ADMM-based Beamforming Optimization for Physical Layer Security in a Full-Duplex Relay System

New York Institute of Technology

B. K. Chalise

†Department of Electrical and Computer Engineering, New York Institute of Technology, USA, Email: {bchalise@nyit.edu }

Introduction

- Optimum beamforming in full-duplex communications can be solved with the semidefinite relaxation (SDR) approach whose computational complexity increases rapidly with the problem size.
- To reduce complexity, an alternating direction of multiplier method (ADMM) which minimizes the augmented Lagrangian of the dual of the SDR and handles the inequality constraints with the slack variables is proposed.
- The proposed ADMM is applied for optimizing relay beamformer to maximize the secrecy rate.
- Simulation results show that the proposed ADMM perfoms as good as the SDR approach.

Proposed ADMM

- Consider the following SDP problem in its standard form

$$\min_{\mathbf{X}\succeq 0} \ \mathrm{tr}(\mathbf{C}\mathbf{X}) \quad \text{s.t.} \ \bar{\mathcal{A}}(\mathbf{X}) = \bar{\mathbf{b}}, \ \bar{\mathcal{B}}(\mathbf{X}) \geq \bar{\mathbf{d}}. \qquad (1)$$

$$\min_{\mathbf{X}\succeq 0, \{u_i\geq 0\}_{i=1}^{q}} \ \mathrm{tr}(\mathbf{C}\mathbf{X}) \quad \text{s.t.} \ \bar{\mathcal{A}}(\mathbf{X}) = \bar{\mathbf{b}}, \ \bar{\mathcal{B}}(\mathbf{X}) - \mathbf{u} = \bar{\mathbf{d}}. \qquad (2)$$

- Here, $\{\mathbf{C}, \mathbf{X}\} \in \mathcal{C}^{n\times n}$, $\bar{\mathbf{b}} \in \mathcal{R}^{m\times 1}$, $\bar{\mathbf{d}} \in \mathcal{R}^{q\times 1}$, $\bar{\mathcal{A}}(\mathbf{X}) = [\mathrm{tr}(\mathbf{A}_1\mathbf{X}), \cdots, \mathrm{tr}(\mathbf{A}_m\mathbf{X})]^T$, and $\bar{\mathcal{B}}(\mathbf{X}) = \left[\mathrm{tr}(\mathbf{B}_1\mathbf{X}), \cdots \mathrm{tr}(\mathbf{B}_q\mathbf{X})\right]^T$. $\mathbf{u} = [u_1, \cdots, u_q]^T$ is a vector of positive slack variables.
- The Lagrangian multiplier function for (2) is expressed as

$$\mathcal{L}(\bar{\mathbf{y}}, \mathbf{v}, \boldsymbol{\lambda}, \mathbf{S}) = \mathrm{tr}\left((\mathbf{C} + \mathcal{A}^*(\bar{\mathbf{y}}) + \mathcal{B}^*(\mathbf{v}) - \mathbf{S})\,\mathbf{X}\right) - \bar{\mathbf{y}}^T\bar{\mathbf{b}} - \mathbf{v}^T\bar{\mathbf{d}} - (\mathbf{v}+\boldsymbol{\lambda})^T\mathbf{u}, \qquad (3)$$

where $\mathbf{S} \succeq \mathbf{0}$, $\boldsymbol{\lambda} \geq \mathbf{0}$, $\bar{\mathbf{y}} \in \mathcal{R}^{m\times 1}$ and $\mathbf{v} \in \mathcal{R}^{q\times 1}$ are the dual variables, $\mathcal{A}^*(\bar{\mathbf{y}}) = \sum_{i=1}^{m} \bar{y}_i\mathbf{A}_i$ and $\mathcal{B}^*(\mathbf{v}) = \sum_{i=1}^{q} v_i\mathbf{B}_i$ with $\bar{\mathbf{y}} \triangleq [\bar{y}_1, \cdots, \bar{y}_m]^T$ and $\mathbf{v} \triangleq [v_1, \cdots, v_q]^T$.

- The optimal dual and primal variables are obtained from $\max_{\{\bar{\mathbf{y}},\mathbf{v},\boldsymbol{\lambda}\}} \min_{\{\mathbf{X},\mathbf{u}\}} \mathcal{L}(\bar{\mathbf{y}}, \mathbf{v}, \boldsymbol{\lambda}, \mathbf{S})$, where $\min_{\{\mathbf{X},\mathbf{u}\}} \mathcal{L}(\bar{\mathbf{y}}, \mathbf{v}, \boldsymbol{\lambda}, \mathbf{S})$ is given by

$$\min_{\{\mathbf{u}\}} -\bar{\mathbf{y}}^T\bar{\mathbf{b}} - \mathbf{v}^T\bar{\mathbf{d}} - (\mathbf{v}+\boldsymbol{\lambda})^T\mathbf{u}, \ \text{ s.t. } \ \mathbf{C} + \mathcal{A}^*(\bar{\mathbf{y}}) + \mathcal{B}^*(\mathbf{v}) - \mathbf{S} = \mathbf{0}. \qquad (4)$$

- For given $\mathbf{v}$ and $\boldsymbol{\lambda}$, the optimum $\mathbf{u}$ is given by $\mathbf{u} = \max(\mathbf{0}, \mathbf{v}+\boldsymbol{\lambda})$. Substituting this $\mathbf{u}$ into (4), the resulting outer maximization is

$$\min_{\{\bar{\mathbf{y}},\mathbf{v},\boldsymbol{\lambda},\mathbf{S}\succeq 0\}} \ \bar{\mathbf{y}}^T\bar{\mathbf{b}} + \mathbf{v}^T\bar{\mathbf{d}} + (\mathbf{v}+\boldsymbol{\lambda})^T\max(\mathbf{0}, \mathbf{v}+\boldsymbol{\lambda}) \quad \text{s.t.} \ \mathbf{C} + \mathcal{A}^*(\bar{\mathbf{y}}) + \mathcal{B}^*(\mathbf{v}) - \mathbf{S} = \mathbf{0}. \qquad (5)$$

- Clearly, $\boldsymbol{\lambda} = \mathbf{0}$ is optimum. Define $\mathbf{b} \triangleq [\bar{\mathbf{b}}^T, \bar{\mathbf{d}}^T]^T$, $\mathbf{y} \triangleq [\bar{\mathbf{y}}^T, \mathbf{v}^T]^T$, $\mathcal{A}(\mathbf{X}) \triangleq [\bar{\mathcal{A}}^T(\mathbf{X}), \bar{\mathcal{B}}^T(\mathbf{X})]^T$, and $\mathcal{A}^*(\mathbf{y}) \triangleq \mathcal{A}^*(\bar{\mathbf{y}}) + \mathcal{B}^*(\mathbf{v})$. Then, (5) can be expressed as

$$\min_{\{\mathbf{y},\mathbf{S}\succeq 0\}} \ \mathbf{y}^T\mathbf{b} + \mathbf{y}^T\mathbf{P}_m\mathbf{y}, \ \text{ s.t. } \ \mathbf{C} + \mathcal{A}^*(\mathbf{y}) - \mathbf{S} = \mathbf{0}, \qquad (6)$$

- The augmented Lagrangian is

$$\mathcal{L}_\mu(\mathbf{X}, \mathbf{y}, \mathbf{S}) = \mathbf{y}^T\mathbf{b} + \mathbf{y}^T\mathbf{P}_m\mathbf{y} + \mathrm{tr}\left((\mathbf{C} + \mathcal{A}^*(\mathbf{y}) - \mathbf{S})\,\mathbf{X}\right) + \frac{1}{2\mu}||\mathbf{C} + \mathcal{A}^*(\mathbf{y}) - \mathbf{S}||^2. \qquad (7)$$

In ADMM, $\min_{\mathbf{X},\mathbf{y},\mathbf{S}\succeq 0} \mathcal{L}_\mu(\mathbf{X}, \mathbf{y}, \mathbf{S})$ is solved.

Proposed ADMM

- Starting with some $\mathbf{X}^{(k)}$ and $\mathbf{S}^{(k)}$, the ADDM includes three sub-problems

$$\mathbf{y}^{(k+1)} = \mathrm{argmin}_{\mathbf{y}}\mathcal{L}_\mu\left(\mathbf{X}^{(k)}, \mathbf{y}, \mathbf{S}^{(k)}\right), \qquad (8)$$

$$\mathbf{S}^{(k+1)} = \mathrm{argmin}_{\mathbf{S}\succeq 0}\mathcal{L}_\mu\left(\mathbf{X}^{(k)}, \mathbf{y}^{(k+1)}, \mathbf{S}\right), \qquad (9)$$

$$\mathbf{X}^{(k+1)} = \mathbf{X}^{(k)} + \frac{1}{2\mu}\left[\mathbf{C} + \mathcal{A}^*(\mathbf{y}^{(k+1)}) - \mathbf{S}^{(k+1)}\right]. \qquad (10)$$

Proposed Method (Contd.)

Let us assume $\mathbf{B}_1 \triangleq \mathbf{A}_{m+1}, \cdots \mathbf{B}_q \triangleq \mathbf{A}_{m+q}$ define

$$\bar{\mathbf{A}} = \begin{bmatrix} \mathrm{tr}(\mathbf{A}_1\mathbf{A}_1^H) & \cdots & \mathcal{R}e\left(\mathrm{tr}(\mathbf{A}_m\mathbf{A}_1^H)\right) \\ \vdots & \vdots & \vdots \\ \mathcal{R}e\left(\mathrm{tr}(\mathbf{A}_1\mathbf{A}_{m+q}^H)\right) & \cdots & \mathrm{tr}(\mathbf{A}_{m+q}\mathbf{A}_{m+q}^H) \end{bmatrix}.$$

For a given $\mathbf{S}^{(k)}$ and $\mathbf{X}^{(k)}$, the solution of $\min_{\mathbf{y}}\mathcal{L}_\mu\left(\mathbf{X}^{(k)}, \mathbf{y}, \mathbf{S}^{(k)}\right)$ is

$$\mathbf{y}^{(k+1)} = (\bar{\mathbf{A}} + 2\mu\mathbf{P}_m)^{-1}\left\{-\mathcal{A}_R\left((\mathbf{C} - \mathbf{S}^{(k)})^H\right) + \mu\left(-\mathbf{b} - \mathcal{A}(\mathbf{X}^{(k)})\right)\right\}, \ \text{where}$$

$$\mathcal{A}_R\left((\mathbf{C} - \mathbf{S}^{(k)})^H\right) = \begin{bmatrix} \mathcal{R}e\left(\mathrm{tr}(\mathbf{A}_1\left(\mathbf{C} - \mathbf{S}^{(k)})^H\right)\right) \\ \vdots \\ \mathcal{R}e\left(\mathrm{tr}(\mathbf{A}_{m+q}\left(\mathbf{C} - \mathbf{S}^{(k)})^H\right)\right) \end{bmatrix}. \qquad (11)$$

- For given $\mathbf{X}^{(k)}$ and $\mathbf{y}^{(k+1)}$, the solution of $\min_{\mathbf{S}\succeq 0}\mathcal{L}_\mu\left(\mathbf{X}^{(k)}, \mathbf{y}^{(k+1)}, \mathbf{S}\right)$ is

$$\mathbf{S}^{(k+1)} = \mathbf{Q}\boldsymbol{\Lambda}^+_{\mathbf{V}^{(k+1)}}\mathbf{Q}^H \qquad (12)$$

where $\boldsymbol{\Lambda}^+_{\mathbf{V}^{(k+1)}}$ is the diagonal matrix of positive eigenvalues of

$$\mathbf{V}^{(k+1)} = \mathbf{X}^{(k)} + \frac{1}{2\mu}\left(\mathbf{C} + \mathcal{A}^*(\mathbf{y}^{(k+1)})\right)^H, \qquad (13)$$

and $\mathbf{Q}$ is the corresponding matrix of eigenvectors.

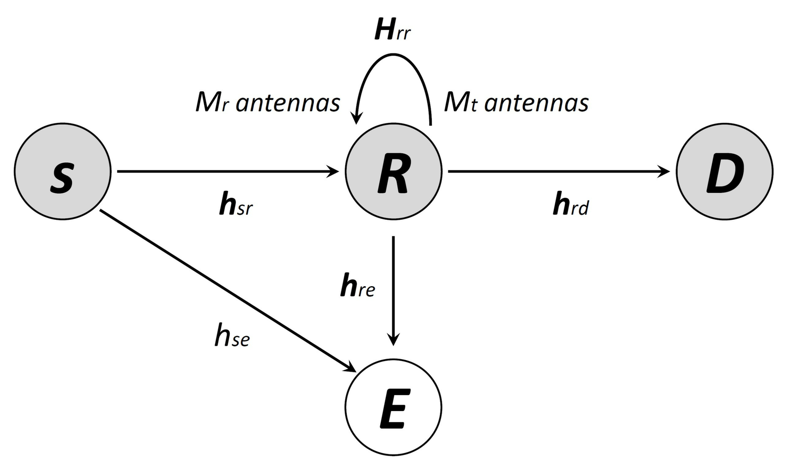
- 1) Initialize $\mathbf{X}^{(k)}$ and $\mathbf{S}^{(k)}$, the maximum number of iterations (N_{it}) and/or convergence accuracy ϵ, and μ.
- 2) Obtain $\mathbf{y}^{(k+1)}$ from (11).
- 3) Obtain $\mathbf{S}^{(k+1)}$ from (12) and (13).
- 4) Update $\mathbf{X}^{(k+1)}$ using (10)
- 5) Update μ
- 6) If $\{y_i^{(k+1)} = 0\}_{i=m+1}^{m+q}$, set ith row of $\bar{\mathbf{P}}_m$ to all-zeros.
- 7) Go to step 2 until convergence.

- Stopping criterion: The algorithm converges if $\max(r^{(k)}_{prim}, r^{(k)}_{dual}) \leq \epsilon$, where $r^{(k)}_{prim} = ||\mathcal{A}(\mathbf{X}^{(k)}) - \mathbf{b}||$ and $r^{(k)}_{dual} = ||\mathbf{C} + \mathcal{A}^*(\mathbf{y}^{(k+1)}) - \mathbf{S}^{(k+1)}||$ are the residuals. The update process for μ is

$$\mu^{(k+1)} = \begin{cases} \tau^u\mu^{(k)} & \text{if } r^{(k)}_{prim} > \rho r^{(k)}_{dual}, \\ \frac{\mu^{(k)}}{\tau^d} & \text{if } r^{(k)}_{dual} > \rho r^{(k)}_{prim}, \\ \mu^{(k)} & \text{otherwise}, \end{cases} \qquad (14)$$

where we choose $\rho = 10$ and $\tau^u = \tau^d = 2$.

Application to Physical Layer Security:



- The secrecy rate is maximized, which is

$$R = \log_2\left\{\left(1 + \min\left\{\rho_1\mathbf{h}_{sr}^H(\rho_2\mathbf{H}_{rr}\mathbf{w}_t\mathbf{w}_t^H\mathbf{H}_{rr}^H + \mathbf{I})^{-1}\mathbf{h}_{sr}, \rho_3|\mathbf{h}_{rd}^T\mathbf{w}_t|^2\right\}\right) - \frac{1}{2}\log_2\left(c^2 + \mathbf{w}_t^H\tilde{\mathbf{B}}\mathbf{w}_t\right)\right\},$$

- Here, $c = 1 + \rho_4|h_{se}|^2$, $\tilde{\mathbf{B}} = \rho_5\mathbf{h}_{re}^*\mathbf{h}_{re}^T$, $\rho_1 = \frac{P_s}{\sigma_r^2}$, $\rho_2 = \frac{P_r}{\sigma_r^2}$, $\rho_3 = \frac{P_r}{\sigma_d^2}$, $\rho_4 = \frac{P_s}{\sigma_e^2}$, and $\rho_5 = \frac{P_r}{\sigma_e^2}$.
- For a given t, using $q(t) \triangleq \frac{||\mathbf{h}_{sr}||^2}{\rho_2} - \frac{1}{\rho_1\rho_2}(t-1)$, and relaxing $\mathbf{W}_t \triangleq \mathbf{w}_t\mathbf{w}_t^H$ to $\mathbf{W}_t \succeq \mathbf{w}_t\mathbf{w}_t^H$

$$\min_{\mathbf{W}_t} \mathrm{tr}\left(\mathbf{W}_t\mathbf{h}_{re}^*\mathbf{h}_{re}^T\right), \qquad (15a)$$

$$\text{s.t.} \ \mathrm{tr}\left(\mathbf{W}_t\mathbf{H}_{rr}^H\left[\rho_2 q(t)\mathbf{I} - \mathbf{h}_{sr}\mathbf{h}_{sr}^H\right]\mathbf{H}_{rr}\right) \geq -q(t), \qquad (15b)$$

$$\frac{(t-1)}{\rho_3} \leq \mathrm{tr}\left(\mathbf{W}_t\mathbf{h}_{rd}^*\mathbf{h}_{rd}^T\right), \mathrm{tr}(\mathbf{W}_t) = 1, \ \mathbf{W}_t \succeq \mathbf{0}, \qquad (15c)$$

- Hence, for the ADMM algorithm

$$\mathbf{X} = \mathbf{W}_t, \ \mathbf{C} = \mathbf{h}_{re}^*\mathbf{h}_{re}^T, \ \mathbf{A}_1 = \mathbf{I}, \mathcal{A}^*(\bar{\mathbf{y}}) = \bar{y}_1\mathbf{I}, \ \bar{\mathbf{b}} = [1],$$

$$\mathbf{B}_1 = \mathbf{H}_{rr}^H\left[\rho_2 q(t)\mathbf{I} - \mathbf{h}_{sr}\mathbf{h}_{sr}^H\right]\mathbf{H}_{rr}, \ \mathbf{B}_2 = \mathbf{h}_{rd}^*\mathbf{h}_{rd}^T,$$

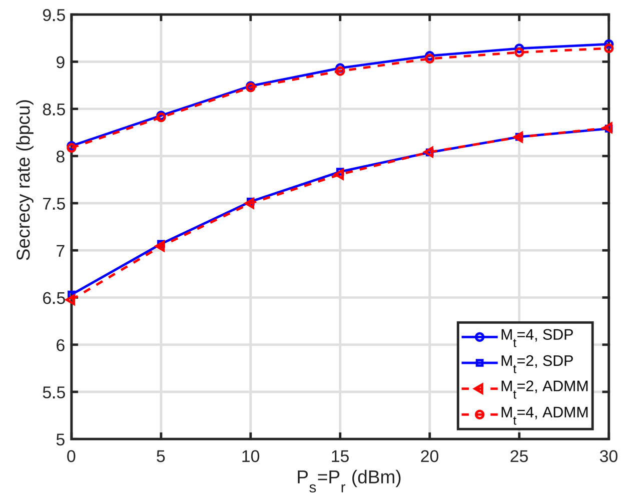
$$\mathcal{B}^*(\mathbf{v}) = v_1\mathbf{H}_{rr}^H\left[\rho_2 q(t)\mathbf{I} - \mathbf{h}_{sr}\mathbf{h}_{sr}^H\right]\mathbf{H}_{rr} + v_2\mathbf{h}_{rd}^*\mathbf{h}_{rd}^T,$$

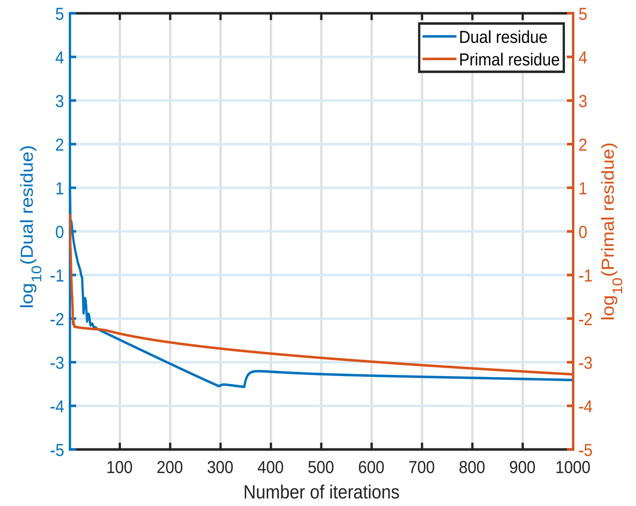
$$\bar{\mathbf{d}} = \left[-q(t), \frac{t-1}{\rho_3}\right]^T. \qquad (16)$$

- A line-search w.r.t. t is then performed to solve the joint optimization.

Numerical Results

- In all simulations of ADMM, we set $M = 8$, $\rho = 10$, $\tau^u = \tau^d = 2$, $N_{it} = 2000$, $\epsilon = 5 \times 10^{-3}$, and initial value of μ to 10.The $\mathtt{S-R}$, $\mathtt{R-D}$, $\mathtt{R-E}$, and $\mathtt{S-E}$ channel distances are set to 40m, 40m, 50m, and 200m, respectively.
- We set $\sigma_r^2 = \sigma_d^2 = \sigma_e^2$ to -80 dBm, the pathloss exponent to 3, the variance of the residual loop-interference to 30 dBm, and choose and $P_s = P_r$.





- For all values of M_t, the performance of the proposed ADMM is similar to that of the SDR method.
- We take $M_t = 6$, $\epsilon = 5 \times 10^{-3}$, and $P_s = 0$ dBm for convergence. As the number of iterations increase, both primal and dual residues converge to a value less than 5×10^{-3} in about 200 iterations.

Conclusions

- We proposed ADMM that minimizes the augmented Lagrangian function of the dual of the SDR and handles inequality constraints through slack variables.
- The algorithm is then applied to optimize full-duplex relay beamforming, wherein the objective is to maximize the secrecy rate.
- Simulation results show that the proposed ADMM provides performance similar to that of the standard SDR method.