Smart Receiver for Multi-antenna Transmitters with Constellation Shaping

Paulo Montezuma[1, 2, 3], **Sara Ribeiro**[1], **Mario Marques da Silva**[2, 4], **and Rui Dinis**[1, 2]

[1]DEE, FCT Universidade Nova de Lisboa, Portugal
[2]IT, Instituto de Telecomunicações, Av. Rovisco Pais, Lisboa, Portugal
[3]Uninova, Instituto de Desenvolvimento de Novas Tecnologias, Quinta da Torre, Caparica, Portugal
[4]Universidade Autonoma de Lisboa, Portugal

Abstract— Spectral and power efficiency together with physical layer security can be achieved by a MISO (Multiple Input Single Output) where multilevel modulations are decomposed as a sum of BPSK (Bi Phase Shift Keying) components that are combined at channel level. The directivity is associated to the transmitted information due to the shaping of the constellation in a desired direction Θ (it is important to note that shaping means a rearrangement of the constellation symbols according to a desired direction Θ) and can be be increased by changes on phases phase shifts between antenna array or changes on the values of the coefficients that define the BPSK components. Consequently, for successful data reception it is necessary to know the configuration parameters used at transmitter. Despite the security achieved by this transmitter structure, a practical application is only possible if authorized receivers are able to decode with success the transmitted data. Here it is demonstrated the validity of the hypothesis of a smart receiver that knows these parameters based on a algorithm that can estimate the set of coefficients applied in constellation shaping and the array configuration. The cases analyzed here and the simulation results presented show that good performance is attainable by the proposed receiver, even when the directivity increases with the number of BPSK components used in the decomposition of the multilevel constellation, which validate our initial assumption.

1. INTRODUCTION

Security, power and spectral efficiencies are important requirements in wireless communication systems. The first one can be achieved by encrypted schemes from higher layers or physical layer security schemes or association of both [1–3]. On the other hand, MIMO (Multiple-input multiple-output) systems can be employed to overpass power and bandwidth constrains so common in wireless communications systems. However, the need of high spectral efficiencies apart from making scarcely recommendable physical security solutions based on codes [3], are also only attainable by multilevel constellations usually characterized by significant envelope fluctuations that compromise efficiency of power amplification. Thus, both redundancy (associated to the coded bits) and restrictions on power amplification should be avoided. These two problems can be overpassed by a transmitter structure where multilevel constellations are the sum result of several uncorrelated BPSK (Bi Phase Shift Keying) that are amplified and transmitted independently by an antenna. Obviously, this transmitter requires a separate RF (Radio frequency)-branch including a power amplifier for each antenna element [4, 5], being each RF chain associated to a BPSK sub-constellation that is combined at channel level to generate the desired multilevel constellation. Power of efficiency of amplification is improved since the constant envelope components allow the use of nonlinear (NL) amplifiers power amplification [6, 7]. Security is assured through the optimization of the transmitted constellation in the desired direction Θ, by a proper shaping of the constellation's symbols. Therefore, instead directivity on radiation pattern we have directivity at information level, i.e., at the transmitted constellation. When non compensated, this constellation shape acts as a nonlinear distortion due to phase rotations of components associated to each amplification branch (it should be noted that phase shifts between antennas also change the distances between constellation's symbols which has impact on system performance). Several factors such as the set of coefficients g_i or the distance between antennas affect directivity and the shape of the constellation. Consequently, for successful data reception it becomes crucial a robust receiver based on an algorithm that estimates the set of coefficients used at the transmitter.

Several indicators are considered to evaluate smart receiver under this security scheme such as mutual information (MI) and the bit error performance (BER) of smart receiver. It is well known that large constellations in general and non-uniform constellations in particular are very sensitive to interference, namely the residual ISI (Inter-Symbol Interference) due to frequency selective channel

effects. To cope with channel effects we consider the use of SC-FDE (Single-Carrier with Frequency-Domain Equalization) schemes, with IB-DFE (Iterative Block Decision Feedback Equalization) that can reduce substantially ISI [8, 9] levels in these constellations.

In this paper we consider how to exploit a multi-branch transmission technique with constellation shaping as a novel signal processing technique to introduce some kind of physical layer security. We admit similar channels between the source and intended receiver and between the source and the eavesdropper. We start in Section 2 by characterizing the new transmission technique. The rest of this paper is organized as follows: A brief characterization of the receiver is made in Section 4. A set of performance results is presented in Section 4.1. Section 5 resumes this paper.

2. TRANSMITTER STRUCTURE

Let us consider the transmitter whose structure is depicted in Figure 1. Contrarily to MIMO, the N_m RF branches are employed to allow an efficient amplification of the signals associated to a large constellation. Firstly, the data bits are mapped into a given constellation (e.g., a QAM (Quadrature Amplitude Modulation) constellation) characterized by the ordered set $\mathfrak{S} = \{s_0, s_1, \ldots, s_{M-1}\}$ following the rule $(\beta_n^{(\mu-1)}, \beta_n^{(\mu-2)}, \ldots, \beta_n^{(1)}, \beta_n^{(1)}) \mapsto s_n \in \mathfrak{S}$, with $(\beta_n^{(\mu-1)}, \beta_n^{(\mu-2)}, \ldots, \beta_n^{(1)}, \beta_n^{(1)})$ denoting the binary representation of n with $\mu = \log_2(M)$ bits. Next, the constellations symbols are decomposed in M_m polar components, i.e.,

$$s_n = g_0 + g_1 b_n^{(1)} + g_2 b_n^{(2)} + g_3 b_n^{(1)} b_n^{(2)} + g_4 b_n^{(3)} + \ldots = \sum_{i=0}^{M-1} g_i \prod_{m=0}^{\mu-1} \left(b_n^{(m)}\right)^{\gamma_{m,i}}, \tag{1}$$

with $(\gamma_{\mu,i}\, \gamma_{\mu-1,i} \ldots \gamma_{2,i}\, \gamma_{1,i})$ denoting the binary representation of i and $b_n^{(m)} = (-1)^{\beta_n^{(m)}}$ is the polar representation of the bit $\beta_n^{(m)}$. Thus, we have M constellation symbols in $\mathfrak{S}$ and M complex coefficients g_i, (1) is a system of M equations that can be used to obtain the coefficients g_i, $i = 0, 1, \ldots, M-1$. Let N_m denote the number of non-zero coefficients g_i coefficients, then a given constellation can be decomposed as the sum of $N_m \leq M$ polar components. Each one of the N_m polar components is modulated as a BPSK signal, that can be a serial representation of an OQPSK signal [10], with reduced envelope fluctuations and compact spectrum (e.g., a gaussian minimum shift keying (GMSK) signal). The corresponding signals are separately amplified by N_m nonlinear amplifiers before being transmitted by N_m antennas.

Since the N_m BPSK components in RF branches are uncorrelated, the N_m antenna array changes the constellation shape to optimize it in a desired direction Θ keeping at same time unchanged the radiation pattern. Consequently, security is assured through the optimization of the transmitted constellation in the desired direction Θ, by a proper shaping of the constellation's symbols. This means that when the set of coefficients g_i and the array configuration are unknown, the receiver is unable to compensate the nonlinear distortion that affects the transmitted constellation. Due to the high number of factors affecting the shape of the transmitted constellation, complexity is also assured (complexity analysis it will be analyzed in future work but now it is beyond the scope of

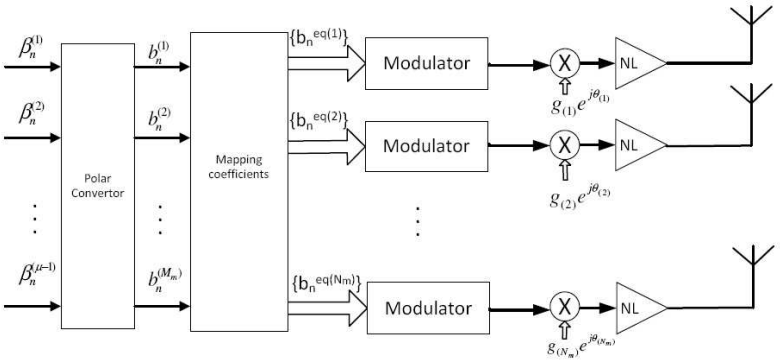

Figure 1: Structure of constellation directive transmitter.

the present paper). However, a smart receiver with knowledge about the set of coefficients g_i and array configuration is able to decode data successfully, as it will be seen in next sections.

3. MOTIVATIONS FOR A SMART RECEIVER

The motivation behind the smart receiver lies on the fact that when are known the transmitter parameters at the receiver the transmitted data can be received with success, as we shall see from the results posted in this section. Having in mind these considerations, we also present some results regarding the mutual information associated to smart receiver that sustain our initial hypothesis. It is assumed that the receiver knows the transmitter coefficients g_i as well as the array configuration. We admit that BPSK components follow a linear and uniform arrangement with antennas equal spaced by $d/\lambda = 1/4$ at the transmitter. We assume an Additive White Gaussian (AWGN) channel. Let $s(t)$ denote the nth transmitted symbol associated to a given block

$$s(t) = s_n h_T(t - nT_S), \tag{2}$$

with T_S denoting the symbol duration and $h_T(t)$ denoting the adopted pulse shape. s_n belongs to a given size-M constellation $\mathfrak{S}$. Under these conditions the received signal is

$$y(t) = f_A(s(t)) + n(t), \tag{3}$$

with $n(t)$ denoting de noise term and where f_A denotes the shaping performed by the transmitter array.

With perfect secrecy we have $I(S;Y) = 0$, with S the sent message, Y the received message and $I(;)$ the mutual information. It should be noted that the mutual information (assuming equiprobable symbols) for a given signal set $\mathfrak{S}$ gives the maximum transmission rate (in bits/channel use) at which error-free transmission is possible with such constellation set [11], and can be written as

$$I(S,Y) = \log_2 M - \frac{1}{M}\sum_{s\in\mathfrak{S}} \mathbf{E}_n \left[\log_2 \left(\sum_{s'_n \in \mathfrak{S}} \exp\left(-\frac{1}{N_0} \left| \sqrt{Es}(s_n - s'_n) + n \right|^2 - |n|^2 \right) \right) \right], \tag{4}$$

where $\mathbf{E}$ denotes the expectation.

16-QAM with gray mapping is characterized by the set of non null coefficients $g_{34} = 2j$, $g_1 = 1$, $g_3 = 2$ and $g_{12} = j$, associated to the antennas $1, 2, 3$ and 4, respectively. 64-QAM is characterized by 6 coefficients with values $2j$, 1, 2, j, 4 and $4j$ associated to the antennas $1, 2, 3, 4, 5$ and 6, respectively.

Average results for MI are assured by independent trials of Monte Carlo experiments. For both constellations sizes, symbols s_n are selected with equal probability from $\mathfrak{S}$. Some MI 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.

In Figure 2 it can be seen the MI behavior with the constellation optimization angle Θ for 16-QAM and 64-QAM, respectively. It is obvious that MI remains practically unaffected for the different values of Θ. This means that our initial hypothesis is valid since the smart receiver is able to decode the sent information independently of the direction in which the constellation is optimized. On the other hand, if coefficients g_i are only approximately known, distortion arises and MI becomes affected. To have an idea of the effects of any imprecision we also include Figures 3 and 6 with the MI results expressed as function of $\frac{E_b}{N_0}$ when errors on g_i estimates lead several Θ estimation errors (estimation errors of 4° and 8° are considered and we assume $\Theta = 75^\circ$). As we can see from these figures, the tolerance against estimation errors decreases with constellation size. For example, in 64-QAM the tolerance is $\Delta\Theta \leq 2^\circ$, since for higher errors the MI values are severely affected. On the other hand, in 16-QAM the MI is less affected by estimation errors, which means higher tolerance to errors on the estimate of Θ. This was expected, since the directivity and corresponding constellation shaping increases with the number of RF branches.

Let assume that a eavesdropper knows the initial set of parameters but is unable to estimate the new parameters related with the constellations optimized for $\Theta + \Delta\Theta$ with $\Delta\Theta = 0^\circ, 4^\circ$ and 8°. From results of Figures 3 and 6 it is obvious the inherent security achieved by this transmitter. Obviously, if the eavesdropper do not have any information about the coefficients g_i and the array configuration the MI is always null for both constellation sizes.

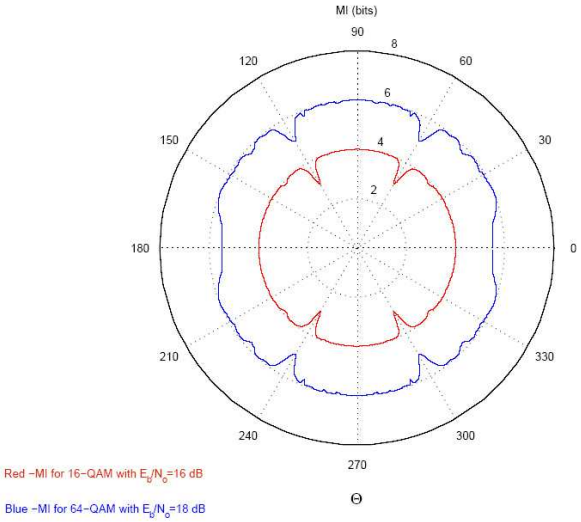

Figure 2: MI behavior with the angle Θ for 16-QAM and 64-QAM.

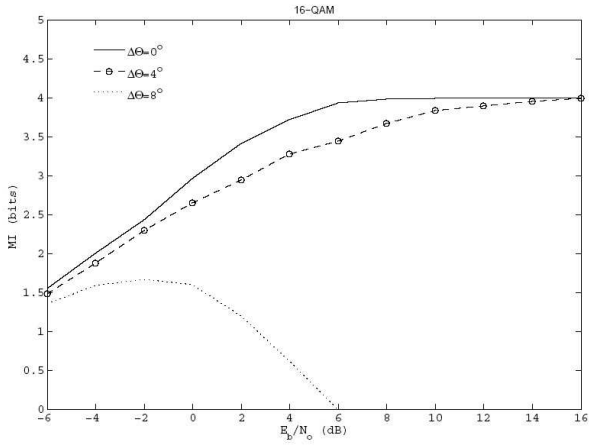

Figure 3: MI evolution for 16QAM and impact of an angle error regarding the transmission direction Θ.

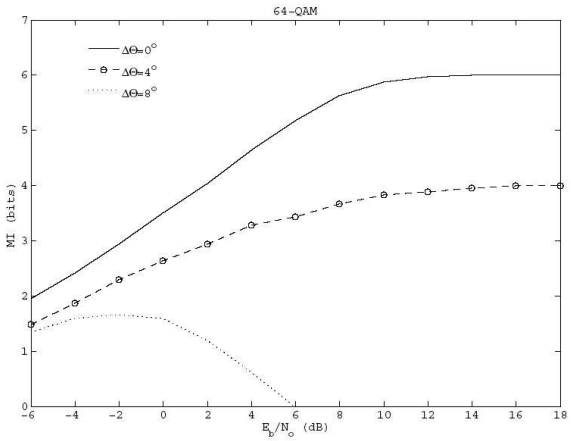

Figure 4: MI evolution for 64QAM and impact of an angle error regarding the transmission direction Θ.

4. BEHAVIOR IN FREQUENCY SELECTIVE CHANNELS

Since we admit that the smart receiver knows the channel and the set of N_m coefficients g_i, phase rotations due to channel or phase shifts associated to the array's configuration can be easily compensated. These operations must be performed before the IB-DFE receiver whose structure is depicted in Figure 5. We assume constant envelope signals in each amplification branch. Under these conditions the signal associated to a given block is

$$s(t) = \sum_{n=-N_G}^{N-1} s_n h_T(t - nT_S), \tag{5}$$

with T_S denoting the symbol duration, N_G denoting the number of samples at the cyclic prefix, N denoting the number of samples at the useful part of the block and $h_T(t)$ denoting the adopted pulse shape. The nth transmitted symbol s_n belongs to a given size-M constellation $\mathfrak{S}$. As usual, the cyclic prefix corresponds to a periodic extension of the useful part of the block, i.e., $s_{-n} = s_{N-n}$ with a length higher than the overall channel impulse response.

The samples associated to the cyclic prefix are discarded, which means null IBI (Inter Block Interference) and reduces the impact of a time-dispersive channel to a scaling factor for each frequency. Thus, the corresponding frequency-domain block is $\{Y_k; k = 0, 1, \ldots, N-1\}$ = DFT

$\{y_n; n = 0, 1, \ldots, N-1\}$), where

$$Y_k = S_k H_k + N_k, \tag{6}$$

with H_k denoting the channel frequency response for the kth subcarrier and N_k the corresponding channel noise.

For a given iteration the output samples are given by

$$\tilde{S}_k = F_k Y_k - B_k \overline{S}_k, \tag{7}$$

where $\{F_k; k = 0, 1, \ldots, N-1\}$ and $\{B_k; k = 0, 1, \ldots, N-1\}$ denote the feedforward and the feedback coefficients, respectively, and $\{\overline{S}_k; k = 0, 1, \ldots, N-1\}$ is the DFT of the block $\{\overline{s}_n; n = 0, 1, \ldots, N-1\}$, with $\overline{s}_n$ denoting the average value of s_n conditioned to the FDE output associated to the previous iteration. It can be shown that the optimum coefficients F_k, B_k and the correlation coefficient ρ are computed as described in [12, 13].

4.1. Numerical Results

To evaluate the smart receiver's performance, here we focus on the performance of the proposed system in a severely time-dispersive channel, characterized by an uniform PDP (Power Delay Profile), with 32 equal-power taps, with uncorrelated rayleigh fading on each tap. We also make the practical assumption of linear power amplification at the transmitter, perfect synchronization and channel estimation at the receiver. Results are expressed as function of $\frac{E_b}{N_0}$. It is assumed that the smart receiver can estimate the transmitter parameters with or without error. It is adopted a SC-FDE modulation with blocks of $N = 256$ useful symbols plus a cyclic prefix of 32 symbols longer than overall delay spread of the channel. We also assumed that the eavesdropper has information about the initial configuration of the transmitter under the direction Θ (for example we assume $\Theta = 75°$, but the results are similar for other values). However, is unable to estimate the small changes made in configuration parameters associated to a change of 4° in the direction Θ. It should be mentioned that when no information is available at eavesdropper the BER assumes a irreducible value near 0.5, for both constellations sizes.

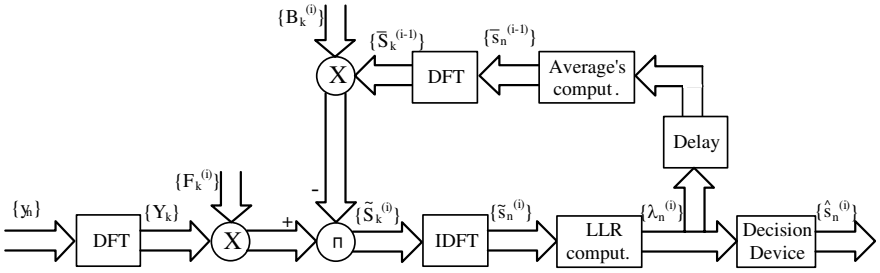

Figure 5: IB-DFE receiver with soft decisions.

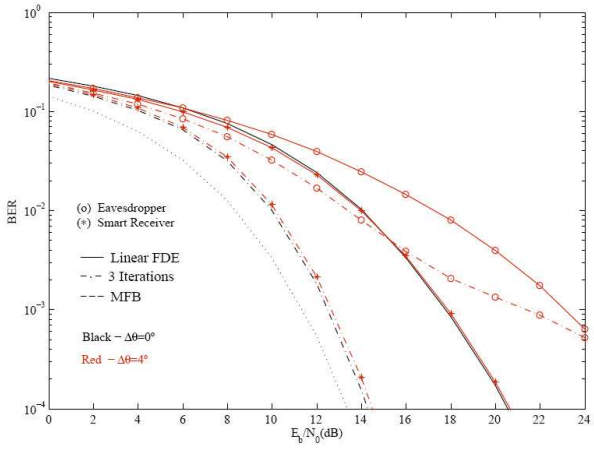

Figure 6: BER performance for size-16 constellations in a frequency selective channel and an angle error regarding to the transmission direction Θ.

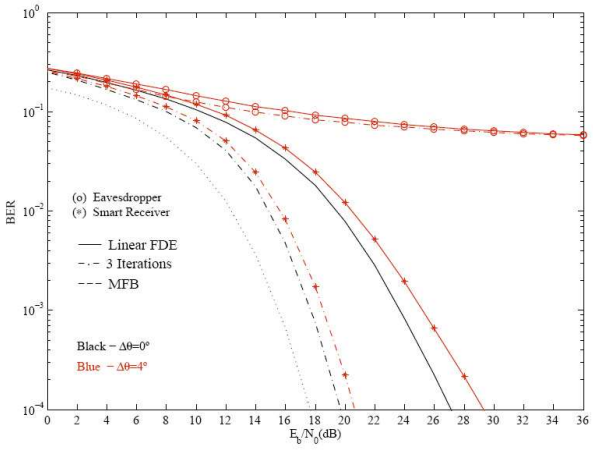

Figure 7: BER performance for size-64 constellations in a frequency selective channel and an angle error regarding to the transmission direction Θ.

In Figure 6 are shown the BER performance results for transmission schemes with 16-size constellations. Simulation results from Figure 6 lead us to conclude that the smart receiver together with the iterations of IB-DFE can cope with change in direction Θ without significant performance degradation. Figure 7 refers constellations with 64-symbols. As we can see, it is obvious the higher impact of estimation errors on BER, when compared with the transmission scheme based on 16-QAM. This was a expectable result, since the number of real components and antennas for 16-QAM is lower than the number of transmission branches in 64-QAM, the smart receiver can estimate more efficiently angle changes in the first case. Results from Figure 6 and 7 also demonstrate that despite the efficiency of smart receiver, the significant degradation associated to any estimation error means a strictly directive communication with the information only optimized in the desired direction Θ. This can be seen on the results regarding the eavesdropper for 64-QAM (for 16-QAM we have a small degradation but we assumed that the initial parameters about the configuration of the transmitter were available to the eavesdropper. So, the error on estimation of 4° has small impact on performance). Therefore, security is also assured since any eavesdropper is unable to decode data successfully without information about transmitter's configuration parameters.

5. CONCLUSIONS

In this paper we considered the smart receiver hypothesis for a system using multi-antenna transmission structure with constellation shaping of the transmitted information. It was shown the validity of the smart receiver hypothesis, since when the receiver is able to estimate the set of coefficients g_i used for constellation shaping at the transmitter, the MI is practically independent of the angle Θ in which the transmitted constellation is optimized. Also results demonstrated the high sensitivity of MI and system performance when estimation errors on g_i coefficients lead to angle estimate errors higher than 2°, which imposes restrictions to any estimation algorithm to be used at receiver level. We also gave some insights about the constellation shaping potential for physical layer security and the capacity of a smart receiver. Further studies shall include the performance analysis of different algorithms for estimation of g_i parameters to be applied in smart receiver implementations for both AWGN and fading channels as well as the optimization of the constellation directivity with other array configurations.

ACKNOWLEDGMENT

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), GALNC EXPL/EEI-TEL/1582/2013, EnAcoMIMOCo EXPL/EEI-TEL/2408/2013 and CoPWIN PTDC/EEI-TEL/1417/2012.

REFERENCES

1. Bloch, M., J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, Vol. 54, No. 6, 2515–2534, June 2008.
2. Massey, J. L., "An introduction to contemporary cryptology," *Proc. IEEE*, Vol. 76, No. 5, 533–549, May 1988.
3. Harrison, W. K., J. Almeida, M. R. Bloch, S. W. McLaughlin, and J. Barros, "Coding for secrecy: An overview of error-control coding techniques for physical-layer security," *IEEE Signal Process. Mag.*, Vol. 30, No. 5, 41–50, September 2013.
4. Marques da Silva, M. and F. A. Monteiro, *MIMO Processing for 4G and Beyond: Fundamentals and Evolution*, CRC Press Auerbach Publications, ISBN: 9781466598072, FL, USA, May 2014, http://www.crcpress.com/product/isbn/9781466598072.
5. Tse, D. N. C. and P. Viswanath, *Fundamentals of Wireless Communications*, Cambridge University Press, Cambridge, UK, 2005.
6. Montezuma, P. and A. Gusmão, "Design of TC-OQAM schemes using a generalised nonlinear OQPSK-type format," *IEE Elect. Letters*, Vol. 35, No. 11, 860–861, May 1999.
7. Astucia, V., 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.
8. Benvenuto, N. and S. Tomasin, "Block iterative DFE for single carrier modulation," *IEE Elec. Let.*, Vol. 39, No. 19, 1144–1145, September 2002.

9. Dinis, R., 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, 579–581, September 2004.
10. Amoroso, F. and J. Kivett, "Simplified MSK signalling technique," IEEE Trans. on Comm., Vol. 25, April 1977.
11. Caire, G., G. Taricco, and E. Biglieri, "Bit-interleaved coded modulation," *IEEE Trans. Inf. Theory*, Vol. 44, 927–947, May 1998.
12. Dinis, R., P. Montezuma, N. Souto, and J. Silva, "Iterative frequency-domain equalization for general constellations," *IEEE Sarnoff Symposium*, Princeton, USA, April 2010.
13. Gusmão, A., P. Torres, R. Dinis, and N. Esteves, "A turbo FDE technique for reduced-CP SC-based block transmission systems," *IEEE Trans. on Comm.*, Vol. 55, No. 1, 16–20, January 2007.