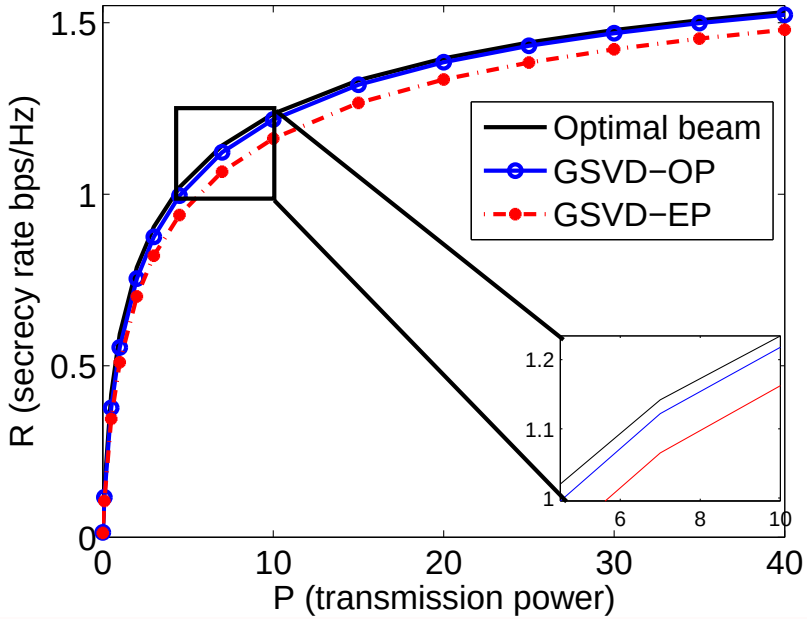
This solution includes several important cases as a special case:

1. $n_r = 1$ (MISO)
   Let $(\lambda_1, \lambda_2) = (0, P)$, find $\theta \longrightarrow$ [Khisti-Wornell'10]
   Solution: beamforming along the direction of the generalized eigenvector generalized eigenvectors of $(\mathbf{H}, \mathbf{G})$
2. $n_t = n_r = 2$ and $n_e = 1$
   Let $(\lambda_1, \lambda_2) = (0, P)$, find $\theta \longrightarrow$ [Shafiee-Liu-Ulukus'09]
3. Any rank-1 channel ($\mathbf{H}^H\mathbf{H} \not\succ \mathbf{G}^H\mathbf{G}$)
   Let $(\lambda_1, \lambda_2) = (0, P)$, find θ
4. MIMO without secrecy
   Let $\mathbf{G} = \mathbf{0} \longrightarrow$ waterfilling (capacity of MIMO)
5. strictly degraded channel ($\mathbf{H}^H\mathbf{H} \succ \mathbf{G}^H\mathbf{G}$)
   [Loyka-Charalambous'16][Fakoorian-Swindlehurst'13]

Simulation Results

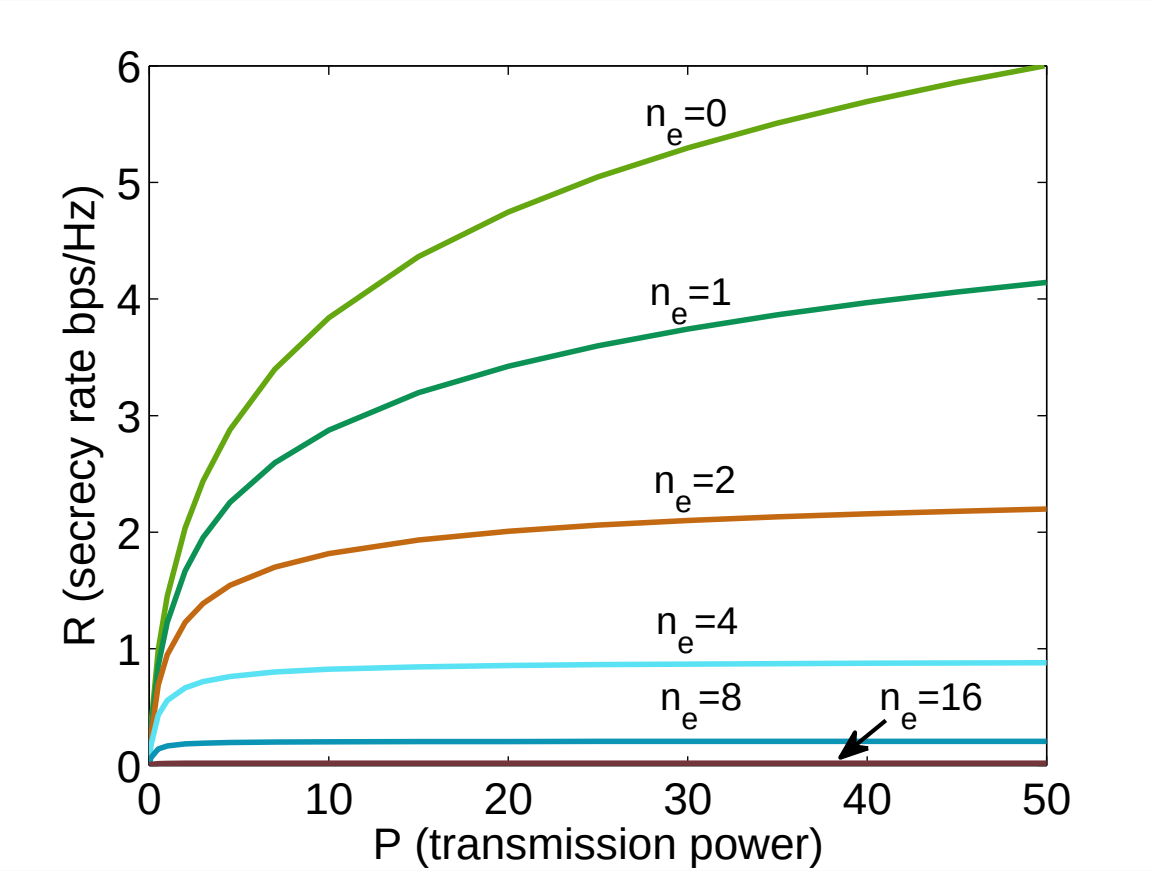


$n_t = 2,\ n_r = 2,\ n_e = 1$



$n_t = 2,\ n_r = 2,\ n_e = 2$

Simulation Results



Secrecy capacity for $n_t = 2$, and $n_r = 4$

Conclusions

Summary

- Linear precoding achieves the capacity of MIMO Gaussian wiretap channels with two antennas at transmitter
- A closed-form solution is developed to find optimal precoding and power allocation
- Beamforming is optimal when $n_r = 1$ and/or $n_e = 1$

Future Work

- Apply this method to MIMO Gaussian broadcast channel with confidential messages
- Extend this approach to complex channels
- Study the case with $n_t > 2$

Thank you!