Secure Multiuser MISO Communication Systems with Quantized Feedback

Berna Özbek*, Özgecan Özdoğan*, Güneş Karabulut Kurt**

*Department of Electrical and Electronics Engineering
Izmir Institute of Technology, Turkey
**Department of Electronics and Communication Engineering
Istanbul Technical University, Istanbul, Turkey

Outline

- Introduction
- System Model
- The proposed secure multiuser MISO system
- Simulation Results
- Conclusions

Introduction

- Physical layer security is a promising approach to provide secure communications by considering the characteristics of wireless channels.
- Secrecy capacity can be enhanced by using multiple antenna techniques by serving multiple legitimate users simultaneously.
- In order to maintain multiuser transmission, the channel state information between base station and legitimate users is required at the transmitter.

Introduction

- The existence of eavesdropper's channel state information at transmitter has a great impact on the secrecy capacity in both single-user and multiuser communications.
- Since the network can be attacked by passive eavesdroppers, the eavesdropper's channel state information is unknown at the transmitter.
- For secure multiantenna single-user systems, the artificial noise is a well-known method to disrupts the reception of eavesdropper.

Introduction

- For multiuser MISO systems, the selection of legitimate users at the transmitter is critical since interuser interference reduces the performance.
- Therefore, we propose a semi-orthogonal selection for a secure multiantenna multiuser system with a quantized feedback link.
- Besides, instead of adding artificial noise to establish secure multiuser MISO systems, we utilize the effect of inter-user interference that disrupts the reception of the eavesdropper.

System Model

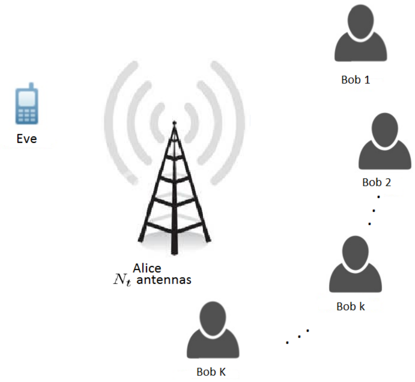

Figure: System Model

System Model

- M legitimate users are scheduled simultaneously and precoding matrix $\hat{\mathbf{W}}$ generated by employing Zero Forcing Beamforming.
- Based on scheduling the M best legitimate users at the transmitter, the received signal at the mth legitimate user:

$$y_{b_m} = ||\mathbf{h}_{b_m}||(\bar{\mathbf{h}}_{b_m}^{\dagger}\hat{\mathbf{w}}_m)s_m + \sum_{j=1, j\neq m}^{M} ||\mathbf{h}_{b_m}||(\bar{\mathbf{h}}_{b_m}^{\dagger}\hat{\mathbf{w}}_j)s_j + n_{b_m}, \quad (1)$$

- The received signal belonging to the mth legitimate user at the eavesdropper:

$$y_{e_m} = \mathbf{h}_e^{\dagger}\hat{\mathbf{w}}_m s_m + \sum_{j=1, j\neq m}^{M} \mathbf{h}_e^{\dagger}\hat{\mathbf{w}}_j s_j + n_e. \quad (2)$$

System Model

- The signal-to-interference-noise ratio (SINR) at mth Bob is determined by,

$$\hat{\gamma}_{b_m} = \frac{\frac{P}{M}||\mathbf{h}_{b_m}||^2|\bar{\mathbf{h}}_{b_m}^{\dagger}\hat{\mathbf{w}}_m|^2}{\sum_{j=1,j\neq m}^{M}\frac{P}{M}||\mathbf{h}_{b_m}||^2|\bar{\mathbf{h}}_{b_m}^{\dagger}\hat{\mathbf{w}}_j|^2+\sigma^2}. \quad (3)$$

- The SINR at Eve belonging to the mth legitimate user is defined by

$$\hat{\gamma}_{e_m} = \frac{\frac{P}{M}\,|\mathbf{h}_e^{\dagger}\hat{\mathbf{w}}_m|^2}{\sum_{j=1,j\neq m}^{M}\frac{P}{M}\left|\mathbf{h}_e^{\dagger}\hat{\mathbf{w}}_j\right|^2+{\sigma_e}^2}. \quad (4)$$

- Secrecy sum capacity under quantized CDI is given by,

$$R = \sum_{m=1}^{M} E\left\{\log_2\left(1+\hat{\gamma}_{b_m}\right)\right\} - E\left\{\log_2\left(1+\hat{\gamma}_{e_m}\right)\right\}. \quad (5)$$

System Model

- The lack of perfect CSI at transmitter causes a degradation on Bobs secrecy capacity since W is not perfectly orthogonal to the channel of legitimate users in quantized the case.
- We design codebook based on the semi-orthogonal selection criterion to reduce the quantization errors of legitimate users.
- However, it is not possible to eliminate the inter-user interference competely, the reception of Eve is still disturbed in the proposed solution.

Semi-orthogonal Selection

- Each user generates the same N_t random orthonormal vectors $\phi_i \in \mathcal{C}^{N_t \times 1}$, $i = 1, \ldots, N_t$.
- Then, they measure the orthogonality between their channels and the random vectors ϕ_i using the chordal distance:

$$d^2(\bar{\mathbf{h}}_k, \phi_i) = 1 - |\bar{\mathbf{h}}_k^\dagger \phi_i|^2 \quad (6)$$

- We can define a spherical cap on $\mathcal{O}^{N_t}$ with center $\mathbf{o}$ and square radius ϵ as the open set :

$$\mathcal{B}_\epsilon(\mathbf{o}) = \left\{\bar{\mathbf{h}}_k \in \mathcal{O}^{N_t} : d^2(\bar{\mathbf{h}}_k, \mathbf{o}) \leq \epsilon\right\} \quad (7)$$

- Then, we apply the criterion $\mathcal{T}_3$ to select the legitimate users

$$\mathcal{T}_3 = \left\{ k \in K : \bar{\mathbf{h}}_k \in \bigcup_{i=1}^{N_t} \mathcal{B}_\epsilon(\phi_i) \text{ and } \|\mathbf{h}_k\|^2 \geq \gamma_{th} \right\} \quad (8)$$

Semi-orthogonal Selection

- The legitimate users which satisfy semi-orthogonality condition but having low norm should not take part in user selection.
  - The reason is that the channel quality of selected users directly affects the secrecy sum rate.
- $\bar{K}$ users on average are allowed to feedback their CSI to transmitter.
- Base station chooses the legitimate users for communications according to the decision mechanism based on selecting users with the highest norm to establish a secure transmission.

Semi-orthogonal Selection with a specific codebook

- We use a specific codebook based on the quantization of the localized region instead of the normalized independent and identically distributed (i.i.d) channel in isotropically distributed in $\mathcal{O}^{N_t}$.
- As in the i.i.d. case, we use a practical vector quantization scheme to design the local packings.
- For the $\mathcal{T}_3$ criterion, the codebook is adapted according to the orthogonal vectors ϕ_i.
- From the local packing associated to the spherical cap $\mathcal{B}_\epsilon(\mathbf{o})$, it is possible to compute $\mathcal{B}_\epsilon(\phi_i)$ using the rotation matrix:

$$\phi_i = \mathbf{U}_r \mathbf{o} \tag{9}$$

where $\mathbf{U}_r$ is the unitary rotation matrix.

Scheduling only one legitimate user

- In the case of quantized CDI, transmitted signal masked with AN for single user can be expressed as,

$$\mathbf{x}_k = \hat{\mathbf{f}}_k s_k + \hat{\mathbf{Q}}_k \mathbf{a}, \tag{10}$$

- The received signal at kth Bob:

$$y_k = ||\mathbf{h}_k||((\bar{\mathbf{h}}_k)^H \hat{\bar{\mathbf{h}}}_k) s_k + ||\mathbf{h}_k||((\bar{\mathbf{h}}_k)^H \hat{\mathbf{Q}}_k)\mathbf{a} + n_k \ , \tag{11}$$

- The received signal at Eve:

$$y_e = \mathbf{h}_e^H \hat{\bar{\mathbf{h}}}_k s_k + \mathbf{h}_e^H \hat{\mathbf{Q}}_k \mathbf{a} + n_e. \tag{12}$$

Scheduling only one legitimate user

- The SINR at kth Bob is given by,

$$\hat{\gamma}_k = \frac{||\mathbf{h}_k||^2 |(\bar{\mathbf{h}}_k)^H \hat{\bar{\mathbf{h}}}_k|^2 aP}{||\mathbf{h}_k||^2 |(\bar{\mathbf{h}}_k)^H \hat{\mathbf{Q}}_k|^2 \frac{1-a}{N_t-1} P + \sigma^2}, \tag{13}$$

- The SINR at Eve can be expressed as,

$$\hat{\gamma}_e = \frac{|(\mathbf{h}_e)^H \hat{\bar{\mathbf{h}}}_k|^2 aP}{|(\mathbf{h}_e)^H \hat{\mathbf{Q}}_k|^2 \frac{1-a}{N_t-1} P + \sigma_e^2}, \tag{14}$$

- Secrecy capacity in quantized case for single user is given as

$$R_b = \mathbb{E}\left\{\log_2\left(1+\hat{\gamma}_k\right)\right\} - \mathbb{E}\left\{\log_2\left(1+\hat{\gamma}_e\right)\right\}. \tag{15}$$

Simulation Parameters

- The number of transmit antennas is $N_t = 2$ at Alice
- An average number of users that is fed back is $\bar{K} = 4$. (γ_{th}, ϵ)=$[(1.65, 0.4), (2, 0.25), (2.3, 0.2), (2.55, 0.18), (2.6, 0.15)]$
- Only the legitimate users that satisfy these thresholds are fed back their B bits corresponding to the codebook index of their quantized CDI to Alice.
- Alice schedules the M legitimate users by performing ZFBF to reduce inter-user interference.
- The worst case scenario which means that no knowledge about CSI of Eve is available at Alice is considered.

Simulation Results

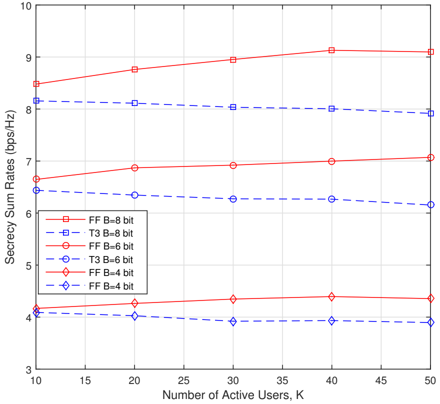

Figure: The comparison between full feedback (FF) and $\mathcal{T}_3$ criterion at $SNR = 20$dB for the different number of active users.

Simulation Results

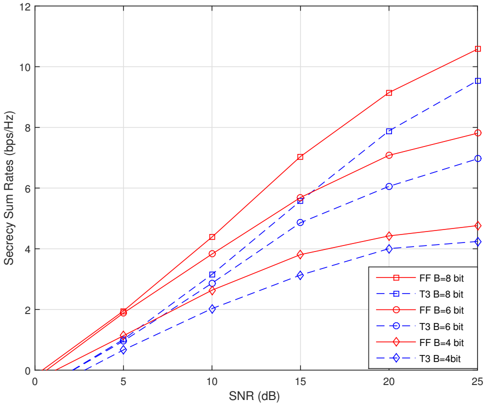

Figure: The comparison between full feedback (FF) and $\mathcal{T}_3$ criterion at $K = 50$ for different SNR values.

Simulation Results

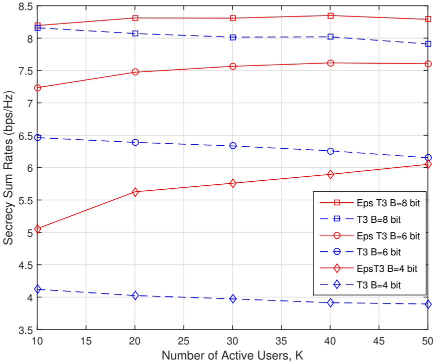

Figure: The comparison between $\mathcal{T}_3$ criterion with and without a special codebook design for $SNR = 20$dB.

Simulation Results

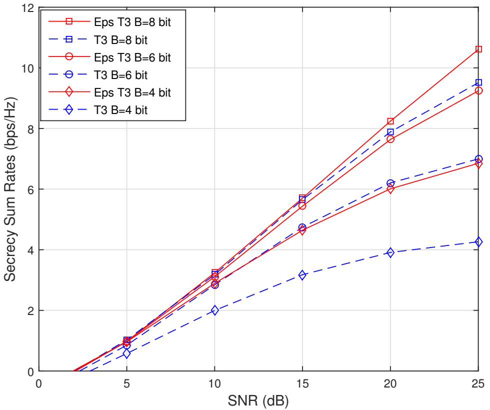

Figure: The comparison between $\mathcal{T}_3$ criterion with and without proposed codebook at $K = 50$ for different SNR values.

Simulation Results

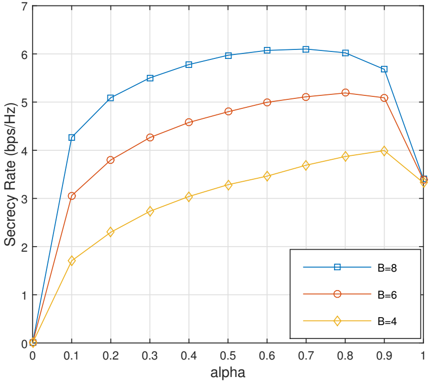

Figure: Power allocation parameter for different number of bits in single user case at $SNR = 20\text{dB}$.

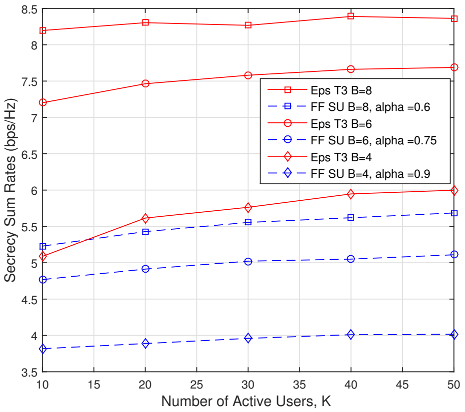

Figure: The comparison between single user MISO with full feedback (FF) case and multiuser MISO with $\mathcal{T}_3$ criterion with special codebook design at $SNR = 20$dB.

Conclusion

- We have selected more than one legitimate user at the transmitter side to construct inter-symbol interference under quantized feedback link to disrupt the reception of eavesdropper.
- We have employed specific codebook thanks to the properties of semi orthogonal selection.
- By performing semi orthogonal selection, we have reduced the overhead through preventing the user having poor channel conditions to feedback their channel state information.
- We have illustrated that secrecy capacity is increased significantly for low number of quantization bits, which leads to design robust physical layer security systems against to channel estimation errors.