Robust Energy-Efficient Transmit Design for MISOME Wiretap Channels

Weidong Mei, Zhi Chen, and Jun Fang

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

Background

- **Physical-layer (PHY) security**
  - **PHY security can overcome the inherent difficulties of cryptographic methods.**
  - **Most research activities focussed on the issue of secrecy rate maximization.**
  - **It is also an imporatnt problem to characterize the tradeoff between the secrecy performance and the energy consumption.**
- **PHY security and energy efficiency (EE)**
  - **Secrecy EE (SEE): the ratio of the achievable secrecy rate to the total power consumption.**
  - **considered only in a few existing works, with simple system settings (e.g., perfect CSI, one Eve).**
- Main contributions
  - **More general channel setting: MISOME wiretap channel with imperfect CSI on all links**
  - **Problem formulation: maximization of the worst-case SEE (WC-SEE) with secrecy rate constraint**
  - **The optimal covariance matrix is obtained by applying the fractional programming and rank relaxation methods.**
  - **The rank relaxation is proved to be tight.**

System Model

- **A multi-antenna transmitter (Alice) intends to send confidential information to a single-antenna legitimate receiver (Bob), in the presence of K multi-antenna eavesdroppers (Eves).**

$$y_b = \mathbf{h}_b \mathbf{x} + z_b,$$
$$\mathbf{y}_{e,k} = \mathbf{G}_{e,k}\mathbf{x} + \mathbf{z}_{e,k}, \forall k \in \mathcal{K}$$

where $\mathcal{K} \triangleq \{1,2,\ldots,K\}$, $\mathbf{h}_b \in \mathbb{C}^{1\times N_b}$ is the channel response between Alice and Bob, N_t is the number of transmit antennas employed by the transmitter, $\mathbf{G}_{e,k} \in \mathbb{C}^{N_e \times N_b}$ is the channel response between Alice and Eve k, $N_{e,k}$ is the number of transmit antennas employed by Eve, z_b and $\mathbf{z}_{e,k}$ are AWGN, and $\mathbf{x}$ is the coded confidential information following $\mathbf{x} \sim CN(0,\mathbf{Q}_c)$.

- **Deterministically bounded CSI error model**

$$\mathbf{h}_b = \tilde{\mathbf{h}}_b + \Delta\mathbf{h}_b, \|\Delta\mathbf{h}_b\|_F \le \varepsilon_b$$
$$\mathbf{G}_{e,k} = \tilde{\mathbf{G}}_{e,k} + \Delta\mathbf{G}_{e,k}, \|\Delta\mathbf{G}_{e,k}\|_F \le \varepsilon_{e,k}, \forall k \in \mathcal{K},$$

- **The worst-case secrecy rate**

$$R_s^{\text{worst}}(\mathbf{Q}_c) = \min_{\mathbf{h}_b \in B_b} \log(1+\mathbf{h}_b\mathbf{Q}_c\mathbf{h}_b^H) - \max_{k=1,\ldots,K} \max_{\mathbf{G}_{e,k}\in B_{e,k}} \log\det(\mathbf{I}+\mathbf{G}_{e,k}\mathbf{Q}_c\mathbf{G}_{e,k}^H)$$

where B_b and $B_{e,k}$ are the sets of all admissible CSI associated with $\mathbf{h}_b$ and $\mathbf{G}_{e,k}$, respectively.

- **Power consumption model [Xu et al. ’13]**

$$P_t = \mathrm{Tr}(\mathbf{Q}_c) + P_c$$

where P_c is a constant transmit independent power.

- **Problem Formulation**

Our work focuses on the design of $\mathbf{Q}_c$, to maximize the WC-SEE with QoS and total power constraints.

$$\max_{\mathbf{Q}_c} \frac{R_s^{\text{worst}}(\mathbf{Q}_c)}{\mathrm{Tr}(\mathbf{Q}_c)+P_c} \quad \text{s.t. } R_s^{\text{worst}}(\mathbf{Q}_c) \ge \tau_s, \mathrm{Tr}(\mathbf{Q}_c) \le P, \mathbf{Q}_c \succeq \mathbf{0}. \qquad (1)$$

where τ_s is preset requirement of the worst-case secrecy rate.

Problem Solving

- **A Dinkelbach Method-based Reformulation**

We first define a parametric problem with respect to λ as follow.

$$F(\lambda) = \max_{\mathbf{Q}_c \in \mathcal{F}} R_s^{\text{worst}}(\mathbf{Q}_c) - \lambda(\mathrm{Tr}(\mathbf{Q}_c)+P_c) \qquad (2)$$

where $\mathcal{F}$ is the feasible set of problem (1).

Lemma 1 $F(\lambda)$ is a strictly decreasing and continuous function w.r.t. λ, and it has a unique zero solution.
Lemma 2 Assume that λ^* is the unique zero solution to F(λ), then F(λ*) and (1) have the same optimal solution, and the optimal objective function value of (1) is λ*.

Our strategy is to optimize (2) and obtain $F(\lambda)$ with a given λ, and employ the ***Dinkelbach method*** to seek the optimal λ.

Introducing a slack variable β, one can check that (2) is equivalent to the following problem (3).

$$F(\lambda) = \max_{\mathbf{Q}_c,\beta} \left\{\log(\beta^{-1}+\beta^{-1}\min_{\mathbf{h}_b\in B_b}\mathbf{h}_b\mathbf{Q}_c\mathbf{h}_b^H) - \lambda(\mathrm{Tr}(\mathbf{Q}_c)+P_c)\right\}$$
$$\text{s.t. } \log\det(\mathbf{I}+\mathbf{G}_{e,k}\mathbf{Q}_c\mathbf{G}_{e,k}^H) \le \log\beta, \forall k \in \mathcal{K}, \mathbf{G}_{e,k}\in B_{e,k}$$
$$\log(1+\mathbf{h}_b\mathbf{Q}_c\mathbf{h}_b^H) - \log\beta \ge \tau_{cs}, \forall \mathbf{h}_b \in B_b,$$
$$\mathrm{Tr}(\mathbf{Q}_c) \le P, \mathbf{Q}_c \succeq \mathbf{0} \qquad (3)$$

- **A tight rank relaxation**

Lemma 3 The following inequality holds, det(**I** + **A**) ≥ 1 + Tr(**A**) for any PSD matrix **A**. Moreover, the equality holds if and only if rank(**A**) ≤ 1.

By applying Lemma 3, problem (3) can be relaxed as

$$F_{relax}(\lambda) = \max_{\mathbf{Q}_c,\beta} \left\{\log(\beta^{-1}+\beta^{-1}\min_{\mathbf{h}_b\in B_b}\mathbf{h}_b\mathbf{Q}_c\mathbf{h}_b^H) - \lambda(\mathrm{Tr}(\mathbf{Q}_c)+P_c)\right\}$$
$$\text{s.t. } 1+\mathrm{Tr}(\mathbf{G}_{e,k}\mathbf{Q}_c\mathbf{G}_{e,k}^H) \le \beta, \forall k \in \mathcal{K}, \mathbf{G}_{e,k}\in B_{e,k}$$
$$\log(1+\mathbf{h}_b\mathbf{Q}_c\mathbf{h}_b^H) - \log\beta \ge \tau_{cs}, \forall \mathbf{h}_b \in B_b,$$
$$\mathrm{Tr}(\mathbf{Q}_c) \le P, \mathbf{Q}_c \succeq \mathbf{0} \qquad (4)$$

with $F_{\text{relax}}(\lambda) \ge F(\lambda)$.

slack variable η introduced

- **A two-stage reformulation of (4)**

Outer problem

$$F_{\text{relax}}(\lambda) = \max_{\eta} \{\log\gamma(\lambda,\eta) - \eta\}$$
$$\text{s.t. } \lambda(\eta_{\min}+P_c) \le \eta \le \lambda(P+P_c), \qquad (5)$$

The inner problem

$$\gamma(\lambda,\eta)=\max_{\mathbf{Q}_c,\beta}\ \beta^{-1}(1+\min_{\mathbf{h}_b\in B_b}\mathbf{h}_b\mathbf{Q}_c\mathbf{h}_b^H)$$
$$\text{s.t.}\quad \lambda(\mathrm{Tr}(\mathbf{Q}_c)+P_c)\le\eta, \tag{6}$$
$$\text{constraints in (4) satisfied.}$$

❑SDP-based Reformulation of the Inner Problem

Step 1: variable transformation

Introduce the transformation $\alpha=1/\beta,\mathbf{Z}=\mathbf{Q}_c/\beta$ to rewrite (6) as

$$\gamma(\lambda,\eta)=\max_{\mathbf{Z},\alpha}\min_{\mathbf{h}_b\in B_b}\alpha+\mathbf{h}_b\mathbf{Z}\mathbf{h}_b^H$$
$$\text{s.t.}\quad \lambda(\mathrm{Tr}(\mathbf{Z})+\alpha P_c)\le\alpha\eta,$$
$$\alpha+\mathrm{Tr}(\mathbf{G}_{e,k}\mathbf{Z}\mathbf{G}_{e,k}^H)\le 1,\forall k\in\mathcal{K},\mathbf{G}_{e,k}\in B_{e,k} \tag{7}$$
$$\alpha+\mathbf{h}_b\mathbf{Z}\mathbf{h}_b^H\ge 2^{\tau_{cs}},\forall\mathbf{h}_b\in B_b,$$
$$\mathrm{Tr}(\mathbf{Z})\le P\alpha,\mathbf{Z}\succeq\mathbf{0}.$$

Step 2: S-procedure

$$\alpha+\mathrm{Tr}(\mathbf{G}_{e,k}\mathbf{Z}\mathbf{G}_{e,k}^H)\le 1,\forall k\in\mathcal{K},\mathbf{G}_{e,k}\in B_{e,k}\Leftrightarrow$$

$$\mathbf{X}_k(\rho_k,\alpha,\mathbf{Z})=$$
$$\begin{bmatrix}\rho_k\mathbf{I}_{N_tN_{e,k}}-(\mathbf{Z}^T\otimes\mathbf{I}_{N_{e,k}}) & -(\mathbf{Z}^T\otimes\mathbf{I}_{N_{e,k}})\tilde{\mathbf{g}}_{e,k}\\ -\tilde{\mathbf{g}}_{e,k}^H(\mathbf{Z}^T\otimes\mathbf{I}_{N_{e,k}})^H & -\rho_k\varepsilon_{e,k}^2-\tilde{\mathbf{g}}_{e,k}(\mathbf{Z}^T\otimes\mathbf{I}_{N_{e,k}})\tilde{\mathbf{g}}_{e,k}^H+1-\alpha\end{bmatrix}\succeq\mathbf{0}$$

in which $\tilde{\mathbf{g}}_{e,k}=\mathrm{vec}(\widetilde{\mathbf{G}}_{e,k})$, please refer to our paper for details.

$$\alpha+\mathbf{h}_b\mathbf{Z}\mathbf{h}_b^H\ge 2^{\tau_{cs}},\forall\mathbf{h}_b\in B_b,\Leftrightarrow$$
$$\mathbf{U}(t,\alpha,\mu,\mathbf{Z})=\begin{bmatrix}t\mathbf{I}+\mathbf{Z} & \mathbf{Z}\tilde{\mathbf{h}}_b^H\\ \tilde{\mathbf{h}}_b\mathbf{Z} & -\mu\varepsilon_b^2+\tilde{\mathbf{h}}_b\mathbf{Z}\tilde{\mathbf{h}}_b^H-v+\alpha\end{bmatrix}\succeq\mathbf{0}$$

in which $v\triangleq\max\{2^{\tau_{cs}},\mu\}$.

Then problem (7) can be transformed into an SDP problem given in (8), which can be efficiently solved via CVX. The outer problem can be handled via a one-dimensional search.

$$\gamma(\lambda,\eta)=\max_{\mathbf{Z},\alpha,\mu,t,\{\rho_k\}_{k\in K}}\ \mu$$
$$\text{s.t.}\quad \lambda(\mathrm{Tr}(\mathbf{Z})+\alpha P_c)\le\alpha\eta,$$
$$\mathbf{X}_k(\rho_k,\alpha,\mathbf{Z})\succeq\mathbf{0},\rho_k\ge 0,\forall k\in\mathcal{K} \tag{8}$$
$$\mathbf{U}(t,\alpha,\mu,\mathbf{Z})\succeq\mathbf{0},t\ge 0,$$
$$\mathrm{Tr}(\mathbf{Z})\le P\alpha,\mathbf{Z}\succeq\mathbf{0},$$

❑Overall Algorithm

Algorithm 1 Dinkelbach Algorithm for Solving the WC-SEE Maximization Problem (3)

1: Initiate $n=0$, $\epsilon>0$ and λ_n such that $F(\lambda_n)\ge 0$.
2: **Repeat**
3: Perform a one-dimensional line search over η to get $(\eta^*,\gamma(\lambda_n,\eta^*))$, wherein each $\gamma(\lambda_n,\eta)$ is returned by solving the problem (8) ;
4: Retrieve the corresponding $\mathbf{Q}_c^*$ via the variable transformation;
5: Compute $F(\lambda_n)=R_s^{\text{worst}}(\mathbf{Q}_c^*)-\lambda_n(\mathrm{Tr}(\mathbf{Q}_c^*)+P_c)$;
6: Update $\lambda_{n+1}=\frac{R_s^{\text{worst}}(\mathbf{Q}_c^*)}{\mathrm{Tr}(\mathbf{Q}_c^*)+P_c}$;
7: Update $n=n+1$;
8: **until** $|F(\lambda_{n-1})|\le\epsilon$
9: Output λ_n as the maximum WC-SEE.

Dinkelbach method

❑Tightness proof of the relaxation

Proposition 1 There exist an optimal solution ($\mathbf{Q}_c^*$,η^*) of problem (4), for which rank($\mathbf{Q}_c^*$)≤1, and the optimal $\mathbf{Q}_c^*$ can be constructed by solving a power minimization problem (9).

Sketch of proof: Suppose that we have solved (6) with the optimal value E_η. Then, we study the power minimization problem below.

$$\min_{\mathbf{Q}_c\succeq\mathbf{0}}\ \mathrm{Tr}(\mathbf{Q}_c)$$
$$\text{s.t.}\quad \min_{\mathbf{h}_b\in B_b}1+\mathbf{h}_b\mathbf{Q}_c\mathbf{h}_b^H\ge\beta E_\eta,$$
$$\lambda(\mathrm{Tr}(\mathbf{Q}_c)+P_c)\le\eta, \tag{9}$$
$$1+\mathrm{Tr}(\mathbf{G}_{e,k}\mathbf{Q}_c\mathbf{G}_{e,k}^H)\le\beta,\forall k\in\mathcal{K},\mathbf{G}_{e,k}\in B_{e,k}$$
$$\log(1+\mathbf{h}_b\mathbf{Q}_c\mathbf{h}_b^H)-\log\beta\ge\tau_{cs},\forall\mathbf{h}_b\in B_b.$$

Problem (9) can be converted into an SDP problem via *S*-procedure. The remaining proof consists of two steps:
Step 1: It can be proved, by contradiction, that the optimal solution of (9) is bound to be optimal to (6). Hence, it suffices to prove that the optimal $\mathbf{Q}_c$ of (9) is of rank one.
Step 2: By checking the Karush-Kuhn-Tucker (KKT) conditions of (9), one can verify that the optimal $\mathbf{Q}_c$ of (9) is of rank one. The details are omitted here. Similar proof can be found in [Li et al.'13].

Numerical Results

❑ Benchmark scheme (worst-case secrecy rate maximization, WC-SRM)

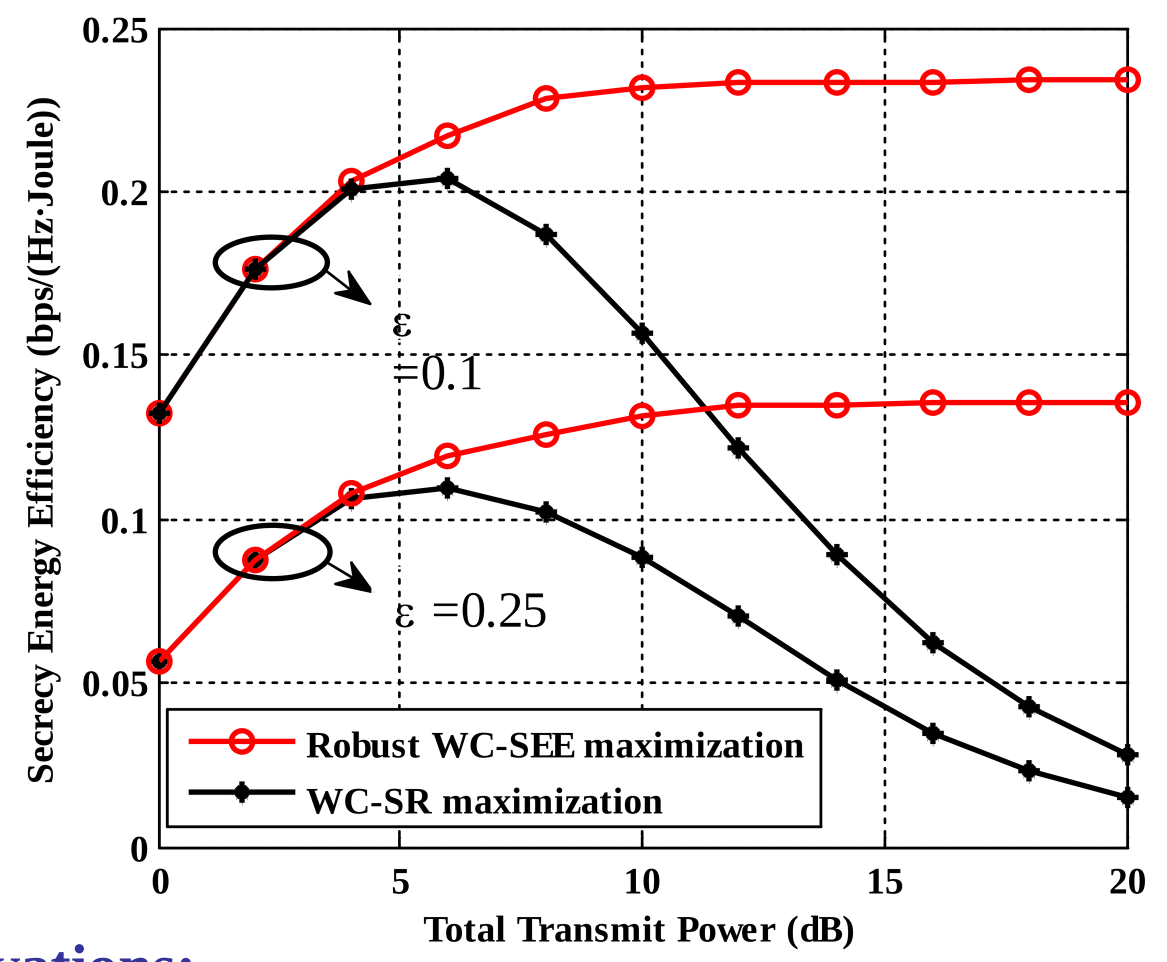
$$\hat{\mathbf{Q}}_c=\arg\max_{\mathbf{Q}_c\succeq\mathbf{0},\mathrm{Tr}(\mathbf{Q}_c)\le P}R_s^{\text{worst}}(\mathbf{Q}_c)$$
$$\text{s.t.}\quad R_s^{\text{worst}}(\mathbf{Q}_c)\ge\tau_s. \tag{10}$$

the resultant SEE

$$SEE_{\text{SRM}}=\frac{R_s^{\text{worst}}(\hat{\mathbf{Q}}_c)}{\mathrm{Tr}(\hat{\mathbf{Q}}_c)+P_c} \tag{11}$$

❑Simulation setting

- Transmit antenna#: N_t=6
- Eves#: K=2
- Eves' antennas#: $N_{e,k}$=3 for all k
- Transmit independent power P_c=7dB
- Required secrecy rate τ_s=1.5bps/Hz
- Channel uncertainty $\varepsilon_b=\varepsilon_{e,k}=\varepsilon$
- Average of 100 channel trials



Observations:
✓When P≤4dB, both schemes increase with the transmit power and achieve identical SEE performance.
✓After that, the performance achieved by the WC-SRM scheme degrades significantly, since it has used up all power budget.

Concluding Remarks

❑ The input transmit covariance was optimized to maximize the WC-SEE with constrained QoS.

❑ By resorting to the fractional programming theory and introducing a tight convex relaxation, we manage to recast the primal fractional optimization problem as a sequence of SDP problems.

❑ We proved that our obtained method can admit a rank-one solution, which guarantees the tightness of the convex relaxation.

❑Numerical results showed that our proposed WC-SEE maximization optimal strategy achieves SEE no less than that achieved by the WC-SR maximization optimal strategy.