Exploiting Reciprocal Channel Estimations for Jamming to Secure Wireless Communications

Gustavo Anjos[1], Daniel Castanheira[1], Adão Silva[1], and Atílio Gameiro[1].
[1]Instituto de Telecomunicações and DETI, University of Aveiro, Portugal

***Abstract*–The work in this manuscript proposes to enhance the secrecy level of wireless systems through the use of a jamming technique that uses uncorrelated reciprocal channel estimations from the legitimate channel as a common random source to select discrete jamming signals in both sides of the legitimate link. After that selection, these jamming signals are combined with data at the legitimate transmitter, being posteriorly canceled at legitimate receiver. In order to improve the secrecy level of the proposed scheme, an algorithm that efficiently combines data with discrete jamming signals is also developed. The comparison of the scheme proposed in this manuscript with a jamming technique discussed in [13], allowed to verify that the proposed scheme achieves a level of secrecy that does not fall to zero with the signal-to-noise ratio (SNR) increase, instead it saturates in a positive level becoming independent of the power conditions. The results have also showed that making an efficient selection of the jamming signals that will be combined with data, the level of secrecy can be further improved.**

Index Terms—physical layer secrecy, jamming, channel reciprocity, interference cancellation.

I. Introduction

The security vulnerability inherent to the open nature of a wireless communication channel makes the design of secrecy schemes an issue of critical importance in the definition of a secure wireless standard. Since the release of the initial standards, higher layer cryptographic protocols have been used as the main security platform to protect wireless communications against unintended receivers. Although the widespread implementation of such protocols, it is not possible to assure absolute secrecy without the assumption of computational resources limitation at the eavesdropper [1], [2].

In recent years', physical layer security based schemes have been proposed as a solution to complement the limitations of standalone cryptographic protocols [3], [4]. Contrary to cryptography, physical layer secrecy does not make any assumption about the level of computational resources at the eavesdropper, being the required secrecy provided through the forcing of some kind of channel advantage in relation to the eavesdropper. One research path that has been followed to advance physical layer security targets the development of channel coding techniques designed not only to provide error detection and correcting capabilities, but also implement some level of secrecy in a wiretap channel [5], [6]. This kind of codes are commonly defined as wiretap codes. Another direction that has been focused by the research community is the use of jamming techniques to intentionally degrade eavesdropper channel [7]-[13].

The work presented in this article analyzes the secrecy level of a jamming technique that selects discrete jamming signals based on uncorrelated reciprocal channel estimations, acquired from the legitimate physical wireless channel. After the combining operation of data with jamming signals at the legitimate transmitter (Alice), and assuming the incapacity of the eavesdropper to get access to those estimations, the legitimate receiver (Bob) has all the information required to easily cancel the intentional interference, while at the eavesdropper side (Eve), that cancellation cannot be verified. In order to further improve the secrecy level of the scheme mentioned above, an algorithm that efficiently selects the best combination of data with jamming signals is also developed and integrated in the suggested scheme.

The numerical results achieved by the proposed scheme are compared with a blind cooperative jamming technique proposed in [13]. That comparison has shown that for discrete jamming signals, with fixed cardinality, the proposed scheme achieves a level of secrecy that monotonically increases with the SNR, while in the case of the scheme considered in [13] the secrecy level increases for low values of SNR and decreases for high values of SNR. To achieve a monotonically increasing secrecy rate, the scheme proposed in [13] requires that the cardinality of the jamming signals increases proportionally to the SNR.

The remainder of the paper is organized as follows: Section II makes an overview of some relevant work suggested in the literature. Section III defines the general system characterization as well the secrecy metric used in the numerical evaluations. A briefly analysis of a cooperative jamming scheme of [13] is described in section IV. The jamming scheme proposed in this manuscript is formulated in V. In section VI the numerical evaluation results are presented. Finally, the main conclusions are outlined in VII.

Notations: Boldface capital letters denote matrices and boldface lowercase letters denote column vectors. $\mathbf{A}(j,l)$ denotes the element at row j and column l of the matrix $\mathbf{A}$.

II. Related Work

In [9] several linear precoding schemes were discussed to provide secrecy in multiple-input-multiple-output (MIMO) relay networks using a partial and full cooperative jamming solution. For partial cooperative jamming only the inactive nodes in each phase of communication are used as jammers, while in full cooperative jamming both inactive and active nodes jam the eavesdropper. The design of the precoders uses the concepts of null-space generation to define jamming directions as well the creation of orthogonal subspaces to allow the separation of data from

jamming. In [10], two schemes assuming Eve and no Eve channel-state-information (CSI) were presented to enhance security in a MIMO wiretap channel. In both schemes, legitimate transmitter (Alice) splits the available power between data and a jamming signal in way that a defined minimal signal-to-interference-plus-noise ratio (SINR) at legitimate receiver (Bob) is always granted. The developed schemes try to compute the optimal power ratio between data and jamming signals in order to maximize the ratio between SINR at Bob and SINR at Eve. Techniques based on Singular-Value-Decomposition (SVD) of the channel are considered. The paper [11] proposed two cooperative jamming schemes that aim to enhance the secrecy capacity of ad-hoc networks. The cooperative jamming schemes are Coordinated Cooperative Jamming (CCJ) and Uncoordinated Cooperative Jamming (UCJ). In CCJ, Bob signal space is divided into data and jamming subspaces, being that subspaces shared among all the helpers to allow interference alignment (IA) [16]. In UCJ, the subspaces are not shared, making that Alice uses their channel right singular vector with highest singular value to beamform data to Bob, while the jammers use the right singular vector with smallest singular value. In [13], the secure Degrees-of-Freedom (DoF) of the wiretap channel were obtained considering the use of L cooperative jammers. Without the need of eavesdropper CSI at the legitimate nodes, the authors in [13] showed that positive secure DoF are achieved through the use of IA to align the jamming signals at the legitimate receiver. The same authors of [13], compute again in [12] the secure DoF of several network structures, which include: wiretap channel with L helpers; 2 user interference channel with confidential messages; broadcast channel with confidential messages and L helpers; and K-user multiple access wiretap channel. As in [13], the achievability schemes are based on real IA and cooperative jamming. Contrarily to [13], in this case it is assumed that global CSI, including eavesdropper channel, is available at all transmitters.

The manuscript in [14] makes an overview and performance evaluation of existing schemes that use the wireless channel as a random source to generate cryptographic keys used to secure a wireless communication. The considered schemes are divided in two types: the ones that use received signal strength (RSS) as random source, and the ones that use channel phase estimations. The particularities of each scheme in terms of the main steps required to implement them are analyzed. In [15], a specific protocol applied also to generate common secure cryptographic keys between two nodes that communicate through a wireless channel was suggested. Using the randomness and reciprocity feature of the channel, jointly with the help of relay nodes, a sequence of channel phase estimations is used as the random source for key generation.

III. General Model Structure and Metrics

In this section the general model structure as well common aspects shared between the schemes defined in sections IV and V are presented.

A. System Model

In Fig. 1 is depicted the general setup used in the schemes described in sections IV and V. The system is formed by single antenna elements, being 'A' the legitimate transmitter, 'J' the cooperative jammer, 'B' the legitimate receiver and 'E' the eavesdropper. In Fig. 1, d^n represents the data that 'A' wants to exchange securely with 'B', u_A^n and u_J^n are discrete jamming signals transmitted by 'A' and 'J' respectively, y_B^n and y_E^n correspond to received signals, $h_{BA}^n, h_{BJ}^n, h_{EA}^n$ and h_{EJ}^n are complex Gaussian fading channel coefficients, and finally, $\tilde{n}_B$, $\tilde{n}_E$ models reception noise using a Gaussian random variable with zero mean and variance σ_N^2. It is assumed that node 'A' and 'J' have knowledge of h_{BA}^n and h_{BJ}^n respectively, node 'B' is aware of h_{BA}^n as well h_{BJ}^n, and finally node 'E' can only access h_{EA}^n and h_{EJ}^n. The index of the independent subcarrier/time-slot channel realization is defined by n.

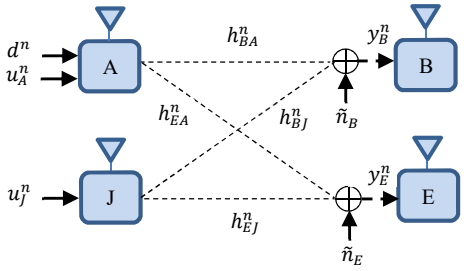

Fig. 1 – General system model

It is well known that the use of a complex Gaussian distribution to model channel coefficients, means that the magnitude of the channel is a Rayleigh random variable, and the phase is modeled by a uniform distribution. Note that the higher level of entropy verified in a uniform distribution makes of the channel phase a good source of randomness. This observation will be useful in the scheme proposed in section V.

B. Decoding

The optimal maximum likelihood (ML) decoding scheme is considered at 'B' and 'E', being the general formulation defined in expression (1) and (2) respectively.

$$\hat{d}_B^n = \arg \min_{d^n, u_A^n, u_J^n \in Q} \left| y_B^n - \hat{y}_B^n \right|^2 \quad (1)$$

$$\hat{d}_E^n = \arg \min_{d^n, u_A^n, u_J^n \in Q} \left| y_E^n - \hat{y}_E^n \right|^2 \quad (2)$$

Equations (1) and (2) define general formulas which will be adapted in sections IV and V for the respective schemes.

C. Secrecy Metric

The secrecy metric used in the evaluation of the schemes presented in the next two sections is the secrecy capacity C_s, which is formulated as,

$$C_s = I(D^N, \hat{D}_B^N) - I(D^N, \hat{D}_E^N) \quad (3)$$

where $I(D^N, \hat{D}_B^N)$ and $I(D^N, \hat{D}_E^N)$ define the discrete mutual information (4) expressions between two random variables, being $D^N = [d^n, ..., d^{n+N}]$ and $\hat{D}_{B,E}^N = [\hat{d}_{B,E}^n, ..., \hat{d}_{B,E}^{n+N}]$.

$$I\left(D^N; \hat{D}_{B,E}^N\right) = \sum_{d^n \in Q_{d^n}} \sum_{\hat{d}_{B,E}^n \in Q_{\hat{d}_{B,E}^n}} p_{d^n, \hat{d}_{B,E}^n}\left(d^n, \hat{d}_{B,E}^n\right) \log_2 \frac{p_{d^n, \hat{d}_{B,E}^n}\left(d^n, \hat{d}_{B,E}^n\right)}{p_{d^n}\left(d^n\right) p_{\hat{d}_{B,E}^n}\left(\hat{d}_{B,E}^n\right)} \quad (4)$$

In regular words, the mutual information measures the amount of information shared between two random variables, i.e. it allows to quantify the amount of information acquired from one of the variables through the observation of the other variable. Therefore, the target of each secrecy scheme is to maximize $I(D^N, \hat{D}_B^N)$ and minimize $I(D^N, \hat{D}_E^N)$.

IV. Blind Cooperative Jamming

In this section, we briefly describe the blind cooperative jamming technique proposed in [13]. The authors in [13] suggested a jamming solution that allow to achieve $L/(L + 1)$ secure DoF using L cooperative jammers and without the requirement of eavesdropper channel knowledge at the legitimate nodes.

A. Mathematical Formulation

The structure of the signals transmitted by 'A' and 'J' is described in (5) and (6) respectively. The signals x_A^n and x_J^n are designed in order to force interference alignment of u_A^n and u_J^n in the same dimension at 'B'.

$$x_A^n = d^n + \frac{1}{h_{BA}^n} u_A^n \quad (5)$$

$$x_J^n = \frac{1}{h_{BJ}^n} u_J^n \quad (6)$$

In the evaluation performed in this manuscript the total power is constrained to P, being divided by node 'A' and node 'J' as defined in (7) and (8) respectively. In 'A', $P/2$ is allocated to data, while $P/4$ is assigned to jamming signal.

$$E[|x_A^n|^2] \le \frac{3P}{4} \quad (7)$$

$$E[|x_J^n|^2] \le \frac{P}{4} \quad (8)$$

After sending x_A^n and x_J^n through the wireless channel, the signal received at 'B' is formulated in (9), while the signal received at 'E' is described in (10).

$$y_B^n = h_{BA}^n d^n + u_A^n + u_J^n + \tilde{n}_B \quad (9)$$

$$y_E^n = h_{EA}^n d^n + \frac{h_{EA}^n}{h_{BA}^n} u_A^n + \frac{h_{EJ}^n}{h_{BJ}^n} u_J^n + \tilde{n}_E \quad (10)$$

Finally, in order to decode d^n, the optimal ML estimator defined in (1) and (2) is applied at 'B' and 'E' respectively.

B. Working Concept

From the structure of the received signal at 'B' and defined in (9), is possible to verify that $u_A^n + u_J^n$ and d^n align in rationally independent dimensions, allowing therefore fully separation of d^n from $u_A^n + u_J^n$ using a minimal constellation cardinality seen by the ML decoder at 'B'. In the case of (10), u_A^n and u_J^n are not aligned in the same dimension, which will make that the cardinality of the channel output constellation seen by 'E' will be higher than the one experimented by 'B'. Considering that both constellations have the same average power, the average minimal distance between points of the constellation defined by (9) will be larger than the one defined by (10). This makes that in a finite SNR range, the leakage of information about d^n in 'B' will be higher than the one experimented by 'E'. The behavior described above is the basic working principle that allows the secrecy capacity increase proportionally with the SNR, making that positive secure DoF can be experimented in this scheme.

V. Jamming Based on Reciprocal Channel

In this paper we consider a jamming scheme that uses uncorrelated reciprocal channel estimations from the legitimate channel as a common random source between 'A' and 'B' to select discrete jamming signals. After that selection, these jamming signals are combined with data at 'A', being posteriorly canceled at 'B'. Contrarily to the scheme presented in section IV, in the one proposed the cooperative jammer node 'J' is not used, being all the jamming applied by 'A'. The channel reciprocity requirement limits the use of this scheme only for TDD systems, being that the implementation at FDD would require the secure exchange of a significant amount of feedback information. It should be emphasized that the current trend in the literature is the use of channel reciprocity to generate keys for cryptographic protocols, here we suggest the use of channel reciprocity to define jamming signals at physical layer.

A. Mathematical Formulation

Considering the general system setup in Fig. 1, the signal transmitted by 'A' is described in expression (11), while the signals received by 'B' and 'E' are defined in equations (13) and (14), respectively. In this case, the selection of the jamming signal $u_A^n\left(\Theta_{BA}^m\right)$ is a function of the phase Θ_{BA}^m of the reciprocal channel h_{BA}^m estimated in 'A' and 'B', considering $m \neq n$.

$$x_A^n = d^n + u_A^n\left(\Theta_{BA}^m\right) \quad (11)$$

$$x_J^n = 0 \quad (12)$$

$$y_B^n = h_{BA}^n d^n + h_{BA}^n u_A^n\left(\Theta_{BA}^m\right) + \tilde{n}_B \quad (13)$$

$$y_E^n = h_{EA}^n d^n + h_{EA}^n u_A^n\left(\Theta_{BA}^m\right) + \tilde{n}_E \quad (14)$$

The total power is constrained to $E\left[\left|x_A^n\right|^2\right] \le P$, being half of the power applied to data and the other half to jamming. As shown in (15) and (16), the channel h_{BA}^m estimated in 'A', and the channel $h_{BA}^{m'}$ estimated in 'B', are decomposable in a magnitude and a phase. If the reciprocal estimation is perfect at 'B' and 'A', $a_{BA}^m = a_{BA}^{m'}$ and $\Theta_{BA}^m = \Theta_{BA}^{m'}$.

$$h_{BA}^{m} = a_{BA}^{m} e^{j\Theta_{BA}^{m}} \tag{15}$$

$$h_{BA}^{m'} = a_{BA}^{m'} e^{j\Theta_{BA}^{m'}} \tag{16}$$

At 'A' and 'B', the selection of the discrete jamming signals is done from a finite constellation set $\mathbf{Q} = \{q_0, q_1, \ldots, q_{M-1}\}$ using the mathematical formulation defined in (17) and (18). The value of the phase is defined in the range of $\Theta^m \in]0, 360°]$.

$$i = \left\lceil \frac{M \times \Theta^m}{360} \right\rceil \tag{17}$$

$$u_A^n\left(\Theta^m\right) = q_i \tag{18}$$

The decoding operation at 'B' and 'E' is done using the optimal ML estimator. In the estimation process at 'B', interference cancellation can be applied before estimating d^n, as shown in (19). In the case of 'E', that cancellation is not possible, forcing the ML equalizer to deal with the effect of the additional interference.

$$y_{Bc}^n = h_{BA}^n d^n + h_{BA}^n u_A^n\left(\Theta_{BA}^m\right) - h_{BA}^{n'} u_A^n\left(\Theta_{BA}^{m'}\right) + \tilde{n}_B \tag{19}$$

Assuming perfect reciprocal estimation of Θ_{BA}^m and $\Theta_{BA}^{m'}$, as well h_{BA}^n and $h_{BA}^{n'}$, interference cancellation is total, and (20), (21) and (22) are obtained.

$$h_{BA}^n = h_{BA}^{n'} \tag{20}$$

$$u_A^n\left(\Theta_{BA}^m\right) = u_A^n\left(\Theta_{BA}^{m'}\right) \tag{21}$$

$$y_{Bc}^n = h_{BA}^n d^n + \tilde{n}_B \tag{22}$$

Considering d^n from a finite constellation set Q, the ML estimator at 'B' is mathematically described in equation (23). In the case of 'E', the ML estimation is formulated in (24), i.e. the same expression of (2).

$$\hat{d}_B^n = \arg\min_{d^n \in \mathrm{Q}} \left| y_{Bc}^n - \hat{y}_{Bc}^n \right|^2 \tag{23}$$

$$\left(\hat{d}_E^n, \hat{u}_A^n\right) = \arg\min_{d^n, u_A^n \in \mathrm{Q}} \left| y_E^n - \hat{y}_E^n \right|^2 \tag{24}$$

As it will be explained in the next section, the scheme formulated above achieves a level of secrecy that saturates in a positive value with the increase of SNR.

B. *Working Concept*

This section makes an analyses of the mechanism that allows the proposed scheme to achieve a constant positive secrecy level in the high SNR regime assuming an M-QAM constellation for d^n and $u_A^n\left(\Theta_{BA}^m\right)$. Starting by checking (23) and (24), it is easy to see that in the high SNR regime, $P\left(d^n \neq \hat{d}_B^n\right)$ will always reach 0, which means that there is no reduction of the original message entropy in the observation of the received signal at 'B'. In the case of the signal received at 'E' (14), the alignment of data with the jamming signal in the same dimension imposes that only some specific combinations of d^n and $u_A^n\left(\Theta_{BA}^m\right)$ allow the correct estimation of d^n without any possibility of error in the high SNR regime. There are other combinations in which equivocation in the optimal ML decoder at (24) is verified, meaning that there is a reduction of the original message entropy in the observation of the received signal at 'E'. In order to intuitively understand the secrecy mechanism, lets follow a simple example in which a QPSK constellation is used for both d^n and u_A^n (Fig. 2). Let's start by considering that $\sigma_N^2 = 0$ and the signal received at 'E' is described in (25).

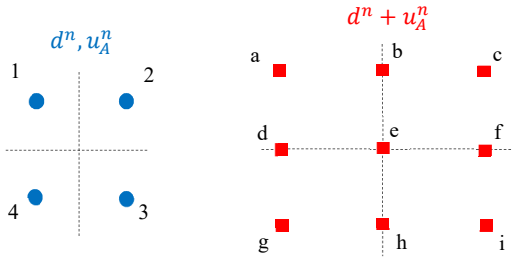

Fig. 2 – QPSK constellation d^n, u_A^n and $d^n + u_A^n$

TABLE I

CORRESPONDENCE BETWEEN d^n, u_A^n AND $d^n + u_A^n$

$d^n + u_A^n$	d^n, u_A^n			
a	1,1	-	-	-
b	1,2	2,1	-	-
c	2,2	-	-	-
d	1,4	4,1	-	-
e	2,4	4,2	1,3	3,1
f	2,3	3,2	-	-
g	4,4	-	-	-
h	4,3	3,4	-	-
i	3,3	-	-	-

$$y_E^{n'} = h_{EA}^n\left(d^n + u_A^n\right) \tag{25}$$

Note that once given h_{EA}^n at 'E', the eavesdropper tries to get d^n from $d^n + u_A^n$, which is possible only in some particular situations. To check that, let us focus on Fig. 2 (right), which represents constellation $d^n + u_A^n$, i.e. two QPSK constellations added together. The correspondence between all possible combinations of d^n, u_A^n and $d^n + u_A^n$ is defined in Table I.

From the analysis of Table I is possible to verify that the only situations in which 'E' can always decode d^n correctly are the cases of 'a', 'c', 'g' and 'i', i.e. when $d^n = u_A^n$. In 'b', 'd', 'f' and 'h', the eavesdropper sees that there are 2 options for d^n, but doesn't know which one is the right one. Finally, case 'e' verifies the highest level of confusion when $d^n = -u_A^n$, having 4 possible combinations to select only one as the correct, which is unknown to 'E'.

The behavior observed above is the reason that allows to achieve a positive secrecy that doesn't falls to zero with the in-

Algorithm for Jamming Block Selection ($\mathbf{d}$, $\mathbf{u}'_A$, K)

$\mathbf{J}$ = *permute*($\mathbf{u}'_A$);
$\mathbf{Y}$ = $\mathbf{d}$ + *each* $\mathbf{J}$ *column;*
$\boldsymbol{C}$ = *zeros*(K , $K!$);

for each row i and column j of $\mathbf{Y}$
  if $Y(i,j)$ *is equalto 'e', then* $C(i,j) = 0$
  elseif $Y(i,j)$ *is equalto 'b','d','f','h', then* $C(i,j)=1$
  else $C(i,j)=2$
  endif
endfor

a = *sum all rows for each column in* **C**;
*index = find(***a** *equalto min(***a** *));*
$\mathbf{u}_A$ = **J** *(*1 *to K, index);*

return ($\mathbf{u}_A$)

Fig. 3- Efficient Data and Jamming Signal Combining pseudocode (QPSK)

crease of the SNR, instead it saturates in a positive level. Another important observation is the fact that increasing the constellation order, the number of situations where more than one constellation point is optimal (accordingly to the ML criterion) as well as the cardinality of the optimal ML set increases, leading therefore to a higher secrecy rate.

C. *Efficient Data and Jamming Signal Combination*

In order to improve the secrecy level of the scheme suggested above, an algorithm that selects optimal combinations of d^n and u_A^n at the combining operation in 'A', is designed for the above scheme. Instead to define the value of $u_A^n\left(\Theta_{BA}^m\right)$ at (11) without the use of any criteria, i.e. just through the random selection of a channel m , the algorithm proposed in this section makes a careful choice of $u_A^n\left(\Theta_{BA}^m\right)$ with the target of maximize the number of $d^n + u_A^n$ cases where the cardinality of the optimal ML set is higher, which in QPSK case correspond to the situations 'e', 'b', 'd', 'f' and 'h' presented in Table I. Although the implementation and evaluation of the algorithm proposed here is done just to the particular QPSK case, their extension to a general QAM modulation order can be done using the same basic principle.

The algorithm starts to buffer a predefined number of K data symbols $\mathbf{d}$, then, a block of jamming signals $\mathbf{u}'_A$ with the same size of the data buffer is acquired through reciprocal channel estimations. After the generation of all possible permutations of the jamming signals block ($\mathbf{J}$), the permutated block $\mathbf{u}_A$ - selected from a column of $\mathbf{J}$ - that maximizes the cardinality of the optimal ML set, is the chosen one to combine with the data buffer, where each position of the selected jamming block is

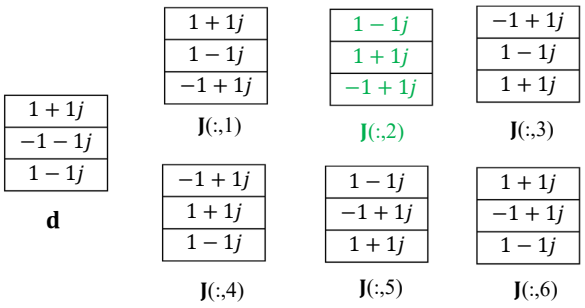

Fig. 4- Efficient Data and Jamming Signal Combining for QPSK and K=3

combined with the respective position of the data buffer. Then, the index of the selected jamming block is sent to 'B' in order to allow the correct cancellation of the interference. Note that 'B' already knows the block of jamming signals that must be permutated, therefore 'A' only needs to send the index of the selected permutation. Even that 'E' acquires the index sent by 'A', he does not have access to the jamming signals, therefore the index can be transmitted without using any secrecy constraint. This process is repeated for each new buffer of K data symbols $\mathbf{d}$. The pseudo-code of the proposed algorithm is presented in Fig. 3. In order to allow an easier understanding of the proposed algorithm, a simple application example described in Fig. 4 considering $K = 3$ is given. In the case of $K = 3$, the number of possible permutations is $K! = 6$, therefore the matrix $\mathbf{J}$ is formed by 6 columns and 3 rows, being each column a particular permutation as show in Fig. 4. Using the proposed algorithm and given the value of $\mathbf{d}$, the selected permutation is $\mathbf{J}(:,2)$. Check that using $\mathbf{d}$ and $\mathbf{J}(:,2)$ in the combining operation, is possible to define 2 'e' cases and 1 'f' case, which correspond to the two cases among all permutated vectors that maximize the cardinality of the optimal ML set. The secrecy rate of this algorithm grows with the increase of K, being the cost of this improvement associated with the computational complexity of the algorithm as well as the number of bits required to quantize the index of the selected jamming block.

The configuration used in the practical application of this algorithm defines a trade-off between complexity and secrecy improvement.

D. *Practical Issues*

The implementation of the jamming scheme proposed in this manuscript is subject to some practical aspects that should be analyzed. First, the use of this scheme requires orthogonal time/frequency resources to perform the required reciprocal phase estimations, therefore using that channels as random source to generate jamming signals will decrease the amount of resources available for data. A second aspect is related to the need that those channels must be uncorrelated, imposing that the time/frequency resources used in the estimations must be selected in order to verify that. Third consideration is related to the impact of phase estimation mismatch between 'A' and 'B'. Note that in the case of high order constellations that mismatch can have a critical impact in the performance of the scheme. The

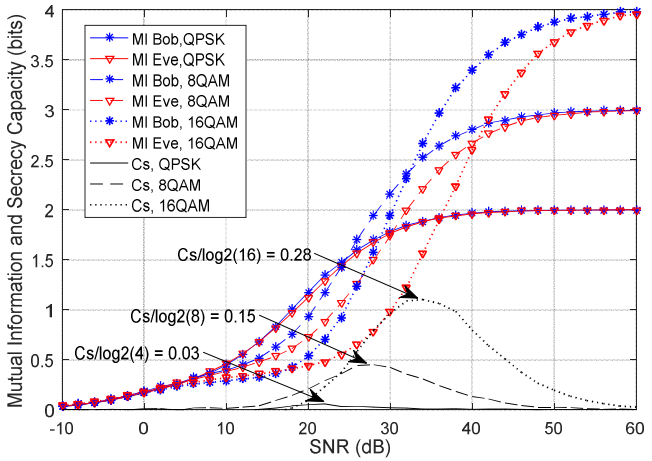

Fig. 5 - $I(D^N, \hat{D}_B^N)$ at Bob, $I(D^N, \hat{D}_E^N)$ at Eve, and C_s for the Blind Cooperative Jamming Scheme

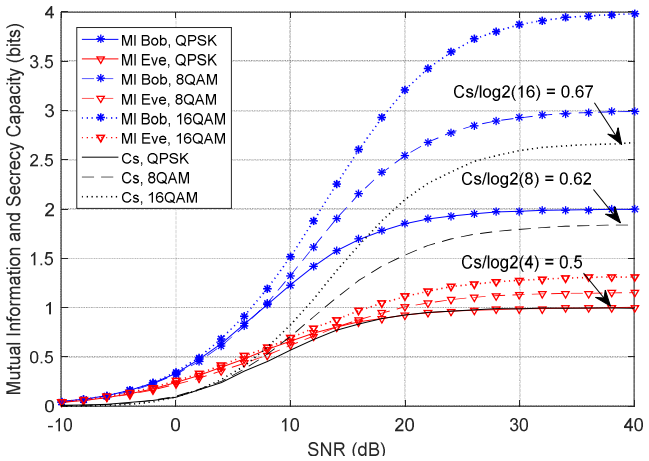

Fig. 6 - $I(D^N, \hat{D}_B^N)$ at Bob, $I(D^N, \hat{D}_E^N)$ at Eve, and C_s for the proposed Jamming Based on Reciprocal Channel Scheme

scope of this paper is not to analyze in detail the issues mentioned above, therefore only a brief reference to the most important ones is done in this point.

VI. Numerical Results

In this section we evaluate the proposed schemes described in section V. The performance is compared with the one briefly described in Section IV and proposed in [13]. The metrics used are defined in section C.III.

Starting by making a comparative analysis of the mutual information conditions between the scheme in [13] and the proposed one, is possible to observe from Fig. 5 and Fig. 6 that Eve mutual information $I(D^N, \hat{D}_E^N)$ in [13] always reach the same value of Bob mutual information $I(D^N, \hat{D}_B^N)$ with the SNR increase. Therefore, as shown by the C_s black curves, a positive secrecy level is only available in a finite SNR range. For the proposed algorithm, Eve mutual information $I(D^N, \hat{D}_E^N)$ always saturate before reaching $I(D^N, \hat{D}_B^N)$, allowing therefore experiment a positive secrecy level C_s that from a given SNR point is constant. For the proposed scheme, the alignment of d^n with u_A^n makes that the optimal ML estimator in 'E' is only able to decode correctly $d^n + u_A^n$, therefore, in order to assure that there isn't an unintentional reduction of the maximum value of the mutual information $I(D^N, \hat{D}_E^N)$, the evaluation at 'E' must be done for $\hat{D}_E^N = [\hat{d}_E^n + \hat{u}_A^n, ..., \hat{d}_E^{n+N} + \hat{u}_A^{n+N}]$. For instance, in the cases of $d^n + u_A^n$ where exists confusion at the ML estimator, if any blind selection of a possible solution is done, the conditional entropy $H(D^N / \hat{D}_E^N)$ increases, making that $I(D^N, \hat{D}_E^N)$ reduces bellow the maximum value that should be considered, which is not a correct assessment. It also should be mention that the mutual information results are not normalized to 1, therefore

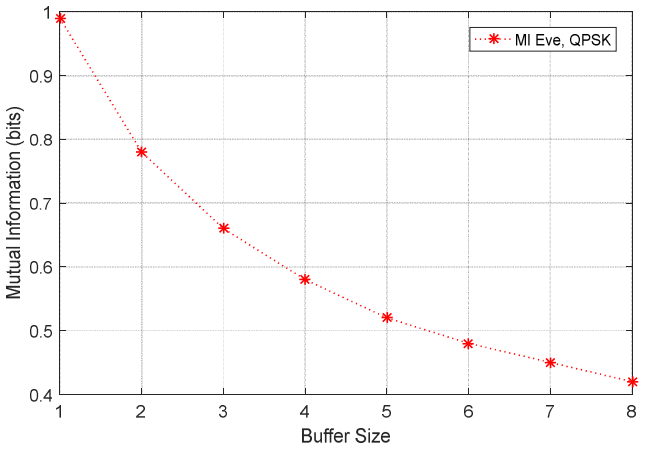

Fig. 7- Reduction of $I(D^N, \hat{D}_E^N)$ at Eve, considering the Efficient Data and Jamming Signal Combining Algorithm in the proposed scheme

when $I(D^N, \hat{D}_B^N)$ and $I(D^N, \hat{D}_E^N)$ reach the value of $log_2(M)$, all the information about D is acquired. One interpretation of the mutual information curves in Fig. 5 and Fig. 6 could be done assuming that per each $log_2(M)$ bits that 'A' try to exchange securely with 'B', $I(D^N, \hat{D}_B^N)$ bits are acquired by 'B', while $I(D^N, \hat{D}_E^N)$ bits are obtained by 'E'.

Another aspect that should be analyzed is related to the peaks of the normalized $C_s / log_2(M)$ secrecy, whose values are pointed out in Fig. 5 and Fig.6 through arrows indicating where these occur. Although these peaks increase faster and almost linearly in the scheme of [13], their absolute values for the considered constellations are always higher for the proposed scheme.

The numerical results also confirm the increase of the secrecy capacity with the increase of the constellation order, as predicted in the previous section.

TABLE II

TRADEOFF BETWEEN CS INCREASE AND OVERHEAD

	Efficient Combining Algorithm (QPSK)							
Buffer Size	1	2	3	4	5	6	7	8
C_s **Inc. %**	Ref	22	34	42	46	52	55	58
Overhead %	Ref	20	33	38	41	45	48	50

The results shown up to now were obtained without the integration of the efficient combining algorithm proposed in Section V.C, i.e. the selection of the jamming signals in the results presented above was totally arbitrary. Fig. 7 shows the obtained reduction of information leakage at 'E' considering the efficient combining algorithm in the scheme proposed in this paper. The evaluation in Fig. 7 was done without considering reception noise, therefore for all buffer sizes and using QPSK, $I(D^N, \hat{D}_B^N) = 2$, meaning that the C_s improvement is defined by the reduction of $I(D^N, \hat{D}_E^N)$, which is shown in Fig. 7. Both the computational complexity and overhead of the combining algorithm increases with the factorial of the buffer size, $O(K!)$, therefore an equilibrium must be defined. Table II shows the cost in terms of overhead to achieve a given increase in the secrecy level using as reference the case of buffer size equal to 1 for QPSK $(C_s = 1)$, i.e. the algorithm presented in Section V.C) is not used.

Analyzing Table II is possible to see that using the algorithm with a buffer size of 2, the secrecy level increases 22% with the cost of in each 5 bits transmitted, 1 bit must be used as overhead. In the case of buffer size equal to 3, an increase of 34% of secrecy level is achieved, but per each 3 bits exchanged 1 bit is overhead. In the limit case, i.e. buffer size equal to 8, the secrecy level increases 58% but it is required to send the same amount of overhead as data information, which represent a high cost.

The selection of the algorithm configuration in terms of buffer size, should be done taking in account the secrecy requirements versus the latency and throughput used by the application.

VII. CONCLUSION

The numerical results achieved in the evaluation of the proposed jamming scheme allowed to verify that the secrecy capacity saturates in a positive level after a given SNR point, remaining there independently of the power conditions. As predicted in section V, the numerical results also confirmed the secrecy improvement with the increase of constellations cardinality. In order to enhance even more the performance of the considered scheme, an efficient combining algorithm was designed revealing a considerable security increase in the proposed jamming technique.

ACKNOWLEDGEMENT

This work is supported through project SWING2 (PTDC/EEI-TEL/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 - Fundação para a Ciência e a Tecnologia, through project POCI-01-0145-FEDER-016753.

REFERENCES

[1] M. Atallah, G. Kaddoum and L. Kong, "A Survey on Cooperative Jamming Applied to Physical Layer Security," in *Ubiquitous Wireless Broadband (ICUWB), 2015 IEEE Int. Conf. on*, Montreal, Oct. 2015.

[2] 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. Survey & Tutorials*, vol. 16, no. 3, pp. 1550-1573, 2014.

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

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

[5] M. Bloch, M. Hayashi, A. Thangaraj, "Error-Control Coding for Physical-Layer Secrecy," in *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1725-1746, Sept. 2015.

[6] W.K. Harrison, 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," in *IEEE Signal Processing Mag.*, vol. 30, no. 5, pp. 41-50, Sept. 2013.

[7] Z. Ding, M. Peng, Hsiao-Hwa Chen, "A General Relaying Transmission Protocol for MIMO Secrecy Communications," in *IEEE Trans. Commun.*, vol. 60, no. 11, pp. 3461-3471, Nov. 2012.

[8] J. Yang, Il-Min Kim and Dong In Kim, "Optimal Cooperative Jamming for Multiuser Broadcast Channel with Multiple Eavesdroppers," in *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2840-2852, Jun. 2013.

[9] J. Huang and A. Lee Swindlehurst, "Cooperative Jamming for Secure Communications in MIMO Relay Networks," in *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871-4884, Jul. 2011.

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

[11] J. Wang and A. Lee Swindlehurst, "Cooperative Jamming in MIMO Ad-Hoc Networks," in *Conference Record of the Forty-Third Asilomar Conference on Signals, Systems and Computers*, Nov. 2009.

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

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

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

[15] 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.

[16] D. Castanheira, A. Silva, A. Gameiro, "Retrospective Interference Alignment for the K -User M x N MIMO Interference Channel", *IEEE Trans. on Wireless Communications*, accepted for publication, pp. 1 - 12, Sep. 2016