Diogo dos Santos das Neves Pinheiro Gonçalves

Licenciado em Engenharia Electrotécnica e de Computadores

Segurança no nível físico em sistemas multi-antena com diretividade na informação

Dissertação para obtenção do Grau de
Mestre em Engenharia Electrotécnica e de Computadores

Orientador: Prof. Doutor Paulo Montezuma,
Professor Auxiliar, FCT-UNL

Co-orientador: Prof. Doutor Rui Dinis,
Professor Auxiliar com Agregação, FCT-UNL

Júri:

Presidente:	Doutor Nuno Filipe Silva Veríssimo Paulino
Arguente:	Doutor Luis Filipe Lourenço Bernardo
Vogal:	Doutor Paulo Miguel de Araújo Borges Montezuma de Carvalho

FACULDADE DE CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE NOVA DE LISBOA

Setembro, 2015

Segurança no nível físico em sistemas multi-antena com diretividade na informação

Agradecimentos

Em primeiro lugar gostaria de agradecer ao Professor Doutor Paulo Montezuma pelo incalculável trabalho na orientação ao longo do último ano, assim como ao Professor Doutor Rui Dinis e Professor Doutor Marko Berko por todos os recursos providenciados e todo o tempo disponibilizado na ajuda da resolução de problemas e dúvidas relacionadas com a investigação. Gostaria também de agradecer à instituição Faculdade de Ciências e Tecnologias da Universidade Nova de Lisboa, pelas instalações e material indispensável à realização da dissertação. Não posso deixar de agradecer aos meus colegas, Sara Ribeiro, Ricardo Martinho, António Bernardino e José Pedro Reis pelo tempo disponibilizado para me ouvirem sobre o meu trabalho, bem como algum apoio técnico relacionado com o mesmo, Por último, gostaria de agradecer aos meus amigos Clara Pereira, David Cardoso, e João Margarido, por todo o apoio ao longo de vários anos, e à minha mãe e ao meu pai, por tudo. Não teria sido possível sem todos vós.

RESUMO

Os sistemas de comunicação sem fios são sistemas de difusão por natureza. Devido a essa sua natureza, um dos problemas inerentes à mesma deve-se à segurança e ao secretismo, pois se o canal é partilhado a informação facilmente é obtida por um utilizador não autorizado, ao contrário dos sistemas de comunicação com fios. Tradicionalmente, a introdução de segurança em sistemas de comunicação, resulta na encriptação da informação, resultante de protocolos de encriptação. No entanto, a segurança através da criptografia baseia-se na premissa de que o utilizador não autorizado tem uma capacidade de processamento limitada, pois senão poderia simplesmente tentar todas as combinações possíveis e obter a chave de encriptação. Como a capacidade de processamento tem crescido exponencialmente, este tipo de sistemas tem se tornado cada vez mais complexos para não se tornarem obsoletos. A introdução de segurança na camada física torna-se então uma opção apelativa pois pode servir como um complemento, visto que os sistemas de criptografia funcionam em camadas superiores independentes da camada fisica, apresentando assim uma abordagem multi-camada em termos de segurança. Tipicamente as técnicas de segurança no nível físico podem se agrupar em 2 tipos: técnicas que se baseiam em códigos, ou técnicas que exploram variações temporais e espaciais do canal. As primeiras diminuem a eficiência espectral do sistema, e as segundas apresentam bons resultados em ambientes dinâmicos, mas em ambientes estáticos não são muito promissores. Há também a necessidade de aumentar as taxas de transmissão nos próximos sistemas de comunicação. Devido a estes requisitos, uma das tecnologias propostas para a nova geração de comunicações, é uma tecnologia baseada numa arquitectura Multiple-Input-Multiple-Output(MIMO). Esta tecnologia é promissora e consegue atingir taxas de transferências que correspondem aos requisitos propostos. Apresenta-se assim uma nova técnica de segurança no nível físico, que explora as caracteristicas físicas do sistema, como um complemento a outras medidas de segurança em camadas mais altas. Esta técnica não provoca diminuição da eficiência espectral e é independente do canal, o que tenta solucionar os problemas das restantes técnicas já existentes.

Palavras-chave: MIMO, segurança na camada física, criptografia, diversidade

Abstract

Wireless communication systems are broadcast by nature. Due to that feature, security is a main issue on them, because if the channel is shared the information can easily be obtain by a non-authorized user. Traditionally, the introduction of security in communications systems is made by encrypting the information using cryptography techniques. However, security by encryption relies on thinking that an eavesdropper have limited processing capacity, because with unlimited processing capacity, he would just try every combination possible and get the key to decrypt it. As computing power drastically increases over the years, cryptography systems have to become more complex not to become obsolete. Introduction of security at physical layers becomes an appealing offer, as a complement to other security techniques because cryptography techniques work in upper layers, creating a multi-layer security approach. Typically, physical layer security techniques can be grouped in two types: techniques based on codes, or techniques that exploit spatial or temporal channel variations. The first ones, reduce spectral efficiency. The second ones rely on dynamic environments. In static environments they don't show good results. There is also a need to increase transmission rates in the next generation of communication systems. One of the proposed technologies are based on Multiple-Input-Multiple-Output (MIMO) systems. MIMO systems presents promising results. A new technique for physical layer security that exploits MIMO systems features is presented. This technique is independent of channel and does not reduce spectral efficiency, so it resolves the problems presented in current techniques.

Keywords: MIMO, Physical layer security, cryptography, diversity

CONTEÚDO

LISTA DE FIGURAS

LISTA DE TABELAS

GLOSSÁRIO

AWGN Additive white Gaussian noise.

BER Bit Error Rate.

BPSK Bi-phase Shift Keying.

CIR Channel impulse Response.

DFE Decision Feedback Equalization.

IB-DFE Iterative Block - Decision Feedback Equalization.

IQI In Phase Quadrature Interference.

ISI Inter-Symbol Interference.

LS Least Square.

LTE Long Term Evolution.

MAN Metropolitan Area Network.

MIMO Multiple-Input-Multiple-Output.

MISO Multiple-Input-Single-Output.

MMSE Minimum Mean Square Error.

OQPSK Offset Quadrature Phase Shift Keying.

PbMFB Probability of Matched Filter Bound.

PDP Power Delay Profile.

Pe Bit error probability.

QAM Quadrature Amplification Modulation.

QPSK Quadrature Phase Shift Keying.

SC-FDE Single Carrier - Frequency Domain Equalization.

SIMO Single-Input-Multiple-Output.

SISO Single-Input-Single-Output.

SNR Signal to Noise Ratio.

CAPÍTULO 1

INTRODUÇÃO

1.1 Contexto

Os sistemas de comunicação sem fios são sistemas de difusão por natureza, o que os torna muito mais vulneráveis do que sistemas de comunicação com fios. Devido a essa característica, a segurança das comunicações é essencial neste tipo de sistemas. Atualmente, a segurança é assegurada através de protocolos de encriptação dos dados, onde a informação é encriptada sendo a sua descodificação possível mediante o conhecimento da chave usada.

Dado o crescimento exponencial da capacidade de processamento, os sistemas de criptografia têm vindo a tornar-se cada vez mais complexos para não ficarem obsoletos e fáceis de ultrapassar. Estes protocolos de segurança tipicamente funcionam nas camadas mais altas dos sistemas de comunicação independentemente da camada física. Portanto, a introdução de segurança na camada física pode complementar a segurança já existente, através de uma abordagem multi-camada.

Usualmente, as técnicas de segurança no nível físico baseam-se em códigos ou em sistemas que tentam explorar variações espaciais ou temporais no canal. As primeiras, diminuem a eficiência espectral e as segundas, necessitam de canais que variem, o que não acontence em todos os casos. Ora sistemas muito dependentes do canal de transmissão não são muito desejáveis por não garantirem uma neutralidade entre os utilizadores, e portanto ambas as técnicas de segurança no nível físico apresentam algumas limitações, havendo a necessidade de encontrar outro tipo de soluções. Os requisitos dos futuros sistemas de comunicação apontam para um aumento das velocidades de transferência de informação, maior eficiência energética, maior eficiência espectral e de uma maior cobertura de sinal.

Uma das tecnologias propostas para a nova geração de comunicações, é uma tecnologia baseada numa arquitetura Multiple-Input-Multiple-Output (MIMO). Esta tecnologia é

promissora e consegue atingir taxas de transferências que correspondem aos requisitos propostos[10].

A presente dissertação propõe uma nova abordagem de segurança no nível físico, recorrendo as caracteristicas físicas de uma arquitetura MIMO, apresentando análises e simulações realizadas com uma estrutura multi-antena proposta.

1.2 Objetivo

O principal objetivo do presente trabalho reside na exploração das características de transmissão/receção de um sistema MIMO ou Multiple-Input-Single-Output (MISO), para a introdução de segurança no nível físico, como complemento a outras técnicas de segurança aplicadas em outras camadas. Inclui-se a apresentação de uma estrutura multi-antena para o transmissor e a caracterização da segurança que pode ser obtida por alterações das caracteristicas da estrutura do transmissor. Também inclui o desenvolvimento de um simulador do sistema, que permite avaliar o desempenho e a segurança do mesmo. São analisadas diversas configurações do transmissor e comparados os graus de segurança e diretividade da informação associada a a cada configuração do transmissor. Também se inclui a definição de algoritmos para os recetores e respetiva avaliação de desempenho.

1.3 Organização da dissertação

A presente dissertação encontra-se organizada da seguinte forma:

O primeiro capítulo está reservado à introdução. O segundo capítulo consiste numa breve descrição das diferentes estruturas multi-antenas existentes, bem como uma contextualização do trabalho apresentado na dissertação. Foca-se nos problemas e vantagens das diferentes arquiteturas, nomeadamente a arquitetura convencional de única antena emissora e única antena recetora, chamada arquitetura Single-Input-Single-Output (SISO), na secção 2.1, e as diversas arquiteturas multi-antena: Single-Input-Multiple-Output (SIMO) na secção 2.2, MISO na secção 2.3 e MIMO na secção 2.4. O capítulo trata também ao longo das secções 2.1, 2.2, 2.3 e 2.4 de uma comparação entre as diferentes arquiteturas. Na secção 2.5 é caraterizado o beamforming. Aborda-se as constelações multi-camada na secção 2.6, como solução para um aumento da eficiência espectral necessária. A secção 2.7 introduz os amplificadores não-linear como medida para uma maior eficiência energética. Por fim, há uma descrição da estrutura proposta e são apresentados os problemas associados a essa estrutura.

O terceiro capítulo reside na exploração da segurança no nível físico. São analisadas diferentes configurações possíveis para a estrutura do transmissor, visando encontrar as melhores configurações em termos de segurança e desempenho. Na secção 3.1 faz-se uma introdução ao conceito de segurança e a alguns indicadores usados para quantificar e qualificar a segurança. Na secção 3.2 faz-se uma descrição do modelo utilizado e dos parâmetros variáveis na estrutura proposta para análise do desempenho e da segurança.

As secções 3.3 e 3.4 apresentam as análises e os resultados efetuados para os seguintes casos respetivamente: BER para constelações otimizadas para determinados ângulos com espaçamentos uniformes e com ou sem rotações de fase adicionais introduzidas ao nível da amplificação; Informação mútua com otimizações das constelações; informação mútua em função do ângulo θ de otimização com arrays de antenas de espaçamentos uniformes e não uniformes, com ou sem rotações adicionais de fase e BER com arrays de antenas de espaçamento não uniforme com rotações adicionais de fase.

O quarto capítulo trata do problema da estimativa dos parâmetros de emissão com recurso a pilotos, para a correção dos diferentes coeficientes das antenas, com a apresentação dos novos resultados e respetiva comparação com os resultados obtidos no terceiro capítulo. As análises efectuadas são realizadas para constelações 16QAM e 64QAM.

Finalmente no capítulo 5 são apresentadas as conclusões e algumas linhas orientadoras para trabalhos futuros.

CAPÍTULO 2

ESTRUTURAS MULTI-ANTENA

2.1 Introdução

Uma das propostas referentes a sistemas de quinta geração de comunicações móveis refere-se à introdução de uma arquitetura baseada no uso massivo de antenas, quer na transmissão, quer na receção. Muito do interesse relacionado com os sistemas MIMO deve-se aos trabalhos pioneiros de Winters [29], Foschini [6] e Telatar [25]. O MIMO convencional, tem um número muito limitado de antenas quer na transmissão quer na receção. Isto deve-se maioritariamente ao facto das antenas terem o seu tamanho e espaçamento dependente da frequência de trabalho das mesmas. Por exemplo, o Long Term Evolution (LTE) trabalha na gama de frequência dos 2.6 Ghz o que corresponde a um espaçamento entre as antenas na ordem das dezenas de centímetros, ou seja, estamos limitados a um número reduzido de antenas devido ao espaço disponível num telemóvel.

É no entanto sabido que a capacidade de um canal e a relação sinal-ruído aumentam com o aumento do número de antenas de transmissão e receção [2]. A arquitetura MIMO permite a utilização de arrays de antenas na transmissão que podem ser usados para aumentar o débito de transmissão reduzindo ao mesmo tempo a potência de cada antena. Os arrays usados nos sistemas MIMO também permitem obter diretividade ao nível da potência radiada de forma a criar diversos feixes diretivos de dados e minimizar assim a interferência do sistema. Obviamente que esta diretividade é conseguida desde que os sinais nas antenas de um determinado array sejam iguais, isto é a diretividade é conseguida com sacrifício do débito. Permitem também a implementação de esquemas de diversidade para aumento da capacidade de um sistema: quanto mais antenas, maior a capacidade do mesmo[28].

Existem diferentes tipos de arquiteturas que recorrem ao uso de múltiplas antenas, contrariamente aos sistemas tradicionais de única antena na transmissão e receção, nomeadamente MISO, SIMO e MIMO. Os sistemas apresentam características diferentes:

Enquanto num sistema SIMO, temos diversidade na receção, num sistema MISO temos diversidade na transmissão e num MIMO temos diversidade em ambas. Uma apresentação das diferentes técnicas usando múltiplas antenas, bem com vantagens e desvantagens das mesmas são expostas nas secções 2.2, 2.3 e 2.4.

O aumento do ritmo de transmissão em sistemas multi-antena pode ainda ser melhorado através do aumento da eficiência espectral da modulações empregues. O requisito de alta eficiência espectral só consegue ser atingido com recurso a constelações multidimensionais. Contudo, estas constelações têm flutuações de envolvente que impedem o uso de amplificadores de trabalhar próximo da saturação sem introdução de distorção não linear no sinal resultante da amplificação. Este problema pode ser evitado mediante a adopção de estruturas de emissão, como as apresentadas na secção 2.5, baseadas na decomposição da constelação em sub-constelações de envolvente constante ou quase constante, que são amplificadas e transmitidas independentemente umas das outras por diversas antenas. Esta decomposição só é possível se cada antena tiver o seu próprio circuito de radiofrequência, o que significa que cada ramo associado a uma das sub-constelações terá um amplificador ligado a uma antena. Nestas condições, cada amplificador pode trabalhar na zona de saturação e consegue-se uma amplificação linear de uma modulação baseada numa constelação de elevada ordem com recurso a amplificadores não lineares. Com isto conseguem-se eficiências energéticas superiores. Dado que da decomposição da constelação em componentes de envolvente constante resultam sinais incorrelacionados em cada um dos ramos de rádio frequência, o array não introduz directividade ao nível da potência radiada. No entanto, a forma da constelação transmitida, que é obtida por soma no canal dos diversos sinais transmitidos pelas antenas, vai depender do arranjo das antennas no array, pelo que se pode falar em diretividade de informação. Como se verá mais adiante, esta directividade pode ser usada para garantir segurança no nível físico.

2.2 Arquitetura SIMO

Os sistemas SIMO usam uma antena na transmissão, e múltiplas antenas na receção conforme se apresenta na figura 2.1.

Um dos problemas existentes nas comunicações sem fios, consiste no efeito de multipercurso que cria efeitos conhecidos como o desvanescimento temporal (fading), *cut-out* e receção intermitente. Estes efeitos acarretam uma diminuição das taxas de transmissão e um aumento do número de erros. O uso de várias antenas na receção pode minimizar o efeito multi-percurso, permitindo uma melhoria substancial do desempenho do sistema em situações em que o desvanecimento temporal é severo. Um recetor com diversidade na receção pode ter a estrutura apresentada na figura 2.2, onde o w representa os diferentes pesos de cada antena usados na combinação dos sinais, associada a cada ramo da receção.

Os sistemas SIMO são amplamente utilizados em televisão digital, em redes metropolitanas (Metropolitan Area Network (MAN)) e em comunicações móveis. As diferentes

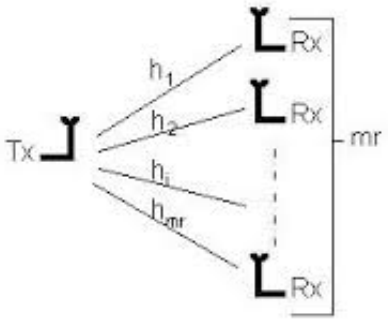

Figura 2.1: Arquitetura SIMO

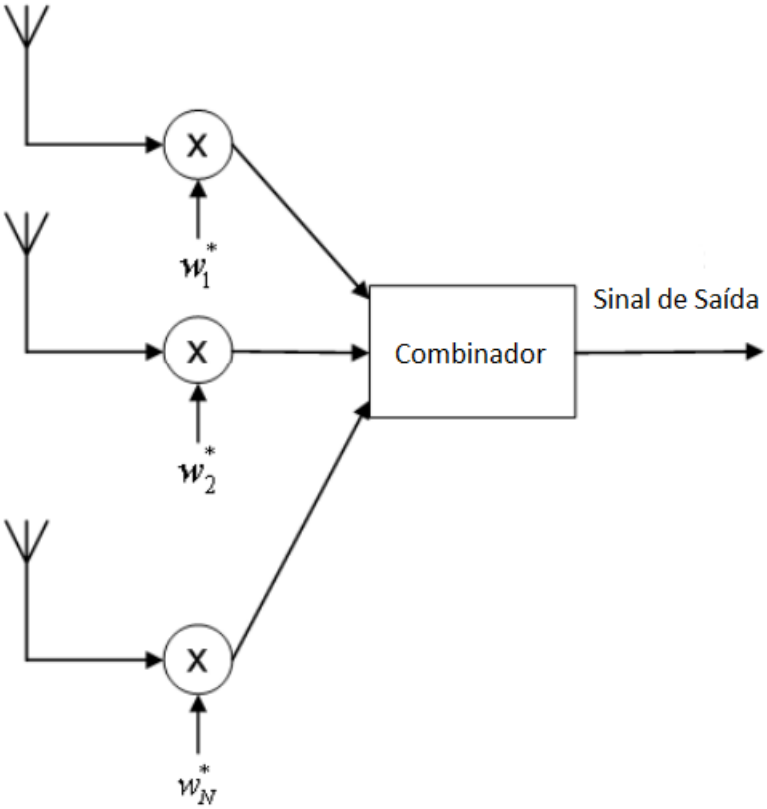

Figura 2.2: Esquema do recetor com diversidade na receção

técnicas de combinação associadas aos sistemas SIMO, podem-se agrupar em três tipos: seleção, combinação de rácio máximo e combinação de ganho igual.

2.2.1 SIMO de diversidade por seleção

Neste tipo de técnica de diversidade é selecionada a antena que tiver o sinal mais forte, ou seja, aquela que tiver um maior Signal to Noise Ratio (SNR). O sinal recebido pelas outras antenas continua a ser analisado, mas não está presente na saída do combinador. Se outra antena receber um sinal com um maior SNR, então esse sinal passa a ser selecionado até surgir uma outra antena com um sinal mais forte. Seja o sinal recebido por uma das antenas ao longo do tempo descrito por

$$y(t) = h(t) * s(t) + n(t), \tag{2.1}$$

onde $s(t)$ é a potência do sinal transmitido, $h(t)$ representa o canal, $n(t)$ representa o ruído e $(*)$ representa o operador convolução. A potência de sinal durante o período do símbolo, T_s na antena associada ao ramo de receção l, desde que o canal se mantenha constante, é dada por

$$P = \frac{1}{T_s}\int_0^{T_s} \left|h_l(t)^2\right| \left|s(t)^2\right| dt = \frac{\left|h_l(t)^2\right|}{T_s}\int_0^{T_s} \left|s(t)^2\right| dt = \left|h_l(t)^2\right|. \tag{2.2}$$

Sendo σ^2 a variância do ruído e de acordo com a equação (2.2), a relação sínal-ruído é dada por

$$E\left[\left|n_l(t)\right|^2\right] = \sigma^2 \Rightarrow SNR = \frac{\left|h_l(t)^2\right|}{\sigma^2}. \tag{2.3}$$

A seleção é depois feita escolhendo o ramo que têm um maior SNR para posterior processamento, com o peso desse ramo w_i igualado a 1 e o peso dos outros nulos, ou seja, apenas o sinal da antena com melhor SNR chega ao combinador. A desvantagem desta técnica reside no facto da mesma não aproveitar convenientemente a potência recebida, pois na obtenção do sinal estamos a excluir $N-1$ sinais do array de antenas.

2.2.2 SIMO de combinação do rácio máximo

Neste tipo de técnica todas as antenas contribuem para o sinal recebido. Usa a diversidade na receção para poder somar com pesos de ponderação distintos as contribuições dos diferentes ramos para obter um SNR ótimo. O sinal recebido continua a ser descrito por (2.1), mas com $\boldsymbol{h} = [h_0\ h_1\ h_2 ... h_{L-1}]^t$ e $\boldsymbol{n} = [n_0\ n_1\ n_2 ... n_{L-1}]^t$. Os pesos de cada antena são dados por [1]

$$w_l = \left|h_l\right| e^{jarg(h_l)} \Rightarrow w^H h = \sum_{l=0}^{L-1} \left|h_l\right|^2. \tag{2.4}$$

Portanto, na saída do combinador, o sinal é dado por

$$r(t) = \boldsymbol{W}^H y(t) = \boldsymbol{W}^H \boldsymbol{h} s(t) + \boldsymbol{W}^H \boldsymbol{n}. \tag{2.5}$$

[1] As matrizes e os vetores são representados a ***bold***.

Como

$$SNR = \frac{\left|\boldsymbol{W}^H \boldsymbol{h}\right|^2}{E\left[\left|\boldsymbol{W}^H \boldsymbol{n}\right|^2\right]} P_n \Rightarrow E\left[\left|\boldsymbol{W}^H \boldsymbol{n}\right|^2\right] = \sigma^2 \left|w\right|^2, \tag{2.6}$$

então

$$SNR = \frac{\left|\boldsymbol{W}^H \boldsymbol{h}\right|^2}{\sigma^2}, \left|w\right|^2 = 1. \tag{2.7}$$

Para $\boldsymbol{W} = \boldsymbol{h}$ temos o valor máximo de SNR, com

$$SNR = \sum_{l=0}^{L-1} SNR_l. \tag{2.8}$$

Conclui-se então que o SNR final é igual a soma dos SNR dos vários ramos. O combinador só pode escolher os pesos de cada ramo. O combinador de rácio máximo obtém um SNR ótimo, mas necessita que os pesos variem com o desvanecimento temporal dos sinais recebidos em cada uma das antenas, o que pode resultar em flutuações muito grandes dos valores dos coeficientes w_i.

2.2.3 SIMO de combinação de ganho igual

Um combinador de ganho igual resolve o problema da variação dos coeficientes w_i de cada ramo, já que assume um ganho unitário para cada ramo de receção, limitando as flutuações dos valores dos coeficientes w_i. Não apresenta resultados tão bons como a técnica de combinação de rácio máximo, mas pode ser o mais indicado em canais com forte desvanecimento temporal.

2.3 Arquitetura MISO

Ao contrário da estrutura SIMO, no MISO existem múltiplas antenas no transmissor e uma única antena do receção (ver figura 2.3). A mesma informação pode ser enviada pelas diversas antenas, de uma forma redundante.

Figura 2.3: Arquitectura Multiple-input-Single-Output

Este tipo de arquitetura pode ter vantagens nas redes móveis em relação a arquiteturas SIMO pois o processamento e a codificação redundantes são feitas pelo transmissor. No entanto, o facto de haver redundância na transmissão pressupõe alguma diminuição da

eficiência espectral para melhoria do SNR. Vale a pena referir duas abordagem diferentes para sistemas com múltiplas antenas na transmissão: Diversidade espacial e multiplexagem espacial. Na diversidade espacial, as múltiplas antenas enviam o mesmo sinal, utilizando a redundância da informação para mitigar os efeitos de desvanecimento temporal e melhorar a qualidade da ligação entre o emissor e o recetor. Tem como principal objetivo aumentar a relação sinal-ruído. A multiplexagem espacial consiste no uso das várias antenas para criar novas ligações entre emissor e recetor, fazendo uso da diretividade na informação proporcionada por transmissores multi-antena, o que permite aumentar a capacidade do sistema.

2.4 Arquitetura MIMO

Quando temos várias antenas no emissor e no recetor dizemos que estamos perante uma arquitetura MIMO (ver figura 2.4). Um sistema MIMO aumenta consideravelmente a

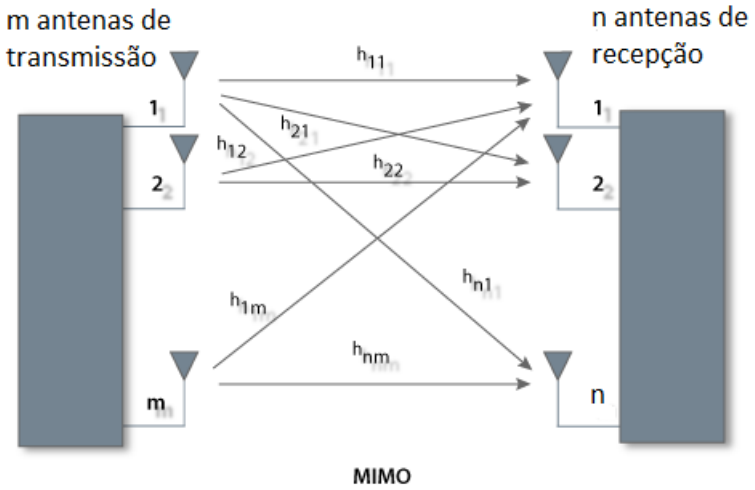

Figura 2.4: Arquitectura Multiple-input-Multiple-Output

complexidade de implementação dado que são necessários cuidados extras no projeto dos circuitos de radiofrequência, bem como algoritmos mais complexos de processamento de sinal. Podem-se usar sistemas MIMO para melhorar o SNR, ou para aumentar a capacidade de um sistema. O aumento da SNR permite o uso de constelações multi-dimensionais maiores, ou uma diminuição da potência de sinal transmitida. Ambas são descritas nas subsecções seguintes.

2.4.1 Multiplexagem espacial

O principal objetivo de uma técnica MIMO com multiplexagem espacial consiste no aumento da taxa de transferência em relação aos sistemas SISO.

Na multiplexagem espacial, a informação é repartida em M blocos que são transmitidos simultaneamente na mesma banda de frequência, o que aumenta o ritmo por um fator de M (ganho por multiplexagem). No recetor, os diferentes blocos são separados por algoritmos que visam cancelar a interferência entre os mesmos. Portanto, só é necessário o conhecimento do canal por parte do recetor. Tipicamente, para um bom desempenho considera-se um número maior de antenas no emissor do que no recetor $M \geq N$. Um exemplo de MIMO com multiplexagem espacial é apresentado na figura 2.5, onde h_{ij} representa o canal entre a antena de emissão i e a antena de receção j, s_i o sinal transmitido pela antena i e r_j o sinal recebido pela antena j.

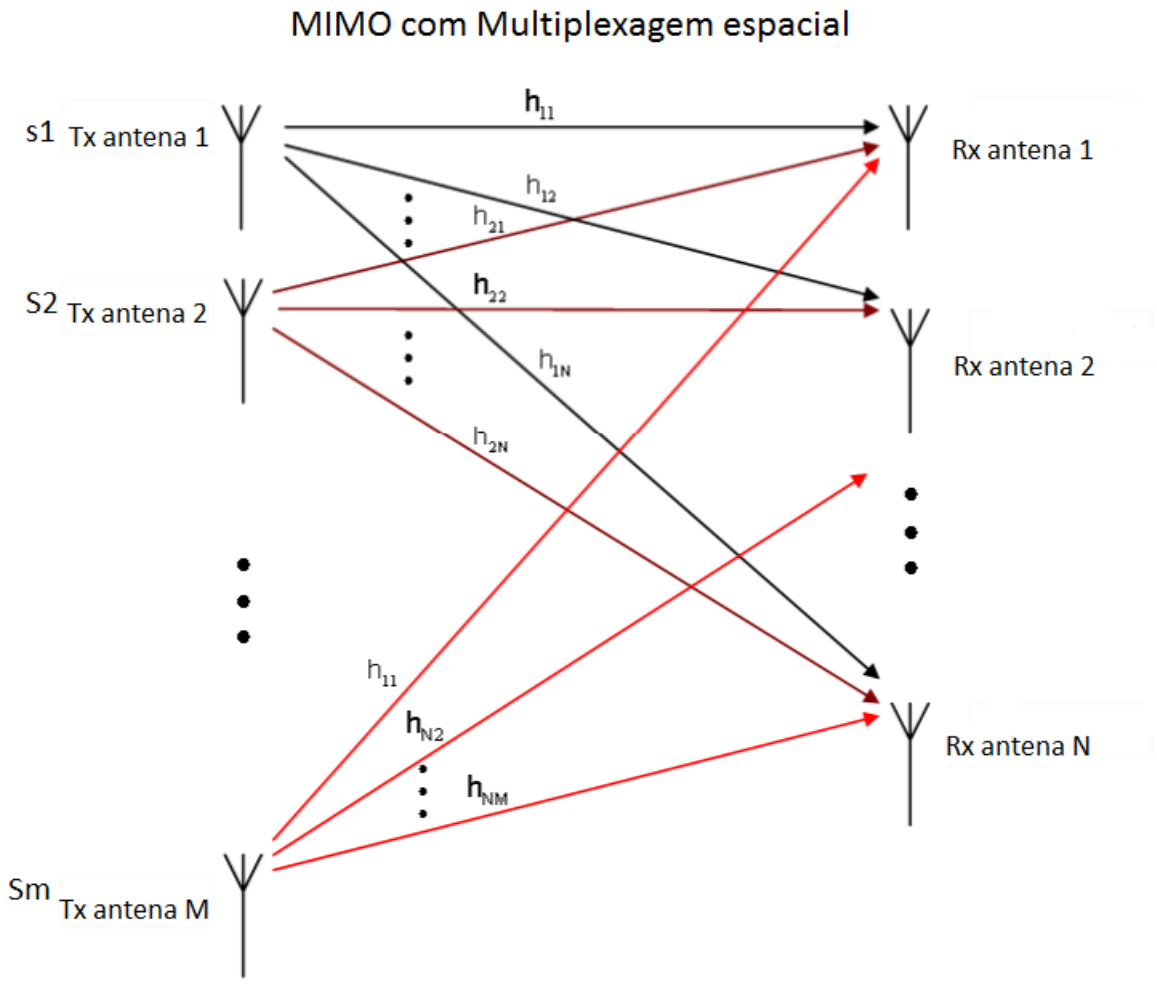

Figura 2.5: Esquema de um sistema MIMO com multiplexagem espacial

2.4.2 Melhoramento do SNR

Um esquema particularmente elegante de diversidade espacial em sistemas MIMO foi criado por Alamouti [20]. Publicado pela primeira vez em 1998, o esquema mais simples

tem apenas diversidade na transmissão, com um array de duas antenas no transmissor, e uma única antena no recetor(ver figura 2.6). Assume-se que :

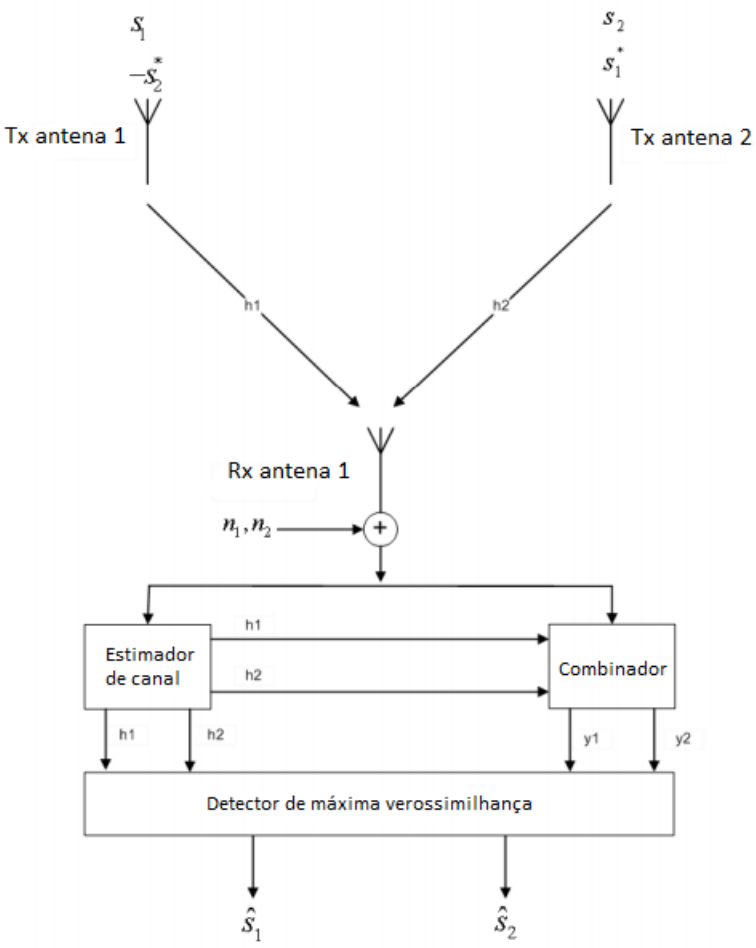

Figura 2.6: Esquema do código de Alamouti

- Aquando de uma transmissão, os símbolos são enviados duas vezes.
- O símbolo s_0 é enviado pela antena 1 no instante de tempo t.
- O símbolo s_1 é enviado pela antena 2 no instante de tempo t.
- No instante de tempo $t + T_s$ a antena 1 envia s_1^* e antena 2 envia s_0^*.

Assume-se também que o canal se mantém invariante durante a transmissão de dois

símbolos consecutivos. Assim sendo, os sinal recebidos são dados por

$$\begin{cases} r_1 = r(t) = h_1 s_1 + h_2 s_2 + n_1 \\ r_2 = r(t+T_s) = -h_1 s_2^* + h_2 s_1^* + n_2 \end{cases} \Rightarrow \begin{bmatrix} r_1 \\ r_2 \end{bmatrix} = \begin{bmatrix} s_1 & s_2 \\ -s_2^* & s_1^* \end{bmatrix} \begin{bmatrix} h_1 \\ h_2 \end{bmatrix} + \begin{bmatrix} n_1 \\ n_2 \end{bmatrix}, \tag{2.9}$$

em que r_1 e r_2 representam os sinais recebidos à saída do recetor, n_1 e n_2 são os termos do ruído, h_1 e h_2 representam o canal e $(*)$ é o operador do complexo conjugado. Combinando os sinais resulta

$$\begin{aligned} y_1 &= h_1^* r_1 + h_2 r_2^* = h_1^* h_1 s_1 + h_1^* h_2 s_2 + h_1^* n_1 - h_2 h_1^* s_2 h_2^* h_2 s_1 + h_2 n_2^*, \\ y_2 &= h_2^* r_1 - h_1 r_2^* = h_2^* h_1 s_1 + h_2^* h_2 s_2 + h_2^* n_1 + h_1 h_1^* s_2 - h_2^* h_1 s_1 - h_1 n_2^*. \end{aligned} \tag{2.10}$$

Como o canal é invariante ao longo dos dois símbolos consecutivos podemos descrever os sub-canais como

$$\begin{aligned} h_1(t) &= h_1(T_s + t) = h_1, \\ h_2(t) &= h_2(T_s + t) = h_2. \end{aligned} \tag{2.11}$$

em que T_s representa a duração de um símbolo. No recetor, após o combinador têm-se

$$\begin{aligned} y_1 &= \left(|h_1|^2 + |h_2|^2\right) s_1 + h_1^* n_1 + h_2 n_2^*, \\ y_2 &= \left(|h_1|^2 + |h_2|^2\right) s_2 - h_1^* n_2 + h_2^* n_1. \end{aligned} \tag{2.12}$$

O mesmo esquema pode ser generalizado para N antenas no recetor. Tem uma complexidade semelhante à técnica de combinação de rácio máximo descrito na secção 2.2. O esquema de Alamouti tem particular interesse uma vez que as vantagens inerentes ao mesmo são independentes de alguma informação que o transmissor possa dar ao recetor e da largura de banda utilizada. O esquema também não necessita de uma complexidade computacional elevada.

2.4.3 Beamforming

Para aproveitar a diretividade da informação de arrays de antenas em sistemas MIMO, recorre-se a técnicas de processamento de sinal baseadas em filtragem espacial. Estas técnicas consistem no uso da directividade para garantir selectividade espacial da informação, mediante a criação de zonas onde os sinais sofrem uma interferência construtiva, aumentando a potência de sinal e reduzindo noutras, onde os sinais sofrem uma interferência destrutiva, conforme se encontra representado na figura 2.7.

Os principais desafios do beamforming consistem no combate à interferência intersimbólica e no combate da interferência co-canal [27].

As técnicas de beamforming podem ser divididas em dois tipos:

- Beamforming convencional, onde os desvios de fase e a contribuição das diversas antenas têm um número fixo de variações possíveis para serem posteriormente combinados, havendo um número finito de adaptações que o beamformer pode tomar.

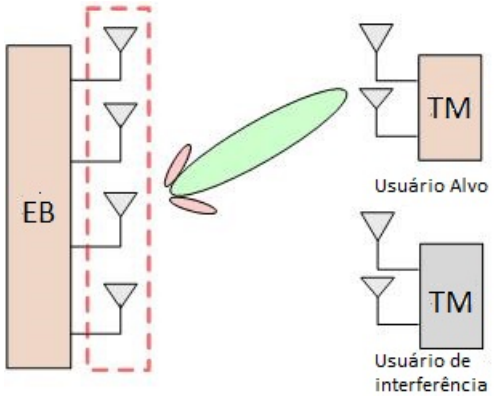

Figura 2.7: Beamforming num sistema MIMO. TM - Terminal Móvel EB- Estação base.

- Beamforming adaptativo, que através da informação das propriedades do sinal, e das variações do mesmo reage de maneira a diminuir a interferência e otimizar o sinal. O beamforming adaptativo recorre a estimações do sinal para uma melhor otimização.

As técnicas de beamforming aumentam consideravelmente a eficiência espectral à custa de um maior processamento de sinal. No entanto, e apesar das vantagens referidas, não são consideradas este tipo de técnicas neste trabalho.

2.4.4 Amplificação tradicional de sistemas MIMO

Tipicamente nos sistemas MIMO o sinal transmitido pelas antenas é amplificado antes de ser enviado para estas [26]. Embora se possam ter vários ramos no transmissor, o sinal que é amplificado é um sinal de envolvente variável que resulta da combinação dos sinais gerados paralelamente ou não. Como tal, amplificação será ineficiente uma vez que o sinal tem flutuações de envolvente. Dado que se tem de garantir conseguirmos níveis de distorção baixos, o rendimento do andar de amplificação fica logo à partida limitado no seu desempenho energético. Estas eficiências baixas de amplificação resultam num aumento do consumo de potência, o que por sua vez resulta numa redução da duração da bateria e do seu ciclo de vida[11].

2.5 Constelações Multi-camada

Já foi referido que a eficiência espectral aumenta à medida que o tamanho das constelações aumenta. Para reduzir os custos associados à amplificação de modulações multi-dimensionais, e consequentemente aumentar a eficiência energética dos amplificadores de potência, pode-se recorrer a uma técnica de decomposição de constelações em vários componentes Bi-phase Shift Keying (BPSK), Quadrature Phase Shift Keying (QPSK) ou Offset Quadrature Phase Shift Keying (OQPSK) [19]. Considere dois sinais OQPSK, $x_p(t)$ e

$x_{p'}(t)$, com envolventes complexas, cada um associado a uma constelação QAM e descritas pelas envolventes

$$x_p(t) = \sum_{n'}^{\infty} b_{n'}^{(p)} x^{(p)}(t - n'T), \tag{2.13}$$

e

$$x_{p'}(t) = \sum_{n'}^{\infty} b_{n'}^{(p')} x^{(p')}(t - n'T). \tag{2.14}$$

Assume-se a mesma forma para os pulsos de ambos os sinais, isto é $k_p r(t)$ e $k_{p'} r(t)$, respetivamente.

Combinando os sinais temos

$$x(t) = \sum_{n'}^{\infty} b_{n'}^{(p)} x^{(p)}(t - n'T) + \sum_{n'}^{\infty} b_{n'}^{(p')} x^{(p')}(t - n'T), \tag{2.15}$$

Assumindo que os coeficientes $k_p \neq k_{p'}$ para cada instante de amostragem tem-se

$$k_p b_{n'}^{(p)} + k_{p'} b_{n'}^{(p')} = a_{n'}', \tag{2.16}$$

onde $a_{n'}$ assume os valores $\pm k_p \pm k_{p'}, \pm jk_p \pm k_{p'}, \pm k_p \pm jk_{p'}, \pm jk_p \pm jk_{p'}$ que correspondem aos 4 sub-conjuntos de 4 símbolos de uma constelação 16QAM. De igual modo, uma constelação 64QAM pode ser vista como uma soma de 3 sinais OQPSK. Convém salientar que cada constelação OQPSK pode ser definida como uma soma de dois componentes BPSK em quadratura. Um sinal BPSK pode ser descrito por

$$s_i = g_{Nm} e^{j\theta_{Nm}}, \tag{2.17}$$

onde g_{Nm} é o coeficiente da antena. Logo, os símbolos de uma dada constelação podem ser descritos na forma

$$a_n = g_0 + g_1 b_n^{(1)} + g_2 b_n^{(2)} + g_3 b_n^{(1)} b_n^{(2)} + ... = \sum_{i=0}^{M-1} g_i \prod_{m=1}^{\mu} (b_n^{(m)})^{\gamma_{m,i}}, \tag{2.18}$$

com cada $a_n \in a$, onde $(\gamma_{\mu,i}, ..., \gamma_{1,i})$ são as representações binárias de i. Como temos M símbolos na constelação e M coeficientes complexos g_i, a equação anterior é um sistema de M equações que pode ser usado para obter os coeficientes g_i. Escrevendo (2.18) no seu formato matricial, obtém-se

$$\boldsymbol{a} = \boldsymbol{W}\boldsymbol{g} \tag{2.19}$$

Conclui-se então que, dada uma constelação, é possível obter os respetivos coeficientes g_i a partir do inverso da transformada de Hadamard de cada ponto da constelação. Conclui-se também que uma constelação genérica pode ser descrita como a soma de $M/2$ sub-constelações OQPSK ou M sub-constelações BPSK. Logo, em sistemas MIMO ou MISO, cada antena pode estar associada a uma componente BPSK. Para as constelações M-QAM são apenas necessárias $log_2(M)$ componentes BPSK.

2.6 Amplificação Linear a partir de amplificadores não-lineares

Os amplificadores de potência são componentes importantes nos sistemas de comunicação, garantindo a potência de sinal necessária para compensar o desvanecimento temporal lento. No entanto, existem alguns problemas inerentes aos mesmos. Estes componentes consomem uma parte muito elevada da energia total do sistema. O consumo de potência associado aos amplificadores de potência define o ciclo de vida das baterias nos dispositivos móveis[11]. Tipicamente os amplificadores trabalham como dispositivos lineares em condições de baixa potência de saída como apresentado na secção 2.4.4, e vão-se tornando dispositivos não lineares à medida que o sinal é amplificado para valores maiores. A eficiência do amplificador também aumenta à medida que a potência de saída aumenta, havendo então uma necessidade de otimizar a eficiência do amplificador, ou seja, a duração da bateria e a distorção de sinal obtida. Para a maioria das aplicações comerciais as limitações são impostas pela interferência entre utilizadores adjacentes, e portanto, o nível de amplificação de sinal é mantido a operar longe da sua eficiência máxima.

Com a decomposição das constelações numa soma de sub-constelações de envolvente constante ou quase constante, que são amplificadas e transmitidas por uma antena independentemente uma das outras. Nestas condições, cada antena funciona então com um circuito de radio frequência individual, sendo a constelação à saída a combinação dos componentes de saída de cada antena. Logo, é possível ter todos os amplificadores a trabalhar na zona não linear, uma vez que se podem ter componentes de envolvente constante em cada um dos ramos. Isto permite aumentar a eficiência energética já que os amplificadores podem estar na saturação sem causar distorção não linear em cada um dos componentes BPSK. Uma imagem de um esquema de um transmissor recorrendo a esta abordagem é apresentado na figura 2.8. Este tipo de estrutura vai ao encontro de propostas para aumentar a eficiência energética através da colocação dos amplificadores a trabalhar na zona de saturação [12].

Dado que da decomposição da constelação em componentes de envolvente constante resultam sinais não correlacionados em cada um dos ramos de rádio frequência, o array não introduz diretividade ao nível da potência radiada. No entanto, a forma da constelação transmitida, que é obtida por soma no canal dos diversos sinais transmitidos pelas antenas, vai depender do arranjo das antenas no array, pelo que se pode falar em diretividade de informação. Como se verá mais adiante, esta directividade pode ser usada para garantir segurança no nível físico.

2.7 Estrutura Proposta

A estrutura do transmissor consiste num array de N_m antenas cada uma com um circuito de radiofrequência individual para garantir uma amplificação eficiente dos sinais através da execução dos seguintes passos: os bits são primeiro mapeados numa dada constelação (por exemplo 64QAM) caracterizada pelo seguinte conjunto de símbolos $\varsigma = S_1, S_2, ..., s_{M-1}$

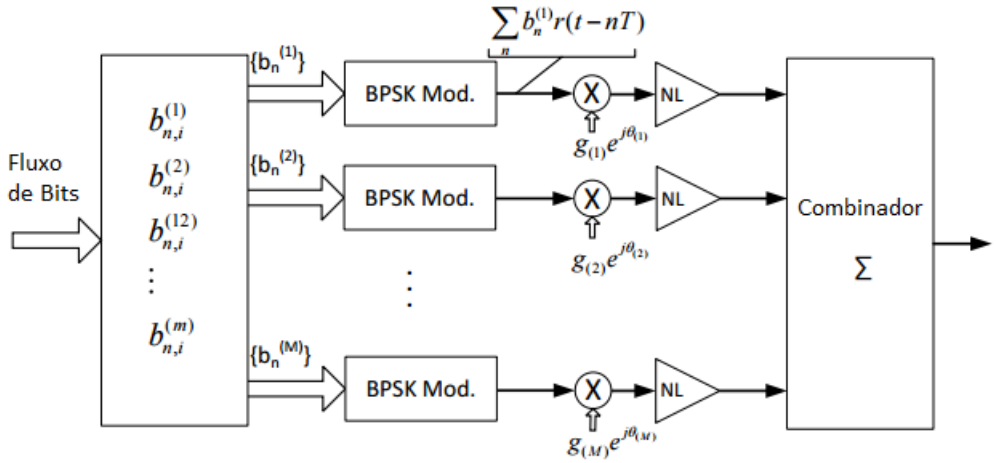

Figura 2.8: Amplificação individual de componentes BPSK

seguindo a seguinte regra $(\beta_n^\mu, \beta_n^\mu, \beta_n^{\mu-1}, ..., \beta_n^2, \beta_n^1) \mapsto s_n \in \varsigma$, com $(\beta_n^\mu, \beta_n^\mu, \beta_n^{\mu-1}, ..., \beta_n^2, \beta_n^1)$ correspondendo as representações binárias de n com $\mu = \log_2(M)$ bits. De seguida, os símbolos são decompostos em $M = N_m$ componentes polares, por exemplo

$$s_n = g_0 + g_1 b_n^{(2)} + g_2 b_n^{(2)} + g_3 b_n^{(1)} b_n^{(2)} + g_4 b_n^{(3)} + ... = \sum_{i=0}^{M-1} g_i \prod_{m=1}^{\mu} (b_n^{(m)})^{\gamma_{m,i}}, \tag{2.20}$$

com $(\gamma_{\mu,i}\gamma_{\mu-1,i}...\gamma_{2,i}\gamma_{1,i})$ a serem as representações binárias de i e $b_n^m = (-1)^{\beta_n^m}$ a representação polar do bit β_n^m.

Com isto, temos M símbolos da constelação e M coeficientes g_i das antenas o que significa que (2.3) é um sistema de M equações que pode ser usado para obter os coeficientes g_i. Como as saídas dos N_m amplificadores só são somadas ao nível do canal de transmissão são evitadas perdas de combinação de sinais. Devido ao facto dos diversos componentes BPSK não estarem correlacionados, a diretividade só é introduzida ao nível da informação. Isto tudo significa que, a forma e o mapeamento da constelação podem ser modificados de acordo com os valores dos coeficientes g_i em cada ramo. Alterando os coeficientes das antenas podemos ter constelações otimizadas segundo um certo ângulo, criando directividade na informação. Consequentemente, o número de constelações possíveis torna-se muito elevado. A construção de constelações a partir de sub-constelações permite que cada antena tenha o seu próprio circuito de radiofrequência e criar sistemas de amplificação lineares com amplificadores não lineares, uma vez que os sinais amplificados em cada ramo têm envolvente constante. Alterando os valores dos coeficientes g_i é também possível obter constelações rodadas o que aumenta consideravelmente o número de constelações possíveis de obter, e cria uma certa otimização para determinados ângulos. Consequentemente, garante-se segurança pois um recetor não autorizado precisa

de estimar os coeficientes g_i que afetam as antenas e os desvios de fase entre as antenas [15]. A estrutura é apresentada na figura 2.9.

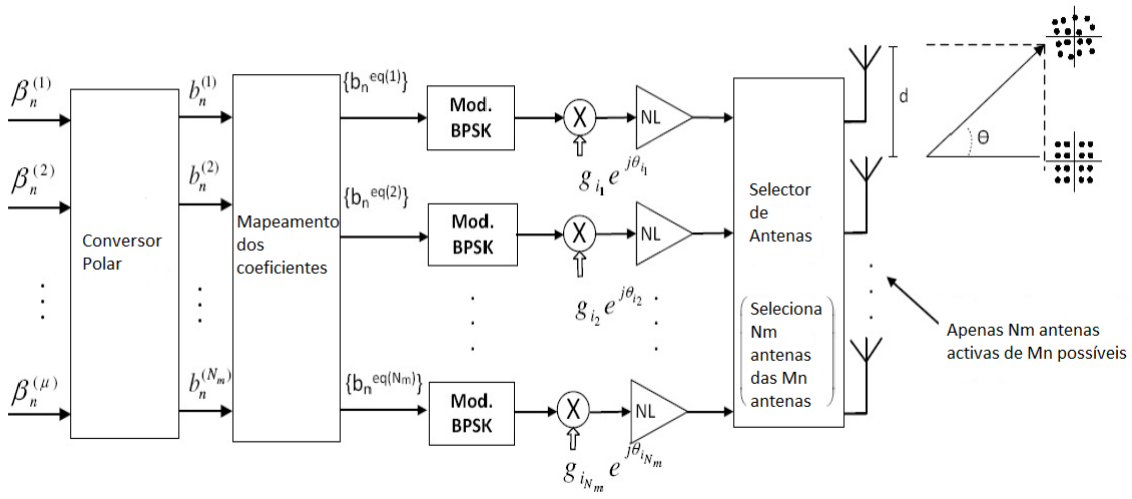

Figura 2.9: Estrutura do transmissor multi-antena

2.8 Problemas associados à estrutura de emissão

A estrutura proposta garante elevada eficiência espectral devido à utilização de constelações multi-dimensionais M-QAM, com M=16, 32 ou 64, ou constelações Voronoi e a eficiência energética é garantida mediante o uso de amplificadores a operar na zona de funcionamento não-linear, em cada circuito de rádio frequência. Uma das particularidades dos transmissores multi-antenas reside na possibilidade de não ter todas as antenas a contribuir para criação do sinal. Por exemplo, um transmissor com Nm antenas pode ter num determinado momento Nu antenas ativas a contribuir para a criação do sinal, com $Nm \geq Nu$. Desta forma podem ser consideradas rotações de fase adicionais correspondentes a contribuições de antenas não ativas entre duas antenas ativas, aqui chamadas de antenas fantasma. A inclusão destas rotações de fase permite aumentar consideravelmente a complexidade do sistema e consequentemente melhorar a segurança. Nestas condições, o número de combinações possíveis com um transmissor de Nm antenas e apenas Nu antenas ativas é

$$\frac{N_m!}{(N_m - N_u)!N_m!}. \tag{2.21}$$

Este número não reflete o verdadeiro número de combinações pois na prática o desfasamento entre as antenas pode ser qualquer número real, resultando num desfazamento entre antenas $\delta\theta$ que pode ser qualquer número real entre 0 e 2π. No entanto, constelações multi-dimensionais têm os seus ganhos de eficiência espectral, à custa do aumento da Inter-Symbol Interference (ISI), o que aumenta a taxa de erros, diminuindo o desempenho geral do sistema. As constelações rodadas podem diminuir ainda mais a distância entre os seus símbolos. O recetor utilizado consiste num recetor Iterative Block - Decision Feedback Equalization (IB-DFE), pois apresenta bons resultados para sistemas MIMO [17, 24]. O

recetor está otimizado para constelações multi-dimensionais para mitigar a ISI e a In Phase Quadrature Interference (IQI), associadas a estes tipos de constelações. Como os símbolos da constelação estão mais próximos uns dos outros, o recetor tem de estimar perfeitamente os coeficientes g_i das antenas que constroem a constelação, e a configuração das fases do array, senão a constelação recebida sofre, além de outros efeitos indesejáveis, distorções não lineares provocadas pelas rotações de fase associadas a cada ramo de amplificação que o recetor é incapaz de compensar. Com erros na estimação a forma da constelação pode alterar drasticamente. Nas figuras 2.10, 2.11 e 2.12, são apresentados três exemplos do efeito de erros na estimação do ângulo θ segundo o qual a constelação se encontra otimizada. Consideram-se os resultados para 16QAM, 64QAM e 16Voronoi, que incluem para efeitos de comparação as constelações sem rotação, e com erros de 2º e 4º. Pode-se observar que a distorção é tanto maior quanto maior for o erro e/ou a dimensão da constelação. Para a mesma dimensão, é notório que a distorção associada ao erro é maior na constelações de Voronoi (no resto do trabalho a análise limita-se a M-QAM regulares).

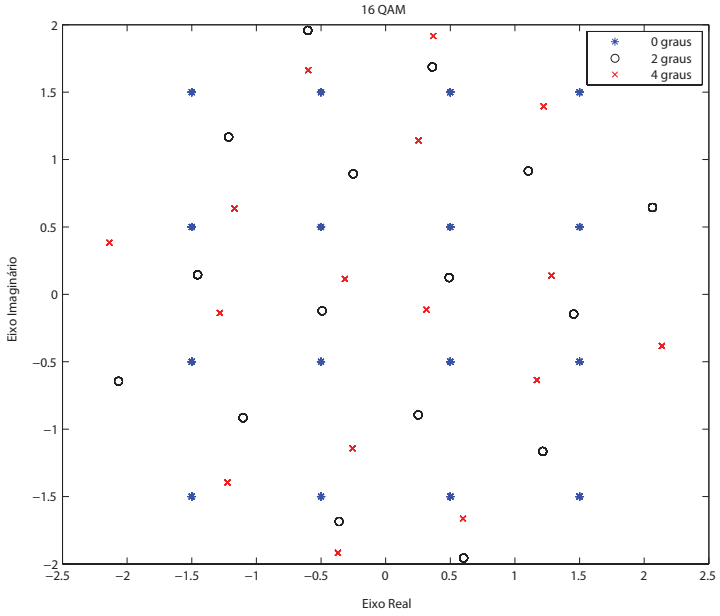

Figura 2.10: Efeito de um erro na estimação do ângulo de otimização numa constelação 16QAM

Notar que estes erros podem ser devido a erros de estimação dos coeficientes complexos g_i que têm efeitos similares a desequilibrios de ganho e fase entre os amplificadores usados nos diversos ramos do transmissor. Ora se a estimação não for precisa, apenas um desvio pequeno pode alterar completamente a forma da constelação. Essa sensibilidade

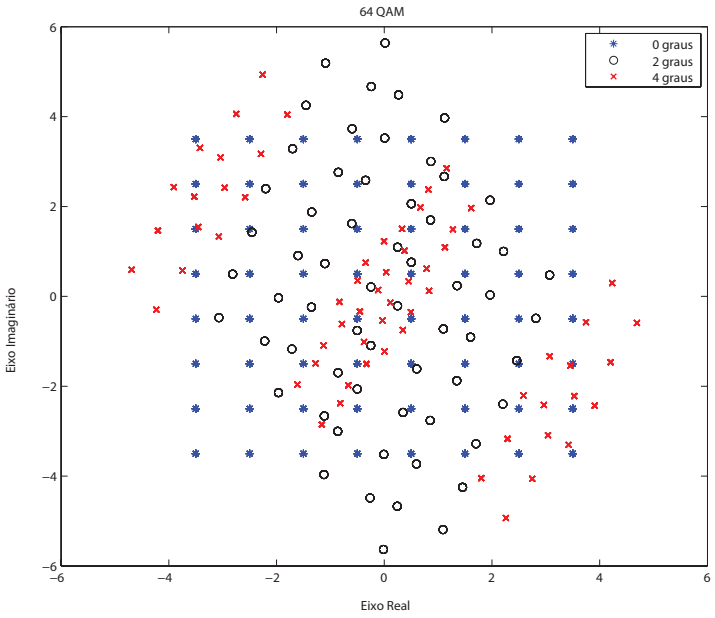

Figura 2.11: Efeito de um erro na estimação do ângulo de otimização numa constelação 64QAM

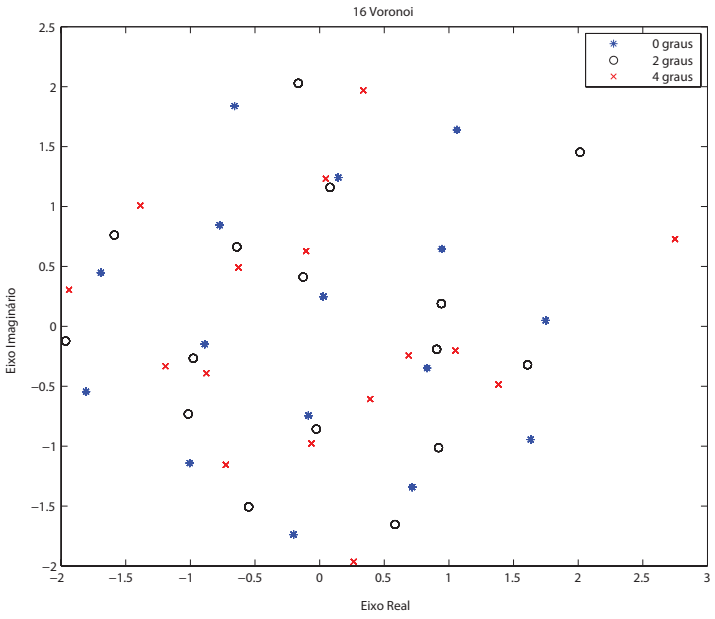

Figura 2.12: Efeito de um erro na estimação do ângulo de otimização numa constelação 16voronoi

pode ser usada para efeitos de segurança, uma vez que um recetor deve saber perfeitamente os coeficientes g_i e arranjos das antenas, pois caso contrário será incapaz de receber com sucesso a informação transmitida.

CAPÍTULO 3

ANÁLISE DE SEGURANÇA E CONFIGURAÇÃO DO SISTEMA

Neste capítulo é analisada a segurança do nível físico inerente à estrutura de transmissor proposta no capítulo 2. São efetuadas análises ao sistema, nomeadamente cálculos da informação mútua e do BER, para diferentes configurações.

3.1 Segurança

Os fundamentos da teoria de informação usada nos conceitos modernos de segurança empregues em telecomunicações, foram postulados por Shannon no seu trabalho em 1949 [22]. Tipicamente a segurança é garantida por técnicas de criptografia baseadas em chaves que trabalham na camada de rede ou camadas superiores [13]. No entanto, as vulnerabilidades associadas a este tipo de técnicas [3] [9] [21], motivam a busca de outras técnicas e de esquemas complementares. As técnicas de segurança no nível físico foram primeiramente estudadas teoricamente por Wyner e Maurer [1], mas só recentemente os aspectos ligados à segurança implementada no nível físico tem suscitado interesse. Tipicamente as técnicas de segurança na camada física usam códigos para comunicar de maneira segura [8], ou exploram variações temporais e espaciais do canal [4]. Contudo, as técnicas baseadas em códigos diminuem a eficiência espectral devido ao uso de bits redundantes e as técnicas baseadas nas variações de canal prossupõem ambientes dinâmicos, o que nem sempre acontece (em ambientes estáticos este tipo de técnicas tem um fraco desempenho [7]). Com a estrutura proposta na secção 2.8, consegue-se segurança independente do canal sem diminuição da eficiência espetral. A segurança é assegurada com cada sequência de bits do emissor a serem convertidos em símbolos de uma dada constelação, definida pelos coeficientes g_i, e que são apenas conhecidos pelo emissor e pelo recetor. Como a forma da constelação transmitida depende dos coeficientes, uma pequena variação destes provoca

alterações na forma da constelação e consequentemente na organização dos símbolos e/ou mapeamentos dos mesmos, o que dificulta a extração de informação quando os g_i e os arranjos destes pelas antenas não são conhecidos.

3.2 Configuração da estrutura

O problema mais simples de segurança consiste no cenário proposto na secção 2.8, com um recetor autorizado 'Bob' e um recetor não autorizado 'Eva', conforme apresentado na figura 3.1.

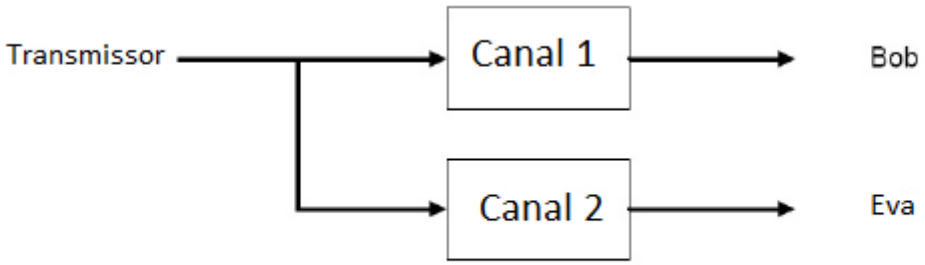

Figura 3.1: Canal Gausseano não degradado

Seja $s(t)$ o n-ésimo símbolo transmitido associado ao bloco

$$s(t) = s_n h_{T(t-nT_s)}, \tag{3.1}$$

com T_s a representar o período do símbolo e $h_T(t)$ a forma do pulso adotado. Nestas condições os sinais recebidos pelo intruso e pelo recetor autorizado são respetivamente

$$, y(t) = f_A(s(t)) * h(t) + n_1(t), \tag{3.2}$$

e

$$z(t) = f_A(s(t)) * h(t) + n_2(t), \tag{3.3}$$

em que $n_1(t)$ e $n_2(t)$ são os termos dos ruídos, f_A a fator do array que altera a forma da constelação e $h(t)$ a resposta impulsiva do canal. Para efeitos de simplificação, considera-se inicialmente um canal Additive white Gaussian noise (AWGN).

Uma segurança perfeita implica que $I(MS; RE) = 0$, em que MS é a mensagem enviada, RE representa a mensagem recebida pelo recetor não autorizado e $I(:;:)$ representa a informação mútua (MI- Mutual Information). Importa referir que a informação mútua (assumindo símbolos equiprováveis para um conjunto de sinais definido num alfabeto $\mathfrak{S}$ dá o valor máximo do ritmo de transmissão que é possível na ausência de erros e pode ser

dada por

$$I(S,Y) = \log_2 M - \frac{1}{M}\sum_{s\in\mathfrak{S}} \boldsymbol{E}_n \left[\log_2\left(\sum_{s'_n\in\mathfrak{S}} \exp(-\frac{1}{N_0}|\sqrt{E_s}(s_n - s'_n) + n|^2 - |n|^2)\right)\right], \tag{3.4}$$

onde $\boldsymbol{E}$ representa o valor esperado e E_s representa a energia de símbolo. A capacidade de secretismo é a diferença entre as informações mútuas do recetor autorizado e do recetor não autorizado. Numa situação em que "Eva"não tem informação acerca da configuração do transmissor, isto é o conjunto de coeficientes complexos g_i, o arranjo destes nas antenas e a configuração do array, a informação mútua é sempre nula. Como tal a capacidade de secretismo coincide simplesmente com a informação mútua do recetor autorizado, ou seja, a MI do "Bob".

Para efeitos do cálculo da MI, na simulação consideram-se os valores médios resultantes de 1000 ciclos de Monte-Carlo independentes e um canal AWGN. Os símbolos s_n são selecionados aleatoriamente a partir de uma constelação M-QAM (só se consideram constelações com dimensões de 16 e 64). Também se assume uma amplificação linear ao nível do transmissor, sincronização no tempo e na frequência perfeitas e uma estimativa perfeita do canal no caso em que se consideram canais dispersivos. Os resultados são representados quer em função de $\frac{E_b}{N_0}$, onde $N_0/2$ é a variância do ruído e E_b a energia de bit (bits transmitidos), quer em função do ângulo θ segundo o qual a constelação se encontra otimizada. Nos resultados referentes à evolução da MI com θ, caso não seja dito nada em contrário, as relações sinal ruído são de 14 dB e 18 dB, para 16-QAM e 64-QAM, respetivamente.

Para os cálculos da BER usam-se canais reais com uma dispersão temporal severa, caracterizado por um Power Delay Profile (PDP) uniforme. O canal é representado por um conjunto de 32 raios atrasados não correlacionados, com um desvanecimento de Rayleigh. As BER calculadas são comparadas com os resultados para um filtro Probability of Matched Filter Bound (PbMFB), onde o SNR é otimizado. Embora existam várias regras de mapeamento para constelações M-QAM e Voronoi, só se consideram as constelações 16QAM e 64QAM retangulares e as constelações resultantes da sua otimização segundo uma determinada direção θ. A constelação 16QAM consegue ser definida como a soma de duas constelações OQPSK, ou seja, quatro componentes BPSK. Para 16QAM e 64QAM os conjuntos de coeficientes que definem estas constelações são os que constam das tabelas 3.1 e 3.2.

Tabela 3.1: coeficientes g_i associadas às das antenas do emissor (16QAM)

16QAM	Antenas			
	1	2	3	4
Coeficientes gi	2j	1	2	j

Tabela 3.2: Coeficientes g_i associadas às antenas do emissor (64QAM)

64QAM	Antenas					
	1	2	3	4	5	6
Coeficientes gi	2j	1	2	j	4	4j

As constelações Voronoi necessitam de M-1 coeficientes não nulos na sua definição. Outras constelações podem ser obtidas variando os valores dos coeficientes g_i. A segurança inerente ao transmissor deve-se ao facto dos bits enviados serem convertidos em símbolos de uma dada constelação cuja forma é definida pelos coeficientes complexos g_i e pela configuração de um array de antenas que têm de ser conhecidas pelo recetor. Visto que o recetor autorizado tem conhecimento dos coeficentes g_i e da configuração do array de antenas, é capaz de descodificar os símbolos nos respetivos bits. Ou seja, a segurança está inerente à constelação que é mapeada de forma customizada segundo um ângulo θ para a ligação entre o recetor e emissor. Em relação à configuração do array de antenas é possível introduzir rotações adicionais de fase, o que corresponde a alterar o espaçamento entre as antenas. Estes desvios de fase vão provocar alterações na constelação transmitida, o qual introduz segurança visto o recetor ter que saber essas mesmas rotações de fase para obter a constelação correta.

Na receção assumimos que temos conhecimento dos coeficientes g_i e da configuração das antenas. É utilizada uma estrutura semelhante ao transmissor, com M antenas em paralelo, seguidas por um recetor IB-DFE, implementado no domínio da frequência que consegue lidar com a alta sensibilidade na interferência inter-simbólica das constelações utilizadas[14]. O IB-DFE é uma forma iterativa de um Decision Feedback Equalization (DFE) para Single Carrier - Frequency Domain Equalization (SC-FDE) que utiliza filtros feedback e feedforward implementados no domínio da frequência. As amostras obtidas na saída do IB-DFE, no domínio da frequência, são dadas por

$$S_k^{(t)} = F_k^{(t)} Y_k - B_k^{(t)} S_k^{(t-1)}, \tag{3.5}$$

onde $\left\{F_k^{(t)}; k = 0, 1, ...N-1\right\}$ e $\left\{B_k^{(t)}; k = 0, 1, ...N-1\right\}$ representam os coeficientes feed-forward e feedback, respetivamente e $\left\{S_k^{(t-1)}; k = 0, 1, ...N-1\right\}$ a representar uma transformada de fourier direta do sinal amostrado. Pode ser demonstrado que os coeficientes ótimos F_k e B_k podem ser dados por [16, 18]

$$F_k = \frac{\kappa H_k^*}{E[|N_k|^2]/E[|S_k|^2] + (1-\rho^2)|H_k|^2}, \tag{3.6}$$

e

$$B_k = F_k H_k - 1, \tag{3.7}$$

com N_k a representar o ruído do canal , ρ o coeficiente de correlação e com o κ escolhido para garantir

$$\sum_{k=0}^{N-1} F_k H_k / N = 1. \tag{3.8}$$

O esquema do recetor utilizado é apresentado na figura 3.2.

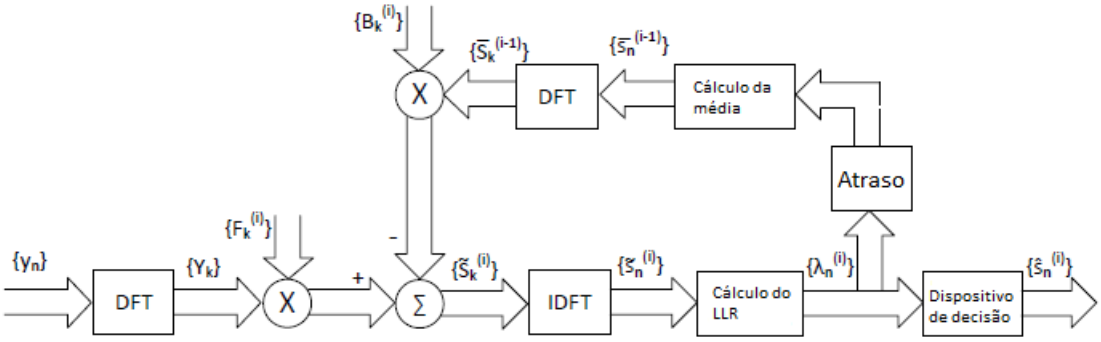

Figura 3.2: Receptor iterativo IB-FDE

Neste trabalho foram estudadas diferentes configurações para a estrutura do transmissor, nomeadamente um transmissor com um array de antenas de espaçamentos uniformes, arrays de antenas de espaçamento não-uniforme e os efeitos de permutações das componentes BPSK nos ramos do transmissor. No caso de haver espaçamento não-uniforme realizou-se o estudo para espaçamentos que correspondem a um múltiplo inteiro de d e admite-se que $d = \lambda/4$. Os arrays não-uniformes podem ainda pode ser obtidos com espaçamentos que sejam múltiplos reais de d, o que aumenta as possibilidades de configuração.

3.3 Análise da configuração com array de antenas de distância uniforme

Numa primeira abordagem, adotou-se um array de antenas em que estas estão equi-espaçadas de um múltiplo inteiro de $d/\lambda = 1/4$ (ver figura 3.3).

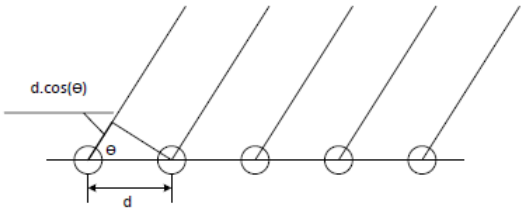

Figura 3.3: vector de antenas com distância uniforme d

Para este espaçamento foram analisadas os casos com constelação 16QAM e 64QAM.

Primeiramente, calcularam-se as informações mútuas em função da relação sínal ruído para analisar o impacto de um erro na estimação do ângulo θ segundo o qual a constelação transmitida se encontra otimizada. Simulou-se então o sistema mais simples, com um espaçamento uniforme entre as antenas e sem rotações de fase adicionais introduzidas pelos amplificadores. A constelação está otimizada para um ângulo θ. Os erros de estimação do θ podem ser $\Delta\theta = 0^o, 1^o, 2^o, 4^o$ e 6^o, tanto para constelações 16QAM como para constelações 64QAM. Os resultados obtidos são os apresentados na figura 3.4 para o caso da constelação 16QAM e na figura 3.5 para o caso da constelação 64QAM. Como se pode ver até um erro de 2^o, o recetor continua a ser capaz de receber quase a totalidade dos bits. Com um desvio superior a 2 graus a informação mútua decresce para cerca de 0.75 do seu valor máximo o que impossibilita a receção com sucesso dos 4 bits enviados. É conveniente relembrar que caso "Eva"não tenha qualquer informação acerca da configuração do transmissor a informação mútua é sempre nula, ou seja é incapaz de extrair qualquer informação útil. No caso da constelação 64QAM o impacto na informação mútua dos erros de estimação do ângulo θ ainda é mais acentuado. Podemos concluir, em ambos os casos, que para valores do erro superiores a quatro graus a receção dos dados transmitidos não pode ser feita com sucesso pois os valores da informação mútua situam-se abaixo de 50% do valor máximo no caso da constelação 64QAM e 75% do valor máximo no caso da constelação 16QAM. Esta elevada sensibilidade da informação mútua face aos erros de estimação do ângulo θ, implica uma complexidade acrescida para um recetor como a "Eva"na medida em que a margem de erro para um algoritmo de intersecção é muito reduzida. Por outro lado, quando se considera o recetor autorizado verifica-se que este deverá ser capaz de estimar com exactidão os valores dos ângulos segundo as quais as constelações transmitidas estão otimizadas (no capítulo 4 ver-se-á que com base no conhecimento de alguns parâmetros de configuração do transmissor e uso de pilotos é possível estimar com muita exactidão

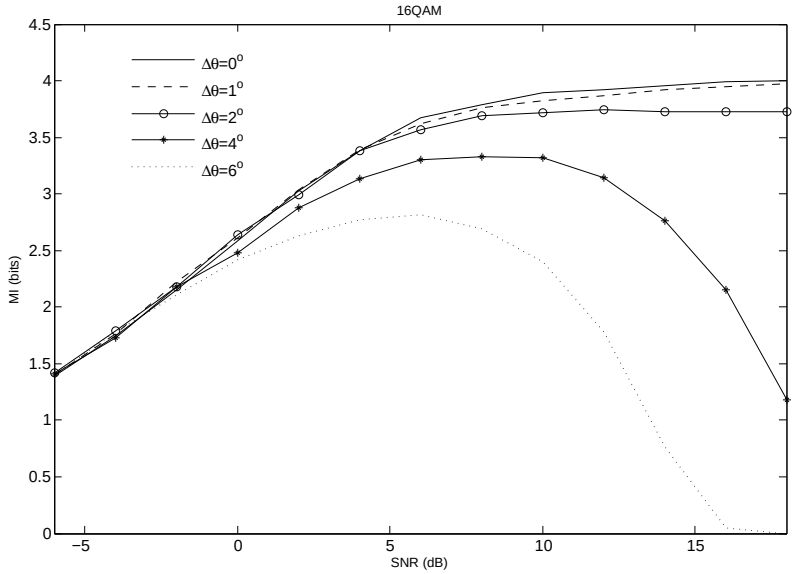

Figura 3.4: Impacto do erro de estimação de θ na Informação mútua para arrays uniformes sem antenas fantasmas para ângulos otimizados com uma constelação 16QAM

os valores de θ e evitar degradações a nível do desempenho do sistema).

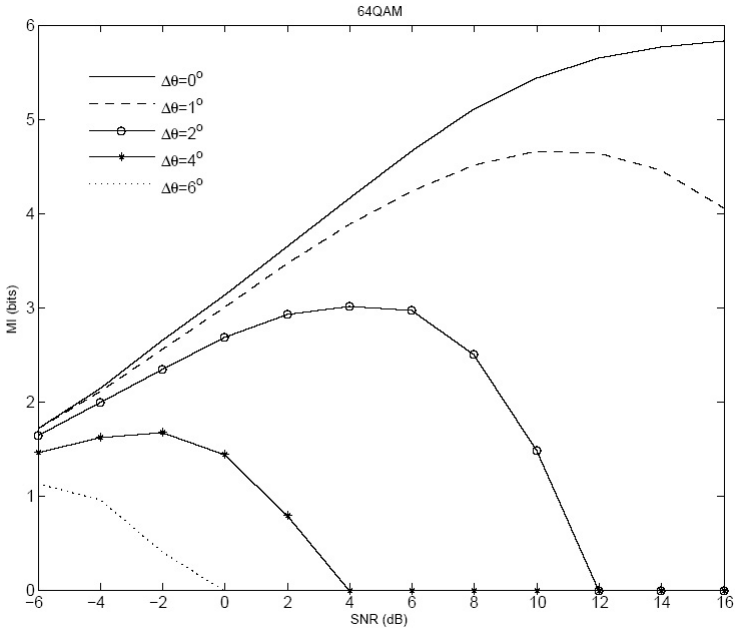

Figura 3.5: Impacto do erro de estimação de θ na Informação mútua para arrays uniformes sem antenas fantasmas para ângulos otimizados com uma constelação 64QAM

3.3.1 Evolução da informação mútua em função do ângulo de otimização

3.3.1.1 Sem rotações de fase adicionais

Mantendo o array de antenas sem rotações adicionais de fase e com uma distância uniforme entre elas, mapeou-se a informação mútua para todos os ângulos de otimização θ da constelação com incrementos de um grau (nota: nos resultados da informação mútua apresentados ao longo deste capítulo admitem-se SNRs de 14 dB e 18 dB para para a constelação 16QAM e 64QAM, respectivamente). Os gráficos obtidos para as constelações 16QAM e 64QAM são apresentados na figura 3.6.

Em ambos os casos, verifica-se que a informação mútua mantém-se praticamente constante ao longo da gama de valores de θ. Em ambos os casos existem ligeiras flutuações em torno do valor máximo para um número reduzido de ângulos, que obviamente devem ser evitados. No caso da constelação 16QAM temos os valores de 60^o, 120^o, 240^o e 300^o. No caso da constelação 64QAM os valores são 0^o e 180^o. Existem também zonas de decréscimo da informação mútua nos 0^o e nos 180^o graus, apesar de serem menos significativas. Estas variações podem ser usadas para incrementar a segurança do sistema, uma vez que a otimização das constelações transmitidas para ângulos na vizinhança dos valores referidos anteriormente, aumenta o impacto de qualquer erro de estimação de uma "Eva", já que pode conduzir aos ângulos onde se verificam os mínimos da informação mútua (logo existe um reforço da degradação da MI).

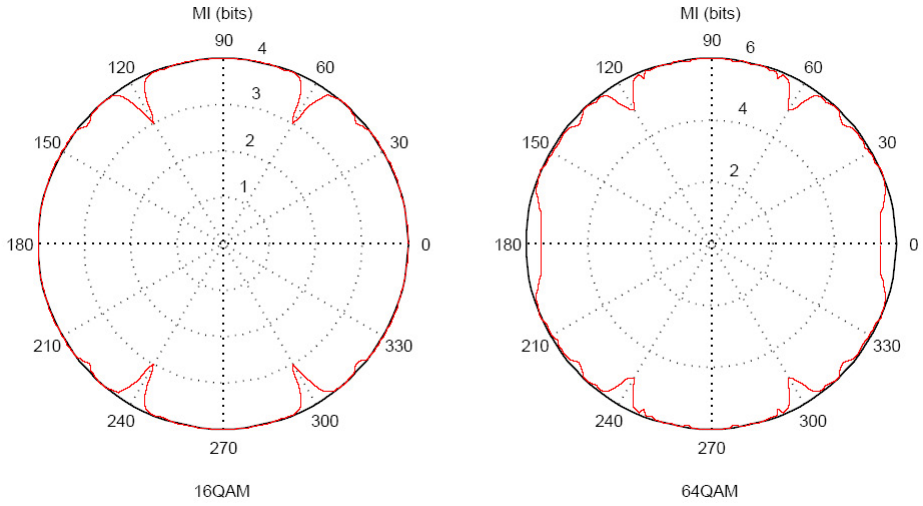

Figura 3.6: Informação mútua com array de antenas de espaçamento uniforme sem rotações adicionais de fase.

3.3.1.2 Rotações de fase adicionais

Os desvios de fase adicionais entre ramos de amplificação, podem ser comparados ao efeito de antenas fantasmas num array de antenas. Quer seja um array uniforme quer seja um array não uniforme, a inclusão de rotações de fase adicionais e proporcionais a $\frac{d}{\lambda} = \frac{1}{4}$ é equivalente à contribuição de uma antena fantasma entre duas antenas ativas (note-se que estas rotações de fase não implicam um re-arranjo das distâncias entre as antenas). Ao longo do texto vai-se usar o termo de antenas fantasma com o intuito de descrever configurações em que se consideram desvios de fase adicionais entre os ramos do array de antenas. Estes desvios adicionais de fase provocam alterações no mapeamento da constelação de transmissão, o que origina um grau de liberdade extra, pois é necessário saber perfeitamente os desvios de fase para um recetor conseguir obter a informação.

Com o arranjo entre as antenas a manter-se uniforme, testou-se o sistema com rotações de face adicionais correspondentes ao efeito de um espaçamento adicional de 1d a 4d, isto é, à contribuição de uma a quatro antenas fantasma. Para cada um dos casos a disposição das antenas ativas é apresentada na tabela 3.3.

Tabela 3.3: Representação do espaçamento entre as antenas provocado pelas antenas fantasma na constelação 16QAM, com $\frac{d}{\lambda} = \frac{1}{4}$

Número de antenas fantasma	1	2	3	4
Antenas	Disposição das antenas ativas face a antena 1			
1	-	-	-	-
2	3d	4d	5d	6d
3	5d	7d	9d	11d
4	7d	10d	13d	16d

É visível uma maior dependência da informação mútua face ao ângulo de otimização θ. Na figura 3.7 é apresentado o gráfico com a evolução da informação mútua em função do ângulo de otimização, com uma antena e duas antenas fantasma entre as antenas activas, encontra-se na figura 3.7. O caso A representa a situação com uma rotação de fase correspondente á contribuição de uma antena fantasma e o caso B representa a situação com uma rotação de fase correspondente à contribuição de duas antenas fantasma.

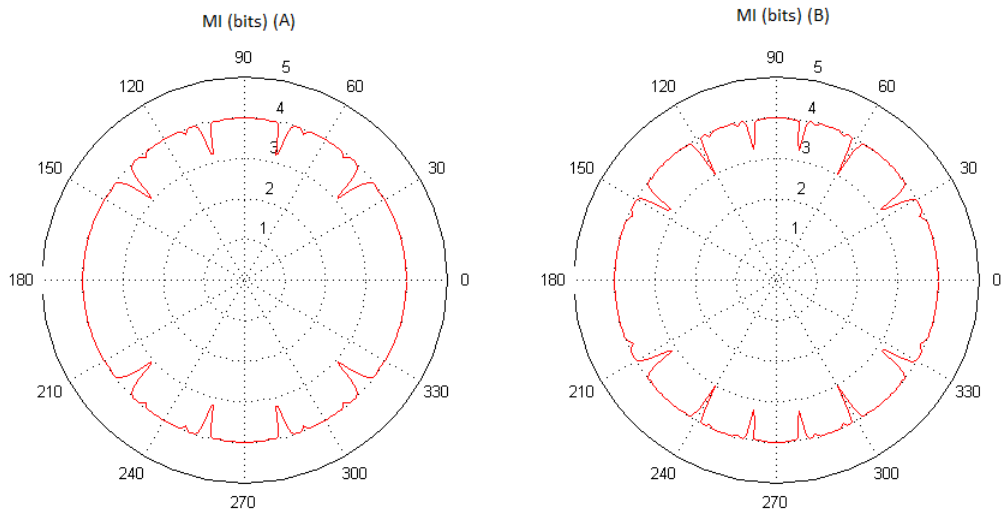

Figura 3.7: Informação mútua com 1 e 2 antenas fantasmas em função do ângulo de otimização θ, para uma constelação 16 QAM

Em ambos os casos, com a introdução de rotações adicionais de fase, a informação mútua é mais sensível ao valor do ângulo θ segundo o qual a constelação está otimizada. Isto pode ser usado para aumentar a segurança, uma vez que se a constelação transmitida estiver otimizada para um valor de θ, o efeito do erro de estimação do θ na informação mútua será mais acentuado.

Para rotações de fase adicionais correspondentes à contribuição de três e quatro antenas fantasma os resultados obtidos são os apresentados na figura 3.8. O caso A representa o sistema com 3 antenas fantasmas entre as antenas ativas e o caso B representa o sistema com 4 antenas fantasma entre as antenas ativas.

Para o caso do 64QAM as rotações de fase adicionais consideram os efeitos equivalentes à introdução de uma antena fantasma até oito antenas fantasma. Notar que a distância entre antenas mantem-se igual logo o array continua uniforme. Para cada um dos casos a

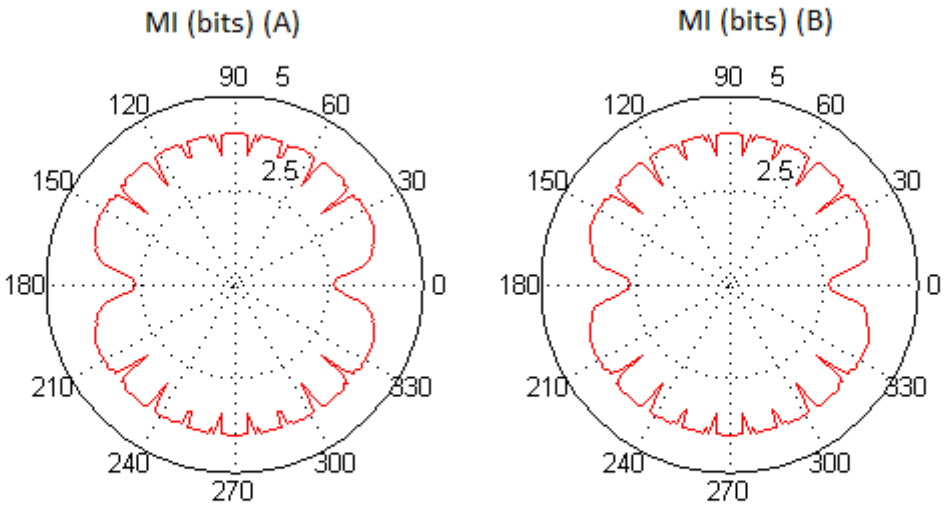

Figura 3.8: Evolução da informação mútua com o ângulo de otimização θ para arrays uniformes com 3 e 4 antenas fantasmas, para uma constelação 16 QAM

disposição das antenas ativas é apresentada na tabela 3.4.

Tabela 3.4: Representação do espaçamento entre as antenas provocado pelas antenas fantasmas, com $\frac{d}{\lambda} = \frac{1}{4}$ (64QAM)

Número de antenas fantasma	1	2	3	4	5	6	7	8
Antenas	Disposição das antenas ativas face a antena 1							
1	-	-	-	-	-	-	-	-
2	3d	4d	5d	6d	7d	8d	9d	10d
3	5d	7d	9d	11d	13d	15d	17d	19d
4	7d	10d	13d	16d	19d	22d	25d	28d
5	9d	13d	17d	21d	25d	29d	33d	37d
6	11d	16d	21d	26d	31d	36d	41d	46d

Os gráficos obtidos para os diversos casos são apresentados nas figuras 3.9, 3.10, 3.11 e 3.12. Nos gráficos apresentados é notório o aumento da sensibilidade da informação mútua face a θ à medida que o número de antenas fantasma aumenta. Este aumento da sensibilidade da informação mútua é visível quer para a constelação 64QAM quer para a 16QAM. Este efeito pode provocar problemas na receção se o recetor não souber perfeitamente qual o ângulo θ para qual constelação esta otimizada.

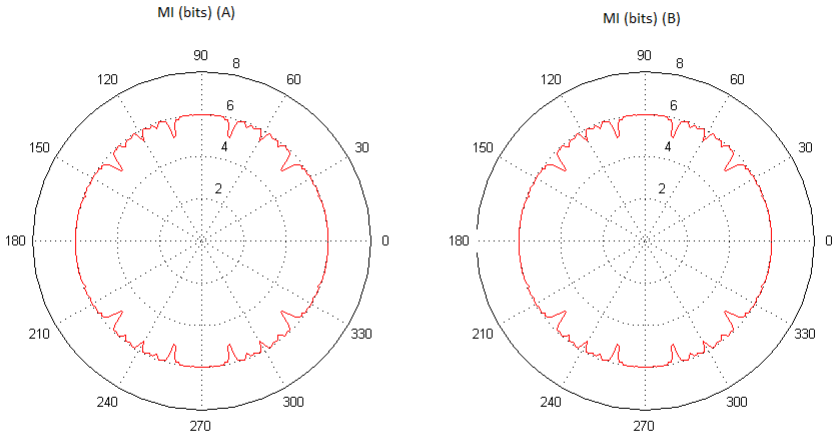

Figura 3.9: Evolução da informação mútua com o ângulo de otimização θ para arrays uniformes com 1 e 2 antenas fantasma para constelações 64QAM. (A-1 antena fantasma B-2 antenas fantasmas)

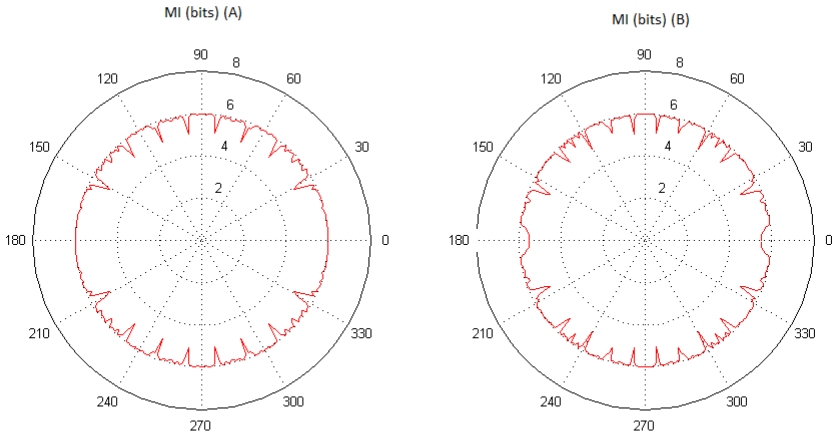

Figura 3.10: Evolução da informação mútua com o ângulo de otimização θ para arrays uniformes com 3 e 4 antenas fantasmas para constelações 64QAM. (A-3 antenas fantasmas B-4 antenas fantasmas)

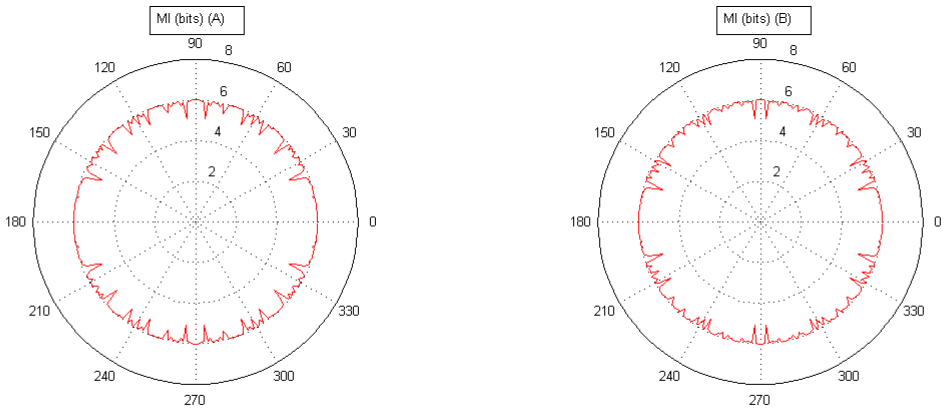

Figura 3.11: Evolução da informação mútua com ângulo de otimização θ para arrays uniformes com 5 e 6 antenas fantasmas para constelações 64QAM. (A-5 antenas fantasmas B-6 antenas fantasmas)

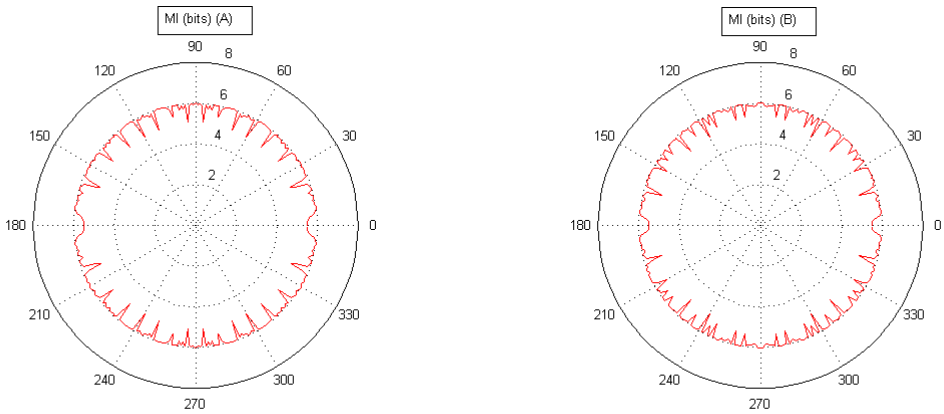

Figura 3.12: Evolução da informação mútua com ângulo de otimização θ para arrays uniformes com 7 e 8 antenas fantasmas para constelações 64QAM. (A-7 antenas fantasmas B-8 antenas fantasmas)

3.3.2 BER's com otimização da constelação

A primeira análise efetuada incidiu sobre o desempenho de um sistema baseado num transmissor com a constelação otimizada para um determinado ângulo, conhecido pelo recetor, e depois desviou-se o ângulo de otimização de forma a que o erro do recetor na estimação de θ seja 1ª, 2º, 3º e 4º. Análisamos as constelações 16QAM e 64QAM, otimizadas a 58º e 120º, dada a maior sensibilidade da informação mútua na vizinhança destes ângulos de otimização. O gráfico obtido para a constelação 16QAM é apresentado na figura 3.13. O gráfico da BER para a constelação 64QAM é apresentado na figura 3.14.

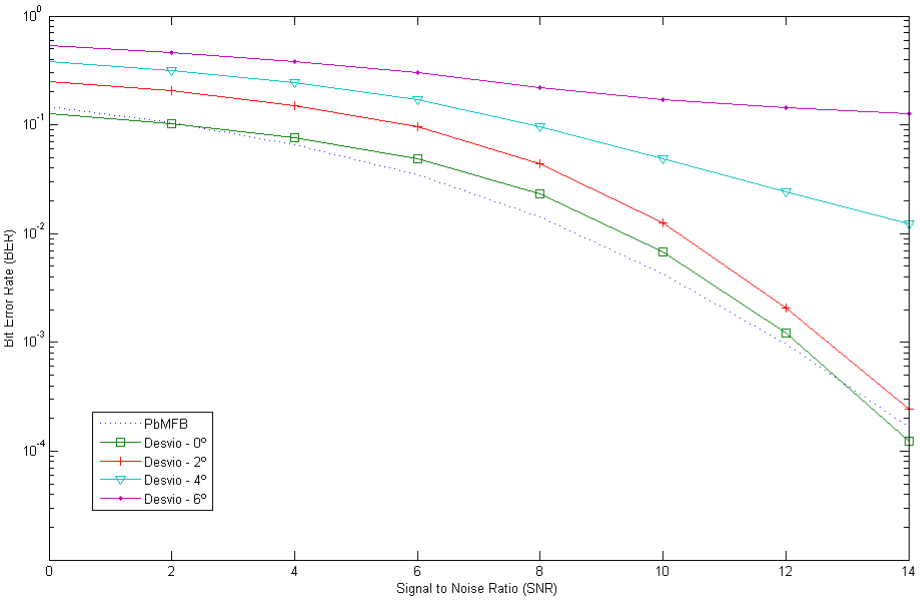

Figura 3.13: BER com array de antenas de espaçamento uniforme (16QAM).

Em ambos os gráficos os sistemas têm um comportamento robusto em termos de desempenho. No caso da constelação 64QAM a taxa de erro de bit aumenta de forma abrupta a partir de um erro de estimação de θ superior a 2º. A constelação 64QAM é consideravelmente mais sensível a erros de estimação do ângulo otimizado do que a constelação 16QAM.

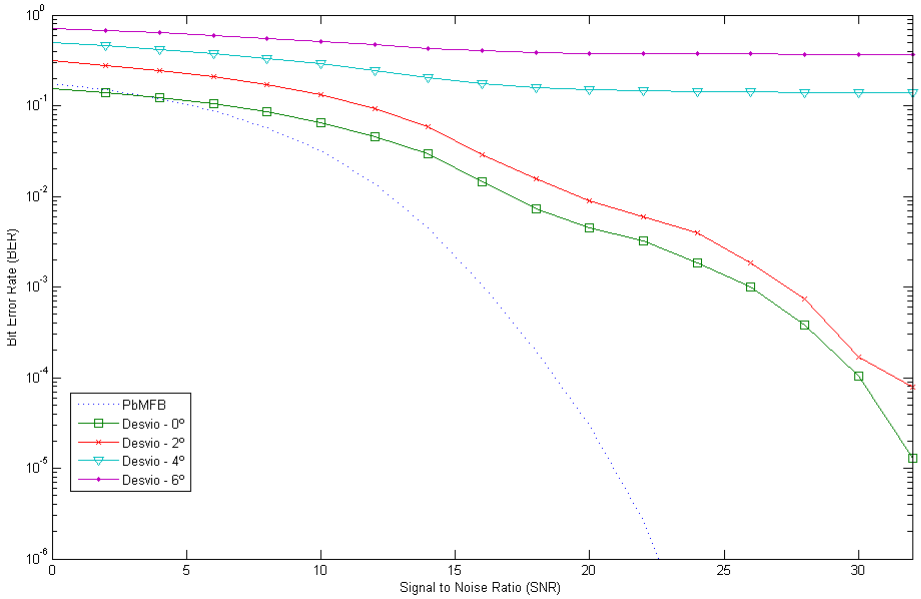

Figura 3.14: BER com array de antenas de espaçamento uniforme (64QAM).

3.4 Análise da configuração com array de antenas de espaçamento não-uniforme

Outra alteração da configuração do transmissor reside na alteração dos espaçamentos entre antenas, de maneira a que as distâncias $d_1, d_2, ..., dn$ entre as mesmas sejam diferentes. Até esta fase, foram apenas realizados testes com distâncias uniformes de antenas. É preciso também saber como os sistemas se comportam se forem introduzidos arrays de distâncias não uniformes. Ora para o caso de termos arrays de distâncias não uniformes, o número de combinações possíveis é enorme, pelo que excluiu-se a possibilidade de introdução de espaçamentos não uniformes que não sejam múltiplos de $\frac{\lambda}{4}$. Consequentemete, o número de combinações possíveis para 16QAM ficou limitado a 4^4, e para 64QAM o número de combinações é 6^6.

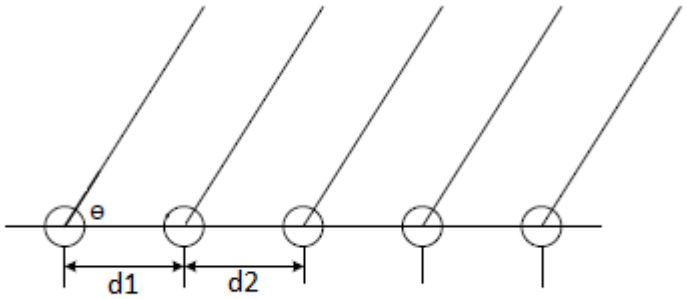

Figura 3.15: array de antenas com distâncias não-uniformes.

Isto altera as rotações de fase entre os componentes e aumenta o *shaping* da constelação na direção desejada. Como tal, será de esperar uma maior diretividade da informação e consequentemente maior dificuldade por parte de um intruso para estimar os coeficientes complexos das antenas.

3.4.1 Informação Mútua com arrays de espaçamento não-uniforme

Os resultados apresentados para a constelação 16QAM correspondem aos quatro casos identificados como os que exibem maior diretividade de informação, ou seja, em que a informação mútua é mais sensível face ao ângulo θ. Os espaçamentos das antenas para cada um dos casos são expostos na tabela 3.5.

Tabela 3.5: 16QAM : arranjo dos coeficientes g_i das antenas e do espaçamento entre as mesmas

16QAM	Ordem das antenas			
	1	2	3	4
Coeficientes gi	2j	1	2	j
Espaçamentos em relação à antena 1		4d	6d	8d
		4d	6d	9d

Os gráficos da evolução da informação mútua em função do ângulo de otimização da constelação θ, são apresentados na figura 3.16. O caso A representa o transmissor com os espaçamentos das antenas em relação à primeira de 4d, 6d e 8d e o caso B um espaçamento de 4d, 6d e 9d.

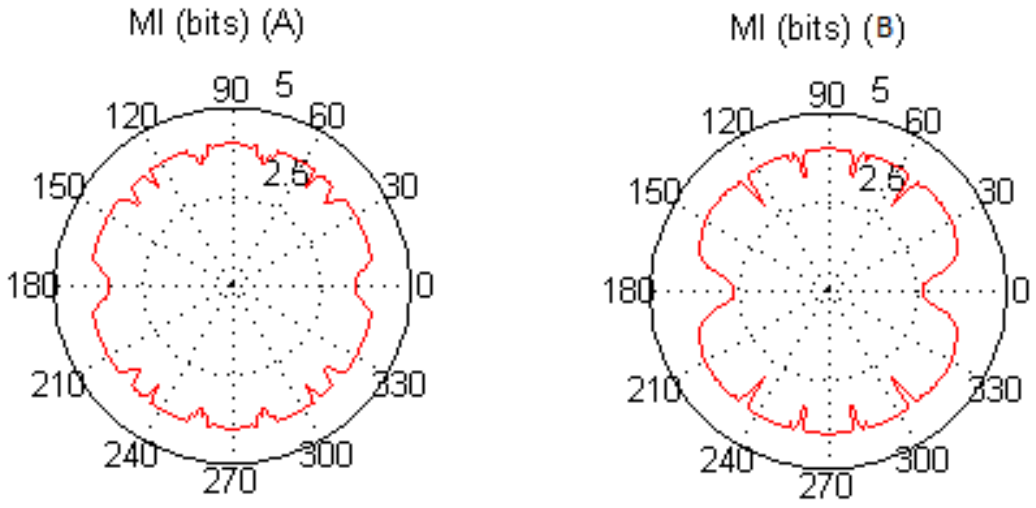

Figura 3.16: Informação mútua com array de antenas de espaçamento não-uniforme.

Escolheram-se ainda outros dois casos apresentados na tabela 3.6.

Tabela 3.6: 16QAM : arranjo dos coeficientes gi das antenas e do espaçamento entre as mesmas

16QAM	Ordem das antenas			
	1	2	3	4
Coeficientes gi	2j	1	2	j
Espaçamentos em relação à antena 1		4d	8d	10d
		4d	8d	11d

Os gráficos associados são apresentados na figura 3.17, com o caso A a representar um transmissor com os espaçamentos das antenas em relação à primeira antena de 4d, 8d e 10d e o caso B espaçamentos de 4d, 8d e 11d.

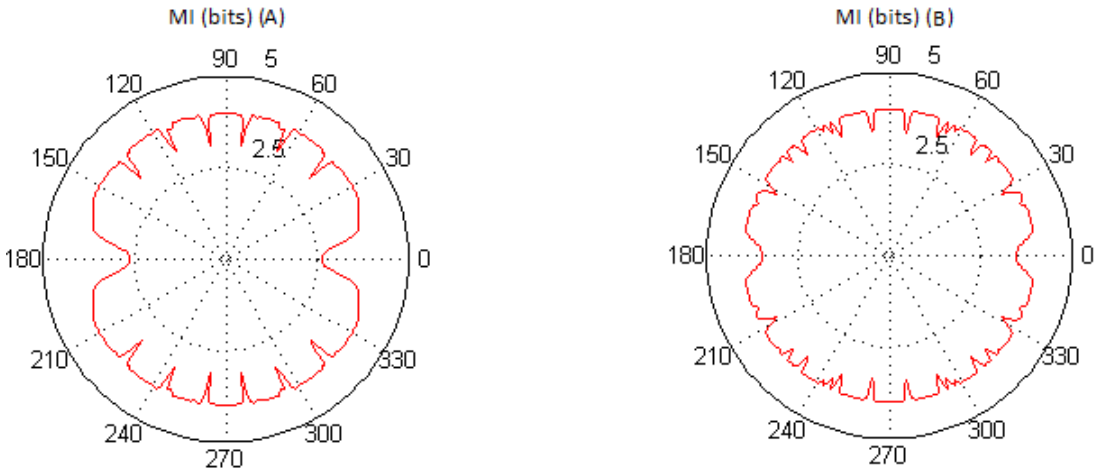

Figura 3.17: Informação mútua com array de antenas de espaçamento não-uniforme.

No caso do sistema com constelações 64QAM também foram escolhidos quatro casos que exibem maior diretividade e dependência face ao ângulo θ. Os espaçamentos entre as antenas são os que constam da tabela 3.7.

Tabela 3.7: 64QAM: arranjos dos coeficientes das antenas e do espaçamento entre as mesmas

64QAM	Casos	Ordem das antenas					
		1	2	3	4	5	6
Coeficientes gi		2j	1	2	j	4	4j
Espaçamentos em relação à antena 1	A	1d	6d	9d	18d	25d	27d
	B	1d	6d	9d	18d	20d	27d
	C	1d	6d	9d	16d	25d	27d
	D	1d	6d	9d	16d	18d	27d

Na figura 3.18 são apresentadas as dependências da informação mútua com o ângulo θ para os 4 casos considerados. Os casos A, B, C e D representam os casos com os

espaçamentos apresentados na tabela 3.7.

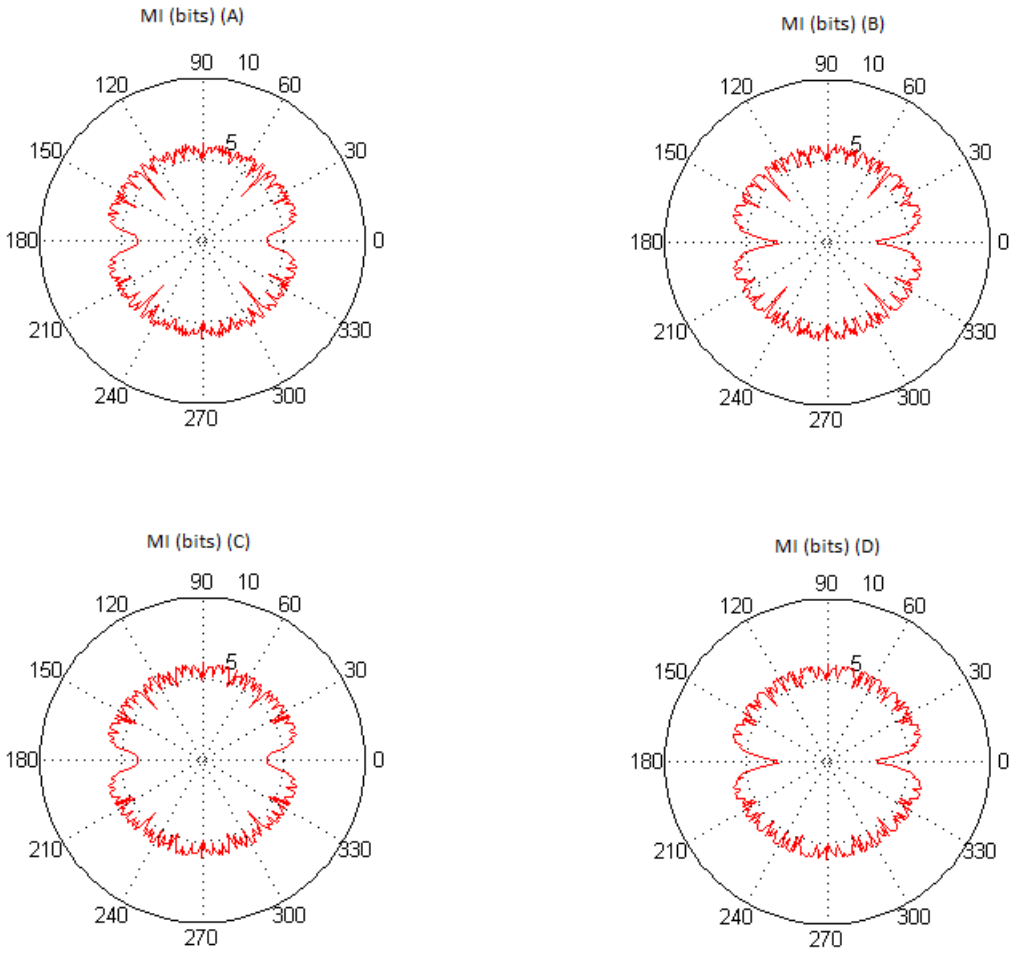

Figura 3.18: Evolução da informação mútua com o ângulo otimizado θ para arrays de antenas não uniformes (64QAM)

Nos gráficos da figura 3.18, são perfeitamente notórias as variações bruscas de informação mútua ao longo da gama de valores de θ. Consequentemente, obtém-se um sistema em que a informação mútua tem uma sensibilidade acrescida face a erros na estimação dos coeficientes complexos g_i das antenas. Importa ainda referir que esta sensibilidade acrescida da informação mútua com o ângulo θ, pode ser usada para aumentar a segurança, já que a transmissão pode ser otimizada para valores próximos de ângulos que estejam associados a mínimos e assim minimizar a tolerância face a erros de estimação por parte do recetor não autorizado. Embora muito vantajoso em termos de segurança, isto implica que o recetor autorizado conheça perfeitamente a configuração do emissor, isto é, os coeficientes g_i e a configuração do array de antenas (com tal um recetor autorizado deverá ser capaz de estimar com exatidão o ângulo θ e eventuais flutuações em torno deste devido a desequilíbrios de fase e ganho entre amplificadores). Como seria de esperar, a constelação 64 QAM apresenta maior sensibilidade a variações do ângulo segundo o qual

a constelação está otimizada.

3.4.2 Análise das BER para arrays de antenas de espaçamento não uniforme

Foi necessário recalcular as BER para os arrays não uniformes, para ver como é que o sistema reagia em termos de desempenho, visto os gráficos de informação mútua mostrarem uma grande sensibilidade às alterações dos coeficientes g_i. Para a constelação 16QAM o espaçamento utilizado foi o usado no caso B apresentado na figura 3.17. Para a constelação 64QAM foi o usado no caso B apresentado na figura 3.18. Como é visível nos gráficos da evolução da informação mútua em função do ângulo de otimização, algumas otimizações são boas mas têm declínios de informação mútua abruptos, o que torna os sistemas robustos em termos de segurança pois pequenas alterações no ângulo de otimização assumido por um recetor provoca grandes perdas da informação mútua. Testou-se então o desempenho para essas otimizações, onde os declínios eram mais acentuados. Para a constelação 16QAM calculou-se as BER para otimizações nos 30^o e nos 120^o. Para a constelação 64QAM calculou-se com otimização nos 50^o. Os gráficos das BER's obtidas para a constelação 16QAM, são apresentados na figura 3.19 e na figura 3.20, respectivamente.

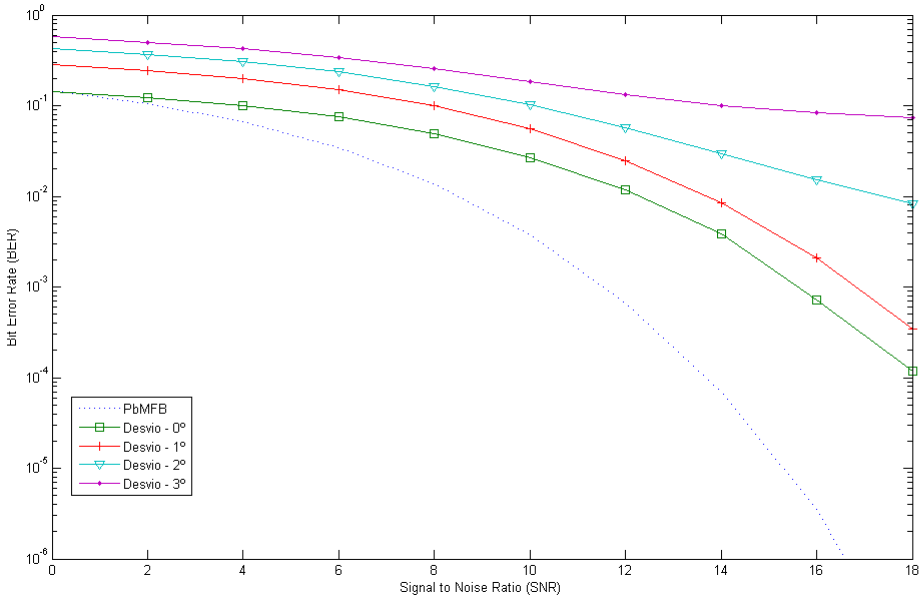

Figura 3.19: BER para um transmissor com um array de antenas de espaçamento não-uniforme com a constelação transmitida optimizada para o ângulo $\theta = 120^o$

Para o caso é que o ângulo de otimização é 120^o, mesmo quando o recetor sabe o ângulo de otimização, o sistema não apresenta bons desempenhos. Isto deve-se à grande sensibilidade do desempenho do sistema devido à introdução de espaçamentos não-uniformes. Se o recetor não souber perfeitamente os coeficientes complexos g_i das antenas,

a taxa de erros é elevada.

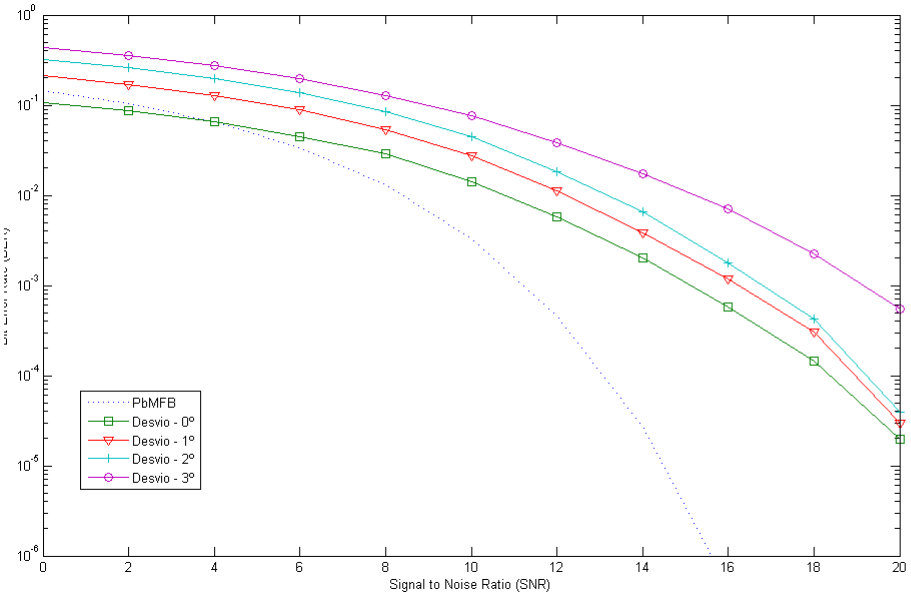

Figura 3.20: BER com a constelação otimizada a 30º num sistema com espaçamento não-uniforme.

O caso da constelação 64QAM otimizado em 50º é apresentado na figura 3.21. De forma semelhante à situação verificada para a constelação 16QAM, na presença de desvios do ângulo de otimização superiores a dois graus, o recetor não consegue extrair com sucesso a informação enviada, o que acarreta vantagens a nível de segurança. É de referir que para todos os casos considerados, a grande sensibilidade do sistema a variações dos coeficientes e arranjos das antenas acarreta um problema para o desempenho do sistema, quando devido a imperfeições na calibragem dos amplificadores do transmissor existe um desvio no valor do ângulo θ que é desconhecido à priori pelo recetor autorizado, sendo necessário tomar medidas para mitigar o problema.

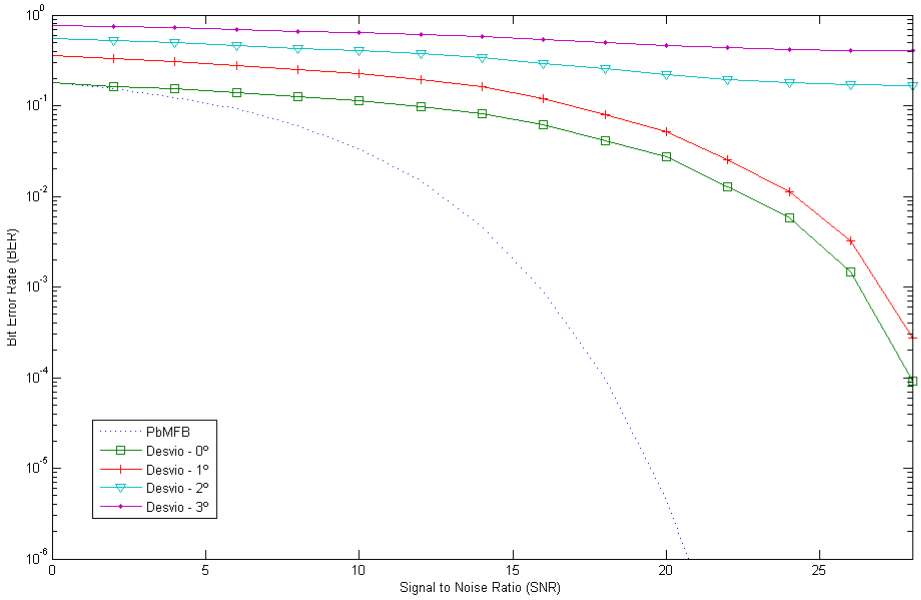

Figura 3.21: BER com constelação otimizada a 50 graus para array de antenas de espaçamento não uniforme.

CAPÍTULO 4

PROBLEMÁTICA DO ERRO NA ESTIMATIVA DE θ

Um dos problemas verificados nos resultados das BER obtidos no capítulo anterior, consiste na elevada sensibilidade a erros de estimação dos coeficientes das antenas, principalmente na presença de arrays de antenas de espaçamento não uniforme (embora menor o mesmo problema coloca-se para os transmissores baseados em arrays uniformes). Isto implica que o recetor saiba perfeitamente quais são esses coeficientes para que o sistema tenha um bom desempenho.

Variações do canal ou problemas de sincronização dos diversos circuitos de radiofrequência resultam em erros nos coeficientes ou desequilíbrios na fase e no ganho. Uma das maneiras de compensar eventuais efeitos de imperfeições no transmissor que conduzam a desequilíbrios de fase e ganho entre os ramos em paralelo do array, consiste na aplicação de técnicas de estimação dos g_i e do ângulo θ efectivamente usado através do envio de pilotos. Este tipo de técnicas podem ser baseadas em estimadores do tipo Least Square (LS) ou estimadores do tipo Minimum Mean Square Error (MMSE) [23]. Normalmente a estimação do canal é feita com recurso a um envio de um conjunto de símbolos conhecidos pelo recetor, únicos ao transmissor, que são enviados em cada bloco de símbolos transmitidos. Devido ao efeito multi-percurso presente em sistemas MIMO, e devido ao uso de constelações com dimensões grandes, o efeito de ISI é notório no sinal recebido, sendo necessário o conhecimento do Channel impulse Response (CIR) para uma boa equalização no recetor [5]. No entanto, a estimação do canal com base em pilotos está fora do âmbito do presente trabalho, dado que se admite que esta é perfeita, pelo que se restringe a análise ao problema da estimação dos coeficientes g_i, por meio do uso de pilotos. Por conseguinte, é apresentado neste capítulo um método de estimação dos g_i para 16QAM, que pode ser facilmente extendido para outro tipo de constelações como 64QAM ou Voronoi. O desempenho do método de estimação é avaliado através do cálculo das BER para transmissores baseados em arrays uniformes e não uniformes com constelações 16QAM.

4.1 Estimação de *theta* com base em pilotos para uma constelação 16QAM

Para o caso da constelação de 16QAM, com os coeficientes complexos apresentados na tabela (3.2.1), o mapa de símbolos da constelação é o apresentado na figura 4.1. Os valores

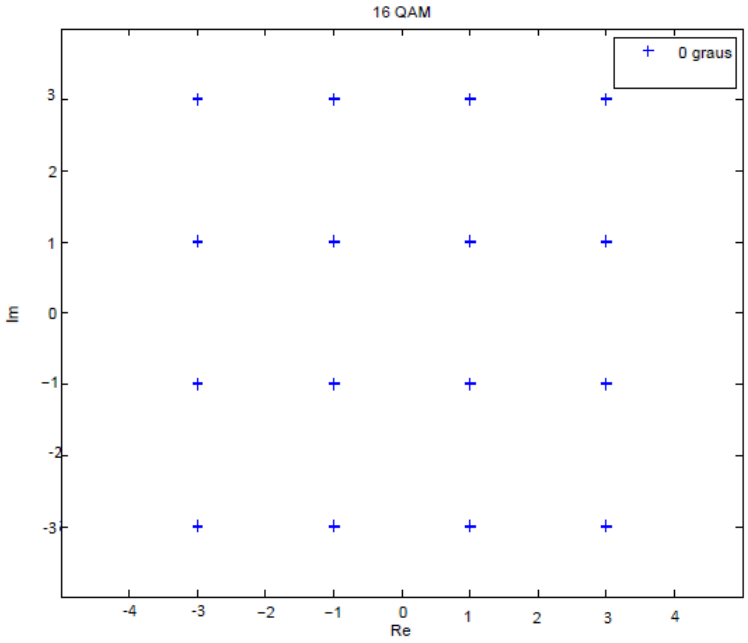

Figura 4.1: Mapa da constelação 16QAM sem rotação

dos pilotos de referência estão apresentados na tabela 4.1.

Tabela 4.1: Valor dos pilotos de referência

16QAM	Antennas				Valor dos pilotos de Referência
Coeficientes gi	2j	1	2	j	
P1	2j+j + 1+2				3j+3
P2	2j+j -1+2				3j +1
P3	2j-j -1+2				j +1
P4	2j-j + 1+2				j +3
P5	2j-j + 1-2				j - 1
P6	-2j+j + 1-2				-j -1
P7	2j+j + 1-2				3j -1
P8	-2j+j + 1+2				-j +3

Para a estimativa da constelação apenas é necessário um conjunto de 5 pilotos, pertencentes à constelação: P1, P2, P4, P7 e P8, desde que este conjunto símbolos englobe todas as componentes g_i usadas na construção dos símbolos da constelação. Convém referir que o sub-conjunto de símbolos usado como pilotos pode ser outro, desde que a totalidade

dos g_i seja usada na sua definição (por exemplo para 64QAM são necessários pelo menos 6 pilotos distintos de forma a abranger todos os g_i).

A estimação é feita recorrendo ao envio de N repetições de cada um dos pilotos. Dado o fato do ruído ser Gaussiano de média nula, o aumento do número N de pilotos considerados para a obtenção do valor médio. contribui para minimizar a constribuição residual do ruído no resultado final da média. No caso de um canal com desvanecimento, admite-se que este é invariante durante as N repetições dos pilotos enviados. Após a sua receção, o recetor calcula a média da distância entre os pilotos recebidos $p^r_{k,i}$ e $p^r_{p,i}$, através de:

$$\delta_{k,p} = \frac{\sum_{i=0}^{N} p^r_{k,i} - \sum_{r=0}^{N} p^r_{p,i}}{N} \tag{4.1}$$

onde N é o número de repetições de cada um dos pilotos e $k = 1$ e $p = 2, 4, 7, 8$. Para os quatro casos, na ausência de ruído, obtem-se equação (4.2).

$$\begin{aligned}
\delta_{12} &= \frac{\sum_{i=0}^{N} p_{(1,i)} - \sum_{i=0}^{N} p_{(i,2)}}{256} = 2 = 2g_2^{ref}, \\
\delta_{14} &= \frac{\sum_{i=0}^{N} p_{(1,i)} - \sum_{i=0}^{N} p_{(i,4)}}{256} = 2j = 2g_3^{ref}, \\
\delta_{17} &= \frac{\sum_{i=0}^{N} p_{(1,i)} - \sum_{i=0}^{N} p_{(i,7)}}{256} = 4 = 2g_4^{ref}, \\
\delta_{18} &= \frac{\sum_{i=0}^{N} p_{(1,i)} - \sum_{i=0}^{N} p_{(i,8)}}{256} = 4j = 2g_1^{ref},
\end{aligned} \tag{4.2}$$

onde os g_i^{ref}, com $i = 1, 2, 3, 4$, são os valores dos coeficientes de referência. Na presença de ruído obtem-se

$$\begin{aligned}
\delta_{12} &= 2 + \varepsilon_{1,2} = 2g_2 = 2g_2^{ref} e^{j\Delta\theta_2}, \\
\delta_{14} &= 2j + \varepsilon_{1,4} = 2g_4 = 2g_4^{ref} e^{j\Delta\theta_4}, \\
\delta_{17} &= 4 + \varepsilon_{1,7} = 2g_3 = 2g_3^{ref} e^{j\Delta\theta_3}, \\
\delta_{18} &= 4j + \varepsilon_{1,8} = 2g_1 = 2g_1^{ref} e^{j\Delta\theta_1},
\end{aligned} \tag{4.3}$$

onde $\varepsilon_{k,p}$ são os termos residuais de ruído resultantes da média e $g_i = g_i^{ref} e^{j\Delta\theta_i}$ são os coeficientes recebidos em que $e^{j\Delta\theta_i}$ representa o um termo complexo multiplicativo devido a uma diferença de fase face ao coeficiente de referência, devido a uma configuração do transmissor diferente da original que está associada aos coeficientes de referência. Por conseguinte os coeficientes obtidos relacionam-se com os de referência, à parte de um termo residual de ruído $\varepsilon_{k,p}$, através de $g_i = g_i^{ref} e^{j\Delta\theta_i}$, pelo que é válido escrever:

$$z_{\theta_i} = e^{j\Delta\theta_i} = \frac{\sum_{i=0}^{N} p^r_{k,i} - \sum_{r=0}^{N} p^r_{p,i}}{2.N.g_i^{ref}} = \frac{\delta_{k,p}}{2.N.g_i^{ref}}, \tag{4.4}$$

em que $i = 2$ para $k = 1$ e $p = 2$, $i = 4$ para $k = 1$ e $p = 4$, $i = 3$ para $k = 1$ e $p = 7$ e $i = 4$ para $k = 1$ e $p = 8$. Note-se que no caso das constelações serem otimizadas para um determinado ângulo, a constelação deixa de ser representada pela constelação da figura 4.1, e os coeficientes das antenas g_{iref} são multiplicados por uma rotação de fase $\Delta\theta$.

De seguida, calculam-se as rotações de fase relacionadas com os valores obtidos no cálculo anterior, através de

$$\Delta\theta = \arctan\left(\frac{real(z_{\theta_i})}{imag(z_{\theta_i})}\right). \tag{4.5}$$

Com base nestas rotações de fase, consegue-se obter as estimativas $\hat{g}_i$ dos coeficientes complexos g_i por meio da relação

$$\hat{g}_i = g_i^{ref} e^{j\Delta\theta_i}. \tag{4.6}$$

Uma vez estimados os coeficientes, os pilotos estimados (isto é, compensados ou não das rotações de fase que afectam os g_i) são obtidos através do produto da matriz de Hadamard pelos coeficientes estimados

$$P_e = \boldsymbol{H} \cdot \hat{g}_i. \tag{4.7}$$

O valor N adotado é definido de acordo com um valor de limiar a partir do qual o termo residual associado ao ruído é desprezado. No nosso caso os valores de limiar $\boldsymbol{\kappa} = [k_1, k_2, k_3, k_4]$ definidos foram um centésimo do valor do coeficiente complexo g_i.

$$\boldsymbol{\kappa} \leq \frac{|\boldsymbol{g_i}|^2}{F}, \tag{4.8}$$

com $\boldsymbol{g} = [g_1, g_2, g_3, g_4]$ a representar os coeficientes que afectam cada um dos ramos rádio frequência do transmissor e F é um factor de atenuação. No contexto das simulações efetuadas neste capítulo, adoptou-se um valor de $f = 100$ o que corresponde a um termo residual de ruído 20 dB abaixo da energia de cada um ds componentes BPSK (obviamente que o valor de f pode ser maior ou menor consoante o desempenho máximo que se pretenda para o sistema de forma a evitar um efeito de "floor"devido ao ruído residual). Consequentemente, na transmissão dos pilotos existe uma fase de aprendizagem, uma vez que enquanto o valor do limiar estabelecido para todos os coeficientes não for atingido o processo de envio de pilotos repete-se com um número N de pilotos cada vez maior. O processo de estimação é executado outra vez até a condição expressa por (4.8) se verificar.

4.2 Correcção de rotações de fase

Com o cálculo dos coeficientes complexos $\hat{g}_i$ estimados e os pilotos estimados, consegue-se mapear uma nova constelação. Quando o valor de limiar é atingido, é calculada uma matriz $\boldsymbol{Z_{16*16}}$ onde são guardados todos os valores de distância entre um piloto estimado e todos os símbolos da constelação (original ou rodada consoante se compense ou não as rotações de fase dos coeficientes $\hat{g}_i$).

$$\boldsymbol{Z_i} = P_e - P_r, \tag{4.9}$$

com P_r a representar o vector dos pilotos recebidos (a média de cada um dos pilotos recebidos) e P_e o vector dos pilotos estimados. Das 16 amostras de distâncias por símbolo,

é escolhida a que têm menor distância é que é guardada o símbolo correspondente, construindo assim a nova constelação estimada $\psi^{'}$.

$$\psi_i^{'} = \min |\boldsymbol{Z}_i| \,. \tag{4.10}$$

4.3 Análise dos resultados

O cálculo das BER realizou-se para a constelação 16QAM. Numa primeira fase, os testes foram feitos para um array de antenas de espaçamento uniforme. Posteriormente, as simulações foram feitas para um array não-uniforme. Os parâmetros de simulação adotados para o cálculo da BER são os mesmos que foram adotados para os sistemas apresentados no capítulo 3, na presença de um canal dispersivo.

4.3.1 Array de antenas uniforme

Para o caso do sistema com array de antenas de espaçamento uniforme, realizou-se o cálculo da BER para o transmissor sem antenas fantasmas e com a constelação otimizada para um ângulo de 0º. Os resultados são apresentados na figura 4.1. Ora, o resultado sem

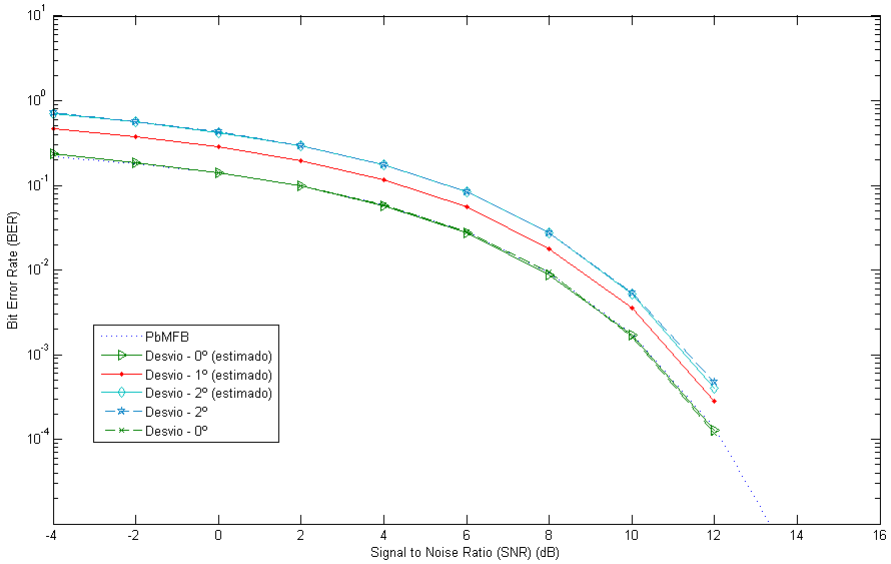

Figura 4.2: BER com a constelação otimizada a 0º num sistema com espaçamento uniforme e com estimação dos coeficientes.

estimação já apresentava resultados semelhantes. Todavia, o número de erros baixou em todos os casos de maneira uniforme.

4.3.2 Array não-uniforme de antenas

Para o caso do sistema com array de antenas de espaçamento não uniforme, os testes foram efecutados para os mesmos casos apresentados no capítulo 3, na secção 3.4.2. Os resultados obtidos para uma constelação otimizada segundo um ângulo de 120º e um ângulo de 30º podem ser vistos na figura 4.2 e 4.3, respetivamente. No sistema que recorre à estimação do canal através do envio de pilotos resultou num melhor desempenho. Quanto muito os desempenhos são iguais quando não existe qualquer erro. A estimação efectuada pressupõe um conhecimento à partida dos pilotos enviados (ordem dos símbolos na constelação adotada) e dos coeficientes g_i de referência (o tipo de componente associada a cada coeficiente). Dado que esta informação não está disponível para um potêncial intruso, a segurança associada a este método de transmissão não fica comprometida, pelo que as melhorias de desempenho só ocorrem para um recetor autorizado.

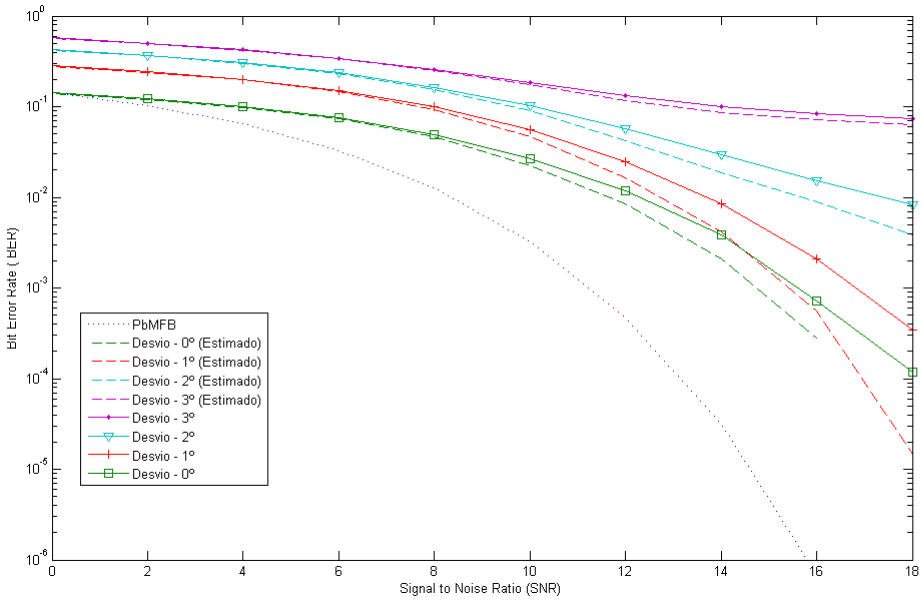

Figura 4.3: BER com a constelação otimizada a 120º num sistema com espaçamento não-uniforme com antenas fantasma e com estimação dos coeficientes, numa constelação 16 QAM

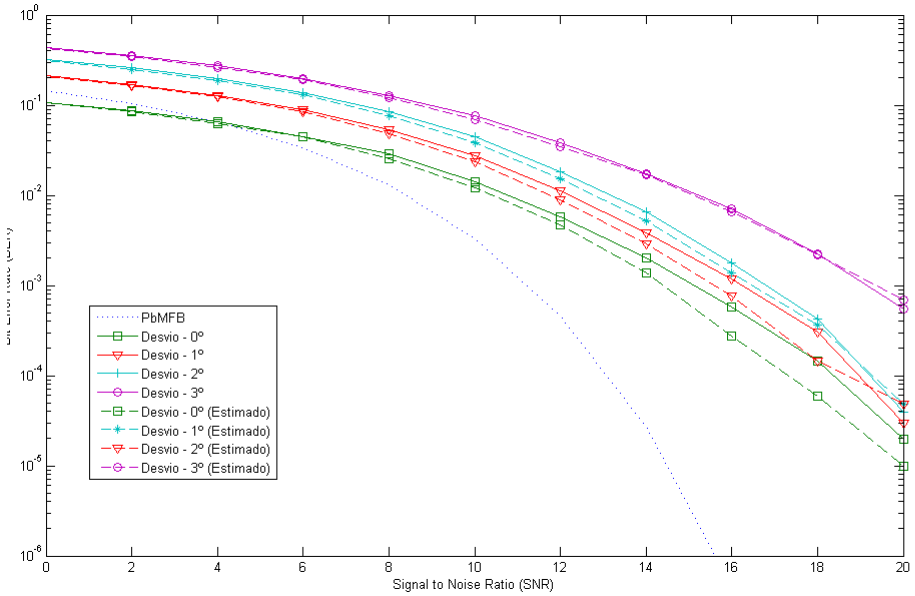

Figura 4.4: BER com a constelação otimizada a 30º num sistema com espaçamento não-uniforme com estimação dos coeficientes, numa constelação 16 QAM

Em ambos os casos, o recetor é capaz de obter melhores desempenhos. A estimação permite uma melhoria no desempenho geral do sistema e maior tolerância face a eventuais rotações, pois no caso da figura 4.3 para mais de 1^o de erro, o sistema sem estimação já não conseguia retirar informação útil ao contrário do que acontece com o método proposto.

CAPÍTULO 5

CONCLUSÃO E TRABALHO FUTURO

5.1 Conclusão

O principal objetivo da dissertação consistiu no estudo da segurança introduzida no nível físico pela estrutura de emissão proposta. Foca-se na exploração das características físicas de estruturas multi-antena no transmissor, com vista ao aumento da segurança com base na natureza direcional da informação transmitida. Como a introdução de segurança no nível físico está intrinsecamente ligada ao desempenho do mesmo, é necessário realizar testes também ao nível do desempenho.

Primeiramente, foram analisadas as BER do sistema baseado num array de distâncias uniformes, tanto para a constelação 16QAM como para a constelação 64QAM, com a constelação otimizada a 0^o em ambos os casos. De seguida foi analisado o comportamento da informação mútua para os mesmos casos.

Dividiram-se os testes em duas partes, nomeadamente transmissores com array de antenas uniformes e não uniformes. Para arrays uniformes analisou-se o nível de segurança na presença ou não de rotações de fase adicionais. Em todos os casos, a análise da informação mútua abrangeu todas as possibilidades de ângulo de otimização. Por último, efetuou-se a análise da BER para ambos os tipos de arrays.

Verificou-se, que configurações do emissor com maior diretividade de informação que a informação mútua tem decréscimos muito acentuados na vizinhança de certos valores de θ segundo os quais a constelação se encontra otimizada, o que indica que pequenos erros na estimação do ângulo de otimização podem resultar na perda total da informação útil. Esta propriedade pode ser usada para tornar a interseção de dados por parte do intruso muito difícil desde que ele não saiba qual o ângulo de otimização. No caso da constelação 64QAM as variações da informação mútua ocorrem em muitos mais valores de ângulos de otimização θ, apesar dos piores casos terem comportamentos semelhantes

aos da constelação 16QAM. Conclui-se também que a introdução de rotações adicionais de fase devido ao efeito equivalente da presença de antenas fantasma consegue garantir um nível de segurança superior tornando a informação mútua ainda mais diretiva. Da análise das BER's, o desempenho do sistema de uma maneira geral degrada-se ligeiramente. Para os casos em que a informação mútua decresce abruptamente, consegue-se observar um comportamento semelhante nas BER: apesar o desvio de poucos graus no ângulo de otimização, a BER estabiliza num valor elevado que inviabiliza a obtenção de qualquer informação útil por parte do recetor.

Com o intuito de minimizar a degradação do desempenho dos sistemas devido a existência de desequílibrios de fase é introduzido um método de estimativa dos coeficientes complexos g_i baseado no envio de pilotos. Os testes realizados efetuaram-se somente para emissores com estruturas de arrays com distâncias uniformes e para a constelação 16QAM (isto é, com quatro antenas). Nos resultados da BER verificou-se uma melhoria do desempenho do sistema, sem com isto afetar a segurança já que a complexidade associada a uma interseção mantem-se elevada dado o grande número de graus de liberdade existentes. A extrapolação do método proposto para outro tipos de constelação é imediata. No entanto, a aplicação do mesmo a outros tipos de constelações como 16 ou 64 Voronoi, deverá ser objecto de investigação futura.

De uma maneira geral, a introdução de segurança no nível físico apresenta resultados promissores como um complemento a outros esquemas de segurança implementados por níveis superirores (como criptografia, codifcação, etc...), sem prejudicar o desempenho do sistema.

5.2 Trabalhos futuros

Um dos focos no trabalho realizado incidiu no uso de arrays de antenas de distância não uniforme no recetor. Não foram investigados os casos em que as distâncias entre as antenas correspondem a qualquer múltiplo real de λ. Isto acarreta a introdução de um número muito maior de combinações possíveis para a configuração dos transmissores. A introdução de técnicas de beamforming combinadas com a diretividade na informação com vista a minimizar o problema da interferência entre os diferentes utilizadores também deverá ser analizada em futuros trabalhos.

A presente análise deverá ser extendida para outro tipo de constelações, nomeadamente constelações 32QAM e 128QAM, e constelações Voronoi.

Deverá também ser estudado o desempenho do método de estimação dos coeficientes complexos g_i baseado do envio de pilotos para as outros tipos de constelações ou constelações de maior dimensão e analisar o impacto de uma ISI residual no processo de estimação.

BIBLIOGRAFIA

[1] J. H. e. A. L. S. Amitav Mukherjee S. Ali A. Fakoorian. "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey". Em: *Communications Surveys and Tutorials, IEEE* (2014).

[2] N. J. Andrea Goldsmith Syed Ali Jafar e S. Vishwanath. "Capacity limits of MIMO Systems". Em: *Selected Areas in Communications, IEEE Journal on* (2003).

[3] A. Barenghi, L. Breveglieri, I. Koren e D. Naccache. "Fault Injection attacks on Cryptografic devices: Theory, Pratice, and countermeasures". Em: *Proc. IEEE* (2012).

[4] J. Croft, N.Patwari e S. Kasera. "Robust uncorrelated bit extration methodologies for wireless sensors". Em: IPSN '10 Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks. 2010.

[5] Z. L. e Dawei Huang. "General MMSE Channel Estimation for MIMO-OFDM Systems". Em: Vehicular Technology Conference, 2008. VTC 2008-Fall. IEEE 68th. 2008.

[6] G. J. Foschini. "Layered space-time arquitecture for wireless Communication in fading environment when using multi-element antennas". Em: *Bell Labs Technical Journal (Volume:1 , Issue: 2)* (1996).

[7] S. Gollakota e D.Katabi. "Physical layer wireless security made fast and channel independent". Em: INFOCOM, 2011 Proceedings IEEE. 2011.

[8] W. Harrison. "Coding for Secrecy: An overview of error-control coding techniques for physical-layer security". Em: *Signal Processing Magazine, IEEE (Volume:30 , Issue: 5)* (2013).

[9] G. Kapoor e S. Piramithu. "Vulnerabilities in some recent proposed RFID ownership transfer protocols". Em: Networks e Communications, 2009. NETCOM '09. First International Conference on. 2010.

[10] E. G. Larsson. "Massive MIMO for Next Generation of Wireless Systems". Em: *Communications Magazine, IEEE (Volume:52 , Issue: 2)* (2014).

[11] L.E.Larson. "Radio frequency integrated circuit technology for low power wireless communications". Em: *Personal Communications, IEEE (Volume:5 , Issue: 3)* (1998).

[12] C.-P. Liang e W. E. Stark. "Nonlinear Amplifier Effects in Communication Systems". Em: *IEEE TRANSACTIONS ON MICROWAVE THEORY AND TECHNIQUES, VOL. 47, NO. 8* (1999).

[13] J. L. Massey. "An introduction to contemporary criptology". Em: Proceedings of the IEEE (Volume:76 , Issue: 5). 1988.

[14] P. Montezuma e V. Astucia. "On the use of Multiple Amplifiers and Antennas for efficient Directive Transmission with large Constellations". Em: Military Communications Conference, MILCOM 2013 - 2013 IEEE. 2013.

[15] P. Montezuma e D. Goncalves. "Ensuring physical layer security through transmissions with directivity at constellations level". Em: (2015).

[16] A. G. e Rui Dinis e P.Torres e N.Esteves. "A turbo FDE technique for Reduced-CP SC-based block Transmission systems". Em: *Communications, IEEE Transactions on (Volume:55 , Issue: 1)* (2007).

[17] D. Rui Dinis R.Kalbasi e A. Banihashemi. "Iterative layered Space-Time Receivers for Single-Carrier Transmission over Severe Time-Dispersive Channels". Em: *Communications Letters, IEEE (Volume:8 , Issue: 9)* (2004).

[18] N. S. e. J. Rui Dinis Paulo Montezuma. "Iterative Frequency-Domain Equalization for General Constellations". Em: Sarnoff Symposium, 2010 IEEE. 2010.

[19] P. C. e Mario Marques da Silva e Rui Dinis. "Multiple input multiple output system with multi user support based on directive information transmission". Em: Proc Progress in Electromagnetics Research Symp. - PIERS, Guangzhou, China, 2014.

[20] A. S. "A simple transmit diversity technique for wireless communications". Em: *Selected Areas in Communications, IEEE Journal on (Volume:16 , Issue: 8)* 16.8 (1998).

[21] B. Schneier. "Cryptografic design vulnerabilities". Em: *IEEE Computer* (1998).

[22] C. Shannon. "Communication Theory of Secrecy Systems". Em: (1949).

[23] A. P. Sinem Coreli Mustafa Ergen e A. Bahai. "Channel Estimation Techniques Based on Pilot Arrangement in OFDM Systems". Em: *Broadcasting, IEEE Transactions on (Volume:48 , Issue: 3)* (2002).

[24] N. B. e S.Tomasin. "Block Iterative DFE for Single Carrier Modulation". Em: *Electronics Letters (Volume:38 , Issue: 19)* (2002).

[25] E. Telatar. "Capacity of multi-antenna Gaussian channels". Em: *European Trans. on Telecomm. ETT, vol.10* (1999).

[26] D. N. C. Tse e P. Viswanath. *Fundamentals of Wireless Communications*. 2005.

[27] D. Vouyioukas. "A Survey on Beamforming Techniques for Wireless MIMO Relay Networks". Em: *International Journal of Antennas and Propagation Volume 2013 (2013)* (2013).

[28] J. Winters. "On the Capacity or Radio Communication Systems with Diversity in a Rayleigh Fading Environment". Em: *Selected Areas in Communications, IEEE Journal on (Volume:5 , Issue: 5)* (1987).

[29] J. Winters. “The impact of antenna diversity on the capacity of wireless Communication systems”. Em: *IEEE Trans. Commun , vol.42* (1994).

APÊNDICE A

INFORMAÇÃO MÚTUA

Informação mútua é um conceito da teoria da probabilidade que consiste numa quantificação da dependência mútua entre duas variáveis diferentes. Matematicamente, a informação mútua de duas variáveis contínuas X e Y pode ser definida como:

$$I(X:Y) = \int_X \int_Y p(x,y) log(\frac{p(x,y)}{p(x)p(y)}) dxdy \tag{A.1}$$

onde $p(x,y)$ é a função densidade da probablidade conjunta entre as duas variáveis e, $p(x), p(y)$ são as funções densidade da probabilidade marginais das variáveis X e Y, respectivamente.

Assumindo símbolos equiprováveis de uma dada constelação φ,é possível escrever:

$$I(S,Y) = \log_2 M - \frac{1}{M} \sum_{s \in \varphi} E_n \left[log_2 \left(\sum_{s_n' \in \varphi} \exp(-\frac{1}{N_0} \left| \sqrt{Es}(s_n - s_n') + n \right|^2 - |n|^2) \right) \right] \tag{A.2}$$

A informação mútua é medida em bits.

APÊNDICE B

BIT ERROR RATE

BER é um conceito utilizado nas telecomunicações para medir o desempenho de um sistema. Consiste na divisão do número de erros B_e pelo número total de bits enviados, durante um intervalo de tempo.

$$BER = \frac{B_e}{Bit_{total}} \tag{B.1}$$

A BER não têm uma unidade de medida, sendo muitas vezes medida expressa em percentagem. O cálculo da BER vem associado ao cálculo da Bit error probability (Pe). A Pe consiste no valor esperado para a BER. Logo, a BER pode ser considerada como uma estimativa da Pe, pelo que quanto maior o intervalo de tempo e o número de bits enviados melhor será a estimativa.

APÊNDICE C

ARTIGO CIENTÍFICO

Ensuring physical layer security through transmissions with directivity at constellations level

Paulo Montezuma[1,3], Diogo Gonçalves[1], Rui Dinis[1,2], and Marko Beko [1,3]

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

Abstract - Common approaches to achieve security at the physical layer rely on code design or channel variations of the wireless environment. In the first security is assured with sacrifice of spectral efficiency and the second approach is not suitable for wireless systems where the channel remains static for most of the time. Thus, a code and channel independent physical layer security measure is more appropriate for such scenarios. In this work, we focus on the information secrecy performance of the signals sent by a multiple-input single-output (MISO) transmitter, based on the decomposition of multilevel modulations in constant envelope sub-constellations. We investigate this new approach to implement security that is independent of channel variations, and thus works even when the channel is static. To achieve security, both transmitter and receiver use constellation shaping and mapping defined by a set of coefficients g_i and antenna array configuration parameters unknown a priori to the eavesdropper. Experimental results of secrecy rate show that the eavesdropper has minimum probability of success. Moreover, the high bit error rate (BER) values make impractical the decoding process by the eavesdropper.
Index Terms: channel independent physical layer security, multilevel modulations, MISO, constellation shaping.

I. Introduction

It is well known that the broadcast nature of wireless communication systems makes them more vulnerable to eavesdropping attacks than the wired counterpart. This justifies why security becomes a critical issue in wireless systems [1]. Commonly, security is assured by encrypted schemes from higher layers, such as key cryptography protocols [2], [3]. Physical layer security can operate independently of higher layers or as a complement. Thus, by introducing security at the physical layer overall security can be increased, since they can be used in a a multilayered approach to reinforce already existing security measures. Common physical layer security implementations use codes for secure communications [4], or exploit channel variations across time and space [5]. The first one sacrifices spectral efficiency due to the use of redundant bits. In the second approach, the assumption of an highly mobile or dynamic environment with significant variations in channel characteristics, is not always valid for all scenarios where wireless communications may occur, and for static channels, physical layer security schemes based on the variation of channel characteristics perform poorly [6]. For these scenarios a channel independent security scheme without redundant coded bits is more appropriate.

Increasingly, the high data rates of communication systems are supported by multiple-input multiple-output (MIMO) systems which can increase throughput with a reduction of the transmitted power by each antenna. Despite the use of multi-antenna transmitters, the high spectral efficiencies needed are only attainable by multilevel constellations characterized by envelope fluctuations that that may impose restrictions on power amplification. This problem can be overpassed by a transmitter structure where multilevel constellations are decomposed into several uncorrelated quasi/constant envelope bi-phase shift keying (BPSK) components, that are amplified and transmitted independently by an antenna. Through this technique the efficiency of power amplification may be improved since it is possible to use nonlinear (NL) amplifiers in such operation [7], [8]. As current multi-antenna transmitters adopted in MIMO systems, this transmitter requires a separate radio frequency (RF)-chain including a power amplifier for each antenna element [9]. One main difference relies on the fact that each RF chain is associated to a sub-constellation that is combined, at channel level, with the other sub-constellations to generate the desired multilevel constellation. Due to the uncorrelated BPSK components the radiation pattern remains unchanged, but the constellation shape is changed to allow a optimization of the transmitted constellation only in a specific angle Θ. This means, that we have directivity at the information level, i.e. the shape and mapping of the transmitted constellation are modified according to an angle Θ. Secrecy is assured since any sequence of bits from the sender is converted into symbols on the constellation space using a set of coefficients g_i (associated to the set of M BPSK components), only known by the sender and the intended receiver.

In this paper, we study a physical layer security technique, independent on channel characteristics. It is shown how to exploit a multi-branch transmission technique with constellation shaping to assure security at the physical layer. We analyze some transmitter properties that may increase

security, such as the sub-constellations arrangements along transmitter antennas, their order and spacing. In section II we start by characterizing the transmission technique. The rest of this paper is organized as follows: Several possibilities of transmitter configuration and the complexity associated to the estimation of these parameters are characterized in section III. In section IV the impact of permutations in the antenna arrangements in uniform and nonuniform antenna arrays is discussed. A set of performance results that sustain our initial assumptions is also presented in section IV-A. Section V resumes this paper.

II. Transmitter Structure

The transmitter is shown in figure 1, where N_m antenna elements are employed to allow an efficient amplification of the signals associated to a large constellation through the following steps: firstly, the data bits are mapped into a given constellation (e.g., a quadrature amplitude modulation (QAM) constellation) characterized by the ordered set $\mathfrak{S} = \{s_0, s_1, ..., s_{M-1}\}$ following the rule $(\beta_n^{(\mu)}, \beta_n^{(\mu-1)}, ..., \beta_n^{(2)}, \beta_n^{(1)}) \mapsto s_n \in \mathfrak{S}$, with $(\beta_n^{(\mu)}, \beta_n^{(\mu-1)}, ..., \beta_n^{(2)}, \beta_n^{(1)})$ denoting the binary representation of n with $\mu = \log_2(M)$ bits. Next, the constellations symbols are decomposed in N_m polar components, i.e.,

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

with $(\gamma_{\mu,i}\ \gamma_{\mu-1,i}\ ...\ \gamma_{2,i}\ \gamma_{1,i})$ denoting the binary representation of i and $b_n^{(m)} = (-1)^{\beta_n^{(m)}}$ is the polar representation of the bit $\beta_n^{(m)}$ (it should be mentioned that we have M constellation symbols in $\mathfrak{S}$ and M complex coefficients g_i, which means that (1) is a system of M equations that can be used to obtain the coefficients g_i, $i = 0, 1, ..., M-1$ [11]). Usually, a given constellation can be decomposed as the sum of $N_m \leq M$ polar components, i.e. it is defined by a set of N_m non-zero coefficients g_i coefficients. The N_m uncorrelated polar components are modulated as N_m BPSK signals with reduced envelope fluctuations (e.g., a gaussian minimum shift keying (GMSK)) that are separately amplified by N_m nonlinear amplifiers and posteriorly transmitted by N_m antennas. Since the outputs of the N_m amplifiers are only combined at channel's level combination losses are also avoided. Thank to the uncorrelated BPSK components in each RF branch, directivity is only introduced at information level due to constellation shaping. This means that shape and mappings of the transmitted constellation are modified according the angle Θ in which the constellation is optimized. Moreover, shaping and symbol mapping can vary with changes of g_i coefficients' order and phases (in fig. 1 g_{i_j} denote the N_m coefficients selected to define the constellation, but for the sake of simplicity we will use g_i along this paper). Consequently, secrecy is assured since any non authorized receiver (also known as Bob) must estimate the set of constellations coefficients $g_i, i = 1, ..N_m$ and the array phase configuration used by the transmitter, otherwise the received constellation suffers, among other effects, a NL distortion due to phase rotations of components associated to each amplification branch that the receiver is unable to compensate (it should be noted that these phase imbalances also may change inter-symbol distances as well as the mapping rule). Therefore, for a successful data reception it becomes crucial the knowledge or the estimate of the set of coefficients $g_i, i = 1, .., N_m$ used at the transmitter, that may vary dynamically over time (in our analysis we consider only static configurations).

Several possibilities for the arrangement of BPSK components along the N_m antennas and the spacing between antennas are discussed in next section.

III. Transmitter configuration possibilities and security

Using (1) several mapping rules can be defined for M-QAM constellations and Voronoi constellations. For instance, for a 64-QAM constellation with Gray mapping we only need 6 non-zero g_i coefficients: $g_4 = 4$, $g_6 = 2$, $g_7 = 1$, $g_{32} = 4j$, $g_{48} = 2j$ and $g_{56} = j$). 16-QAM constellations with Gray mapping are the sum of 4 BPSK signals and can be defined by the set of non-zero complex coefficients $g_2 = 2j$, $g_3 = j$, $g_8 = 2$ and $g_{12} = 1$ (actually, this corresponds to only two QPSK constellations). On the other hand, the energy optimized Voronoi constellations need $M - 1$ non-null coefficients g_i. Other mapping rules or constellations can be easily obtained by changes on the set of coefficients g_i. Clearly, there is a inherent security since a sequence of bits from the sender is converted into symbols on the constellation space using the set of coefficients g_i and an antenna array configuration only known by the sender and the intended receiver. Since the intended receiver knows the set of coefficients g_i and the array configuration, it will be able to decode with success the original data. This means that in every transmission both the sender and the intended receiver use a custom constellation mapping, which may act as a secret key to any interception from a eavesdropper (also known as Eve). For the particular case of M-ary constellations there are $M!$ possible mappings, which becomes impractical for the eavesdropper to decode when transmissions are based on constellations with sizes equal or greater than 64.

In this paper we do not explore the potential of mapping diversity since we restrict our analysis to security assured by directivity (however the secrecy level assured by constellation mapping diversity should be conveniently addressed in further work). Another factor that also increases the complexity of any non authorized interception relies on the relation between constellation shaping and the configuration of the transmitter array. For any set of coefficients g_i the order of the transmit antennas can be changed. Since the number of active antennas is the same of BPSK components, i. e., N_m components, for each mapping rule and uniform configuration of the antenna array there are $N_m! - N_m$ different array configurations and consequently $N_m! - N_m$ different spacial arrangements for the symbols of the transmitted constellation. Permutations of

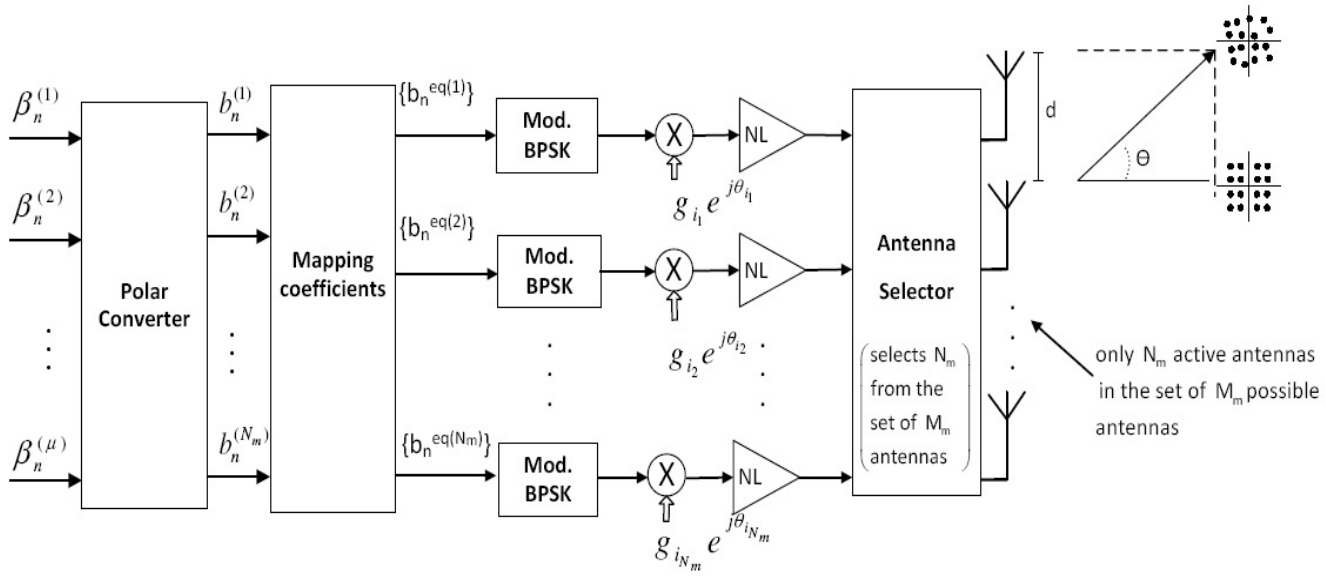

Fig. 1. Structure of constellation directive transmitter

the BPSK components on the RF branches also change the shape of the resulting constellation at channel level (recall that constellation mapping can also suffer changes due to phase rotations of BPSK components). Thus, combining both mapping possibilities and g_i permutations between antennas, for any interception the eavesdropper needs to compute $M! \times (N_m! - N_m)$ combinations (if the transmitter uses Voronoi constellations, even for the smallest constellation with 16 symbols we have 2×10^{13} combinations) .

Complexity can be even increased trough non-uniform spacing between antennas. Consider again the transmitter structure of figure 1 with equal spaced N_a antennas, where only N_m antennas are active in each instant. Since the active antennas can be any set of N_m antennas among the N_a, we have $\frac{N_a!}{(N_a-N_m)!N_m!}$ combinations. Obviously, this situation do not reflects the real number of possibilities, since the spacing between antennas can be any real multiple of λ, leading to a phase shift between antennas $\Delta\theta \in [0, 2\pi]$. Despite this fact, simulation results presented here are restricted to the transmitter configuration of fig. 1, where the distance between antennas is restricted to an integer multiple of $d = \lambda/4$ (in a real case the spacings between antennas are not necessarily restricted to an integer multiple as shown in 1).

IV. Information directivity and achieved security

Having in mind the considerations from previous section a question arises: what will be the secrecy level assured by this transmission scheme and what will be the tolerance against errors on the estimation of transmitter's parameters? To answer this question in this section we present some results related with the mutual information (MI) associated to both authorized receiver and eavesdropper, and the secrecy capacity of the proposed system.

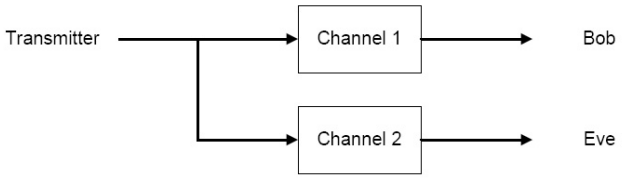

Fig. 2. Non-degraded Gaussian wiretap channel

We assume an non-degraded Gaussian wiretap channel depicted in figure 2, where both channel 1 and channel 2 are both 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 $\mathfrak{S}$. Under these conditions 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 antenna array. With perfect secrecy we have $I(S; Z) = 0$, with S the sent message and Z the received message by the eavesdropper and where $I(;)$ denotes MI. 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

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

where $\boldsymbol{E}_n$ denotes the expectation. Under these conditions, the secrecy capacity is given by

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

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 MI of the intended receiver and $I(S;Z)$ represents the MI of eavesdropper (the capacity is always positive, since due to the absence of information regarding the transmitter configuration the eavesdropper receives always a distorted version of the transmitted signal).

A. Numerical results

We considered transmitters with uniform and non-uniform spacing between antennas. For the transmitters based in uniform arrays, it was evaluated the effect of permutations of BPSK components between antennas. In the transmitters with non-uniform spacing, it was evaluated the effect of permutations on the spacing between antennas. For both options it is characterized their impact on the achievable secrecy rate of an arbitrary downlink transmission with authorized users and a user acting as potential eavesdropper. In the first option the antennas are equal spaced by $d/\lambda = 1/4$ at the transmitter. In non-uniform arrangements the spacing between antennas is always an integer multiple of the distance $d/\lambda = 1/4$. The combinations between coefficients g_i and antennas, for transmitters based on 16-QAM and 64-QAM follow the arrangements of tables I and II. Spacing between antennas for uniform and non-uniform array arrangements are also presented in these tables (it should be mentioned that the values are referred to antenna 1).

TABLE I
16-QAM: g_i ARRANGEMENTS AND DISTANCES BETWEEN ANTENNAS FOR UNIFORM AND NON-UNIFORM ARRAYS.

16-QAM	Antenna order			
	1	2	3	4
coefficients g_i	2j	1	2	j
Spacing to antenna 1		3d	4d	5d
		2d	5d	8d
		3d	4d	6d
		3d	4d	7d

We assume that Bob knows the set of coefficients g_i and the corresponding antenna array configuration. Regarding Eve two different hypotheses are considered:

- I- Eve only knows the set of coefficients g_i, but do not knows the array configuration, i. e., the spacing between antennas and the direction in which the constellation it is optimized.
- II-Eve is unaware about the exact values of the coefficients associated to the constellation optimized for the angle Θ, but can estimate the coefficients g_i that lead to a small error $\Delta\Theta$ (perhaps due to the help of a genie).

TABLE II
64-QAM: g_i ARRANGEMENTS AND DISTANCES BETWEEN ANTENNAS FOR UNIFORM AND NON-UNIFORM ARRAYS.

64-QAM	Antenna order					
	1	2	3	4	5	6
coefficients g_i	2j	1	2	j	4	4j
Spacing to antenna 1		8d	12d	18d	20d	21d
		8d	14d	16d	17d	21d
		8d	14d	16d	20d	21d
		8d	14d	18d	19d	21d

The computation of MI uses Monte Carlo experiments to obtain the average results for MI, which 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 both options, symbols s_n are randomly selected with equal probability from a M-QAM constellation (values of $M = 16$ and $M = 64$ are considered). It is assumed linear power amplification at the transmitter and perfect synchronization for both receiver types.

In hypothesis I, we performed all possible permutations between g_i coefficients and antennas for 16-QAM and 64-QAM. It was observed that MI results for the authorized receiver (Bob) are largely unaffected by changes on antennas permutations. This finding applies equally to both constellation sizes as well as to the eavesdropper (the MI associated to Eve is always null). Having in mind this behavior, in figure 3, we present the MI evolution with Θ for uniform arrays. The permutations between g_i and antennas presented on tables I and II correspond to the 21th and 679th possible permutations for the transmitters based on 16-QAM and 64-QAM, respectively. It can be seen that the MI is practically unaffected by the optimization angle in which the constellation is configured (thus despite the secrecy achieved Bob is always able to decode with success the message). Results regarding non-uniform arrays are presented in figure 4. It is obvious that the MI is more sensitive to the direction Θ in which the constellation is optimized. Despite this higher sensitivity, the MI values are slightly affected over the range of the optimization angle Θ. Still, there are some directions where the MI is lower. The cause for that relies on the constellation shaping that may reduce significantly the separation between constellation's symbols in these cases. It is also worth to mention that the MI values for Bob are practically unaffected by changes on non-uniform arrangements between antennas for both constellations sizes. Similarly to the uniform arrays, the MI associated to Eve is always null for all the arrangements previously analyzed (so the case considered here gives a good example about the behavior of C_s in non-uniform arrays). The same behavior happens even when the g_i values are known but information about the array configuration is absent. This means

that the secrecy rate C_s is equal to the MI of the authorized receiver.

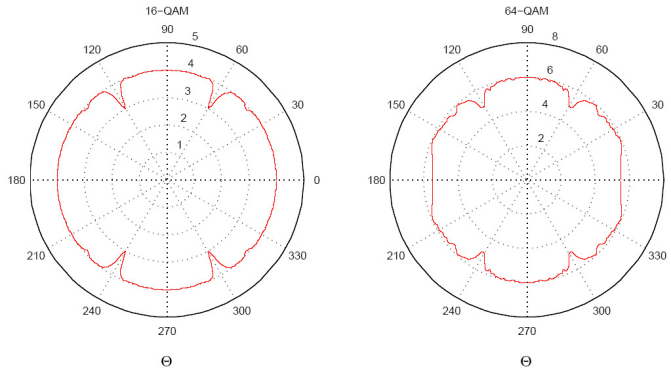

Fig. 3. Uniform arrays: MI behavior with the angle θ in which the transmitted constellation is optimized.

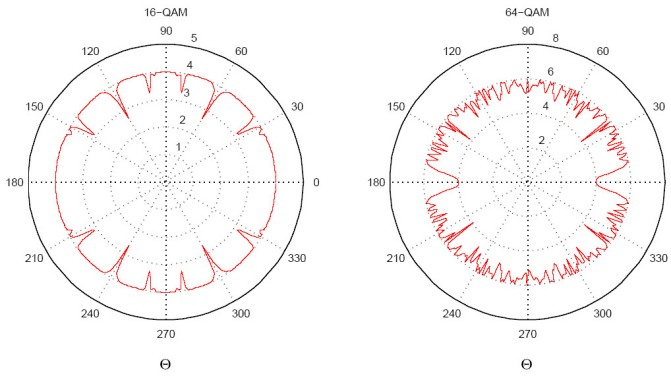

Fig. 4. Non-uniform arrays: MI behavior with the angle θ in which the transmitted constellation is optimized.

From previous results seems obvious that MI values for Bob and Eve are similar in both options. Despite this fact, uniform and non-uniform arrangements may have different effects on tolerance against estimation errors. Let now consider the hypothesis II, where the eavesdropper can estimate the the set of coefficients g_i and the phase shifts between antennas with an error that leads to an estimate $\Theta + \Delta\Theta$. We assume that estimation errors $\Delta\Theta$ that are limited to the set of values $6^o, 10^o$ in 16-QAM, and to $4^o, 6^o$ in 64-QAM. For comparison purposes we also include the results of hypothesis I, where Eve didn't know the array configuration (notwithstanding, Eve may have information about the original constellation defined by the set of coefficients g_i). The non-uniform array spacing configurations for 16-QAM and 64-QAM are those presented on tables I and II, respectively. In uniform array, we consider equal spaced antennas by $d = \lambda/4$. Figures 6 and 7 show the secrecy rates assured by uniform and non-uniform arrangements. Clearly, in both options the secrecy rate increases with the number of coefficients g_i involved in the definition of the constellation. For errors on g_i estimates leading to estimation errors $\Delta\Theta$ higher than 6^o, as

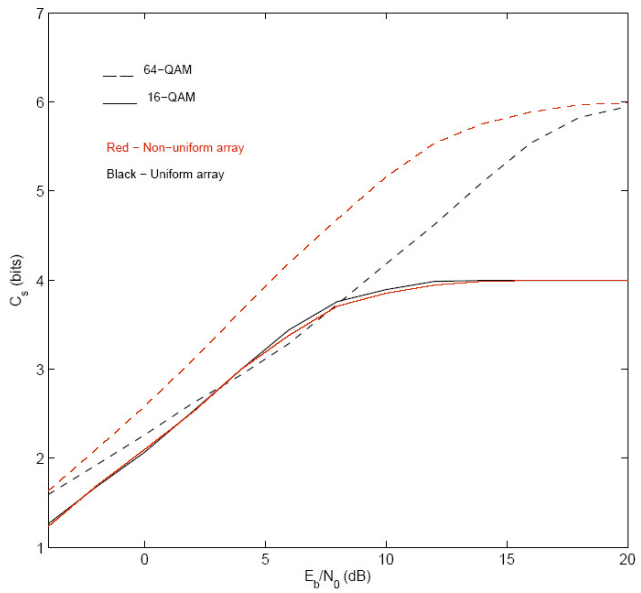

Fig. 5. C_s evolution with $\frac{E_b}{N_0}$ for hypothesis I.

the $\frac{E_b}{N_0}$ increases, C_s remains practically unaffected in both constellations sizes. Only for small signal-to-noise ratio (SNR) values where the system preforms poorly, even in the absence of an eavesdropper the secrecy rate is affected. Results of fig. 7, regarding the 64-QAM, exhibit practically the same behavior, but now even for small estimation errors the C_s values are close to the results of hypothesis I. However, it is important to note that C_S is only affected when SNR values are below the threshold at which the system performance becomes reasonable. For instance, to achieve a BER of 10^{-5} in 16-QAM and 64-QAM the SNR must be 14 dB and 18 dB, respectively. Above these values of SNR, the capacity reaches its maximum value and remains constant. Results also show that non-uniform arrays outperform the uniform ones, due to the lower tolerance against any estimation error. This low tolerance together with the complexity, already mentioned in section II, means that the computational load associated to any interception by Eve can be prohibitive, due to the high number of parameters that must be estimated (the same conclusion is still valid for uniform configurations). Additional increases on security can be achieved by changing dynamically between successive transmitted blocks the configuration of coefficients g_i according to a pattern known by the transmitter and the intended user.

V. Conclusions

The multi-antenna transmitter based on multilevel modulations decomposition as a sum of BPSK components, introduces channel independent security at the physical layer without sacrifices on spectral and power amplification efficiencies. We have shown that secrecy is assured for several configurations of the transmitter and can be increased using non-uniform spacing between the antennas or changing other

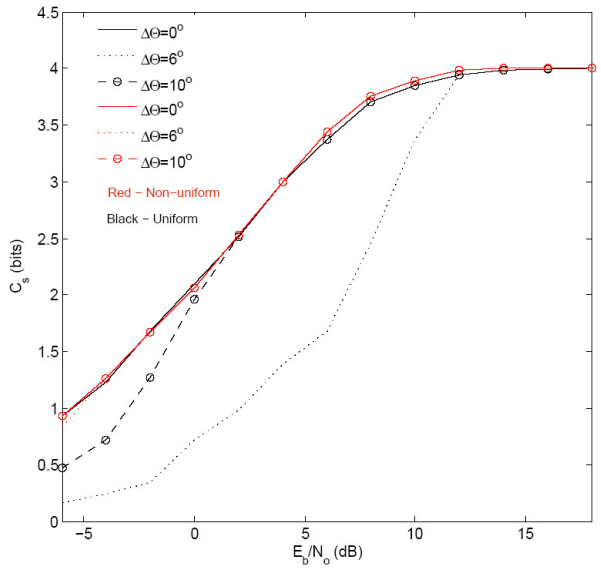

Fig. 6. C_s evolution for 16QAM and impact of angle estimation error $\Delta\Theta$.

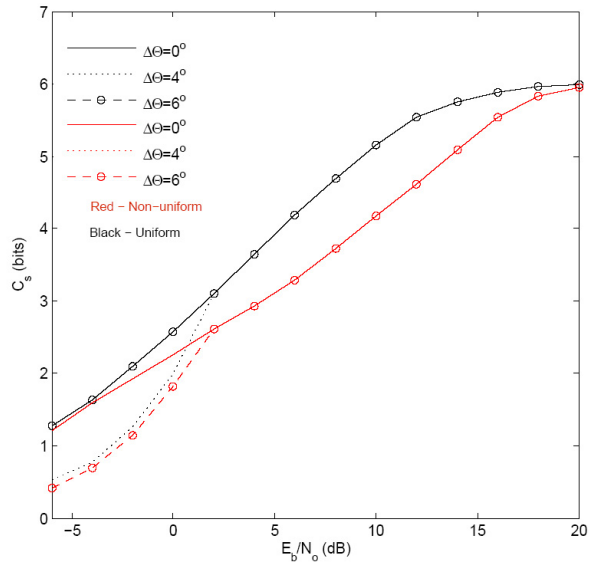

Fig. 7. C_s evolution for 64QAM and impact of angle estimation error $\Delta\Theta$.

parameters such as the g_i coefficients associated to each RF branch. The low tolerance of MI against estimation errors of Θ implies that the set of transmitter g_i coefficients should be perfectly known by the eavesdropper, otherwise it will be unable to decode data with success. This means that the complexity involved in a real time estimation process can be prohibitive for any unauthorized interception. Further studies shall include the level of security provided by dynamic changes on mapping rule and constellation shaping as well as the optimization of the constellation directivity with other array configurations.

ACKNOWLEDGMENTS

This work was supported in part by CTS multi-annual funding project PEst-OE/EEI/UI0066/2011,IT UID/EEA/50008/2013 (plurianual founding and project GLANCES), GALNC EXPL/EEI-TEL/1582/2013, EnAcoMIMOCo EXPL/EEI-TEL/2408/2013 and CoPWIN PTDC/EEI-TEL/1417/2012.

REFERENCES

[1] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security", *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515-2534, June 2008.

[2] J. L. Massey, "An introduction to contemporary cryptology", *Proc. IEEE*, vol. 76, no. 5, pp. 533-549, May 1988.

[3] B. Schneier, "Cryptographic design vulnerabilities", *IEEE Computer*, vol. 31, no. 9, pp. 26-33, Sep. 1998.

[4] 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", *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 41-50, Sep. 2013.

[5] J. Croft, N. Patwari and S. K. Kasera, "Robust uncorrelated bit extraction methodologies for wireless sensors", *in IPSN*, 2010, pp. 7081.

[6] S. Gollakota and D. Katabi, "Physical layer wireless security made fast and channel independent", *INFOCOM*, 2011 Proceedings IEEE, Apr. 2011, pp. 1125-1133.

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

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

[9] D. N. C. Tse and P. Viswanath, Fundamentals of Wireless Communications. Cambridge, UK: Cambridge University Press, 2005.

[10] G. Caire, G. Taricco, and E. Biglieri, "Bit-interleaved coded modulation", *IEEE Trans. Inf. Theory*, vol. 44, pp. 927-947, May 1998.

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

[12] F. Amoroso and J. Kivett, "Simplified MSK Signalling Technique", IEEE Trans. on Comm., Vol. 25, Apr. 1977.

[13] Paulo Montezuma, Rui Dinis, Daniel Marques and Marko Beko, "Robust Frequency-Domain Receivers for A Transmission Technique with Directivity at the Constellation Level", *VTC2014-Fall*, 14-17 September 2014, Vancouver, Canada.

2015	Diogo Gonçalves	Segurança no nível físico em sistemas multi-antena com diretividade na informação