Semi-orthogonal selection for secure multiuser MISO communication systems with quantized feedback

Berna Özbek and Özgecan Özdoğan
Department of Electrical and Electronics Engineering
Izmir Institute of Technology
Izmir, Turkey
Email:{bernaozbek,ozgecanozdogan}@iyte.edu.tr

Güneş Karabulut Kurt
Wireless Communications Reserach Laboratory
Department of Electronics and Communication Engineering
Istanbul Technical University, Istanbul, Turkey
Email: gkurt@itu.edu.tr

***Abstract*—Physical layer security is a promising approach to provide secure communications by considering the characteristics of wireless channels. In this work, we propose a semi-orthogonal selection for a multiple input single output (MISO) multiuser system with an eavesdropper with a quantized feedback link. We assume that eavesdropper is passive and its channel state information (CSI) is not available at transmitter. In order to disrupt reception of passive eavesdropper, we schedule more than one legitimate user. For the sake of ensuring secure communication, the CSI of legitimate users has great impact on overall secrecy capacity performance. The proposed solution applies semi-orthogonal selection at the legitimate user side with a specific codebook design to improve the secrecy capacity by reducing the quantization errors for legitimate users and disrupting the reception of the eavesdropper.**

I. Introduction

Information security is a critical issue in wireless communication due to the inherent open nature of wireless medium and it has received considerable attention. The problem of secure communication so called "wiretap channel" first was introduced by Wyner [1]. In this pioneering work, point to point communication has been considered, i.e., there are three terminals, one sender, one receiver and one eavesdropper. Physical layer security techniques that exploit different characteristics of wireless communication channels e.g., fading, noise, interference and multiple antenna techniques that enable multiuser secure communication improves the overall performance for secure systems.

Secrecy capacity is defined as the amount of information that can be reliably transmitted from transmitter to intended receiver, with any eavesdropper able to intercept the transmission gaining an arbitrarily small amount of information. Secrecy capacity can be enhanced by using multiple antenna techniques. For secure single user multiple output single input (MISO) systems, in order to increase secrecy capacity, an artificial noise (AN) has been added [2]. In this approach, the transmitter injects AN into the null space of legitimate user' channel without effecting intended user. Thus, it disrupts the reception of eavesdropper that maliciously try to attain information from legitimate user's signal. However, the transmit power is partitioned between the information signal and AN to mask the desired signal from any potential eavesdropper. When the transmit power is determined properly, positive secrecy capacity can be guaranteed even if eavesdropper has better channel conditions than legitimate user.

For multiuser MISO systems, the system capacity can be improved by scheduling and resource sharing mechanisms with serving multiple legitimate users simultaneously. Zero forcing beamforming (ZFBF) can be performed to schedule the legitimate users to mitigate the effects of inter-user interference between them. Subsequently, the multiuser systems with security considerations have been investigated in [3]- [6].

The existence of eavesdropper's channel state information (CSI) at transmitter has great impact on system design in both single user and multiuser communications. In the single user case, the CSI of eavesdropper is assumed to be known perfectly known at transmitter in [7], [8] and [9]. Ergodic secrecy sum rates for multiuser MISO have been investigated and closed form expressions have been obtained according to CSI of eavesdropper at the transmitter: The presence of external passive eavesdropper that we have only statistical knowledge of it, has been discussed in [10]. Likewise, the case of internal eavesdropper with imperfect CSI at the transmitter has been covered in [11] and [12]. While protecting confidential messages, no information regarding the eavesdropper has been presumed at the transmitter, which is highly probable scenario in practical cases since network can be attacked by eavesdroppers that listen passively without revealing their CSI.

For multiuser MISO systems, the CSI of the legitimate users are required at the transmitter to perform ZFBF. It is not possible to completely eliminate the interuser interference in the case of quantized feedback and inter-user interference has a pivotal role in multiuser communication. However, it can be used as an useful tool to disrupt reception of any possible eavesdropper for secure multiuser MISO systems. A large number of selected legitimate users will result higher inter-user interference, resulting in a reduction in the capacity of the legitimate users. On the other hand, the interference between the legitimate users will disrupt eavesdropper transmission and

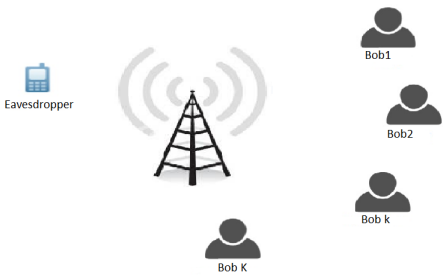

Fig. 1: Multiuser MISO downlink communication system with security consideration

thus it degrades the performance of eavesdropper as in the case of using AN without allocation any power [13].

In this work, we propose a semi-orthogonal selection with a specific codebook at the legimate users' side for multiuser MISO systems. Thus, we prevent to CSI feedback from the users having poor channel conditions to reduce feedback overhead while increasing secrecy sum rate with a specific codebook design which reduces quantization error for legitimate users and increases AN effect for eavesdropper.

The rest of this paper is organized as follows. Section II describes the system model for secure multiuser MISO systems. Section III proposes a semi orthogonal selection with a specific codebook design. Section IV introduces only one legitimate user case. Section V examines simulation results and discussions. Finally, section VI gives the conclusions.

II. System model

We consider a multiuser MISO downlink system operating under secrecy constraints as illustrated in Figure 1. The transmitter is equipped with N_t transmit antennas. The aim of the transmitter is to send confidential messages to intented $M \leq N_t$ legitimate users (Bobs) which are selected for secure communication from the set of active $K > N_t$ users. We assume that there is an eavesdropper whose aim is to attain information from these M selected users. Also, the eavesdropper is passive and its channel state information (CSI) is not available at the transmitter. All these K legitimate users and the eavesdropper (Eve) have only one receive antenna.

The transmitted signal $\mathbf{x}$ is expressed as,

$$\mathbf{x} = \hat{\mathbf{W}}\mathbf{s}, \tag{1}$$

where $\mathbf{s} = [s_1, s_2, \ldots, s_M]$ is an information symbol vector and $\hat{\mathbf{W}} = [\hat{\mathbf{w}}_1, \hat{\mathbf{w}}_2 \ldots, \hat{\mathbf{w}}_m, \ldots, \hat{\mathbf{w}}_M]$ is the precoding matrix generated by employing ZFBF precoding as $\hat{\mathbf{W}} = \hat{\mathbf{H}}(\mathbb{M})^\dagger(\hat{\mathbf{H}}(\mathbb{M})\hat{\mathbf{H}}(\mathbb{M})^\dagger)^{-1}$. The columns of $\hat{\mathbf{W}}$ is normalized, by $||\hat{\mathbf{w}}_m|| = 1$. Thus, we send confidential messages to M selected legitimate users simultaneously while eliminating inter-user interference.

The channel matrix, $\hat{\mathbf{H}}(\mathbb{M}) \in \mathcal{C}^{M\times N_t}$, includes channel vectors of selected legitimate users as $\hat{\mathbf{H}}(\mathbb{M}) = [\hat{\mathbf{h}}_1, \hat{\mathbf{h}}_2 \ldots, \hat{\mathbf{h}}_m, \ldots, \hat{\mathbf{h}}_M]^T$ where $\hat{\mathbf{h}}_m$ is the quantized version of the m^{th} legitimate user channel vector, $\mathbf{h}_m \in \mathcal{C}^{N_t\times 1}$ that is modelled by $\mathcal{CN}(0, \mathbf{I})$.

While addressing the lack of perfect CSI at the transmitter, it is possbile to quantize channel direction information (CDI), $\bar{\mathbf{h}}_k = \frac{\mathbf{h}_k}{||\mathbf{h}_k||}$, and channel quality information (CQI), $||\mathbf{h}_k||$ where $k = 1, ..., K$.

In this work, we assume that CQI is perfectly known at the transmitter. Therefore, each legitimate user k, (Bob), quantizes its CDI $\bar{\mathbf{h}}_k$ to an unit norm vector $\hat{\bar{\mathbf{h}}}_k$ selected from a predetermined codebook with the size of 2^B where B is the number of quantization bits. Random Vector Quantization (RVQ) based codebooks with $\mathbf{C}_k = \left\{\hat{\bar{\mathbf{h}}}_{k_1}, \hat{\bar{\mathbf{h}}}_{k_2}, \ldots, \hat{\bar{\mathbf{h}}}_{2^B}\right\}$ are adapted. Each user chooses an optimal codeword to quantize its CDI according to following criterion:

$$k_j^* = arg \max_{1\leq j\leq 2^B} \left|\bar{\mathbf{h}}_k^\dagger \hat{\bar{\mathbf{h}}}_{k_j}\right| \tag{2}$$

Then, we construct the quantized channel vector for each legitimate user by $\hat{\mathbf{h}}_k = \hat{\bar{\mathbf{h}}}_{k_j^*}||\mathbf{h}_k||$.

The relation between CDI $\bar{\mathbf{h}}_k$ and codeword $\hat{\bar{\mathbf{h}}}_k$ is modelled by,

$$\bar{\mathbf{h}}_k = \hat{\bar{\mathbf{h}}}_k \cos\theta_k + \mathbf{h}_\perp^k \sin\theta_k \tag{3}$$

where $\mathbf{h}_\perp^k$ is a unit norm vector orthogonal to $\bar{\mathbf{h}}_k$ and θ_k is the angle between $\bar{\mathbf{h}}_k$ and $\hat{\bar{\mathbf{h}}}_k$.

Based on scheduling the M best legitimate users at the transmitter, the received signal at the m^{th} legitimate user is written as,

$$y_{b_m} = ||\mathbf{h}_{b_m}||(\bar{\mathbf{h}}_{b_m}^\dagger \hat{\mathbf{w}}_m)s_m + \sum_{j=1, j\neq m}^{M} ||\mathbf{h}_{b_m}||(\bar{\mathbf{h}}_{b_m}^\dagger \hat{\mathbf{w}}_j)s_j + n, \tag{4}$$

The received signal belonging to m^{th} message at the eavesdropper is expressed by

$$y_{e_m} = \mathbf{h}_e^\dagger \hat{\mathbf{w}}_m s_m + \sum_{j=1, j\neq m}^{M} \mathbf{h}_e^\dagger \hat{\mathbf{w}}_j s_j + n_e. \tag{5}$$

where n and n_e are additive white Gaussian noise with zero mean, variances σ^2 and σ_e^2 respectively.

The SINR at m^{th} Bob is determined by,

$$\hat{\gamma}_{b_m} = \frac{\frac{P}{M}||\mathbf{h}_{b_m}||^2 |\bar{\mathbf{h}}_{b_m}^\dagger \hat{\mathbf{w}}_m|^2}{\sum_{j=1, j\neq m}^{M} \frac{P}{M}||\mathbf{h}_{b_m}||^2 |\bar{\mathbf{h}}_{b_m}^\dagger \hat{\mathbf{w}}_j|^2 + \sigma^2}. \tag{6}$$

The SINR at Eve for m^{th} message is defined by

$$\hat{\gamma}_{e_m} = \frac{\frac{P}{M}\ |\mathbf{h}_e^\dagger \hat{\mathbf{w}}_m|^2}{\sum_{j=1, j\neq m}^{M} \frac{P}{M}\left|\mathbf{h}_e^\dagger \hat{\mathbf{w}}_j\right|^2 + {\sigma_e}^2}. \tag{7}$$

Secrecy sum capacity under quantized CDI [13] is given by,

$$R = \sum_{m=1}^{M} E\left\{\log_2\left(1 + \hat{\gamma}_{b_m}\right)\right\} - E\left\{\log_2\left(1 + \hat{\gamma}_{e_m}\right)\right\}. \tag{8}$$

Lack of perfect CSI at transmitter causes a degradation on Bobs' capacity. Since $\hat{\mathbf{W}}$ is not perfectly orthogonal to the channel of legitimate users in quantized case, interuser interference that negatively affects reception of Bobs occurs. Therefore, we design codebook based on the semi-orthogonal selection criterion to reduce the quantization errors of legitimate users. Due to the fact that interuser interference can not completely eliminated, the reception of Eve is disturbed.

III. The semi-orthogonal selection

In order to maximize the secrecy capacity of the downlink MISO system under an average power constraint P while achieving multiuser diversity, it is necessary to choose the best combination of M users. Therefore, the users having poor channel (low norm or/and interfering with good users) should not take part in the user selection algorithm, nor feedback their channel information.

Interuser interference is a pivotal factor in multiuser communications. On the other hand, it may have a positive impact on the secrecy capacity since it causes interference to eavesdropper transmission. Therefore, the user scheduling at the transmit side is very critical to improve secrecy capacity. In this work, we propose to apply semi-orthogonal criterion with a specific codebook design at the legitimate users side and only give permission to these users to feedback their CSI to the transmitter by using the specific codebook rather than RVQ. Along with that, we select M legitimate users having the highest norms at the transmitter side to achieve higher secrecy capacity.

In order to select the legitimate users, we propose to apply the criterion $\mathcal{T}_3$ described in the following [14]:

$$\mathcal{T}_3 = \left\{ k \in K : \bar{\mathbf{h}}_k \in \bigcup_{i=1}^{N_t} \mathcal{B}_\epsilon(\phi_i) \text{ and } \|\mathbf{h}_k\|^2 \geq \gamma_{th} \right\} \quad (9)$$

where ϵ is the threshold on semi-orthogonality criterion and γ_{th} is the given threshold on norm to discriminate the users with low norms. Thus, the legitimate users which satisfy semi-orthogonality condition but having low norm should not take part in user selection for reason that channel quality of selected users directly affects the secrecy sum rate.

In order to apply semi-orthogonal criterion which selects the legitimate users whose CDI are semi-orthogonal, 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:

$$d^2(\bar{\mathbf{h}}_k, \phi_i) = 1 - |\bar{\mathbf{h}}_k^\dagger \phi_i|^2 \quad (10)$$

Let $\mathcal{O}^{N_t}$ be the unit sphere lying in $\mathcal{C}^{N_t}$ and centered at the origin. Using the chordal distance metric, for any $\epsilon < 1$, we can define a spherical cap on $\mathcal{O}^{N_t}$ with center $\mathbf{o}$ and square radius ϵ as the open set :

$$\mathcal{B}_\epsilon = \left\{ \bar{\mathbf{h}}_k \in \mathcal{O}^{N_t} : d^2(\bar{\mathbf{h}}_k, \mathbf{o}) \leq \epsilon \right\} \quad (11)$$

Consequently, $\bar{K}$ users on average are allowed to feedback their CSI to transmitter and they become candidate legitimate users for secure communication. Base station chooses the legitimate users for communications according to the decision mechanism based on selecting users with favorable channel conditions. Thus, transmitter selects users with highest norms for secure transmission.

The threshold values are calculated to have the number of average users $\bar{K}$ to feedback their CSI for the criterion T_3 [14]:

$$\bar{K} = K N_t \sum_{b=0}^{N_t - 1} \frac{\exp(-\gamma_{th})(\gamma_{th})^b}{b!} \epsilon^{N_t - 1} \quad (12)$$

A. Codebook design

In contrast to the normalized i.i.d. channel isotropically distributed in $\mathcal{O}^{N_t}$ [15], an important aspect of codebook tailored to a spherical cap region is the quantization of the localized region or local packing to reduce the error quantization. Therefore, for the T_3 criterion, the codebook is adapted according to the orthogonal vectors ϕ_i. A local Grassmannian packing with parameters N_t, N, $\mathbf{o}$, ϵ is a set of N vectors, constrained to a spherical cap $\mathcal{B}_\epsilon(\mathbf{o})$ in $\mathcal{O}^{N_t}$ where $N = 2^B$ is the codebook size.

From the local packing associated to the spherical cap $\mathcal{B}_\epsilon(\mathbf{o})$, it is possible to compute the local packing, $\mathcal{B}_\epsilon(\phi_i)$, using the rotation matrix [14],

$$\phi_i = \mathbf{U}_{rot} \mathbf{o} \quad (13)$$

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

IV. Scheduling only one legitimate user

In order to illustrate that we provide performance gain compared to the case where only the best legitimate user is scheduled rather than M users, we define the quantized secrecy capacity for the secure MISO systems including AN to disturb Eve reception.

In the case of quantized CDI, transmitted signal that is masked with artificial noise for single user can be expressed as,

$$\mathbf{x}_k = \mathbf{f} s_k + \hat{\mathbf{Q}} \mathbf{a}. \quad (14)$$

where s_k is the information-bearing signal with power $E\{|s_k|^2\} \leq P_s$, $\mathbf{f} \in \mathcal{C}^{N_t \times 1}$ is the precoding vector, $\mathbf{a} = [a_1, a_2, \ldots, a_{N_t - 1}]^T$ is the AN vector which is modelled by Gaussian distribution with power $E\{||\mathbf{a}||^2\} \leq P_a$, $\mathbf{Q} \in \mathcal{C}^{N_t \times N_t - 1}$ is the AN beamformer with orthonormal columns that form the AN subspace. The beamformers $\mathbf{f}$ and $\hat{\mathbf{Q}}$ are determined through quantized CSI as $\mathbf{f} = \hat{\bar{\mathbf{h}}}_k$ and $\hat{\bar{\mathbf{h}}}_k \hat{\mathbf{Q}} = \mathbf{0}_{1 \times N_t - 1}$.

Thus, the received signal at legitimate user and eavesdropper can be written as

$$y_k = ||\mathbf{h}_k|| (\bar{\mathbf{h}}_k{}^\dagger \hat{\bar{\mathbf{h}}}_k) s_k + ||\mathbf{h}_k|| (\bar{\mathbf{h}}_k{}^\dagger \hat{\mathbf{Q}}) \mathbf{a} + n_k \ , \quad (15)$$

$$y_e = \mathbf{h}_e^\dagger \hat{\bar{\mathbf{h}}}_k s_k + \mathbf{h}_e^\dagger \hat{\mathbf{Q}} \mathbf{a} + n_e. \quad (16)$$

where n_k and n_e are additive white Gaussian noise with zero mean and variances of σ^2 and σ_e^2 respectively.

Thus, SINR at k^{th} legitimate user (Bob) is given by,

$$\hat{\gamma} = \frac{||\mathbf{h}_k||^2 |\bar{\mathbf{h}}_k{}^\dagger \hat{\bar{\mathbf{h}}}_\mathbf{k}|^2 \alpha P}{||\mathbf{h}_k||^2 |\bar{\mathbf{h}}_k{}^\dagger \hat{\mathbf{Q}}|^2 \frac{1-\alpha}{N_t-1} P + {\sigma_k}^2}, \tag{17}$$

SINR at eavesdropper can be expressed as

$$\hat{\gamma}_e = \frac{|\mathbf{h}_e{}^\dagger \hat{\bar{\mathbf{h}}}_\mathbf{k}|^2 \alpha P}{|\mathbf{h}_e{}^\dagger \hat{\mathbf{Q}}|^2 \frac{1-\alpha}{N_t-1} P + \sigma_e^2}. \tag{18}$$

where P is the total power for message and AN signals. α denotes the power allocation parameter that adjust the ratio between P_s and P_a. Thus, P_s is equal to αP and $P_a = \frac{1-\alpha}{N_t-1} P$.

Then, secrecy capacity in quantized case for single user is given in [15] as

$$R = E\left\{\log_2(1 + \frac{||\mathbf{h}_k||^2 |\bar{\mathbf{h}}_k{}^\dagger \hat{\bar{\mathbf{h}}}_\mathbf{k}|^2 P_s}{||\mathbf{h}_k||^2 |\bar{\mathbf{h}}_k{}^\dagger \hat{\mathbf{Q}}|^2 P_a + {\sigma_k}^2})\right\} - E\left\{\log_2(1 + \frac{|\mathbf{h}_e{}^\dagger \hat{\bar{\mathbf{h}}}_\mathbf{k}|^2 P_s}{|\mathbf{h}_e{}^\dagger \hat{\mathbf{Q}}|^2 P_a + \sigma_e^2})\right\}.$$

In contrast to the case that CSI is perfectly known at transmitter, an AN leakage occurs in the quantized feedback case. This AN leakage term, $||\mathbf{h}_k||^2 |\bar{\mathbf{h}}_k{}^\dagger \hat{\mathbf{Q}}|^2$, negatively affects the reception of legitimate user and it reduces the secrecy capacity.

V. Simulation Results

We illustrate the simulation results for $N_t = 2$ transmit antennas at the base station. The pair of (γ_{th}, ϵ) for T3 criterion is calculated in order to have an average number of users in the cell $\bar{K} = 4$. Therefore, the pair is chosen as $[(1.65, 0.4)(2, 0.25)(2.3, 0.2)(2.55, 0.18)(2.6, 0.15)]$. Only the legitimate users that satisft these thresholds values are fed back their B bits corresponding to the codebook index of their quantized CDI to base station. Exploiting this feedback information, the base station selects the M legitimate users and perform ZFBF to reduce interuser interference.

The secrecy capacity comparison for T3 criterion and full feedback case in which all users feedback their CSI to the transmitter are illustrated in Figures 2 and 3 depending on the number of active users and signal-to-noise (SNR) values. Through T3, overhead is significantly reduced from 60% to 90% depending on the number of active users on the expense of reduction on capacity between 20% and 50% depending on SNR values.

In Figures 4 and 5, we compare the secrecy capacity for the case of special codebook design is employed. The results indicate that the proposed codebook design improves the secrecy capacity especially when the number of quantization bits is low, which leads a promising solution for overhead reduction even at low SNR values.

For secure single user MISO systems with perfect CSI case, the power is shared between message signal and AN equally as an optimal manner. However, for the quantized case, as shown in Figure 6, when the number of quantization bits are reduced, the power allocation parameter α should be increased to maximize secrecy capacity. As a result, as the number of quantization bits reduces, most of the available power at base station should be used for transmitting information signal rather than AN.

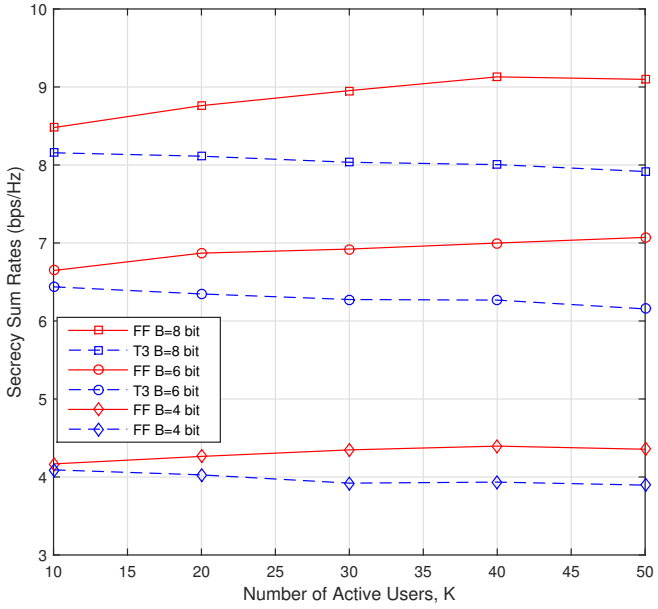

Fig. 2: The comparison between full feedback (FF) and T3 criterion at SNR=20 dB for the different number of active users.

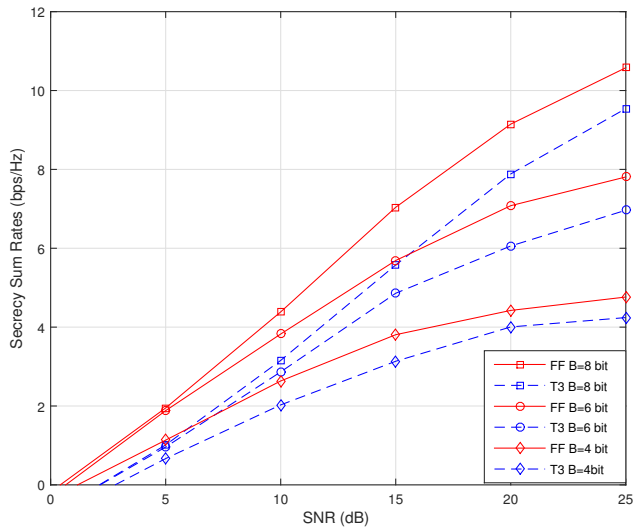

Fig. 3: The comparison between full feedback (FF) and T3 criterion at K=50 for different SNR values.

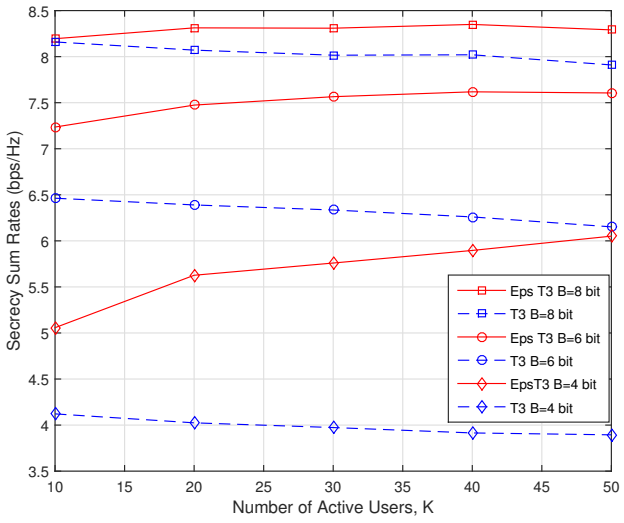

Fig. 4: The comparison between T3 criterion with and without proposed codebook for SNR=20 dB.

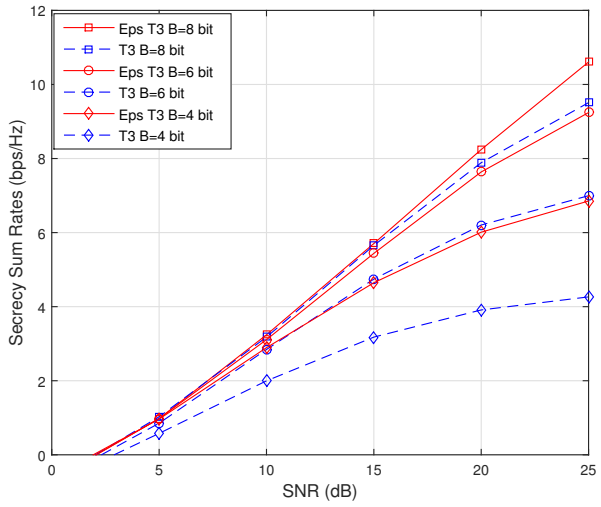

Fig. 5: The comparison between T3 criterion with and without proposed codebook at K=50 for different SNR values.

In Figure 7 , we compare the secrecy capacity for the system that perform semi-orthogonal selection having specific codebook and the system that schedules only one legitimate user with AN having optimal power allocation based on Figure 6. The performance results are shown that the proposed scheme provides much better secrecy capacity performance than single user case while having much less overhead.

VI. Conclusion

In this work, we have applied the semi orthogonal selection at legitimate users side for multiuser MISO systems with secrecy constraints. In practical systems, information regarding the eavesdropper is not possible to obtain at the

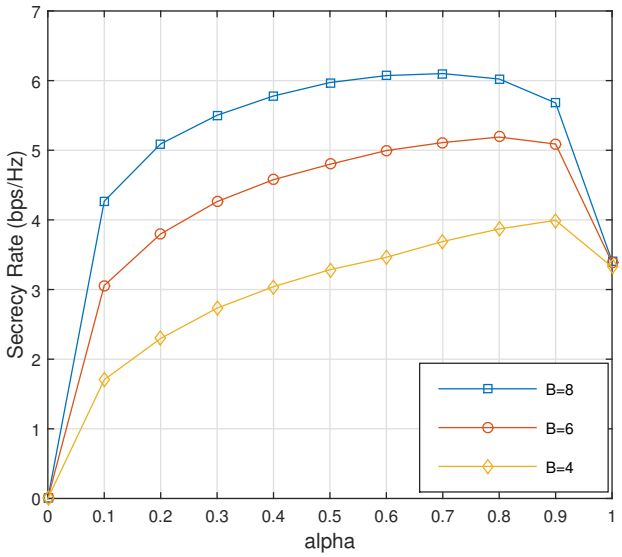

Fig. 6: Power allocation parameter for different number of bits in single user case at 20dB.

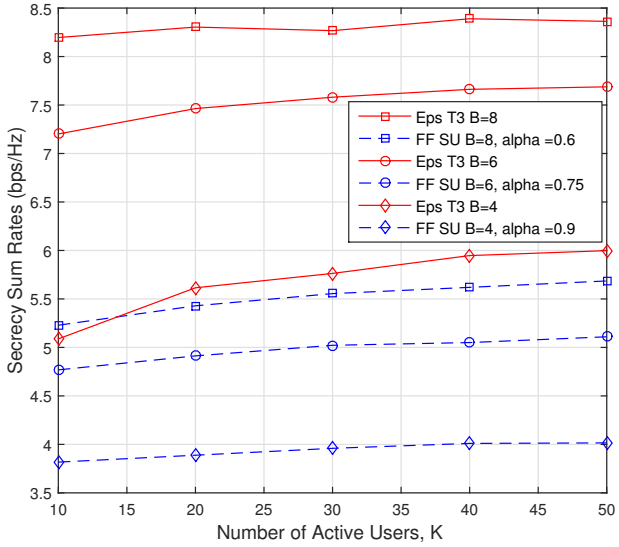

Fig. 7: The comparison between single user MISO with full feedback case and multiuser MISO with T3 with codebook desgin at SNR=20dB.

transmitter, since eavesdropper is passive, we consider the case that transmitter has no knowledge of eavesdropper CSI. Since CSI of Eve is unavailable at the transmitter, we have selected more than one legitimate user at the transmitter side to contrcut intersymbol interference under quantized feedback link to disrupt the reception of eavesdropper. By performing semi orthogonal selection, we have reduced the overhead through preventing the user having poor channel conditions to feedback their CSI. Besides that, we have employed specific

codebook thanks to the properties of semi orthogonal selection. We have illustrated that we have increased secrecy capacity significantly for low number of quantization bits, which leads to design robust physical layer security systems against to channel estimation errors.

ACKNOWLEDGMENT

This work has been carried out in the framework of TUBITAK 114E626 Project.

REFERENCES

[1] A. D. Wyner, The wire-tap channel, Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[2] S. Goel, R. Negi, Guaranteeing secrecy using artificial noise, IEEE Trans. Wireless Commun., vol. 7, no. 6, pp.2180-2189, June 2008.

[3] I. Csiszar and J. Korner, Broadcast channels with confidential messages, IEEE Trans. Inf. Theory, vol. 24, no. 3, pp. 339-348, May 1978.

[4] Y. Liang and H. V. Poor, Multiple-access channels with confidential messages, IEEE Trans. Inf. Theory, vol. 54, no. 3, pp. 976-1002, March 2008.

[5] A. Khisti, A. Tchamkerten, and G. W. Wornell, Secure broadcasting over fading channels, IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2453-2469, June 2008.

[6] Y. Liang, H. V. Poor, and S. Shamai, Secure communication over fading channels, IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2470-2492, June 2008.

[7] Z. Li,W. Trappe,R. Yates, Secret Communication via Multi-Antenna Transmission, 41st Annual Conference on Information Sciences and Systems, pp. 905-10, Baltimore, 2007.

[8] S. Shafiee and S. Ulukus, Achievable rates in Gaussian MISO channels with secrecy constraints, in IEEE ISIT, Nice, France, June 2007.

[9] S. Shafiee , N. Liu, and S. Ulukus, Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel, IEEE Trans. Inf. Theory, vol. 55, no. 9, pp. 4033-4039, Sep. 2009.

[10] X. Chen,R. Yin, Performance analysis for physical layer security in multi-antenna downlink networks with limited CSI feedback IEEE Wireless Communications letters, Vol. 2,No. 5,October 2013.

[11] G. Geraci,R. Couillet, J. Yuan, M. Debbah,I. B. Collings, Secrecy sum-rates with regularized channel inversion precoding under imperfect CSI at the transmitter, IEEE ICASSP, Vancouver, 2013.

[12] N. Li, X. Tao, J. Xu, Ergodic secrecy sum-rate for downlink multiuser MIMO systems with limited CSI feedback IEEE Communications letters, vol.18,No.6,June 2014.

[13] X. Chen, Y. Zhang, "Mode Selection in MU-MIMO downlink networks: a physical layer security perspective" IEEE Systems Journal,doi:10.1109/JSYST.2015.2413843,2015.

[14] B. Ozbek and D. Le Ruyet, Feedback strategies for wireless communication systems. Springer-Engineering Series Book, Springer Science Business Media New York, U.S.A, 2014.

[15] A. Narula, M. J. Lopez, M. D. Trott, G. W. Wornell, Efficient use of side information in multiple antenna data transmission over fading channels, IEEE Journal on Sel. Areas in Commun., pp.1423-1436, Oct. 1998.