Lattice-Reduction Aided Successive Optimization Tomlinson-Harashima Precoding Strategies for Physical-Layer Security in Wireless Networks

Xiaotao Lu [1], Keke Zu [2] and Rodrigo C. de Lamare [3]

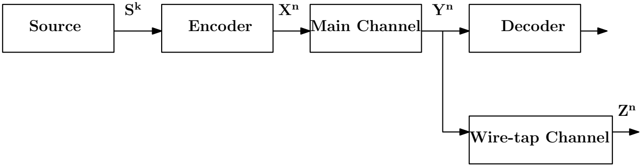
[1] University of York
[2] Ericsson Research, Sweden
[3] CETUC/PUC-Rio

[1] *xtl503@york.ac.uk*, [2] *zukeke@gmail.com*, [3] *rcdl500@york.ac.uk*

August 20, 2014

Outline

Definition of Physical Layer Security



- In 1949, shannon in the paper [Shannon, 1949] gives the theorem of cryptography from the view of information theory.
- In [Wyner, 1975], Wyner proposed the wire-tap channel which is described in the figure.

Shannon, Claude (1949)
Communication Theory of Secrecy Systems
Bell System Technical Journal 28(4), 656715.

Aaron D. Wyner (1975)
The Wire-Tap Channel
Bell System Technical Journal 54(8), 1355-1387.

Physical Layer Security Capacity for MIMO System

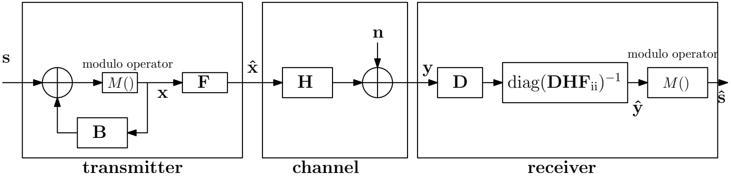
- In [F. Oggier, 2008], Oggier and Hassibi give the secrecy capcity for a MIMO system

Secrecy Capacity for MIMO System

$$
\begin{aligned}
C_s &= \max_{\boldsymbol{Q}_s \geq 0, \mathrm{Tr}(\boldsymbol{Q}_s) \leq \mathrm{E_s}} [I(X_s^N; Y^N) - I(X_s^N; Z^N)]^+ \\
&\geq [\max_{\boldsymbol{Q}_s \geq 0, \mathrm{Tr}(\boldsymbol{Q}_s) \leq \mathrm{E_s}} [I(X_s^N; Y^N)] \\
&- \max_{\boldsymbol{Q}_s \geq 0, \mathrm{Tr}(\boldsymbol{Q}_s) \leq \mathrm{E_s}} [I(X_s^N; Z^N)]]^+ \\
&= R
\end{aligned} \tag{1}
$$

F. Oggier, B. Hassibi (2008)
The Secrecy Capacity of the MIMO Wiretap Channel
IEEE International Symposium on Information Theory 2008, 524 - 528.

Conventional SO-THP Algorithm



- In [V. Stankovic, 2008], Stankovic and Haardt have proposed SO-THP algorithm to approach the channel capacity of a multi-user MIMO system.

V. Stankovic, M. Haardt (2008)
Generalized Design of Multi-User MIMO Precoding Matrices
IEEE Transactions on Wireless Communications 7(3), 953-961 .

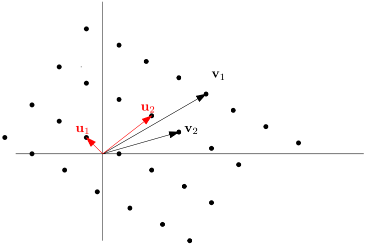
S-GMI Algorithm

- In [S.Hakjea, 2009], a generalized minimum mean-squared error (MMSE) channel inversion algorithm was proposed for users with multiple antennas to overcome the drawbacks of the Block diagonalization (BD) for multiuser MIMO systems.

S.Hakjea, L. Sang-Rim, L. Inkyu (2009)
Generalized channel inversion methods for multiuser MIMO systems
IEEE Transactions on Communications 57(11), 3489 - 3499 .

- Later In [Keke Zu, 2013], Keke Zu has extended the GMI algorithm to a simplified GMI algorithm.

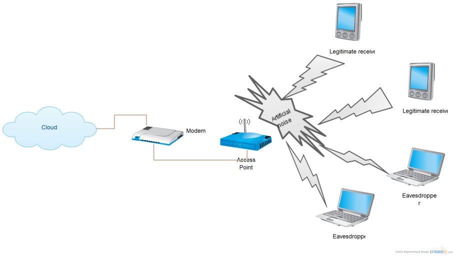
Keke Zu, R. C. de Lamare, M. Haardt (2013)
Generalized Design of Low-Complexity Block Diagonalization Type Precoding Algorithms for Multiuser MIMO Systems
IEEE Transactions on Communications 61(10), 4232 - 4242 .



- Suppose the users' channel is $\boldsymbol{H}$. A basis change may lead to improved performance as corroborated by lattice reduction techniques [S. Liu, 2002]. The more correlated the columns of $\boldsymbol{H}$, the more significant the improvements will be.

S. Liu, Y. Hong, E. Viterbo (2002)
Lattice-reduction-aided detectors for MIMO communication systems
Global Telecommunications Conference Vol.1, 424-428 .

Artificial Noise



- In [S. Goel, 2008], an approach of adding artificial noise at the transmitter of a multi-user MIMO system is introduced. The transmit signal can be expressed as

$$\boldsymbol{x}_r = \boldsymbol{P}_r \boldsymbol{s}_r + \boldsymbol{P}'_r \boldsymbol{s}'_r, \tag{2}$$

S. Goel, R. Negi (2008)
Guaranteeing Secrecy using Artificial Noise
IEEE Transactions on Wireless Communications 7(6), 2180-2189.

Motivation of Proposed Algorithm

Secrecy Rate

The proposed novel non-linear precoding algorithm is designed to achieve high secrecy rate for multi-user systems.

Reliable Transmission

Without affecting the secrecy rate performance, the proposed algorithm enhances the reliability of the transmission between transmitter and users.

Computational Complexity

The proposed algorithm requires a reduced complexity as compared to existing solutions such as BD, RBD and others.

Proposed LR-SO-THP+S-GMI Algorithm

Example (CLR procedure)

$$[\boldsymbol{H}_{red_n} \quad \bar{\boldsymbol{Q}}_n] = \mathrm{CLLL}(\boldsymbol{H}_\mathrm{n})$$
$$\boldsymbol{G}_n = ({\boldsymbol{H}_{red_n}}^H \boldsymbol{H}_{red_n} + \alpha \boldsymbol{I})^{-1} {\boldsymbol{H}_{red_n}}^H$$
$$\boldsymbol{G}_n \bar{\boldsymbol{Q}}_n = \tilde{\boldsymbol{U}}_n \tilde{\boldsymbol{\Sigma}}_n {\tilde{\boldsymbol{V}}_n}^H$$
$$\boldsymbol{P}_n = \bar{\boldsymbol{Q}}_n {\tilde{\boldsymbol{V}}_n}^{(1)}$$

- Compared to the conventional SO-THP algorithm, the lattice reduced channel matrix $\boldsymbol{H}_{red_n}$ is employed in the conventional S-GMI algorithm.
- With the CLLL algorithm the lattice reduced channel matrix is decomposed with a QR decomposition.

Details of Proposed Algorithm

for $i = 1 : T$ **do**
- $\boldsymbol{G}_i = \boldsymbol{H}_i$;
- $\boldsymbol{G}_i = \boldsymbol{U}_i \boldsymbol{\Sigma}_i [\boldsymbol{V}_i{}^{(1)} \boldsymbol{V}_i{}^{(0)}]^H$;
- $\boldsymbol{F}_i = \boldsymbol{V}_i{}^{(1)}$;
- $C_{max,i} =$ $\log_2 det \left(\boldsymbol{I} + \boldsymbol{R}_{k,i}^{-1} \boldsymbol{G}_i \boldsymbol{F}_i \boldsymbol{F}_i{}^H \boldsymbol{G}_i{}^H \right)$;

end for

$\boldsymbol{M} = \boldsymbol{H}$;

loop
- **while** $i = T : 1$ **do**
  - **for** $n = 1 : i$ **do**
    - $[\boldsymbol{H}_{red_n} \quad \bar{\boldsymbol{Q}}_n] = \mathrm{CLLL}(\boldsymbol{H}_\mathrm{n})$
    - $\boldsymbol{G}_n =$ $(\boldsymbol{H}_{red_n}{}^H \boldsymbol{H}_{red_n} + \alpha \boldsymbol{I})^{-1} \boldsymbol{H}_{red_n}{}^H$
    - $\boldsymbol{M}_n \bar{\boldsymbol{Q}}_n = \tilde{\boldsymbol{U}}_n \tilde{\boldsymbol{\Sigma}}_n \tilde{\boldsymbol{V}}_n{}^H$
    - $\boldsymbol{P}_n = \bar{\boldsymbol{Q}}_n \tilde{\boldsymbol{V}}_n{}^{(1)}$
  - **end for**
  - **for** $j = 1 : i$ **do**
    - $C_j =$ $\log_2 \det \left(\boldsymbol{I} + \boldsymbol{R}_{\mathrm{k,j}}^{-1} \boldsymbol{M}_\mathrm{j} \boldsymbol{P}_\mathrm{j} \boldsymbol{P}_\mathrm{j}{}^\mathrm{H} \boldsymbol{M}_\mathrm{j}{}^\mathrm{H} \right)$;
  - **end for**
  - $a_i = \arg\min_j (C_{max,j} - C_j)$;
  - $\boldsymbol{F}_i = \boldsymbol{P}_{a_i}$;
  - $\boldsymbol{D}_i = \tilde{\boldsymbol{U}}_{a_i}{}^H$;
  - $\boldsymbol{M} =$ $[\boldsymbol{H}_1{}^T \quad \cdots \quad \boldsymbol{H}_{a_i-1}{}^T \boldsymbol{H}_{a_i+1}{}^T \quad \cdots \quad \boldsymbol{H}_R{}^T]^T$
- **end while**

end loop

$$\boldsymbol{F} = (\boldsymbol{F}_1 \cdots \boldsymbol{F}_R);$$

$$\boldsymbol{D} = \begin{pmatrix} \boldsymbol{D}_1 & & \\ & \ddots & \\ & & \boldsymbol{D}_T \end{pmatrix}$$

$$\boldsymbol{B} = \text{lower triangular} \left(\boldsymbol{DHF} \bullet \text{diag} \left([\boldsymbol{DHF}]_{ii}^{-1} \right) \right)$$

- Similar to the conventional SO-THP, the received signal can be expressed as

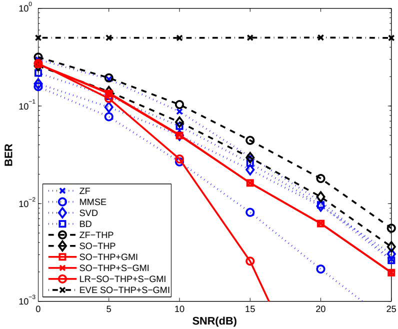
$$\hat{\boldsymbol{y}} = \boldsymbol{D} \beta (\boldsymbol{H} \frac{1}{\beta} \boldsymbol{F} \boldsymbol{x} + \boldsymbol{n}) \qquad (3)$$

- The transmit signal

$$\boldsymbol{x} = \boldsymbol{B}^{-1} \boldsymbol{x} \qquad (4)$$

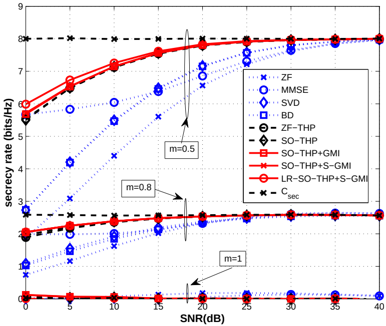
BER Performance of Proposed Algorithm

A system with $N_t = 8$ transmit antennas and $T = 2$ users as well as $K = 1, 2$ eavesdroppers is considered.



From the BER performance plot, the Lattice-Reduction aided Strategy will siginificantly improve the BER performance of the system.

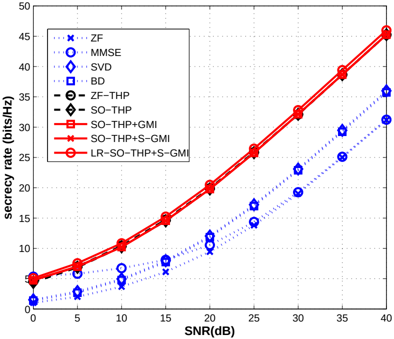
Secrecy rate Performance of Proposed Algorithm



When $T = K$

- At low SNR, the proposed LR-SO-THP+S-GMI algorithm achieves a higher secrecy rate than other techniques.
- At high SNR, the secrecy rate will converge to a constant.
- The convergence of secrecy rate is related to the ratio between the legitimate users' channel and eavesdroppers' channel coefficients.

Secrecy rate Performance with Artificial Noise



If Artificial Noise is added and the total transmit power E_s is the same. The simulation result shows that the secrecy rate tends to infinity when the transmit power increases

Contribution of Proposed Algorithm

The proposed algorithm can be implemented in a multi-user MIMO system, and it has the following advantages,

- A non-linear LR-SO-THP+S-GMI algorithm is proposed to achieve high secrecy rate.
- Compared with conventional algorithm, the proposed algorithm have low computational complexity performance.
- In terms of BER performance, the proposed algorithm outperforms other algorithms.
- The proposed algorithms can be cooperated with AN technique to enhance the secrecy rate performance.

Thank you