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

University of Electronic Science and Technology of China

Weidong Mei, Zhi Chen, and Chuan Huang

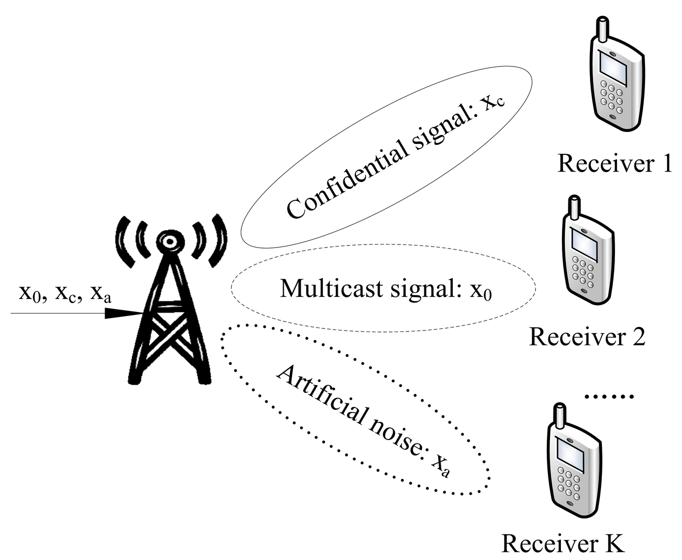
National Key Laboratory of Science and Technology on Communications, No.2006, Xiyuan Ave, Chengdu, China

Background

- Physical-layer (PHY) security and multicasting
  - PHY security can overcome the inherent difficulties of cryptographic methods.
  - PHY-multicasting transmits common messages in a way that all receivers can decode them.
  - Traditionally they are independently investigated.
- PHY service integration
  - merging multiple services into one integral service for one-time transmission.
  - enable coexisting services to share the same resources, thereby significantly increasing the spectral efficiency.
- Motivation
  - Many works focused on PHY service integration only from the viewpoint of information theory.
    - ✓ DMBC (Csiszar et al. '78)
    - ✓ MIMO (Ly et al. '10)
    - ✓ Bidirectional relay (Wyrembelski et al. '12)
    - ✓ Compound BC with uncertainties (Wyrembelski et al. '12)
  - How to derive certain transmit design to achieve the boundary points of the 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 received signal at receiver k

$$y_k = \mathbf{h}_k \mathbf{x} + z_k$$

$\mathbf{h}_k$-*k*th receiver's channel response z_k-AWGN

- Transmitted components

$$\mathbf{x} = \mathbf{x}_0 + \mathbf{x}_c + \mathbf{x}_a$$

$\mathbf{x}_0$-multicast message, $\mathbf{x}_0 \sim CN(\mathbf{0},\mathbf{Q}_0)$

$\mathbf{x}_c$-confidential message, $\mathbf{x}_c \sim CN(\mathbf{0},\mathbf{Q}_c)$

$\mathbf{x}_a$-artificial noise, $\mathbf{x}_a \sim CN(\mathbf{0},\mathbf{Q}_a)$

- Deterministically bounded CSI error model

$$\mathbf{h}_k = \tilde{\mathbf{h}}_k + \mathbf{e}_k, \|\mathbf{e}_k\|_F^2 \le \varepsilon_k^2$$

Robust Scheme

- Worst-case secrecy rate region

Under the above described deterministically bounded CSI error model, an achievable worst-case secrecy rate region is determined by [Ly et al. '10]

$$R_c \le \min_{k\in\mathcal{K}_e} \log \frac{\min_{\mathbf{h}_1\in B_1} 1+(1+\mathbf{h}_1\mathbf{Q}_a\mathbf{h}_1^H)^{-1}\mathbf{h}_1\mathbf{Q}_c\mathbf{h}_1^H}{\max_{\mathbf{h}_k\in B_k} 1+(1+\mathbf{h}_k\mathbf{Q}_a\mathbf{h}_k^H)^{-1}\mathbf{h}_k\mathbf{Q}_c\mathbf{h}_k^H}$$

$$R_0 \le \min_{\substack{k\in\mathcal{K}\\ \mathbf{h}_k\in B_k}} \log\left(1+\frac{\mathbf{h}_k\mathbf{Q}_0\mathbf{h}_k^H}{1+\mathbf{h}_k(\mathbf{Q}_c+\mathbf{Q}_a)\mathbf{h}_k^H}\right)$$

where $B_k = \{\mathbf{h}_k | \mathbf{h}_k = \tilde{\mathbf{h}}_k + \mathbf{e}_k\}, \mathcal{K} = \{1,2,...,K\}, \mathcal{K}_e = \mathcal{K}/\{1\}$

- Problem Formulation

$$g^*(\tau) = \max_{\mathbf{Q}_0,\mathbf{Q}_a,\mathbf{Q}_c} \log \frac{\min_{\mathbf{h}_1\in B_1} 1+(1+\mathbf{h}_1\mathbf{Q}_a\mathbf{h}_1^H)^{-1}\mathbf{h}_1\mathbf{Q}_c\mathbf{h}_1^H}{\max_{k\in\mathcal{K}_e,\mathbf{h}_k\in B_k} 1+(1+\mathbf{h}_k\mathbf{Q}_a\mathbf{h}_k^H)^{-1}\mathbf{h}_k\mathbf{Q}_c\mathbf{h}_k^H}$$

$$\begin{aligned} s.t.\quad & \min_{\substack{k\in\mathcal{K}\\ \mathbf{h}_k\in B_k}} \left\{\log\frac{1+\mathbf{h}_k(\mathbf{Q}_c+\mathbf{Q}_a+\mathbf{Q}_0)\mathbf{h}_k^H}{1+\mathbf{h}_k(\mathbf{Q}_c+\mathbf{Q}_a)\mathbf{h}_k^H}\right\} \ge \tau, \\ & \mathrm{Tr}(\mathbf{Q}_0+\mathbf{Q}_a+\mathbf{Q}_c) \le P, \\ & \mathbf{Q}_0 \succeq \mathbf{0}, \mathbf{Q}_a \succeq \mathbf{0}, \mathbf{Q}_c \succeq \mathbf{0}, \end{aligned} \quad \textbf{(1)}$$

Demand for QoMS

This optimization problem also provides us a way to determine the boundary points of the secrecy rate region, by traversing all possible τ's.

Further simplify (1) by introducing a slack variable β

$$g^*(\tau) = \max_{\mathbf{Q}_0,\mathbf{Q}_a,\mathbf{Q}_c,\beta} \min_{\mathbf{h}_1\in B_1} \log\left(\frac{1+\mathbf{h}_1(\mathbf{Q}_c+\mathbf{Q}_a)\mathbf{h}_1^H}{\beta(1+\mathbf{h}_1\mathbf{Q}_a\mathbf{h}_1^H)}\right)$$

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

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

Since this problem is non-convex and challenging to solve directly. To deal with it, we recast it into a two-stage optimization problem.

- Problem Re-Formulation

The outer-stage part is with regard to (w.r.t.) β

$$\gamma^*(\tau') = \max_{\beta} \eta(\tau',\beta)$$

$$s.t.\quad 1 \le \beta \le 1 + P\min_{\mathbf{h}_1\in B_1}\|\mathbf{h}_1\|^2$$

where $\log\gamma^*(\tau')=g^*(\tau')$. The inner-stage part calculates $\eta(\tau',\beta)$ for a fixed β

$$\eta(\tau',\beta) = \max_{\mathbf{Q}_0,\mathbf{Q}_a,\mathbf{Q}_c} \min_{\mathbf{h}_1\in B_1} \frac{1+\mathbf{h}_1(\mathbf{Q}_c+\mathbf{Q}_a)\mathbf{h}_1^H}{\beta(1+\mathbf{h}_1\mathbf{Q}_a\mathbf{h}_1^H)}$$

$$\begin{aligned} s.t.\quad & (\beta-1)(1+\mathbf{h}_k\mathbf{Q}_a\mathbf{h}_k^H)-\mathbf{h}_k\mathbf{Q}_c\mathbf{h}_k^H \ge 0, \forall \mathbf{h}_k \in B_k, k\in\mathcal{K}_e, \quad \textbf{(3)} \\ & \mathbf{h}_k\mathbf{Q}_0\mathbf{h}_k^H - \tau'\mathbf{h}_k\mathbf{Q}_a\mathbf{h}_k^H - \tau'\mathbf{h}_k\mathbf{Q}_c\mathbf{h}_k^H - \tau' \ge 0, \forall \mathbf{h}_k\in B_k, k\in\mathcal{K}, \\ & \mathrm{Tr}(\mathbf{Q}_0+\mathbf{Q}_a+\mathbf{Q}_c) \le P, \\ & \mathbf{Q}_0 \succeq \mathbf{0}, \mathbf{Q}_a \succeq \mathbf{0}, \mathbf{Q}_c \succeq \mathbf{0}. \end{aligned}$$

❑ The inner-stage optimization

➢ By resorting to the *S-procedure* [1], we can recast the above optimization as follows

$$\eta(\tau',\beta)=\max_{\substack{\mathbf{Q}_0,\mathbf{Q}_a,\mathbf{Q}_c,\\ \{t_k\}_{k\in\mathcal{K}_e},\{\delta_k\}_{k\in\mathcal{K}}}}\ \min_{\mathbf{h}_1\in B_1}\frac{1+\mathbf{h}_1(\mathbf{Q}_c+\mathbf{Q}_a)\mathbf{h}_1^H}{\beta(1+\mathbf{h}_1\mathbf{Q}_a\mathbf{h}_1^H)}$$

$$\begin{aligned} s.t.\ & \mathbf{T}_k(\beta,\mathbf{Q}_c,\mathbf{Q}_a,t_k)\succeq\mathbf{0}, t_k\geq 0,\forall k\in\mathcal{K}_e,\\ & \mathbf{S}_k(\tau',\mathbf{Q}_c,\mathbf{Q}_a,\mathbf{Q}_0,\delta_k)\succeq\mathbf{0},\delta_k\geq 0,\forall k\in\mathcal{K},\\ & \mathrm{Tr}(\mathbf{Q}_0+\mathbf{Q}_a+\mathbf{Q}_c)\leq P,\\ & \mathbf{Q}_0\succeq\mathbf{0},\mathbf{Q}_a\succeq\mathbf{0},\mathbf{Q}_c\succeq\mathbf{0}. \end{aligned} \quad \textbf{(4)}$$

where

$$\mathbf{T}_k(\beta,\mathbf{Q}_c,\mathbf{Q}_a,t_k)=\begin{bmatrix} t_k\mathbf{I}+(\beta-1)\mathbf{Q}_a-\mathbf{Q}_c & ((\beta-1)\mathbf{Q}_a-\mathbf{Q}_c)\tilde{\mathbf{h}}_k^H \\ \tilde{\mathbf{h}}_k((\beta-1)\mathbf{Q}_a-\mathbf{Q}_c) & \tilde{\mathbf{h}}_k((\beta-1)\mathbf{Q}_a-\mathbf{Q}_c)\tilde{\mathbf{h}}_k^H-t_k\varepsilon_k^2+\beta-1 \end{bmatrix}$$

$$\mathbf{S}_k(\tau',\mathbf{Q}_c,\mathbf{Q}_a,\mathbf{Q}_0,\delta_k)=\begin{bmatrix} \delta_k\mathbf{I}+\mathbf{Q}_0-\tau'(\mathbf{Q}_a+\mathbf{Q}_c) & (\mathbf{Q}_0-\tau'(\mathbf{Q}_a+\mathbf{Q}_c))\tilde{\mathbf{h}}_k^H \\ \tilde{\mathbf{h}}_k(\mathbf{Q}_0-\tau'(\mathbf{Q}_a+\mathbf{Q}_c)) & -\delta_k\varepsilon_k^2-\tau'+\tilde{\mathbf{h}}_k(\mathbf{Q}_0-\tau'(\mathbf{Q}_a+\mathbf{Q}_c))\tilde{\mathbf{h}}_k^H \end{bmatrix}$$

– *S-procedure*

Let $\varphi_k(\mathbf{x})=\mathbf{x}^H\mathbf{A}_k\mathbf{x}+2\Re\{\mathbf{b}_k^H\mathbf{x}\}+c_k$, where $\mathbf{A}_k\in\mathbb{H}^n$ $\mathbf{b}_k\in\mathbb{C}^n$, $c_k\in\mathbb{R}$. The implication $\varphi_1(\mathbf{x})\leq 0\Rightarrow\varphi_2(\mathbf{x})\leq 0$ holds if and only if there exists a $\mu\ \geq\ 0$ such that

$$\mu\begin{bmatrix}\mathbf{A}_1 & \mathbf{b}_1\\ \mathbf{b}_1^H & c_1\end{bmatrix}-\begin{bmatrix}\mathbf{A}_2 & \mathbf{b}_2\\ \mathbf{b}_2^H & c_2\end{bmatrix}\succeq\mathbf{0}$$

The remaining difficulty in solving (4) lies in its objective function, especially the uncertainty therein.

[1] S. Boyd and L. Vandenberghe, Convex optimization. Cambridge university press, 2009..

➢ Identification of the quasi-concavity of (4)

Property 1: Let us define

$$f(\mathbf{Q}_c,\mathbf{Q}_a)=\min_{\mathbf{h}_1\in B_1}\frac{1+\mathbf{h}_1(\mathbf{Q}_c+\mathbf{Q}_a)\mathbf{h}_1^H}{\beta(1+\mathbf{h}_1\mathbf{Q}_a\mathbf{h}_1^H)}$$

Then $f(\mathbf{Q}_c,\mathbf{Q}_a)$ is a quasi-concave function on the problem domain of (4), and hence the maximization problem (4) is a quasi-concave problem.

Proof: We just need to verify the convexity of the α-superlevel set of $f(\mathbf{Q}_c,\mathbf{Q}_a)$.

$$S_\alpha=\{f(\mathbf{Q}_c,\mathbf{Q}_a)|\mathbf{Q}_a\succeq\mathbf{0},\mathbf{Q}_c\succeq\mathbf{0},f(\mathbf{Q}_c,\mathbf{Q}_a)\geq\alpha\}$$

By using the *S-procedure* again, one can easily obtain

$$f(\mathbf{Q}_c,\mathbf{Q}_a)\geq\alpha\Leftrightarrow\mathbf{X}(\beta,\mathbf{Q}_c,\mathbf{Q}_a,\rho)\succeq\mathbf{0}$$

where

$$\mathbf{X}(\beta,\mathbf{Q}_c,\mathbf{Q}_a,\rho)=\begin{bmatrix} \rho\mathbf{I}+(1-\alpha\beta)\mathbf{Q}_a+\mathbf{Q}_c & ((1-\alpha\beta)\mathbf{Q}_a+\mathbf{Q}_c)\tilde{\mathbf{h}}_k^H \\ \tilde{\mathbf{h}}_k((1-\alpha\beta)\mathbf{Q}_a+\mathbf{Q}_c) & \tilde{\mathbf{h}}_k((1-\alpha\beta)\mathbf{Q}_a+\mathbf{Q}_c)\tilde{\mathbf{h}}_k^H-\rho\varepsilon_1^2-\alpha\beta+1 \end{bmatrix}$$

The proof is completed . ■

Consequently, the optimization problem (4) can be efficiently solved by combining a bisection search [1] with a convex optimization solver, e.g., CVX.

Numerical Results

➢ N_t=2, K=5

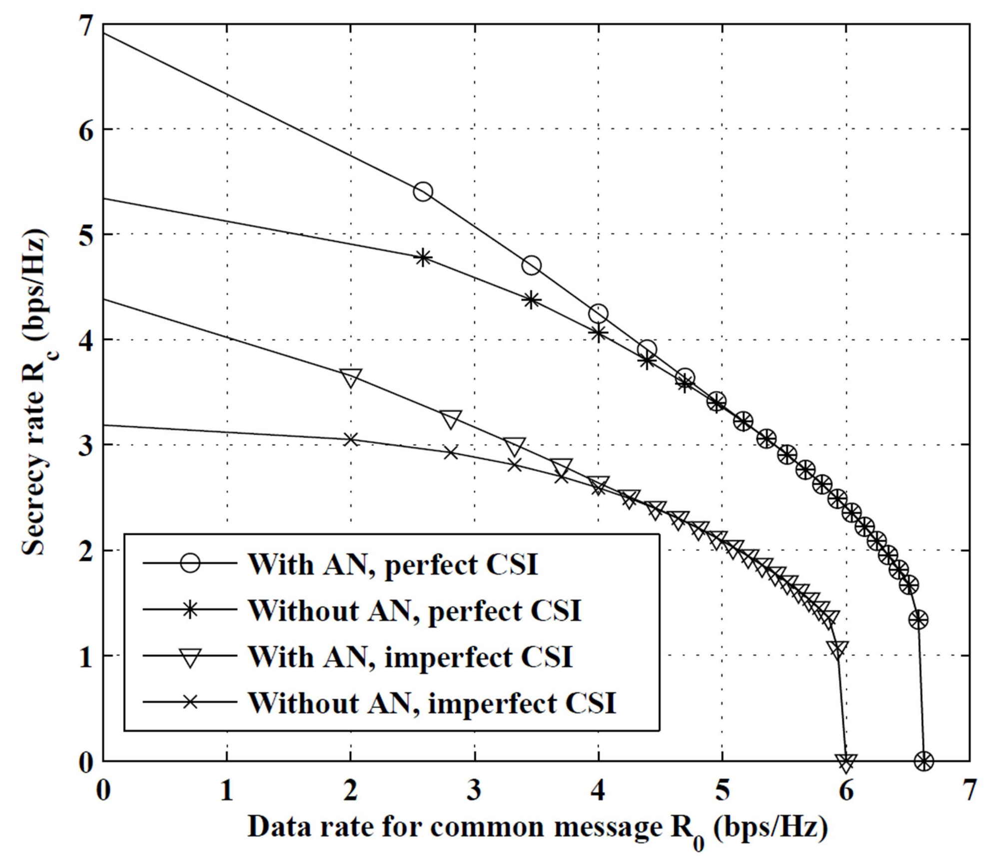
➢ Channel responses

$$\tilde{\mathbf{h}}_1=[2,0.4],\tilde{\mathbf{h}}_k=[0.9-0.1k,0.5+0.1k],k\in\mathcal{K}_e$$

➢ P=20dB

➢ ε_k=0.2 for all k

❑ Worst-case secrecy rate regions

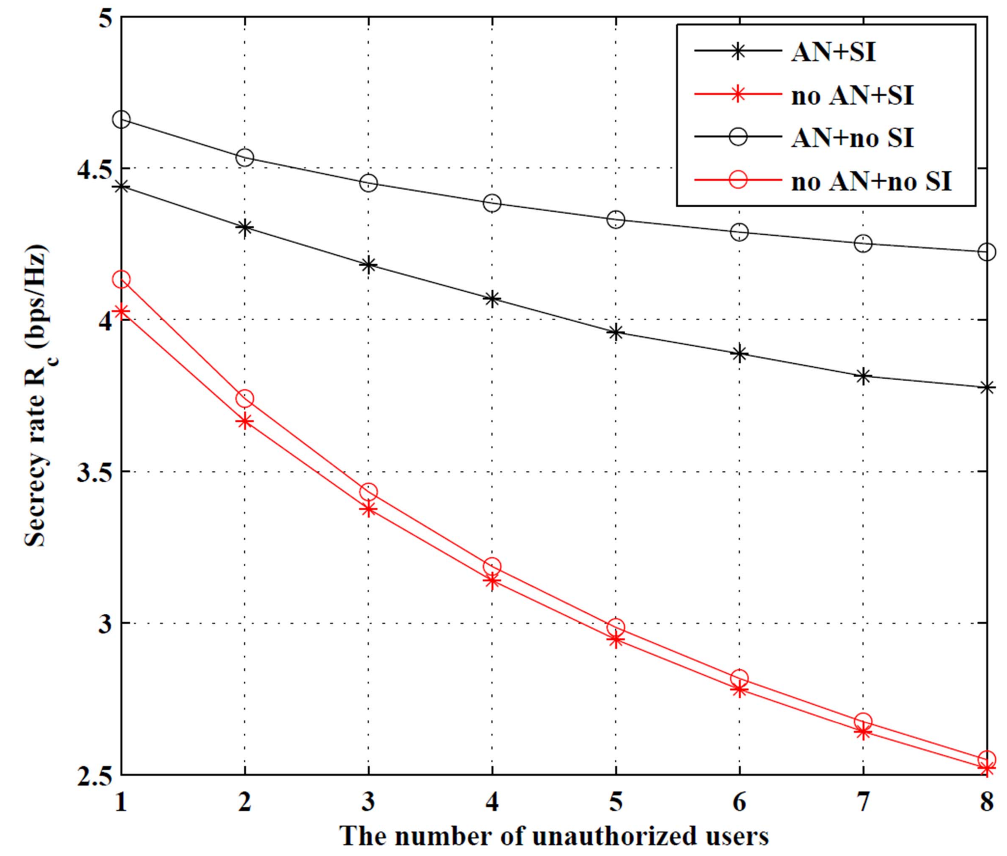


➢ The existence of channel uncertainty dramatically diminishes the achievable secrecy rate region

➢ AN indeed enhances the security performance without compromising the QoMS.

➢ The gap tends to be reduced, which implies that AN is prohibitive at high QoMS region.

❑ Secrecy rate versus #unauthorized receivers



➢ The worst secrecy rates drops with the number of unauthorized receivers.

➢ Incorporating service integration restrains the maximum worst-case secrecy rates

Concluding Remarks

❑ Considered the optimal robust AN-aided transmit design for multiuser MISO broadcast channel with confidential service and multicast service .

❑By resorting to a two-stage reformulation, the problem can be handled by solving a sequence of fractional SDPs.

❑AN can effectively fortify the transmission security, but high demand for QoMS will confine its use in turn.