Rui Miguel Horta da Silva Mendes

Licenciado em Engenharia Eletrotécnica e de Computadores

Segurança a Nível Físico em Sistemas MIMO

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

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

Co-orientador: Prof. Doutor Rui Dinis, Professor Associado, FCT-UNL

Júri:

Presidente: Prof. Doutor Pedro Miguel Ribeiro Pereira

Arguentes: Prof. Doutor João Francisco Martinho Lêdo Guerreiro

Vogais: Prof. Doutor Paulo Miguel de Araújo Borges Montezuma de Carvalho

Setembro, 2021

FACULDADE DE CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE NOVA DE LISBOA

Agradecimentos

Em primeiro lugar gostaria de agradecer ao meu orientador Prof. Doutor Paulo Montezuma por todo o seu tempo, trabalho e apoio que disponibilizou para a realização desta tese e por todas as conversas mais informais que se teve que trouxeram sempre momentos alegres.

Queria agradecer também ao Engenheiro Pedro Viegas pela ajuda dada à resolução de dúvidas e problemas relacionadas com o tema.

Gostaria de agradecer também à minha família pelo apoio todo que me deram para conseguir chegar aqui a esta etapa.

Queria também agradecer em especial à Marta Silva, por toda paciência, motivação, exigência e carinho. Sem ti não teria sido capaz de ultrapassar momentos mais desagradáveis e foste a minha melhor amiga que me ajudou sempre em tudo. Neste momento estou onde estou graças a ti, e devo-te muito.

Por último queria agradecer aos meus amigos Rodrigo Matos e André Rosário por me terem dado muitas vezes na cabeça nos momentos que começava a desleixar, pelo apoio todo que me deram e uma amizade que sei que durará para sempre.

Resumo

Os sistemas de comunicação móveis estão em constante evolução e a sua utilização é cada vez maior. Para além disso, são sistemas do tipo broadcast, ou seja, a informação pode ser partilhada com utilizadores não autorizados. Assim sendo, torna-se prioritário garantir que haja segurança nestes sistemas. Já existem esquemas de segurança nas camadas mais superiores que dependem da encriptação de chaves, mas que com a evolução na capacidade de processamento podem não ser suficientes no futuro próximo.

Nesta tese propomos a implementação de esquemas de segurança na camada física. Estes esquemas de segurança utilizam a decomposição dos símbolos enviados, ou da envolvente do sinal, em vários componentes ou sub-portadoras, permitindo manipular a fase e amplitude de uma dada constelação. No caso dos sistemas multi portadora é usada uma estrutura de transmissão baseada no QDA (Quantized Digital Amplification) que tal como o primeiro também consegue elevada eficiência energética na amplificação, mesmo com PAPRs (Peak-to-Power Ratios) elevados. Em ambos os esquemas, mediante a manipulação das fases dos símbolos ou das fases das amostras da envolvente é garantido secretismo com uma baixa complexidade. Além das vantagens já mencionadas, estes dois esquemas permitem obter uma segurança na camada física que complementa esquemas já existentes noutras camadas, sem qualquer tipo de impacto negativo no sistema de comunicação móvel.

Palavras-chave: Sistemas de comunicação móveis, camada física, segurança, eficiência energética, QDA (Quantized Digital Amplification).

Abstract

Wireless communication systems are constantly evolving as there is an increase in demand for their usage. Also, these are broadcast systems which means the information can be shared with unauthorized users. Thus, it is essential to ensure there is security in these communication systems. Already some security systems exist in the higher layers of the system, and these depend on key encryption. However, with the evolution of processing capacity, these security systems might not be enough.

In this thesis, we propose the implementation of a security scheme in the physical layer. These proposed security schemes decompose either the symbols that are sent or the signal's envelope into several components and manipulate the phase and amplitude of a given constellation or envelope. Multi-carrier systems use a structure based on QDA (Quantized Digital Amplification), that also allows achieving high energy efficiency, even with high PAPRs (Peak-to-Power Ratios). In both security schemes, secrecy is assured with low complexity through the manipulation of the symbol phases or phases of the envelope samples. Furthermore, both security schemes allow security in the physical layer that can complement the existing security schemes from other layers without any kind of negative impact on the wireless communication system.

Key words: Wireless communication systems, physical layer, security, quantizers, QDA (Quantized Digital Amplification).

Índice

Lista de Tabelas

Lista de Figuras

LISTA DE ACRÓNIMOS

AWGN	Additive White Gaussian Noise
BER	Bit Error Rate
BPSK	Binary Phase Shift Keying
CP	Cyclic Prefix
CSI	Channel State Information
DAC	Digital-to-Analog Converter
DFT	Discrete Fourier Transform
EVM	Error Vector Magnitude
FPGA	Field Programmable Gate Array
IB-DFE	Iterative Block Decision Feedback Equalizer
IBI	Inter Block Interference
IM	Informação Mútua
ISI	Inter Symbol Interference
LTE	Long Term Evolution
MC	Multi-Carrier
MIMO	Multiple Input Multiple Output

MISO	Multiple Input Single Output
OFDM	Orthogonal Frequency Division Multiplexing
OQPSK	Offset Quadrature Phase Shift Keying
PAE	Power Added Efficiency
PAPR	Peak-to-Average Power Ratio
QAM	Quadrature Amplitude Modulation
QDA	Quantized Digital Amplification
QPSK	Quadrature Phase Shift Keying
SC	Single-Carrier
SC-FDE	Single-Carrier Frequency Domain Equalization
SC-FDMA	Single-Carrier Frequency Division Multiple Access
SNR	Signal-to-Noise Ratio
SVD	Singular Value Decomposition

1

Introdução

A segurança é um dos grandes problemas que sistemas de comunicação sem fios apresentam. Isto deve-se ao facto deste sistema ser do tipo broadcast, o que agrava mais este problema, tornando ainda mais exigente a sua resolução.

Atualmente já se utiliza sistemas de encriptação complexos e que são utilizados nas camadas mais altas do sistema de comunicação e nenhuma delas é dependente da camada física. Logo surge a oportunidade de adicionar segurança a nível físico, de modo, a adicionar mais segurança, impedindo o sucesso de invasão de terceiras pessoas que denominamos de eavesdropper.

Tendo em conta as diferentes tecnologias que se podem utilizar na segurança a nível físico, deve-se também ter sempre em consideração que estas não devem ser facilmente intercetadas pelo eavesdropper, mas se forem, não deve ser posta em causa a integridade do recetor. Isto é, mesmo que o eavesdropper tenha acesso a uma das mensagens trocadas entre o transmissor e o recetor, a tecnologia utilizada deve garantir que o eavesdropper não consiga examinar corretamente a mensagem. Outra limitação que se tem de ter em conta é que estes métodos de segurança não devem afetar a eficiência espectral e energética. Os sistemas de comunicação sem fios como o LTE (Long Term Evolution) e atualmente os sistemas 5G utilizam OFDM (Orthogonal Frequency-Division Multiplexing), que exigem elevada eficiência espetral para garantir os ritmos exigidos e elevada eficiência energética para suporte da qualidade de serviço necessária. Para além disso, o OFDM por si só já possui uma baixa eficiência energética na amplificação, pelo que a adoção de esquemas de segurança que reduziram essa eficiência não deverá ser solução. Finalmente, a segurança não pode ser demasiado complexa devido às limitações a nível de capacidade computacional dos recetores dos dispositivos móveis.

Esta tese está organizada da seguinte maneira:

No presente capítulo é feita uma introdução ao tema e explicada a motivação subjacente a este trabalho. É também descrita como é organizada a tese com uma explicação sumarizada para cada um dos capítulos.

No capítulo 2, são caracterizadas e apresentadas algumas soluções de segurança de nível físico e também é realizada uma análise das vantagens e desvantagens que cada uma delas traz. É também feita uma contextualização do trabalho apresentado na tese. A secção 2.1 é dedicada à segurança com base no canal, e são descritos os métodos de Switched beam beamforming e SVD (Singular Value Decomposition). Na secção 2.2 é

apresentada uma técnica de segurança através da introdução de ruído artificial. A secção 2.3 é dedicada a esquemas de segurança por chave. Na secção 2.4 são apresentados os esquemas de segurança baseados na diretividade da constelação e por alteração do mapeamento de uma constelação personalizada. Por fim, na secção 2.5 são descritas as vantagens e desvantagens de cada um dos esquemas, assim como a estrutura proposta para o trabalho apresentado na tese.

No capítulo 3 aborda-se a segurança por diretividade da constelação. É feita uma análise deste esquema de segurança, abrangendo a sua estrutura, configuração e os seus desempenhos. Na secção 3.1 é feita uma análise de como a segurança é implementada e uma descrição dos parâmetros da estrutura e configuração implementada. Na secção 3.2 é analisado o desempenho do sistema implementado, sendo este caracterizado pelos níveis de BER (Bit-Error Ratio) e Informação Mútua (IM) que foram obtidos através de simulações no Matlab.

No capítulo 4 é apresentado um esquema de segurança em sistemas Multi-Carrier (MC) baseado numa decomposição da envolvente do sinal. É apresentada a sua estrutura e configuração juntamente com os resultados a nível de performance. Na secção 4.1 faz-se uma introdução à transmissão MC nomeadamente o OFDM, ao QDA (Quantized Digital Amplification) e uma análise de como é feita a segurança. Na secção 4.2 é descrita a estrutura do sistema e o modo como a segurança é implementada. Na secção 4.3 é analisado o desempenho do sistema proposto, através de simulações feitas em MATLAB que avaliam os níveis de BER, EVM (Error Vector Magnitude) e de IM.

Finalmente no capítulo 5, são apresentadas as conclusões e algumas sugestões para trabalhos futuros.

2

Estado de arte

Existem vários tipos de segurança que podem ser implementados a nível físico. A segurança por constelação, que explora a diversidade da constelação das comunicações sem fios, utiliza um mapeamento personalizado entre o transmissor e o recetor. A segurança por introdução de ruído, que se faz a introdução de um ruído artificial utilizando a técnica de beamforming. A segurança por chave envolve a utilização de uma chave no início de cada mensagem trocada, entre o transmissor e o recetor, e que varia sempre entre cada mensagem. E por fim a segurança com base no canal.

Neste capítulo serão discutidas estas abordagens na secção 2.1, 2.2, 2.3 e 2.4. Na secção 2.1 são caracterizados dois tipos de seguranças com base no canal, o Switched beam beamforming e o SVD. Na secção 2.2 é descrita a segurança por introdução de ruído artificial. Na secção 2.3 é descrita a segurança por chave. Na secção 2.4 são caracterizados dois tipos de segurança por constelação nomeadamente o Mapeamento de uma constelação personalizada e a segurança por diretividade da constelação. Finalmente, na secção 2.5 serão descritas as vantagens e desvantagens de cada um dos esquemas de segurança, bem como as razões inerentes à escolha do tipo de esquemas de segurança adotados no trabalho apresentado nesta tese.

2.1 Segurança com base no canal

2.1.1 Switched beam beamforming

Segundo a teoria de informação, se o canal do eavesdropper for degradado, uma comunicação segura pode ser garantida utilizando apenas segurança a nível físico [1,2], mesmo se o eavesdropper tiver grandes capacidades computacionais. Se o transmissor tiver várias antenas, a transmissão por beamforming pode ser aplicada para melhorar a capacidade do canal do recetor e degradar o canal do eavesdropper, aumentado assim o secrecy rate [3,4]. A desvantagem desta abordagem é que a fonte deve ter conhecimento perfeito do CSI (Channel State Information) para a transmissão por beamforming, sendo o CSI do canal do eavesdropper especialmente difícil de se obter. Para além disso, a fonte não consegue ter conhecimento do canal do eavesdropper que varia aleatoriamente, tornando-se impossível fornecer uma secrecy rate fixa. Neste caso, o secrecy outage capacity é adotado como métrica para avaliar a segurança, que é definida pela taxa máxima sob a condição de que a probabilidade de a verdadeira taxa

de transmissão ser maior que um dado valor atribuído ao secrecy capacity. Num sistema multi-antena, o switched beam beamforming é popular pela sua baixa complexidade e alta performance. No artigo [5], os autores propõem adotar beamforming para aumentar a capacidade do recetor autorizado e derivar uma expressão que define a probabilidade em termos de secrecy outage capacity.

Considere-se um transmissor com N antenas que comunica com um receptor com uma única antena. Existe uma outra antena recetora que será do eavesdropper que também recebe o sinal e tenta intercetá-lo. Os sinais recebidos do recetor e do eavesdropper são dados respetivamente por

$$y_r = \sqrt{P}\, a_r h^H w_i x + n_r \tag{2.1}$$

e

$$y_e = \sqrt{P}\, a_e g^H w_i x + n_e \tag{2.2}$$

onde x é a distribuição Gaussiana do sinal transmitido, P é a potência transmitida, n_r e n_e é o ruído do respetivo recetor e eavesdropper. Os canais do recetor e do eavesdropper são descritos respetivamente por $a_r h$ e $a_e g$. Consequentemente, as capacidades de canal do recetor e do eavesdropper podem ser expressas por

$$C_r = W log_2(1 + \gamma_r) \tag{2.3}$$

e

$$C_e = W log_2(1 + \gamma_e) \tag{2.4}$$

onde W é a largura de banda, $\gamma_r = P\, a_r^2 |h^H w_{i^*}|^2$ e $\gamma_e = P\, a_e^2 |g^H w_{i^*}|^2$ são o SNR (Signal-to-Noise Ratio) do recetor e do eavesdropper, respetivamente. Portanto, o secrecy capacity é dada por $C_{sec} = |C_r - C_e|^+$, onde $[x]^+ = \max(x, 0)$. Visto que não há conhecimento do canal do eavesdropper por parte do transmissor, é impossível fornecer um secrecy capacity fixo. Os autores usam o secrecy outage capacity R_{sec} como métrica de performance, sendo este definido como a taxa máxima sob a condição de que a probabilidade a taxa de transmissão supera o secrecy capacity é igual ε que é dado por

$$P_s(R_{sec} > C_r - C_e) = \varepsilon \tag{2.5}$$

substituindo (2.3) e (2.4) na equação (2.5), transforma-se em

$$\varepsilon = P_s\left(\gamma_r < 2^{R_{sec}/W}(1 + \gamma_e) - 1\right) = \int_0^{\infty} \int_0^{2^{\frac{R_{sec}}{W}}(1+\gamma_e)-1} f_{\gamma_r}(x) f_{\gamma_e}(y)\, dx dy$$

$$= \int_0^{\infty} F_{\gamma_r}\left(2^{R_{sec}/w}(1+y)-1\right) f_{\gamma_e}(y)dy\ , \tag{2.6}$$

onde $f_{\gamma_e}(y)$ é a função de densidade da probabilidade de γ_e, $f_{\gamma_r}(x)$ e $F_{\gamma_r}(x)$ são a função de densidade da probabilidade e a função de distribuição de γ_r, respetivamente. Como w_{i^*} é independente de g, pode-se então ter

$$f_{\gamma_e}(y) = \left(1 - \exp\left(\frac{x}{Pa_e^2}\right)\right). \tag{2.7}$$

Semelhantemente, $|h^H w_{i*}|^2$ pode ser considerado como o máximo de N variáveis independentes aleatórias distribuídas exponencialmente causadas pela seleção do beamforming tem-se

$$F_{\gamma_r}(x) \ = \ (1 \ - \ \exp\left(\frac{x}{Pa_r^2}\right))^N. \tag{2.8}$$

Substituindo (2.7) e (2.8) na equação (2.6) tem-se então

$$\varepsilon \ = \ 1 \ + \ \sum_{n=1}^{N} \binom{N}{n} (-1)^n \left(\frac{1}{1 + \ n2^{R_{sec}/w} a_e^2/a_r^2}\right) * exp\left(-\frac{n(2^{R_{sec}/w}-1)}{Pa_r^2}\right)$$

$$= G(R_{sec}, P)\ . \tag{2.9}$$

Finalmente a partir da equação (2.9), podemos obter a probabilidade de se ter secrecy positivo como

$$P_s(C_{sec} \ > \ 0) \ = \ 1 \ - \ G(0,P) = \ 1 \ - \ \frac{a_r^2}{a_e^2} B\left(\frac{a_r^2}{a_e^2}, N \ + \ 1\right) \tag{2.10}$$

onde B(x,y) é a função Beta. Conclui-se a partir da equação (2.10) que a probabilidade $P_s(C_{sec} > 0)$ é independente de P. E consoante o número de antenas do transmissor aumenta, a probabilidade aumenta conformemente, por causa dos ganhos obtidos pelo switched beamforming. Para além disso, (2.10) também revela que o acesso à curta distância por parte do recetor é benéfico para garantir a segurança dos seus dados.

2.1.2 MIMO-SVD

Uma técnica que pode ser aplicada em sistemas MIMO (Multiple-Input Multiple-Output) é o esquema SVD. Este esquema combina pré-codificação e descodificação ao nível da frequência, juntamente com um recetor baseado no IB-DFE (Iterative Block-Decision Feedback Equalizer), que permite um bom desempenho, mesmo em canais dispersivos. Em [6] é proposto uma estrutura MIMO-SVD combinado com técnicas SC-

FDE (Single Carrier-Frequency Domain Equalization). Tirando vantagem dos diferentes canais do recetor e do eavesdropper, analisa-se o potencial da segurança que se pode ter a nível físico utilizando este esquema. É provado que o secrecy rate aumenta com a distância entre o eavesdropper e o transmissor ou recetor. Isto significa que se pode ter segurança em comunicações MIMO sempre que o eavesdropper não se encontra localizado perto do transmissor ou do recetor, mesmo se o eavesdropper for capaz de receber todos os blocos de treino partilhados entre o recetor e o transmissor.

Considera-se um sistema MIMO ponto a ponto com um transmissor com T antenas um recetor com R antenas e finalmente um eavesdropper com R antenas que tenta intercetar os sinais transmitidos entre o transmissor e o recetor. Este cenário é demonstrado na figura seguinte:

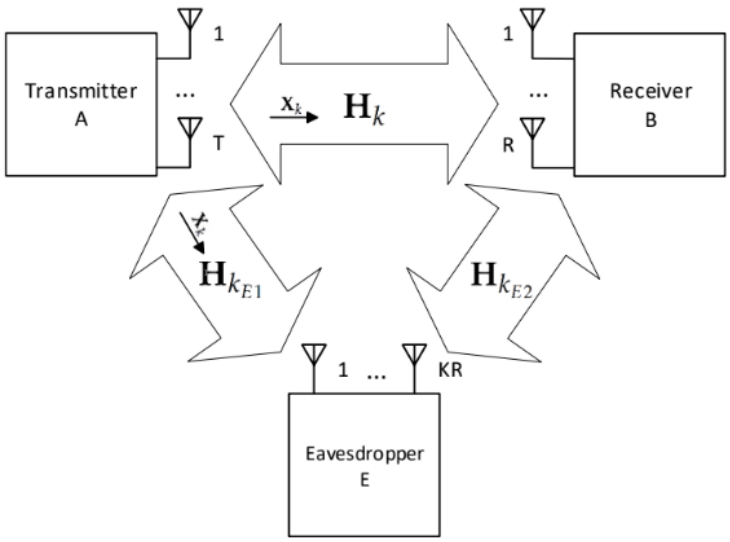

Figura 2.1- Sistema MIMO-SVD com eavesdropper. Adaptado de "On the Physical Layer Security Characteristics for MIMO-SVD Techniques for SC-FDE Schemes" J. Madeira, J. Guerreiro, R. Dinis, P. Montezuma e L. M. Campos, Out 2019

Assume-se que a distância entre antenas no transmissor e no recetor é maior que o comprimento de onda do sinal transmitido e que o recetor está fora da região distante do transmissor. O transmissor consegue enviar até $C = R$ streams de dados sobre um canal altamente seletivo na frequência. Para compensar a forte ISI (Inter-symbol interference) associadas a este tipo de canais, implementa-se técnicas de transmissão SC-FDE. Os blocos de dados são compostos por N símbolos QPSK (Quadrature Phase

Shift Keying), mais um CP (Cyclic Prefix) com duração igual ao delay spread máximo do canal. O diagrama de blocos do sistema é ilustrado na figura 2.2.

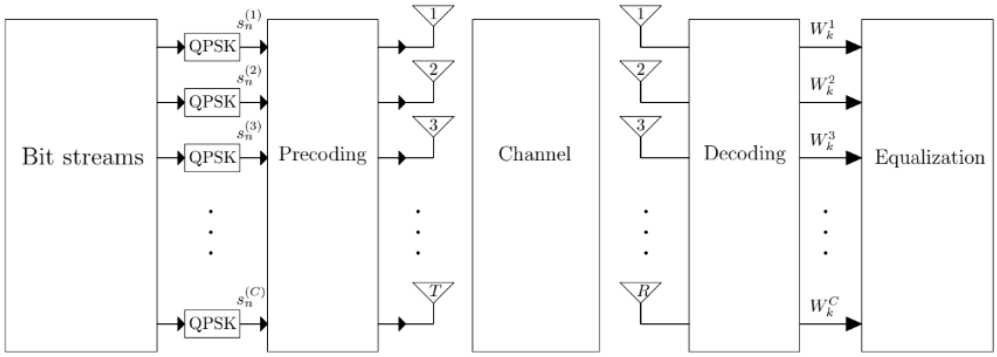

Figura 2.2- Sistema MIMO-SVD, com T antenas transmissor e R antenas recetoras. Adaptado de "On the Physical Layer Security Characteristics for MIMO-SVD Techniques for SC-FDE Schemes" J. Madeira, J. Guerreiro, R. Dinis, P. Montezuma e L. M. Campos, Out 2019

Os símbolos de dados transmitidos pelos C SC streams de dados podem ser associados a uma matriz **s** de dimensão N x C, onde cada stream é representado como um vetor $s_n^{(c)} = [\, s_1^{(c)} s_2^{(c)} \ldots s_N^{(c)}]$ de dimensão N x 1. $s_n^{(c)} = [\, s_1^{(c)} s_2^{(c)} \ldots s_N^{(c)}]$. O grupo de símbolos associado à n-ésima sub-portadora é representado como um vetor $S_k = [\, s_k^{(1)} s_k^{(2)} \ldots s_k^{(C)}]$ de dimensão 1 x C.

A resposta em frequência do canal na enésima sub-portadora é modelado pela matriz R x T

$$H_k = \begin{bmatrix} H_k^{(1,1)} & \cdots & H_k^{(1,T)} \\ \vdots & \ddots & \vdots \\ H_k^{(R,1)} & \cdots & H_k^{(R,T)} \end{bmatrix}. \tag{2.11}$$

Visto que estamos a considerar uma comunicação ponto a ponto onde temos várias antenas transmissoras e recetoras, a separação das streams MIMO pode ser feita utilizando técnicas de SVD [7]. Para executar o SVD, é necessário o conhecimento do canal quer no transmissor como no recetor. Para tal, o transmissor e o recetor trocam entre eles sequências de treino.

A técnica SVD permite obter os C canais desassociados para se poder multiplexar C streams de dados. Uma vez que se está a utilizar esquemas SC-FDE a decomposição é feita ao nível da sub-portadora. Assim, pode-se decompor a matriz do canal associado a uma dada sub-portadora H_k como

$$H_k = U_k \Lambda_k V_k^H, \tag{2.12}$$

onde U_k é a matriz de descodificação R x R, V_k é a matriz de pré-processamento T x T e Λ_k é a matriz diagonal C x C composta pelos valores singulares de H_k, que são ordenados por ordem decrescente de acordo com a sua potência.

Como descrito previamente, o canal do transmissor estimado requer a computação da matriz pré-codificada, que pode ser obtida através da troca de sequências de treino entre o transmissor e o recetor. De seguida, o recetor calcula a matriz de deteção, executa a equalização do canal e finaliza a decomposição SVD. O eavesdropper escuta ambas as sequências de treino do transmissor e do recetor de modos a calcular a sua própria estimativa do canal.

Este processo pode-se resumir em 3 passos. No primeiro passo o recetor envia a sequência de treino ao transmissor, que é escutado pelo eavesdropper. Quer o transmissor, quer o eavesdropper obtêm estimativas do canal. No segundo passo, o transmissor envia uma sequência de símbolos de treino para que o recetor possa obter uma estimativa do canal e calcular a matriz de descodificação para completar o SVD. O eavesdropper também escuta esta sequência e obtém outra estimativa do canal. Por fim, no terceiro passo é iniciada a transmissão de dados. O transmissor usa a sua estimativa do canal para pré-codificar o sinal, enquanto o recetor usa a sua estimativa do canal de modo a efetuar a descodificação do sinal recebido. Do mesmo modo, o eavesdropper tenta descodificar esse mesmo sinal. Para aumentar a precisão da sua deteção, o eavesdropper calcula o canal estimado, como a média dos dois canais que anteriormente estimados. Este processo é ilustrado na figura 2.3

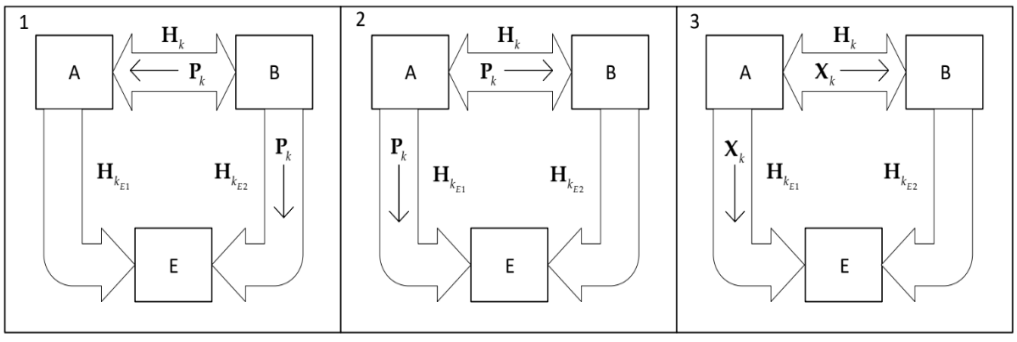

Figura 2.3- Passos para obter as estimativas dos canais. Adaptado de "On the Physical Layer Security Characteristics for MIMO-SVD Techniques for SC-FDE Schemes" J. Madeira, J. Guerreiro, R. Dinis, P. Montezuma e L. M. Campos, Out 2019

Como descrito em [8], o canal pode ser expresso como

$$H_k = \rho_A \hat{\mathrm{H}}_{k_A} + \epsilon_k, \tag{2.13}$$

onde $\hat{\mathrm{H}}_{k_A}$ é o canal estimado utilizado pelo transmissor, ρ_A é o fator de correlação com o verdadeiro canal, e ϵ_k é o erro associado ao processo de estimação do canal. A decomposição SVD de $\hat{\mathrm{H}}_{k_A}$ é

$$\hat{\mathrm{H}}_{k_A} = \hat{\mathrm{U}}_{k_A} \Lambda'_{k_A} V'^{H}_{k_A}. \tag{2.14}$$

Portanto, o transmissor calcula os símbolos pré-codificados com T x 1 vetor $V'^{H}_{k_A}$ como

$$X_k = V'_{k_A} S'_k. \tag{2.15}$$

Tanto o recetor como o eavesdropper implementam a mesma abordagem de receção. No entanto, os canais que eles observam irão ser diferentes, ou seja, eles irão trabalhar com estimativas de canais diferentes. Neste caso, o eavesdropper deverá estar numa posição diferente do transmissor ou do recetor, logo não poderá descodificar com sucesso a troca de dados entre o recetor e o transmissor.

2.2 Segurança por introdução de ruído artificial

De acordo com o trabalho desenvolvido em [9] num sistema que envolve múltiplas antenas com CSI imperfeito, o beamforming com ruído artificial é uma técnica eficiente para assegurar a transmissão de dados. Para além do sinal transmitido com os dados, parte da potência é alocada para gerar ruído artificial com o objetivo de confundir qualquer eavesdropper que tente intercetar o sinal. Especificamente, o ruído gerado será aplicado na parte do canal não utilizado para transmissão de dados úteis do recetor.

Esta técnica depende do CSI instantâneo do recetor, mas não requer o CSI instantâneo do canal do eavesdropper. O canal do recetor anula o ruído artificial, e como tal o recetor não será afetado pelo ruído. O conceito básico deste beamforming com ruído artificial é ilustrado na figura seguinte.

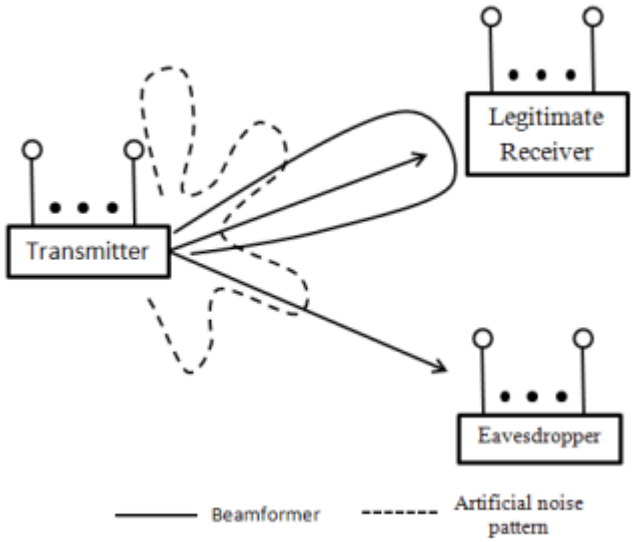

Figura 2.4- Beamforming com ruído artificial. Adaptado de "Wireless Physical Layer Security with Imperfect Channel State Information" B. He, X. Zhou and T. D. Abhayapala, Jul 2013

2.3 Segurança por chave

Segundo [10], o conceito base da segurança por chave é a execução de várias operações matemáticas por parte do transmissor na mensagem de modo a conseguir encriptá-la. Neste caso, a única maneira de se inverter isso é sabendo o algoritmo utilizado na encriptação e qual a chave de encriptação. O recetor que sabe o algoritmo que foi utilizado decifra a mensagem encriptada com a sua própria chave. Por outro lado, mesmo que o eavesdropper saiba o algoritmo utilizado, não conseguirá decifrar a mensagem se não souber a chave.

No entanto, este método impõe que o recetor partilhe uma chave para o transmissor de modo que este consiga encriptar a mensagem e o recetor consiga decifrá-la. Isto significa que se não houver segurança suficiente o eavesdroper consegue descobrir a chave, e com isso intercetar e decifrar a mensagem. Para evitar este cenário pode-se utilizar a encriptação baseada numa chave pública. Esta encriptação consiste na partilha de uma chave pública que servirá apenas para encriptar a mensagem, e de uma chave secreta que será apenas conhecida pelo recetor e que servirá para decifrar a mensagem. Neste caso deixa de haver a necessidade de segurança na partilha da chave

de encriptação porque se o recetor conseguir manter em segredo a chave secreta, o eavesdropper nunca poderá decifrar a mensagem mesmo sabendo a chave pública.

Para melhorar esta segurança pode-se utilizar os dois métodos em conjunto. O transmissor pode encriptar a mensagem utilizando uma chave partilhada por ambos o transmissor e o recetor e essa chave partilhada pode ser encriptada utilizando a criptografia baseada numa chave pública. Nesta situação, o único trabalho do recetor consiste manter em segredo a sua chave secreta.

2.4 Segurança por constelação

2.4.1 Mapeamento de uma constelação personalizada

Um dos métodos de segurança que se poderá utilizar no nível físico é por constelação. Este método envolve utilizar um mapeamento da constelação personalizado sugerido em [11], e que seja conhecido pelo transmissor e recetor sem ter de adotar métodos intensos de mecanismos de encriptação no sistema. Sendo que esta técnica de segurança é baseada na diversidade da constelação, a mesma não irá depender das características do canal. Esta técnica baseia-se na conversão da sequência de bits provenientes do transmissor em símbolos que serão representados como pontos num plano complexo de duas dimensões que se carateriza como diagrama de constelação.

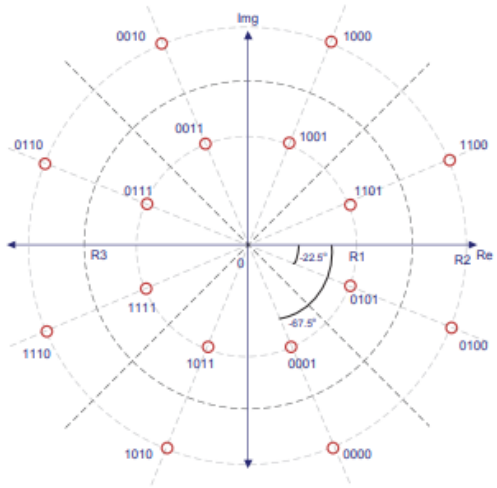

Figura 2.5 - Constelação Circular 16-QAM. Adaptado de "Physical Layer Security In Wireless Networks through Constellation Diversity" M. I. Husain, S. Mahant and R. Sridhar, Aug 2011

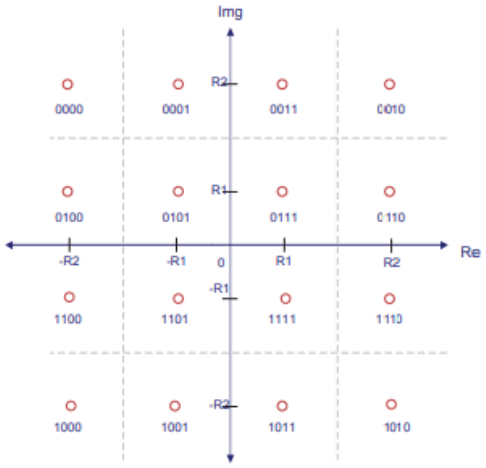

Figura 2.6 - Constelação Retangular16-QAM. Adaptado de "Physical Layer Security In Wireless Networks through Constellation Diversity" M. I. Husain, S. Mahant and R. Sridhar, Aug 2011

As figuras 2.5 e 2.6 mostram exemplos de diagramas de constelação. A figura 2.5 mostra um diagrama de constelação de uma modulação 16-QAM (Quadrature Amplitude Modulation) circular e a figura 2.6 mostra uma alternativa para um diagrama de constelação que é conhecida por constelação retangular 16-QAM. O transmissor envia uma sequência de bits, definindo a sua parte real e imaginária de acordo com a constelação em questão, o sinal pode ser expresso com a seguinte fórmula matemática:

$$s(t) = I(t).\cos(2\pi f_c t) + Q(t).\sin(2\pi f_c t), \qquad (2.16)$$

onde I(t) é a parte real e Q(t) é a parte imaginária dos símbolos da constelação e f_c é a frequência portadora. Para descodificar esta mensagem é necessário o recetor saber quer o tipo de modulação utilizado quer o mapeamento de símbolo para sequência de bits que será apenas conhecido pelo transmissor e no recetor pretendido. Apenas utilizando esse mapeamento é que será possível descodificar o sinal e voltar a construir a mensagem original. Deste modo, mesmo no caso de existir um eavesdropper a interferir entre o transmissor e o recetor, este nunca poderá descodificar o sinal corretamente sem o conhecimento prévio deste mapeamento. Ou seja, nunca conseguirá construir a mensagem da mesma maneira que o recetor que tem conhecimento desse mapeamento.

Para esta codificação ter um funcionamento correto é necessário também haver conhecimento do tipo de modulação (BPSK (Binary Phase Shift Keying), QPSK e QAM, por exemplo) que será utilizado entre o recetor e o transmissor. Isto também é utilizado como segurança, pois significa que o eavesdropper também necessita de saber qual é o tipo de modulação para conseguir obter a mensagem trocada entre o recetor e o transmissor. Ainda assim, o eavesdropper pode utilizar técnicas baseadas em machine learning [12] para identificar o tipo de modulação. Porém, em relação ao mapeamento da constelação, a complexidade é bastante maior, porque para M-QAM o eavesdropper tem *M!* possibilidades diferentes, o que torna bastante difícil descodificar a mensagem, já que o eavesdropper nunca saberá o mapeamento correto, mesmo se tentar todas as hipóteses.

2.4.2 Segurança por diretividade da constelação

Atualmente, os sistemas de comunicação móveis têm de suportar múltiplos utilizadores e ao mesmo tempo manter a privacidade do conteúdo dos mesmos. No entanto, os métodos utilizados para manter a privacidade dos utilizadores podem comprometer a eficiência espetral ou não ser adequados para canais estáticos. Por estas razões, é preferível um esquema de segurança a nível físico sem utilização de código e que seja independente de CSI. Assim sendo, segurança pode ser alcançada através de mapeamento de constelações e moldando essas constelações para direções especificas que são introduzidas ao nível do transmissor.

As constelações resultantes pelos transmissores MIMO e MISO (Multiple Input Single Output) trazem diretividade a nível de constelação que pode ser implementada para garantir segurança a nível físico [13]. Portanto, a segurança neste método resume-se na diretividade da constelação, ou seja, na direção em que a constelação é optimizada. Adicionalmente esta segurança pode ser melhorada pela mudança de coeficientes de fase ou utilizando constelações que podem ser decompostas por um número maior de componentes BPSK. Isto traz uma grande complexidade computacional associada à interceção da mensagem, pois cada utilizador tem de ter conhecimento dos coeficientes associados aos componentes BPSK, fases e sua distribuição pelos diferentes ramos do array de antenas. Para além disso, esta segurança implementada não compromete eficiência espetral e é independente do estado do canal.

Esta estrutura é proposta em [14], onde é usada uma configuração MISO, que envolve vários transmissores e apenas um recetor. A constelação transmitida para o recetor será o resultado da combinação de N_m sinais de envolvente constante que serão amplificados por N_m amplificadores não-lineares antes de serem transmitidos pelas N_m antenas transmissoras. Este método evita perda de combinações e aumenta a eficiência de amplificação de potência, uma vez que os outputs dos N_m amplificadores são combinados no canal e é possível utilizar amplificadores não lineares operando na eficiência máxima [15,16]. A figura 3 mostra a estrutura do transmissor:

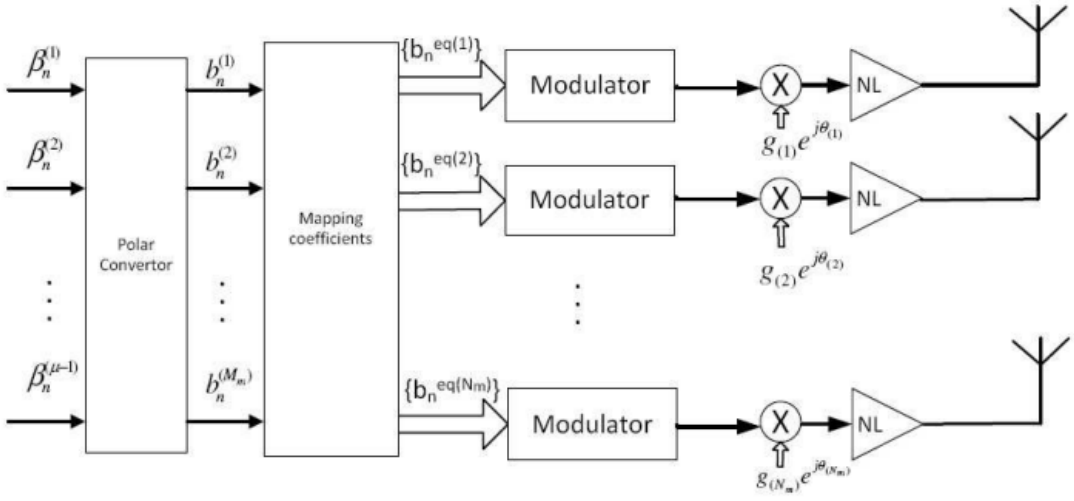

Figura 2.7 - Estrutura do transmissor com informação diretiva. Adaptado de "Physical Layer Security Scheme Based on Power Efficient Multi-Antenna Transmitter" P. Montezuma, R. Dinis and M. Beko, Vol. 35, No. 11, pp. 860-861, July 2015

Nesta estrutura de transmissão, primeiramente os bits de dados são mapeados numa dada constelação caracterizada por $\mathfrak{S} = \{s_0, s_1, \dots, s_{M-1}\}$ seguindo a regra $\left(\beta^{(\mu-1)}, \beta^{(\mu-2)}, \dots, \beta^{(1)}, \beta^{(1)}\right) \mapsto s_n \in \mathfrak{S}$, com $\left(\beta^{(\mu-1)}, \beta^{(\mu-2)}, \dots, \beta^{(1)}, \beta^{(1)}\right)$ indicando a representação binária de n com $\mu = log_2(M)$ bits. De seguida os símbolos da constelação são decompostos por M_m componentes polares com amplitudes distintas, de acordo com a regra de decomposição

$$s_n = g_0 + g_1 b_n^{(1)} + g_2 b_n^{(2)} + g_3 b_n^{(1)} b_n^{(2)} + g_4 b_n^{(3)} + \cdots$$
$$= \sum_{i=0}^{Mm-1} g_i \prod_{m=0}^{\mu-1} \left(b_n^{(m)}\right)^{\gamma_{m,i}} \quad (2.17)$$

em que $(\gamma_{\mu,i}, \gamma_{\mu-1,i}, \dots, \gamma_{2,i}, \gamma_{1,i})$ indica a representação binária de i e $b_n^{(m)} = (-1)^{\beta_n^{(m)}}$ é a representação polar do bit $\beta_n^{(m)}$. No caso dos coeficientes g_i serem reais obtém-se uma decomposição em componentes BPSK com M_m amplitudes distintas. Quando os coeficientes g_i são complexos, o símbolo é decomposto em componentes QPSK ou OQPSK (Offset Quadrature Phase Shift Keying) de amplitudes distintas.

Apesar de não haver diretividade na energia devido ao facto dos componentes BPSK dos diferentes ramos serem descorrelacionados, existe uma diretividade ao nível de informação já que a constelação transmitida está otimizada para um ângulo específico Θ. Por conseguinte existe implicitamente um esquema de segurança de nível físico, pois qualquer utilizador não autorizado tem de ter conhecimento dos coeficientes g_i da constelação, assim como a configuração dos componentes BPSK ou QPSK pelo array de antenas de modo a conseguir descodificar os dados transmitidos. Outro aspeto associado à segurança imposta por este sistema é a complexidade que ela traz a qualquer interceção de mensagem, dado que o transmissor tem a liberdade de mudar a sua configuração, ou seja o mapeamento dos componentes BPSK ou QPSK pelos ramos e as diferenças de fase entre os ramos. Logo, podem-se obter mapeamentos distintos alterando os valores dos coeficientes g_i ou alterando a associação entre os componentes BPSK e as antenas de transmissão.

2.5 Tipo de segurança proposta

Como discutido anteriormente, a adição de segurança ao nível da camada física é uma forma de consolidar a segurança uma vez que esta pode ser combinada com esquemas de segurança das camadas superiores. No entanto, a segurança de nível físico não pode comprometer a qualidade de serviço do utilizador e a sua instalação não pode ser complexa. A eficiência energética e espetral não pode ser prejudicada, e deverá ser pouco exigente a nível de capacidade computacional por parte dos recetores autorizados e não deve também depender dos canais do transmissor ou do recetor.

Não é aconselhável a utilização de uma segurança por introdução de ruído artificial, pois como se viu a implementação da estrutura é bastante complexa quer para o transmissor como para o recetor. Para além disso, a qualidade de serviço pode ser afetada porque se o CSI do recetor não for perfeito, a adição do ruído artificial pode corromper os dados transmitidos para o recetor.

A segurança por chave obriga o transmissor e o recetor a trocar entre si bits redundantes de modo a manterem uma comunicação segura, que poderiam ser utilizados para transmitir dados. Isto reduz tanto a eficiência espectral como a eficiência energética, além de exigir uma capacidade computacional alta e da alocação de recursos no transmissor e no recetor para a geração de chaves, encriptação e desencriptação.

A segurança com base no canal pode ser ineficaz quando o canal mantém-se estático ou quando este exibe elevada correlação entre o recetor autorizado e o eavesdropper.

Assim, decidiu-se optar por um esquema segurança de nível físico com base na diretividade na informação baseado na estrutura de emissão apresentada na secção anterior ou em variantes desta técnica . O seu funcionamento não depende de cenários móveis ou estáticos e não exige grandes recursos e capacidades computacionais. É também bastante flexível, pois funciona com todos os tipos de modulações e não compromete a eficiência espectral nem a eficiência energética.

Nos próximos capítulos irão ser apresentados dois esquemas de segurança: um para Single-Carrier e outro adequado ao Multi-Carrier. No Capítulo 3, referente a transmissão do tipo Single-Carrier, é implementada uma segurança por diretividade da constelação. O sinal que se quer transmitir irá entrar num decompositor onde o símbolo

transmitido em cada instante é decomposto em componentes, cuja fase e amplitude são alterados com o intuito de introduzir segurança. Para testar a performance deste sistema foram realizadas simulações ao nível da BER e da IM com recurso ao Matlab. No Capítulo 4, referente a transmissão do tipo Multi-Carrier, é implementada a segurança introduzindo uma quantização da envolvente e sua decomposição em componentes e posterior inversão de fase. Também é analisado o desempenho deste sistema ao nível da BER, IM e adicionalmente são também incluídos resultados relativos ao EVM obtido.

3

Segurança por diretividade da constelação

Já foi mencionado que a segurança nas camadas superiores pode não ser o suficiente para garantir secretismo para um utilizador autorizado. Neste Capítulo é estudada a implementação de um esquema de segurança na camada física, adequado a sistemas mono-portadora. É de salientar ainda que, este esquema de segurança de nível físico pode ser implementado paralelamente aos esquemas de segurança garantidos pelas camadas superiores.

Por conseguinte, este esquema de segurança será baseado na diretividade da informação garantida pela estrutura do emissor. O objetivo é dividir a constelação do símbolo M-QAM transmitido em várias componentes do mesmo, por forma a poder alterar a fase e amplitude de cada componente da constelação. Para testar a performance do método proposto, serão realizadas no Matlab simulações que irão descrever os níveis de BER e os níveis de IM.

Na secção 3.1 é apresentada a estrutura e a configuração do esquema de segurança proposto.

Na secção 3.2 são apresentados resultados de desempenho obtidos por simulações em Matlab, que demonstram a viabilidade do esquema proposto como uma solução de segurança para o nível físico.

3.1 Estrutura e configuração do sistema

O sinal transmitido x(t) é do tipo SC e é gerado com os bits transmitidos sendo mapeados por $\{S_1, S_2, \dots, S_M\}$ símbolos, é utilizado como input seguindo a regra $\left(\beta^{(\mu-1)}, \beta^{(\mu-2)}, \dots, \beta^{(2)}, \beta^{(1)}\right) \mapsto s_n$, com $\left(\beta^{(\mu-1)}, \beta^{(\mu-2)}, \dots, \beta^{(2)}, \beta^{(1)}\right)$ indicando a representação binária de cada símbolo s_n com $\mu = \log_2(M)$ bits. De seguida os símbolos da constelação são decompostos por M componentes polares, seguindo a regra

$$\begin{aligned} s_n &= g_0 + g_1 b_n^{(1)} + g_2 b_n^{(2)} + g_3 b_n^{(1)} b_n^{(2)} + g_4 b_n^{(3)} + \cdots \\ &= \sum_{i=0}^{M-1} g_i \prod_{m=0}^{\mu-1} \left(b_n^{(m)}\right)^{\gamma_{m,i}} \end{aligned} \tag{3.1}$$

onde $(\gamma_{\mu,i}, \gamma_{\mu-1,i}, \dots, \gamma_{2,i}, \gamma_{1,i})$ designa a representação binária de i e $b_n^{(m)} = (-1)^{\beta_n^{(m)}}$ é a representação polar do bit $\beta_n^{(m)}$. No caso dos coeficientes g_i serem reais obtém-se uma decomposição em componentes BPSK com M_m amplitudes distintas. Quando os

coeficientes g_i são complexos, obtém-se uma decomposição em componentes QPSK ou OQPSK de amplitudes distintas.

Estas componentes podem ser combinadas antes de serem transmitidas para o canal, conforme se pode ver na estrutura da Figura 3.1. Outra alternativa consiste na estrutura do transmissor da Figura 3.2, no qual cada uma das componentes é enviada separadamente por uma antena, sendo a combinação das componentes realizada ao nível do canal. Utilizando múltiplas antenas resulta numa menor interferência entre utilizadores, melhorando assim o desempenho na segurança e na qualidade de serviço.

A segurança pode ser obtida através da manipulação da fase em cada componente, ou mediante uma alteração simultânea da fase e amplitude de cada componente, que pode ser realizada de forma independente.

Assim, à medida que se aumenta a ordem da constelação M-QAM usada, maior será o número de componentes resultantes da sua decomposição, o que resultará numa maior complexidade de segurança no sistema, pois maior será o número de combinações possíveis.

As alterações de fase e amplitude de cada componente serão apenas conhecidas pelo transmissor e recetor, ou seja, mesmo que um utilizador não autorizado descubra a ordem de modulação M-QAM utilizada na transmissão do sinal, terá ainda dificuldade em descobrir as inúmeras combinações possíveis das componentes do sinal.

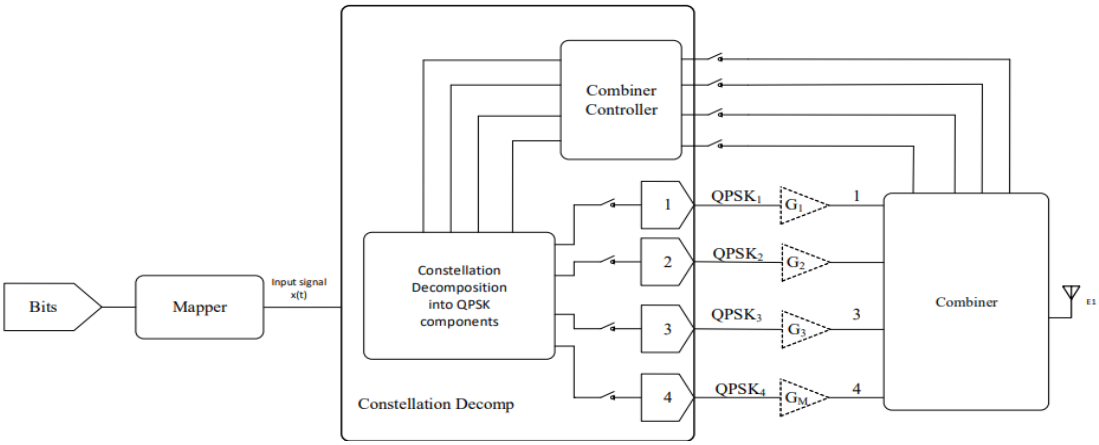

Figura 3.1- Configuração do Decompositor com combinador

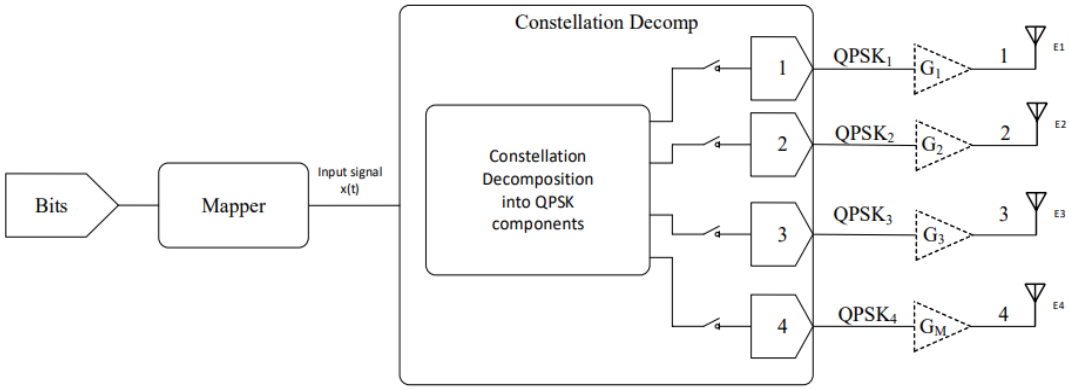

Figura 3.2- Configuração do Decompositor com antenas para cada componente

Cada componente é uma parte do símbolo transmitido, sendo o número de componentes QPSK e OQPSK dado por $Log_4 M$ e por $Log_2 M$ no caso da decomposição em componentes BPSK. Obviamente que a maneira como cada uma das componentes vai ser alterada é apenas conhecida pelo transmissor e pelo recetor.

Nas figuras 3.3 a 3.6 é possível ver o efeito de uma rotação de fase nas diversas componentes QPSK na constelação resultante da combinação destas componentes alteradas. No que diz respeito ao 64-QAM, este é decomposto em 3 componentes QPSK com energias distintas, sendo a primeira componente $\pm 1 \pm j$, a segunda componente $\pm 2 \pm 2j$ e a terceira igual a $\pm 4 \pm 4j$. Nas figuras 3.3, 3.4, 3.5 e 3.6, é apresentado o efeito na constelação com um desvio de fase de 45º numa das componentes e/ ou em todas as suas componentes.

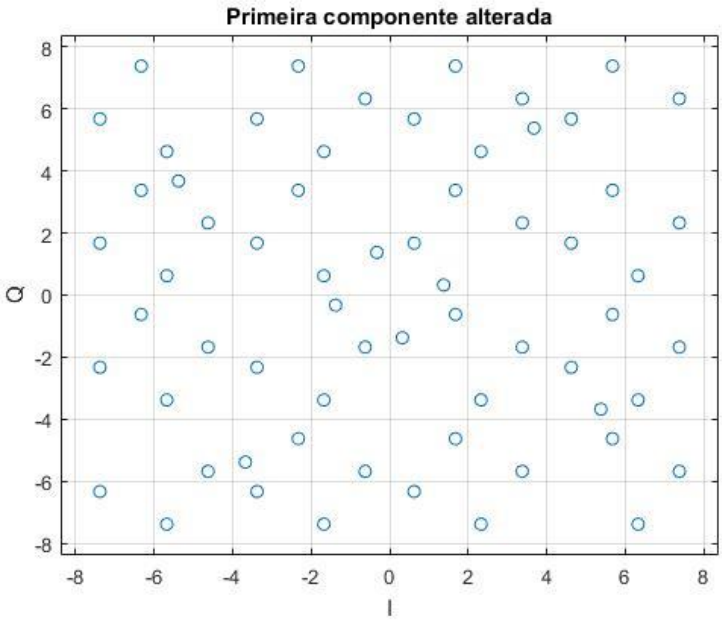

Figura 3.3 - Constelação 64 QAM com a sua primeira componente alterada

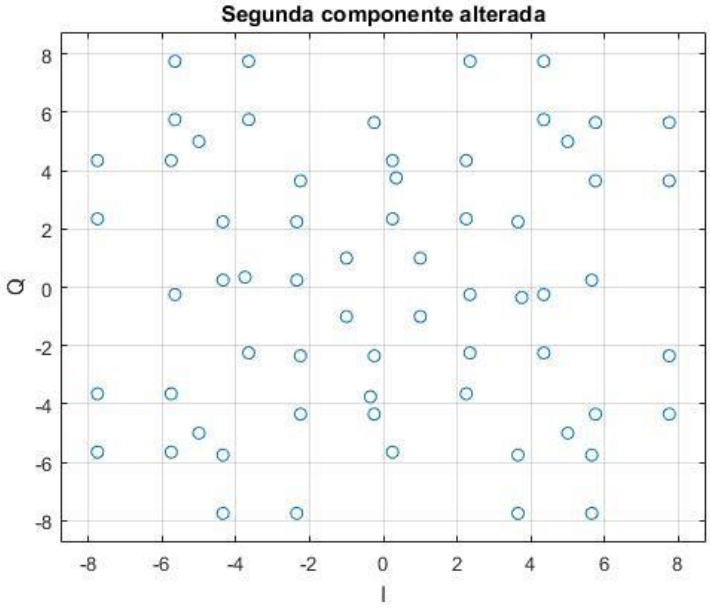

Figura 3.4- Constelação 64 QAM com a sua segunda componente alterada

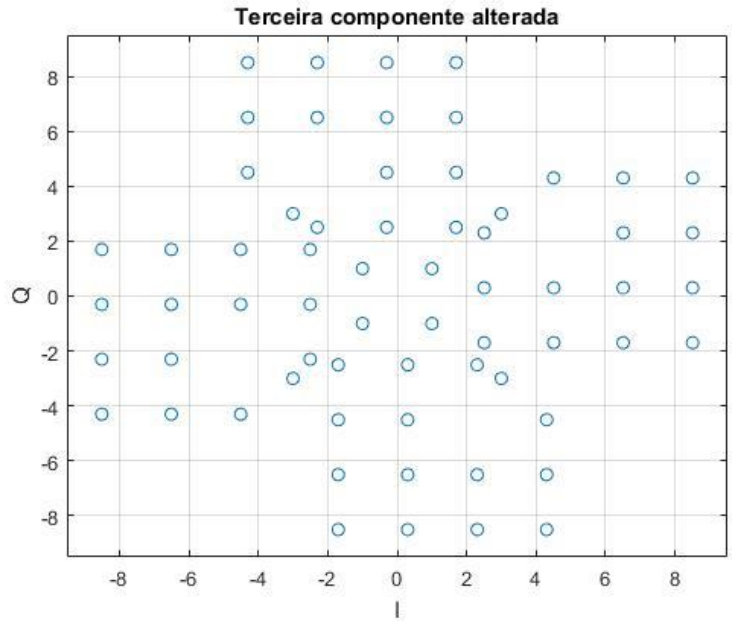

Figura 3.5- Constelação 64 QAM com a sua terceira componente alterada

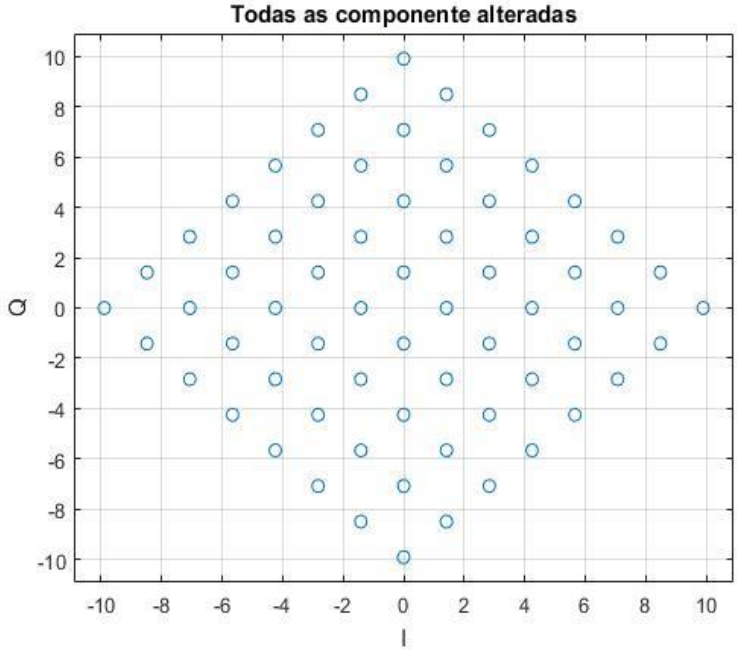

Figura 3.6- Constelação 64 QAM com todas as componentes alterada

Como pode ser observado nas figuras 3.3, 3.4, 3.5 e 3.6, as rotações de fase das componentes do sinal têm efeitos distintos na constelação resultante, podendo assim equivaler a diferentes níveis de segurança.

Assim sendo, e por forma a melhor exemplificar a aplicação deste método, vamos considerar um sistema de transmissão SC-FDE com três terminais composto por um transmissor, um utilizador autorizado (Bob), e um utilizador não autorizado (Eve), onde o transmissor deseja comunicar uma mensagem privada S para o Bob utilizando o esquema de segurança de nível físico apresentado.

Para tal, o sinal $x(t)$ transmitido é gerado de acordo com o mapeamento dos bits de dados transmitidos em símbolos $\{s_n$; n = 0, 1, …, N-1}, onde s_n é selecionado de acordo com a regra de mapeamento duma constelação adequada do tipo M-QAM e que corresponde a uma amplitude complexa associada ao n-ésima símbolo do bloco. Para um esquema SC-FDE convencional $\{S_k$; k = 0, 1, …, N-1} representa o bloco de dados no domínio da frequência. Na presença de canais dispersivos no tempo, é adicionado um prefixo cíclico ao bloco que consiste numa extensão periódica da parte útil do bloco, isto é $s_n = s_{N-n}$com uma duração maior que o atraso máximo ou delay spread máximo do canal. Aplicando alterações de fase e amplitude, ao nível do canal obtém-se um sinal modificado s_n'.

No que diz respeito ao recetor, as amostras associadas ao prefixo cíclico são descartadas, o que significa que não existe IBI (Inter Block Interference) e reduz o impacto dum canal dispersivo no tempo para um fator de escala para cada frequência. Nestas condições o sinal recebido é descrito por

$$y_n' = s_n' * h_n + n_n \tag{3.2}$$

onde h_n corresponde à resposta impulsiva do canal e n_n ao ruído do canal no n-ésimo símbolo do bloco transmitido. Em relação ao sinal y_n', este é sujeito a uma DFT de forma a se obter o bloco no domínio da frequência correspondente do tipo $\{ Y_k'; k = 0,1, \dots, N-1 \} = DFT \{y_n'; n = 0,1, \dots, N-1\}$, onde

$$Y_k' = S_k' H_k + N_k, \tag{3.3}$$

com H_k sendo a resposta a nível da frequência no canal para o k-ésima sub-portadora e N_k sendo o ruído do canal correspondente.

Por forma a avaliar o desempenho dos níveis de segurança no contexto apresentado, isto é, no contexto do sistema de transmissão composto pelo transmissor e os dois recetores (onde apenas um dos recetores está autorizado), será introduzido o conceito de Informação Mútua (IM), para que possa ser feita a comparação entre os dados recebidos pelo utilizador autorizado (Bob) e o não autorizado (Eve).

A IM (assumindo símbolos equiparáveis) para um dado sinal '$\mathfrak{S}$' quantifica a informação (em bits) que uma constelação contém em relação a outra, e pode nestas condições ser escrita como

$$\mathrm{I(s,y)} = log_2 M - \frac{1}{M}\sum_{s\in\mathfrak{S}} E_n \left[log_2 \left(\sum_{{s'}_n\in\mathfrak{S}} \exp\left(-\frac{1}{N_0}\left|\sqrt{E_s}(s_n - {s'}_n) + w_n\right|^2 - |w_n|^2\right)\right)\right], \quad (3.4)$$

onde E indica o valor esperado e w_n o ruído no domínio do tempo. Com perfeito secretismo tem-se I(s, y)= 0, com *s* sendo a mensagem enviada, *y* a mensagem recebida pela Eve e I(s;y) a IM.

Na secção 3.2 apresenta-se um conjunto de resultados relativos a esta técnica de segurança, incluindo-se resultados de desempenho como o BER e a IM.

3.2 Desempenho e resultados

Para avaliar o desempenho em termos de segurança deste esquema foram obtidos por simulação os resultados de BER e a IM. Assume-se que o utilizador não autorizado ou eavesdropper, denominado a partir de agora por Eve conhece as constelações originais e partilha o mesmo canal que o recetor autorizado denominado por Bob. Também se assume que o Bob, e a Eve têm um conhecimento perfeito do canal, e um sincronismo temporal e de fase perfeitos.

3.2.1 Informação Mútua

Os resultados da IM foram obtidos através de 1000 ensaios independentes de Monte Carlo com um canal AWGN (Additive White Gaussian Channel). Os símbolos são selecionados de uma constelação M-QAM (com dimensões de M = 16, 64 e 256). Os resultados da IM são expressos com função de $\frac{E_b}{N_0}$, onde ${N_0}/{2}$ é a variação do ruído e E_b é a energia dos bits transmitidos.

À semelhança da secção anterior, as constelações 16-QAM são decompostas em duas componentes QPSK $\pm 1 \pm j$ e $\pm 2 \pm 2j$. As constelações 64-QAM são decompostas em 3 componentes, com a primeira componente $\pm 1 \pm j$, a segunda componente $\pm 2 \pm$

$2j$ e a terceira igual a $\pm 4 \pm 4j$. Já as constelações 256-QAM têm uma quarta componente dada por $\pm 8 \pm 8j$.

Os resultados referem-se a duas configurações distintas.

Na primeira consideraram-se alterações de fase iguais para todas as componentes QPSK do sinal, correspondendo desta forma a uma rotação da constelação. Para 16 e 64-QAM são considerados valores $\theta = 5º, 10º, 15º \; e \; 20º$. Para 256-QAM, os valores considerados são $\theta = 1º, 2º, 3º, 4º, 5º, 10º, 15º \; e \; 20º$.

Das figuras pode-se verificar que para valores baixos de SNR o efeito do ruído é predominante sendo o sistema de transmissão para o eavesdropper similar a um canal do tipo AWGN. Com o aumento SNR aumenta a influência dos desvios de fase e a IM será afetada por estes mesmo efeitos. Por exemplo, na figura 3.7 referente ao 16-QAM é notório que para 20 graus a IM atinge um pico nos 2 dB e partir daí decresce até ser quase nula. O mesmo comportamento se pode verificar para 64-QAM na figura 3.8 com a diferença que acontece logo a partir dos 10 graus e para 256-QAM na figura 3.9 onde este comportamento ocorrer a partir dos 4 graus.

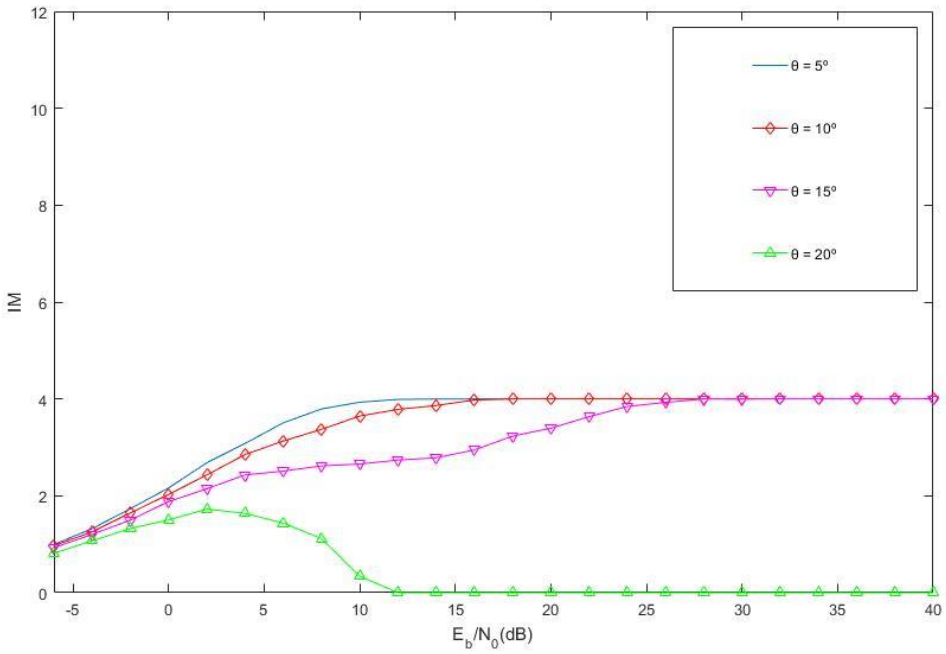

Figura 3.7 - Evolução da IM no eavesdropper para 16-QAM com alteração na fase em todas as componentes

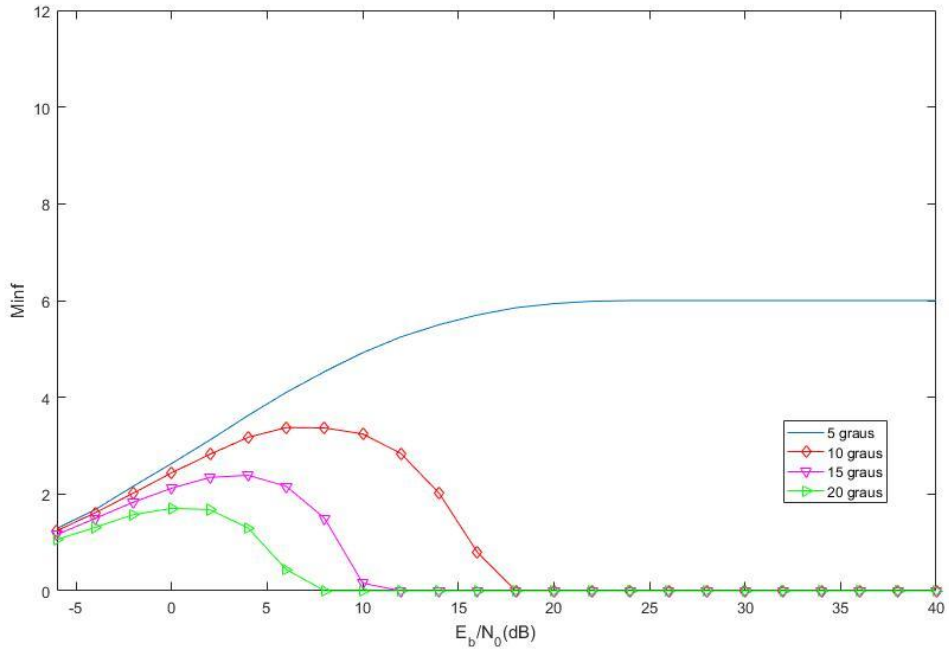

Figura 3.8 - Evolução da IM no eavesdropper para 64-QAM com alteração na fase em todas as componentes

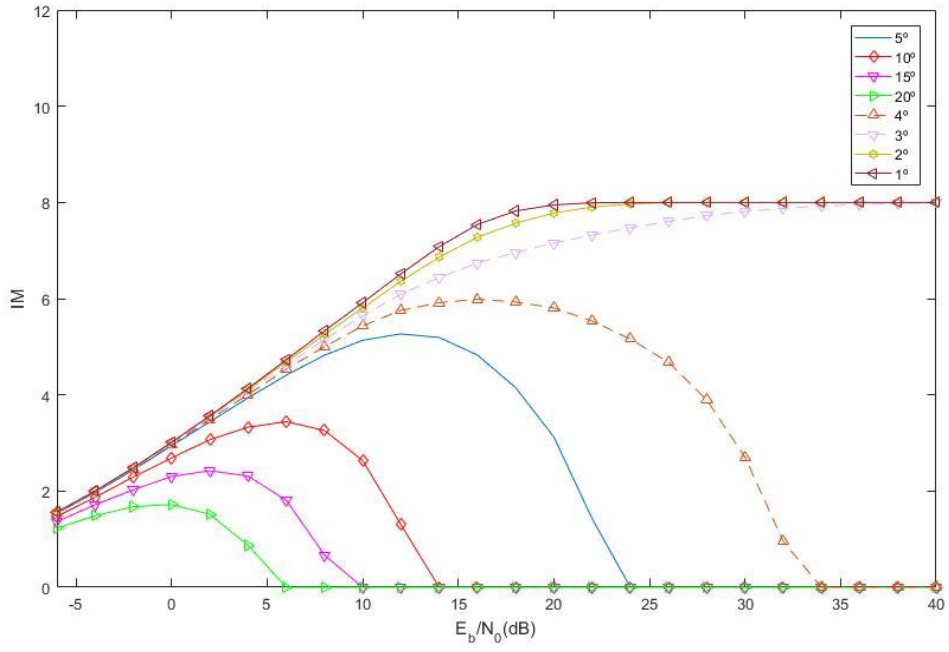

Figura 3.9 - Evolução da IM no eavesdropper para 256-QAM com alteração na fase em todas as componentes

Na segunda configuração alteram-se quer as fases quer as amplitudes. Agora os desvios de fase são distintos para as diferentes componentes em que o sinal sofreu alterações de fase e de amplitude. Para o 16-QAM, considera-se a tabela 3.1 para os desvios de fase das componentes do sinal, sendo que cada linha representa um sinal e cada coluna a sua componente respetiva. Além disso, houve uma atenuação na amplitude das componentes, sendo a primeira componente atenuada em 10% e a segunda componente em 20%. Os resultados obtidos são apresentados na figura 3.10.

	1º Componente	2º Componente
θ	5º	3º
θ	5º	10º
θ	10º	5º
θ	5º	10º
θ	10º	20º
θ	20º	10º

Tabela 3.1 - Desvios de fase para 16-QAM

Para o 64 e 256-QAM, considera-se a tabela 3.2 e 3.3 respetivamente para os desvios de fase das componentes do sinal. Sendo que novamente cada linha representa um sinal e cada coluna a sua componente. Além disso houve uma atenuação na amplitude das componentes, sendo a primeira componente atenuada em 10% e a segunda componente em 20% e a terceira componente por 30%. Os resultados obtidos são apresentados na figura 3.11 para o 64-QAM e na figura 3.12 para o 256-QAM.

	1º Componente	2º Componente	3º Componente
θ	1º	2º	3º
θ	1º	3º	5º
θ	2º	5º	10º
θ	5º	3º	1º
θ	5º	10º	15º
θ	10º	5º	2º
θ	10º	15º	20º
θ	15º	10º	5º
θ	20º	15º	10º

Tabela 3.2 - Desvios de fase para 64-QAM

	1º Componente	2º Componente	3º Componente	4º Componente
θ	1º	2º	3º	4º
θ	1º	2º	4º	5º
θ	2º	4º	5º	10º
θ	2º	5º	10º	12º
θ	4º	3º	2º	1º
θ	5º	4º	2º	1º
θ	10º	5º	4º	2º
θ	12º	10º	5º	2º

Tabela 3.3 - Desvios de fase para 256-QAM

Nos casos onde se alteraram as fases das componentes de forma distinta e as amplitudes, nota-se na figura 3.10, referente ao 16-QAM, que a IM tem um pico nos 6dB e a partir desse valor começa a decrescer até 0 quando se altera a primeira componente

por 10 graus e a segunda por 20 graus. Contudo o mesmo não acontece, quando se altera a primeira componente por 20 graus e a segunda por 10 graus. Nos resultados obtidos para 64-QAM e 256-QAM e representados nas figuras 3.11 e 3.12, a IM apresenta novamente o mesmo tipo de comportamento, ou seja, tem na maioria dos casos um pico até começar a decrescer até 0. Tal como era esperado, quanto maior o tamanho da constelação maior será a sensibilidade da IM aos desvios de fase e alterações amplitude, e consequentemente melhor será o nível de segurança obtido.

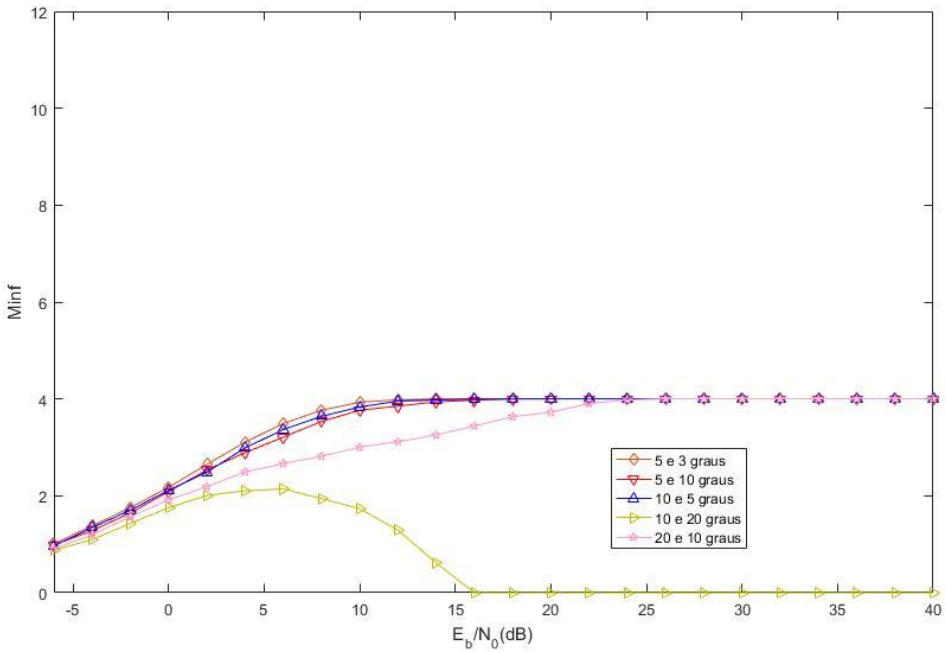

Figura 3.10 - Evolução da IM no eavesdropper para 16-QAM com alteração na fase e peso de forma diferente para cada componente

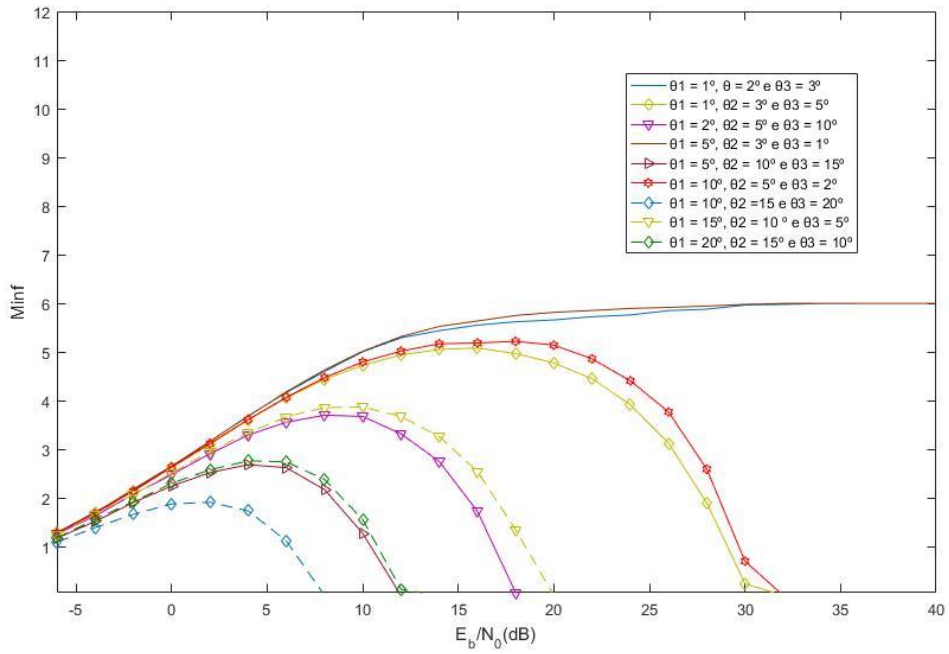

Figura 3.11 - Evolução da IM no eavesdropper para 64-QAM com alteração na fase e peso de forma diferente para cada componente

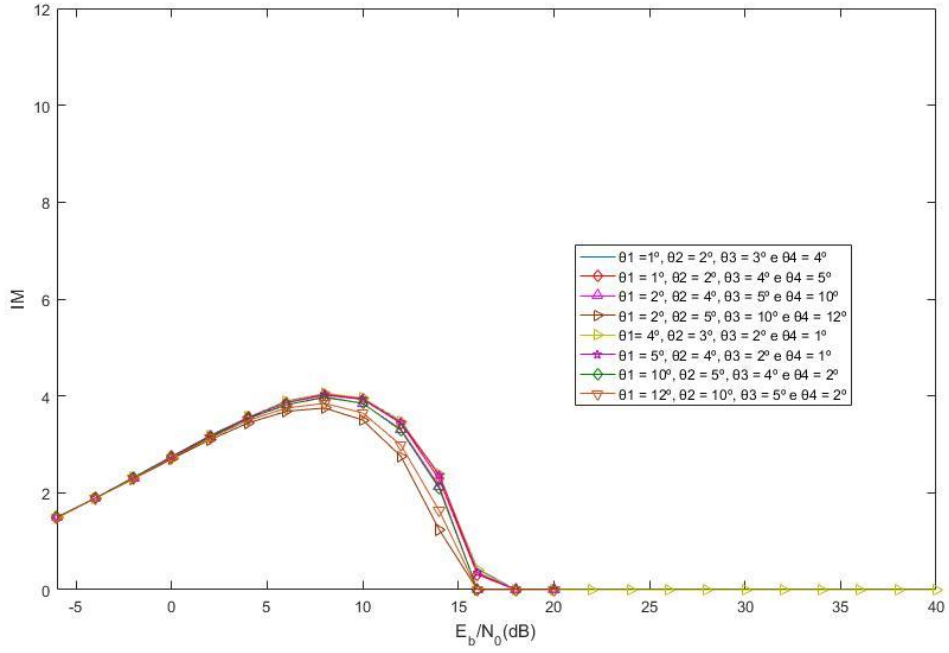

Figura 3.12 - Evolução da IM no eavesdropper para 256-QAM com alteração na fase e peso de forma diferente para cada componente

3.2.2 Performance de BER

Nesta secção vai-se avaliar os valores de BER nas várias modulações e diferentes seguranças implementadas. Estes resultados foram obtidos para um canal do tipo AWGN. Novamente, considera-se que o eavesdropper tem conhecimento do tipo de constelação utilizado em cada transmissão, sem ter no entanto conhecimento dos atrasos em fase e das alterações de amplitude de cada componente. Os símbolos transmitidos podem pertencer a constelações M-QAM, com M = 16, 64 e 256. O cálculo da BER utiliza 1000 ensaios de Monte Carlo independentes para obter resultados médios com relevância estatística.

As figuras 3.13, 3.14 e 3.15 mostram resultados de BER para os quais houve uma alteração igual de fase em todas as componentes, ou seja, houve uma alteração de fase na constelação completa. É possível observar que a BER vai sendo cada vez maior como pretendido com o aumento dos desfasamentos aplicados. Também é de notar que quando o tamanho da constelação aumenta, os valores da BER também aumentam. Aliás isto já seria de esperar atendendo ao decrescimento do valor da IM com o aumento da constelação e número de componentes. Pode-se observar na figura 3.13, referente ao 16-QAM, que a partir dos 20 graus os valores de BER começam a ser superiores a 10^{-1}. O mesmo comportamento se observa nas figuras 3.14 e 3.15, referentes a 64 e 256-QAM respetivamente. A partir de 10 graus no 64-QAM, a BER começa a ter valores superiores a 10^{-1} e o mesmo acontece para 256-QAM a partir de 4 graus.

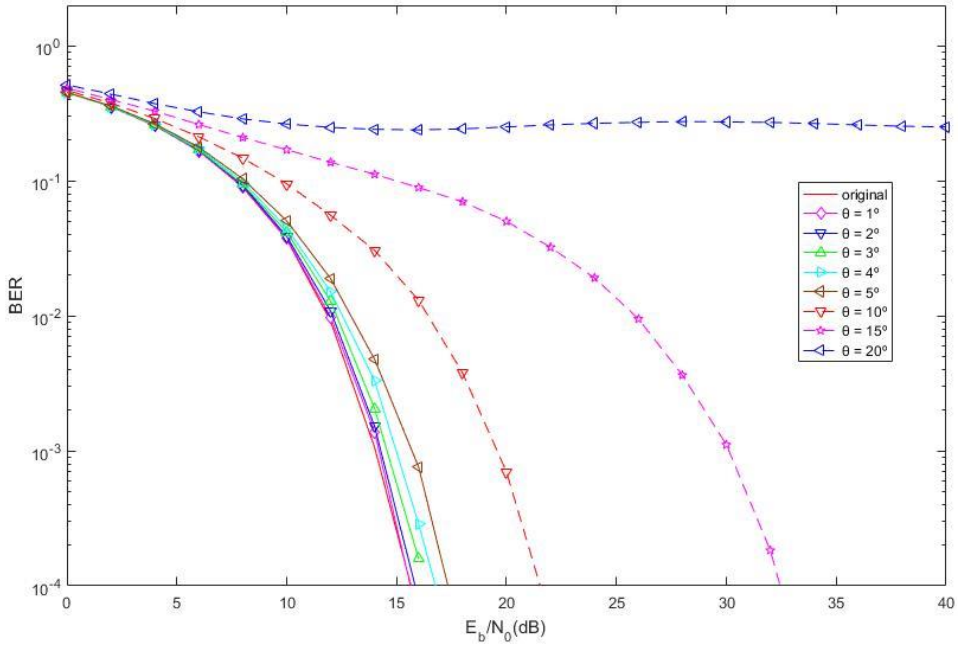

Figura 3.13 - BER performance para 16 QAM com alteração na fase em todas as componentes

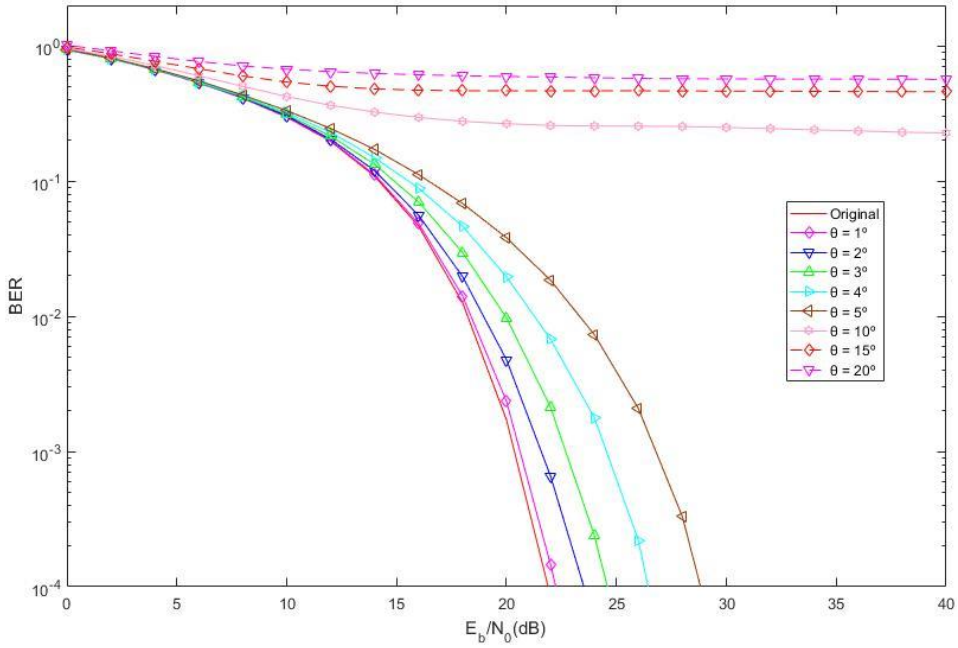

Figura 3.14 - BER performance para 64 QAM com alteração na fase em todas as componentes

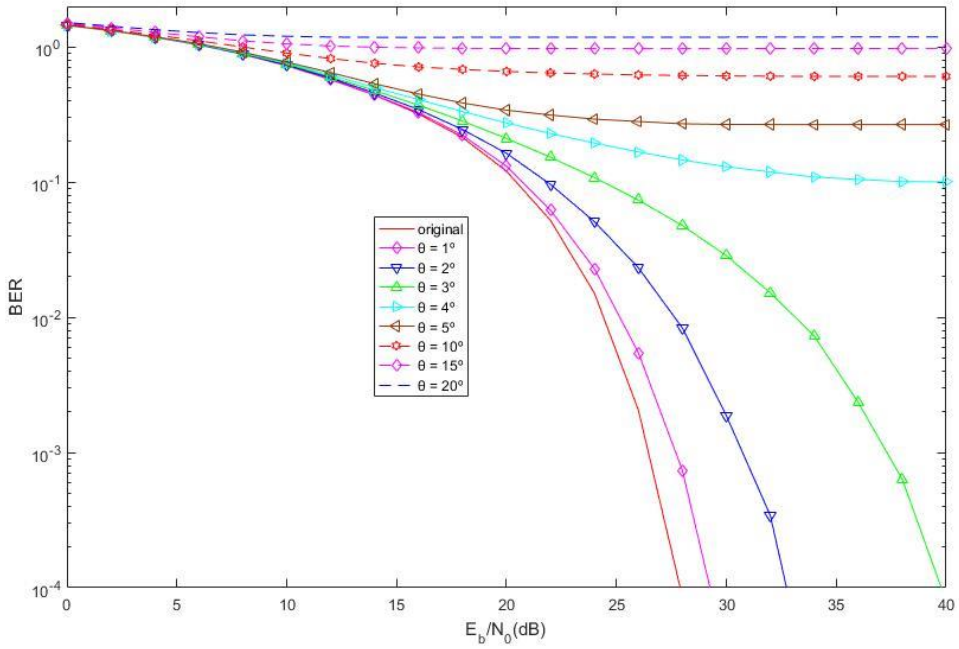

Figura 3.15 - BER performance para 256 QAM com alteração na fase em todas as componentes

As figuras 3.16, 3.17 e 3.18 mostram resultados de BER onde as componentes em que cada símbolo é decomposto são afetadas por desvios de fase distintos juntamente com uma alteração de amplitude. Em todas as figuras, a curva contínua a vermelho representa o resultado da BER obtido na ausência de qualquer alteração de fase ou de amplitude das componentes, e que serve de termo de comparação para os casos onde se pretende obter segurança.

Pode-se observar no 16 QAM que a BER se degrada conforme pretendido quando se altera as fases de forma diferente em cada uma das suas componentes com valores entre os 10º e 20º (neste caso a BER é plana e assume um valor acima de 10^{-1}, o que torna a descodificação impossível). Observa-se também em todos os valores de M que quanto mais dispersos forem as alterações nas componentes melhores são os resultados em termos de BER.

É possível observar na figura 3.16, para 16-QAM os valores de BER tornam-se superiores a 10^{-1} quando se altera ambos os valores por mais de 10 graus. Para 64 e 256-QAM os valores de BER são maiores que $5x10^{-1}$ quando se alteram todas as

componentes por pelo menos 1 grau, o que significa uma taxa de erro de 50%, ou seja, uma segurança perfeita. Aliás, a IM tende para zero nestes casos.

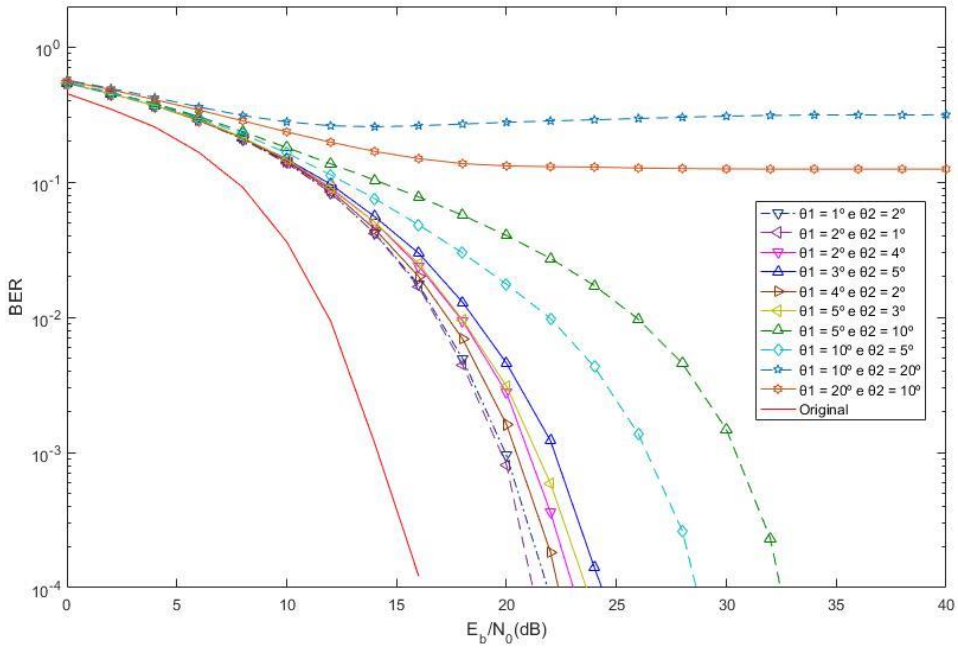

Figura 3.16- BER performance para 16-QAM com alteração na fase e peso de forma diferente para cada componente

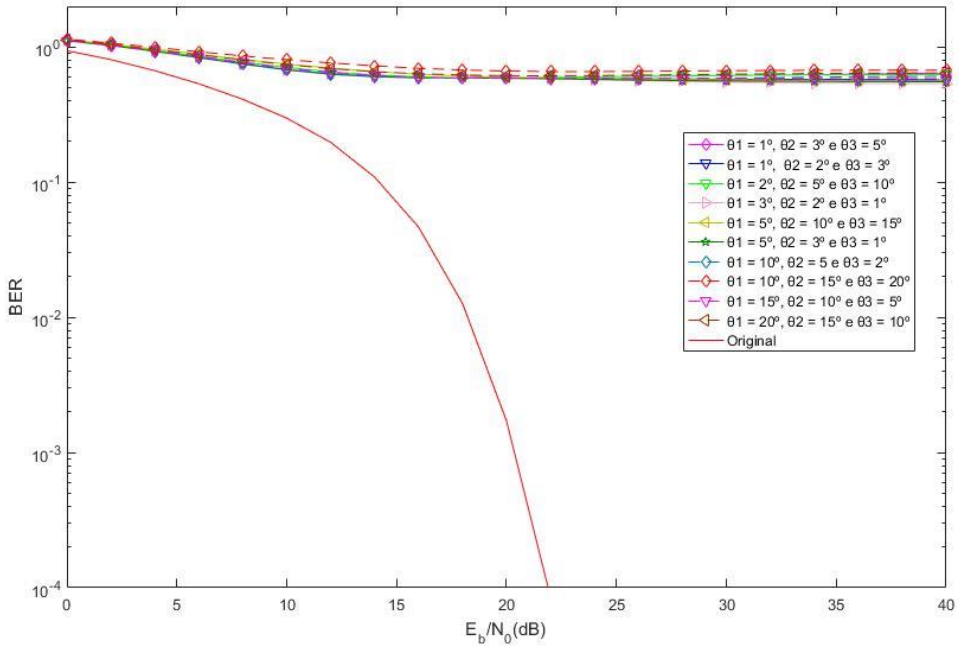

Figura 3.17 - BER performance para 64-QAM com alteração na fase e peso de forma diferente para cada componente

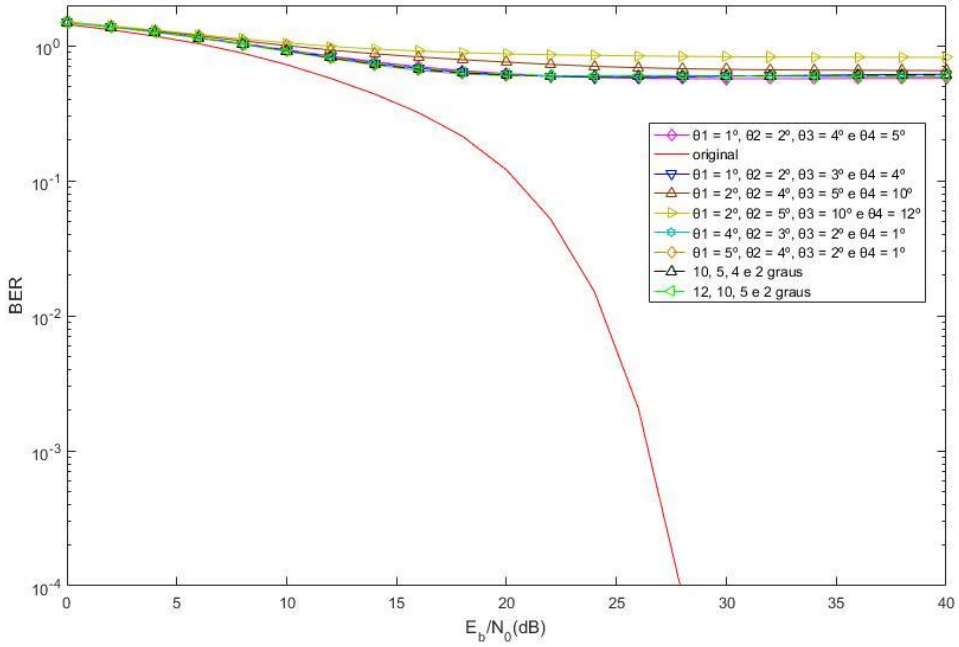

Figura 3.18 - BER performance para 256-QAM com alteração na fase e peso de forma diferente para cada componente

4

Segurança em sistemas Multi Carrier

Já se referiu que os sistemas de comunicações móveis são sistemas do tipo broadcast, no sentido em que o canal é partilhado por todos os utilizadores, o que torna difícil impedir que os sinais transmitidos sejam intercetados por utilizadores não autorizadas e levar a sobreposição de vários sinais no recetor [17]. Logo, a segurança é crucial neste tipo de sistemas. Neste capítulo é apresentada a segunda técnica de segurança da camada física que para além de não comprometer a eficiência espetral e não usar bits redundantes, não baixa a eficiência energética. Esta técnica de segurança de nível físico baseia-se no método QDA que pode ser aplicado na amplificação de esquemas OFDM que são utilizados na transmissão nos sistemas de comunicações móveis atuais.

A técnica e os resultados apresentados neste Capítulo, fazem parte do manuscrito de um artigo científico Mendes *et. al* 2021 "Quantized digital amplification physical layer security schemes" submetido para a MILCOM Conference 2021.

4.1 Análise de segurança

A transmissão do tipo MC, é um tipo de transmissão que possui várias portadoras. Mais concretamente, no OFDM adotado no 4G e 5G, consiste em dividir os dados que se quer transmitir pelas várias por N sub-portadoras ortogonais entre si.

O esquema de segurança apresentado neste capítulo utiliza o QDA que transforma qualquer sinal numa soma de componentes de sinais de PAPR (Peak-to-Average Power Ratio) nula, sendo isto um resultado de um processo de quantização. O QDA resolve o problema de eficiência energética que o 4G e o 5G trazem, pelo facto de exigirem altos ritmos binários que são apenas possíveis com elevadas larguras de banda combinadas com modulações de elevada eficiência espectral. Esta combinação leva a uma elevada PAPR, trazendo consequências para a eficiência do processo de amplificação

O QDA abre a possibilidade de utilizar amplificadores computados ao nível das componentes geradas, evitando distorções não lineares, resultando numa melhor eficiência energética. De seguida, as componentes amplificadas são combinadas a partir de um combinador. Neste caso, a eficiência será dada a partir do produto da média da eficiência dos amplificadores pela eficiência do combinador. Para além da eficiência energética associada, o QDA também permite segurança de nível físico através, de uma

mudança da operação do mapeamento através de inversões de polaridade das componentes geradas. Logo, o transmissor QDA tem uma segurança embebida que pode ser utilizada.

Outra desvantagem em constelações de elevada ordem consiste na sensibilidade aos efeitos de canais dispersivos. Esquemas do tipo OFDM são excelentes esquemas para sistemas de comunicação móveis com um custo baixo a nível de transmissores permitindo também uma complexidade baixa a nível de recetor, dada a simplicidade da compensação dos efeitos do canal.

Nas restantes secções do presente capítulo será apresentado e caracterizado este tipo segurança de nível físico baseado no conceito de QDA aplicado a sinais OFDM.

4.2 Estrutura e configuração do sistema

De seguida passa-se a descrever a estrutura típica de emissão associada ao QDA. O sinal transmitido x(t) é do tipo OFDM e é gerado da seguinte forma: os bits de dados transmitidos são mapeados em símbolos $\{S_k; k = 0, 1, \ldots, N-1\}$, onde S_k é selecionado de acordo com a regra de mapeamento duma constelação adequada do tipo M-QAM e que corresponde a uma amplitude complexa associada ao k-ésima sub-portadora. Para um esquema OFDM convencional $\{S_k; k = 0, 1, \ldots, N-1\}$ representa o bloco de dados no domínio da frequência. De seguida, é calculado o seu IDFT (Inverse Discrete Fourier Transform) de modo a conseguir obter as amostras no domínio do tempo $\{s_n; n = 0, 1, \ldots, N-1\}$ do sinal x(t). Na presença de canais dispersivos no tempo, é adicionado um prefixo cíclicos ao bloco que consistem numa extensão periódica da parte útil do bloco, isto é $s_{-n} = s_{N-n}$com uma duração maior que o atraso máximo ou delay spread máximo do canal.

A estrutura do transmissor pode ser vista na Figura 4.1, e é composta por um bloco quantizador com N_{bq} bits de quantização que quantiza as amostras do sinal transmitido x(t), um bloco de mapeamento que converte os bits em N_{bq} componentes polares que serão moduladas como sinais BPSK que serão depois amplificados por N_{bq} amplificadores. Os sinais BPSK correspondentes são amplificados cada um pelo seu próprio amplificador antes de serem combinados no combinador inteligente como apresentado na Figura 4.1. Outra possibilidade consiste na combinação feita através no

ar, onde o combinador inteligente seria substituído por antenas diretamente conectadas a cada amplificador. Neste caso evitam-se quaisquer perdas de combinação sendo a eficiência energética igual à média das eficiências dos amplificadores comutados. No transmissor QDA são realizados os seguintes passos:

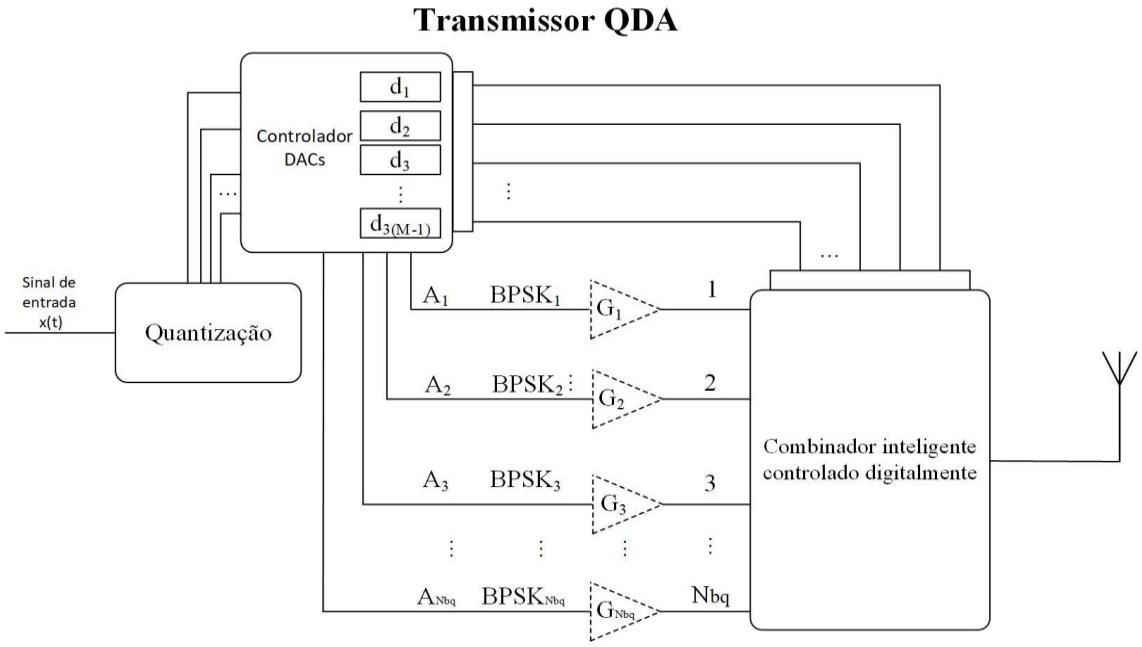

Figura 4.1 - Configuração QDA simulada

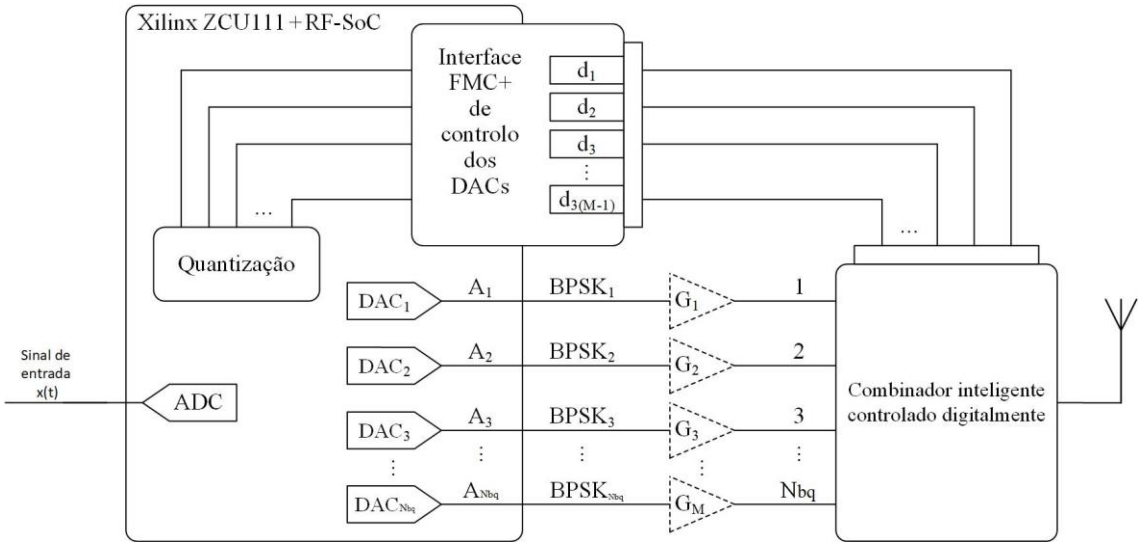

Figura 4.2 - Configuração do protótipo QDA

1. Quantização: As amostras do sinal x(t) são quantizadas num quantizador uniforme com N_{bq} bits de quantização e $Q = 2^{N_{bq}}$ níveis, que é representado

por um função não-linear h(·). Para minimizar o erro de quantização, é considerado uma resolução M como "clipping level" otimizado. A quantização da n-ésima amostra resulta uma palavra digitalizada com um conjunto de bits representados por $b_n = \left\{b_{n,1}, b_{n,2}, \dots, b_{n,N_{bq}}\right\} = h(x_n)$. Estes bits de quantização são usados para definir conjuntos de bits de controlo adicionais $(c_{n,1}, c_{n,2}, \dots, c_{n,3(N_{bq}-1)})$ que são usados para controlar os blocos funcionais do QDA, nomeadamente: (i) Controlar os N_{bq} conversores DAC (Digital-to-Analog Converter) que constam no protótipo representado na figura 4.2, que são responsáveis por gerar os diferentes componentes do sinal que serão amplificados e combinados. (ii) Para controlar o On/Off dos amplificadores que são necessários em cada momento para amplificar as componentes do sinal que resultam da decomposição de cada valor quantizado. (iii) Finalmente para controlar o combinador inteligente e para selecionar os componentes que são utilizados em cada instante para combinar e para aumentar ao máximo a eficiência da sua combinação.

2. Geração de Componentes: A estrutura QDA utiliza amplificadores comutados. Isto significa que o conjunto de componentes do sinal gerado em cada um dos conversores DAC são sinais de envolvente constante. O conjunto de componentes do sinal em que cada valor quantizado é decomposto pelos conversores DAC pode ser visto como um conjunto componentes BPSK com pesos ou amplitudes distintas. Portanto, em cada ramo, cada conversor DAC produz componentes com amplitudes diferentes, com uma soma igual à potência desejada para o valor quantizado da amostra dada. A componente BPSK produzida pela m-ésimo conversor DAC é definida por

$$s_m(t) = A_m \sin(2\pi f_c t + \phi_m), \tag{4.1}$$

onde f_c é a frequência da portadora, $A_m = \sqrt{k_{(2^m-1)} \times P}$ (sendo P a potência "base" em Watts (W)), e $\phi_m$representa a fase em cada componente. Deve-se notar que ϕ_m tanto pode ter o valor de 0 ou π, de acordo com o sinal da amostra do quantizador.

3. Andar de amplificação: O conjunto de N_{bq} amplificadores em paralelo é utilizado entre os processos de geração do sinal e a combinação do sinal. Como se pode verificar na Figura 4.1, cada ramo de amplificação tem o seu próprio amplificador, que é especificamente concebido e otimizado para a potência correspondente da componente BPSK do seu ramo. Visto que todas as

componentes do sinal são de envolvente constante, são usados amplificadores comutados com diferentes níveis de potência e que trabalham sempre no ponto ótimo, correspondente à eficiência máxima. Devido à envolvente constante não é introduzida distorção pelos amplificadores. Nestas condições os N_{bq} amplificadores de potência podem ser modulados como ganhos que afetam as componentes, pelo que genericamente o ganho do m-ésimo amplificador de potência pode ser representado por G_m.

O "Digitally Controlled Smart Combiner" que se encontra na Figura 4.1 representa a fase da combinação inteligente digitalmente controlada. Ora, o processo de quantização produz uma palavra digital que controla a combinação das componentes do sinal BPSK. Ao utilizar $N_{N\,bq}$ bits, $Q = 2^{N_{bq}}$ combinações diferentes podem ser geradas.

O sinal produzido na combinação no n-ésimo instante, considerando a palavra digital b_n, pode ser descrito pela seguinte fórmula

$$y_n(t) = \sum_{m=1}^{N_{bq}} b_{n,m} G_m \, s_m(t) \tag{4.2}$$

Logo, o sinal o sinal combinado ao longo do tempo pode ser representado por

$$y(t) = \sum_{n=-\infty}^{+\infty} y_n(t - nT_s) \tag{4.3}$$

Para além do objetivo de amplificar de forma eficiente o sinal OFDM através dum conjunto de amplificadores de potência altamente eficazes, o sinal combinado descrito por (4.3) deve ser o mais próximo possível do sinal x(t), de modo a que a quantização tenha o mínimo de influência na performance no sistema de transmissão. Na realidade, a diferença entre o y(t) e x(t) é principalmente devido ao ruído relacionado com a quantização de N_{bq} bits que define a resolução do quantizador N_{bq}.

Existem várias maneiras de implementar segurança a nível físico com o QDA. A primeira, e a mais simples, consiste em inverter a polaridade dos valores quantizados das amostras resultantes a cada N_i amostras, onde o espaçamento N_i entre os valores quantizados invertidos das amostras podem ser fixos ou pode mudar consoante uma regra aleatória. Uma outra opção encontra-se em inverter as fases de uma ou mais componentes BPSK em que os valores quantizados são decompostos. A desvantagem deste método reside no fato de haver uma complexidade adicional na parte de recetor. A terceira opção é através da combinação feita no ar, utilizando os DACs para introduzir mudanças de fase entre as várias antenas conectadas aos amplificadores de forma a introduzir diretividade na envolvente do sinal. Todas estas opções podem ser utilizadas

em conjunto para uma solução de várias camadas de proteção a nível físico, sem comprometer a eficiência energética ou a eficiência espectral. Neste trabalho apenas se considerou a primeira opção.

Portanto, quando uma inversão de fase é aplicada para todos as componentes de um sinal BPSK, o mapeamento no n-ésimo instante de tempo do sinal produzido pode ser escrito da seguinte maneira

$$y'_n(t) = \sum_{m=1}^{N_{bq}} b_{n,m} G_m s_m(t) e^{j\psi n}, \tag{4.4}$$

onde ψ indica a mudança da inversão de fase de π ciclicamente aplicada numa amostra em em cada sub-conjunto de N_i amostras da envolvente quantizada do sinal x(t).

Vamos considerar um sistema com três terminais composto por um transmissor, o utilizador autorizado (Bob), e um utilizador não autorizado, Eve, onde o transmissor deseja comunicar uma mensagem privada S para o Bob utilizando o esquema de segurança do QDA com inversão de fase. No recetor OFDM, as amostras associadas ao prefixo cíclico são descartadas, o que significa que não existe IBI (Inter Block Interference) e reduz o impacto dum canal dispersivo no tempo para um fator de escala para cada frequência. Assim, para o correspondente o bloco no domínio da frequência é $\{ Y'_k; k = 0,1, \dots, N-1 \}$ = DFT ($y'_n; n = 0,1, \dots, N-1\}$), onde

$$Y'_k = S'_k H_k + N_k, \tag{4.5}$$

com H_k sendo a resposta a nível da frequência no canal para a subportadora k e N_k sendo o ruído do canal correspondente.

A IM (assumindo símbolos equiparáveis) para um dado sinal '$\mathfrak{S}$' quantifica a informação (em bits) que uma constelação contém em relação a outra, e pode nestas condições ser escrita como

$$\mathrm{I(S,Y)} = log_2 M - \frac{1}{M} \sum_{s \in \mathfrak{S}} E_n \left[log_2 \left(\sum_{S'_k \in \mathfrak{S}} \exp\left(-\frac{1}{N_0} \left| \sqrt{E_s}(S_k - S'_k) + N_k \right|^2 - |N_k|^2 \right) \right) \right], \tag{4.6}$$

onde E indica a expectativa e N_k o ruído no domínio da frequência. Com perfeito secretismo nós temos I(S, Y)= 0, com S sendo a mensagem enviada, Y a mensagem recebida pela Eve e I(;) a IM.

4.3 Desempenho e resultados

Para avaliar os efeitos da inversão de fase em amostras cíclicas na segurança a nível físico, são considerados agora três indicadores de performance. O primeiro consiste na IM. O segundo é o EVM obtido para os diferentes valores de N_i. O terceiro é a BER. Assume-se que a Eve conhece as constelações e o número de sub-portadoras usadas pelo sinal OFDM e partilha o mesmo canal que o Bob (esta hipótese é irrealista sob canais com fading, mas elimina a influência que o canal tem em relação à segurança alcançada). Também se assume que o recetor Bob e o eavesdropper Eve têm perfeito conhecimento do canal, e sincronismos de fase e temporal perfeitos.

4.3.1 Informação Mútua

Os resultados da IM foram obtidos através de 1000 ensaios independentes de Monte Carlo com um canal AWGN. Em cada ensaio a parte útil do bloco OFDM é igual ao tamanho da constelação, com todos os símbolos possíveis da constelação. Os símbolos S_k são selecionados de uma constelação M-QAM (com dimensões de M = 4, 16, 64 e 256). Os resultados da IM são expressos como função de $\frac{E_b}{N_0}$, onde $N_0/2$ é a variação do ruído e E_b é a energia dos bits transmitidos. A periocidade N_i entre as inversões de fase muda com o tamanho da constelação. Para 4-QAM N_i tem valores de 2 e 4. Para estes valores a IM para a Eve é sempre nula, logo há um secretismo perfeito. Para 16-QAM são considerados os valores $N_i = 2,4,8$ e 16. Para 64-QAM e 256-QAM, os valores que N_i pode tomar são 32 e 64, respetivamente.

As figuras 4.3 e 4.4 mostram o comportamento da IM em relação ao SNR para esquemas de 16 e 64-QAM. Os resultados da IM mostram que, independentemente do tamanho da constelação, para valores de $N_i \leq 8$ a Eve é incapaz de descodificar com sucesso a informação transmitida. O mesmo comportamento acontece para $N_i \leq 32$ no caso do 256-QAM. As inversões de fase em conjunto com o DFT (Discrete Fourier Transform) têm um impacto similar em termos de distorção na constelação transmitida, que foi introduzida por um canal não linear com uma característica AM/AM e AM/PM não nula. É claro que a IM foi afetada severamente para todos os tamanhos de

constelação pelo efeito da inversão da fase e a DFT. Para valores baixos de SNR o efeito do ruído é predominante sendo que o sistema de transmissão para o eavesdropper é similar a um canal do tipo AWGN. Para valores mais elevados de SNR a influência da distorção de fase torna-se mais significativa e o efeito que traz para a IM correspondente redução torna-se mais notável. Isto pode ser evidenciado na curva da IM para $N_i = 8$ no 16-QAM, que alcança o seu pico por volta dos 9 dB e partir desse valor decresce. O mesmo comportamento se pode verificar para 64-QAM e 256-QAM nas figuras 4.4 e 4.5, onde a IM mostra novamente um pico até começar a decrescer para valores mais altos da SNR. Como esperado, a maior a sensibilidade face a distorções de fase das constelações de ordem mais elevada justifica o impacto mais forte deste esquema nos valores da IM para 64 e 256-QAM.

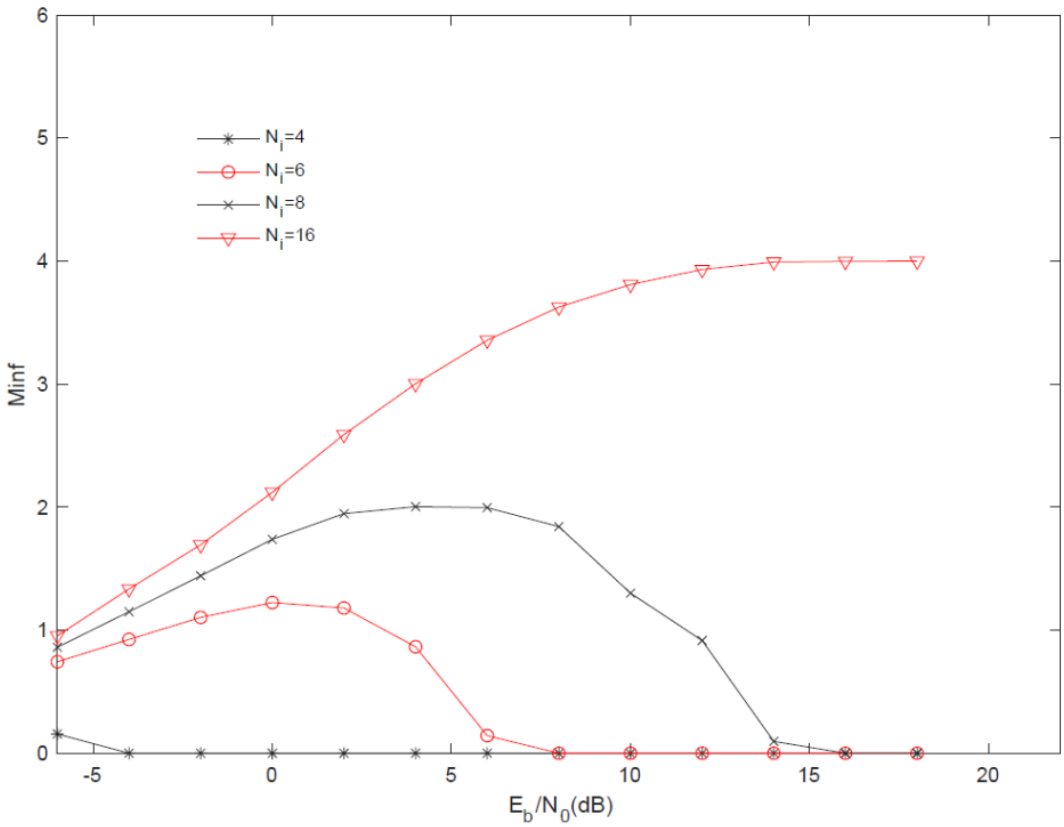

Figura 4.3 - Evolução da IM para 16-QAM no eavesdropper

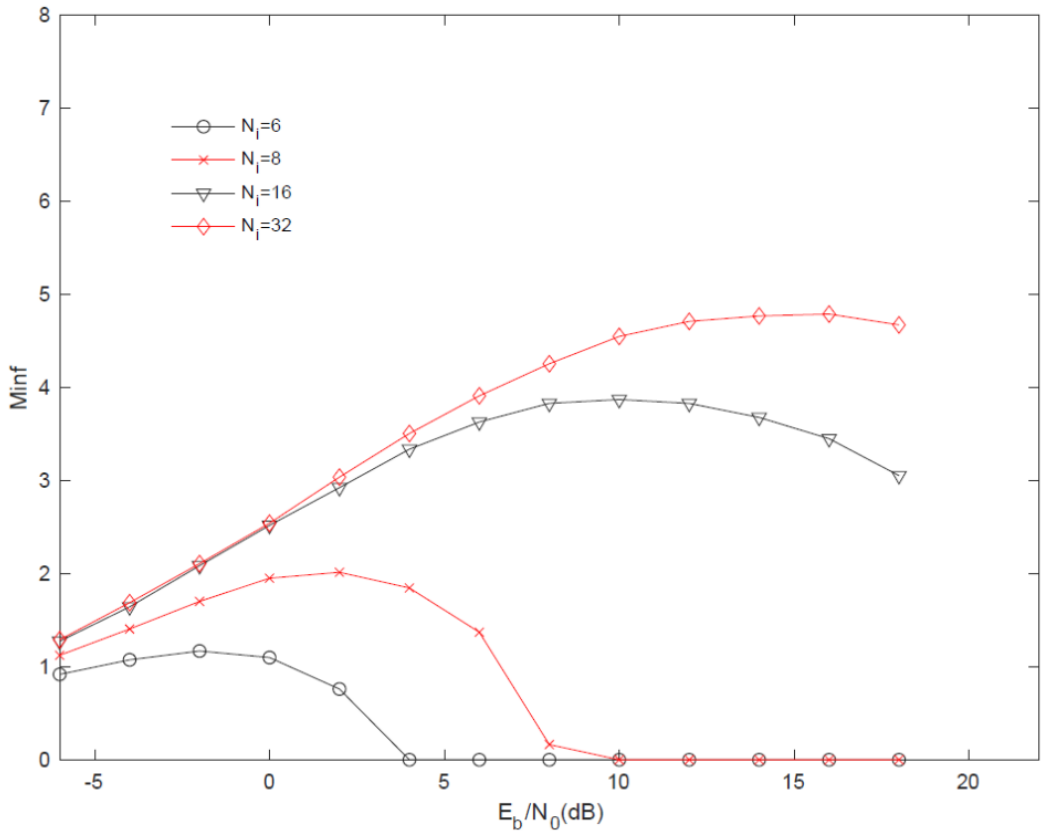

Figura 4.4 - Evolução da IM para 64-QAM no eavesdropper

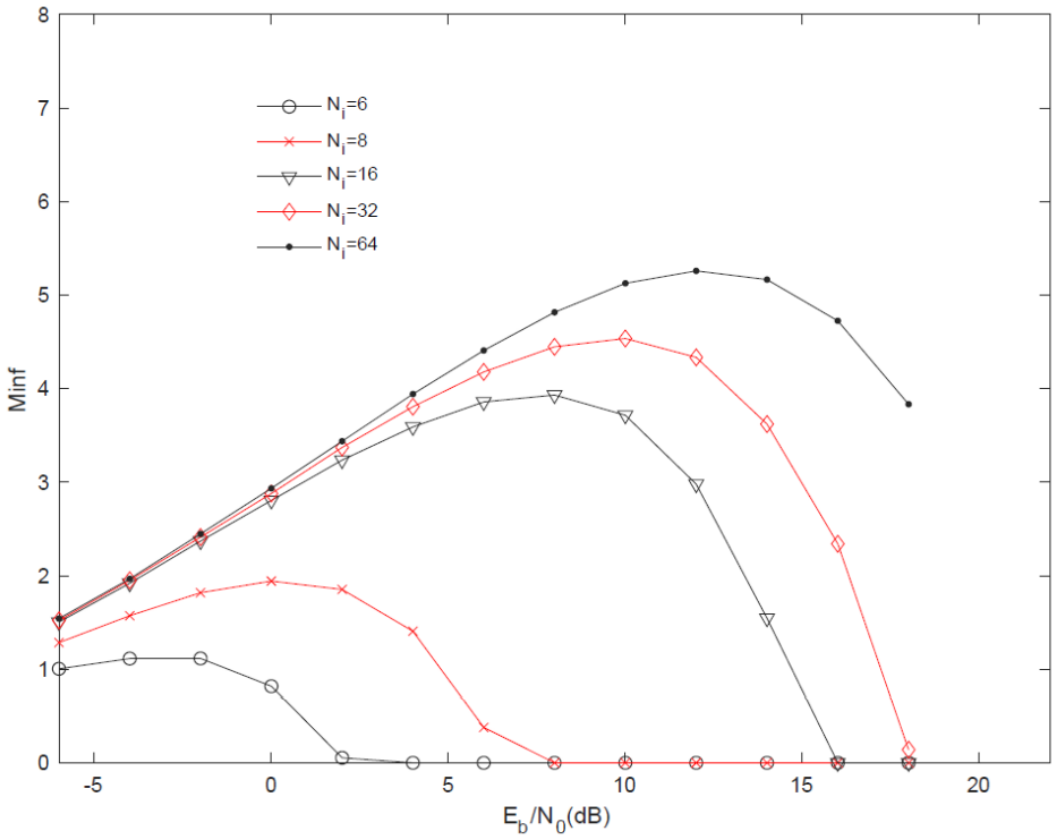

Figura 4.5 - Evolução da IM para 256-QAM no eavesdropper

4.3.2 Performance de BER

Os resultados de BER consideram-se canais do tipo AWGN. É de notar que a BER em canais dispersivos do tipo rayleigh tem comportamentos semelhantes aos do canal AWGN (por esta razão não se considerou este tipo de canal). Assume-se que o eavesdropper Eve tem sincronização perfeita de tempo e frequência. A Eve também tem conhecimento do tamanho do bloco OFDM e do tipo de constelação utilizado em cada transmissão. No entanto, Eve não tem conhecimento acerca das inversões de fase feitas no QDA e a periodicidade destas também é desconhecida. Os símbolos pertencem a uma constelação M-QAM (com dimensões de M = 4, 16, 64 e 256). Assume-me também que a amplificação de potência linear do QDA realizada no transmissor é baseada num quantizador com 6 bits, ou seja, 6 ramos de amplificação. O cálculo da BER e EVM utiliza

1000 ensaios de Monte Carlo independentes para obter resultados médios com relevância estatística.

A tabela 4.1 mostra os resultados do EVM para as inversões de fase com diferentes valores de periodicidade N_i ($N_i = 0$ corresponde aos casos sem alguma inversão de fase). O EVM representa a diferença entre a voltagem complexa esperada de um símbolo desmodulado e o valor do símbolo recebido. Enquanto o BER dá uma decisão binária simples em relação ao erro de um bit, o EVM é uma medida de erros entre os símbolos quantificados e os símbolos esperados [23]. Dois valores diferentes de EVM são apresentados. Os resultados EVM_1 referem-se à média do valor EVM que resultou de 1000 ensaios com a parte útil dos blocos OFDM igual ao tamanho da constelação e no qual ocorrem todos os símbolos possíveis na constelação. EVM_2 são os resultados obtidos com uma parte útil dos blocos OFDM com um tamanho N=16M sendo M o tamanho da constelação e uma geração aleatória dos bits e consequentemente dos símbolos que são selecionados a partir de uma constelação M-QAM. Da tabela 4.1 pode-se observar que ambos os resultados de EVM estão em conformidade com os resultados anteriores de IM. O EVM para os valores de $N_i = 2{,}4$ e 8, terão um impacto grande para a performance da BER do sistema e justifica também a razão dos valores baixos de IM obtidos para estes mesmos casos, até para constelações de ordem baixa. Para valores de $N_i = 16\ e\ 32$, há um impacto baixo no secretismo para constelações de ordem baixa como 4 e 16-QAM, isto porque os valores de EVM nestes casos estão pertos dos valores de EVM definidos em várias normas. Contudo, os valores de EVM têm um grande impacto nos valores de performance de BER para qualquer valor de N_i para constelações 64 e 256-QAM. 16-QAM deverá também ser afetada para valores de N_i até 8.

N_i	EVM_1	EVM_2
0	1.43%	1.26%
2	144.13%	137.51%
4	78.06%	68.80%
8	32.60%	33.90%
16	14.29%	14.11%
32	11.49%	10.87%

Tabela 4.1 - Valores de EVM com inversões de fase cíclicas

As figuras 4.6, 4.7, 4.8 e 4.9 referem-se aos resultados de BER num canal do tipo AWGN, com blocos de OFDM de tamanho N=16M. O impacto que a inversão de fase tem na performance cresce consoante é são o tamanho da constelação. Nas figuras 4.8 e 4.9 os resultados da BER para 64 e 256-QAM mostram que até para valores de $N_i = 32$ compromete significativamente a BER, e para $N_i = 16$ os valores de BER são sempre superiores a 10^{-2} (para 256 pode-se observar o mesmo comportamento para valores de $N_i = 64$ onde a BER não ultrapassa valores a 6×10^{-2}). Nas figuras 4.6 e 4.7, pode-se observar que os valores de BER são sempre superiores a 10^{-1} para valores de N_i até 4. É de notar que a performance da BER não depende do número de componentes BPSK envolvidos no processo de QDA, porque o efeito da inversão de fase dos valores quantizados e os componentes BPSK correspondentes aos símbolos da constelação estão espalhados ao longo dos símbolos dentro dos blocos devido ao DFT efetuado no OFDM no lado do recetor. É também importante mencionar que o tamanho do bloco não tem qualquer tipo de influência ao nível de secretismo associado.

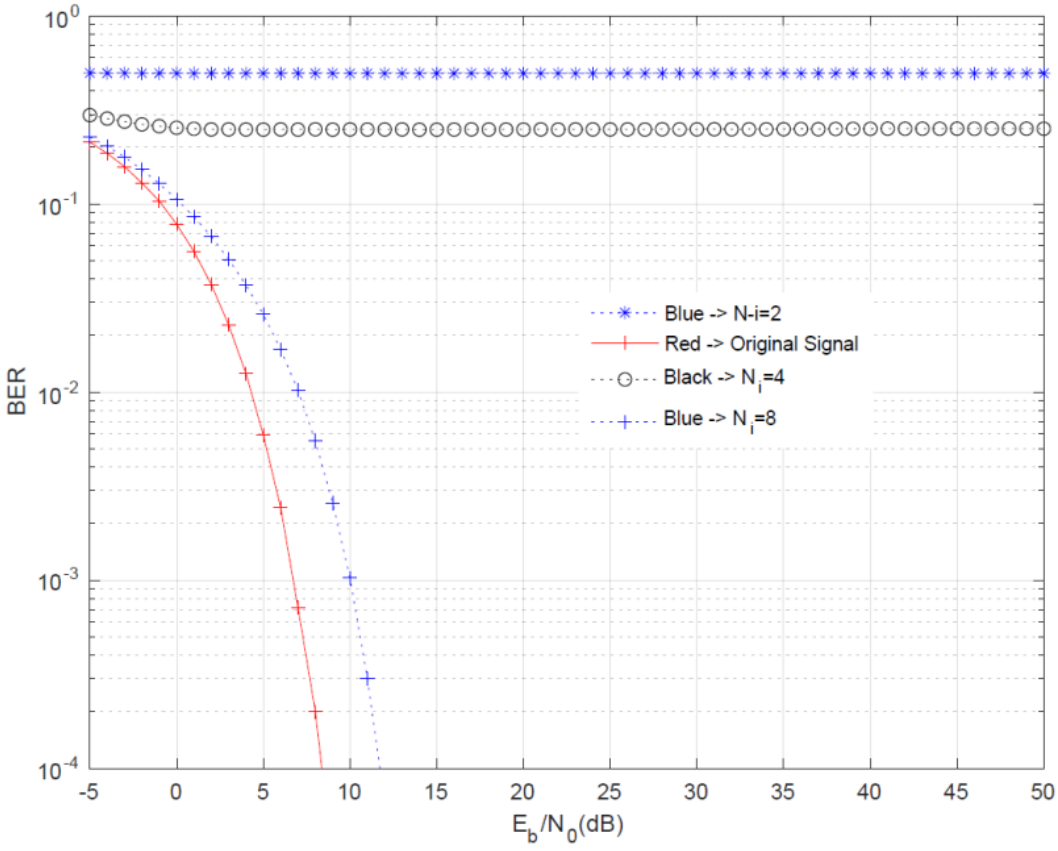

Figura 4.6 - Performance da BER para QPSK com inversões de fase no sinal quantizado

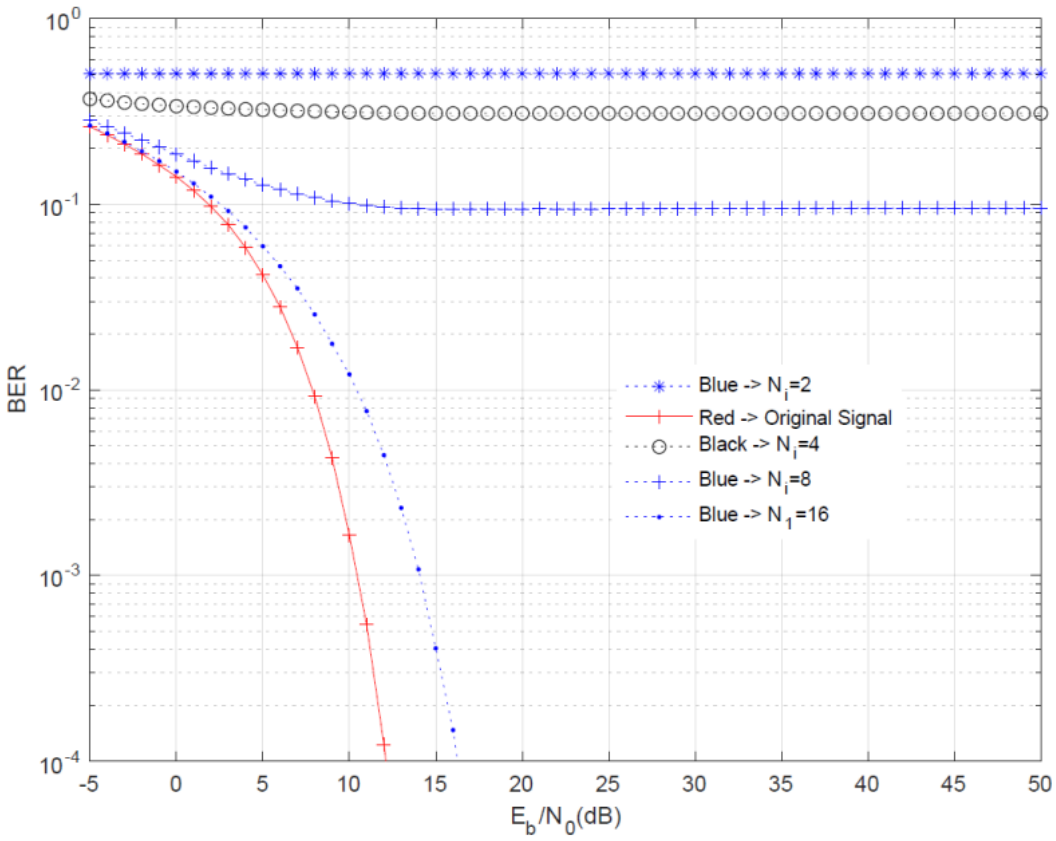

Figura 4.7- Performance da BER para 16-QAM com inversões de fase no sinal quantizado

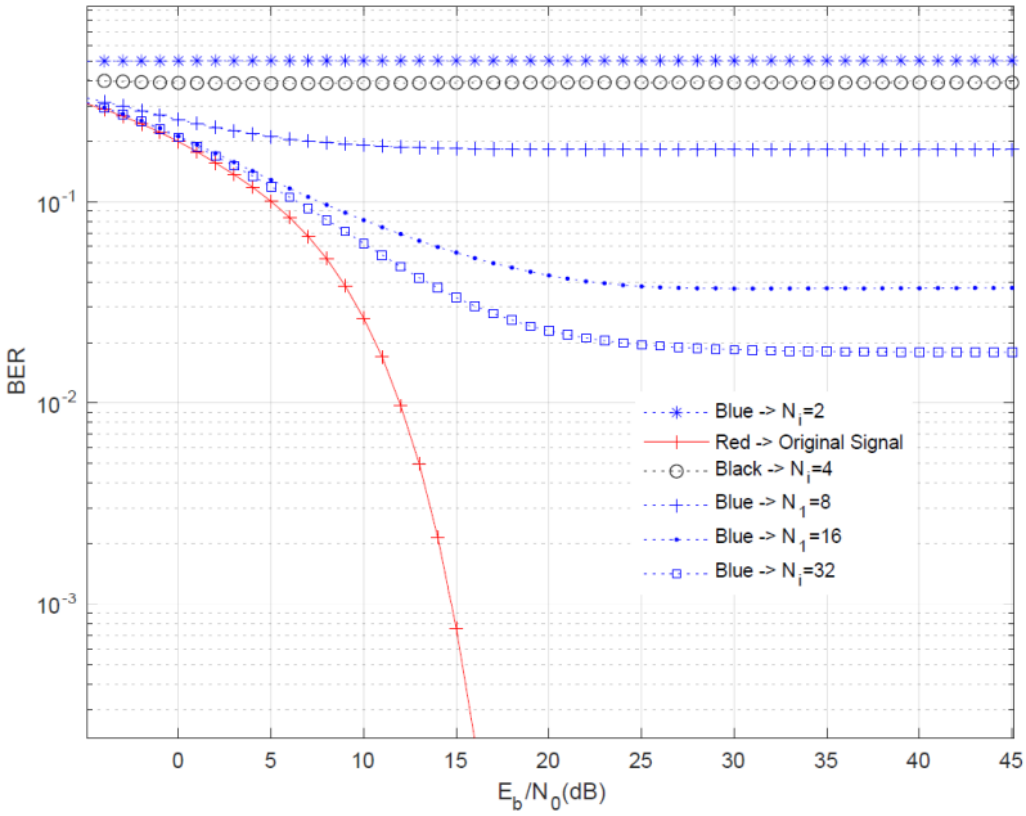

Figura 4.8 - Performance da BER para 64-QAM com inversões de fase no sinal quantizado

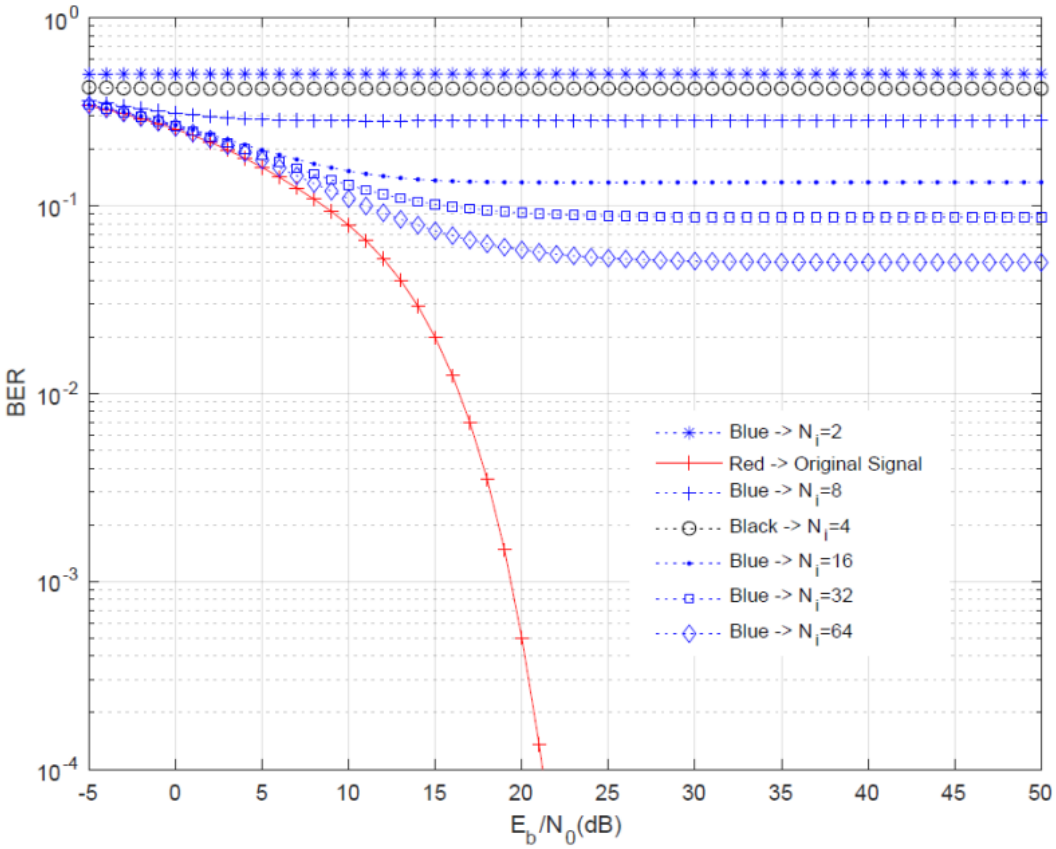

Figura 4.9 - Performance da BER para 256-QAM com inversões de fase no sinal quantizado

A segurança pode ser melhorada ao ser adotada uma regra de inversão de fase onde se seleciona aleatoriamente o espaçamento entre amostras sucessivas. Melhorias adicionais na segurança podem ser alcançadas mudando dinamicamente entre os blocos transmitidos, a ordem das amostras que sofreram uma inversão de fase de acordo com um padrão que será conhecido apenas pelo transmissor e o utilizador pretendido. Quando o QDA é utilizado com combinação feita através do ar, uma solução pode ser implementada na camada física, podendo combinar este esquema de segurança com esquemas de segurança semelhantes como por exemplo os de [24]. Nessa situação em particular, os esquemas de QDA que requerem mais componentes de BPSK vai melhorar no geral a segurança, isto porque a sensibilidade da constelação transmitida para a direção transmitida será também maior.

5

Conclusões

Este trabalho teve como objetivo a implementação de esquemas de segurança no nível físico adequados a sistemas de comunicação móveis. As soluções de segurança focaram-se em estruturas transmissoras baseadas na decomposição dos sinais em várias componentes de envolvente constante e na diretividade da informação. Implementaram-se dois esquemas de segurança adequados para transmissões single-carrier e transmissões de multi-carrier baseados em OFDM. Ambos os esquemas implementados, apesar da baixa complexidade, permitem atingir bons níveis de segurança ao mesmo tempo que é assegurada elevada eficiência energética na amplificação que permite a maximização da eficiência espectral. De forma a validar os esquemas propostos foram realizados testes e simulações relativos ao desempenho e capacidade de secretismo atingíveis.

Primeiramente testaram-se os níveis de BER e de IM no cenário single-carrier. Para introduzir segurança alteraram-se as fases e amplitudes das componentes resultantes da decomposição dos símbolos em sub-constelações. Também foram consideradas constelações 16, 64 e 256-QAM de forma a poder avaliar o impacto da ordem da constelação, na BER e IM.

Verificou-se que consoante se aumentava a fase, os níveis de BER aumentavam e os de IM baixavam. Para determinados valores de fase, a IM tem decréscimos muito acentuados tendendo para 0. Também se notou que um sinal com uma constelação onde se altera uma dada fase θ na componente mais forte tem um comportamento similar ao caso em que se alteram as fases de todas as componentes com o um valor igual de θ. Finalmente observou-se que com o aumento da dimensão da constelação, os valores de fase θ necessários tendem a ser menores para obter os valores de BER e de IMs pretendidos para assegurar um nível de segurança ótimo.

Os mesmos testes foram feitos para os esquemas de segurança com sinais OFDM, com a adição do EVM como parâmetro adicional de desempenho. Neste esquema de segurança foram invertidas as fases das componentes associadas às amostras quantizadas com uma periodicidade N_i entre amostras. Foram igualmente feitos testes com diferentes valores de N_i para QPSK, 16, 64 e 256-QAM. Verificou-se que quanto menor fosse a periodicidade N_i, ou seja quantos mais amostras quantizadas da envolvente se invertiam melhores seriam os resultados de EVM, BER e IM necessários para garantir um bom nível de segurança. Também se verificou que alguns valores N_i garantem um nível de secretismo quase perfeito, nos quais a IM quanto maior fosse a

ordem da constelação adotada ao nível de cada sub-portadora melhor seria o nível de segurança obtido.

Trabalhos futuros devem ter em consideração camada físicas onde se utilizam esquemas baseados QDA combinando as duas opções diferentes que foram mencionadas neste trabalho. Seguranças de camadas superiores onde usam a camada física para complementar a mesma. Finalmente esquemas de melhoria de eficiência energética e aumento da qualidade de serviço como a velocidade da rede móvel podem utilizar esquemas QDA.

Referências

[1] A. D. Wyner, “The wire-tap channel”, Bell Syst. Tech. J., vol. 54, pp. 1355-1387, Oct. 1975.

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

[3] T. Liu, and S. Shamai, “A note on the secrecy capacity of the multiple antenna wiretap channel”, IEEE Trans. Inf. Theory, vol. 55, no. 6, pp. 2547-2553, Jun. 2009.

[4] A. Khisti, and G. W. Wornell, “Secure transmission with multiple antennapart II: the MIMOME wiretap channel”, IEEE Trans. Inf. Theory, vol. 56, no. 11, pp. 5515-5532, Nov. 2010.

[5] X. Chen and L. Lei, "Energy-Efficient Optimization for Physical Layer Security in Multi-Antenna Downlink Networks with QoS Guarantee", Feb 2013.

[6] J. Madeira, J. Guerreiro, R. Dinis, P. Montezuma and L. M. Campos, "On the Physical Layer Security Characteristics for MIMO-SVD Techniques for SC-FDE Schemes", October 2019.

[7] G. Lebrun, J. Gao, and M. Faulkner "MIMO transmission over a time-varying channel using SVD", IEEE Trans. Wirel. Commun. 2005, vol. 4, no. 2, pp. 757–764, March 2005.

[8] J. Guerreiro, R. Dinis, and P. Montezuma, "Analytical Performance Evaluation of Pre-coding Techniques for Nonlinear Massive MIMO Systems with Channel Estimation Errors" IEEE Trans. Commun. 2018, vol. 66, no. 4, pp. 1440–1451, April 2018.

[9] B. He, X. Zhou, and T. D. Abhayapala, "Wireless Physical Layer Security with Imperfect Channel State Information: A Survey", Jul 2013.

[10] E. Jorswieck, A. Wolf, and S. Gerbracht, "Secrecy on the Physical Layer in Wireless Networks", March 2010.

[11] M. I. Husain, S. Mahant, and R. Sridhar, "Physical Layer Security in Wireless Networks through Constellation Diversity", Aug 2011.

[12] E. Ekrem and S. Ulukus, “Secrecy capacity of a class of broadcast channels with an eavesdropper,” EURASIP J. Wireless Comm. and Networking, vol. 2009, June 2009.

[13] C. A. Balanis, "Antenna Theory Analysis and Design", Wiley, New York, 1997.

[14] P. Montezuma, R. Dinis, and M. M. da Silva, "Physical Layer Security Scheme Based on Power Efficient Multi-Antenna Transmitter", July 2015.

[15] 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.

[16] V. Astucia, P. Montezuma, R. Dinis, and M. Beko, "On the use of multiple grossly nonlinear amplifiers for highly efficient linear amplification of multilevel constellations", Proc. IEEE VTC2013-Fall, Las Vegas, NV, US, September 2013.

[17] 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.

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

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

[20] A. Barenghi, L. Breveglieri, I. Koren, and D. Naccache, "Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures", Proc. IEEE, vol. 100, no. 11, pp. 3056-3076, Nov. 2012.

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

[22] S. Gollakota and D. Katabi, "Physical layer wireless security made fast and channel independent", newblockINFOCOM, 2011 Proceedings IEEE, pp. 1125-1133, April 2011.

[23] R. A. Shafik, Md. S. Rahman, A. R. Islam, and N. S. Ashraf, "On the error vector magnitude as a performance metric and comparative analysis", March 2007.

[24] A. Ferreira, G. Gaspar, P. Montezuma and R. Dinis, "Combining info and spatial directivities in multiple antenna transmission systems" , IEEE YEF-ECE 2017, Costa da Caparica, May 2017.