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

\[ R_c = C_b - C_e \]

\[ Q_c \triangleq |s|^2 vv^H \]

\[ C_b = \log \left( 1 + \frac{hQ_c h^H}{\sigma_b^2} \right), \quad C_e = \log \left( 1 + \frac{gQ_e g^H}{\sigma_e^2} \right) \]

The maximization of \( C_b \) admits closed-form expressions.
Background

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

![Diagram of AN-aided transmit beamforming](image)

Bob’s channel nulls out the artificial noise.

Fig.2. The idea of AN-aided transmit beamforming

[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)

![MISO Multicasting System Model](image)

\[ y_1 = h_1 F s + n_1 \]
\[ y_K = h_K F s + n_K \]

Fig. 3. MISO Multicasting System Model\(^\text{[2]}\)

[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.
Background

- A brief review of PHY multicasting

Achievable rate of multicasting system is given by

\[ R_m = \min_k \log \left( 1 + \frac{h_k Q_0 h_k^H}{\sigma_k^2} \right) \]

The multicast capacity in the presence of CSIT is given by

\[ C_{MC}(P) = \max_{Q_0 \in H^N} \min_{i=1,2,...,K} \log(1 + \frac{h_i^H Q_0 h_i}{\sigma_i^2}) \]

s.t. \( Q_0 \preceq 0, \text{Tr}(Q_0) \leq P \).

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 matrices 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.

Design the input covariance matrices to find and achieve these boundary points.

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
Problem Formulation

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

\[
R_0 \leq \min_{k \in \mathcal{K}} C_{k,mc},
\]

\[
R_c \leq C_1 - \max_{k \in \mathcal{K}_e} C_k
\]

\[
C_{k,mc} = \log \left( 1 + \frac{h_k Q_0 h_k^H}{1 + h_k (Q_c + Q_a) h_k^H} \right), k \in \mathcal{K}
\]

\[
C_1 = \log \left( 1 + \frac{h_1 Q_c h_1^H}{1 + h_1 Q_a h_1^H} \right), C_k = \log \left( 1 + \frac{h_k Q_c h_k^H}{1 + h_k Q_a h_k^H} \right), k \in \mathcal{K}_e.
\]

$Q_c$ (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).
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

\[
\begin{align*}
\max_{Q_0, Q_a, Q_c} & \quad \log \frac{1 + (1 + h_1 Q_a h_1^H)^{-1} h_1 Q_c h_1^H}{\max_{k \in \mathcal{K}_c} \left( 1 + (1 + h_k Q_a h_k^H)^{-1} h_k Q_c h_k^H \right)} \\
\text{s.t.} & \quad \min_{k \in \mathcal{K}} \left\{ \log \frac{1 + h_k (Q_c + Q_a + Q_0) h_k^H}{1 + h_k (Q_c + Q_a) h_k^H} \right\} \geq \tau, \\
& \quad \text{Total power constraint} \\
& \quad \text{Demand for QoMS}
\end{align*}
\]

\[
\begin{align*}
& \quad \text{Tr}(Q_0 + Q_a + Q_c) \leq P, \\
& \quad Q_0 \succeq 0, Q_a \succeq 0, Q_c \succeq 0,
\end{align*}
\]

Remarks: This optimization problem also provides us a way to determine the boundary points of the secrecy rate region.
Further simplify (1) by introducing a slack variable $\alpha$, then we obtain

$$g^*(\tau) = \max_{Q_0, Q_a, Q_c, \alpha} \log \left( \frac{1 + h_1(Q_c + Q_a)h_1^H}{\alpha(1 + h_1 Q_a h_1^H)} \right)$$

Nonconvex objective function!!

s.t.  

$$\nonumber (\alpha - 1)(1 + h_k Q_a h_k^H) - h_k Q_c h_k^H \geq 0, \forall k \in \mathcal{K}_e,$$

Nonconvex constraint!!

$$\nonumber h_k Q_0 h_k^H - \tau' h_k Q_a h_k^H - \tau' h_k Q_c h_k^H - \tau' \geq 0, \forall k \in \mathcal{K},$$

$$\nonumber Tr(Q_0 + Q_a + Q_c) \leq P,$$

$$\nonumber Q_0 \preceq 0, Q_a \preceq 0, Q_c \preceq 0,$$

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

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 $\alpha$

\[ \gamma^*(\tau') = \max_{\alpha \geq 1} \eta(\alpha, \tau') \quad \text{(3)} \]

$\alpha$'s upper bound can be determined by

\[ \alpha \leq 1 + P\left\|h_1\right\|^2 \]

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

Inner problem w.r.t $Q_0, Q_c, Q_a$

\[ \eta(\alpha, \tau') = \max_{Q_0, Q_c, Q_a} \frac{1 + h_1(Q_c + Q_a)h_1^H}{\alpha(1 + h_1Q_a h_1^H)} \]

\[ \text{s.t.} \quad (\alpha - 1)(1 + h_k Q_a h_k^H) - h_k Q_c h_k^H \geq 0, \forall k \in \mathcal{K}_c, \]

\[ h_k Q_0 h_k^H - \tau' h_k Q_a h_k^H - \tau' h_k Q_c h_k^H - \tau' \geq 0, \forall k \in \mathcal{K}, \]

\[ \text{Tr}(Q_0 + Q_a + Q_c) \leq P, \]

\[ Q_0 \succeq 0, Q_a \succeq 0, Q_c \succeq 0. \]

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

Quasiconvex optimization problem [Boyd’09]

Affine constraint

\[ (\alpha - 1)(1 + h_k Q_a h_k^H) - h_k Q_c h_k^H \geq 0, \forall k \in \mathcal{K}_c, \]
Charnes-Cooper transformation-based reformulation of (4)

By applying the Charnes-Cooper transformation

\[ Q_c = Z / \xi, \quad Q_a = \Gamma / \xi, \quad Q_0 = \Phi / \xi, \]

We rewrite (4) as

\[
\eta(\alpha, \tau') = \max_{\xi, \Gamma, \Phi, \xi} \xi + h_1(Z + \Gamma)h_1^H
\]

\[ s.t. \quad \xi + h_1\Gamma h_1^H = \alpha^{-1}, \]

\[
(\alpha - 1)(\xi + h_k\Gamma h_k^H) \geq h_k Z h_k^H, \quad \forall k \in \mathcal{K}_e,
\]

\[
h_k \Phi h_k^H - \tau' h_k\Gamma h_k^H - \tau' h_k Z h_k^H - \xi \tau' \geq 0, \quad \forall k \in \mathcal{K},
\]

\[ Tr(\Phi + \Gamma + Z) \leq P \xi, \]

\[ \Phi \succeq 0, \quad \Gamma \succeq 0, \quad Z \succeq 0, \]

Convex optimization problem!!

(5)
The optimality of transmit beamforming

**Proposition 1:** The optimal transmit covariance matrix of the confidential message, $Q_c^*$, has a rank equal to 1.

**Proof:** It suffices to prove the optimal $Q_c$ to (4) is of rank one, for any given $\alpha$.

\[
\eta(\alpha, \tau') = \max_{Q_0, Q_a, Q_c} \frac{1 + h_1(Q_c + Q_a)h_1^H}{\alpha(1 + h_1Q_a h_1^H)}
\]

Recall (4) s.t.
\[
(\alpha - 1)(1 + h_k Q_a h_k^H) - h_k Q_c h_k^H \geq 0, \forall k \in \mathcal{K}_c,
\]
\[
h_k Q_0 h_k^H - \tau' h_k Q_a h_k^H - \tau' h_k Q_c h_k^H - \tau' \geq 0, \forall k \in \mathcal{K},
\]
\[
\text{Tr}(Q_0 + Q_a + Q_c) \leq P,
\]
\[
Q_0 \succeq 0, Q_a \succeq 0, Q_c \succeq 0.
\]

**Optimal solution**
\[
\left( \overline{Q}_0, \overline{Q}_c, \overline{Q}_a \right)
\]

**Optimal objective value**
\[
\overline{R}_\alpha
\]
Step 1: We prove (4) has identical solutions to a power minimization problem (6).

\[
\min_{Q_0, Q_a, Q_c} \quad Tr(Q_0 + Q_a + Q_c)
\]

s.t. \[
\log \left( \frac{1 + h_1(Q_c + Q_a)h_k^H}{\alpha (1 + h_1Q_a h_1^H)} \right) \geq R_\alpha,
\]

Same constraints as (4)

Optimal solution \( (\tilde{Q}_0, \tilde{Q}_c, \tilde{Q}_a) \)

The optimal value of (4)

\[
(\alpha - 1)(1 + h_k Q_a h_k^H) - h_k Q_c h_k^H \geq 0, \forall k \in \mathcal{K}_e,
\]

\[
h_k Q_0 h_k^H - \tau' h_k Q_a h_k^H - \tau' h_k Q_c h_k^H - \tau' \geq 0, \forall k \in \mathcal{K},
\]

\[
Q_0 \succeq 0, Q_a \succeq 0, Q_c \succeq 0.
\]
The optimality of transmit beamforming

Some quick implications

The definition of $\overline{R}_\alpha$

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

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

$$\text{Tr}(\overline{Q}_0 + \overline{Q}_a + \overline{Q}_c) \leq \text{Tr}(\overline{Q}_0 + \overline{Q}_a + \overline{Q}_c) \leq P,$$

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

$$\log\left(\frac{1+\mathbf{h}_1(\overline{Q}_c + \overline{Q}_a)\mathbf{h}_1^H}{\alpha(1+\mathbf{h}_1\overline{Q}_a\mathbf{h}_1^H)}\right) \leq \overline{R}_\alpha, \quad \text{From (6)} \quad \log\left(\frac{1+\mathbf{h}_1(\overline{Q}_c + \overline{Q}_a)\mathbf{h}_1^H}{\alpha(1+\mathbf{h}_1\overline{Q}_a\mathbf{h}_1^H)}\right) \geq \overline{R}_\alpha,$$

The optimality of $\left(\overline{Q}_0, \overline{Q}_c, \overline{Q}_a\right)$ to (4)
The optimality of transmit beamforming

The Lagrangian associated with (7)

\[ L(Q_0, Q_a, Q_c, \lambda, \eta, \sigma, A, B, C) = Tr(Q_0 + Q_a + Q_c) - \lambda [h_1(Q_c + \mu Q_a)h_1^H + \mu] - \]

\[ \sum_{k=2}^{K} \eta_k [(\alpha - 1)(1 + h_k Q_a h_k^H) - h_k Q_c h_k^H] - \]

\[ \sum_{k=1}^{K} \sigma_k [h_k Q_0 h_k^H - \tau' h_k Q_a h_k^H - \tau' h_k Q_c h_k^H - \tau'] - \]

\[ Tr(AQ_a) - Tr(BQ_0) - Tr(CQ_c), \]

\[ \lambda > 0, \]

\[ \eta \triangleq [\eta_2, \eta_3, ..., \eta_K] \succeq 0, \]

\[ \sigma \triangleq [\sigma_1, \sigma_2, ..., \sigma_K] \succeq 0, \]

\[ A \succeq 0, B \succeq 0, C \succeq 0 \]
Karush-Kuhn-Tucker (KKT) conditions of (6)

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

(9.1)

\[C \tilde{Q}_c = 0,
\]

(9.2)

\[\tilde{Q}_c \geq 0,
\]

(9.3)

\[\eta_k \geq 0, \forall k \in \mathcal{K}_e,
\]

(9.4)

\[\sigma_k \geq 0, \forall k \in \mathcal{K}.
\]

(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 $\tilde{Q}_c$ and making use of (9.2) yield

$$(I + \sum_{k=2}^{K} \eta_k h_k^H h_k + \tau' \sum_{k=1}^{K} \sigma_k h_k^H h_k)\tilde{Q}_c = \lambda h_1^H h_1 \tilde{Q}_c,$$  \hspace{1cm} (10)

(9.3) and (9.4) imply

$$I + \sum_{k=2}^{K} \eta_k h_k^H h_k + \tau' \sum_{k=1}^{K} \sigma_k h_k^H h_k > 0$$

$$\text{rank} \left( (I + \sum_{k=2}^{K} \eta_k h_k^H h_k + \tau' \sum_{k=1}^{K} \sigma_k h_k^H h_k)\tilde{Q}_c \right)$$

$$= \text{rank}(\tilde{Q}_c) = \text{rank}(\lambda h_1^H h_1 \tilde{Q}_c) \leq 1,$$  \hspace{1cm} (11)

Eliminating the trivial solution, we have completed our proof.
The optimality of transmit beamforming

How about the multicast message and AN?

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

\[
\text{rank}(Q_0^*) = 1, \quad \text{rank}(Q_a^*) \leq 1.
\]

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

\[
\begin{align*}
\min_{X_1, X_2, \ldots, X_L} & \sum_{l=1}^{L} \text{Tr}(C_l X_l) \\
\text{s.t.} & \sum_{l=1}^{L} \text{Tr}(A_{ml} X_l) \geq_{m} b_m, \quad m = 1, 2, \ldots, M \\
& X_l \succeq 0, \quad l = 1, 2, \ldots, L.
\end{align*}
\]

- \(C_l\) and \(A_{ml}\) are Hermitian matrices (not necessarily positive semidefinite)
- \(b_m\) is a real number, and \(\geq_{m} \in \{\leq, \geq, =\}\)
- \(X_l, \quad l = 1, 2, \ldots, L,\) 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]

\[ \text{rank}^2(Q_0^*) + \text{rank}^2(Q_a^*) + \text{rank}^2(Q_c^*) \leq M, \]

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

When *K* = 2, incorporating \( \text{rank}(Q_c^*) = 1 \) yields

\[ \text{rank}(Q_0^*) \leq 1, \text{rank}(Q_a^*) \leq 1 \]

[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.
Some observations from Fig.2

- 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.

Fig.2. Secrecy rate regions with and without AN