Applying energy efficient physical layer security into spatial multiplexed massive MIMO point-to-point communications

Pedro Viegas(1), David Borges(1,2), Akshkumar Rajaram(1,3), Paulo Montezuma(1,2), Dushantha Nalin K. Jayakody(3), Rui Dinis(1,2) and João Oliveira(2,4)

(1) IT, Instituto de Telecomunicações, Av. Rovisco Pais, Lisboa, Portugal.
(2) DEE, FCT Universidade Nova de Lisboa, Portugal
(3) National Research Tomsk Polytechnic University, Tomsk, Russia
(4) CTS, UNINOVA, Campus da Caparica, Portugal.

Abstract - Point-to-point wireless communications can benefit from massive multiple-input multiple-output systems (mMIMO) to attain higher data rates. But even with mMIMO systems the joint optimization of spectral and energy efficiencies can be only achieved by multilevel modulations with an efficient power amplification. Also, wireless channels are prone to be intercepted which compromises security. These constrains can be overpassed by a transmitter using several amplification branches that result from the decomposition of a multilevel constellation as a sum of quasi constant envelope signal components that are sent independently. Under these conditions, the better power amplification efficiency comes together with a physical security due to the constellation shaping according to the direction in which the antenna arrangement is optimized. Besides, this multi-amplifier structure when inserted in a multi-layered structure where the antenna arrays connected to several multi branch structures in parallel could achieve the high data rates attainable by mMIMO with spatial multiplexing, assuring at same time similar performances to conventional mMIMO systems.

Index Terms: massive MIMO systems, efficient power amplification, constellation shaping, physical layer security.

I. Introduction

One advantage of multiple-input multiple-output (MIMO) or massive MIMO (mMIMO) systems relies on the reduction of the transmitted power [1]. On the other hand, high spectral efficiency requirements of modern broadband wireless communication systems are only attainable with the use of multilevel modulations, characterized by high peak-to-average power ratio (PAPR). Although, power amplification efficiency can be improved by a transmitter structure, where multilevel constellations symbols are decomposed into a sum of several signal components that can be modulated as bi-phase shift keying (BPSK) or quadrature PSK (QPSK) signals, designed to have quasi-constant envelope [2]. The main idea behind this technique is to employ the decomposition of multilevel constellation symbols as a sum of polar components, that are modulated by as BPSK signals or that may combined in pairs to generate a set of QPSK components that are amplified by a nonlinear (NL) power amplifier [3], [2]. Since the output of each power amplifier is directly connected to an antenna, the transmitted constellation symbol will be obtained at channel level through the sum of all transmitted signals components. This structure when combined with antenna arrays makes possible the definition of a layered structure, where first layer is composed by the multi-branch amplification structure, the second layer is composed by the antenna array connected to each amplifier's output and the third layer associated to spatial multiplexing is composed by several layers 1 and 2 in parallel [4].

On the other hand high rates required by future and present wireless point-to-point communications are only possible with broadband channels prone to suffer the effects of a frequency selective channel. To cope with these effects, it is considered a single-carrier with frequency domain equalization (SC-FDE) scheme [6], [7]. Although the lower PAPR of SC-FDE schemes when compared with orthogonal frequency division multiplexing schemes (OFDM), the layer 1 multi-branch structure minimizes problems that may result from nonlinear distortion effects when high order constellations are employed in transmission.

In [5] it is was shown that a transmitter based on a double layer structure with information directivity and horizontal beamforming achieves same robustness against interference than transmitters with the common beamforming (based on a 2-D array) without penalties on system's performance. However, the applicability of this structure to mMIMO spatial multiplexing should be also analyzed, which is the purpose of this paper.

The reminder of this paper is organized as follows. Section II characterizes the transmission technique. System characterization is done in section III. Simulation results are presented in section IV. The conclusions are given in section V.

II. Layered transmitter architecture

It was already shown that multilevel constellations can be decomposed in polar components and the constellation symbols can be expressed as a function of the corresponding bits [8]. Let $\mathcal{S} = \{s_0, s_1, ..., s_(N-1)\}$, a constellation with M points (i.e., $\#\mathcal{S} = M$), where $s_n \in \mathbb{C}$. To each constellation point s_n we associate a set of $\mu = \log_2(M)$ bits in polar form $\mathcal{B} = \{b_n^0, b_n^1, ..., b_n^{(\mu-1)}\}$, with $b_n^{(i)} = \pm 1 = 2\beta_n^{(i)} - 1, \beta_n^{(i)}$ = 0 or 1. The set of μ bits can be decomposed in $M = 2^\mu$ different subsets $\mathcal{B}_m$, $m = 0, 1, ..., M-1$.

Having M constellation points in $\mathcal{S}$ and M different subsets of $\mathcal{B}$, $\mathcal{B}_0, \mathcal{B}_1, ..., \mathcal{B}_{M-1}$, we can write

$$s_n = \sum_{m=0}^{M-1} g_m \prod_{b_n^{(i)} \in \mathcal{B}_m} b_n^{(i)}, n = 0, 1, ..., M-1 \tag{1}$$

which corresponds to a system of M equations (one for each s_n and M unknown variables g_m). Without loss of generality, we can associate m to its corresponding binary representation with μ bits, i.e., $m = (\gamma_{(\mu-1,m)}, \gamma_{(\mu-2,m)}, ..., \gamma_{(1,m)}, \gamma_{(0,m)})$ and define $\mathcal{B}_m$ as the set of bits where the bit $b_n^{(i)}$ is included if and only $\gamma_{(i,m)}$ is 1. Based on that we may write

$$s_n = \sum_{m=0}^{M-1} g_m \prod_{i=0}^{\mu-1} (b_n^{(i)})^{\gamma_{(i,m)}}. \tag{2}$$

The transmitter layered structure of Fig. 1 takes advantage of this decomposition in polar components, and uses a mMIMO scheme with $N_v \times N_m \times N_b$ antenna elements, arranged in N_v sets of $N_m \times N_b$ antennas. Conventional beamforming schemes could be implemented by a layer 2 with N_b antenna elements connected to each one of N_m amplification branches. For spatial multiplexing a layer 3 with a set of $N_v \times N_m$ antennas is needed, where the N_m antennas of layer 1 are associated to the signal components of the constellation symbol and N_v sets of N_m antennas are used to transmit simultaneously N_v different constellation symbols (an example of a transmitter based on a layer 1 and layer 3 combination can be seen in Fig. 2).

It follows that power efficiency comes improved due the lower PAPR of the component signals and the possible use of NL amplifiers in layer 1 [3], [2]. Another important aspect lies on the fact that each RF chain transmits uncorrelated signals, which means an omnidirectional radiation pattern for each set of N_m antennas. However, each set of N_m antennas implements directivity at information level, since the constellation points of the transmitted signal maintain their positions at the desired direction Θ but are scrambled for other directions (it is important to mention that the phases of the NL amplifiers could be adjusted to assure configure the info directivity due to constellation shaping). Therefore, the authorized receiver can demodulate the received signal, while the undesired receivers cannot extract any useful information from the scrambled constellation. Hence, for a proper reception, the receiver needs to be in the right direction Θ_j and should know the transmitter parameters of layer 1.

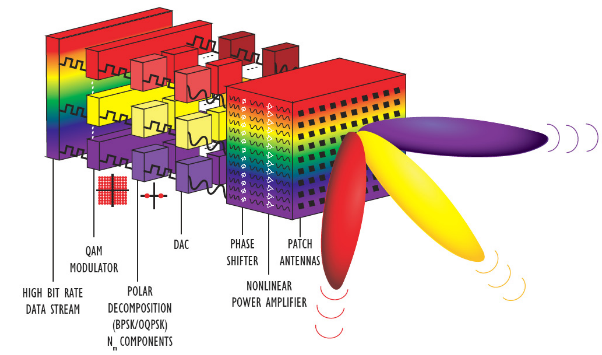

Fig. 1. Transmitter layered structure

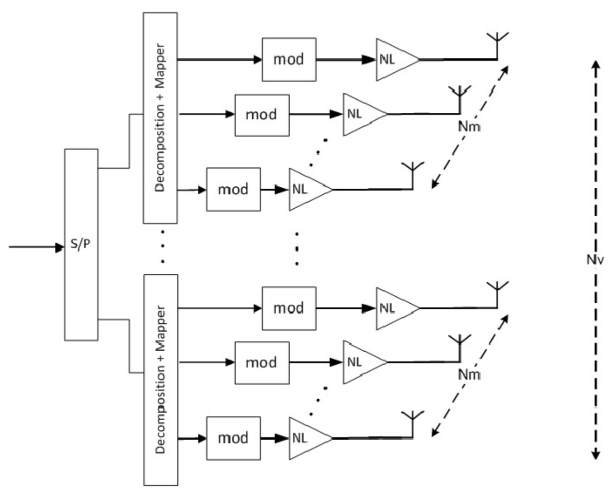

Fig. 2. Layered transmitter structure with layer 1 and layer 3.

III. System Characterization

Consider now the MIMO scenario shown in fig. 3 characterized by a point-to-point communication link between a transmitter with $T = N_v \times N_m$ antennas and a receiver with $R \geq T$ receive antennas. The transmitter's configuration has the layered structure shown in fig. 2, but were Layer 3 is composed by a set of N_v transmitters each one composed by N_m amplification branches in parallel (for QPSK and for 16-quadrature amplitude modulation (16-QAM) we have $N_m = 2$ and $N_m = 4$, respectively). This means a third layer with $T = N_v \times N_m$ antennas that transmits simultaneously N_v symbol constellations (more exactly the components of N_v symbols from a QPSK or from a 16-QAM constellation, depending on the order of the original constellation). To emphasize the physical layer security, two different kind of users are considered: one authorized named "Bob" and an unauthorized user called "Eve". Bob knows the transmitter configuration and it is also positioned in the right direction Θ (in which the constellation is optimized). On the other hand, the angular position of Eve may differ from Bob by $\Delta\Theta$. To exclude the influence of the channel, it is assumed that Eve may estimate the channel between the transmitter and Bob. By assuming this, any contribution from the channel to the security could be discarded (this situation can be generated in a scenario with a static channel or when the channel remains constant among several transmitted blocks, which is not the case of real wireless channel conditions). It is important to mention that we consider the unrealistic hypothesis that Eve could compute with a small error $\Delta\Theta$ the direction in which the constellation is optimized (this is only possible if Eve could estimate the transmitter's configuration, i.e. the spacing between antennas and the arrangements of the components among the amplification branches, since the constellation shaping is a function of both factors).

Coupling effects among antennas are avoided by a horizontal spacing of $\lambda/2$ between antennas of layer 1 and a vertical spacing of λ between each set of N_m antennas. It is assumed that all antennas at transmitter are assigned to an authorized receiver with R antennas (also Eve has the same number of antennas). For comparison purposes, a transmitter with only spatial multiplexing with 4 antennas transmitting QPSK or 16-QAM constellations without any kind of shaping according a specific direction Θ is also considered.

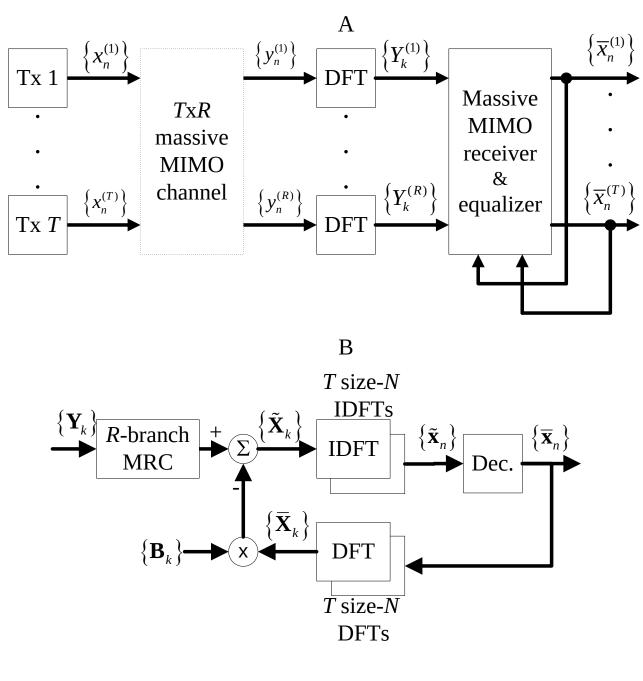

Fig. 3. Overall massive MIMO system for SC-FDE schemes (A) and detail of the massive MIMO receiver and equalization (B).

The channels between transmit and receive antennas are assumed to be time-dispersive and a SC-FDE block transmission technique is employed. To compensate the channel's frequency selectivity it can be adopted an iterative block decision feedback equalization (IB-DFE) receiver whose structure is depicted in fig. 3 [9], [10]. At transmitter the t^{th} antenna sends the block of N data symbols $\{x_n^{(t)}; n = 0, 1, ..., N-1\}$ being $\{y_n^{(r)}; k = 0, 1, ..., N-1\}$ the received block at the rth receiver's antenna. Also, an cyclic prefix with a length higher than the overall channel impulse response is appended to each transmitted block and removed at the receiver. Under these conditions, the corresponding frequency-domain received block $\{Y_k^{(r)}; k = 0, 1, ..., N-1\}$ is given by

$$\mathbf{Y}_k = \left[Y_k^{(1)} \; ... \; Y_k^{(R)}\right]^T = \mathbf{H}_k\mathbf{X}_k + \mathbf{N}_k, \tag{3}$$

where $\mathbf{H}_k$ denotes the $R \times T$ channel matrix for the kth frequency, with (r,t)th element $H_k^{(r,t)}$, $\mathbf{X}_k = \left[X_k^{(1)} \; ... \; X_k^{(T)}\right]^T$ and $\mathbf{N}_k$ denotes the channel noise.

For an iterative minimum mean squared error (MMSE) receiver the data symbols for a given iteration can be obtained from the inverse discrete Fourier transform (IDFT) of the block $\{\tilde{X}_k^{(t)}; k = 0, 1, ..., N-1\}$, where

$$\tilde{\mathbf{X}}_k = [\tilde{X}_k^1 ... \tilde{X}_k^{(R)}]^T = \mathbf{F}_k\mathbf{Y}_k - \mathbf{B}_k\overline{\mathbf{X}}_k, \tag{4}$$

(see details in [12], e.g.), where $\mathbf{I}$ is an appropriate identity matrix and $\alpha = E[|N_k^{(r)}|^2]/E[|X_k^{(t)}|^2]$ is assumed identical for all antennas t and r. Interference cancelation is done using $\overline{\mathbf{X}}_k = \left[\overline{X}_0 ... \overline{X}_{N-1}\right]$, with $\overline{X}_k$ denoting the frequency-domain average values conditioned to the FDE output for the previous iteration, which can be computed as described in [11], [12]. Coefficients F_k, B_k and the correlation coefficient ρ can be computed as described in [8], [10], [12]. Since in first iteration no information is available about the transmitted symbols and $\overline{\mathbf{X}}_k = \mathbf{0}$, this receiver can be regarded as a linear frequency-domain MMSE receiver. Next iterations will employ the average values conditioned to the receiver output from previous iteration to remove the residual intersymbol interference (ISI).

Due to matrix inversions the IB-DFE receiver has a computational complexity of $O({N_R}^3)$. To avoid this problem other two low-complexity iterative frequency-domain receivers, denoted as maximum ratio detection (MRD) and equal gain detection (EGD) are also considered [13]. Similarly to [13] the ratios R/T between receiving and transmitting antennas considered here are at least equal or higher than 4.

As mentioned in [13], the MRD receiver (see Fig. 3(B)) is characterized by

$$\tilde{\mathbf{X}}_k = \mathbf{\Psi}\mathbf{H}_k^H\mathbf{Y}_k - \mathbf{B}_k\overline{\mathbf{X}}_k, \tag{5}$$

and

$$\mathbf{B}_k = \mathbf{\Psi}\mathbf{H}_k^H\mathbf{H}_k - \mathbf{I}. \tag{6}$$

where $\mathbf{\Psi}$ denotes a diagonal matrix whose (t,t)th element is given by $\left(\sum_{k=0}^{N-1}\sum_{r=1}^{R}|H_k^{(r,t)}|^2\right)^{-1}$, takes advantage of the fact that

$$\mathbf{H}_k^H\mathbf{H}_k \approx R\mathbf{I}, \tag{7}$$

which is accurate when $R >> 1$ and the channels between different transmit and receive antennas have small correlation. On the other hand, the EGD characterized by

$$\mathbf{B}_k = \mathbf{\Psi}\mathbf{A}_k^H\mathbf{H}_k - \mathbf{I}. \tag{8}$$

where $\mathbf{\Psi}$ denotes a diagonal matrix whose (t,t)th element is given by $\left(\sum_{k=0}^{N-1}\sum_{r=1}^{R}|H_k^{(r,t)}|\right)^{-1}$, takes advantage of the fact that for mMIMO systems with $R \gg 1$ and small correlation between the channels associated to different transmit and receive antennas, the elements outside the main diagonal of

$$\mathbf{A}_k^H\mathbf{H}_k \tag{9}$$

are much lower than the ones at its diagonal, where $(i,i')th$ element of the matrix $\mathbf{A}$ is $[\mathbf{A}]_{i,l} = \exp(j\arg([\mathbf{A}]_{i,l}))$.

IV. Simulation results

Monte Carlo experiments are used to obtain the average results of bit error rate (BER) for a Rayleigh channel. Regarding layer 1 configuration two hypotheses are considered: in the first one we have $N_m = 2$ and an QPSK as original constellation that is decomposed into BPSK components. In the second one we have a 16-QAM constellation that is decomposed in $N_m = 4$ BPSK components. For both hypotheses we have $N_v = 4$. In both hypothesis the transmitted symbols x_n are selected with equal probability from the original constellation. It is assumed linear power amplification at the transmitter and perfect synchronization at the receiver. The results are expressed as function of $\frac{E_b}{N_0}$, where $N_0/2$ is the noise variance and E_b is the energy of the transmitted bits.

Results shown in Figs. 4 and 5 refer a layer 1 with $N_m = 2$ and angular separations between Bob and Eve of $\Delta\Theta = 5^o$, $\Delta\Theta = 10^o$ and $\Delta\Theta = 15^o$ (it is worth recalling that $\Delta\Theta = 0^o$ corresponds always to the case of the transmission between the transmitter and the authorized receiver Bob). Values of $R/T = 4$ and $R/T = 8$ are adopted in Figs. 4 and 5, respectively. From the comparison of both figures, it becomes clear that when the ratio R/T grows the gap between the MRD and the EGD receiver vanishes (as we can see in Fig. 5 performance curves of receivers overlap which is not the case of Fig. 4). It is also clear that despite the performance improvement achieved by the higher value of R/T, the performance impact of constellation shaping is similar in both situations (a degradation near to 8 dB for a BER of 10^-4 and 4 iterations). It is also observed that the IB-DFE exhibits more robustness to the constellation shaping, even for an angular separation of $\Delta\Theta = 15^o$. On the other hand, both MRD and EGD are severely affected by angular separations higher than $\Delta\Theta = 10^o$. Also, as expected both IB-DFE and MRD receivers perform better than EGD. Also, the result for $\Delta\Theta = 0^o$ are the same obtained by a conventional spatial multiplexing scheme, which means that combination of layer 1 and layer 3 can be adopted without sacrificing system's performance. Regarding the security level assured by this transmitter, it is obvious that more components should be applied in layer 1, since the sensitivity of all receivers to any angular separation between Bob and Eve should be increased.

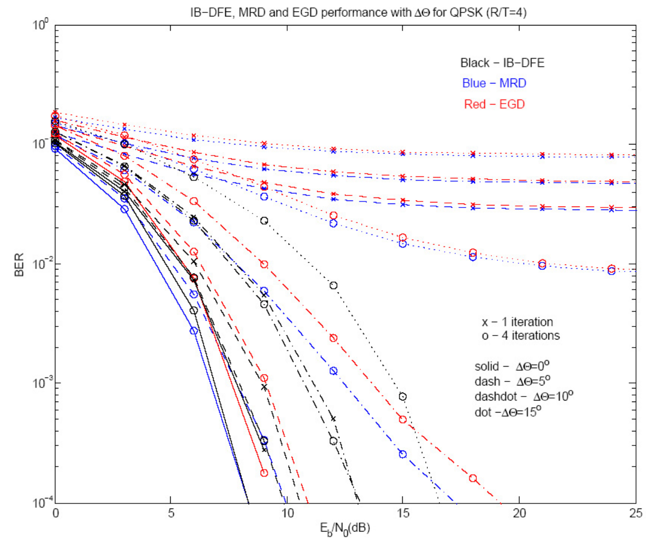

Fig. 4. BER performance with $N_m = 2$ with $\Delta\Theta$ and $R/T = 4$.

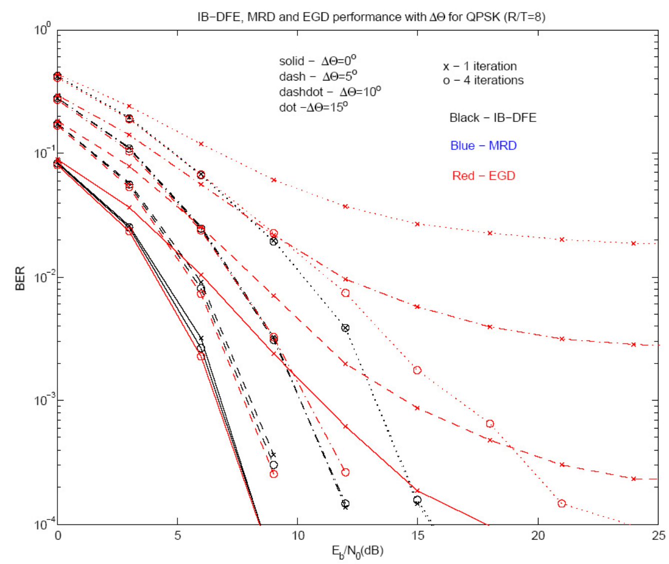

Fig. 5. BER performance with $N_m = 2$ with $\Delta\Theta$ and $R/T = 8$.

In the next set of simulations it is considered the second hypotesis with a layer 1 with $N_m = 4$, i.e. a 16-QAM decomposed into 4 BPSK components. Since we have a stronger shaping of the constellation symbols due to the higher number of components, different and smaller angular separations are now considered between Bob and Eve. Instead of $\Delta\Theta$ until 15^o the values of $\Delta\Theta$ are now 2^o and 5^o. Also, a value of 8 is adopted for the ratio R/T (as seen in previous results this ratio assures better performance. Thus, it is important to evaluate if higher ratios could compromise the physical security achieved by schemes with higher N_m).

From the results of Fig. 6 it is clear that both IB-DFE and MRD receivers have similar performances (the curves of both overlap for the various numbers of iterations). Also, as expected, for Bob, these two receivers perform better than the EGD one. Also, the results for $\Delta\Theta = 0^o$ are the same obtained by a conventional spatial multiplexing scheme, which means that combination of layer 1 and layer 3 can be adopted without sacrificing system's performance. On the other hand, better security is assured. This can be seen in Fig. 7 where it is obvious the higher impact on system performance of any angular error. For $\Delta\Theta = 5^o$ the BER near 0.5 means that Eve can't decode any useful information. Even when $\Delta\Theta = 2^o$ at least 4 iterations are needed to assure a BER of 10^{-3} (which is only attainable by the EGD receiver for a SNR of 25 dB, since the other two ones are severed affected by the angle offset). It can be also observed the high sensitivity exhibited by the IB-DFE and MRD receivers to any angular separation between Bob and Eve. This behavior can be seen in the results for $\Delta\Theta = 2^o$, where both IB-DFE and MRD receivers perform worse than the EGD.

Also, all performance results show that security due to constellation shaping is achieved independently the type of adopted receiver, since the performance of all receivers is severely affected when $\Delta\Theta \geq 10^o$ or $\Delta\Theta \geq 2^o$ for $N_m = 2$ and $N_m = 4$, respectively. More interestingly, good physical security can be assured in point-to-point communication links with only 4 antennas (for $N_m = 2$ previous results showed good tolerance against $\Delta\Theta \leq 10^o$, which can compromise the security when Eve is placed near Bob).

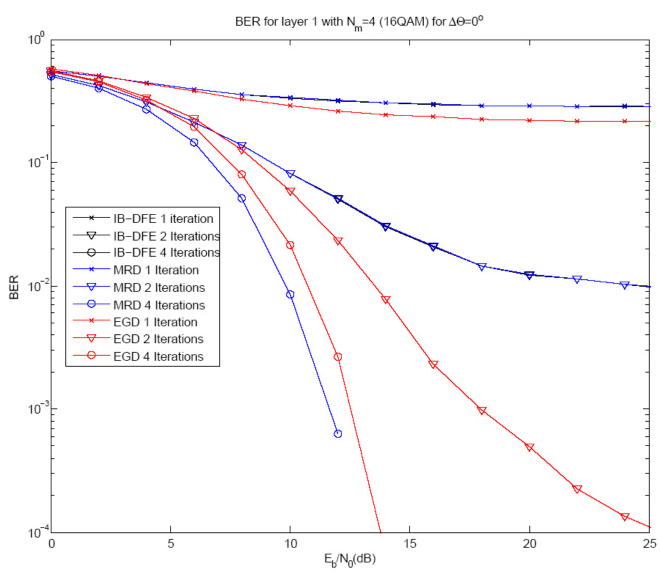

Fig. 6. BER performance with $N_m = 4$ with $\Delta\Theta = 0$ and $R/T = 8$.

V. Conclusions

In this paper it was shown that a transmitter based on a double layer structure with information directivity and spatial multiplexing could be employed with multilevel constellations to improve power amplification efficiency and to assure physical security. Since BER results achieved by both options for $\Delta\Theta = 0^o$ are similar to those of classical spatial MIMO multiplexing, the higher power amplification efficiency and physical layer security came without sacrifice on system's performance.

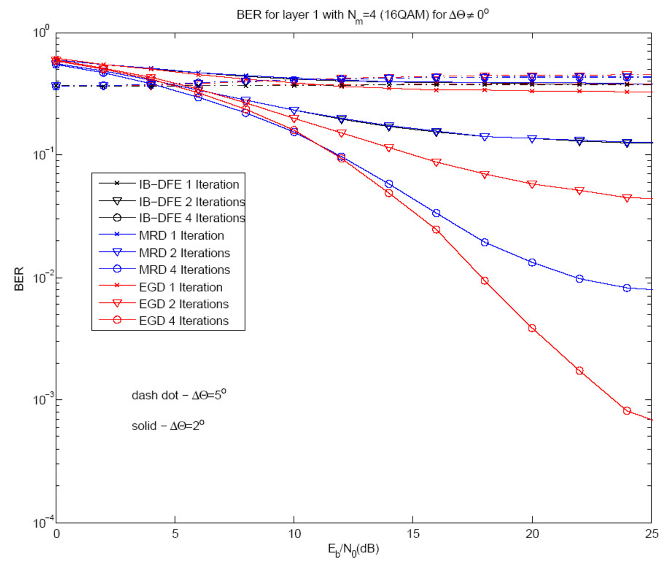

Fig. 7. BER performance with $N_m = 4$ with $\Delta\Theta = 2^o$ or $\Delta\Theta = 5^o$ and $R/T = 8$.

Despite of using more antennas than the traditional scheme, in further millimetric wave communication systems this factor will be not a restriction.

Acknowledgments

This work was supported in part by CTS multi-annual funding project PEst-OE/EEI/UI0066/2011,IT UID/EEA/50008/2013 (plurianual founding and project GLANCES) and UID/EEA/50008/2013 - MM5G.

References

[1] F. Boccardi, R. Heath, A. Lozano, T. Marzetta, P. Popovski, "Five disruptive technology directions for 5G", *IEEE Communications Magazine*, Vol. 52, No. 2, pp.74-80, Feb. 2014.

[2] V. Astucia, P. Montezuma, R. Dinis and M. Beko, "On the use of Multiple grossly Nonlinear amplifiers for Higly Efficient Linear amplification of multilevel constellations", *Proc. IEEE VTC2013-Fall*, Las Vegas, NV, US, September 2013.

[3] P. Montezuma and A. Gusmão, "Design of TC-OQAM Schemes Using a Generalised Nonlinear OQPSK-type Format",*IEE Elect. Letters*, Vol. 35, No. 11, pp. 860-861, May 1999.

[4] P. Montezuma and R. Dinis, "Implementing Physical Layer Security Using Transmitters with Constellation Shaping", *Proc. IEEE ICCCN2015*, Las Vegas, NV, US, August 2015.

[5] A. Ferreira, G. Gaspar, P. Montezuma and R. Dinis,"Combining info and spatial directivities in multiple antenna transmission systems", *IEEE YEF-ECE 2017*, Costa da Caprica, May 2017.

[6] D. Falconer, S. Ariyavisitakul, A. Benyamin-Seeyar and B. Eidson, "Frequency Domain Equalization for Single-Carrier Broadband Wireless Systems", *IEEE Comm. Mag.*, vol. 4, no. 4, pp.5866, April 2002.

[7] A. Gusmão, R. Dinis, J. Conceicão and N. Esteves, "Comparison of Two Modulation Choices for Broadband Wireless Communications",*IEEE VTC00(Spring)*, vol. 2, May 2000.

[8] R. Dinis, P. Montezuma, N. Souto, and J. Silva, ”Iterative Frequency-Domain Equalization for General Constellations”, *IEEE Sarnoff Symposium*, Princeton, USA, Apr. 2010.

[9] N. Benvenuto and S. Tomasin, “Block Iterative DFE for Single Carrier Modulation”, *IEE Elec. Let.*, Vol. 39, No. 19, pp. 1144–1145, Sep. 2002.

[10] R. Dinis, R. Kalbasi, D. Falconer and A. Banihashemi, “Iterative Layered Space-Time Receivers for Single-Carrier Transmission over Severe Time-Dispersive Channels”, *IEEE Comm. Letters*, Vol. 8, No. 9, pp. 579–581, Sep. 2004.

[11] F. Silva, R. Dinis and P. Montezuma, ”Estimation of the feedback reliability for IB-DFE receivers”, *ISRN Communications and Networking*, Vol. 2011, Article No. 30, Jan. 2011.

[12] P. Silva, R. Dinis, *Frequency-domain multiuser detection for CDMA systems*, River Publishers, Aalborg, 2012.

[13] David Borges, Paulo Montezuma, Rui Dinis, ”Low complexity MRC and EGC based receivers for SC-FDE modulations with massive MIMO schemes”, *2016 IEEE GlobalSip*, Washington, DC, USA, Dec. 2016.