Secrecy Analysis of EGT and MRT Precoders for M-QAM Constellations

Gustavo Anjos, Daniel Castanheira, Adão Silva, Atílio Gameiro
Instituto de Telecomunicações and DETI, University of Aveiro, Aveiro, Portugal

***Abstract*– This work presents an information theoretical analysis of the intrinsic secrecy of circular and square *M*-QAM signals when these constellations are precoded with equal gain transmission (EGT) and maximum ratio transmission (MRT) techniques. The main results show that for low order constellations, a significant percentage of the exchanged information is intrinsically protected by the EGT precoder, while in the MRT case, an interesting result shows that the secrecy level doesn't scale with the entropy of the source, and therefore perfect secrecy rate can be achieved asymptotically increasing the constellation order *M*. Furthermore, the results provided in this work can be used to quantify a minimum entropy value that a shared secret key must have to fully secure the information from an eavesdropper.**

Index Terms — wireless communications, physical layer security, QAM, channel coherent precoding.

I. INTRODUCTION

In wireless communications, the use of an open channel is the fundamental condition that allows users to access the information in a mobility context. At the same time, this broadcast nature also makes wireless technology extremely vulnerable to eavesdropping attacks, which has become more and more advanced in recent years. Since the release of initial standards, cryptographic protocols have been used to protect information, remaining over the last years relatively secure against known threats. Although the wide acceptance of cryptographic systems, the secrecy provided by these kind of techniques is always supported by the assumption that some mathematical operations are computationally hard to perform. For instance, in asymmetric cryptosystems, information secrecy relies on the assumption that factorizing the product of two large prime numbers is a task impossible to perform taking into account the computational capacity available at the eavesdropper. However, with the recent progresses of quantum processing, the factorization of large prime numbers will be feasible, putting at test the secrecy level provided by current cryptosystems. The technological advances described above reinforces the need to find new security schemes that can overcome the vulnerabilities associated with current cryptographic protocols [1], [2].

In order to address these threats, the development of secrecy schemes supported on physical layer security principles is being considered by the research community as a promising solution to complement current secrecy solutions. In physical layer security, the random impairments present in the wireless channel are used to force a channel advantage in relation to the eavesdropper, being the quantification of the secrecy level provided by such schemes done from an information theoretic perspective, without making any assumption regarding the computational resources available at the eavesdropper [3]. In wireless communications, the noise and fading impairments can be exploited to protect information, providing a solution to improve security in these networks.

In 1949 Claude Shannon formulated some of the information theoretical basis used today in the design of secure communication channels. In [4], Shannon demonstrated that perfect secrecy is achieved when a secret key with the same size and entropy of the information source is used to secure the communication channel. However, in his work Shannon didn't exploited the noise and fading impairments typical of a wireless channel, considering that the secret key was the only information not shared between the legitimate nodes and the eavesdropper. A few years later, assuming different discrete memory less channels, Wyner showed in [5] that coding can be used to reach positive secrecy if the eavesdropper channel is degraded in relation to the legitimate channel. The secrecy capacity of the Gaussian wiretap channel was formulated by the first time in [6]. Although the lack of practical applications, these initial works were important to define some of the basic principles applied today in the design and analysis of advanced physical layer security schemes.

The recent state-of-art regarding physical layer security can be divided into two major domains, which are: the coding domain and the signal level domain. Considering the signal domain, four main sub-topics can be outlined, which are: jamming based on interference alignment (IA) [7], [8], [9], [10]; artificial noise (AN) generation [11], [12], [13]; secure power allocation schemes [14], [15]; and PHY-key generation techniques [16], [17], [18], [19], [20]. The secure degrees-of-freedom (DoF) of the wiretap channel were obtained in [8] using single-antenna cooperative jammers. In this work, assuming that the eavesdropper channel knowledge is not available at the legitimate terminals, the authors demonstrate that positive secure DoF can be achieved combining interference alignment techniques together with *M*-PAM jamming signals. The work presented in [8] was extended in [9] considering different network structures and assuming knowledge of the eavesdropper channel at the legitimate transmitters. Despite the necessity of having jammers willing to cooperate, the work in [9] only find application in the case of passive eavesdropper scenarios. The problem of pilot contamination attacks in massive MIMO systems considering multi-cell multiuser configurations is analyzed in [12]. To address the secrecy capacity reduction caused by such attacks, the authors of [12] propose the exploitation of the additional degrees of freedom available in a massive MIMO system to generate AN using random shaping matrix precoding as well null-space (NS) based precoding.

Another important line of work that has been object of inten-

978-1-5386-5005-9/18/$31.00 ©2018 IEEE

sive research, focus the generation of secret keys using the reciprocal channel condition observed in time division duplex (TDD) systems. In [16], [17], received-signal-strength (RSS) measurements and channel phase estimations are proposed as an efficient way to generate shared secret keys among the legitimate parties. While some works focus on the processes for efficient secret key extraction from the channel, other ones propose secrecy schemes based on those keys to generate strong equivocation at the eavesdropper [18], [19], [20]. The authors of [18] proposed a secrecy solution that extracts an information (key) from the reciprocal channel phase in order to randomly define *M*-QAM jamming signals at the legitimate parties. The numerical evaluations show that perfect secrecy is reached by increasing the cardinality of the jamming component. A more efficient solution was suggested in [19] considering a massive MIMO scenario employing MRT precoding at the legitimate transmitter. Instead of mapping the secret key to a jamming signal, the authors of [19] randomly rotate the *M*-PSK symbols using the reciprocal channel phase information. As in the pioneering work of Shannon in [4], the authors of [19] considered secret keys with the same size and entropy of the information source, not exploiting or analyzing the intrinsic secrecy already provided by the combination of the channel coherent precoder and the modulation scheme.

This work presents an information theoretical analysis of the intrinsic secrecy of circular and square *M*-QAM signals when these constellations are precoded with equal gain transmission (EGT) and maximum ratio transmission (MRT) techniques. The main results show that for low order constellations, a significant percentage of the exchanged information is intrinsically protected by the EGT precoder, while in the MRT case, an interesting result shows that the secrecy level doesn't scale with the entropy of the source, and therefore perfect secrecy rate can be achieved asymptotically increasing the constellation order *M*. Furthermore, the results provided in this work can be used to quantify a minimum entropy value that a shared secret key must have to fully secure the information from an eavesdropper.

Notations: Boldface capital letters denote matrices and boldface lowercase letters denote column vectors. The norm of vector $\mathbf{x}$ is given by $\|\mathbf{x}\|$, being the vector of absolute values of the individual elements of $\mathbf{x}$ defined as $\mathbf{x}_{\|}$. The absolute value of the scalar x is defined as $x_{\|}$ or $|x|$, while the vector of individual phases of the elements of $\mathbf{x}$ is defined as $\mathbf{x}_{\measuredangle}$.

II. System Model and Evaluation Metric

This section presents the system model as well as the evaluation metrics used to assess the performance of the analyzed constellations.

A. System Model

The system model considered for the secrecy analysis presented in this work is depicted in Fig. 1, being 'A' the legitimate transmitter (Alice), 'B' the legitimate receiver (Bob) and 'E' is the eavesdropper (Eve). In the considered model, node 'B' is a single antenna terminal, being 'E' and 'A' multiple antenna nodes equipped with N_E and N_A elements respectively.

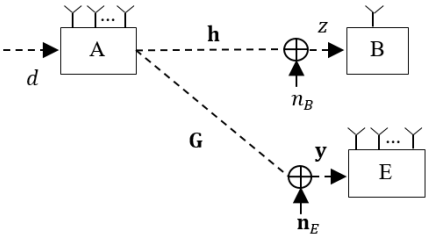

Fig. 1- System model

In Fig. 1, the random variable d represents information that 'A' pretends to secretly exchange with the legitimate receiver 'B'. The channel between the legitimate nodes 'A' and 'B' is defined by the complex vector $\mathbf{h}=\begin{bmatrix} h_1 & h_2 & \dots & h_{N_A} \end{bmatrix}$, while $\mathbf{G}=\begin{bmatrix} \mathbf{g}_1 & \mathbf{g}_2 & \dots & \mathbf{g}_{N_A} \end{bmatrix}$ is a $N_E \times N_A$ complex matrix used to represent the eavesdropper channel response, with $N_E \geq N_A$. The elements of $\mathbf{h}$ and $\mathbf{G}$ are modeled by independent complex Gaussian random variables with zero mean and unitary variance. The variables n_B and $\mathbf{n}_E$ define zero mean complex Gaussian noise at 'B' and 'E' with variance σ_B^2 and σ_E^2, respectively. The signal transmitted at node 'A' is defined as

$$\mathbf{x}=\mathbf{p}d\,, \tag{1}$$

being $\mathbf{p}$ the channel coherent precoder used at the legitimate transmitter. The formulation of the signals received at nodes 'B' and 'E' is given by

$$z=\mathbf{h}\mathbf{x}+n_B\,, \tag{2}$$

$$\mathbf{y}=\mathbf{G}\mathbf{x}+\mathbf{n}_E\,. \tag{3}$$

In this work we assume that 'E' is a passive eavesdropper and has no access to the legitimate channel $\mathbf{h}$, i.e. only $\mathbf{G}$ is available at node 'E'. Furthermore, perfect channel estimation of $\mathbf{h}$ is verified at node 'A', being the transmitted power constrained to $E\left[\|\mathbf{x}\|^2\right]\leq 1$. All the baseband processing is applied to an independent flat fading channel realization.

B. Evaluation Metric

In order to evaluate the amount of information acquired by node 'E' when the considered precoders are combined with *M*-QAM modulation schemes, the mutual information $I(d;\mathbf{y})$ is used as metric. The polar formulation of $I(d;\mathbf{y})$ defined in (4) is considered in the secrecy analysis presented in this work, since we are working in the complex domain.

$$\begin{aligned} I(d;\mathbf{y}) &= I(d_{\|};\mathbf{y}_{\|})+I(d_{\measuredangle};\mathbf{y}_{\measuredangle}\,|\,d_{\|}) \\ &+I(d_{\|};\mathbf{y}_{\measuredangle}\,|\,\mathbf{y}_{\|})+I(d_{\measuredangle};\mathbf{y}_{\|}\,|\,d_{\|},\mathbf{y}_{\measuredangle}) \end{aligned} \tag{4}$$

Additionally, the mutual information $I(d;\mathbf{y})$ can be also defined as

$$I(d;\mathbf{y})=h(d)-h(d\,|\,\mathbf{y})\,, \tag{5}$$

where $h(d)$ is the entropy of the information source and $h(d\,|\,\mathbf{y})$ is the equivocation at the eavesdropper.

III. Secrecy Analysis

The purpose of this section is evaluate the intrinsic security observed in square and circular *M*-QAM modulations when these signals are combined with conventional EGT and MRT precoders.

A. Intrinsic Secrecy of Channel Coherent Precoders

In this sub-section we demonstrate how to quantify the leakage of information $I(d;\mathbf{y})$ at node 'E' when both EGT and MRT precoding schemes are applied. In order to quantify the maximum amount of information $I(d;\mathbf{y})$ leaked at node 'E' resultant from the signal structure generated by the combination of the precoder with the modulation scheme, the noiseless regime is considered at node 'E', i.e. $\sigma_E^2 = 0$. Please note that the assumption $\sigma_E^2 = 0$ represents a worst case scenario in terms of secrecy, since the superposition of random noise with the signal observed at 'E' reduces always the amount of information extracted by the eavesdropper.

In the following, without loss of generality we assume that $\mathbf{G}$ is equalized at the eavesdropper, and therefore the estimated signal

$$\hat{\mathbf{y}} = \mathbf{p}d \tag{6}$$

is used at node 'E' to acquire information relative to the source d. As it will be demonstrated next, depending on the type of precoder and modulation scheme applied to d, different levels of secrecy are naturally added to the system.

1) Secrecy Analysis of EGT Precoder

Considering the polar representation of the data signal and channel gain $d = |d|e^{j\theta_d}$ and $h_i = |h_i|e^{j\theta_i}, i = 1,2,...,N_A$, the EGT precoder is formulated as

$$\mathbf{p} = \frac{1}{\sqrt{N_A}}\begin{bmatrix} e^{-j\theta_1} & e^{-j\theta_2} & \dots & e^{-j\theta_{N_A}} \end{bmatrix}^T, \tag{7}$$

being

$$\hat{y}_i = \frac{1}{\sqrt{N_A}}|d|e^{j\theta_d}e^{-j\theta_i} \tag{8}$$

the signals observed at node 'E'. Because the elements of $\mathbf{h}$ follow a complex Gaussian distribution, the phases $\theta_i, i = 1,2,...,N_A$ are uniformly distributed, and therefore the amount of information acquired by 'E' from $\hat{\mathbf{y}}$ can be derived from (4) and (5) as

$$\begin{aligned} I(d;\hat{\mathbf{y}}) &= I(d_{\|};\hat{\mathbf{y}}_{\|}) \\ &= h(d_{\|}) - h(d_{\|}\,|\,\hat{\mathbf{y}}_{\|}), \\ &= h(d_{\|}) \end{aligned} \tag{9}$$

which means that the information carried in the phase of d is secured. Since θ_i is uniform and $\mathbf{h}$ is independent of d, the only term in (4) different from zero is $I(d_{\|};\hat{\mathbf{y}}_{\|})$. Therefore, as shown in (9), the amount of information obtained by the eavesdropper is quantified by the entropy of the magnitude of the information source d.

2) Secrecy Analysis of MRT Precoder

For the case of MRT, using again the polar definition of $\mathbf{h}$, the precoder is defined as

$$\mathbf{p} = \frac{1}{\|\mathbf{h}\|}\begin{bmatrix} |h_1|e^{-j\theta_1} & |h_2|e^{-j\theta_2} & \dots & |h_{N_A}|e^{-j\theta_{N_A}} \end{bmatrix}^T, \tag{10}$$

and

$$\hat{y}_i = \frac{1}{\|\mathbf{h}\|}|d||h_i|e^{j\theta_d}e^{-j\theta_i} \tag{11}$$

are the signals observed by node 'E'. Using the same arguments considered in the EGT case, and assuming that the magnitudes $\mathbf{h}_{\|}$ of the legitimate channel are available at node 'E',

$$\begin{aligned} I(d;\hat{\mathbf{y}}) &= I(d_{\|};\hat{\mathbf{y}}_{\|}) \\ &\le I(d_{\|};\hat{\mathbf{y}}_{\|}\,|\,\mathbf{h}_{\|}) \\ &= h(d_{\|}) - h(d_{\|}\,|\,\hat{\mathbf{y}}_{\|},\mathbf{h}_{\|}) \\ &= h(d_{\|}) \end{aligned}. \tag{12}$$

can be used as an upper bound for $I(d;\mathbf{y})$ in the MRT case. However, as we will see by the numerical results, this upper bound can be significantly improved.

B. Magnitude Entropy Derivation

This sub-section presents theoretical derivations for the magnitude entropy $h(d_{\|})$ of *M*-QAM signals considering square and circular configurations. For the case of square *M*-QAM signals, the presented analysis is done for $M = 4^m$, with m a positive integer. Additionally, we assume that d is uniformly distributed over the input set.

1) Square M-QAM

The irregular structure of the magnitude in a square *M*-QAM constellation makes complex the exact quantification of the respective magnitude entropy, therefore in this work a tight upper bound for $h(d_{\|})$ is formulated. Due to the symmetric configuration of an *M*-QAM signal, the magnitude entropy can be fully defined analyzing the signal structure in the first quadrant.

To derive the upper bound on $h(d_{\|})$ we will start by consider that each symbol in the region $0 < \theta \le \pi/4$ generates a different magnitude. Hence, in the case of the symbols aligned in $\theta = \pi/4$, each magnitude is generated with probability

$$p_{\pi/4} = \frac{4}{M}, \tag{13}$$

while for the remaining points in $0 < \theta < \pi/4$ each magnitude is generated with probability,

$$p_{0,\pi/4} = \frac{8}{M}. \tag{14}$$

Since the number of symbols aligned in $\theta = \pi/4$ and within the region $0 < \theta < \pi/4$ is given by

$$K_{\pi/4} = \frac{\sqrt{M}}{2}, \tag{15}$$

$$K_{0,\pi/4} = \frac{\left(\sqrt{M}-2\right)\sqrt{M}}{8}, \tag{16}$$

respectively, an upper bound for $h(d_{\|})$ can be derived as

$$\begin{aligned} h(d_{\|}) &= -\sum_{d_{\|}} p(d_{\|}) \log_2 (d_{\|}) \\ &\le -K_{\pi/4} p_{\pi/4} \log_2 \left(p_{\pi/4} \right) \\ &\quad -K_{0,\pi/4} p_{0,\pi/4} \log_2 \left(p_{0,\pi/4} \right) \\ &= -\frac{\sqrt{M}}{2} \times \frac{4}{M} \times \log_2 \left(\frac{4}{M} \right) \\ &\quad -\left[\frac{\left(\sqrt{M} - 2 \right) \sqrt{M}}{8} \right] \times \frac{8}{M} \times \log_2 \left(\frac{8}{M} \right) \\ &= -\frac{2\sqrt{M}}{M} \log_2 \left(\frac{4}{M} \right) - \left(1 - \frac{2\sqrt{M}}{M} \right) \log_2 \left(\frac{8}{M} \right) \\ &= \log_2 (M) + \frac{2\sqrt{M}}{M} - 3 \end{aligned} \tag{17}$$

Note that when M is large, in reality there are some points in the region $0 < \theta < \pi/4$ that shares the same magnitude of a symbol aligned in $\theta = \pi/4$, however, the number of magnitudes in which that overlap happens is very reduced, making the derivation in (17) a tight upper bound.

When $M \to \infty$ the asymptotic behavior of the normalized version of $h(d_{\|})$ converges to

$$\begin{aligned} &\lim_{M \to \infty} \left(\log_2 (M) + \frac{2\sqrt{M}}{M} - 3 \right) \times \frac{1}{\log_2 (M)} \\ &= \lim_{M \to \infty} \left(1 + \frac{2\sqrt{M}}{M \log_2 (M)} - \frac{3}{\log_2 (M)} \right) \\ &= 1 \end{aligned} \quad , \tag{18}$$

meaning that for $M \to \infty$ the normalized entropy of the shared secret key tends to entropy of the information source d , however, in absolute terms at least 3 bits are always secured.

2) *Circular M-QAM*

As it is explicit from the observation of Fig. 3, contrarily to the square M-QAM constellation, the regular magnitude structure of a circular configuration makes the exact derivation of the magnitude entropy a simple task.

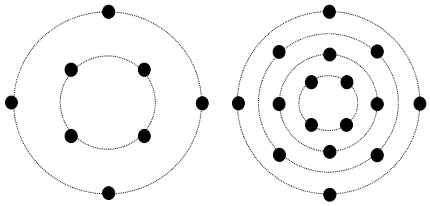

Fig. 3 – Circular 8-QAM (left) and circular 16-QAM (right)

Considering $M = 2^m$ with m a positive integer, the number of magnitudes in a circular M-QAM signal is equal to $M/4$, being the probability of each magnitude defined as $4/M$, i.e. the same probability for all magnitudes. Hence, the magnitude entropy of a circular M-QAM signal can be formulated as

$$h(d_{\|}) = \log_2 \left(\frac{M}{4} \right), \tag{19}$$

i.e. for each possible value of M, only two bits are secured.

Making again the same asymptotic analysis presented in (18), it is possible to conclude that when M goes to infinity,

$$\lim_{M \to \infty} \frac{h(d_{\|})}{\log_2 (M)} = 1 \ . \tag{20}$$

The results in (17) and (19) can be interpreted as lower bounds on the entropy that a shared secret key must have to fully protect information when EGT and MRT precoding schemes are applied to square and circular QAM structures.

IV. Results

The numerical and theoretical results regarding the magnitude entropy (exact mutual information for the EGT precoder) of circular and square M-QAM constellations are presented in Fig. 4 and Fig. 5.

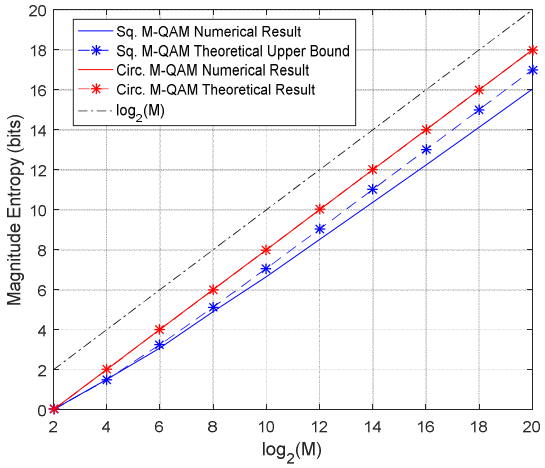

Fig. 4 – Mutual information $I(d_{\|}; \hat{\mathbf{y}}_{\|})$ for EGT precoder

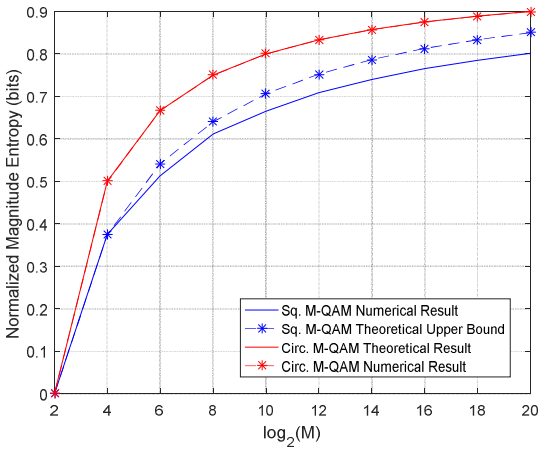

Fig. 5 – Normalized mutual information $I(d_{\|}; \hat{\mathbf{y}}_{\|})$ for EGT precoder

Starting by analyzing the entropy results for the square *M*-QAM configuration, Fig. 4 shows that the derived upper bound is pretty close to the numerical value of the exact magnitude entropy, confirming therefore the quality of the analytical result for the EGT precoder. Furthermore, from Fig. 4 we can also note that the intrinsic secrecy provided by the square *M*-QAM configuration is always larger than the one obtained with the circular structure, which is two bits for all the range of *M*. Finally, the normalized entropy curves depicted in Fig. 5 allows to conclude in a more clearly way that although for $M \to \infty$ the percentage of intrinsic secrecy of the transmission scheme approaches to zero, for low values of *M* the amount of secrecy provided by the combination of the precoder and modulation scheme is significant and therefore can be used to reduce the entropy that a shared secret key must have to fully protect the legitimate link.

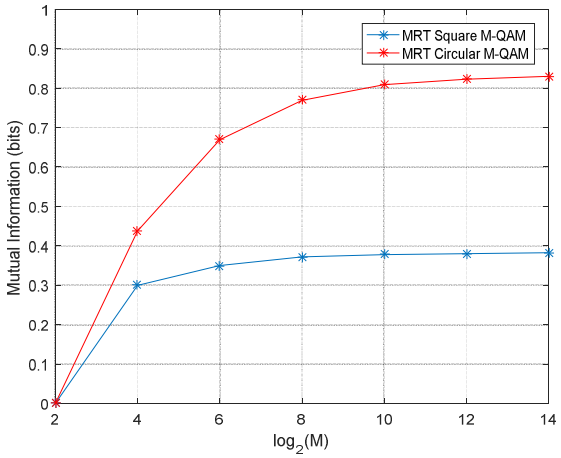

Fig. 6 – Numerical evaluation of mutual information $I(d_{\|};\hat{\mathbf{y}}_{\|})$ for the MRT precoder

In Fig. 6 are depicted the numerical results for the exact value of $I(d_{\|};\hat{\mathbf{y}}_{\|})$ in the case of the MRT precoder. As it is evident, the level of secrecy provided by the MRT precoder is significantly higher than the one provided by the EGT. Another important difference between the EGT and the MRT results, is that while the normalized secrecy level of the EGT tends to zero with the increase of the constellation order *M*, the MRT tends to perfect secrecy, i.e. $\left[I(d_{\|};\hat{\mathbf{y}}_{\|})/\log_2(M)\right] \to 0$. The mutual information curves presented in Fig. 6 were obtained numerically using the nearest neighbor method proposed in [21].

V. Conclusion

The results presented in this work revealed that for the considered modulations, the secrecy level provided by the MRT precoder is significantly larger than the one obtained with the EGT. Additionally, we also demonstrate that for a specific precoder, the circular structure of the QAM signal is always less secure than the square one. In overview, this work shows that the combination of the coherent precoder with the considered modulation schemes has always some intrinsic secrecy, which can be exploited to reduce the entropy requirements that a shared secret key must have to fully secure the system.

Acknowledgement

This work was supported through project SWING2 (PTDC/EEITEL/3684/2014), funded by Fundos Europeus Estruturais e de Investimento (FEEI) through Programa Operacional Competitividade e Internacionalização-COMPETE 2020 and by National Funds from FCT - Fundos Europeus Estruturais e de Investimento, through Project POCI-01-0145-FEDER-016753.

References

[1] B. Schneier, "Cryptographic design vulnerabilities„" in *IEEE Computer*, vol. 31, no. 9, pp. 29-33, Sep. 1998.

[2] M. Sandirigama and R. Idamekorala, "Security Weaknesses of WEP Protocol IEEE 802.11b and Enhancing the Security With Dynamic Keys," in *Science and Technology for Humanity (TIC-STH), 2009 IEEE Toronto International Conf.*, Toronto, pp. 433-438, Sep. 2009.

[3] A. Mukherjee, S. Ali A. Fakoorian, J. Huang and A. Lee Swindlehurst, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey," in *IEEE Commun. Surveys Tuts*, vol. 16, no. 3, pp. 1550-1573, Feb. 2014.

[4] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.,* vol. 28, pp. 656-715, 1949.

[5] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.,* vol. 54, no. 8, pp. 1355–1367, Oct. 1975.

[6] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory,* vol. 24, no. 4, pp. 451–456, Jul. 1978.

[7] D. Castanheira, A. Silva and A. Gameiro, "Retrospective Interference Alignment: Degrees of Freedom Scaling with Distributed Transmitters," *IEEE Trans. on Information Theory,* Vol. 63, No. 3, pp. 1721 - 1730, Mar. 2017.

[8] J. Xie and S. Ulukus, "Secure degrees of freedom of the Gaussian wiretap channel with helpers and no eavesdropper CSI: Blind cooperative jamming," *Proc. Conf. Inf. Sci. Syst,* Baltimore, MD, USA, Mar. 2013.

[9] J. Xie and S. Ulukus, "Secure Degrees of Freedom of One-Hop Wireless," *IEEE Trans. on Inf. Theory,* vol. 60, no. 6, pp. 3359-3378, Jun. 2014.

[10] P. Mukherjee and S. Ulukus, "Secure Degrees of Freedom of the Multiple Access Wiretap Channel With Multiple Antennas," *IEEE Trans. on Inf. Theory,* vol. 64, no. 3, pp. 2093 – 2103, March 2018.

[11] Satashu Goel and Rohit Negi, "Guaranteeing Secrecy using Artificial Noise," in *IEEE Trans. On Wireless Commun.*, vol. 7, no. 6, pp. 2180 – 2189, Jun. 2008.

[12] Jun Zhu, Robert Schober and Vijay K. Bhargava, "Secure Transmission in Multicell Massive MIMO Systems," in *IEEE Trans. On Wireless Commun.*, vol. 13, no. 9, pp. 4766 – 4781, Sep. 2014.

[13] J. Zhu, R. Schober and V. K. Bhargava, "Linear Precoding of Data and Artificial Noise in Secure Massive MIMO Systems," *IEEE Trans. Wireless Commun.,* vol. 15, no. 3, pp. 2245 – 2261, March 2016.

[14] A. Lee Swindlehurst, "Fixed SINR Solutions for the MIMO Wiretap Channel," in *IEEE Int. Conf. on Acoustics, Speech and Signal Processing*, pp. 2437-2440, Apr. 2009.

[15] P. K. Gopala, L. Lai and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory,* vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[16] K. Ren, H. Su and Q. Wang , "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Comm.,* vol. 18, no. 4, pp. 6-12, Aug. 2011.

[17] Q. Wang , K. Xu and K. Ren, "Cooperative Secret Key Generation from Phase Estimation in Narrowband Fading Channels," *IEEE J. Sel. Areas Commun.,* vol. 30, no. 9, pp. 1666-1674, Oct. 2012.

[18] G. Anjos, D. Castanheira, A. Silva and A. Gameiro, "Exploiting Reciprocal Channel Estimations for Jamming to Secure Wireless Communications," in *Wireless Days 2017 Conf.*, Mar. 2017.

[19] G. Anjos, D. Castanheira, A. Silva, A. Gameiro, M. Gomes and J. P. Vilela, "Joint Design of Massive MIMO Precoder and Security Scheme

for Multiuser Scenarios Under Reciprocal Channel Conditions," *Wireless Communications and Mobile Computing,* vol. 2017, pp. 1 - 10, 2017.

[20] Bin Chen, Chunsheng Zhu, Lei Shu, Man Su, Jibo Wei, Victor C. M. Leung and Joel J. P. C. Rodrigues, "Securing Uplink Transmission for Lightweight Single-Antenna UEs in the Presence of a Massive MIMO Eavesdropper," in *IEEE Access*, vol. 4, pp. 5374 – 5384, Sep. 2016.

[21] B. C. Ross, "Mutual Information between Discrete and Continuous Data Sets," *PLOS one,* vol. 9, no. 2, Feb. 2014.