Secure ISAC Downlink Beamforming: A SDR Approach with Tightness Guaranteed

Wai-Yiu Keung[†‡], Hoi-To Wai[§], Wing-Kin Ma[†]

[†]Department of Electronic Engineering
[§]Department of System Engineering and Engineering Management
[‡]Department of Computer Science and Engineering

The Chinese University of Hong Kong

June 4, 2023

Slides available at www.cse.cuhk.edu.hk/~wykeung/slides/secure-isac.pdf

Motivation

- the fight for bandwidth resources has always been competitive; spectrum congestion remains critical in 5G & beyond as comm. sys. eye at the radar band

- radar-communication coexistence: use interference management techniques to allow both radar and comm. systems to service in the same band

- integrated sensing and communication (ISAC): to leverage the assigned resources by designing an unified signal for both radar and comm. purposes

  - advantages: unified hardware means cheap & energy-efficient implementation; allows efficient usage of bandwidth

  - challenges: difficult to employ network layer secrecy measures in dense networks; requires dedicated signal designs that serve both sensing and comm. purposes

- **our goal:** provide a beamformer design framework that serves radar-comm. with physical layer security using the least amount of radiation power

Problem Scenario

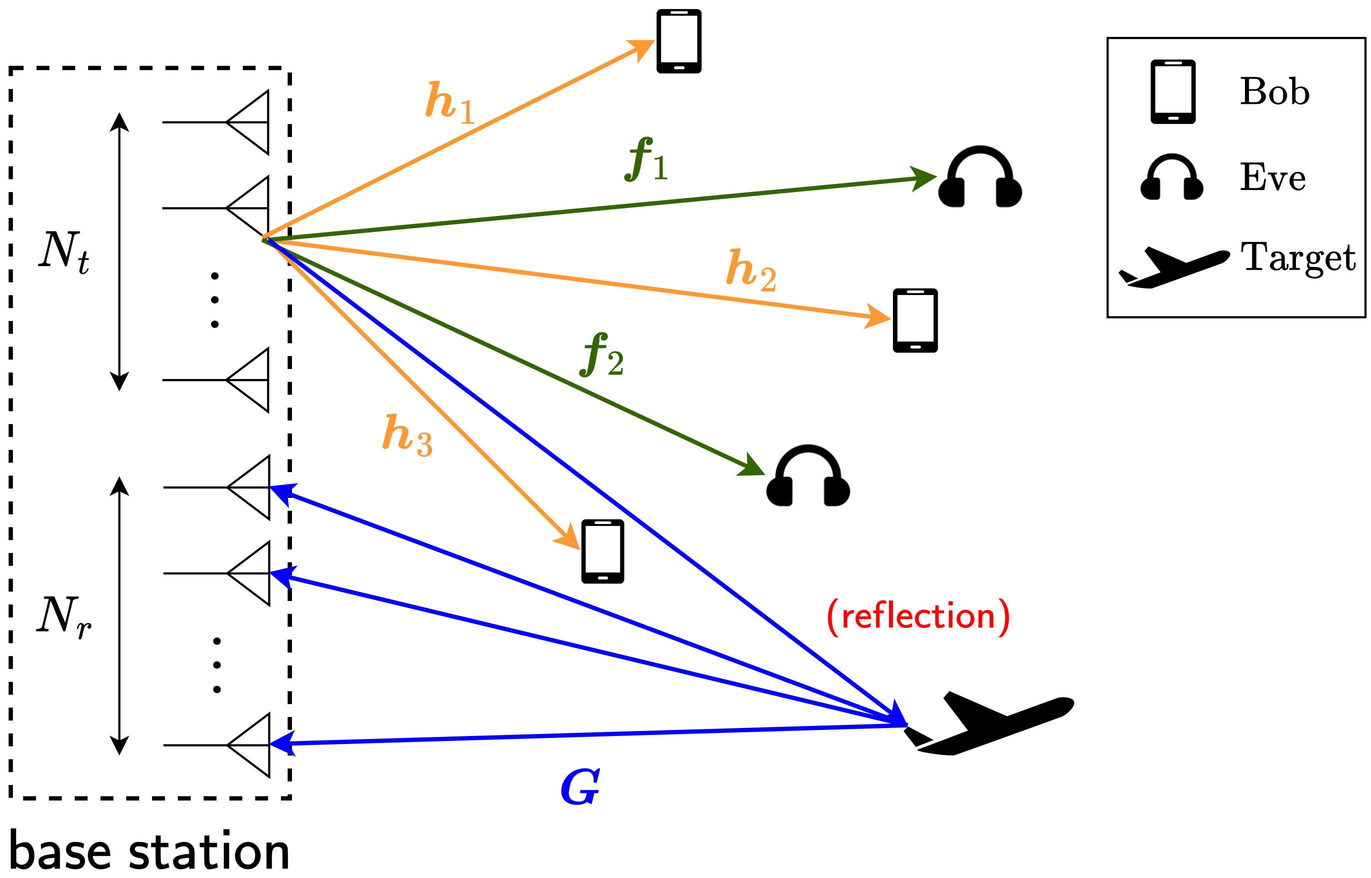


Figure: Illustration of an ISAC beamforming scenario under the presence of eavesdropper.

- the base station (BS) has N_t transmit antenna with N_r sensing antenna, servicing in a cell over a block-fading channel
- BS communicates with K legitimate users (Bobs) with J eavesdroppers (Eves) overhearing the channel; BS also aims to estimate an unknown response matrix $\boldsymbol{G}$ by radar

Signal Model

- $\boldsymbol{x}_t \in \mathbb{C}^{N_t}$ is the signal vector; under some standard assumptions, it can be written as

$$\boldsymbol{x}_t = \sum_{k=1}^{K} \boldsymbol{w}_k s_{k,t} + \boldsymbol{b}_t$$

  where
  - $s_{k,t} \in \mathcal{S}$ is the information carrying symbol, where $\mathcal{S}$ is a finite alphabet
  - $\boldsymbol{w}_k \in \mathbb{C}^{N_t}$ is the beamformer for the k-th Bob
  - $\boldsymbol{b}_t$ is a non-message carrying signal to serve the radar and jamming purposes

- conventionally $\boldsymbol{b}_t \sim \mathcal{CN}(\mathbf{0}, \boldsymbol{\Sigma})$ is called as the artificial noise (AN) in physical layer security; we denote its spatial covariance matrix as $\boldsymbol{\Sigma} = \boldsymbol{W}_{K+1}$ for convenience

- received signal of the k-th Bob, the i-th Eve, and the ℓ-th sensing antenna are:

$$y_{k,t} = \boldsymbol{h}_k^{\mathsf{H}} \boldsymbol{x}_t + v_{k,t}, \quad k = 1, \ldots, K, \qquad \text{(Bob's rx signal)}$$

$$r_{i,t} = \boldsymbol{f}_i^{\mathsf{H}} \boldsymbol{x}_t + v_{i,t}, \quad i = 1, \ldots, J, \qquad \text{(Eves' rx signal)}$$

$$z_{\ell,t} = \boldsymbol{g}_\ell^{\mathsf{H}} \boldsymbol{x}_t + v_{\ell,t}, \quad \ell = 1, \ldots, N_r, \qquad \text{(Radar rx signal)}$$

  where v's are the respective background noise with zero-mean and σ^2-variance

- assumption: the BS knows $\boldsymbol{h}_k$'s and $\boldsymbol{f}_i$'s, but not $\boldsymbol{g}_\ell$'s

Quality of Service: Our Choices

$$\begin{aligned} \underset{\{\boldsymbol{W}_k\}_{k=1}^{K+1}}{\text{minimize}} \quad & \text{signal power} && (2)\\ \text{subject to} \quad & \text{comm. metric} \geq \gamma && (\mathrm{C})\\ & \text{security metric} \leq \rho && (\mathrm{J})\\ & \text{sensing error metric} \leq \beta && (\mathrm{S})\\ & \boldsymbol{W}_{K+1} \succeq \mathbf{0}, \quad \boldsymbol{W}_k = \boldsymbol{w}_k \boldsymbol{w}_k^{\mathsf{H}} \ \ \forall k = 1, \ldots, K \end{aligned}$$

- signal power: $\mathbb{E}(\boldsymbol{x}_t^{\mathsf{H}} \boldsymbol{x}_t) = \sum_{k=1}^{K} \boldsymbol{w}_k^{\mathsf{H}} \boldsymbol{w}_k \mathbb{E}(|s_{k,t}|^2) + \mathbb{E}(\boldsymbol{b}_t^{\mathsf{H}} \boldsymbol{b}_t) = \sum_{k=1}^{K+1} \mathrm{tr}(\boldsymbol{W}_k)$
- comm./ security metric: signal-to-interference-plus-noise ratio, e.g.

$$\mathrm{SINR}_k\left(\{\boldsymbol{W}_i\}_{i=1}^{K+1}\right) = \frac{|\boldsymbol{h}_k^{\mathsf{H}} \boldsymbol{w}_k|^2}{\sum_{j=1, j\neq k}^{K} |\boldsymbol{h}_k^{\mathsf{H}} \boldsymbol{w}_j|^2 + \boldsymbol{h}_k^{\mathsf{H}} \boldsymbol{W}_{K+1} \boldsymbol{h}_k + \sigma^2}$$

  is defined for Bobs; replace $\boldsymbol{h}_k$'s with $\boldsymbol{f}_i$'s for that of Eves
- radar sensing metric: Cramér-Rao bound of the target response matrix estimate **[LLL+22]**:

$$\mathrm{CRB}(\{\boldsymbol{W}_k\}_{k=1}^{K+1}) \propto \mathrm{tr}[(\textstyle\sum_{k=1}^{K+1} \boldsymbol{W}_k)^{-1}]$$

- the QoS requirements are symbolized by γ, ρ and β

Quick Review on Semidefinite Relaxation (SDR)

Problem: complex-valued quadratically constrained quadratic programme (QCQP)

$$\begin{aligned} \underset{\boldsymbol{w}_1,\ldots,\boldsymbol{w}_K \in \mathbb{C}^N}{\text{minimize}} \quad & \textstyle\sum_{k=1}^K \boldsymbol{w}_k^{\mathsf{H}} \boldsymbol{w}_k \\ \text{subject to} \quad & \textstyle\sum_{k=1}^K \boldsymbol{w}_k^{\mathsf{H}} \boldsymbol{C}_i \boldsymbol{w}_k \geq b_i, \quad \boldsymbol{C}_i \in \mathbb{H}^N, b_i \in \mathbb{R} \quad i = 1, \ldots, I \end{aligned}$$

where the constraint matrices $\boldsymbol{C}_i$'s are Hermitian; The problem is non-convex.

SDR: leverage the equivalence of $\boldsymbol{W}_k = \boldsymbol{w}_k \boldsymbol{w}_k^{\mathsf{H}} \iff \boldsymbol{W}_k \succeq \boldsymbol{0}, \mathrm{rank}(\boldsymbol{W}_k) = 1$; dropping the rank one constraint directs us to a convex programme:

$$\begin{aligned} \underset{\boldsymbol{W}_1,\cdots,\boldsymbol{W}_K \in \mathbb{H}^N}{\text{minimize}} \quad & \textstyle\sum_{k=1}^K \mathsf{tr}(\boldsymbol{W}_k) \\ \text{subject to} \quad & \textstyle\sum_{k=1}^K \mathsf{tr}(\boldsymbol{C}_i \boldsymbol{W}_k) \geq b_i, \quad \boldsymbol{C}_i \in \mathbb{H}^N, b_i \in \mathbb{R} \quad i = 1, \ldots, I \\ & \boldsymbol{W}_1, \cdots, \boldsymbol{W}_K \succeq \boldsymbol{0}, \quad \cancel{\mathrm{rank}(\boldsymbol{W}_1) = \cdots = \mathrm{rank}(\boldsymbol{W}_K) = 1} \end{aligned}$$

This allows a comfortable convex approx. scheme for QCQP, and is suitable to many beamforming problems; but several issues remain:

- approx. means the solutions $\boldsymbol{W}_k^\star$ *may or may not* be of rank one
- the relaxation is said to be **tight** if $\mathrm{rank}(\boldsymbol{W}_k^\star) = 1$, or, equivalently $\boldsymbol{W}_k^\star = \boldsymbol{w}_k \boldsymbol{w}_k^{\mathsf{H}}$, for $k = 1, \ldots, K$, i.e. $\boldsymbol{w}_k$ serves as a feasible solution to the QCQP

Existing SDR-based Beamforming Formulations

- one of the most **classical formulations**:

$$\underset{\{\boldsymbol{W}_k=\boldsymbol{w}_k\boldsymbol{w}_k^{\mathsf{H}}\}_{k=1}^K}{\text{minimize}} \quad \text{signal power}$$
$$\text{subject to} \quad \text{Bobs' SINR} \geq \gamma$$

  has its SDR shown to be tight by the uplink-dowlink duality **[BO01]**, or the Shapiro-Barvinok-Pataki SDP rank-reduction result **[HP10]**

- another design for **AN-assisted physical layer security** was studied in **[LM16]**:

$$\underset{\{\boldsymbol{W}_k=\boldsymbol{w}_k\boldsymbol{w}_k^{\mathsf{H}}\}_{k=1}^K, \boldsymbol{W}_{K+1}\succeq \boldsymbol{0}}{\text{minimize}} \quad \text{signal power}$$
$$\text{subject to} \quad \text{Bobs' SINR} \geq \gamma, \quad \text{Eves' SINR} \leq \rho$$

  wherein its SDR is tight

- an **ISAC variation** has been studied in **[LLL+22]**, viz.:

$$\underset{\{\boldsymbol{W}_k=\boldsymbol{w}_k\boldsymbol{w}_k^{\mathsf{H}}\}_{k=1}^K, \boldsymbol{W}_{K+1}\succeq \boldsymbol{0}}{\text{minimize}} \quad \text{CRB of the sensing error}$$
$$\text{subject to} \quad \text{Bobs' SINR} \geq \gamma, \quad \text{signal power} \leq P$$

  in which a rank one solution can be obtained by a cheap post-processing technique

Proposed Formulation

$$\begin{aligned}
\underset{\{\boldsymbol{W}_k\}_{k=1}^{K+1}}{\text{minimize}} \quad & \textstyle\sum_{k=1}^{K} \mathrm{tr}(\boldsymbol{W}_k) + \alpha\, \mathrm{tr}(\boldsymbol{W}_{K+1}) \\
\text{subject to} \quad & \tfrac{1}{\gamma}\mathrm{tr}(\boldsymbol{W}_k\boldsymbol{H}_k) \geq \textstyle\sum_{j=1,j\neq k}^{K+1} \mathrm{tr}(\boldsymbol{W}_j\boldsymbol{H}_k) + \sigma^2 \ (\text{Bob's SINR} \geq \gamma) \qquad \text{(C)} \\
& \tfrac{1}{\rho}\mathrm{tr}(\boldsymbol{W}_k\boldsymbol{F}_i) \leq \textstyle\sum_{j=1,j\neq k}^{K+1} \mathrm{tr}(\boldsymbol{W}_j\boldsymbol{F}_i) + \sigma^2 \ (\text{Eve's SINR} \leq \rho) \qquad \text{(J)} \\
& \mathrm{tr}[(\textstyle\sum_{k=1}^{K+1} \boldsymbol{W}_k)^{-1}] \leq T\beta/\sigma^2 N_r \ (\text{CRB} \leq \beta) \qquad \text{(S)} \\
& \boldsymbol{W}_{K+1} \succeq \boldsymbol{0}, \cancel{\boldsymbol{W}_k = \boldsymbol{w}_k\boldsymbol{w}_k^{\mathsf{H}},} \boldsymbol{W}_k \succeq \boldsymbol{0} \\
& \boldsymbol{H}_k = \boldsymbol{h}_k\boldsymbol{h}_k^{\mathsf{H}},\ \boldsymbol{F}_i = \boldsymbol{f}_i\boldsymbol{f}_i^{\mathsf{H}}, \qquad k = 1, \cdots, K,\ i = 1, \cdots, J.
\end{aligned}$$

- major differences from (2):
  - * the rank one constraints on $\{\boldsymbol{W}_k\}_{k=1}^{K}$ are relaxed to PSD constraints
  - * a linear weighting $0 < \alpha < 1$ is introduced on the AN cov. matrix $\boldsymbol{W}_{K+1}$
- our study reveals that the above problem solves the non-cvx problem (2) **almost exactly**!

Main Result

$$\underset{\{\boldsymbol{W}_k \in \mathbb{H}^{N_t}\}_{k=1}^K}{\text{minimize}} \quad \sum_{k=1}^K \text{tr}(\boldsymbol{W}_k) + \alpha\, \text{tr}(\boldsymbol{W}_{K+1}) \qquad (\mathcal{R})$$

$$\text{subject to} \quad \text{constraints (C, J, S)}$$

$$\boldsymbol{W}_1, \cdots, \boldsymbol{W}_{K+1} \succeq \boldsymbol{0}$$

- **Theorem.** Suppose that the above problem and its dual have optimal solutions, and it attains zero duality gap. If the coefficient $\alpha \in (0, 1)$, then every optimum to $(\mathcal{R})$ satisfies

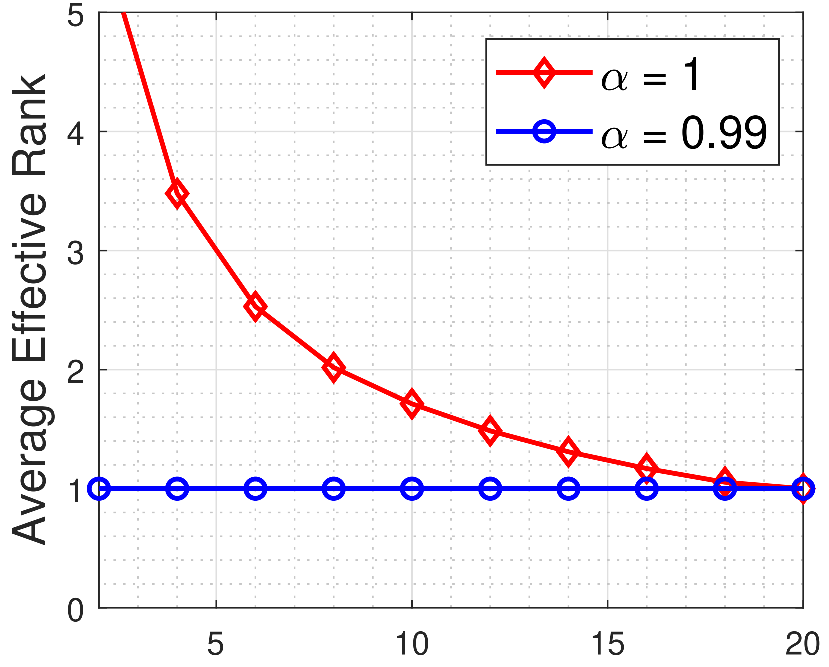
  $$\text{rank}(\boldsymbol{W}_k^\star) \leq 1, \quad k = 1, \ldots, K.$$

  In other words, our SDR is *tight*.

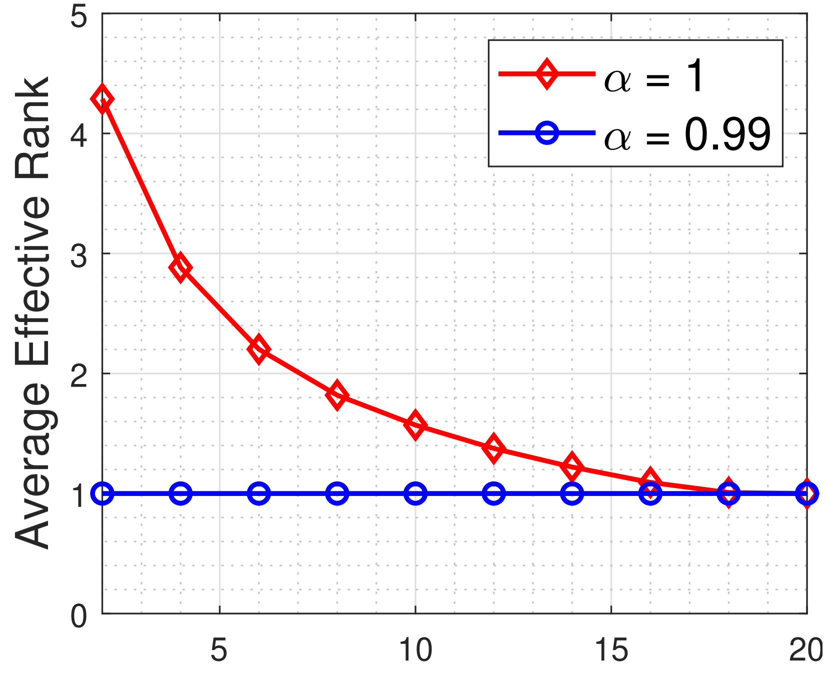
- **Idea of the proof:** check the KKT conditions of $(\mathcal{R})$, and the skeleton mainly follows from the Proof of Theorem 1 in **[LM16]**; also we exploit the SINR constraint's structure

- **Implication:** despite the original formulation (2) is very challenging to solve, our formulation $(\mathcal{R})$ is capable of solving (2) *almost exactly*, i.e. when α is *very close to one*, and the solution to $(\mathcal{R})$ must admit rank one

Experiment: Rank One Guarantee



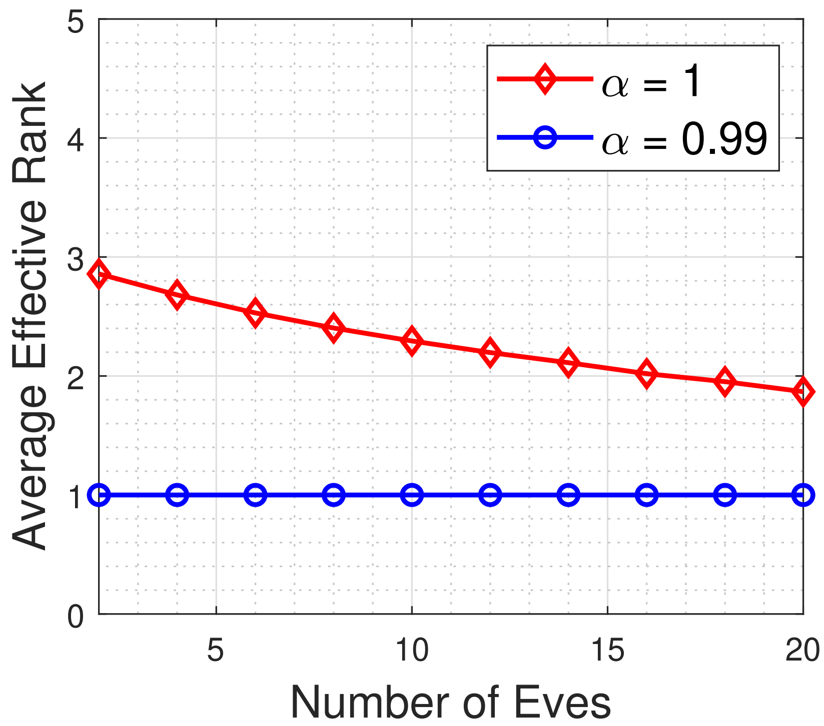
(a) When there are 6 Eves



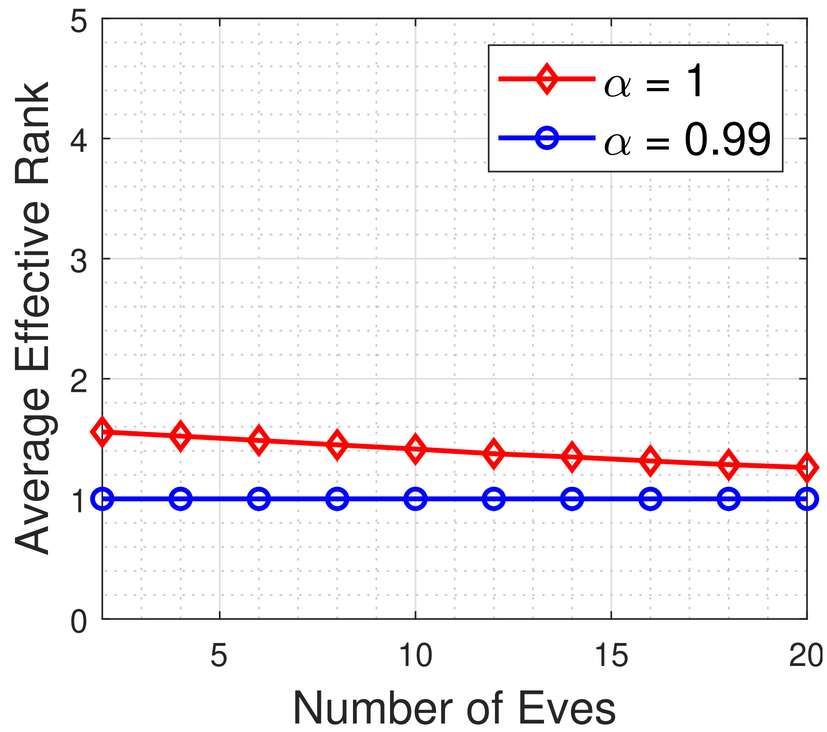
(b) When there are 12 Eves

Average effective rank of the solution to $(\mathcal{R})$ under different number of Bobs and Eves. $N_t = 20$, $N_r = 30$, block length $T = 800$, $\sigma^2 = 0\text{dB}$; performance bounds are $\gamma = 10\text{dB}$, $\beta = \rho = -10\text{dB}$

Experiment: Rank One Guarantee



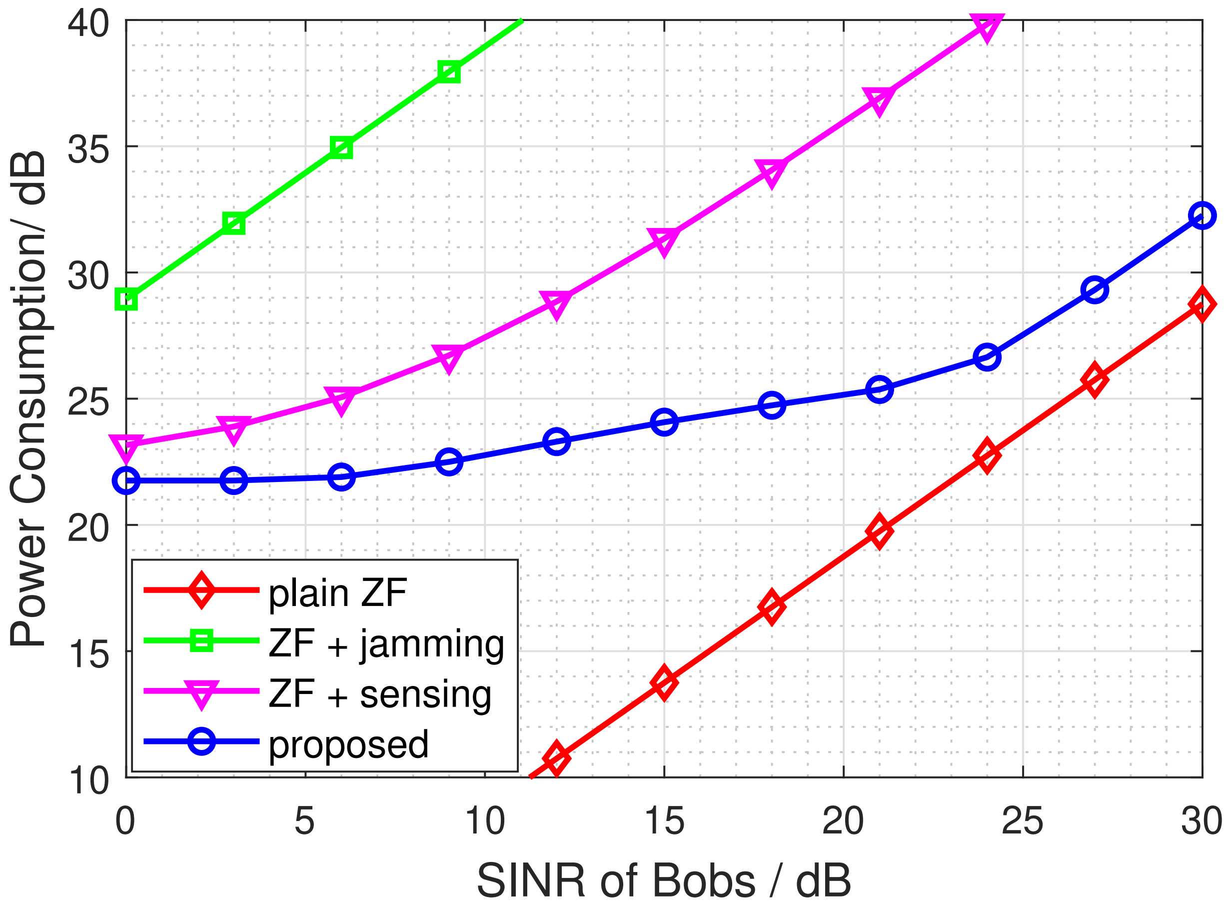
(c) When there are 6 Bobs



(d) When there are 12 Bobs

Average effective rank of the solution to $(\mathcal{R})$ under different number of Bobs and Eves. $N_t = 20$, $N_r = 30$, block length $T = 800$, $\sigma^2 = 0\text{dB}$; performance bounds are $\gamma = 10\text{dB}$, $\beta = \rho = -10\text{dB}$

Experiment: Power Consumption Versus Bobs' SINR γ



Average power consumption against the SINR requirement of Bobs γ. $N_t = 20$, $N_r = 30$, block length $T = 800$, $J = K = 12$, $\beta = \rho = -15\mathrm{dB}$; proposed method $(\mathcal{R})$ is run with $\alpha = 0.99$.

Conclusions

- we have reformulated the secure ISAC beamforming problem to achieve a tight SDR
- both theoretical analysis and numerical simulations agree with our argument

That's all. Thank you! Questions?

Key References

[BO01] M. Bengtsson and B. Ottersten, *Optimal and suboptimal transmit beamforming*, Handbook of Antennas in Wireless Communications (2001).

[HP10] Y. Huang and D. P. Palomar, *Rank-constrained separable semidefinite programming with applications to optimal beam-forming*, IEEE Trans. on Sig. Proc. **58** (2010), no. 2, 664–678.

[LLL+22] F. Liu, Y.F. L., A. Li, et al., *Cramér-rao bound optimization for joint radar-communication beamforming*, IEEE Trans. on Sig. Proc. **70** (2022), 240–253.

[LM16] Q. Li and W.K. Ma, *A new low-rank solution result for a semidefinite program problem subclass with applications to transmit beamforming optimization*, 2016 IEEE ICASSP, 2016, pp. 3446–3450.