SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

Going beyond Secrecy Rate via Information Jamming

Haiyang Zhang and Lingjie Duan

Singapore University of Technology and Design (SUTD)

December 12, 2018

Outline

- Background
- System Model & Problem Formulation
- Optimal Information Jamming Beamforming Design
- Suboptimal Design of Information Jamming
- Numerical Results
- Conclusion

Background: physical layer security

- The idea of physical layer security was first proposed by Wyner in his pioneering work [1], where the classic wiretap channel model was introduced in a discrete memoryless channel.
- The study in [1] was then extended to a Gaussian wiretap channel [2], where the secrecy rate is defined as the achievable rate difference between the main channel and the eavesdropper channel.
- Since then various techniques have been proposed to enlarge this difference, among which cooperative jamming is regarded as a very efficient approach.

[1] A. D. Wyner,"The wiretap channel," *Bell Sys. Tech. Journ.*, vol. 54, pp. 1355-1387, 1975.
[2] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. 24, pp. 451-456, Jul. 1978.

Background: cooperative jamming

- The cooperative jamming (CJ) approach was first proposed in [3], and its fundamental principle is to jam the eavesdropper by using artificial noise.

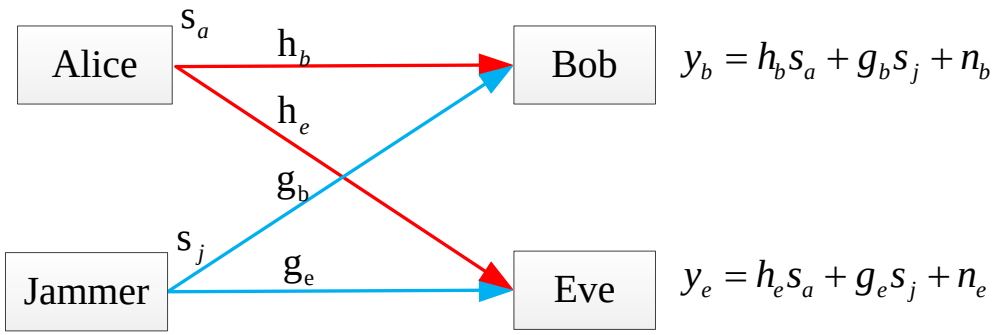

Figure: Illustration of the cooperative jamming approach.

- Though efficient, CJ has an inherent drawback: the jamming signal is independent of the source message (i.e., $s_j \neq s_a$), and thus it can not only disrupt the reception of the eavesdropper but also interfere with the legitimate receiver.

[3] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735-2751, Jun. 2008.

System Model & Motivation

Q1: *Can we design a new cooperative approach to achieve a better secrecy performance?*

We propose a novel approach, namely, *information jamming*, to go beyond the secrecy rate achieved by the cooperative jamming approach.

- A friendly information jammer (iJammer) sends the same source message s_a to strength the received signal at Bob and cancel that at Eve.
- Assume that there is a reliable backhaul link between Alice and iJammer for sharing the source information beforehand.

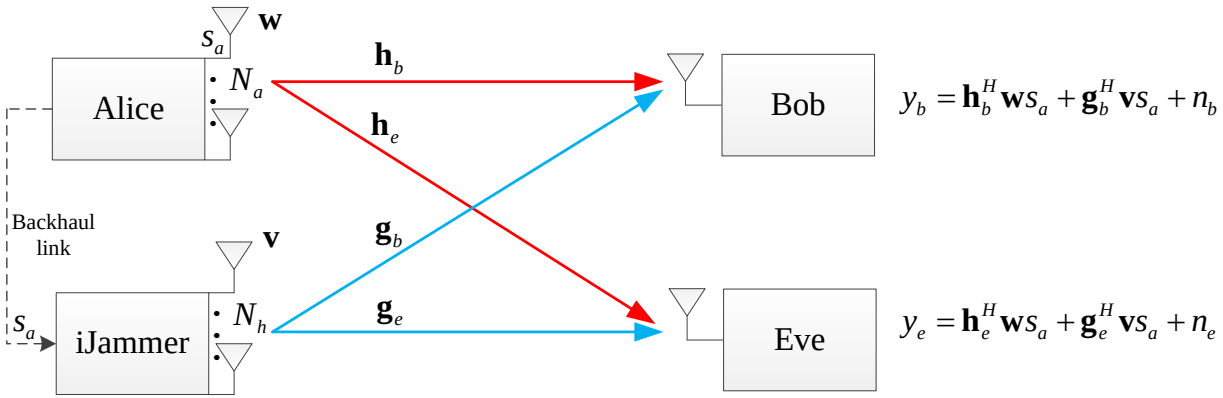

Figure: System model for the MISO wiretap channel with a friendly information jammer.

Problem Formulation-1

The achievable secrecy rate of our information jamming approach is given by

$$R(\mathbf{w},\mathbf{v}) = \Bigg[\underbrace{\log\left(1+\frac{\left|\mathbf{h}_b^H\mathbf{w}+\mathbf{g}_b^H\mathbf{v}\right|^2}{\sigma^2}\right)}_{R_b(\mathbf{w},\mathbf{v})} - \underbrace{\log\left(1+\frac{\left|\mathbf{h}_e^H\mathbf{w}+\mathbf{g}_e^H\mathbf{v}\right|^2}{\sigma^2}\right)}_{R_e(\mathbf{w},\mathbf{v})}\Bigg]^+, \quad (1)$$

where $R_b(\mathbf{w},\mathbf{v})$ and $R_e(\mathbf{w},\mathbf{v})$ denote the achievable rate at Bob and Eve, respectively.

- Notice that if the terms $\mathbf{h}_b^H\mathbf{w}$ and $\mathbf{g}_b^H\mathbf{v}$ in $R_b(\mathbf{w},\mathbf{v})$ add constructively, i.e., $\angle\mathbf{h}_b^H\mathbf{w} = \angle\mathbf{g}_b^H\mathbf{v}$, the achievable rate at Bob is enhanced.
- Similarly, if the terms $\mathbf{h}_e^H\mathbf{w}$ and $\mathbf{g}_e^H\mathbf{v}$ in $R_e(\mathbf{w},\mathbf{v})$ add destructively, i.e., $\angle\mathbf{h}_e^H\mathbf{w} = \pi + \angle\mathbf{g}_e^H\mathbf{v}$, the achievable rate at Eve is reduced.

For comparison, we also review the traditional cooperative jamming approach. If the jammer node sends the independent jamming signals, the corresponding achievable secrecy rate is

$$R^{CJ}(\mathbf{w},\mathbf{v}) = \left[\log\left(1+\frac{\left|\mathbf{h}_b^H\mathbf{w}\right|^2}{\left|\mathbf{g}_b^H\mathbf{v}\right|^2+\sigma^2}\right) - \log\left(1+\frac{\left|\mathbf{h}_e^H\mathbf{w}\right|^2}{\left|\mathbf{g}_e^H\mathbf{v}\right|^2+\sigma^2}\right)\right]^+ \quad (2)$$

Problem Formulation-2

In this work, we focus on the partial cooperative case where Alice does not change its beamforming vector $\mathbf{w}$ to cope with iJammer. In this case, iJammer tries to maximize the secrecy rate by optimizing its beamforming vector $\mathbf{v}$ with a fixed $\mathbf{w}=\bar{\mathbf{w}}$. The optimal beamforming design problem is formulated as

$$\begin{aligned} \max_{\mathbf{v}} \quad & R(\bar{\mathbf{w}},\mathbf{v}) = \log\left(1+\frac{\left|\mathbf{h}_b^H\bar{\mathbf{w}}+\mathbf{g}_b^H\mathbf{v}\right|^2}{\sigma^2}\right) - \log\left(1+\frac{\left|\mathbf{h}_e^H\bar{\mathbf{w}}+\mathbf{g}_e^H\mathbf{v}\right|^2}{\sigma^2}\right) \\ \text{s.t.} \quad & \|\mathbf{v}\|^2 \le P_j, \end{aligned} \tag{3}$$

Note that problem (3) is non-convex due to the non-concave objective function. In what follows, we provide:

- A semi-definite relaxation (SDR)-based numerical optimization approach to solve problem (3) optimally.
- Two suboptimal schemes with lower complexity to gain more analytical insights.

Optimal Solution-1

Problem (3) can be optimally solved via the follows three steps:

Step 1: By defining the augmented vector $\bar{\mathbf{v}} = \begin{bmatrix} \mathbf{v} \\ 1 \end{bmatrix}$, the effective channels $\mathbf{a}_b = \begin{bmatrix} \mathbf{g}_b \\ \bar{\mathbf{w}}^H \mathbf{h}_b \end{bmatrix}$ and $\mathbf{a}_e = \begin{bmatrix} \mathbf{g}_e \\ \bar{\mathbf{w}}^H \mathbf{h}_e \end{bmatrix}$, problem (3) is equivalent to

$$\max_{\bar{\mathbf{v}}} \quad \frac{\left|\mathbf{a}_b^H \bar{\mathbf{v}}\right|^2 + \sigma^2}{\left|\mathbf{a}_e^H \bar{\mathbf{v}}\right|^2 + \sigma^2} \quad \text{s.t.} \quad \|\bar{\mathbf{v}}\|^2 \leq P_j + 1, \bar{\mathbf{v}}\left(N_j + 1, 1\right) = 1. \tag{4}$$

Although problem (4) is more tractable than problem (3), it is still non-convex.

Step 2: By defining $\mathbf{V} = \bar{\mathbf{v}}\bar{\mathbf{v}}^H$ and following the SDR approach to drop the non-convex rank-one constraint, we transform problem (4) into the following quasi-convex problem.

$$\begin{aligned} \max_{\mathbf{V}} \quad & \frac{\mathrm{Tr}\left(\mathbf{a}_b \mathbf{a}_b^H \mathbf{V}\right) + \sigma^2}{\mathrm{Tr}\left(\mathbf{a}_e \mathbf{a}_e^H \mathbf{V}\right) + \sigma^2} \\ \text{s.t.} \quad & \mathrm{Tr}\left(\mathbf{V}\right) \leq P_j + 1, \mathbf{V}\left(N_j + 1, N_j + 1\right) = 1, \mathbf{V} \succeq 0, \\ & \cancel{\mathrm{Rank}\left(\mathbf{V}\right) = 1} \end{aligned} \tag{5}$$

Optimal Solution-2

Proposition 1

The optimal $\mathbf{V}^*$ *to problem* (5) *is of rank one, i.e.,* $\mathrm{Rank}\,(\mathbf{V}^*) = 1$.

- Proposition 1 indicates that the rank relaxation results in no loss of optimality.

Step 3: By introducing two new variables: $\eta = \frac{1}{\left(\mathrm{Tr}\left(\mathbf{a}_e\mathbf{a}_e^H\mathbf{V}\right)+\sigma^2\right)} > 0$ and $\mathbf{Q} = \eta\mathbf{V}$, we further recast problem (5) as

$$\begin{aligned} \max_{\mathbf{Q},\eta} \quad & \mathrm{Tr}\left(\mathbf{a}_b\mathbf{a}_b^H\mathbf{Q}\right) + \eta\sigma^2 \\ \text{s.t.} \quad & \mathrm{Tr}\left(\mathbf{a}_e\mathbf{a}_e^H\mathbf{Q}\right) + \eta\sigma^2 = 1, \mathrm{Tr}\left(\mathbf{Q}\right) \leq \eta\left(P_j+1\right), \\ & \mathbf{Q}\left(N_j+1, N_j+1\right) = \eta, \mathbf{Q} \succeq 0, \eta > 0. \end{aligned} \tag{6}$$

Note that problem (6) is a convex semi-definite program (SDP) problem, which can be efficiently solved by using the existing software, e.g., CVX.

Proposition 2

Problems (5) *and* (6) *are equivalent.*

- Let $(\mathbf{Q}^*, \eta^*)$ denote the optimal solution to problem (6), then the optimal solution to problem (5) is $\mathbf{V}^* = \frac{\mathbf{Q}^*}{\eta^*}$.

Suboptimal Scheme 1: targeting at improving Bob's reception

In this scheme, the iJammer's beamforming vector $\mathbf{v}$ is designed to strengthen the received signal at Bob, while avoiding confidential messages' leakage to Eve, i.e., $\mathbf{g}_e^H\mathbf{v} = 0$. Accordingly, the non-convex problem (3) reduces to

$$\max_{\mathbf{v}} \quad \left|\mathbf{h}_b^H\bar{\mathbf{w}} + \mathbf{g}_b^H\mathbf{v}\right|^2 \quad \text{s.t.} \quad \mathbf{g}_e^H\mathbf{v} = 0, \|\mathbf{v}\|^2 \leq P_j. \tag{7}$$

Proposition 3

The closed-form optimal beamforming solution to problem (7) is given by

$$\widehat{\mathbf{v}}^* = \sqrt{P_j}\frac{\left(\mathbf{I} - \widehat{\mathbf{g}}_e\widehat{\mathbf{g}}_e^H\right)\mathbf{g}_b e^{j\hat{\theta}^*}}{\left\|\left(\mathbf{I} - \widehat{\mathbf{g}}_e\widehat{\mathbf{g}}_e^H\right)\mathbf{g}_b\right\|}, \tag{8}$$

where $\widehat{\mathbf{g}}_e = \frac{\mathbf{g}_e}{\|\mathbf{g}_e\|}$ *and* $\hat{\theta}^* = \angle\mathbf{h}_b^H\bar{\mathbf{w}} - \angle\mathbf{g}_b^H\mathbf{v}_1^*$.

Proposition 3 indicates that iJammer should utilize its total transmit power and further adjust the beamforming direction such that:

- $\mathbf{h}_b^H\bar{\mathbf{w}}$ and $\mathbf{g}_b^H\widehat{\mathbf{v}}_1^*$ have the same phase angle.
- $\widehat{\mathbf{v}}_1^*$ lies in the null space of $\mathbf{g}_e$, i.e., $\mathbf{g}_e^H\widehat{\mathbf{v}}_1^* = 0$.

Suboptimal Scheme 2: targeting at avoiding Eve's reception

In this scheme, the beamforming vector $\mathbf{v}$ is designed to cancel the received signal at Eve as much as possible, while remaining the received signal strength at Bob unchanged, i.e., $\mathbf{g}_b^H\mathbf{v} = 0$. The original beamforming design problem (3) becomes

$$\min_{\mathbf{v}} \quad \left|\mathbf{h}_e^H\bar{\mathbf{w}} + \mathbf{g}_e^H\mathbf{v}\right|^2 \quad \text{s.t.} \quad \mathbf{g}_b^H\mathbf{v} = 0, \|\mathbf{v}\|^2 \le P_j. \tag{9}$$

Proposition 4

The closed-form optimal solution to problem (9) *is given by*

$$\tilde{\mathbf{v}}^* = \sqrt{p_t^*}\frac{\left(\mathbf{I} - \widehat{\mathbf{g}}_b\widehat{\mathbf{g}}_b^H\right)\mathbf{g}_e e^{j\tilde{\theta}^*}}{\left\|\left(\mathbf{I} - \widehat{\mathbf{g}}_b\widehat{\mathbf{g}}_b^H\right)\mathbf{g}_e\right\|}, \tag{10}$$

where $p_t^* = \min\left\{P_j, \frac{\left|\mathbf{h}_e^H\bar{\mathbf{w}}\right|^2}{\left|\mathbf{g}_e^H\mathbf{f}^*\right|^2}\right\}$, $\widehat{\mathbf{g}}_b = \frac{\mathbf{g}_b}{\|\mathbf{g}_b\|}$, $\tilde{\theta}^* = \angle\mathbf{h}_b^H\bar{\mathbf{w}} - \mathbf{g}_b^H\mathbf{v}_2^* - \pi$, $\mathbf{v}_2^* = \sqrt{p_t^*}\mathbf{f}^*$, *and* $\mathbf{f}^* = \frac{\left(\mathbf{I}-\widehat{\mathbf{g}}_b\widehat{\mathbf{g}}_b^H\right)\mathbf{g}_e}{\left\|\left(\mathbf{I}-\widehat{\mathbf{g}}_b\widehat{\mathbf{g}}_b^H\right)\mathbf{g}_e\right\|}$.

Proposition 4 indicates that:

- iJammer may only use part of the transmit power to perfectly cancel the received signal at Eve.
- Using more transmit power over-negate the received signal will leak information to Eve.

Comparison of Two suboptimal Schemes-1

Corollary 1

Once iJammer's power budget is sufficient, i.e., $P_j \geq \frac{\left\|\mathbf{h}_e^H \bar{\mathbf{w}}\right\|^2}{\left\|\mathbf{g}_e^H \mathbf{f}^*\right\|^2}$*, the secrecy rate achieved by the suboptimal scheme 2 serves as an upper-bound of that achieved by the traditional cooperative jamming approach.*

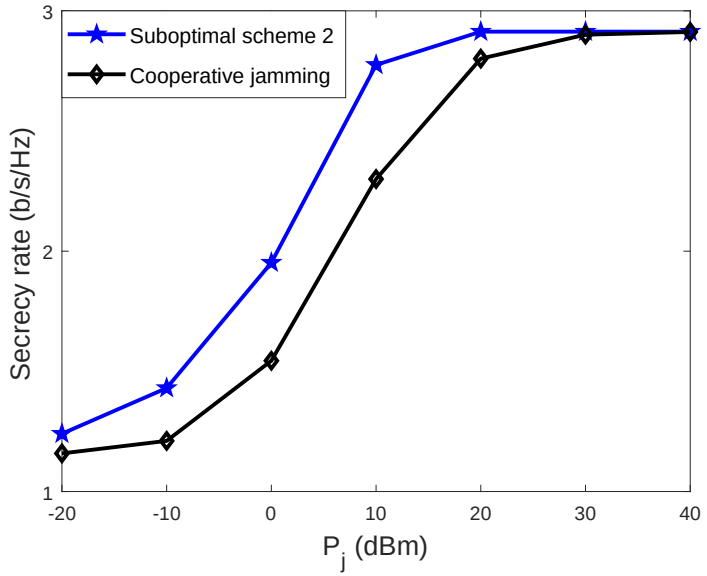

Figure: Comparison of the secrecy rates of the suboptimal scheme 2 and the cooperative jamming approach.

Comparison of Two suboptimal Schemes-2

Corollary 2

The secrecy rate achieved by the suboptimal scheme 1 is higher than that achieved by the suboptimal scheme 2 if the iJammer's power budget is further increased to $P_j \geq \bar{P}_j$, *where* $\bar{P}_j$ *is given by* $\bar{P}_j = \max\left\{\left(\frac{\sqrt{\left(\sigma^2+\left|\mathbf{h}_b^H\bar{\mathbf{w}}\right|^2\right)\left(\sigma^2+\left|\mathbf{h}_e^H\bar{\mathbf{w}}\right|^2\right)}-\sigma^2-\left|\mathbf{h}_b^H\bar{\mathbf{w}}\right|}{\left|\mathbf{g}_b^H\hat{\mathbf{v}}^*\right|}\right)^2, \frac{\left\|\mathbf{h}_e^H\bar{\mathbf{w}}\right\|^2}{\left\|\mathbf{g}_e^H\mathbf{f}^*\right\|^2}\right\}$.

- Corollary 2 implies that if iJammer's transmit power P_j is large enough, it is better to choose the suboptimal scheme 1 for achieving a higher secrecy rate.

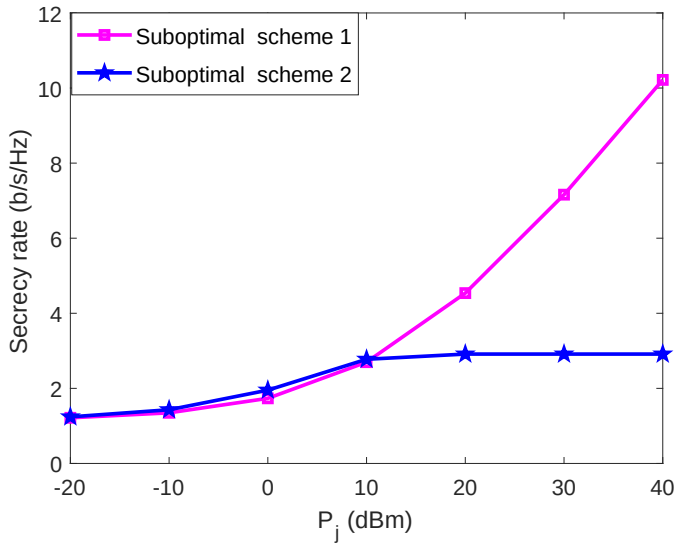

Figure: Comparison of the secrecy rates of the suboptimal schemes 1 and 2.

Numerical Results-1

Table: simulation parameters

Number of transmit antennas at Alice	$N_a = 3$
Number of transmit antennas at iJammer	$N_j = 3$
Maximum transmit power at Alice	$P_a = 10$ dBm
Alice's transmission beamforming vector	$\bar{\mathbf{w}} = \sqrt{P_a}\frac{\mathbf{h}_b}{\|\|\mathbf{h}_b\|\|}$
Noise variance	$\sigma^2 = -70$ dBm
Distance-dependent pass loss model	$L = A_0\left(\frac{d}{d_0}\right)^{-\alpha}$, with $A_0 = 10^{-3}$
Reference distance	$d_0 = 1$ m
Path loss exponent	$\alpha = 2.5$

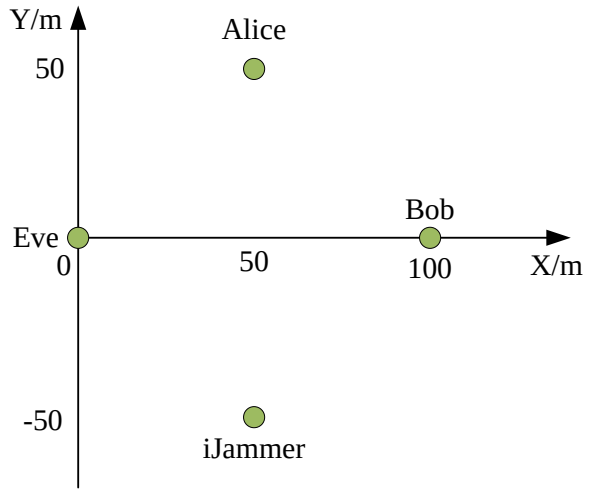

Figure: System setup for simulation on the 2D ground plane.

Numerical Results-2

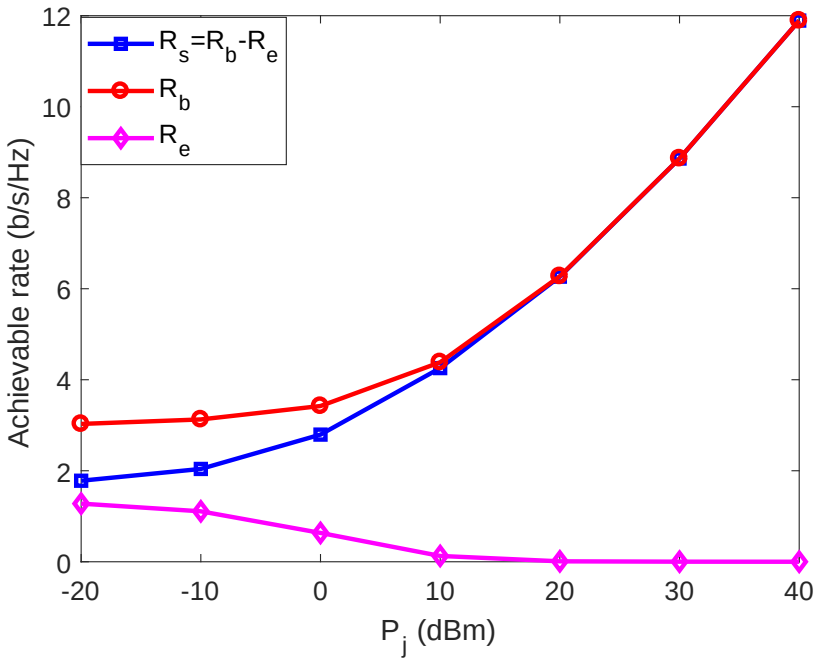

Figure: Illustration of the principle of the proposed information jamming approach.

- This illustrates that our proposed approach is capable of simultaneously improving the received signal strength at Bob and reducing that at Eve.

Numerical Results-3

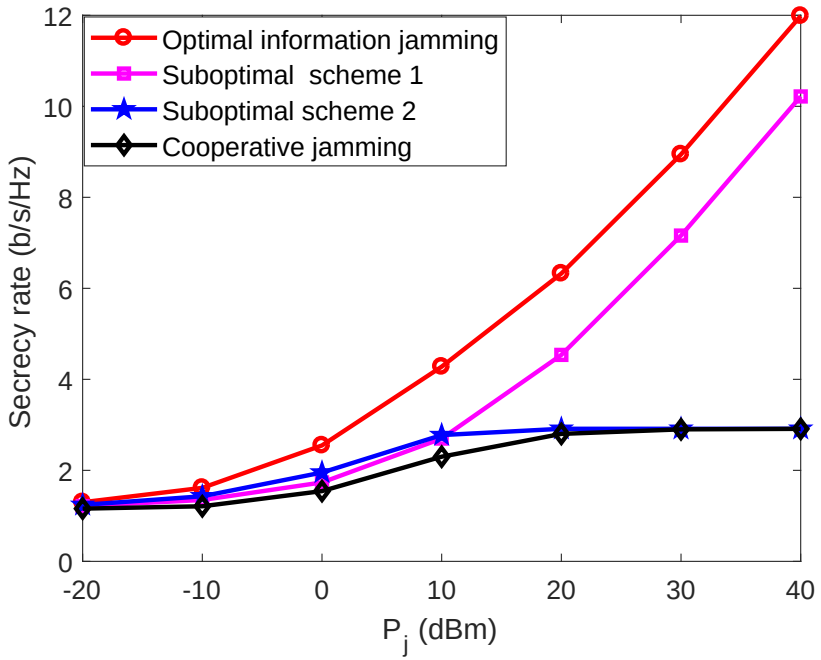

Figure: Comparison of the secrecy rates of our proposed schemes and the cooperative jamming approach.

- We can see that our proposed information jamming approach with the optimal solution significantly outperforms the traditional cooperative jamming approach.

Numerical Results-4

Q2: *Can the full cooperation information jamming approach (i.e., jointly design the beamforming vectors at Alice and iJammer) further increase the achievable secrecy rate?*

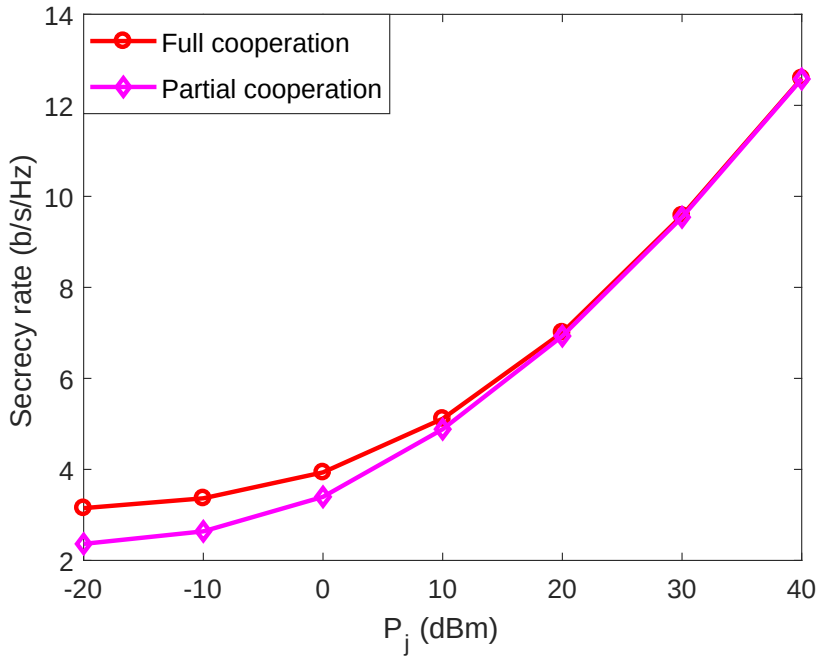

Figure: Comparison of the secrecy rates of the full cooperation case and partial cooperation case.

- The full cooperative beamforming design is meaningful for increasing the achievable secrecy rate when P_j is in the small transmit power regime.

Conclusion

- We propose a novel information jamming approach for going beyond the secrecy rate achieved by the traditional cooperative jamming approach.
- We propose a SDR-based numerical approach to solve the non-convex beamforming problem optimally.
- To obtain analytical results for information jamming design, we also provide two suboptimal information beamforming schemes of low computation complexity and obtain the optimal beamforming vector in the closed-form for each scheme.

Thank you!