Physical Communication 37 (2019) 100863

Contents lists available at ScienceDirect

Physical Communication

journal homepage: www.elsevier.com/locate/phycom

Full length article

Secure multiuser MIMO communication systems with imperfect channel state information

Berna Özbek [a,*], Özgecan Özdogan Şenol [a], Güneş Karabulut Kurt [b]

[a] Department of Electrical and Electronics Engineering, Izmir Institute of Technology, Izmir, Turkey
[b] Wireless Communications Research Laboratory, Istanbul Technical University, Istanbul, Turkey

ARTICLE INFO

Article history:
Received 23 December 2018
Received in revised form 2 August 2019
Accepted 20 September 2019
Available online 3 October 2019

Keywords:
Secure communications
Multiuser MIMO

ABSTRACT

In this paper, we propose a secure wireless communications system through a multiple input multiple output (MIMO) channel which includes a multiple antenna base station and multiple single antenna legitimate users that are overheard by a multiple antenna eavesdropper. By assuming that the eavesdropper's channel is unknown by the base station, an artificial noise beamforming is used to prevent this eavesdropper to decode legitimate users' message in the downlink. Additionally, the base station has only imperfect channel state information (CSI) of legitimate users which is the practically relevant case. Under the condition of imperfect CSI, a noise leakage on legitimate users' signal is occurred and it degrades the achievable average secrecy sum rate. In order to reduce this noise leakage, the semi-orthogonal selection having a rotated codebook is proposed to establish a secure communications link. We demonstrate the average secrecy sum rate results of the proposed algorithm for secure multiuser MIMO systems under imperfect CSI through extensive simulation results.

1. Introduction

The fundamental characteristics of wireless medium complicates to achieve secure communications in the presence of unauthorized receivers. In the existing communication systems, these security tasks are mostly addressed by the upper layers of network protocols with conventional complexity based on cryptographic methods. As a complementary solution to these traditional cryptographic techniques, physical layer (PHY) security methods use the characteristics of wireless channels to enable secure wireless communications. The aim of PHY is to limit the amount of information that can be extracted by any unauthorized user (i.e., eavesdroppers) via utilizing inherent randomness of wireless communication channels. Additionally, the design of PHY security schemes is not based on the assumption that an eavesdropper has limited computational power, contrary to the traditional methods. In fact, the eavesdropper may have infinite computational power. Nevertheless, secure communication can be achieved by the combination of appropriate coding and transmit precoding design.

Multiple antenna techniques are extensively studied in PHY security configurations due to their potential of enhancing average secrecy rate [1–4]. Since eavesdroppers may have more sophisticated devices (i.e., multiple antennas) than legitimate users, employing multiple antennas at the base station (BS) enables to achieve additional degrees of freedom that can be used against them. Multiple antenna eavesdroppers can either monitor the channel listen individually (non-colluding case) or they can share their observations to be more effective (colluding case) [5–8]. The distinction of these adversarial models is important since the colluding case corresponds to increased sophistication, thus more powerful adversaries.

Among various PHY techniques reported in the literature, multiple antenna techniques may be among the most effective methods in improving secrecy capacity. However, their success almost completely depends on the availability of channel state information (CSI) at the transmitter [9], by reason that the BS designs the beamformer according to the present CSI. In practical communication systems, it is hard to acquire even legitimate user's CSI perfectly, since the feedback channel is rate-limited. In order to provide legitimate users' CSI at transmitter, the receiver estimates and sends its quantized CSI back to the transmitter. It is not possible to send the perfect CSI back to transmitter since it requires infinite amount of bandwidth. Thus, the BS is constrained to interpret the available imperfect CSI. In [10], the transmit antenna selection and maximum ratio combining schemes have been examined for multiple input multiple output single user secure communications systems under imperfect CSI.

In order to reach high secrecy rates, proper beamforming schemes should be utilized. The beamforming technique with employing artificial noise (AN) has been examined in [11,12] in

* Corresponding author.
E-mail addresses: bernaozbek@iyte.edu.tr (B. Özbek), ozgecanozdogan@iyte.edu.tr (Ö. Özdogan Şenol), gkurt@itu.edu.tr (G. Karabulut Kurt).

https://doi.org/10.1016/j.phycom.2019.100863
1874-4907/

order to protect the information signal from any potential eavesdropper. It is based on a practical assumption that eavesdroppers are passive and it is not possible to extract their locations. Hence, the transmitter cannot acquire the CSI of eavesdroppers [13,14]. In this method, the AN signal is injected in the direction of legitimate user's null space to ensure that they are not affected by this AN. If the CSI of intended users are perfectly available at the BS then, it can inject AN into the null space of legitimate users' channel to avoid affecting their transmissions. Therefore, a portion of transmit power is allocated to the AN. However, we are interested in the case where legitimate users also receive partial AN because of the imperfect channel state information through the channel estimation error and the quantized channel. This case is referred as the AN leakage problem [15]. In this work, we aim to mitigate the AN leakage on intended users' signal that may severely reduce the secrecy rate for the scenario that multiple legitimate users are employed in the secure wireless system.

In order to increase the secrecy rate and to overcome the noise leakage problem, a large number of quantization bits should be used. As the number of employed antennas increases, the total feedback load becomes even larger with the use of codebooks to quantize CSI. Codebook based transmission schemes that the receiver sends back only the index of the optimum beamformer by a few bits has been commonly adopted in practice [16,17]. Codebook based transmission in PHY security settings have been studied in [18,19].

In order to improve the physical layer security, a resource allocation under the presence of an active eavesdropper has been presented in [20,21]. In this paper, we focus on the system model including passive eavesdroppers.

In [22], we have considered a secure multiple antenna system with only one eavesdropper by allocating multiple legitimate users. We have shown that reception of the eavesdropper is disrupted by inter-user interference. In [23], only one legitimate user has been scheduled by employing a threshold-based legitimate user selection for the secure system with multiple antennas at the BS and eavesdropper. Through extensive performance evaluations, it has been illustrated that the same secrecy rate is achieved as the full feedback scheme. In this paper, a secure multiuser multiple input multiple output (MIMO) is considered by allocating more than one legitimate users and the colluding eavesdroppers that are able to eliminate inter-user interference. A semi-orthogonal selection with rotated codebook to reduce quantization error for a secure multiuser MIMO communications system is presented to increase secrecy rate. In the literature, the reduction of feedback load has not been examined for the secure multiuser MIMO systems yet.

The paper is structured as follows. Section 2 gives the system model for a secure multiuser MIMO system. Section 3 explains a semi-orthogonal criterion with a rotated codebook in detail. Section 4 presents the proposed secure communications for multiuser MIMO systems. Section 5 examines the performance evaluations. Finally, Section 6 gives the conclusions.

2. System model

In this paper, a secure multiuser MIMO downlink system operating under secrecy constraint is examined as illustrated in Fig. 1. The system consists of a BS with N_t antennas, K single antenna legitimate users and an eavesdropper with N_e antennas. One eavesdropper with N_e antennas corresponds to N_e colluding single antenna eavesdroppers that are dispersed geographically. The M legitimate users are selected for the secure communication from the set κ which contains all of the K active legitimate users with $N_t > M$. Then, the BS sends confidential messages to the intended M legitimate users while the eavesdropper overhears the secret

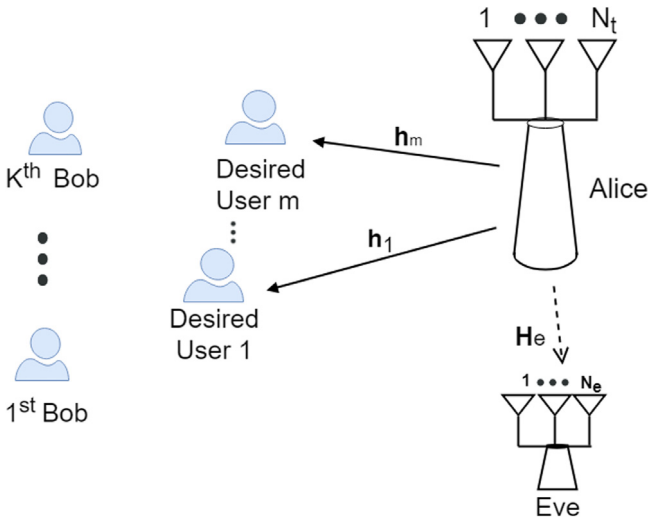

Fig. 1. Secure multiuser MIMO system model.

messages. At the legitimate users' side, the semi-orthogonal user selection criterion is applied to reduce the leakage to the eavesdropper. For the channel estimation, the legitimate users use pilot signals transmitted by the BS. Then, they apply quantization and are fed back the corresponding indexes of their CSI to the BS. Therefore, the BS can acquire only the quantized CSI of legitimate users due to the limited feedback channel link. Also, the BS does not have the CSI of eavesdropper, which is a highly probable scenario in practical, since the eavesdropper is passive and it does not reveal their location or channel characteristics.

The received data signals at the legitimate user m and the eavesdropper respectively are,

$$y_m = \mathbf{h}_m^H \mathbf{x} + n_m, \tag{1}$$

$$\mathbf{y}_e = \mathbf{H}_e^H \mathbf{x} + \mathbf{n}_{e,m}. \tag{2}$$

The vector $\mathbf{h}_m \in \mathbb{C}^{N_t \times 1}$ denotes the channel vector between the BS and the legitimate user m. In this paper, we consider uncorrelated Rayleigh fading (i.e., the channel realizations are independent between users and BS antennas). Thus, each channel vector $\mathbf{h}_m$ has circularly symmetric complex Gaussian distribution $\mathcal{CN}\left(\mathbf{0}_{N_t \times 1}, \mathbf{I}_{N_t \times 1}\right)$. The average signal to noise ratio (SNR) is defined by SNR $= \frac{P}{\sigma^2}$. We assumed that all legitimate users have the same average SNR values. The channel vector of the eavesdropper is $\mathbf{H}_e \in \mathbb{C}^{N_t \times N_e}$ and it is unknown by the BS. The n_m is the complex additive white Gaussian noise (AWGN) at the legitimate user m and $\mathbf{n}_{e,m}$ is the corresponding AWGN at the eavesdropper. The noise distributions are $n_m \sim \mathcal{CN}\left(0, \sigma^2\right)$ and $\mathbf{n}_{e,m} \sim \mathcal{N}_{\mathbb{C}}\left(\mathbf{0}_{N_t \times N_e}, \sigma^2 \mathbf{I}_{N_t \times N_e}\right)$. The transmitted symbol vector is $\mathbf{x} \in \mathbb{C}^{N_t \times 1}$.

First of all, the channel vector of legitimate users, $\mathbf{h}_k; k = 1, 2, \ldots, K$ are estimated based on the pilot signals sent by the BS, $\boldsymbol{\phi} = [\boldsymbol{\lambda}_1, \ldots, \boldsymbol{\lambda}_i, \ldots, \boldsymbol{\lambda}_{N_t}]^T \in \mathbb{C}^{N_t \times \tau}$ where τ is the number of symbols per antenna. The pilot signal $\boldsymbol{\phi}$ has following properties: (i) $\|\boldsymbol{\lambda}_i\|^2 = \beta_i^2$, (ii) $\boldsymbol{\phi}\boldsymbol{\phi}^H = \tau \mathbf{I}_{N_t}$ where β_i^2 is the power of each pilot symbol.

Then, the received pilot signal $\mathbf{y}_k^{pp} \in \mathbb{C}^{1 \times \tau}$ at the legitimate user k is given by,

$$\mathbf{y}_k^{pp} = \mathbf{h}_k^H \boldsymbol{\phi} + \mathbf{z}, \tag{3}$$

where $\mathbf{z} \sim \mathcal{N}_{\mathbb{C}}\left(\mathbf{0}_{1 \times \tau}, \sigma_p^2 \mathbf{I}_{\tau \times \tau}\right)$ is the receiver noise component. The legitimate user k processes this signal by multiplying it with

$\boldsymbol{\phi}^H$ to estimate its channel. Then, the processed received signal $\mathbf{y}_k^p$ at the legitimate user k is

$$\mathbf{y}_k^p = \mathbf{y}_k^{pp}\boldsymbol{\phi}^H = \mathbf{h}_k^H\boldsymbol{\phi}\boldsymbol{\phi}^H + \mathbf{z}\boldsymbol{\phi}^H = \tau\mathbf{h}_k^H + \mathbf{z}\boldsymbol{\phi}^H, \tag{4}$$

where $\mathbf{z}\boldsymbol{\phi}^H \sim \mathcal{N}_{\mathbb{C}}\left(\mathbf{0}_{1\times N_t}, \sigma_p^2\tau\mathbf{I}_{N_t\times N_t}\right)$. Based on the received processed signal $\mathbf{y}_k^p$, the legitimate user estimates its channel with using minimum mean square error (MMSE) estimator as

$$\tilde{\mathbf{h}}_k = \frac{\beta_k}{\tau\beta_k + \sigma_p^2}(\mathbf{y}_k^p)^H, \tag{5}$$

and the channel estimate $\tilde{\mathbf{h}}_k$ has zero mean and covariance matrix

$$\mathbb{E}\left\{\tilde{\mathbf{h}}_k(\tilde{\mathbf{h}}_k)^H\right\} = \frac{\tau\beta_k^2}{\tau\beta_k + \sigma_p^2}\mathbf{I}_{N_t\times N_t}. \tag{6}$$

The channel estimation error $\mathbf{e}_k = \mathbf{h}_k - \tilde{\mathbf{h}}_k$ and its has distribution $\mathbf{e}_k \sim \mathcal{N}_{\mathbb{C}}\left(\mathbf{0}_{N_t\times 1}, \mathbf{C}_k\right)$ where $\mathbf{C}_k = \left(\beta_k - \frac{\tau\beta_k^2}{\tau\beta_k\sigma_p^2}\right)\mathbf{I}_{N_t\times N_t}$. The channel estimation quality is represented by the mean square error (MSE) given by $\mathbb{E}\left\{\|\mathbf{h}_k - \tilde{\mathbf{h}}_k\|^2\right\} = \mathrm{tr}\left(\mathbf{C}_k\right)$. Note that $\tilde{\mathbf{h}}_k$ and $\mathbf{e}_k$ are independent vectors.

Then, at the legitimate users' side semi-orthogonal criterion, which will be explained in the following section, is applied and the selected legitimate users based on this criterion are fed back theirs channel estimates to the BS in a quantized form by using rotated codebooks. The details of rotated codebooks will be discussed in the next section. Then, the BS schedules the best M legitimate users in terms of channel gain and constructs precoding vectors based on the available imperfect CSI.

The transmitted data signal by the BS is masked with AN and it is expressed as

$$\mathbf{x} = \hat{\mathbf{W}}\mathbf{s} + \hat{\mathbf{Q}}\mathbf{a}, \tag{7}$$

where $\hat{\mathbf{W}} = [\hat{\mathbf{w}}_1, \ldots, \hat{\mathbf{w}}_m, \ldots, \hat{\mathbf{w}}_M] \in \mathbb{C}^{N_t\times M}$ denotes the precoding matrix. Each column of $\hat{\mathbf{W}}$, $\hat{\mathbf{w}}_m$ with $m = 1, \ldots, M$, corresponds to the precoding vector of that legitimate user and $\|\hat{\mathbf{w}}_m\|^2 = 1$. Here, $\mathbf{s} \in \mathbb{C}^{M\times 1}$ is the information signal vector, where each element has zero mean and $\mathbb{E}\left\{|s_m|^2\right\} = p_s$. $\hat{\mathbf{Q}} \in \mathbb{C}^{N_t\times(N_t-M)}$ is the quantized orthogonal basis matrix that lies in the null space of $\hat{\mathbf{W}}$. $\mathbf{a} \in \mathbb{C}^{(N_t-M)\times 1}$ is AN vector that is used for jamming the eavesdropper and it has a distribution $\mathbf{a} \sim \mathcal{N}_{\mathbb{C}}\left(\mathbf{0}_{N_t\times 1}, p_a\mathbf{I}_{N_t\times N_t}\right)$. In order to guarantee the existence of matrix $\hat{\mathbf{Q}}$, the number of transmitter antenna N_t, must be higher than number of selected legitimate users M. Furthermore, in order to prevent eavesdropper to eliminate artificial noise $(N_t - M) \geq N_e$ must be satisfied. Thus, we select the number of M legitimate users to send confidential messages simultaneously that satisfies above conditions. After that, in order to mitigate inter-user interference, the zero forcing (ZF) precoding scheme is employed as:

$$\hat{\mathbf{W}} = \hat{\mathbf{H}}(\mathbb{M})^H(\hat{\mathbf{H}}(\mathbb{M})\hat{\mathbf{H}}(\mathbb{M})^H)^{-1}, \tag{8}$$

where $\hat{\mathbf{H}}(\mathbb{M}) = [\hat{\mathbf{h}}_1, \hat{\mathbf{h}}_2 \ldots, \hat{\mathbf{h}}_m, \ldots, \hat{\mathbf{h}}_M]^T$

Under imperfect channel state information, the received signal at the legitimate user m and the eavesdropper respectively are

$$y_m = \mathbf{h}_m^H\hat{\mathbf{w}}_m s_m + \sum_{j=1, j\neq m}^{M}\mathbf{h}_m^H\hat{\mathbf{w}}_j s_j + \mathbf{h}_m^H\hat{\mathbf{Q}}\mathbf{a} + n_m, \tag{9}$$

$$\mathbf{y}_{e,m} = \mathbf{H}_e\hat{\mathbf{w}}_m s_m + \mathbf{H}_e\hat{\mathbf{Q}}\mathbf{a} + \mathbf{n}_{e,m}. \tag{10}$$

It is noted that we assume the worst-case scenario in which eavesdroppers cancel interference coming from other legitimate users and eavesdroppers have the same average SNR values with the legitimate users.

Considering the AN leakage and inter-user interference because of imperfect channel state information, we can re-write (9) as,

$$y_m = \underbrace{\tilde{\mathbf{h}}_m^H\hat{\mathbf{w}}_m s_m}_{\text{desired signal}} + \underbrace{\mathbf{e}_m^H\hat{\mathbf{w}}_m s_m + \sum_{j=1, j\neq m}^{M}\left(\tilde{\mathbf{h}}_m^H\hat{\mathbf{w}}_j s_j + \mathbf{e}_m^H\hat{\mathbf{w}}_j s_j\right) + \tilde{\mathbf{h}}_m^H\hat{\mathbf{Q}}\mathbf{a} + \mathbf{e}_m^H\hat{\mathbf{Q}}\mathbf{a}}_{\nu,\ \text{interference}} + \underbrace{n_m}_{\text{noise}}. \tag{11}$$

Under both the channel estimation and quantization error considering the practical constraints defined in the system model, the achievable data rate at the legitimate user m is calculated by,

$$R_m = \log_2\left(1 + \frac{p_s|\mathbf{h}_m^H\hat{\mathbf{w}}_m|^2}{p_s\sum_{j=1, j\neq m}^{M}|\mathbf{h}_m^H\hat{\mathbf{w}}_j|^2 + p_a\|\mathbf{h}_m^H\hat{\mathbf{Q}}\|^2 + \sigma^2}\right). \tag{12}$$

Assuming perfect inter-user interference cancellation at the eavesdropper, the achievable rate at the eavesdropper upper bound is determined by,

$$R_{e,m} = \log_2\left(1 + p_s(\mathbf{H}_e^H\hat{\mathbf{w}}_m)^H\left(\sigma^2\mathbf{I}_{N_e\times N_e} + p_a(\mathbf{H}_e^H\hat{\mathbf{Q}})(\mathbf{H}_e^H\hat{\mathbf{Q}})^H\right)^{-1} \times (\mathbf{H}_e^H\hat{\mathbf{w}}_m)\right) \tag{13}$$

Thus, the achievable secrecy sum rate lower bound becomes [24],

$$R_s = \mathbb{E}\left\{\sum_{m=1}^{M}\left(R_m - R_{e,m}\right)^+\right\} \tag{14}$$

Here $(x)^+$ indicates $max(x, 0)^+$.

The total transmit power is denoted as P and it is equal to sum of data and AN signal powers $(p_s + p_a)$, where $p_s = \frac{\alpha P}{M}$ and $p_a = \frac{(1-\alpha)P}{N_t - M}$ respectively.

The power allocation between data and AN signals affects the average secrecy sum rate. According to availability of particular CSI at the transmitter (perfect or quantized), the value of α parameter should be chosen wisely as it provides the maximum secrecy rate.

The purpose of AN is to disturb any possible eavesdroppers' reception by beamforming noise in all directions except from the legitimate users' channel directions. However, the lack of perfect CSI at transmitter causes a noise leakage on legitimate users' channels and it degrades achievable secrecy rate. Therefore, we propose to use rotated codebook based on the semi-orthogonal selection criterion to prevent noise leakage while reducing on the quantization errors and mitigating inter user interference.

3. The semi-orthogonal selection with rotated codebook

The best M legitimate users are selected according to both their norms and orthogonality criterion to achieve higher secrecy sum rate. Therefore, the legitimate users having low channel gain and causing high inter-user interference are not fed back their CSI to the BS.

For secure multiuser MIMO systems, we apply a semi-orthogonality user selection criterion at the legitimate users by

employing rotated codebooks [25] to reduce AN leakage and inter-user interference.

The semi-orthogonal criterion selects the legitimate users whose channel direction information (CDI) are semi-orthogonal to the predefined orthogonal vectors. Each legitimate user generates the same N_t complex random orthonormal vectors as $\boldsymbol{\phi}_i \in \mathbb{C}^{N_t \times 1}$, $i = 1, \ldots, N_t$. Then, the legitimate user m in the set κ measures the orthogonality between their estimated CDI and $\boldsymbol{\phi}_i$ using the chordal distance:

$$d^2\left(\tilde{\mathbf{g}}_m, \boldsymbol{\phi}_i\right) = 1 - \left|\tilde{\mathbf{g}}_m^H \boldsymbol{\phi}_i\right|^2. \tag{15}$$

where $\tilde{\mathbf{g}}_m = \frac{\tilde{\mathbf{h}}_m}{\|\tilde{\mathbf{h}}_m\|}$ is the estimated CDI of the legitimate user m.

The unit sphere lying in $\mathbb{C}^{N_t}$ centered at the origin is defined as $\mathbb{O}^{N_t}$. Using the chordal distance metric, for any $0 < \epsilon_{th} < 1$, a spherical cap on $\mathbb{O}^{N_t}$ at the center of $\mathbf{o}$ and square radius ϵ_{th} is defined as follows:

$$\mathcal{B}_{\epsilon_{th}}(\mathbf{o}) = \left\{\tilde{\mathbf{g}}_m \in \mathbb{O}^{N_t} : d^2\left(\tilde{\mathbf{g}}_m, \mathbf{o}\right) \leq \epsilon_{th}\right\}. \tag{16}$$

where ϵ_{th} is the threshold on semi-orthogonality criterion and the dimension of $\mathbf{o}$ is $N_t \times 1$.

Then, we apply the following criterion called $\mathcal{T}_3$:

$$\mathbb{U}_3 = \left\{ m \in \kappa : \tilde{\mathbf{g}}_m \in \bigcup_{i=1}^{N_t} \mathcal{B}_{\epsilon_{th}}(\boldsymbol{\phi}_i) \text{ and } \|\tilde{\mathbf{h}}_m\|^2 \geq \gamma_{th} \right\} \tag{17}$$

where γ_{th} is the threshold on norm.

The average number of legitimate users, $\bar{K}$ which are fed back the corresponding indexes of their CSI to the BS is given by [26],

$$\bar{K} = KPr\{k \in \mathbb{U}_3\} \tag{18}$$

Since the channel norm and channel direction are independent, then it is re-written by,

$$\bar{K} = KPr\{\tilde{\mathbf{g}}_m \in \bigcup_{i=1}^{N_t} \mathcal{B}_{\epsilon_{th}}(\boldsymbol{\phi}_i)\} \times Pr\{\|\tilde{\mathbf{h}}_m\|^2 \geq \gamma_{th}\} \tag{19}$$

Then, $\bar{K}$ is determined by,

$$\bar{K} = KN_t \sum_{b=0}^{N_t-1} \frac{\exp(-\gamma_{th})(\gamma_{th})^b}{b!} \epsilon_{th}^{N_t-1} \tag{20}$$

In order to reduce the quantization error of the legitimate users selected by the criterion $\mathcal{T}_3$, 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 $\mathbb{O}^{N_t}$. From the local packing associated to the spherical cap $\mathcal{B}_{\epsilon_{th}}(\mathbf{o})$ with a center of a spherical cap of $\mathbf{o}$ on $\mathbb{O}^{N_t}$ through unit sphere lying in $\mathbb{C}^{N_t}$, it is possible to compute $\mathcal{B}_{\epsilon_{th}}(\boldsymbol{\phi}_i)$ by using $\mathbf{U}_r = \boldsymbol{\phi}_i \mathbf{o}^{-1}$ where $\mathbf{U}_r$ is the unitary rotation matrix which is the same for all legitimate users [26,27]. The codebook constructed using Lloyd algorithm, $\mathcal{C} = \left\{\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_i, \ldots, \mathbf{c}_{2^B}\right\}$ is then rotated through $\mathbf{U}_r$. Then, the rotated codebook is given by $\mathcal{C}^o = \left\{\mathbf{c}_1^o, \mathbf{c}_2^o, \ldots, \mathbf{c}_i^o, \ldots, \mathbf{c}_{2^B}^o\right\}$ where $\mathbf{c}_i^o = \mathbf{U}_r \mathbf{c}_i$.

The legitimate users selected through $\mathcal{T}_3$ criterion quantize their CDI using these rotated codebooks.

$$k_i' = \arg \max_{1 \leq i \leq 2^B} \left|\left(\tilde{\mathbf{g}}_{k'}\right)^H \mathbf{c}_i^o\right| \quad \forall k' \in \mathbb{U}_3. \tag{21}$$

Consequently, only $\bar{K}$ legitimate users are fed back their quantized CSI to the BS.

Then, at the BS, M legitimate users providing the best sum rate are scheduled in order to establish a secure communications. The equal power allocation is performed among the scheduled M legitimate users.

4. The proposed secure multiuser MIMO

In this work, we propose to apply the semi-orthogonal user selection with rotated codebook for secure multiuser MIMO systems in order to improve the secrecy sum rate while decreasing the AN leakage and inter-user interference. Firstly, the CSI is estimated at each legitimate users. Then, the semi-orthogonal criterion is applied to select the legitimate users which are quantized and fed back their CSI to the BS. The semi-orthogonal criterion relies on the threshold values γ_{th} and ϵ_{th} known by both the transmitter and the receivers, and does not need an additional overhead. After that, the legitimate users which are fed back their CSI are scheduled at the BS. In the proposed secure system, only $\bar{K}$ legitimate users are considered while K legitimate users are taken into account in the full feedback scheme. As a result, the computational complexity is reduced to schedule legitimate users at the BS and decreases the overall feedback load compared to the full feedback scheme. A pseudocode of the proposed secure system with imperfect channel state information is given in Algorithm 1.

Algorithm 1 The proposed secure multiuser MIMO system with imperfect channel state information

At the legitimate users' side:
for $k = 1 : K$ **do**
  At k**th legitimate user:**
  -Estimate CSI $\tilde{\mathbf{h}}_k$.
  -Obtain CQI $\|\tilde{\mathbf{h}}_k\|$ and CDI $\tilde{\mathbf{g}}_k$.
  -Apply $\mathcal{T}_3$ criterion:
  if Eq. (17) is satisfied: **then**
    -Quantize CDI of this legitimate user using the rotated codebook as in Eq. (21).
    Output: The index of the quantized CDI belonging to k'th legitimate user, k_i'.
  end if
end for
At the BS side:
Input: The indexes k_i' of the legitimate users which satisfy $\mathcal{T}_3$ criterion.

- Construct the set of $\mathbb{U}_3$ including the indexes of the quantized CDI of the legitimate users which are fed back them.
- For $k' \in \mathbb{U}_3$, obtain the estimated CQI, $\|\tilde{\mathbf{h}}_{k'}\|$ and the quantized CDI, $\hat{\mathbf{g}}_{k'}$, using the index of k_i' through the rotated codebook.
- Schedule the M legitimate users:
  - Select the legitimate user with the highest CQI.
  - Add $M - 1$ legitimate users having the largest orthogonality indicator to the selected ones.
  - Apply ZF as in Eq. (8).

Output: The precoding matrices, $\hat{\mathbf{W}}$ and $\hat{\mathbf{Q}}$.

The purpose of artificial noise is to disturb any possible eavesdropper reception by beamforming noise in all directions except from legitimate users' channel directions. However, the lack of perfect CSI at transmitter causes a noise leakage on legitimate users' channels and it degrades achievable secrecy rate. Therefore, we use rotated codebook based on the semi orthogonal selection criterion to reduce the quantization errors and to prevent noise leakage.

The proposed secure scheme relies on the predefined threshold values without requiring any additional overhead and is compatible with the existing downlink multiuser MIMO communication systems operating in frequency division duplexing (FDD).

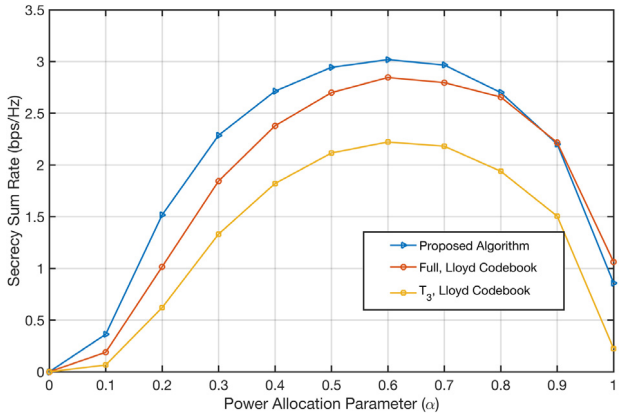

Fig. 2. The power allocation parameter of the full feedback and $\mathcal{T}_3$ criterion with different type of codebooks for $B = 8$, SNR $= 10$ dB and $K = 50$.

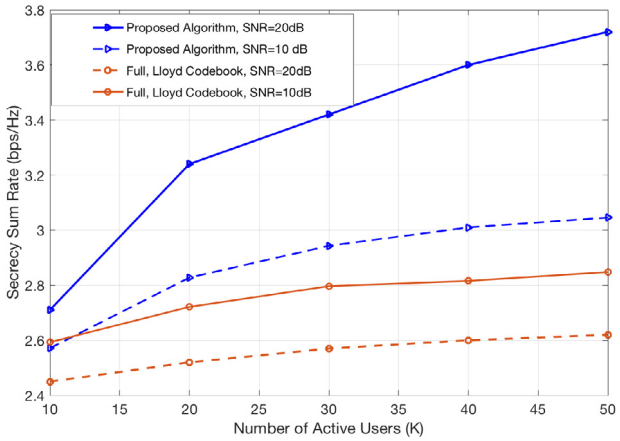

Fig. 3. The comparison results of the full feedback and $\mathcal{T}_3$ criterion for different number of legitimate users for $\alpha = 0.6$ and $B = 8$.

5. Performance evaluations

We show the performance evaluations for the secure multiuser MIMO systems with $N_t = 4$ transmit antennas at the BS and $N_e = 2$ antennas at eavesdropper unless stated otherwise. For this model, the maximum number of scheduled legitimate users simultaneously is $M = 2$. The carrier frequency is 2.6 GHz. The pair of $(\epsilon_{th}, \gamma_{th})$ for $\mathcal{T}_3$ criterion is determined for an average number of legitimate users to be fed back of $\bar{K} = 4$. Then, they are given by $(\epsilon_{th}, \gamma_{th}) = [(0.45, 0.60), (0.322, 0.60), (0.293, 0.60), (0.272, 0.60)]$ for the number of legitimate users from $K = 10$ to $K = 50$. The selected legitimate users based on the proposed criterion are fed back in B bits for their CDI. Therefore, the total number of feedback bits is $4B$ for the proposed solution while it is determined by KB for the full feedback case.

The effect of power allocation parameter α for the quantized case is examined in Fig. 2. The proposed schemes gives better performance for all values except the case where no power is allocated for AN with $\alpha = 1$. Under this setting, no AN leakage occurs and the proposed scheme could not further reduced an AN leakage. Based on the performance results, the optimum value of α for all settings is set to 0.6.

The Fig. 3 compares the average secrecy sum rate for $\mathcal{T}_3$ with rotated codebook and the full feedback with Lloyd codebook by employing AN under different number of legitimate users. There is a mismatch between the exact channel state information and quantized one obtained with Lloyd codebook. The generated AN is orthogonal to quantized channel while it is not orthogonal to legitimate users' exact channel. This causes AN leakage to the legitimate user' signal. In the proposed scheme, the quantization error is reduced by using the rotated codebook which only quantizes the region which is inside the spherical cap with radius ϵ_{th}. As a result, the proposed solution provides much better average secrecy sum rate than the full feedback case while requiring 60% to 92% less bits through the limited feedback link.

The comparison average secrecy sum rate of the full feedback and $\mathcal{T}_3$ with the rotated and Lloyd codebooks for different SNR values is depicted in Fig. 4. Increasing SNR can degrade the average secrecy sum rate significantly in the system using Lloyd codebook for both full feedback and $\mathcal{T}_3$ criterion, since AN leakage is severe and increases with SNR.

In Fig. 5, we compare the effect of quantization bits on the full feedback and the proposed algorithm. As it can be seen, the usage of rotated codebook gives much higher average secrecy sum rate. As a result, the semi-orthogonal criterion with rotated codebook improves the secrecy performance under imperfect CSI since it

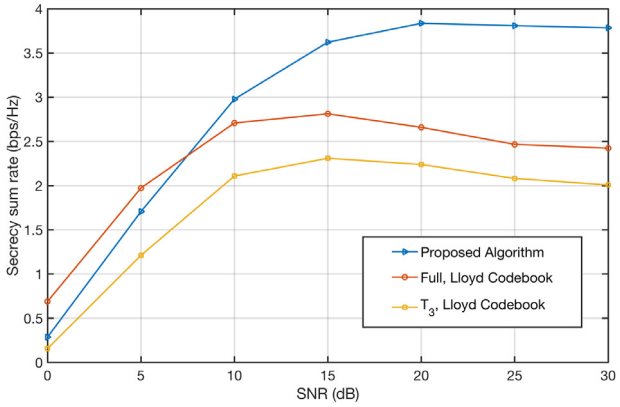

Fig. 4. The comparison results of the full feedback and the proposed algorithm for different type of codebooks and SNR values at $\alpha = 0.6$, $K = 50$ and $B = 8$.

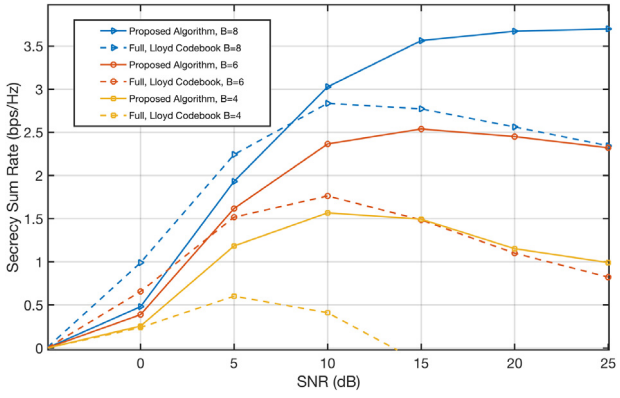

Fig. 5. The comparison results of the full feedback and the proposed algorithm for different number of bits at $K = 50$.

reduces both inter-user interference and AN leakage thanks to the rotated codebooks leading to reduced quantization error. By increasing the number of quantization bits also are decreased AN leakage as well as inter-user interference and achieve better average secrecy rate.

In Fig. 6, the average secrecy sum rate results of the proposed algorithm are compared with the secure system that schedules only one legitimate user. The performance results show that the secure multiuser MIMO system with the semi-orthogonal

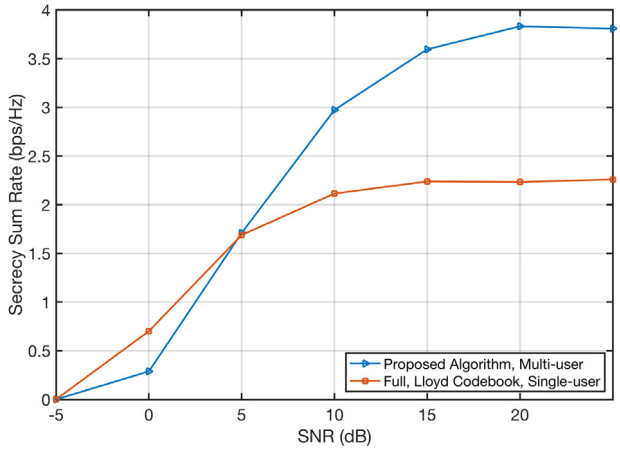

Fig. 6. The comparison results of the proposed secure multiuser MIMO with limited feedback and the secure single legitimate user MIMO with the full feedback where $K = 50$ and $\alpha = 0.6$.

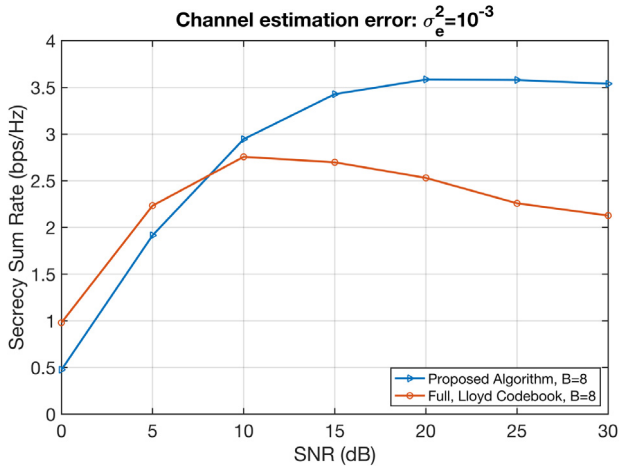

Fig. 7. The comparison of the full feedback and the proposed algorithm for different SNR values where $\alpha = 0.6$, $K = 50$, $B = 8$ and the channel estimation error of $\sigma_e^2 = 10^{-3}$.

criterion having rotated codebook provides better average secrecy sum rate when the SNR is higher than 5dB while requiring much less feedback bits compared to a single legitimate user multiple antenna system with the full feedback.

Fig. 7 compares the performance of the full feedback and the proposed algorithm in the presence of channel estimation error. According to the results, the proposed algorithm still gives a better average secrecy rate performance than the full feedback case in the presence of channel estimation error when the SNR is higher than 7.5 dB.

We also provide the performance evaluations for the secure multiuser MIMO systems by scheduling more than 2 legitimate users in the system including $N_t = 8$ transmit antennas at the BS and $N_e = 3$ antennas at the eavesdropper. The maximum number of simultaneously scheduled legitimate users is set to $M = 3$ among $K = 100$ active legitimate users. The threshold values for $\bar{K} = 4$ are calculated as $(\epsilon_{th}, \gamma_{th}) = [(0.4691, 0.60)]$. As shown in Fig. 8, the proposed algorithm achieves higher average sum secrecy rate between 70% and 50% depending on SNR values compared to the full feedback with Lloyd codebook algorithm. The reason is that the proposed algorithm eliminates AN leakage and inter-user interference which significantly increase for the case of higher number of scheduled legitimate users.

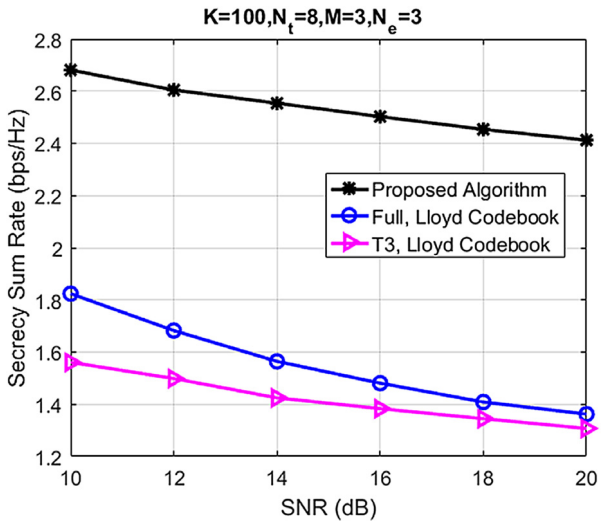

Fig. 8. The comparison results of the full feedback and the proposed algorithm for $N_t = 8$, $N_e = 3$, $M = 3$, $K = 100$, $\alpha = 0.6$ and $B = 8$.

6. Conclusion

In this work, we have considered the case of colluding eavesdroppers that aims to listen legitimate users channel maliciously. The AN masked beamforming has been employed to prevent eavesdroppers to decode message signals. However, the imperfect channel state information of legitimate users at the BS causes a AN leakage. We have examined a semi-orthogonal user selection and rotated codebook to mitigate this AN leakage in secure multiuser MIMO systems. It has been shown that the proposed algorithm with rotated codebook gives better average secrecy sum rates than the full feedback case with Lloyd codebook at moderate SNRs while requiring much less feedback load in secure multiuser MIMO systems. We have demonstrated the feasibility of these PHY security mechanisms by examining the achievable average secrecy sum rates under imperfect channel state information. The proposed algorithm will be applied for the secure non-orthogonal multiple access (NOMA) MIMO systems in cooperative multicell systems for beyond 5G applications to increase the average secrecy sum rates.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

This work is supported by The Scientific and Technical Research Council of Turkey (TUBITAK) under the grant of 114E626 Tubitak-Ardeb-1005 project.

References

[1] T. Liu, S. Shamai, A note on the secrecy capacity of the multiple-antenna wiretap channel, IEEE Trans. Inform. Theory 55 (6) (2009) 2547–2553.
[2] F. Oggier, B. Hassibi, The secrecy capacity of the MIMO wiretap channel, IEEE Trans. Inform. Theory 57 (2011) 4961–4972.
[3] Y.W.P. Hong, P.C. Lan, C.C.J. Kuo, Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches, IEEE Signal Process. Mag. 30 (2013) 29–40.
[4] C.H. Lin, S.H. Tsai, Y.P. Lin, Secure transmission using MIMO precoding, IEEE Trans. Inf. Forensics Secur. 9 (2014) 801–813.

[5] S. Goel, R. Negi, Secret communication in presence of colluding eavesdroppers, in: IEEE Military Communications Conference(MILCOM), 2005.
[6] P.C. Pinto, J. Barros, M.Z. Win, Wireless physical-layer security: The case of colluding eavesdroppers, in: IEEE International Symposium on Information Theory, 2009.
[7] O.O. Koyluoglu, C.E. Koksal, H.E. Gamal, On the effect of colluding eavesdroppers on secrecy capacity scaling, in: European Wireless Conference (EW), 2010.
[8] M. Mirmohseni, P. Papadimitratos, Colluding eavesdroppers in large cooperative wireless networks, in: Iran Workshop on Communication and Information Theory (IWCIT), 2014.
[9] Y.R. Ortega, P.K. Upadhyay, D.B. Costa, et al., Joint effect of jamming and noise on the secrecy outage performance of wiretap channels with feedback delay and multiple antennas, Trans. Emerg. Telecommun. Technol. 3191 (2017).
[10] F.S. Al-Qahtani, Y. Huang, S. Hessien, R.M. Radaydeh, C. Zhong, H.M. Alnuweiri, Secrecy analysis of MIMO wiretap channels with low-complexity receivers under imperfect channel estimation, IEEE Trans. Inf. Forensics Secur. 12 (2) (2017) 257–270.
[11] R. Negi, S. Goel, Secret communication using artificial noise, in: IEEE 62nd Vehicular Technology Conference (VTC), 2005.
[12] S. Goel, R. Negi, Guaranteeing secrecy using artificial noise, IEEE Trans. Wireless Commun. 7 (2008) 2180–2189.
[13] P.H. Lin, S.H. Lai, S.C. Lin, H.J. Su, On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels, IEEE J. Sel. Areas Commun. 31 (2013) 1728–1740.
[14] A. Khisti, G.W. Wornell, Secure transmission with multiple antennas I: The MISOME wiretap channel, IEEE Trans. Inform. Theory 56 (2010) 3088–3104.
[15] S.C. Lin, T.H. Chang, Y.L. Liang, Y.W.P. Hong, C.Y. Chi, On the impact of quantized channel feedback in guaranteeing secrecy with artificial noise: The noise leakage problem, IEEE Trans. Wireless Commun. 10 (2011) 901–915.
[16] IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, 2006.
[17] Physical Channels and Modulation (Release 8).-3GPP 36.211.
[18] S. Bashar, Z. Ding, G.Y. Li, On secrecy of codebook-based transmission beamforming under receiver limited feedback, IEEE Trans. Wireless Commun. 10 (2011) 1212–1223.
[19] C.H. Lin, S.H. Tsai, Y.P. Lin, On quantization for masked beamforming secrecy systems, IEEE Trans. Wireless Commun. 14 (2015) 5616–5628.
[20] M.R. Abedi, N. Mokari, H. Saeedi, H. Yanikomeroglu, Robust resource allocation to enhance physical layer security in systems with full-duplex receivers: Active adversary, IEEE Trans. Wireless Commun. 16 (2) (2017).
[21] M.R. Abedi, N. Mokari, H. Saeedi, How to manage resources to provide physical layer security: Active versus passive adversary? Phys. Commun. 27 (2018) 143–149.
[22] B. Özbek, Ö. Özdogan, G.K. Kurt, Secure multiuser MISO communication systems with quantized feedback, in: IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), 2016.
[23] B. Özbek, Ö. Özdogan, G.K. Kurt, Secure multiuser MISO communication systems with limited feedback link, Springer Ann. Telecommun. 73 (2018) 381–390.
[24] G. Geraci, M. Egan, J. Yuan, A. Razi, I.B. Collings, Secrecy sum-rates for multi-user MIMO regularized channel inversion precoding, IEEE Trans. Commun. 60 (2012) 3472–3482.
[25] B. Özbek, D. Le Ruyet, Feedback Strategies for Wireless Communications Systems, Springer-Verlag, New York, 2014.
[26] H. Khanfir, D. Le Ruyet, B. Özbek, Reduced feedback load using user selection algorithms for the multiuser multi-input single output systems, Trans. Emerg. Telecommun. Technol. (ETT) 24 (2013) 809–819.
[27] V. Raghavan, Jr. R.W., Heath, A.M. Sayeed, Systematic codebook designs for quantized beamforming in corre- lated MIMO channels, IEEE J. Sel. Areas Commun. (JSAC) 25 (2007) 1298–1310.

Dr. Berna Özbek is an Associate Professor in Telecommunication field at the Electrical and Electronics Engineering Department of İzmir Institute of Technology, Turkey and is working in the field of wireless communication systems for more than 15 years. She has graduated from Electrical and Electronics Department of Dokuz Eylul University, Turkey on 1994 and completed her MSc and PhD studies respectively on 1999 and 2004. Afterwards, she received a scholarship and worked as a postdoctoral researcher at CNAM-Paris on 2005. She was awarded as a Marie-Curie Intra-European (EIF) Fellow by European Commission for two years in the project entitled Interference Management Techniques for Multicell Networks on 2010. She has managed 1 international and 4 national projects, served as a consultant for 3 Eureka-Celtic projects and 2 national projects. Under her supervision, 11 master thesis and 2 doctoral dissertations have been completed. Currently, she is supervising 1 PhD and 5 master students. She has published more than 80 peer-reviewed papers, 1 book, 1 book chapter and 2 patents. She is serving as a referee for several international journals, on numerous TPCs for IEEE sponsored conferences, European Commission, Turkish Republic of Ministry of Trade and Industry and The Scientific and Technological Research Council of Turkey. Her research interests are interference management, resource allocation and limited feedback strategies in multi-user, multi-antenna systems, device-to-device and heterogeneous wireless communications, physical layer security, massive MIMO systems, mmwave communications.