Spatial signature for secure MISO-OFDM systems

B. Ozbek✉ and G.K. Kurt

Physical layer security is a promising approach to establish secure communications based on the characteristics of wireless channels. A spatial signature based secure multiple-input single-output (MISO) orthogonal frequency division multiplexing (OFDM) system is proposed to disrupt the reception of a passive eavesdropper by holding two practically relevant assumptions: a limited feedback link for legitimate node and the unavailability of channel state information of eavesdropper. The proposed algorithm achieves a higher average secrecy rate than the conventional secure MISO-OFDM systems in presence of a limited feedback link.

Introduction: Wireless communication channels make a communication system more prone to eavesdropping attacks due to their broadcast nature. However, this broadcast nature also introduces a design freedom to enable secure communication techniques. Referred to as physical layer security approaches in the literature, these techniques rely on two unrealistic assumptions. As the first assumption, the channel state information (CSI) between the legitimate transmitter and the legitimate receiver is assumed to be perfectly available at the legitimate transmitter. This implies that the feedback link between the legitimate receiver and the legitimate transmitter has infinite capacity. Although convenient for analytical purposes, it is not a realistic assumption. As the second assumption, the channel between the legitimate transmitter and the eavesdropper is assumed to be known. However, in case of a passive eavesdropper, the availability of this CSI is also unrealistic [1].

Although there are some works that consider an uncertainty about CSI of eavesdropper, the literature that takes the above-mentioned realistic considerations into account is quite sparse. In [2], artificial noise (AN) has been injected to the null space of the legitimate receiver, avoiding the need for the CSI of the eavesdropper. In [3], AN injection has been performed along both the temporal and spatial dimensions of a legitimate system to secure its transmissions from potential eavesdropping attacks. However, an infinite capacity feedback link between the legitimate transmitter and the legitimate receiver has been considered. The ergodic secrecy capacity has been characterised with limited feedback in [4] and a codebook-based transmission technique to improve secrecy capacity has been examined in [5] in presence of quantised CSI. The impact of the number of feedback bits on the secrecy capacity has been investigated in [6], in presence of AN.

The exploitation of both spatial and frequency diversity to alleviate the channel uncertainty conditions remains an open issue in the current state-of-the-art. In order to address this gap, in this Letter, we propose a spatial signature based secure communication approach that prevents the noise leakage in multiple-input single-output (MISO) orthogonal frequency division multiplexing (OFDM) systems. We focus on the practical applicability of the proposed approach for secure MISO-OFDM systems by considering a limited feedback scenario for the legitimate user. Additionally, we assume that no a priori information is available about the CSI of eavesdropper at the transmitter side. Through numerical simulations, we demonstrate that the proposed spatial signature algorithm achieves a higher secrecy rate than the conventional secure MISO-OFDM systems with limited feedback link.

System model: We consider a MISO-OFDM system with Q clusters including one eavesdropper (Eve) and one legitimate receiver (Bob). The base station (Alice) has N_t transmit antennas, Eve is equipped with N_e antennas and Bob has only a one antenna. Alice aims to send a confidential message to Bob. Concurrently, it transmits AN to disturb the reception of Eve. We assume that CSI of the legitimate user is perfectly estimated at receiver side and the quantised CSI of legitimate user is available at Alice through the limited feedback link. However, Alice has no knowledge about CSI of Eve, which is a highly probable scenario in practical cases since Eve is passive in general. We consider a clustering structure where adjacent subcarriers are grouped and only one representative value for each cluster is selected [7].

The transmitted signal for the qth cluster can be denoted as

$$\boldsymbol{X}_q = \hat{\boldsymbol{W}}_q S_q + \hat{\boldsymbol{Q}}_q \boldsymbol{a}_q, \tag{1}$$

where S_q is the information-bearing signal with power $\mathbb{E}\{|S_q|^2\} \leq (P_s/Q^a)$, where Q^a is the total number of active clusters in transmission. $\boldsymbol{a}_q = [a_{q_1}, a_{q_2}, \ldots, a_{q_{N_\mathrm{t}}}]^\mathrm{T}$ is the AN vector with a power $\mathbb{E}\{||\boldsymbol{a}_q||^2\} \leq (P_a/Q^a)$. The transmitted signal power and AN signal power are, respectively, defined as $P_s = \alpha P$ and $P_a = ((1-\alpha)/(N_t - 1))P$, where the total transmit power is $P = P_a + P_s$, and $\alpha \in (0, 1)$ is the channel condition parameter. As α increases, the power of AN signal decreases. The value of α parameter should be chosen to maximise to the average secrecy rate. Besides, the precoding vector $\hat{\boldsymbol{W}}_q$ and AN beamforming vector $\hat{\boldsymbol{Q}}_q$ are determined through quantised CSI between Alice and Bob.

Then, the received signals for each cluster at Bob and Eve can be written, respectively, as

$$Y_q = \boldsymbol{H}_q^\mathrm{H} \hat{\boldsymbol{W}}_q S_q + \boldsymbol{H}_q^\mathrm{H} \hat{\boldsymbol{Q}}_q \boldsymbol{a}_q + Z_q, \tag{2}$$

$$\boldsymbol{Y}_q^e = (\boldsymbol{H}_q^e)^\mathrm{H} \hat{\boldsymbol{W}}_q S_q + (\boldsymbol{H}_q^e) \hat{\boldsymbol{Q}}_q \boldsymbol{a}_q + \boldsymbol{Z}_q^e. \tag{3}$$

where the channel vectors of Bob and Eve for cluster q are denoted by $\boldsymbol{H}_q \in \mathcal{C}^{N_\mathrm{t} \times 1}$ and $\boldsymbol{H}_q^e \in \mathcal{C}^{N_\mathrm{t} \times N_\mathrm{e}}$, respectively. Z_q is the complex additive white Gaussian noise (AWGN) at Bob with 0 mean and variance σ^2. Each element of $\boldsymbol{Z}_q^e$ corresponds to AWGN at Eve with 0 mean and variance σ_e^2. The average signal-to-noise ratio (SNR) values belonging to Bob and Eve are, respectively, denoted by $\rho = (P/\sigma^2)$ and $\rho_e = (P/\sigma_e^2)$. Since we assume that there is no knowledge about CSI of Eve, we remove the effect of ρ_e completely by setting $(1/\rho_e) = 0$.

The channel direction information (CDI) is defined by $\boldsymbol{G}_q = (\boldsymbol{H}_q/\|\boldsymbol{H}_q\|)$ and $\|\boldsymbol{H}_q\|$ denotes the channel quality information. Bob quantises its CDI to a unit norm vector selected from a predetermined codebook with size 2^B, where B is the number of quantisation bits. For each cluster q, each user chooses an optimal codeword to quantise its CDI according to the minimum chordal distance by

$$q_j = \underset{1 \leq j \leq 2^B}{\arg\min}\, d^2(\boldsymbol{G}_q, \hat{\boldsymbol{G}}_j) = 1 - \left|\boldsymbol{G}_q^\mathrm{H} \hat{\boldsymbol{G}}_j\right|^2, \tag{4}$$

where $\hat{\boldsymbol{G}}_j$ is the jth codeword of the codebook given by $\mathbb{G} = \{\hat{\boldsymbol{G}}_1, \hat{\boldsymbol{G}}_2, \ldots, \hat{\boldsymbol{G}}_{2^B}\}$. After the selection of the codeword, Bob feeds back its CDI index to Alice in B bits for each cluster. The $\hat{\boldsymbol{Q}}_q \in \mathcal{C}^{N_\mathrm{t} \times N_\mathrm{t}}$ is the AN beamformer whose columns form an orthonormal basis for the left null space of $\hat{\boldsymbol{G}}_q$, which is defined by $\hat{\boldsymbol{G}}_q \hat{\boldsymbol{Q}}_q = \boldsymbol{0}_{1 \times N_\mathrm{t}}$. The precoding vector is $\hat{\boldsymbol{W}}_q = \hat{\boldsymbol{G}}_{q_j}$ with the quantised CDI of Bob.

The instantaneous signal-to-interference noise ratio (SINR) at Bob is given by

$$\hat{\gamma}_q = \frac{|(\boldsymbol{H}_q)^\mathrm{H} \hat{\boldsymbol{W}}_q|^2 \alpha K}{|(\boldsymbol{H}_q)^\mathrm{H} \hat{\boldsymbol{Q}}_q|^2 ((1-\alpha)/(N_\mathrm{t}-1))K + (1/\rho)}. \tag{5}$$

where K is the normalised power coefficient under the condition that only Q_a active clusters are used during the transmission instead of Q. In contrast to the case that Alice has the perfect CSI, the limited feedback causes a leakage because of the $|(\boldsymbol{H}_q)^\mathrm{H} \hat{\boldsymbol{Q}}_q|^2 = ||\boldsymbol{H}_q||^2 |\boldsymbol{G}_q^\mathrm{H} \hat{\boldsymbol{Q}}_q|^2$ to the intended user's space because of the quantisation error.

The instantaneous SINR at Eve scenario is given as

$$\hat{\gamma}_q^e = \alpha((\boldsymbol{H}_q^e)^\mathrm{H} \hat{\boldsymbol{W}}_q)^\mathrm{H} \left(\frac{(1-\alpha)}{N_\mathrm{t}-1}((\boldsymbol{H}_q^e)^\mathrm{H} \hat{\boldsymbol{Q}}_q)((\boldsymbol{H}_q^e)^\mathrm{H} \hat{\boldsymbol{Q}}_q)^\mathrm{H}\right)^{-1} ((\boldsymbol{H}_q^e)^\mathrm{H} \hat{\boldsymbol{W}}_q) \tag{6}$$

Then, the average secrecy rate is expressed by

$$\hat{C} = \frac{1}{Q} \sum_{q=1}^{Q} \mathbb{E}\{\log_2(1 + \hat{\gamma}_q)\} - \mathbb{E}\left\{\log_2\left(1 + \hat{\gamma}_q^e\right)\right\}. \tag{7}$$

Proposed spatial signature for secure communications: In order to depict the feedback mechanism in secure MISO-OFDM systems, we propose an algorithm based on spatial signature as given below:

- *Step 1:* For each cluster q, we generate the complex random orthogonal vectors denoted by $\boldsymbol{\phi}_{n,m,q}$ where dimension of $N_\mathrm{t} \times 1$, where $n = 1, \ldots, N_\mathrm{t}$ and $m = 1, \ldots, M$ with M is the number of random orthogonal vectors. All of them are known at both Alice and Bob. Therefore, only the corresponding indexes are fed back to the Alice. $\boldsymbol{\phi}_{n,m,q}$ are generated according to an isotropic distribution and are equally likely pointing in any direction in the complex space. In order to construct $\boldsymbol{\phi}_{n,m,q}$ based on the method of Heiberger, $N_\mathrm{t} \times N_\mathrm{t}$ matrices $\boldsymbol{D}_{m,q}$; $\forall m$ whose entries are Gaussian distributed with 0 mean and 1 variance are generated. Then, a QR factorisation is applied to obtain a matrices $\boldsymbol{E}_{m,q}$ and $\boldsymbol{T}_{m,q}$. The matrix $\boldsymbol{E}_{m,q}$ is composed of N_t orthogonal column vectors. Each of these vectors corresponds to $\boldsymbol{\phi}_{n,m,q}$.

- *Step 2:* We classify the clusters of the legitimate user by using the generated orthogonal vectors, $\boldsymbol{\phi}_{n,m,q}$, generated in *step 1*. Let $\mathcal{O}^{N_\mathrm{t}}$ be the unit sphere lying in $\mathcal{C}^{N_\mathrm{t}}$ and centred at the origin. For any $0 < \epsilon < 1$, we can define a spherical cap on $\mathcal{O}^{N_\mathrm{t}}$ with centre $\boldsymbol{o}$ and square radius ϵ as the open set by, $\mathcal{B}_\epsilon(\boldsymbol{f}, \boldsymbol{o}) = \{\boldsymbol{f} \in \mathcal{O}^{N_\mathrm{t}}{:}d^2(\boldsymbol{f}, \boldsymbol{o}) \leq \epsilon\}$. Then, we classify the clusters of legitimate user as follows:

$$\mathbb{Q}_{n,m,q} = \{q{:}\boldsymbol{G}_q \in \mathcal{B}_\varepsilon(\boldsymbol{G}_q, \boldsymbol{\phi}_{n,m,q})\}. \tag{8}$$

- *Step 3:* In contrast to the normalised independent identically distributed case, the classified CDI of clusters is isotropically distributed in $\mathcal{O}^{N_\mathrm{t}}$. This is an important aspect of designing a codebook tailored to a spherical cap region. Therefore, a local Grassmannian packing with parameters N_t, 2^B, $\boldsymbol{o}$, ϵ is used. For each predefined ϵ value, a codebook constrained to a spherical cap $\mathcal{B}_\epsilon(\boldsymbol{o})$ in $\mathcal{O}^{N_\mathrm{t}}$ is designed by maximising the largest minimum chordal distance. This codebook, namely $\mathbb{C}^\epsilon = [\boldsymbol{C}_1^\epsilon, \ldots, \boldsymbol{C}_{2^B}^\epsilon]$, is available at both Alice and Bob. Then, the codewords in the codebook have to be adapted according to the generated orthogonal vectors $\boldsymbol{\phi}_{n,m,q}$. From the local packing, it is possible to compute the local packing associated with the centre, $\boldsymbol{\phi}_{n,m,q}$, using the rotation matrix $\boldsymbol{U}_{n,m,q}^{\mathrm{rot}} = \boldsymbol{\phi}_{n,m,q}\boldsymbol{o}^{-1}$. We then apply a rotation for each codeword to obtain the rotated codebook for each generated orthogonal vectors by

$$\boldsymbol{C}_{j,n,m,q}^{\mathrm{rot}} = \boldsymbol{U}_{n,m,q}^{\mathrm{rot}}\boldsymbol{C}_j^\epsilon; \quad j = 1, \ldots, 2^B. \tag{9}$$

Then, the rotated codebook for each rotation vector is constructed by $\mathbb{C}_{n,m,q}^{\mathrm{rot}} = [\boldsymbol{C}_{1,n,m,q}^{\mathrm{rot}}, \ldots, \boldsymbol{C}_{2^B,n,m,q}^{\mathrm{rot}}]$. With a specific codebook design, the quantisation error is reduced since only the local region is quantised instead of the whole region [7].

- *Step 4:* By using the rotated codebook designed in *step 3*, the CDI of each cluster in the set of $\mathbb{Q}_{n,m}$ obtained *step 2* is quantised according to the following rule:

$$j_{n,m,q}^{\mathrm{rot}} = \underset{1\leq j\leq 2^B}{\arg\min}\, d_c^2(\boldsymbol{G}_q, \boldsymbol{C}_{j,n,m,q}^{\mathrm{rot}}). \tag{10}$$

Then, the corresponding indexes of the quantised CSI, $j_{n,m,q}^{\mathrm{rot}}$; $\forall n, m, q$, are fed back to the Alice through the limited feedback link. After that, the quantised precoding vector is obtained at Alice by

$$\hat{\boldsymbol{G}}_q = \boldsymbol{C}_{j_{n,m,q}^{\mathrm{rot}},n,m,q}^{\mathrm{rot}}. \tag{11}$$

Performance results: We consider a secure MISO-OFDM system in which Alice and Eve have $N_\mathrm{t} = 2$, $N_\mathrm{e} = 1$ antennas, respectively. We illustrate the benefits of the proposed spatial signature in secure communications through wireless channels by comparing with the conventional scheme which establishes transmission in all clusters and quantises their CSI by using Lloyd's algorithm based codebook design. The wireless channel is modelled using 3GPP-TU with a velocity of 3 km/h and the carrier frequency is 2.4 GHz. The number of clusters are selected as $Q = 48$ which are grouped into 18 subcarriers. The power allocation parameter, α, is chosen as 0.6 in order to achieve the highest secrecy rate at different SNR values for both the conventional and the proposed schemes.

We examine the effect of threshold values, ϵ, and the number of random orthogonal vectors, M, on the performance of average secrecy rate at $B = 8$ and $\rho = 15$ dB as listed in Table 1. For small threshold values and less number of orthogonal vectors, the average secrecy rate reaches higher values, because the quantisation error is decreased based on small spherical cap and the power level per cluster is increased with less number of active clusters. In order to limit the maximum power per cluster as a ratio of 30% more than conventional scheme while achieving the highest average secrecy rate, we set $M = 2$ and $\epsilon = 0.2$.

Table 1: Metrics of proposed algorithm

(ϵ, M)	Q^a	$\hat{C}$	(ϵ, M)	Q^a	$\hat{C}$
(0.1, 2)	17	5.24	(0.1, 4)	28	4.63
(0.2, 2)	31	4.41	(0.2, 4)	42	4.05
(0.3, 2)	40	3.82	(0.3, 4)	47	3.74
(0.4, 2)	46	3.78	(0.4, 4)	48	3.67

In Fig. 1, we illustrate the performance results for the conventional scheme and the proposed solution. The average secrecy rate is increased between 10 and 38% and between 30 and 58% by the proposed solution compared to conventional scheme for $B = 8$ and $B = 4$, respectively. Since all codebook vectors are lying in the spherical cap described by the square radius in the proposed method instead of all hypersphere as in the conventional scheme, the leakage is decreased significantly. Therefore, the higher average secrecy rate is achieved even if the number of quantisation bits is quite low.

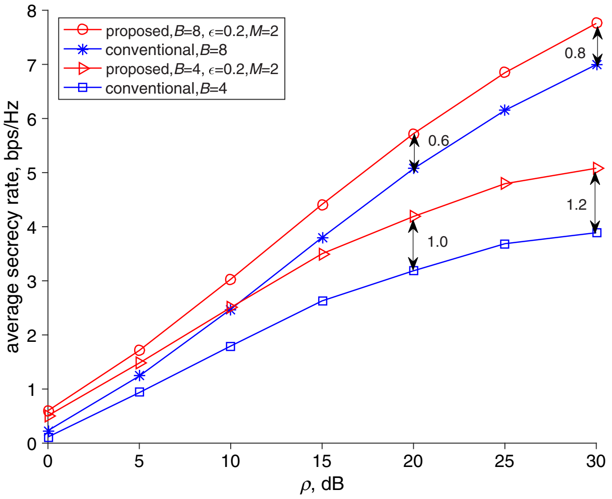

Fig. 1 *Average secrecy rate comparison of proposed algorithm and conventional scheme*

Conclusion: In this Letter, we have proposed a spatial signature for MISO-OFDM system to establish secure communications. In line with practical applications, the CSI of eavesdropper is assumed to be unknown, since eavesdroppers are passive in general. We have employed AN to disrupt the reception of eavesdropper, however this causes a leakage in case of quantised CSI of Bob is available at Alice. In order to reduce this effect, we have classified the clusters of legitimate user and have employed rotated codebook for each class of clusters based on the randomly generated complex orthogonal vectors. We have illustrated that the proposed algorithm achieves a higher secrecy rate compared to the conventional scheme.

Acknowledgment: This work was carried out in the framework of TUBITAK 114E626 Project.

Submitted: *15 February 2018*   E-first: *23 March 2018*
doi: 10.1049/el.2018.0545
One or more of the Figures in this Letter are available in colour online.

B. Ozbek (*Electrical and Electronics Engineering, Izmir Institute of Technology, Izmir, Turkey*)

✉ E-mail: bernaozbek@iyte.edu.tr

G.K. Kurt (*Electronics and Communication Engineering, Istanbul Technical University, Istanbul, Turkey*)

References

1 Hyadi, A., Rezki, Z., and Alouini, M.-S.: 'An overview of physical layer security in wireless communication systems with CSIT uncertainty', *Access*, 2016, **4**, p. 6121

2 Zhou, X., and McKay, M.R.: 'Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation', *Trans. Veh. Technol.*, 2010, **59**, p. 3831

3 Shafie, A.E., Ding, Z., and Al-Dhahir, N.: 'Hybrid spatio-temporal artificial noise design for secure MIMOME-OFDM systems', *Trans. Veh. Technol.*, 2017, **66**, (5), pp. 3871–3886

4 Rezki, Z., Khisti, A., and Alouini, M.S.: 'Ergodic secret message capacity of the wiretap channel with finite-rate feedback', *Trans. Wirel. Commun.*, 2014, **13**, p. 3364

5 Bashar, S., Ding, Z., and Li, G.Y.: 'On secrecy of codebook-based transmission beamforming under receiver limited feedback', *Trans. Wirel. Commun.*, 2011, **10**, p. 1212

6 Zhang, X., McKay, M.R., Zhou, X., *et al.*: 'Artificial-noise-aided secure multi-antenna transmission with limited feedback', *Trans. Wirel. Commun.*, 2015, **14**, p. 2742

7 Ozbek, B., and Le Ruyet, D.: 'Feedback strategies for wireless communications systems' (Springer Verlag, New York, NY, USA, 2014)