Annals of Telecommunications (2018) 73:381–390
https://doi.org/10.1007/s12243-018-0627-6

Secure multiuser MISO communication systems with limited feedback link

Berna Özbek[1] · Özgecan Özdoğan Şenol[1] · Güneş Karabulut Kurt[2]

Received: 4 November 2016 / Accepted: 17 January 2018 / Published online: 3 February 2018

Abstract

Physical layer security is one of the promising techniques for the security of next-generation wireless systems. In this paper, we analyze the impact of the limited feedback link on the secrecy capacity for a system which includes a base station with multiple antennas, a single legitimate user selected from multiple active ones and multiple eavesdroppers. We propose to design a limited feedback link by reducing the feedback load and quantizing the channel state information (CSI) of legitimate users to establish a secure communication system. The feedback load is decreased with a self discrimination criterion at the legitimate users' side while keeping the secrecy capacity constant. The best legitimate user is selected based on the quantized CSI through a limited feedback link. We also analyze the impact of CSI of eavesdroppers, which information may or may not be available at transmitter. In practical cases where eavesdroppers are passive and their location is not known by the transmitter, an artificial noise is used to disrupt their reception. When the CSI of eavesdroppers is known, the generalized singular value decomposition is applied. We illustrate the performance results of the proposed limited feedback link through the availability of CSI of eavesdroppers at the transmitter.

Keywords Physical layer security · Reduced feedback link · Quantized feedback · Multiple antennas

1 Introduction

Security has become even more crucial issue due to the vulnerability of wireless networks to eavesdroppers' attacks. Traditionally, complex cryptographic methods are used for secure communications in the presence of illegitimate users. Rapid developments in computing technology require these solutions to be continually evolving. On the other hand, physical layer security techniques promise to achieve secrecy, even if an eavesdropper has an unlimited computational power. As a complementary security mechanism to cryptographic technologies at upper layers, the physical layer security solutions are implemented at the physical layer. In order to achieve both confidentiality and authentication, the physical layer security explores the random nature of the transmission media.

The basic framework of physical layer security, the *wiretap channel* model, was introduced by Wyner [1]. This model characterizes a point to point communication system under secrecy constraints. It consists of three nodes, the transmitter (Alice), the receiver (Bob), and the eavesdropper (Eve). In his pioneering work, Wyner has defined *secrecy capacity* as the maximum amount of information that can be reliably transmitted from the transmitter to the intended receiver. This work only considers a degraded broadcast channel. In subsequent studies, more general channel models have been analysed from the information point of view. In [2], the authors showed that it is possible to enable secure communications in non-degraded broadcast channels. Introduction of physical layer security in Gaussian channels [3], small-scale fading channels [4–6], multi-antenna channels[7–10], and relay channels [11, 12] have followed these works.

✉ Berna Özbek
bernaozbek@iyte.edu.tr

Özgecan Özdoğan Şenol
ozgecanozdogan@iyte.edu.tr

Güneş Karabulut Kurt
gkurt@itu.edu.tr

[1] Department of Electrical and Electronics Engineering, Izmir Institute of Technology, Izmir, Turkey

[2] Department of Electronics and Communication Engineering, Istanbul Technical University, Istanbul, Turkey

The studies on physical layer security mainly adopt the secrecy capacity as the performance metric. Multiple antennas and beamforming techniques can be employed to increase the secrecy capacity. The knowledge of Eve's channel state information (CSI) plays a critical role in determining the corresponding optimal beamforming scheme. In the literature, ergodic secrecy sum capacity for multiuser multiple input single output (MISO) has been investigated and closed form expressions have been provided according to the CSI availability of multiple Eve at the transmitter. For the case of CSI of multiple Eve is perfectly available at the transmitter, a generalized singular value decomposition (GSVD)-based precoding scheme has been presented in [10].

The presence of external passive Eve, where only statistical knowledge of Eve's CSI is available, has been discussed in [13]. The case of imperfect Eve's CSI case has been studied in [14] and [15]. In order to guarantee positive secrecy capacity without Eve's CSI at the transmitter, an artificial noise (AN) assisted beamforming has been presented in [16, 17]. In this method, information signal is masked with an AN signal, which is generated in the direction of legitimate user's null space. Thus, the reception of Eve is disrupted and the secrecy capacity is maximized with an optimum power allocation parameter. With perfect knowledge of CSI of the legitimate user, it is possible to achieve arbitrarily large secrecy capacity by increasing the transmit power. However, the assumption of perfect CSI at the transmitter is overly simplistic for practical applications. The quantized CSI of legitimate user through limited feedback link causes an AN leakage which degrades the capacity of legitimate user. Therefore, the secrecy capacity decreases under AN leakage [18].

In order to overcome the noise leakage problem and to increase the secrecy capacity, the number of bits for quantization of CSI should be increased. As the number of legitimate users increases, the total feedback load to send back quantized CSI to the base station becomes even larger. In the literature, the reduction of feedback load has not been examined for the secure MISO systems yet. In this paper, we propose to apply a threshold based user selection by using a self-discrimination criterion at legitimate users' side for the secure MISO systems with quantized CSI. The proposed method enables us to reduce the feedback load while keeping secrecy capacity constant. Besides, the noisy feedback link is also considered for the proposed secure scheme. Compared with the work in [19], we analyze a secure communications system including multiple eavesdroppers, which is a reasonably practical scenario since eavesdroppers may be more sophisticated devices than the legitimate users as examined in [20–23]. Moreover, we investigate the scenario in which the CSI of multiple Eve's is known at the transmitter in order to illustrate its impact on the overall secrecy capacity under a limited feedback link.

The rest of this paper is organized as follows. Section 2 describes the system model for the secure multiuser MISO systems for both passive eavesdroppers in which their CSI is not known at the transmitter and active eavesdroppers where their CSI is available at the transmitter. Section 3 presents a threshold based user selection including the quantization aspects. Section 4 gives the proposed secure communication system. Section 5 provides the performance evaluations and Section 6 gives the conclusion.

2 System model

We consider a multiuser MISO downlink system operating under a secrecy constraint. The wireless system consists of one base station with N_t antennas, K active legitimate users where each user has single antenna and N_e cooperating single antenna eavesdroppers. It is also worth to mention that N_e cooperating single antenna eavesdroppers that are dispersed geographically correspond to one eavesdropper with N_e antennas. In the rest of the paper, we will consider the system model including one Eve with N_e antennas. The aim of Alice is to send confidential messages to the intended Bob. In order to maximize the secrecy capacity, the user that has the highest channel gain, Bob, is selected from the set of active K users.

Since Eve may overhear the secret messages illegally, the message signal is masked with AN to disrupt the reception of Eve while guaranteeing secrecy. We assume that the CSI of legitimate users is perfectly estimated at the receiver side. Moreover, we assume that Alice may acquire the perfect or the quantized CSI of legitimate users depending on the considered scenario. In this section, eavesdroppers are passive and they do not reveal their location. Therefore, the transmitter has no knowledge regarding to Eve's CSI, which is a highly probable scenario in practical cases.

The transmitted signal vector $\mathbf{x}_k$ constructed under AN beamforming is expressed as,

$$\mathbf{x}_k = \mathbf{w}_k s_k + \mathbf{Q}_k \mathbf{a}_k \tag{1}$$

where s_k is the information-bearing signal with power $\mathbb{E}\left\{|s_k|^2\right\} \leq P_s$, $\mathbf{w}_k \in \mathcal{C}^{N_t \times 1}$ is the precoding vector at Alice and $\mathbb{E}\{\cdot\}$ denotes the expectation operator. Also, $\mathbf{a}_k = [a_1, a_2, \ldots, a_{N_t}]^T$ is the AN component which is a random Gaussian vector with power $\mathbb{E}\left\{||\mathbf{a}_k||^2\right\} \leq P_a$ and $\mathbf{Q}_k \in \mathcal{C}^{N_t \times N_t}$ is the AN beamformer with orthonormal columns that forms the AN subspace. The beamformers $\mathbf{w}_k$ and $\mathbf{Q}_k$ are determined through the available CSI of legitimate user at Alice.

P is the total transmit power, which is equal to sum of the information and AN signal power. Hence, $P_s = \alpha P$ and

$P_a = \frac{1-\alpha}{N_t-1}P$, where α is the power allocation parameter and its value changes between 0 and 1. As the α parameter increases, the power allocated to the information signal increases and the power of AN signal decreases. Thus, this power partitioning parameter affects the secrecy capacity. According to the availability of CSI of legitimate user at Alice (either perfect or quantized), the α parameter should be chosen to provide an optimum secrecy capacity.

The received signals at kth Bob and Eve are

$$y_k = \mathbf{h}_k^H \mathbf{w}_k s_k + \mathbf{h}_k^H \mathbf{Q}_k \mathbf{a}_k + n_k, \tag{2}$$

$$\mathbf{y}^e = \mathbf{H}^e \mathbf{w}_k s_k + \mathbf{H}^e \mathbf{Q}_k \mathbf{a}_k + \mathbf{n}^e, \tag{3}$$

respectively, where the channel vector of kth legitimate user is $\mathbf{h}_k \in \mathcal{C}^{N_t \times 1}$, the channel matrix of eavesdropper is denoted by $\mathbf{H}^e \in \mathcal{C}^{N_e \times N_t}$, n_k is the complex additive white Gaussian noise (AWGN) modelled by $\mathcal{CN}(0, \sigma^2)$ and each element of $\mathbf{n}^e$ represents complex AWGN on Eve's side with zero mean and variance σ_e^2.

The channel direction information (CDI) of $\mathbf{h}_k$ is expressed as,

$$\mathbf{g}_k = \frac{\mathbf{h}_k}{\|\mathbf{h}_k\|} \tag{4}$$

where $\|\mathbf{h}_k\|$ denotes the channel quality information (CQI), which is assumed to be known perfectly.

The precoding vector is determined by

$$\mathbf{w}_k = \mathbf{g}_k. \tag{5}$$

The columns of AN beamformer matrix, $\mathbf{Q}_k$, form an orthonormal basis for the null space of $\mathbf{g}_k$ defined by

$$\mathbf{g}_k^H \mathbf{Q}_k = 0_{1 \times N_t}. \tag{6}$$

Then, the achievable secrecy capacity with perfect CSI at Alice is given by

$$C = \left(\mathbb{E}\left\{\log_2\left(1 + SNR_k\right)\right\} - \mathbb{E}\left\{\log_2\left|\mathbf{I} + SNR^e\right|\right\}\right)^+ \tag{7}$$

where SNR_k and SNR^e denote the instantaneous signal-noise-ratio (SNR) belonging to the kth Bob and Eve, respectively. They are defined in [20] as

$$SNR_k = \alpha\gamma \|\mathbf{h}_k\|^2 \tag{8}$$

where $\gamma = \frac{P}{\sigma^2}$ is the average SNR of all legitimate users, and

$$SNR^e = \alpha(\mathbf{H}_e\mathbf{g}_k)(\mathbf{H}_e\mathbf{g}_k)^H \times \left(\frac{\sigma_e^2}{P}\mathbf{I} + \frac{(1-\alpha)}{N_t - 1}(\mathbf{H}_e\mathbf{Q}_k)(\mathbf{H}_e\mathbf{Q}_k)^H\right)^{-1}, \tag{9}$$

where the eavesdropper's noise variance, σ_e^2 is assumed to be unknown to the transmitter, hence it is set to zero. Therefore, we consider the worst case scenario in terms of the secrecy capacity.

2.1 Known eve's CSI at alice

We also consider the system model by focusing on the case that Alice has the knowledge of Eve's CSI. In contrast to the case that eavesdropper is hidden and Eve's CSI at Alice is not available, we assume that the eavesdropper channel is somehow detected and its CSI is obtained. This may not be the case in practice, since in general they are passive. Nevertheless, we examine the impact of Eve's CSI at Alice on the secrecy capacity and compare its performance with AN assisted beamforming.

The transmitted signal is formed based on GSVD [10] and the received signals at Bob and Eve are given respectively by

$$y_k = \mathbf{h}_k^H \mathbf{x}_k + n_k, \tag{10}$$

$$\mathbf{y}^e = \mathbf{H}^e \mathbf{x}_k + \mathbf{n}^e, \tag{11}$$

where $\mathbf{x}_k$ is the transmitted signal vector along direction Ψ_{max} and is defined by,

$$\mathbf{x}_k = \Psi_{max} s_k. \tag{12}$$

The power of transmitted signal is given by $\mathbb{E}\left\{||\mathbf{x}_k||^2\right\} = P$.

The secrecy capacity for the case of available Eve's CSI at Alice can be computed as [10]

$$C = \left\{\log_2(\lambda_{\max}(\mathbf{I} + P\mathbf{h}_k\mathbf{h}_k^H, \mathbf{I} + P(\mathbf{H}^e)^H\mathbf{H}^e))\right\}^+ \tag{13}$$

where $\lambda_{\max}$ denotes the largest generalized eigenvalue of its argument pair. It is determined by the maximum of the Rayleigh quotient by,

$$\lambda_{\max}(\mathbf{I} + P\mathbf{h}_k\mathbf{h}_k^H, \mathbf{I} + P(\mathbf{H}^e)^H\mathbf{H}^e) = \max_{\Psi \in C^{N_t}} \frac{\Psi^H(\mathbf{I} + P\mathbf{h}_k\mathbf{h}_k^H)\Psi}{\Psi^H(\mathbf{I} + P(\mathbf{H}^e)^H\mathbf{H}^e)\Psi}. \tag{14}$$

For implementation, the knowledge of $\mathbf{H}^e$ is required at Alice to find the corresponding generalized eigenvector Ψ_{max} and its maximum eigenvalue $\lambda_{\max}$. The direction of beamforming is determined along Ψ_{max}.

3 Threshold based legitimate user selection

In secure multiuser systems, the intended legitimate user can be scheduled according to the most favourable channel conditions to increase the secrecy capacity. The transmitter selects this user through available CSI at Alice. Generally, only quantized CSI is available at Alice due to the capacity limitations on the feedback channel. As the number of active legitimate users, K, increases, the feedback load also increases in multiuser multiantenna sytems. In order to reduce this feedback load while achieving the same secrecy capacity, we apply a threshold at the legitimate user side to determine the ones with poor channel conditions.

Accordingly, the legitimate users with a low channel gain should not take part in the user selection algorithm; hence, it is not required to feedback their CSI. Thus, only legitimate users above this threshold send their CSI to Alice.

The threshold based selection namely the $\mathcal{T}_1$ criterion applies a threshold, γ_{th}, and constructs a set $\mathcal{U}_1$ by selecting the legitimate users that satisfy the following threshold condition [24]

$$\mathcal{U}_1 = \left\{k' \in \{1, 2 \ldots, K\} : \|\mathbf{h}_{k'}\|^2 > \gamma_{th}\right\}. \tag{15}$$

The threshold value can be obtained either analytically or by numerically in order to guarantee an average number of users $\bar{K}$ that are fed back their instantaneous CSI to the base station,

$$\bar{K} = K\Pr\left\{k' \in \mathcal{U}_1\right\} = K\Pr\left\{\|\mathbf{h}_{k'}\|^2 > \gamma_{th}\right\}, \tag{16}$$

where $\Pr\{\cdot\}$ denotes probability expression.

The set of $\mathcal{U}_1$ is determined by the incomplete gamma function $\gamma(N_t, 1)$. This function can be bounded by [25][26]

$$\left[1 - \exp(-\beta\gamma))\right]^{N_t} \leq \int_0^{\gamma_{th}} f_\gamma(\gamma)d\gamma \leq \left[1 - \exp(-\gamma))\right]^{N_t}, \tag{17}$$

where $\beta = (N_t!)^{\frac{-1}{N_t}}$ and $f_\gamma(\gamma)$ is the probability density function with $\chi^2_{2N_t}$.

Then, we can obtain the probability to select legitimate user k' in $\mathcal{U}_1$ as

$$\Pr\left\{k' \in \mathcal{U}_1\right\} = \sum_{b=0}^{N_t-1} \frac{\exp(-\gamma_{th})(\gamma_{th})^b}{b!} \tag{18}$$

Thus, the average number of legitimate users that are fed back their CSI to Alice can be determined by

$$\bar{K} = K \sum_{b=0}^{N_t-1} \frac{\exp(-\gamma_{th})(\gamma_{th})^b}{b!}. \tag{19}$$

For the secure MISO systems, in which the average SNR of all legitimate users are the same, the intended legitimate user is selected at Alice as,

$$k = \arg\max_{k' \in \mathcal{U}_1} \|\mathbf{h}_{k'}\|^2. \tag{20}$$

3.1 Secrecy capacity with quantized feedback link

Each user satisfying the $\mathcal{T}_1$ criterion chooses a codeword to quantize its CDI, $\mathbf{g}_k$ to a unit norm vector $\hat{\mathbf{g}}_k$ selected from a predetermined codebook with a size of 2^B where B is the number of quantization bits. Random vector quantization (RVQ) codebook $\mathbf{C}_k$ is adopted with $\mathbf{C}_k = \left\{\hat{\mathbf{g}}_{k_1}, \hat{\mathbf{g}}_{k_2}, \ldots, \hat{\mathbf{g}}_{k_i}, \ldots, \hat{\mathbf{g}}_{2^B}\right\}$. An optimal codeword to quantize kth CDI is chosen by

$$k_i = \arg\max_{1 \leq i \leq 2^B} \left|\mathbf{g}_k^H \hat{\mathbf{g}}_{k_i}\right|. \tag{21}$$

After selecting the codebook index, each Bob is fed back its CDI to Alice in B bits. A quantization error arises because of the limited feedback link. The relation between perfect CDI $\mathbf{g}_k$, and the codeword $\hat{\mathbf{g}}_k = \hat{\mathbf{g}}_{k_i}$ is given as

$$\mathbf{g}_k = \hat{\mathbf{g}}_k \cos\theta_k + \mathbf{g}_k^\perp \sin\theta_k, \tag{22}$$

where $\mathbf{g}_k^\perp$ is a unit norm vector orthogonal to $\hat{\mathbf{g}}_k$, $\theta_k = \angle(\mathbf{g}_k, \hat{\mathbf{g}}_k)$ and the quantization error follows $\frac{N_t-1}{N_t}\delta \leq \mathbb{E}\{\sin\theta_k\} \leq \delta$ with $\delta = 2^{\frac{-B}{N_t-1}}$ [27].

In the case of quantized CDI, the transmitted signal when the CSI of Eve is not available at Alice can be denoted as

$$\mathbf{x}_k = \hat{\mathbf{w}}_k s_k + \hat{\mathbf{Q}}_k \mathbf{a}_k, \tag{23}$$

where the precoding vector is obtained though quantized CDI by,

$$\hat{\mathbf{w}}_k = \hat{\mathbf{g}}_k, \tag{24}$$

and the quantized version of AN beamformer matrix is determined by,

$$\hat{\mathbf{g}}_k^H \hat{\mathbf{Q}}_k = 0_{1\times N_t}. \tag{25}$$

Then, the received signals at the legitimate receiver and eavesdropper can be written as

$$y_k = ||\mathbf{h}_k||(\mathbf{g}_k{}^H \hat{\mathbf{g}}_k)s_k + ||\mathbf{h}_k||(\mathbf{g}_k^H \hat{\mathbf{Q}}_k)\mathbf{a}_k + n_k, \tag{26}$$

and

$$\mathbf{y}^e = \mathbf{H}^e \hat{\mathbf{g}}_k s_k + \mathbf{H}^e \hat{\mathbf{Q}}_k \mathbf{a}_k + \mathbf{n}^e, \tag{27}$$

respectively.

Thus, the secrecy capacity with quantized CSI at the transmitter is given by

$$C^q = \left(\mathbb{E}\left\{\log_2\left(1 + S\hat{N}R_k\right)\right\} - \mathbb{E}\left\{\log_2\left|\mathbf{I} + S\hat{N}R^e\right|\right\}\right)^+ \tag{28}$$

where $S\hat{N}R_k$ and $S\hat{N}R^e$ are instantaneous SNR values for kth legitimate user and eavesdropper, respectively through a limited feedback link.

The SNR value at kth Bob under quantized CSI can be expressed by

$$S\hat{N}R_k = \frac{\alpha||\mathbf{h}_k||^2|\mathbf{g}_k{}^H\hat{\mathbf{g}}_k|^2}{\frac{1-\alpha}{N_t-1}||\mathbf{h}_k||^2||\mathbf{g}_k{}^H\hat{\mathbf{Q}}_k||^2 + \frac{1}{\gamma}}. \tag{29}$$

A measure of the alignment of the quantized CDI with the exact CDI can be denoted by $\cos^2(\theta_k) = |\mathbf{g}_k{}^H\hat{\mathbf{g}}_k|^2$. Besides, we can use the fact that $|\mathbf{g}_k{}^H\hat{\mathbf{Q}}_k|^2 = 1 - |\mathbf{g}_k{}^H\hat{\mathbf{g}}_k|^2 = \sin^2(\theta_k)$ [18].

Then, the SNR of the kth legitimate user under quantized CDI can be re-written by

$$S\hat{N}R_k = \frac{\alpha||\mathbf{h}_k||^2\cos^2(\theta_k)}{\frac{1-\alpha}{N_t-1}||\mathbf{h}_k||^2\sin^2(\theta_k)+\frac{1}{\gamma}}. \quad (30)$$

The SNR value at Eve under quantized feedback link can be written as

$$S\hat{N}R^e = \alpha(\mathbf{H}^e\hat{\mathbf{g}}_k)(\mathbf{H}^e\hat{\mathbf{g}}_k)^H\left(\frac{1-\alpha}{N_t-1}(\mathbf{H}^e\hat{\mathbf{Q}}_k)(\mathbf{H}^e\hat{\mathbf{Q}}_k)^H\right)^{-1}. \quad (31)$$

In contrast to the case where Alice has perfect CSI of legitimate user, the quantized CDI causes an AN leakage. The noise that leaks from the intended legitimate user's null space, $|\mathbf{g}_k{}^H\hat{\mathbf{Q}}_k|^2 = \sin^2(\theta_k)$, decreases the secrecy capacity. Even when γ goes to infinity, the secrecy capacity in Eq. 28 converges to a constant value as

$$C^q = \left(\mathbb{E}\left\{\log_2\left(1+\frac{\alpha\cos^2(\theta_k)}{\frac{1-\alpha}{N_t-1}\sin^2(\theta_k)}\right) - \log_2\left|\mathbf{I}+S\hat{N}R^e\right|\right\}\right)^+. \quad (32)$$

In the case of the CSI of Eve is available at the transmitter through quantized feedback link, the quantized versions of $\mathbf{h}_k$ and $\mathbf{H}^e$ which are denoted by $\hat{\mathbf{h}}_k$ and $\hat{\mathbf{H}}^e$ are present at Alice, respectively. Thus, the direction of beamforming,$\hat{\Psi}_{max}$, is not along the exact one due to the quantization error and this fact causes a secrecy degradation.

The secrecy capacity under quantized CSI of both Eve and Bob is given by

$$C^q = \left\{\log(\hat{\lambda}_{\max}(\mathbf{I}+P\hat{\mathbf{h}}_k\hat{\mathbf{h}}_k^H, \mathbf{I}+P(\hat{\mathbf{H}}^e)^H\hat{\mathbf{H}}^e))\right\}^+, \quad (33)$$

where

$$\hat{\lambda}_{\max}(\mathbf{I}+P\hat{\mathbf{h}}_k\hat{\mathbf{h}}_k^H, \mathbf{I}+P(\hat{\mathbf{H}}^e)^H\hat{\mathbf{H}}^e) = \max_{\hat{\Psi}\in C^{N_t}}\frac{\hat{\Psi}^H(\mathbf{I}+P\hat{\mathbf{h}}_k\hat{\mathbf{h}}_k^H)\hat{\Psi}}{\hat{\Psi}^H(\mathbf{I}+P(\hat{\mathbf{H}}^e)^H\hat{\mathbf{H}}^e)\hat{\Psi}}. \quad (34)$$

4 The proposed secure communication system

In the proposed secure communications system, firstly, at the receiver side, each legitimate user applies the $\mathcal{T}_1$ criterion based on the threshold value γ_{th} known by both the transmitter and the receivers, which does not request an additional overhead. Then, only legitimate users whose channel gains are higher than a given threshold are considered. This reduces the computational complexity compared to the full feedback case where all legitimate users are quantized their CSI. After that, in the proposed scheme, the $\bar{K}$, legitimate users are fed back their corresponding codebook indexes, which reduces the signaling overhead significantly compared the full feedback case where all legitimate users, K are fed back their CSI. As a result, the computational complexity and signaling overhead are decreased since only a reduced set of legitimate users are quantized their CSI and fed back them to the transmitter.

A pseudocode of the proposed secure communications system by employing reduced and quantized feedback is summarized in Algorithm 1.

Algorithm 1 The proposed secure communications through a limited feedback link

for $k' = 1 : K$ **do**
  At k'**th Bob :**
  Input: Its CQI $\|\mathbf{h}_{k'}\|$ and its CDI, $\mathbf{g}_{k'}$.
  Apply $\mathcal{T}_1$ criterion:
  if $\|\mathbf{h}_{k'}\|^2 > \gamma_{th}$ **then**
    Quantize its CDI as in Eq. (21) using its corresponding codebook.
  end if
  Output: The index of the quantized CDI, k'_i.
end for
At Alice:
Input: The indexes k'_i and $\hat{\mathbf{H}}^e$ for the case of the CSI of Eve is available.
-Construct $\mathcal{U}_1$ consisting the indexes of selected legitimate users which are fed back their CDI.
- For $k' \in \mathcal{U}_1$, obtain the perfect CQI, $\|\mathbf{h}_{k'}\|$ and the quantized CDI, $\hat{\mathbf{g}}_{k'}$, through k'_i using its corresponding codebook.
-Schedule Bob as in Eq. (20).
if CSI of Eve is available **then**
  Provide the beamformer direction $\hat{\Psi}_{max}$ as in Eq. (34).
else
  Determine the precoding vector as in Eq. (24) and AN beamformer as in Eq. (25).
end if
Output: Either $\hat{\mathbf{w}}_k$ and $\hat{\mathbf{Q}}_k$ or $\hat{\Psi}_{max}$.

5 Performance evaluations

In this section, we present simulation results by setting the number of transmitter antennas as $N_t = 4$ at Alice. We assume that all legitimate users have the same average SNR values and the fading effect is modeled by Rayleigh distribution.

The threshold value of the $\mathcal{T}_1$ criterion is adjusted analytically to get average number of users that are fed back their CSI to the transmitter as $\bar{K} = 4$. For the number of

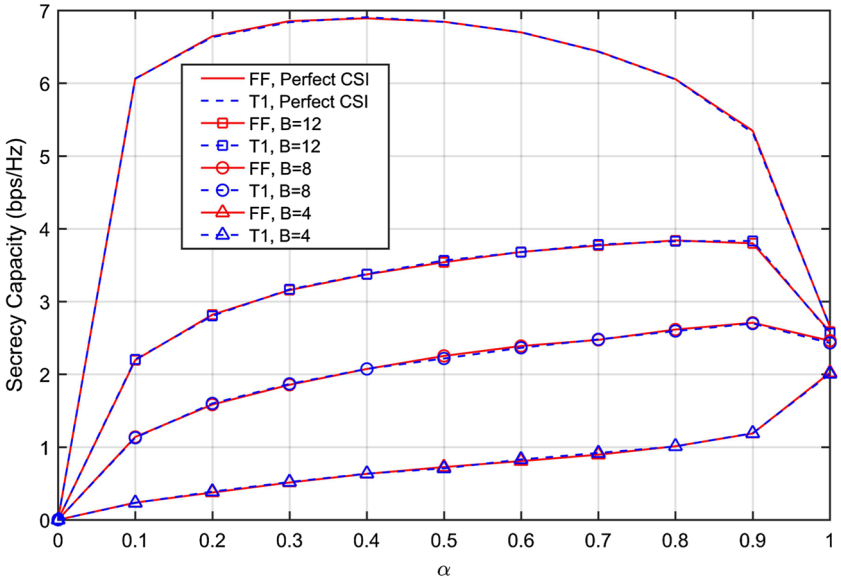

Fig. 1 Secrecy capacity versus α for different number of quantization bits in the case that Eve's CSI is unknown at Alice and $N_e = 2$, $K = 50$, $\gamma = 20$dB

active legitimate users given by $K = [10, 20, 30, 40, 50]$, the corresponding threshold values are determined as $\gamma_{th} = [4.15, 5.5, 6.2, 6.67, 7.0]$. According to these threshold values, the set of $\mathcal{U}_1$ is constructed and legitimate users in this set are fed back their quantized CSI to Alice by employing RVQ in B bits. For $B = 12$ and $K = 50$, the total feedback load is $50 \times 12 = 600$ bits per channel use for the full feedback case. If the $\mathcal{T}_1$ criterion is employed, only 4 users on average are fed back their CSI to Alice and total feedback load reduces to $4 \times 12 = 48$ bits per channel use.

Figure 1 shows the optimal power allocation parameters considering different number of feedback bits for the full feedback (FF) case, where all users are fed back their CSI to Alice and the $\mathcal{T}_1$ criterion. When Eve's CSI is not available at Alice, a portion of the power should be dedicated for AN to interrupt reception of Eve. The optimal power allocation parameter, α depends on the CSI of the legitimate users. If the feedback bits are sufficiently large, the optimal value is calculated by $\alpha = \frac{\sqrt{1}}{\sqrt{1}+\sqrt{Ne}}$ [20]. Then, the parameter α is calculated as 0.414 for $N_e = 2$. However, as the number of quantization bits reduces, less power should be allocated to AN signal in order to prevent severe AN leakage such that α converges to 1. It is also observed that the $\mathcal{T}_1$ criterion does not cause a secrecy capacity degradation compared to the full feedback case while providing a reduction on feedback load which varies between $60\% - 92\%$ depending on the active number legitimate users K.

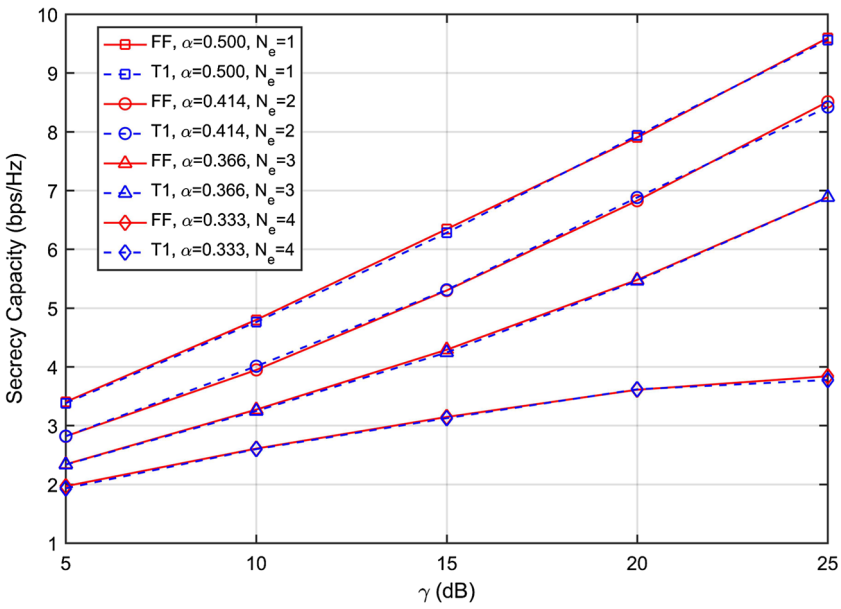

Fig. 2 Secrecy capacity versus SNR for different values of N_e in the case of unknown ECSIT and perfect Bob's CSI at Alice for $K = 50$

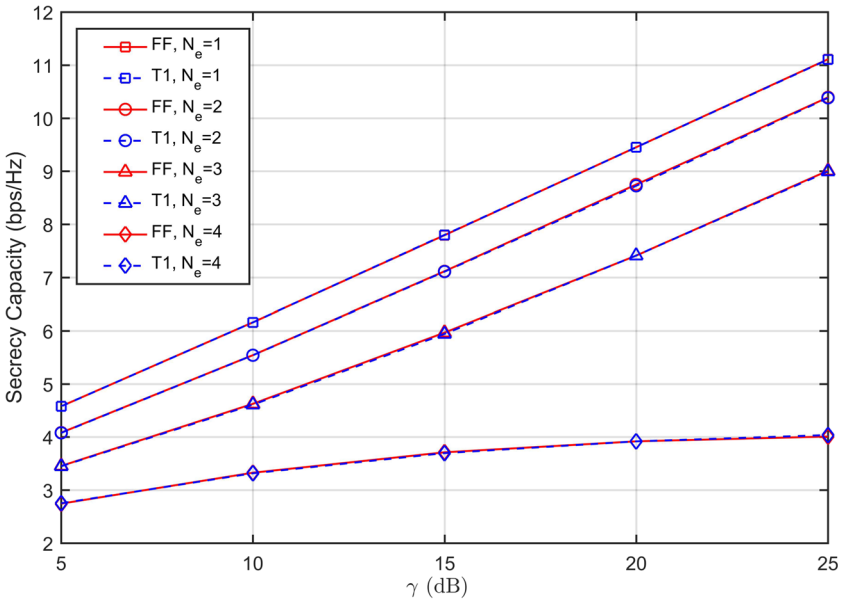

Fig. 3 Secrecy capacity versus SNR for N_e in the case of perfect ECSIT and perfect Bob's CSI at Alice for $K = 50$

In Figs. 2 and 3, for the case of perfect CSI of legitimate users are available at Alice, the effect of the number of antennas at Eve is analyzed for both Eve's CSI is not available (unknown ECSIT) and is known at Alice (known ECSIT) perfectly, respectively. For the unknown ECSIT scenario, the optimal α values are used to maximize the secrecy capacity based on the performance results in Fig. 1. As observed from the results, the secrecy capacity is not bounded and can be increased with SNR for $N_t \geq N_e + 1$. Besides, the gain on secrecy capacity compared to known and unknown ECSIT is given about 1.5 bps/Hz when the number of Eve's antennas is less than the number of antennas at Alice.

In Fig. 4, the secrecy capacity is illustrated for different number of quantization bits for the CSI of both legitimate users and Eve through a limited feedback link. According to the results, an increment in SNR causes a loss in the secrecy capacity since Eve has more antennas than the intended user and beamforming is no longer in the optimal direction. This situation is in sharp contrast to the case of the perfect CSI. In Fig. 5, the secrecy capacity for different number of quantization bits for the CSI of legitimate user

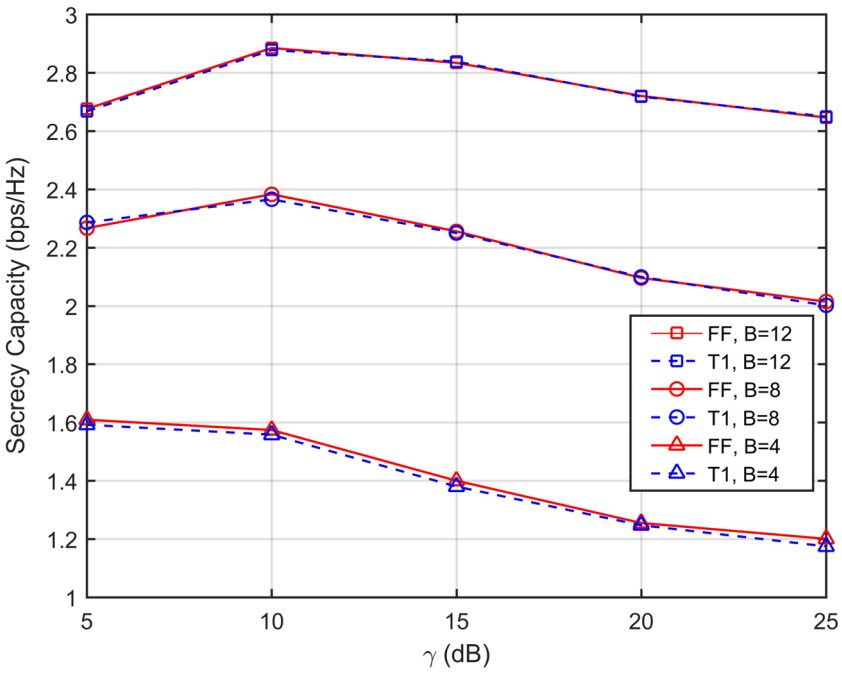

Fig. 4 Secrecy capacity versus SNR in the case of quantized ECSIT and quantized Bob's CSI at Alice for $N_e = 2$, $K = 50$

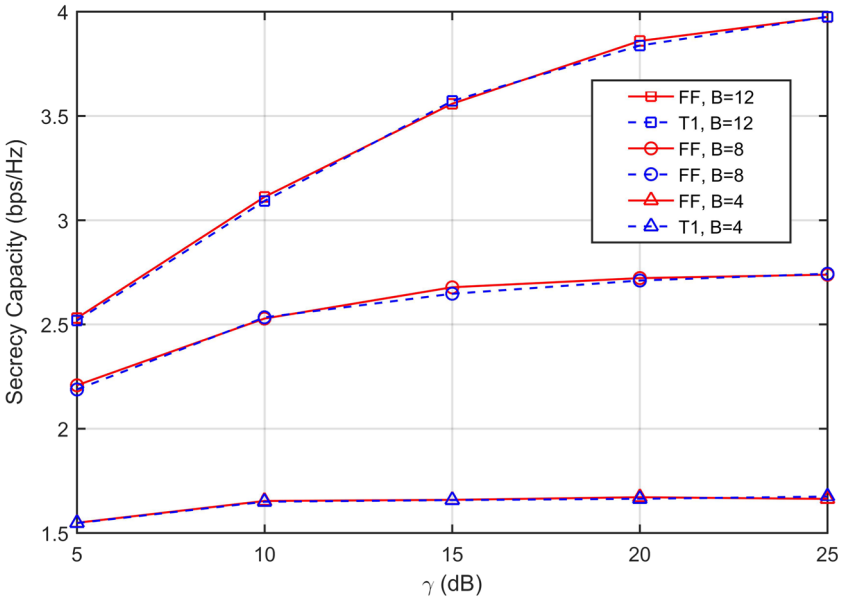

Fig. 5 Secrecy capacity versus SNR in the case of unknown ECSIT and quantized Bob's CSI at Alice for $N_e = 2$, $\alpha = 0.8$, $K = 50$.

is illustrated when Eve's CSI is unknown at Alice. When the number of quantization bits is increased, the gain on the secrecy capacity is also increased since the leakage to Eve is reduced. It shows that if the number of quantization bits is adequately chosen, it is possible to provide secrecy gain with SNR increment in contrast to quantized ECSIT case.

In Fig. 6, we compare the secrecy capacity for the case of known ECSIT and unknown ECSIT by employing the full feedback case and the $\mathcal{T}_1$ criterion through the limited feedback link. When both Bob's CSI and Eve's CSI are perfectly known at Alice, the eavesdropper is not allowed to infer any information. However, the feedback channel is limited and the quantized CSI is available at Alice in practical systems. When the quantized Eve's CSI and quantized Bob's CSI are available at Alice, the secrecy capacity is lower than the case of unknown Eve's CSI. The case of the quantized Bob's CSI and unknown Eve's CSI at Alice provides about 1.5 bps/Hz gain on the secrecy capacity compared the quantized Eve's CSI is available at Alice for both the full feedback case and the $\mathcal{T}_1$ criterion.

In Fig. 7, the secrecy capacity performance under the noisy feedback link is illustrated for both the full feedback case and the $\mathcal{T}_1$ algorithm. According to the results, the loss on the secrecy capacity is only about 0.4 bps/Hz under a severe feedback channel condition.

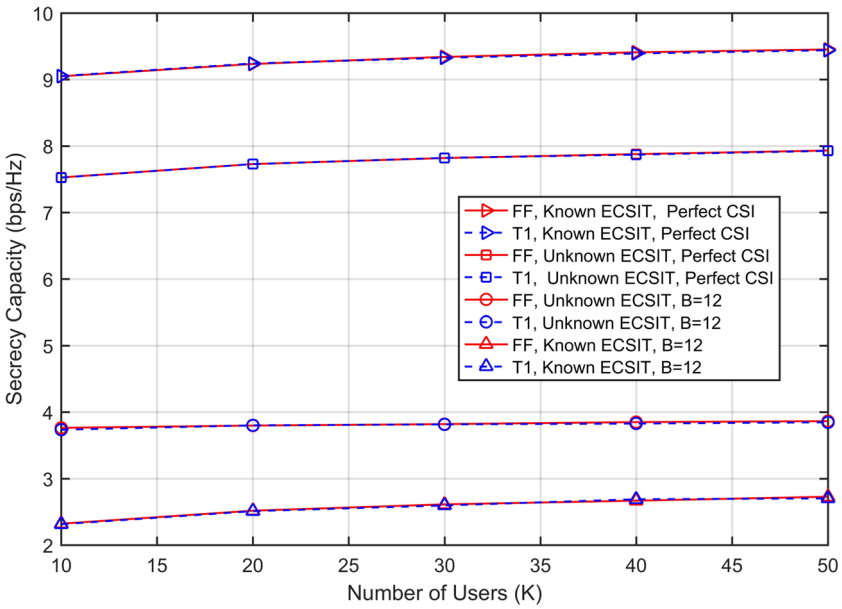

Fig. 6 Secrecy capacity versus K for different availability of CSI for $\gamma = 20$dB

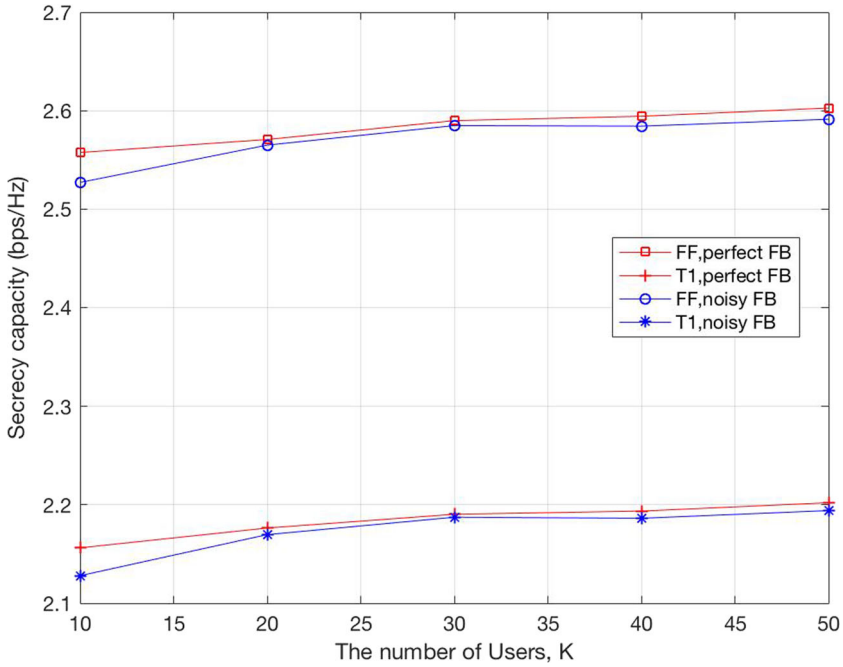

Fig. 7 Secrecy capacity versus K under a noisy feedback link for $\gamma = 20$dB, $B = 8$, $\gamma_{UL} = 0$dB

6 Conclusion

In this paper, we have applied the threshold-based legitimate user selection for the multiuser MISO systems having multiple antennas eavesdropper under secrecy constraints while reducing the feedback load. We have considered different availability cases of Eve's CSI at Alice and the quantized CSI of legitimate users in order to analyze the impact the limited feedback link on the secrecy capacity. It has been shown that the proposed limited feedback link achieves the same secrecy capacity as the full feedback scheme for all considered cases. The availability of quantized Eve's CSI at Alice has not provide any gain on the secrecy capacity compared to the unknown case which is most suitable for practical applications. The proposed secure multiuser MISO system though the limited feedback link is compatible with the existing wireless communications systems since it does not require additional overhead.

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

References

1. Wyner AD (1975) The wire-tap channel. Bell Syst Techn J 54(8):1355–1387
2. Csiszar I, Korner J (1978) Broadcast channels with confidential messages. IEEE Trans Inf Theory 24(3):339–348
3. Leung-Yan-Cheong S, Hellman M (1978) The Gaussian wire-tap channel. IEEE Trans Inf Theory 24(4):451–456
4. Gopala PK, Lai L, El Gamal H (2008) On the secrecy capacity of fading channels. IEEE Trans Inf Theory 54(10):4687–4698
5. Liang Y, Poor HV, Shamai S (2008) Secure communication over fading channels. IEEE Trans Inf Theory 54(6):2470–2492
6. Khisti A, Tchamkerten A, Wornell GW (2008) Secure broadcasting over fading channels. IEEE transactions on information theory 54(6):2453–2469
7. Parada P, Blahut R Secrecy capacity of SIMO and slow fading channels. Proceedings. International Symposium on Information Theory, 2005. ISIT 2005. Adelaide, SA, 2005, pp
8. Li Z, Trappe W, Yates R (2007) Secret Communication via Multi-antenna Transmission, 2007 41st Annual Conference on Information Sciences and Systems, Baltimore, pp 905–910
9. Shafiee S, Ulukus S (2007) Achievable Rates in Gaussian MISO Channels with Secrecy Constraints, 2007 IEEE International Symposium on Information Theory, Nice, pp 2466–2470
10. Khisti A, Wornell GW (2010) Secure transmission with multiple antennas I: The MISOME wiretap channel. IEEE Trans Inf Theory 56(7):3088–3104
11. Lai L, El Gamal H (2008) The relay–eavesdropper channel: Cooperation for secrecy. IEEE Trans Inf Theory 54(9):4005–4019
12. Dong L, Han Z, Petropulu AP, Poor HV (2010) Improving wireless physical layer security via cooperating relays. IEEE Trans Signal Process 58(3):1875–1888
13. Chen X, Yin R (2013) Performance analysis for physical layer security in multi-antenna downlink networks with limited CSI Feedback. IEEE Wirel Commun Lett 2(5):503–506
14. Geraci G, Couillet R, Yuan J, Debbah M, Collings IB (2013) Secrecy sum-rates with regularized channel inversion precoding under imperfect CSI at the transmitter, 2013 IEEE International Conference on Acoustics, Speech and Signal Processing, Vancouver, pp 2896–2900
15. Li N, Tao X, Xu J (2014) Ergodic Secrecy Sum-Rate for Downlink Multiuser MIMO Systems With Limited CSI Feedback. IEEE Commun Lett 18(6):969–972
16. Negi R, Goel S (2005) Secret communication using artificial noise, VTC-2005-Fall. 2005 IEEE 62nd Vehicular Technology Conference, pp 1906–1910

17. Goel S, Negi R (2008) Guaranteeing secrecy using artificial noise. IEEE Trans Wirel Commun 7(6):2180–2189
18. Lin SC, Chang TH, Liang YL, Hong YWP, Chi CY (2011) On the impact of quantized channel feedback in guaranteeing secrecy with artificial noise: the noise leakage problem. IEEE Trans Wirel Commun 10(3):901–915
19. Ozdogan O, Ozbek B, Kurt GK (2016) Performance of secure multiuser MISO systems with threshold based user selection, 2016 24th Signal Processing and Communication Application Conference (SIU), Zonguldak, pp 721–724
20. Li N, Tao X, Wu H, Xu J, Cui Q (2016) Large-system analysis of artificial-noise-assisted communication in the multiuser downlink: Ergodic secrecy sum rate and optimal power allocation. IEEE Trans Veh Technol 65(9):7036–7050
21. Deng H, Wang HM, Liu C, Wang W (2015) Performance Analysis of Linear Precoding for Secure Multiuser MIMO Systems with a Multiple-Antenna Eavesdropper, 2015 IEEE Global Communications Conference (GLOBECOM), San Diego, pp 1–6
22. Mo R, Yuen C, Zhang J, Chen X (2016) Beamforming design for secure downlink transmission of MU-MIMO systems with multi-antenna eavesdropper, 2016 IEEE International Conference on Communications (ICC), Kuala Lumpur, pp 1–6
23. Yang N, Elkashlan M, Duong TQ, Yuan J, Malaney R (2016) Optimal Transmission With Artificial Noise in MISOME Wiretap Channels. IEEE Trans Veh Technol 65(4):2170–2181
24. Gesbert D, Alouini MS (2004) How much feedback is multi-user diversity really worth?. 2004 IEEE International Conference on Communications, Paris, pp 234–238
25. Sharif M, Hassibi B (2005) On the capacity of MIMO broadcast channels with partial side information. IEEE Trans Inf Theory 51(2):506–522
26. Huang K, Heath RW Jr., Andrews JG (2007) SDMA with a sum feedback rate constraint. IEEE Transactions on Signal Processing 55:3879–3891
27. Jindal N (2005) MIMO broadcast channels with finite rate feedback, GLOBECOM '05. IEEE Global Telecommunications Conference, pp 5