IEEE GlobalSIP

3rd IEEE Global Conference on Signal & Information Processing

Orlando, Florida, USA December 14-16 2015

IEEE Signal Processing Society

Artificial-Noise Aided Transmit Design for Multi-User MISO Systems with Integrated Services

Weidong Mei, Lingxiang Li, Zhi Chen, Chuan Huang

National Key Lab of Science and Technology on Communications,
University of Electronic Science and Technology of China

Background

- **Traditionally** multicast transmission and confidential transmission are usually independently investigated in the field of physical (PHY) layer signal processing.
- PHY multicasting offers a way to efficiently transmit common messages that all receivers can decode.
- PHY security can overcome the inherent difficulties of cryptographic methods, i.e., the distribution and management of secrecy keys in wireless networks.
- For signal processing techniques, many literatures focus on finding the optimal covariance matrix of the transmitted message subject to a power constraint, either in PHY multicasting or in PHY security.

Background

- A brief review of PHY security (MISOSE, perfect ECSI)

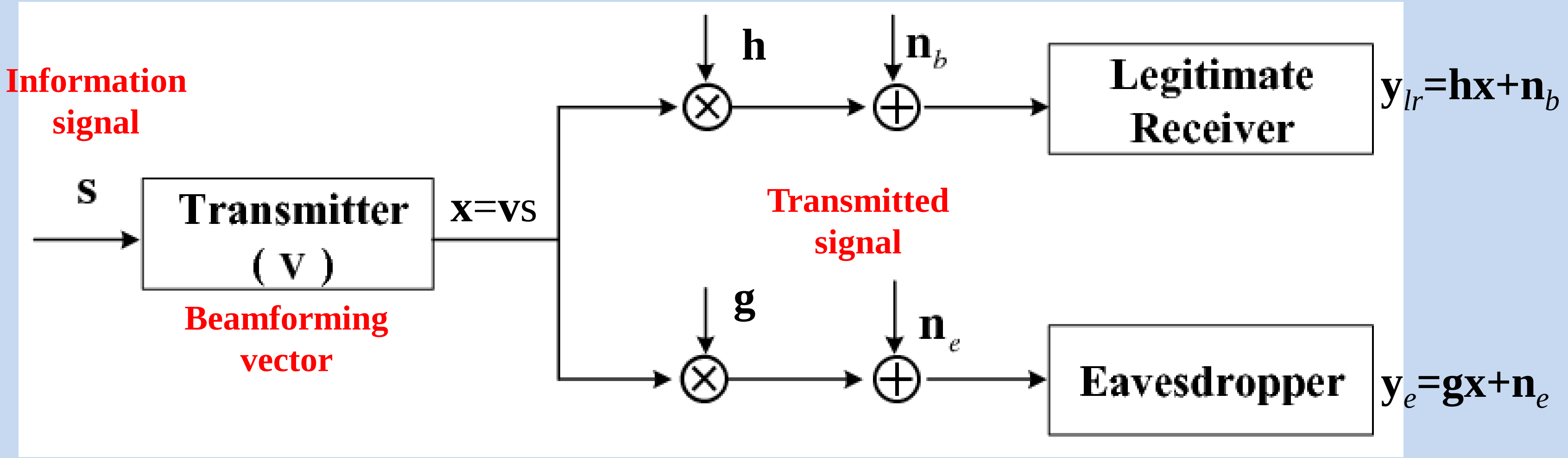


Fig.1. MISO Wiretap System Model

Achievable secrecy rate is given by

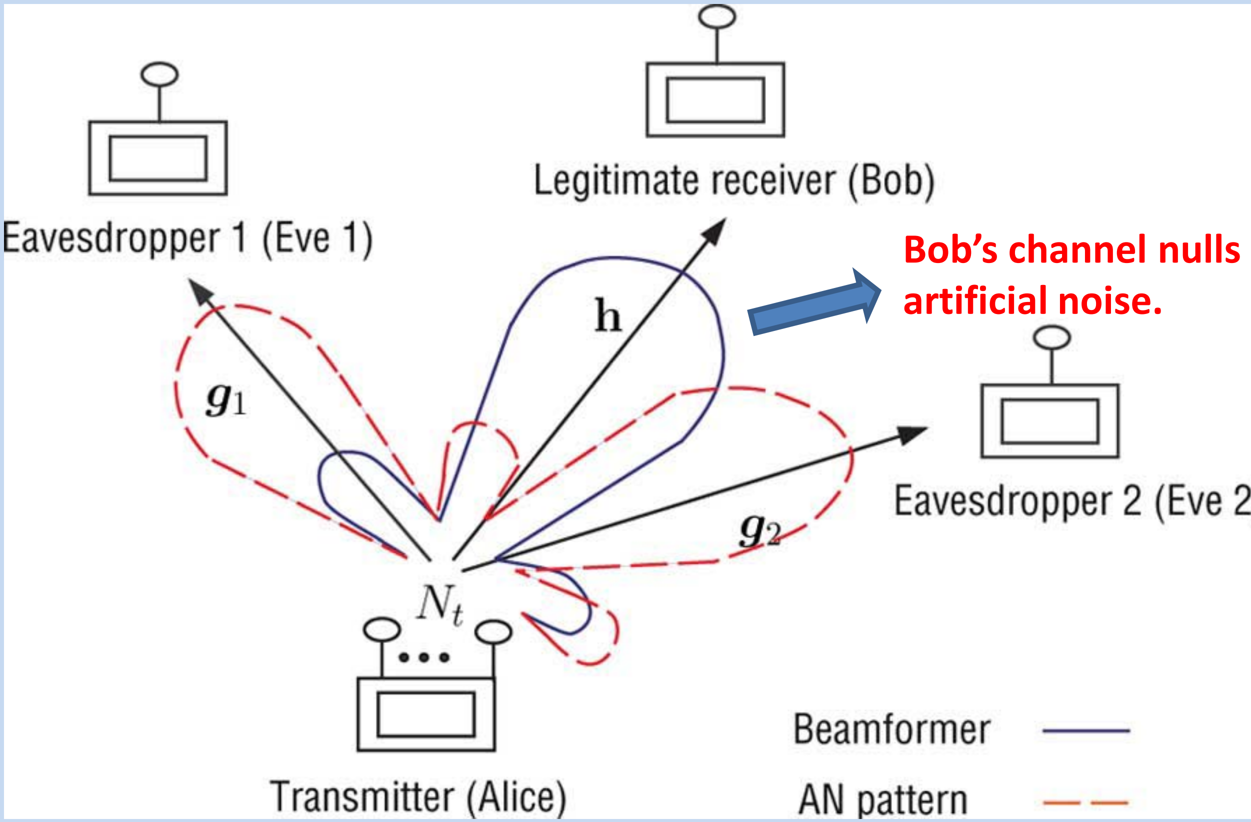
$$R_c = C_b - C_e \qquad \mathbf{Q}_c \triangleq |s|^2 \mathbf{v}\mathbf{v}^H$$

$$C_b = \log\left(1 + \frac{\mathbf{h}\mathbf{Q}_c\mathbf{h}^H}{\sigma_b^2}\right), C_e = \log\left(1 + \frac{\mathbf{g}\mathbf{Q}_c\mathbf{g}^H}{\sigma_e^2}\right)$$

The maximization of C_b admits closed-form expressions.

Background

- A brief review of PHY security (MISOME, AN-aided)



Bob's channel nulls out the artificial noise.

Fig.2. The idea of AN-aided transmit beamforming[1]

[1]W.-C. Liao, T.-H. Chang, W.-K. Ma and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: an optimized artificial-noise-aided approach", *IEEE Trans. Signal Process., vol. 59, no. 3, pp. 1202-1216*, Mar., 2011

Background

- A brief review of PHY multicasting (MU-MISO, perfect CSI)

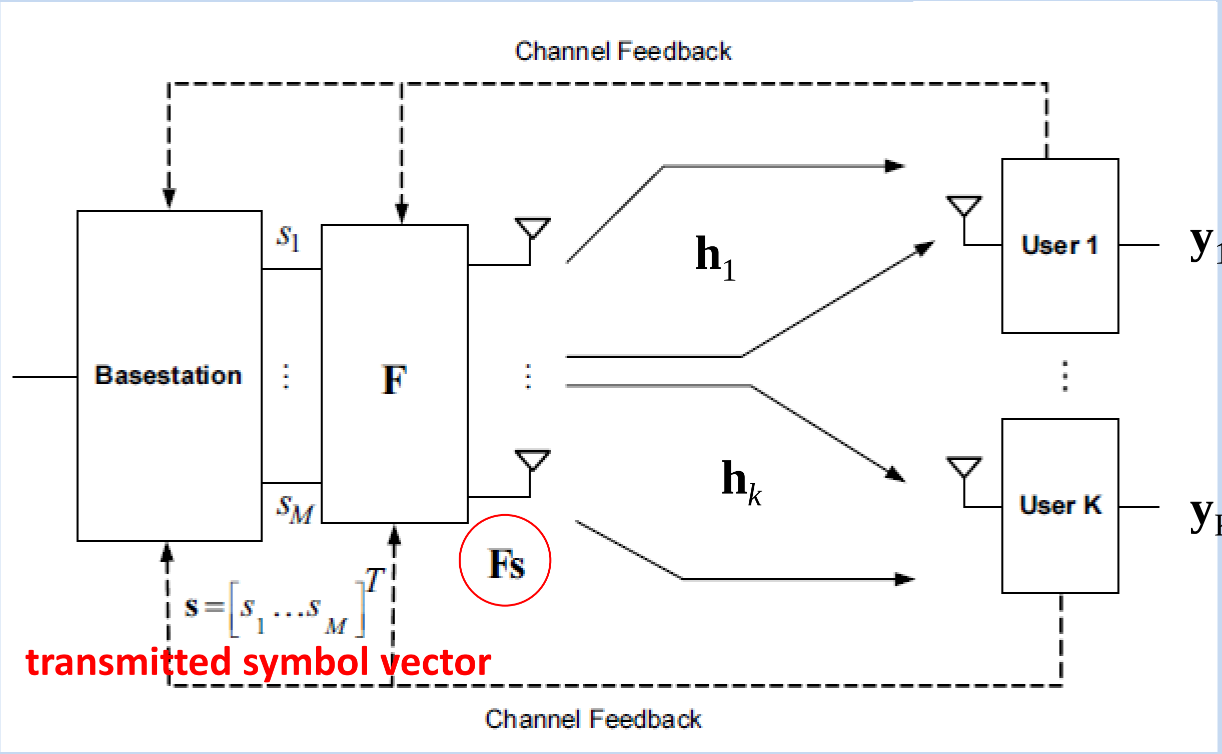


Fig.3. MISO Multicasting System Model[2]

[2]I. H. Kim, D. J. Love, and S. Y. Park, “Optimal and successive approaches to signal design for multiple antenna physical layer multicasting,” *IEEE Trans. Commun.*, vol. 59, no. 8, pp. 2316–2327, 2011.

University of Electronic Science and Technology of China

IEEE GlobalSIP

Background

- A brief review of PHY multicasting

Achievable rate of multicasting system is given by

$$R_m = \min_k \log\left(1 + \frac{\mathbf{h}_k \mathbf{Q}_0 \mathbf{h}_k^H}{\sigma_k^2}\right) \qquad \mathbf{Q}_0 \triangleq \mathbf{F}\mathbf{s}\mathbf{s}^H\mathbf{F}^H$$

The multicast capacity in the presence of CSIT is given by

$$C_{MC}(P) = \max_{\mathbf{Q}_0 \in H^N} \min_{i=1,2,\ldots,K} \log\left(1 + \frac{\mathbf{h}_i^H \mathbf{Q}_0 \mathbf{h}_i}{\sigma_i^2}\right)$$

$$\text{s.t.}\ \mathbf{Q}_0 \succeq \mathbf{0}, \mathrm{Tr}(\mathbf{Q}_0) \le P.$$

This maximization problem can be recast as an SDP problem [3].

[3] S. X. Wu, W.-K. Ma, and A. M.-C. So, “Physical-layer multicasting by stochastic transmit beamforming and Alamouti space-time coding,” IEEE Trans. Signal Process., vol. 61, no. 17, pp. 4230–4245, Sep. 2013.

Background

- **Recently** a heuristic and interesting way is to merge multiple services, e.g., multicast service and confidential service, into one integral service for one-time transmission.
- Service integration in the physical (PHY) layer enables coexisting services to share the same resources, thereby significantly increasing the spectral efficiency.
- Many works focused on PHY service integration from the viewpoint of information theory, i.e., derived capacity results or characterized coding strategies that result in certain rate regions.
- Few works focused on the transmit design to achieve the capacity region, i.e., designing the input covariance matrices of different service information.

Literature	Scenario	Remarks
[Ly-Liu-Liang'10]	With only one confidential message W_1 and one common message W_0	MIMO Gaussian BC, under the matrix power constraint and total power constraint
[Liu-Liu-Poor-Shamai'10]	Two confidential messages W_1 and W_2 and one common message W_0	MIMO Gaussian BC, under the matrix power constraint
[Wyrembelski-Boche'12]	Two-phase communication: two private messages W_1 and W_2, one multicast message W_0, and one confidential message W_3	MIMO Gaussian BBC, under the matrix power constraint and total power constraint

Contributions

- We focus on an AN-aided transmit design and maximize the corresponding achievable secrecy rate region, i.e., finding the optimal input covariance matrice for confidential message, multicast message and AN.
- To this end, we specify variant target QoMS, and meanwhile maximize the corresponding achievable secrecy rates with the aided AN.
- We prove the optimality of beamforming by showing the optimal covariance matrix associated with confidential message is of rank one.

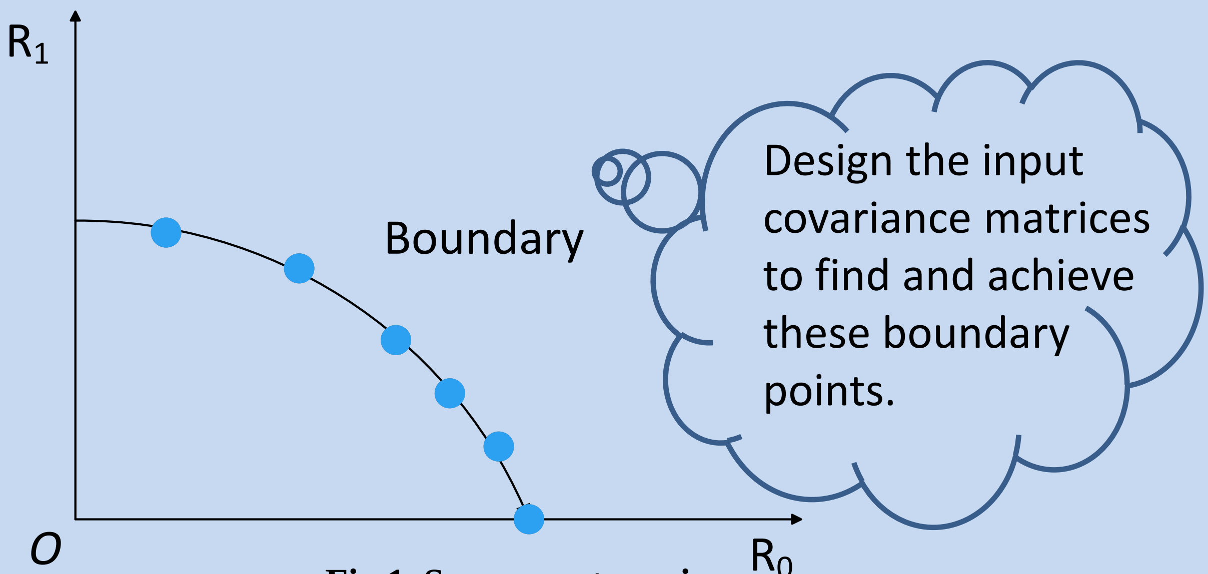


Fig.1. Secrecy rate region

System model

- A multi-antenna transmitter serves K receivers, and each receiver has a single antenna.
- All receivers have ordered the multicast service and receiver 1 further ordered the confidential service.
- The channel state information (CSI) of all receivers is assumed to be available at the transmitter.

MISO multiuser Gaussian broadcast channel

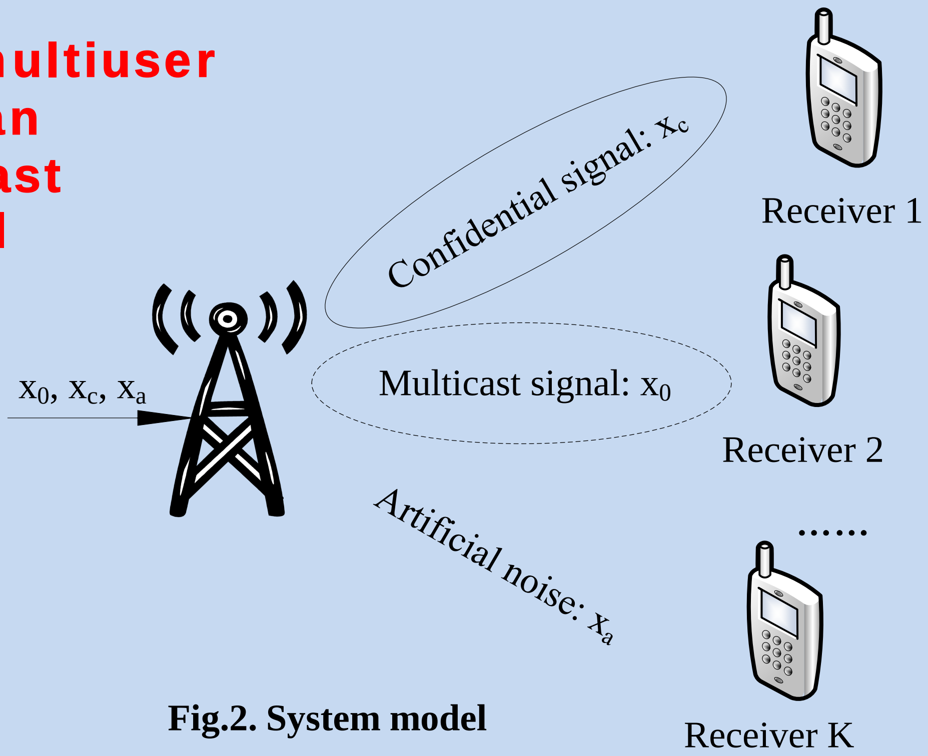


Fig.2. System model

University of Electronic Science and Technology of China

IEEE GlobalSIP

Problem Formulation

- The achievable rate region C_s is given as the set of nonnegative rate pairs (R_0,R_c) satisfying [1]

$$R_0 \le \min_{k\in\mathcal{K}} C_{k,\mathrm{mc}},$$
$$R_c \le C_1 - \max_{k\in\mathcal{K}_e} C_k$$

$$C_{k,mc} = \log\left(1+\frac{\mathbf{h}_k\mathbf{Q}_0\mathbf{h}_k^H}{1+\mathbf{h}_k(\mathbf{Q}_c+\mathbf{Q}_a)\mathbf{h}_k^H}\right), k\in\mathcal{K}$$

$$C_1 = \log\left(1+\frac{\mathbf{h}_1\mathbf{Q}_c\mathbf{h}_1^H}{1+\mathbf{h}_1\mathbf{Q}_a\mathbf{h}_1^H}\right), C_k = \log\left(1+\frac{\mathbf{h}_k\mathbf{Q}_c\mathbf{h}_k^H}{1+\mathbf{h}_k\mathbf{Q}_a\mathbf{h}_k^H}\right), k\in\mathcal{K}_e.$$

Q_c (resp. Q_0, Q_a) represents the covariance matrix of confidential message (resp. multicast message, AN); *K* (resp. K_e) denotes the indices of all receivers (resp. unauthorized receivers).

Problem Formulation

The problem of interest in this paper is to determine the optimal precoding matrix Q_c, Q_0 and Q_a in the following optimization problem

$$\max_{\mathbf{Q}_0,\mathbf{Q}_a,\mathbf{Q}_c} \log \frac{1+(1+\mathbf{h}_1\mathbf{Q}_a\mathbf{h}_1^H)^{-1}\mathbf{h}_1\mathbf{Q}_c\mathbf{h}_1^H}{\max_{k\in\mathcal{K}_e} 1+(1+\mathbf{h}_k\mathbf{Q}_a\mathbf{h}_k^H)^{-1}\mathbf{h}_k\mathbf{Q}_c\mathbf{h}_k^H}$$

C_1

$\max_{k\in\mathcal{K}_e} C_k$

$$s.t. \quad \min_{k\in\mathcal{K}} \left\{ \log \frac{1+\mathbf{h}_k(\mathbf{Q}_c+\mathbf{Q}_a+\mathbf{Q}_0)\mathbf{h}_k^H}{1+\mathbf{h}_k(\mathbf{Q}_c+\mathbf{Q}_a)\mathbf{h}_k^H} \right\} \geq \tau, \qquad (1)$$

Total power constraint

$$\mathrm{Tr}(\mathbf{Q}_0+\mathbf{Q}_a+\mathbf{Q}_c) \leq P,$$

$$\mathbf{Q}_0 \succeq \mathbf{0}, \mathbf{Q}_a \succeq \mathbf{0}, \mathbf{Q}_c \succeq \mathbf{0},$$

$\min_{k\in\mathcal{K}} C_{k,\mathrm{mc}}$

Demand for QoMS

Remarks: This optimization problem also provides us a way to determine the boundary points of the secrecy rate region.

Problem Formulation

Further simplify (1) by introducing a slack variable α, then we obtain

$$g^*(\tau) = \max_{\mathbf{Q}_0,\mathbf{Q}_a,\mathbf{Q}_c,\alpha} \log\left(\frac{1+\mathbf{h}_1(\mathbf{Q}_c+\mathbf{Q}_a)\mathbf{h}_1^H}{\alpha(1+\mathbf{h}_1\mathbf{Q}_a\mathbf{h}_1^H)}\right)$$

Nonconvex objective function!!

$$\begin{aligned}
s.t.\ & \boxed{(\alpha-1)(1+\mathbf{h}_k\mathbf{Q}_a\mathbf{h}_k^H)-\mathbf{h}_k\mathbf{Q}_c\mathbf{h}_k^H \geq 0, \forall k \in \mathcal{K}_e,} \\
& \mathbf{h}_k\mathbf{Q}_0\mathbf{h}_k^H - \tau'\mathbf{h}_k\mathbf{Q}_a\mathbf{h}_k^H - \tau'\mathbf{h}_k\mathbf{Q}_c\mathbf{h}_k^H - \tau' \geq 0, \forall k \in \mathcal{K}, \\
& Tr(\mathbf{Q}_0+\mathbf{Q}_a+\mathbf{Q}_c) \leq P, \\
& \mathbf{Q}_0 \succeq \mathbf{0}, \mathbf{Q}_a \succeq \mathbf{0}, \mathbf{Q}_c \succeq \mathbf{0},
\end{aligned} \quad (2)$$

Nonconvex constraint!!

$$\tau' \triangleq 2^\tau - 1$$

To deal with the non-convexity in (2), next we develop a two-stage reformulation of (2).

A Two-stage Reformulation of (2)

Outer problem w.r.t α

$$\gamma^*(\tau') = \max_{\alpha \geq 1} \eta(\alpha, \tau') \qquad (3)$$

α's upper bound can be determined by $\alpha \leq 1 + P\|\mathbf{h}_1\|^2$

One-dimensional search, e.g., the golden section algorithm, can handle the outer problem.

Inner problem w.r.t $\mathbf{Q}_0, \mathbf{Q}_c, \mathbf{Q}_a$

Bisection method and CVX solver can collectively solve the inner problem.

$$\eta(\alpha, \tau') = \max_{\mathbf{Q}_0, \mathbf{Q}_a, \mathbf{Q}_c} \frac{1 + \mathbf{h}_1(\mathbf{Q}_c + \mathbf{Q}_a)\mathbf{h}_1^H}{\alpha(1 + \mathbf{h}_1\mathbf{Q}_a\mathbf{h}_1^H)}$$

Quasiconvex optimization problem [Boyd'09]

$$\begin{aligned} s.t. \quad & (\alpha - 1)(1 + \mathbf{h}_k\mathbf{Q}_a\mathbf{h}_k^H) - \mathbf{h}_k\mathbf{Q}_c\mathbf{h}_k^H \geq 0, \forall k \in \mathcal{K}_e, \\ & \mathbf{h}_k\mathbf{Q}_0\mathbf{h}_k^H - \tau'\mathbf{h}_k\mathbf{Q}_a\mathbf{h}_k^H - \tau'\mathbf{h}_k\mathbf{Q}_c\mathbf{h}_k^H - \tau' \geq 0, \forall k \in \mathcal{K}, \\ & \mathrm{Tr}(\mathbf{Q}_0 + \mathbf{Q}_a + \mathbf{Q}_c) \leq P, \\ & \mathbf{Q}_0 \succeq \mathbf{0}, \mathbf{Q}_a \succeq \mathbf{0}, \mathbf{Q}_c \succeq \mathbf{0}. \end{aligned} \qquad (4)$$

Affine constraint

Charnes-Cooper transformation-based reformulation of (4)

By applying the Charnes-Cooper transformation

$$\mathbf{Q}_c = \mathbf{Z}/\xi, \mathbf{Q}_a = \mathbf{\Gamma}/\xi, \mathbf{Q}_0 = \mathbf{\Phi}/\xi,$$

We rewrite (4) as

$$\begin{aligned}
\eta(\alpha,\tau') = \max_{\mathbf{Q},\mathbf{\Gamma},\mathbf{\Phi},\xi} \ & \xi + \mathbf{h}_1(\mathbf{Z}+\mathbf{\Gamma})\mathbf{h}_1^H \\
s.t. \quad & \xi + \mathbf{h}_1\mathbf{\Gamma}\mathbf{h}_1^H = \alpha^{-1}, \\
& (\alpha-1)(\xi + \mathbf{h}_k\mathbf{\Gamma}\mathbf{h}_k^H) \geq \mathbf{h}_k\mathbf{Z}\mathbf{h}_k^H, \forall k \in \mathcal{K}_e, \\
& \mathbf{h}_k\mathbf{\Phi}\mathbf{h}_k^H - \tau'\mathbf{h}_k\mathbf{\Gamma}\mathbf{h}_k^H - \tau'\mathbf{h}_k\mathbf{Z}\mathbf{h}_k^H - \xi\tau' \geq 0, \forall k \in \mathcal{K}, \\
& Tr(\mathbf{\Phi}+\mathbf{\Gamma}+\mathbf{Z}) \leq P\xi, \\
& \mathbf{\Phi} \succeq \mathbf{0}, \mathbf{\Gamma} \succeq \mathbf{0}, \mathbf{Z} \succeq \mathbf{0},
\end{aligned} \qquad (5)$$

Convex optimization problem!!

University of Electronic Science and Technology of China

IEEE GlobalSIP

The optimality of transmit beamforming

Proposition 1: The optimal transmit covariance matrix of the confidential message, $\mathbf{Q}_c^*$, has a rank equal to 1.

Proof: It suffices to prove the optimal $\mathbf{Q}_c$ to (4) is of rank one, for any given α.

$$\eta(\alpha,\tau') = \max_{\mathbf{Q}_0,\mathbf{Q}_a,\mathbf{Q}_c} \frac{1+\mathbf{h}_1(\mathbf{Q}_c+\mathbf{Q}_a)\mathbf{h}_1^H}{\alpha(1+\mathbf{h}_1\mathbf{Q}_a\mathbf{h}_1^H)}$$

Recall (4)

$$\begin{aligned} s.t. \quad & (\alpha-1)(1+\mathbf{h}_k\mathbf{Q}_a\mathbf{h}_k^H)-\mathbf{h}_k\mathbf{Q}_c\mathbf{h}_k^H \geq 0, \forall k \in \mathcal{K}_e, \\ & \mathbf{h}_k\mathbf{Q}_0\mathbf{h}_k^H - \tau'\mathbf{h}_k\mathbf{Q}_a\mathbf{h}_k^H - \tau'\mathbf{h}_k\mathbf{Q}_c\mathbf{h}_k^H - \tau' \geq 0, \forall k \in \mathcal{K}, \\ & \mathrm{Tr}(\mathbf{Q}_0+\mathbf{Q}_a+\mathbf{Q}_c) \leq P, \\ & \mathbf{Q}_0 \succeq \mathbf{0}, \mathbf{Q}_a \succeq \mathbf{0}, \mathbf{Q}_c \succeq \mathbf{0}. \end{aligned}$$

Optimal solution $\longrightarrow$ $\left(\bar{\mathbf{Q}}_0, \bar{\mathbf{Q}}_c, \bar{\mathbf{Q}}_a\right)$

Optimal objective value $\longrightarrow$ $\bar{R}_\alpha$

The optimality of transmit beamforming

Step 1: We prove (4) has identical solutions to a power minimization problem (6).

$$\min_{\mathbf{Q}_0,\mathbf{Q}_a,\mathbf{Q}_c} \; Tr(\mathbf{Q}_0+\mathbf{Q}_a+\mathbf{Q}_c)$$

$$s.t. \quad \log\left(\frac{1+\mathbf{h}_1(\mathbf{Q}_c+\mathbf{Q}_a)\mathbf{h}_1^H}{\alpha(1+\mathbf{h}_1\mathbf{Q}_a\mathbf{h}_1^H)}\right) \geq \bar{R}_\alpha,$$

The optimal value of (4)

$$(\alpha-1)(1+\mathbf{h}_k\mathbf{Q}_a\mathbf{h}_k^H)-\mathbf{h}_k\mathbf{Q}_c\mathbf{h}_k^H \geq 0, \forall k \in \mathcal{K}_e,$$

$$\mathbf{h}_k\mathbf{Q}_0\mathbf{h}_k^H-\tau'\mathbf{h}_k\mathbf{Q}_a\mathbf{h}_k^H-\tau'\mathbf{h}_k\mathbf{Q}_c\mathbf{h}_k^H-\tau' \geq 0, \forall k \in \mathcal{K},$$

$$\mathbf{Q}_0 \succeq \mathbf{0}, \mathbf{Q}_a \succeq \mathbf{0}, \mathbf{Q}_c \succeq \mathbf{0}. \tag{6}$$

Same constraints as (4)

Optimal solution

$$\left(\tilde{\mathbf{Q}}_0, \tilde{\mathbf{Q}}_c, \tilde{\mathbf{Q}}_a\right)$$

The optimality of transmit beamforming

Some quick implications

The definition of $\bar{R}_\alpha$ ⟹ $$\log\left(\frac{1+\mathbf{h}_1(\bar{\mathbf{Q}}_c+\bar{\mathbf{Q}}_a)\mathbf{h}_1^H}{\alpha(1+\mathbf{h}_1\bar{\mathbf{Q}}_a\mathbf{h}_1^H)}\right)=\bar{R}_\alpha, \quad (7)$$

⟹ The feasibility of $\left(\bar{\mathbf{Q}}_0,\bar{\mathbf{Q}}_c,\bar{\mathbf{Q}}_a\right)$ to (6)

⟹ $$\mathrm{Tr}(\tilde{\mathbf{Q}}_0+\tilde{\mathbf{Q}}_a+\tilde{\mathbf{Q}}_c)\le\mathrm{Tr}(\bar{\mathbf{Q}}_0+\bar{\mathbf{Q}}_a+\bar{\mathbf{Q}}_c)\le P,$$

⟹ The feasibility of $\left(\tilde{\mathbf{Q}}_0,\tilde{\mathbf{Q}}_c,\tilde{\mathbf{Q}}_a\right)$ to (6)

⟹ $$\log\left(\frac{1+\mathbf{h}_1(\tilde{\mathbf{Q}}_c+\tilde{\mathbf{Q}}_a)\mathbf{h}_1^H}{\alpha(1+\mathbf{h}_1\tilde{\mathbf{Q}}_a\mathbf{h}_1^H)}\right)\le\bar{R}_\alpha,$$ **From (6)** $$\log\left(\frac{1+\mathbf{h}_1(\tilde{\mathbf{Q}}_c+\tilde{\mathbf{Q}}_a)\mathbf{h}_1^H}{\alpha(1+\mathbf{h}_1\tilde{\mathbf{Q}}_a\mathbf{h}_1^H)}\right)\ge\bar{R}_\alpha,$$

⟹ $$\log\left(\frac{1+\mathbf{h}_1(\tilde{\mathbf{Q}}_c+\tilde{\mathbf{Q}}_a)\mathbf{h}_1^H}{\alpha(1+\mathbf{h}_1\tilde{\mathbf{Q}}_a\mathbf{h}_1^H)}\right)=\bar{R}_\alpha,$$

⟹ The optimality of $\left(\tilde{\mathbf{Q}}_0,\tilde{\mathbf{Q}}_c,\tilde{\mathbf{Q}}_a\right)$ to (4)

The optimality of transmit beamforming

The Lagrangian associated with (7)

$$\log\left(\frac{1+\mathbf{h}_1(\mathbf{Q}_c+\mathbf{Q}_a)\mathbf{h}_1^H}{\alpha(1+\mathbf{h}_1\mathbf{Q}_a\mathbf{h}_1^H)}\right)\geq \bar{R}_\alpha \qquad \mu \triangleq 1-\alpha 2^{\bar{R}_\alpha}$$

$$\begin{aligned} L(\mathbf{Q}_0,\mathbf{Q}_a,\mathbf{Q}_c,\lambda,\boldsymbol{\eta},\boldsymbol{\sigma},\mathbf{A},\mathbf{B},\mathbf{C}) = & Tr(\mathbf{Q}_0+\mathbf{Q}_a+\mathbf{Q}_c)-\lambda[\mathbf{h}_1(\mathbf{Q}_c+\mu\mathbf{Q}_a)\mathbf{h}_1^H+\mu]- \\ & \sum_{k=2}^{K}\eta_k[(\alpha-1)(1+\mathbf{h}_k\mathbf{Q}_a\mathbf{h}_k^H)-\mathbf{h}_k\mathbf{Q}_c\mathbf{h}_k^H]- \\ & \sum_{k=1}^{K}\sigma_k[\mathbf{h}_k\mathbf{Q}_0\mathbf{h}_k^H-\tau'\mathbf{h}_k\mathbf{Q}_a\mathbf{h}_k^H-\tau'\mathbf{h}_k\mathbf{Q}_c\mathbf{h}_k^H-\tau']- \\ & Tr(\mathbf{A}\mathbf{Q}_a)-Tr(\mathbf{B}\mathbf{Q}_0)-Tr(\mathbf{C}\mathbf{Q}_c), \end{aligned} \qquad (8)$$

$$\begin{aligned} & \lambda>0, \\ & \boldsymbol{\eta}\triangleq[\eta_2,\eta_3,\ldots,\eta_K]\succeq\mathbf{0}, \\ & \boldsymbol{\sigma}\triangleq[\sigma_1,\sigma_2,\ldots,\sigma_K]\succeq\mathbf{0}, \\ & \mathbf{A}\succeq\mathbf{0},\mathbf{B}\succeq\mathbf{0},\mathbf{C}\succeq\mathbf{0} \end{aligned}$$

The optimality of transmit beamforming

Karush-Kuhn-Tucker (KKT) conditions of (6)

$$\frac{\partial L}{\partial \tilde{\mathbf{Q}}_c} = \mathbf{I} - \lambda \mathbf{h}_1^H \mathbf{h}_1 + \sum_{k=2}^{K} \eta_k \mathbf{h}_k^H \mathbf{h}_k + \tau' \sum_{k=1}^{K} \sigma_k \mathbf{h}_k^H \mathbf{h}_k - \mathbf{C} = \mathbf{0}, \quad (9.1)$$

$$\mathbf{C}\tilde{\mathbf{Q}}_c = \mathbf{0}, \quad (9.2)$$

$$\tilde{\mathbf{Q}}_c \succeq \mathbf{0}, \quad (9.3)$$

$$\eta_k \geq 0, \forall k \in \mathcal{K}_e, \quad (9.4)$$

$$\sigma_k \geq 0, \forall k \in \mathcal{K}. \quad (9.5)$$

- (9.1), (9.4) and (9.5) are actually the constraints of the dual problem of (6)
- (9.3) is actually the inequality constraint of (6)
- (9.2) is the complementary slackness

The optimality of transmit beamforming

Postmultiplying (9.1) by $\tilde{\mathbf{Q}}_c$ and making use of (9.2) yield

$$(\mathbf{I} + \sum_{k=2}^{K} \eta_k \mathbf{h}_k^H \mathbf{h}_k + \tau' \sum_{k=1}^{K} \sigma_k \mathbf{h}_k^H \mathbf{h}_k)\tilde{\mathbf{Q}}_c = \lambda \mathbf{h}_1^H \mathbf{h}_1 \tilde{\mathbf{Q}}_c, \qquad (10)$$

(9.3) and (9.4) imply

$$\mathbf{I} + \sum_{k=2}^{K} \eta_k \mathbf{h}_k^H \mathbf{h}_k + \tau' \sum_{k=1}^{K} \sigma_k \mathbf{h}_k^H \mathbf{h}_k \succ \mathbf{0}$$

$$\Longrightarrow \quad \begin{aligned} &\operatorname{rank}\left((\mathbf{I} + \sum_{k=2}^{K} \eta_k \mathbf{h}_k^H \mathbf{h}_k + \tau' \sum_{k=1}^{K} \sigma_k \mathbf{h}_k^H \mathbf{h}_k)\tilde{\mathbf{Q}}_c \right) \\ &= \operatorname{rank}(\tilde{\mathbf{Q}}_c) = \operatorname{rank}(\lambda \mathbf{h}_1^H \mathbf{h}_1 \tilde{\mathbf{Q}}_c) \le 1, \end{aligned} \qquad (11)$$

Eliminating the trivial solution, we have completed our proof.

University of Electronic Science and Technology of China

IEEE GlobalSIP

The optimality of transmit beamforming

How about the multicast message and AN?

***Proposition 1*: If there only exists a single unauthorized receiver, then**

$$\mathrm{rank}(\mathbf{Q}_0^*) = 1, \mathrm{rank}(\mathbf{Q}_a^*) \le 1.$$

***Proof*: The power minimization problem (6) is a solvable separable SDP problem.**

A general form of separable SDP problem:

$$\begin{aligned} \min_{\mathbf{X}_1, \mathbf{X}_2, \ldots \mathbf{X}_L} & \sum\nolimits_{l=1}^{L} \mathrm{Tr}(\mathbf{C}_l \mathbf{X}_l) \\ s.t \quad & \sum\nolimits_{l=1}^{L} \mathrm{Tr}(\mathbf{A}_{ml} \mathbf{X}_l) \trianglerighteq_m b_m, m = 1, 2, \ldots, M \\ & \mathbf{X}_l \succeq \mathbf{0}, l = 1, 2, \ldots, L. \end{aligned}$$

- **C_l and A_{ml} are Hermitian matrices (not necessarily positive semidefinite)**
- **b_m is a real number, and $\trianglerighteq_m \in \{\le, \ge, =\}$**
- **X_l, l=1,2,…,L, are Hermitian matrices**
- **It is immediate to verify that (6) is a separable SDP.**

The optimality of transmit beamforming

For a solvable SDP problem, the following inequality holds. [Theorem 3.2,5]

$$\operatorname{rank}^2(\mathbf{Q}_0^*)+\operatorname{rank}^2(\mathbf{Q}_a^*)+\operatorname{rank}^2(\mathbf{Q}_c^*) \le M,$$

M **denotes the number of linear equality and inequality in the optimization problem, which is 2*K* in (6).**

When *K* = 2, incorporating $\operatorname{rank}(\mathbf{Q}_c^*) = 1$ **yields**

$$\operatorname{rank}(\mathbf{Q}_0^*) \le 1, \operatorname{rank}(\mathbf{Q}_a^*) \le 1$$

[5] Y. Huang and D. Palomar, "Rank-constrained separable semidefinite programming with applications to optimal beamforming," IEEE Trans. Signal Process., vol. 58, no. 2, pp. 664–678, Sep. 2010.

Numerical Results

Some observations from Fig.2

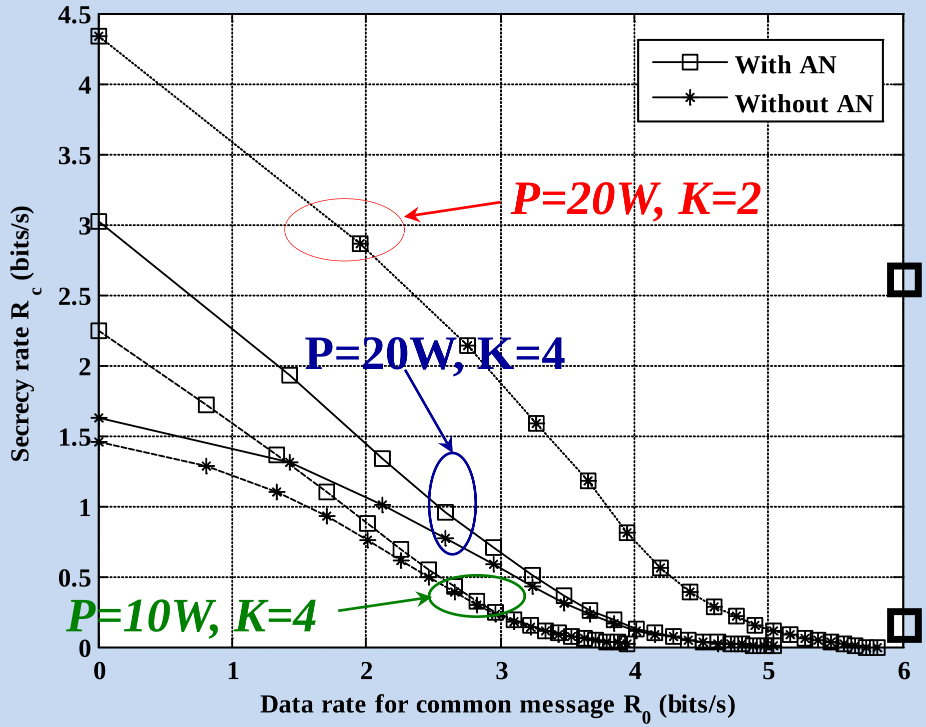


Fig.2. Secrecy rate regions with and without AN

- When *P*=20W, *K*=4
  - Secrecy rates with AN are mostly higher than those without AN.
  - With the increasing demand for QoMS, the two curves tend to be coincident.
- When *P*=10W, *K*=4
  - The gap between these two strategies dramatically reduced.
  - Possible reason: In order to guarantee the QoMS, AN must decrease to reduce the interference at all receivers
- When *P*=20W, *K*=2
  - AN does not offer any secrecy gains.
  - Reason: The unauthorized receivers pose less security threat to the system.