Physical Layer Security Scheme Based on Power Efficient Multi-antenna Transmitter

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

[1]CTS, Uninova, Dep.^{o} de Eng.^{a} Electrotécnica, Faculdade de Ciências e Tecnologia, FCT
Universidade Nova de Lisboa, Caparica 2829-516, 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— Security is a demanding challenge in wireless systems due to the broadcast nature of the channel. One the other hand security at physical layer can increase overall system's security since it can be combined with other security schemes from higher layers. High throughput required by modern wireless networks can be assured by MIMO (Multiple-input multiple-output), but when high spectral efficiencies are needed multilevel modulations with high peak-to-average power ratios should be used, which may affect efficiency of power amplification. This problem can be avoided by the MISO (Multi input Single Output) transmitter considered here, where transmitted multilevel constellations are the result of the combination of several uncorrelated BPSK (Bi-Phase Shift Keying) components, that are amplified and transmitted independently by an antenna. The constellation shaping done by this transmitter means directivity in the transmitted constellation that can be used to assure security at physical layer. Security as well complexity are assured since any eavesdropper must know the set of coefficients associated to each BPSK component as well as the antenna array configuration. It is shown that the inherent security assured by this transmitter allows secrecy at physical layer. Several examples are analyzed and the corresponding results show the effectiveness of the proposed approach to implement a security scheme at physical layer level.

1. INTRODUCTION

Mobile communication systems must support multiple users achieving at same time privacy of users contents. Moreover, the broadcast nature of wireless channel makes it even more demanding any security solution. It is well known that common security solutions are based on encrypted algorithms from higher layers, such as private and public encrypted keys [1–3]. One advantage of physical layer security schemes relies on the fact that they may be combined with other schemes from higher layers to increase overall security. Coding or channel state information can be used to assure physical security. However, these approaches compromise spectral efficiency or are inadequate for static channels. For these reasons, it is desirable a physical security scheme without coding and independent of channel state information, where security is achieved trough constellation mappings and shaping for specific directions that are introduced at transmitter level.

MIMO (Multiple-input multiple-output) as well as MISO (Multiple Input single Output) systems can increase throughput in modern wireless networks and reduce interference [4]. Other advantage of MIMO systems is the reduction of the transmitted power. On the other hand, high spectral efficiency is only attainable by multilevel modulations characterized by high peak-to-average power ratios (PARP), which may affect efficiency of power amplification. This problem can be avoided with a transmission scheme, where the constellations are decomposed on several uncorrelated BPSK (Bi-Phase Shift Keying), QPSK (Quadri Phase Shift Keying) or OQPSK (Offset QPSK) components, being each component amplified and transmitted independently by an antenna [5, 6]. This approach also avoids combination losses since the several signal components are combined at channel level. Security is also assured, since the constellation shaping introduced by the MISO transmitter means that we have directivity at the constellation level that can be employed to assure security at physical layer [7]. Therefore, the inherent security lies on the constellation directivity, i.e., in the direction in which the constellation is optimized, which can be improved by changes on coefficients' phases or using constellations that are decomposed with an higher number of BPSK components. High computational complexity associated to interception is also achieved because each user must know the set of coefficients associated to the BPSK components as well as the array configuration, otherwise receives useless data. Moreover, the security implemented in this case do not compromises spectral efficiency and it is also independent of channel sate variability. The several cases analyzed here show effectiveness of the proposed approach to implement a security scheme at physical layer level.

This work explores a multi-antenna transmission technique as a physical layer security technique independent of channel characteristics. In Section 2 a revision of the transmitter technique is made. The rest of the paper is organized as follows: considerations about the security achieved and complexity are presented in Section 3. A analysis of security and a set of simulation results are also presented in this Section. Section 4 resumes this paper.

2. MISO TRANSMITTER AND CONFIGURATIONS HYPOTHESIS

The basic idea is to employ a transmitter structure where the transmitted constellation (for example a M-QAM (Quadrature Amplitude Modulation)) is the result of the combination at channel level of N_m constant envelope signals that are amplified by N_m nonlinear amplifiers before being transmitted by N_m antennas. This avoids combination losses and increases efficiency of power amplification, since the outputs of the N_m amplifiers are combined at the channel and it is possible to use nonlinear (NL) amplifiers in each radio frequency (RF) branch [5, 6]. Figure 1 shows the structure of such transmitter, where firstly the data bits are mapped into a given constellation (e.g., a QAM constellation) characterized by the ordered set $\mathfrak{S} = \{s_0, s_1, \dots, s_{M-1}\}$ following the rule $(\beta_n^{(\mu-1)}, \beta_n^{(\mu-2)}, \dots, \beta_n^{(1)}, \beta_n^{(1)}) \mapsto s_n \in \mathfrak{S}$, with $(\beta_n^{(\mu-1)}, \beta_n^{(\mu-2)}, \dots, \beta_n^{(1)}, \beta_n^{(1)})$ 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.,

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

with $(\gamma_{\mu,i}\ \gamma_{\mu-1,i}\ \dots\ \gamma_{2,i}\ \gamma_{1,i})$ denoting the binary representation of i and $b_n^{(m)} = (-1)^{\beta_n^{(m)}}$ is the polar representation of the bit $\beta_n^{(m)}$. Since 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, $i = 0, 1, \dots, M-1$. In practice, a given constellation can be decomposed as the sum of $N_m \leq M$ polar components, since $g_0 = 0$ (which represents the center of mass of the constellation) and other g_i can also be 0 [8]. Each one of the N_m polar components is modulated as a BPSK signal, being each one a serial representation of an OQPSK signal [9], with reduced envelope fluctuations and compact spectrum (e.g., a gaussian minimum shift keying (GMSK) signal). Finally, the corresponding signals are separately amplified by N_m nonlinear amplifiers and posteriorly transmitted by N_m antennas. Despite the uncorrelation between BPSK components, there is directivity at information level since the transmitted constellation shape is optimized for a specific angle Θ. So, security arises as a consequence of constellation shaping, since any unauthorized user must know the constellation coefficients g_i as well as the array configuration to decode with success the transmitted data. Another important aspect is the complexity associated to any interception. In this case, complexity relies on the several configuration freedom degrees that are possible at the transmitter. Mappings cab be changed by setting different values to the set of coefficients g_i or changing association between BPSK components and transmit antennas. For example, assuming the a equal number of active antennas and BPSK components, i.e., N_m components, the number of possible configurations will be $log2(M)! \times (N_m! - N_m)$, where $N_m^{N_m}! - N_m$ denote the number of different permutations of coefficients g_i between antennas. Moreover, if the array have M antennas with only N_m active, the number of permutations is given by $M!/((M - N_m)!N_m!)$ which leads to the total number of combinations $\log 2(M)!M!/((M - N_m)!N_m!)$. Actually, the number of possibilities is higher since we must take into account the directions in which the constellation can be optimized ($\Theta \in [0, 2\pi]$) and also the spacing between antennas.

3. SECURITY LEVEL AND SIMULATION RESULTS

To characterize the security achieved by this scheme we consider the simplest scenario with a three-terminal system comprising a transmitter, the intended receiver, and an unauthorized receiver (eavesdropper), wherein the transmitter wishes to communicate a private message to the receiver. Having in mind the the analysis of the secrecy level assured by this transmission scheme and the tolerance against errors on the estimation of transmitter's parameters (closely related with the complexity), the mutual information (MI) associated to both authorized receiver and eavesdropper will be evaluated. For this purpose, we assume that the authorized receiver knows the

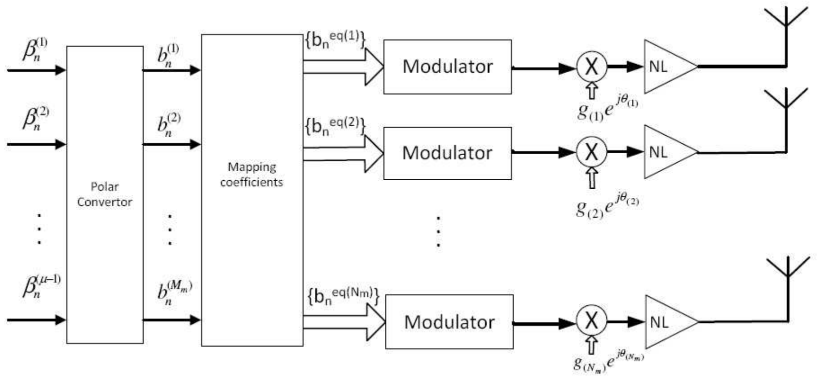

Figure 1: Structure of constellation directive transmitter.

transmitter coefficients g_i. Regarding the eavesdropper we admit two possibilities: in the first one the eavesdropper do not have any information about g_i and array configuration. In the second the configuration parameters associated to the constellation optimized for the angle Θ are known, but the eavesdropper is unable to estimate the exact coefficients g_i and the array configuration that lead to an new optimization angle $\Theta + \Delta\Theta$).

Despite the variety of possible parameters that can be changed in the configuration of this transmitter, we restrict our analysis to transmitters with equal number of antennas and BPSK components and an uniform spacing between antennas equal to $d/\lambda = 1/4$. We assume an non-degraded Gaussian wiretap channel, where both channels are Additive White Gaussian (AWGN) channels.

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 $\mathfrak{S}$. The received signals by the authorized receiver and the eavesdropper are

$$y(t) = f_A(s(t)) + n_1(t), \tag{3}$$

and

$$z(t) = f_A(s(t)) + n_2(t), \tag{4}$$

with $n_1(t)$ and $n_2(t)$ denoting de noise terms and f_A denotes the shaping performed by the transmitter array. It is well known that perfect secrecy implies that $I(S;Z) = 0$, with S the sent message and Z the received message by the eavesdropper and where $I(;)$ denotes 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 signal set [10], and can be written as

$$I(S,Y) - \log_2 M - \frac{1}{M}\sum_{s\in\mathfrak{S}} \mathbf{E}_n \left[\log_2\left(\sum_{s'_n\in\mathfrak{S}} \exp(-\frac{1}{N_0}|\sqrt{Es}(s_n - s'_n) + n|^2 - |n|^2)\right)\right], \tag{5}$$

where $\mathbf{E}$ denotes the expectation. It can be shown that the secrecy capacity is given by the difference of mutual informations

$$C_s = \max_{s\in F}\left[I(S;Y) - I(S;Z)\right] \tag{6}$$

where F is the set of all probability density functions at the channel input under power constrain at the transmitter, $I(S;Y)$ denotes the mutual information of the intended receiver and $I(S;Z)$ represents the mutual information of eavesdropper. It is important to recall that when coefficients g_i are not known the distortion effects on the transmitted constellation are comparable to nonlinear distortion introduced by a nonlinear channel with a AM/AM and a AM/PM non null characteristic. Therefore, we can expect a null MI value for the case where there is no information about transmitter configuration available for the eavesdropper.

3.1. Simulation Results

For MI computation we consider average results based on independent trials of Monte Carlo experiments. Also the symbols s_n are selected with equal probability from a M-QAM constellation (dimensions of $M = 16$ and $M = 64$ are considered). The transmitter based on 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. For 64-QAM we have is 6 non-null coefficients with values $2j$, 1, 2, j, 4 and $4j$ associated to the antennas $1, 2, 3, 4, 5$ and 6, respectively. 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 the second hypothesis the $\Delta\Theta$ values are 6° and 8°. Only for comparison purposes and to see what is the effect of an higher number of RF branches on secrecy capacity in second hypotheses, we consider also a Voronoi constellation with 16 symbols characterized by the set of complex coefficients $g_0 = 0$, $g_1 = -0.58 + j0.57$, $g_2 = -0.712 + j0.545$, $g_3 = -0.014 - j0.124$, $g_4 = 0.028 + j0.248$, $g_5 = -0.186 + j0.273$, $g_6 = -0.2 + j0.149$, $g_7 = -0.014 - j0.124$, $g_8 = -0.1 + j0.074$, $g_9 = 0.085 - j0.198$, $g_{10} = 0.358 + j0.272$, $g_{11} = 0.859 - j0.198$, $g_{12} = -0.1 + j0.074$, $g_{13} = -0.085 - j0.198$, $g_{14} = -0.1 + j0.074$ and $g_{15} = 0.085 - j0.198$ (Voronoi constellations are optimized to assure the best energy efficiency).

Figure 2 shows MI behavior with the optimization angle θ for transmitters using 4 and 6 RF branches, i.e., for 16-QAM and 64-QAM constellations, respectively. It can be seen that when the intended receiver knows the transmitter parameters the MI is practically unaffected by the optimization angle in which the constellation is configured. This means that, independently of Θ, the authorized receiver is able to decode with success the transmitted data.

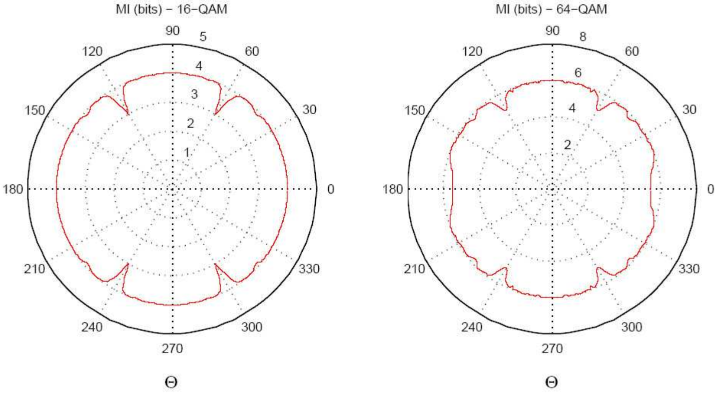

Figure 2: MI behavior with the transmission direction θ for the authorized user.

It should be mentioned that, when no information about transmitter configuration is available at the eavesdropper, the MI value is always null (under these conditions the eavesdropper assumes a regular M-QAM constellation with gray mapping, and is unable to compensate the nonlinear distortion due to the constellation shaping). This is shown in the results of Figure 3, regarding the secrecy evolution with $\frac{E_b}{N_0}$, where it can be seen that the secrecy capacity equals the mutual information of the authorized receiver. In this case the MI values agree with the secrecy capacity.

Figures 4 and 5 show the results regarding the second hypothesis, where the eavesdropper knows the initial set of parameters associated to the optimized constellation for angle Θ, but is unable to accurately estimate the associated parameters in a new direction $\Theta + \Delta\Theta$. Clearly, the MI for the eavesdropper is severely affected when is unable to estimate the angle $\Theta + \Delta\Theta$. As expected, the higher number of RF branches implies stronger impact on MI values. This is valid for 16-Voronoi constellation where the secrecy is practically equal to the results of Figure 3 (in this case the MI for the eavesdropper is near zero). The same conclusion is valid for 64-QAM as we can see from Figure 5 (the 64-Voronoi was not included since our previous analysis showed that the effect on secrecy rate is similar to 16-Voronoi). Therefore, the resort to constellations requiring more BPSK components implies lower tolerance to estimation errors. This is good since it means high complexity in the computational process to estimate the transmitter parameters by any eavesdropper.

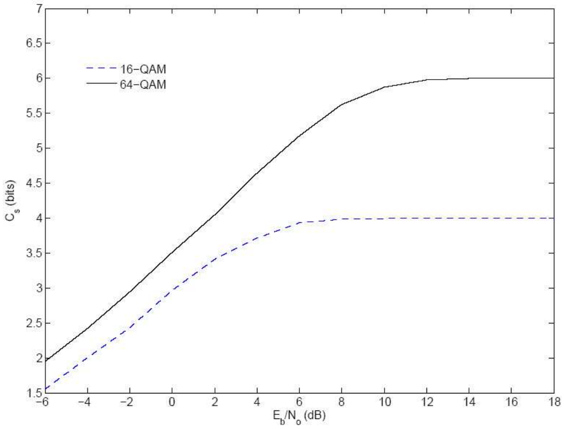

Figure 3: Secrecy rate for 16-QAM and 64-QAM when only the information about the set of g_i coefficients is available to the eavesdropper.

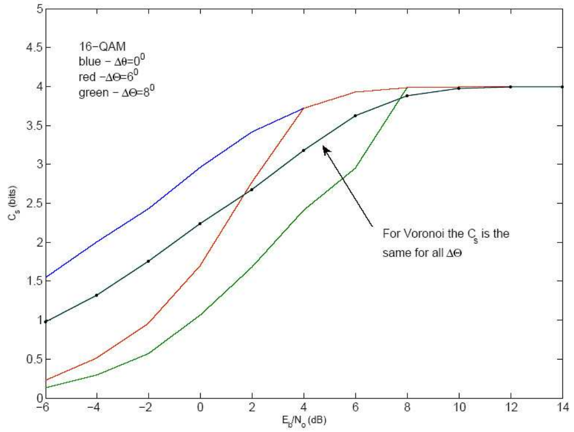

Figure 4: Secrecy rate for 16-QAM and 16-Voronoi for the second hypothesis about eavesdropper.

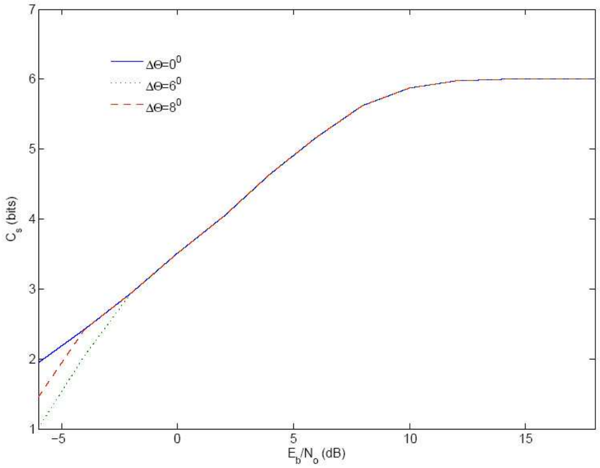

Figure 5: Secrecy rate for 64-QAM and 16-Voronoi for the second hypothesis about eavesdropper.

4. CONCLUSIONS

In this paper we considered constellation shaping achieved by a MISO transmission structure as a technique to implement physical layer security. The basic idea relies on the fact that the constellation shaping performed for a specific direction Θ can be used to assure secrecy on communication. The several freedom degrees regarding the configuration of transmitter lead to complexity levels that makes very difficult any successful interception by an eavesdropper. These assumptions were confirmed by a set of simulation results where it was possible to see the good level of secrecy attainable by these kind of transmitters. Notwithstanding the analysis and results presented here, a full characterization of the secrecy attainable by this transmitter should be addressed in future work.

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. Schneier, B., “Cryptographic design vulnerabilities,” *IEEE Computer*, Vol. 31, No. 9, 26–33, Sep. 1998.
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. 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.
6. 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.
7. Balanis, C. A., *Antenna Theory Analysis and Design*, Wiley, New York, 1997.
8. Dinis, R., P. Montezuma, N. Souto, and J. Silva, “Iterative frequency-domain equalization for general constellations,” *IEEE Sarnoff Symposium*, Princeton, USA, Apr. 2010.
9. Amoroso, F. and J. Kivett, “Simplified MSK signalling technique”, IEEE Trans. on Comm., Vol. 25, Apr. 1977.
10. G. Caire, G. Taricco, and E. Biglieri, “Bit-interleaved coded modulation,” *IEEE Trans. Inf. Theory*, Vol. 44, 927–947, May 1998.