Análise do Impacto de *Jamming* Modulado em Frequência em um Sistema OFDM na Presença de Desvanecimento

Carlos Alexandre Griebler, Ugo Silva Dias

***Resumo*— Este artigo apresenta um estudo da interferência de sinais maliciosos modulados em frequência em um sistema de comunicação baseado em OFDM na presença de um canal com desvanecimento. Por meio de simulações, verifica-se a eficiência de ataques ao sistema OFDM com a utilização de um sinal malicioso facilmente obtido por meio de modulação analógica.**

***Palavras-Chave*— *Jamming*, OFDM, Desvanecimento, Interfência.**

***Abstract*— This article presents an study of interference from malicious frequency modulated signals in a OFDM based communication system under presence of a fading channel. By means of simulations, the efficiency of attacks against the OFDM system with a malicious signal easly obtained by analog modulation is verified.**

***Keywords*— Jamming, OFDM, Fading, Interference.**

I. Introdução

Os principais sistemas de comunicação de dados, como, por exemplo, os padrões IEEE 802.11 [1], 3GPP *Long Term Evolution* (LTE) [2] e o ISDB-T, utilizam a técnica de Multiplexação por Divisão de Frequências Ortogonais (OFDM) na transmissão de sinais digitais. No Brasil, estes padrões representam os serviços de acesso sem fio e móvel à Internet e de televisão. Em vista a isso, ameaças que exploram as fragilidades do OFDM podem comprometer seriamente a comunicação de uma determinada área.

O OFDM é utilizado principalmente por sua robustez às degradações causadas por canais seletivos em frequência, devido à facilidade de equalização no domínio da frequência. Por meio do envio de tons pilotos no sinal, um sistema OFDM é capaz de estimar a resposta do canal para cada subportadora para eliminar os efeitos do canal no sinal. Dessa forma, estes tons pilotos são de grande importância para a confiabilidade do sistema e, sendo assim, a principal forma de se atacar um sistema OFDM é, então, fazer com que os tons pilotos recebidos não reflitam as características do canal, como é mostrado em [3], [4], [5].

Para que o ataque aos tons pilotos seja eficiente, entretanto, é necessário que o interferente (*jammer*) conheça algumas características da transmissão, como a posição dos tons pilotos nos símbolos OFDM e sincronização de frequência. Modelagens de sistemas digitais sendo atacados por *jammers*, como em [5], geralmente, fazem uma abordagem menos detalhada dos componentes e acabam por negligenciar alguns parâmetros dos sistemas, como o desvio de frequência e saturação dos receptores. Deste modo, este trabalho visa investigar os efeitos do desconhecimento de algumas características do sistema a ser atacado por parte do interferente. Para fins de diversidade, o sinal *jammer* será resultado de uma modulação analógica. Assim, é possível avaliar até que ponto o conhecimento dos parâmetros da transmissão é crucial para um ataque efetivo.

As demais partes deste artigo estão divididas da seguinte maneira: o modelo do sistema, incluindo a composição dos sinais, tipo de canal e características da simulação, são apresentados na Seção II. A Seção III traz os parâmetros utilizados na simulação e algumas premissas consideradas no trabalho. Na Seção IV, são apresentados os resultados obtidos nas simulações. E, por fim, as conclusões do trabalho e discussões acerca do tema são feitas na Seção V.

Os autores do texto pertencem ao Departamento de Engenharia Elétrica, Faculdade de Tecnologia, Universidade de Brasília, Distrito Federal, Brasil, e-mails: carlos.griebler@aluno.unb.br, udias@unb.br.

II. Modelo do Sistema

O modelo utilizado neste trabalho busca representar a interferência proposital e maliciosa (*jamming*) de um sinal analógico modulado em frequência (FM) em um sistema OFDM. O sistema modelado apresenta grande parte dos componentes de um sistema de comunicação digital baseado em OFDM, bem como um canal de comunicação com desvanecimento e ruído. A Figura 1 representa o diagrama de blocos do modelo.

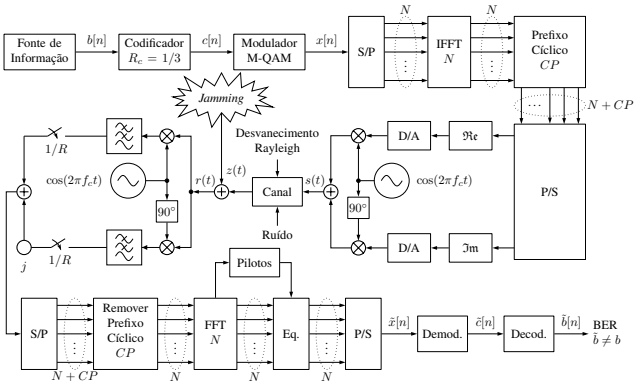

Fig. 1. Diagrama de blocos do sistema de comunicação modelado.

Em um sistema OFDM, a modulação em N portadoras é feita digitalmente por meio da implementação da Transformada Discreta de Fourier Inversa (IDFT), que é computada

por meio do algoritmo de Transformada Rápida de Fourier Inversa (IFFT). Assim, aplicando a IFFT em um conjunto de N símbolos, é gerado um sinal discreto de N pontos representando os símbolos modulados por N subportadoras espaçadas de Δf em que a taxa de amostragem é

$$f_a^{OFDM} = N \cdot \Delta f. \tag{1}$$

O sinal discreto resultante da modulação OFDM é um sinal complexo em banda básica igual a $\frac{N \cdot \Delta f}{2}$. Para simular um sistema em banda passante, é preciso modular o sinal OFDM por meio de uma portadora em fase e outra em quadratura com frequências f_c. Portanto, o sinal OFDM em banda básica deve ser sobreamostrado em R vezes por meio de interpolação, simulando assim o conversor digital-analógico (D/A), e modulado para frequências maiores. O valor de R deve ser tal que a taxa de amostragem total do sistema, f_a, satisfaça o critério de Nyquist. Entretanto, é possível trabalhar com qualquer sinal em banda básica por meio de sua envoltória complexa. Seja $s(t)$ o sinal modulado por uma portadora em f_c e $s_I(t)$ e $s_Q(t)$ suas componentes em fase e em quadratura, respectivamente,

$$s(t) = s_I(t)\cos(2\pi f_c t) + s_Q(t)\sin(2\pi f_c t).$$

A envoltória complexa de $s(t)$ é dada por $\tilde{s}(t)$ tal que

$$s(t) = \mathfrak{Re}\left\{\tilde{s}(t)e^{j2\pi f_c t)}\right\}.$$

Como $\tilde{s}(t)$ é um sinal complexo em banda básica, a taxa de amostragem do sistema e, consequentemente, o número de amostras necessárias são muito menores. Assim, o sinal OFDM será sobreamostrado em R vezes apenas para gerar um sistema com banda maior que o sinal OFDM, sendo possível gerar sinais interferentes de bandas superiores à banda do sinal.

O canal do sistema é modelado como um canal com desvanecimento Rayleigh. Para simular o efeito Doppler no sinal, o canal é gerado utilizando-se o modelo de Jakes [6]. Um canal desse tipo é seletivo em frequência e irá atenuar cada subportadora do sinal OFDM de forma aleatória. Espera-se, então, que o sinal interferente seja capaz de confundir o sistema OFDM de modo que a equalização do sinal não consiga compensar os efeitos do canal. Além disso, outras imperfeições do canal são modeladas como ruído gaussiano branco aditivo (AWGN).

O sinal interferente é um sinal senoidal modulado em frequência,

$$z(t) = A_z \cdot \cos\left(2\pi f_z t + 2\pi k_f \int_0^t m(a)da\right) \tag{2}$$
$$m(t) = A_m \cos(2\pi f_m t),$$

sendo k_f a sensibilidade do modulador. Para $m(t)$ sendo um sinal senoidal, a Equação 2 pode ser reescrita como

$$z(t) = A_z \cos\left(2\pi f_z t + \beta \sin(2\pi f_m t)\right), \tag{3}$$

com $\beta = \frac{k_f \cdot A_m}{f_m}$ sendo o índice de modulação do sinal FM. Por fim, a Equação 3 pode ser decomposta e reescrita como

$$z(t) = A_z \sum_{k=-\infty}^{\infty} J_k(\beta)\cos\left(2\pi(f_z + k f_m)t\right), \tag{4}$$

sendo $J_k(x)$ a função de Bessel de primeira espécie. Deste modo, é possível gerar, analogicamente e com facilidade, tons ortogonais com separação de f_m entre si.

Um sinal interferente com tons ortogonais é um *jammer* de sistemas OFDM, pois pesquisas mostram que a configuração ótima para os tons pilotos é que estes sejam igualmente espaçados e tenham potências iguais [7] e é justamente assim que grandes padrões implementam o sistema.

A envoltória complexa do sinal $z(t)$ é

$$\tilde{z}(t) = A_z e^{j\beta \sin(2\pi f_m t)} e^{j2\pi f_\Delta t}, \tag{5}$$

em que f_Δ é o desvio de frequência entre o sinal $z(t)$ e o sinal OFDM $s(t)$.

III. Simulação

Os parâmetros utilizados para a realização das simulações foram escolhidos tomando como base algumas definições do padrão 3GPP LTE 10 MHz.

A. Codificação

No codificador, o padrão LTE foi um pouco simplificado. Ao invés de códigos turbo, o trabalho utiliza um codificador convolucional de taxa $R_c = 1/3$ com embaralhamento das palavras-código. No receptor, o código é desembaralhado e decodificado pelo algoritmo de Viterbi com decisão *hard*.

B. Modulação

O mapeamento de bits em símbolos é feito por um modulador M-QAM quadrado. Os símbolos possuem energia normalizada e a potência do sinal é ajustada apenas antes da entrada no canal.

C. OFDM

De acordo com o padrão LTE, a separação entre as subportadoras é de 15 kHz. Em um sistema de banda 10 MHz, é definido que 10% da banda é utilizada como banda de guarda. Sendo assim, os 9 MHz restantes alocam $N = 600$ subportadoras com espaçamento Δf = 15 kHz. Nenhum tom nulo é enviado. Os símbolos originados no modulador são organizados paralelamente em blocos de tamanho N e a IFFT é realizada.

Os tons pilotos estão posicionados a cada três subportadoras e são enviados da seguinte maneira: no primeiro símbolo OFDM, são enviados os tons pilotos apenas nas subportadoras pares (6, 12, 18, ...). No quinto símbolo OFDM, são enviados os tons pilotos apenas nas subportadoras ímpares (3, 9, 15, ...). O padrão se repete após dois símbolos OFDM, conforme mostra a Figura 2. Após a realização da IFFT, é adicionado o prefixo cíclico de tamanho $CP = N/8$.

Na recepção, o sistema conhece os valores enviados nas portadoras piloto e estima a resposta em frequência do canal para cada subportadora. Sendo $p_{n,k}$ e $q_{n,k}$ os valores enviado e recebido, respectivamente, no k-ésimo tom piloto da subportadora n, o equalizador calcula a distorção em frequência do canal pela média das distorções em cada subportadora.

$$e_{n,k} = \frac{q_{n,k}}{p_{n,k}}.$$

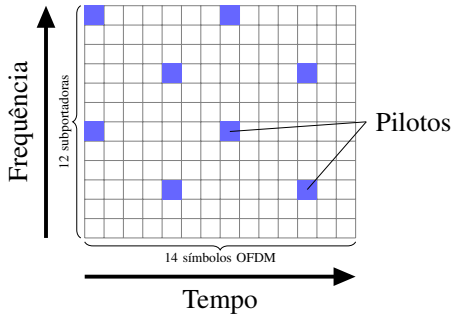

Fig. 2. Configuração de tons pilotos nos símbolos OFDM.

Como o canal é variante no tempo, a média é calculada a cada 14 símbolos OFDM, como mostra a Figura 3. Os valores das subportadoras em que não são enviados pilotos são obtidos por interpolação linear.

Com todos as estimativas da distorção canal, as amostras do equalizador são $h_n = 1/e_n$. Sendo $h[n]$ o filtro equalizador e $y[h]$ o resultado da FFT do símbolo OFDM recebido, os símbolos $\tilde{x}[n]$ equalizados e passados ao demodulador são, então, $\tilde{x}[n] = y[n] \cdot h[n]$.

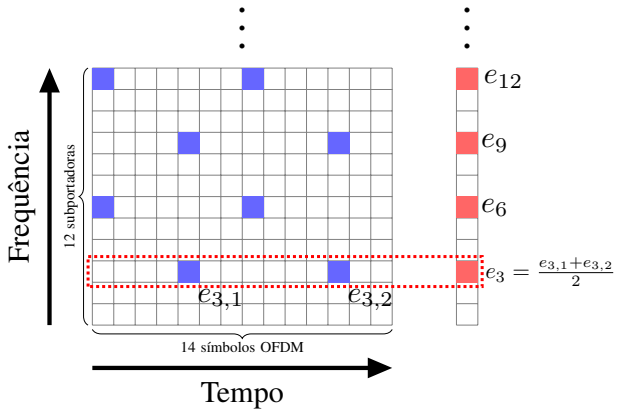

Fig. 3. Estimação da resposta em frequência do canal.

D. Canal

O canal possui resposta impulsional complexa de 42 *taps* de atraso, de forma a gerar alta seletividade na frequência, e é gerado pelo modelo de Jakes com desvio Doppler máximo, f_D, dado por

$$f_D = \frac{v}{c} f_c, \tag{6}$$

sendo c a velocidade da luz e v a velocidade de deslocamento entre o transmissor e o receptor. Considerando f_c = 788 MHz, uma das frequências do LTE 10 MHz no Brasil, e v = 40 km/h, obtém-se um desvio Doppler máximo de, aproximadamente, 30 Hz. A resposta em frequência do desvanecimento Rayleigh utilizado neste trabalho é mostrada na Figura 4.

Além dos efeitos de multipercurso, é adicionado ruído ao sinal na entrada do receptor, sendo que a relação sinal-ruído (SNR) é calculada como a razão entre a potência do sinal recebido (após sofrer desvanecimento) e a potência do ruído.

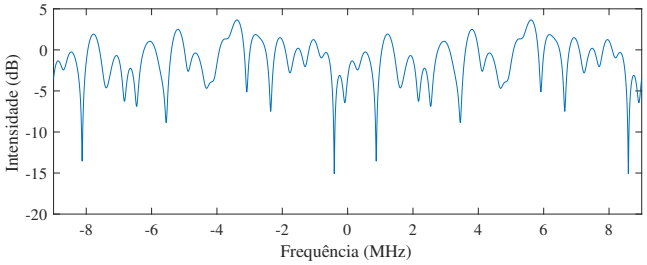

Fig. 4. Resposta em frequência do canal.

E. Jamming

Para analisar a influência de um sinal *jammer* no sistema, os parâmetros A_m, β, f_m e f_Δ da Equação 5 serão variados. A banda do sistema será duas vezes maior que a banda do sinal OFDM, permitindo um sinal interferente com banda de até 18 MHz. Além disso, o sinal de *jamming* não é exposto ao canal com multipercurso, como se possuísse apenas visada direta com o receptor OFDM.

IV. Resultados

Como as subportadoras com tons piloto estão espaçadas em $3\Delta f$, definindo o valor de $f_m = 3\Delta f$, é possível interferir apenas nos tons pilotos, obtendo a melhor interferência no sistema de acordo com [5]. Contudo, para se interferir em todos os tons pilotos, é necessário que a banda do sinal interferente seja pelo menos igual a banda do sinal OFDM. De acordo com a Equação 4, a potência das componentes do sinal FM decaem de acordo com a função de Bessel de primeira espécie. A Figura 5 mostra o comportamento da função de Bessel $J_k(x)$ em função de k para alguns valores de x. É possível perceber, portanto, que, para sinais senoidais modulados em frequência, quanto maior o valor de β, maior a banda do sinal, entretanto, menor é a potência de cada componente frequencial.

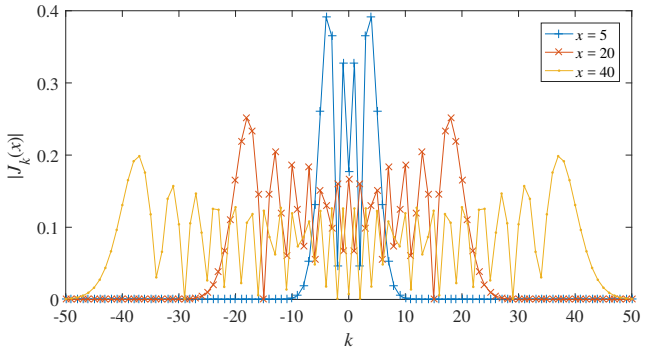

Fig. 5. Magnitude da função de Bessel.

A banda do sinal FM senoidal é $B_{FM} = 2f_m(\beta + 1)$. Portanto, escolhendo $f_m = k\Delta f$, a razão entre a banda do sinal FM e a banda do sinal OFDM é dada por

$$\frac{B_{FM}}{B_{OFDM}} = \frac{2k(\beta+1)}{N}. \tag{7}$$

Assim, é possível analisar como a escolha de f_m influencia na capacidade de interferência do sinal FM no sistema OFDM. A Figura 6 compara o desempenho da interferência de um sinal FM com $f_m = k\Delta f$ em um sistema OFDM com modulação 16-QAM, SNR de 15 dB e relação sinal-interferência (SNI) de 0 dB. Foram utilizados 1.008.000 bits nas simulações, totalizando 1260 símbolos OFDM transmitidos.

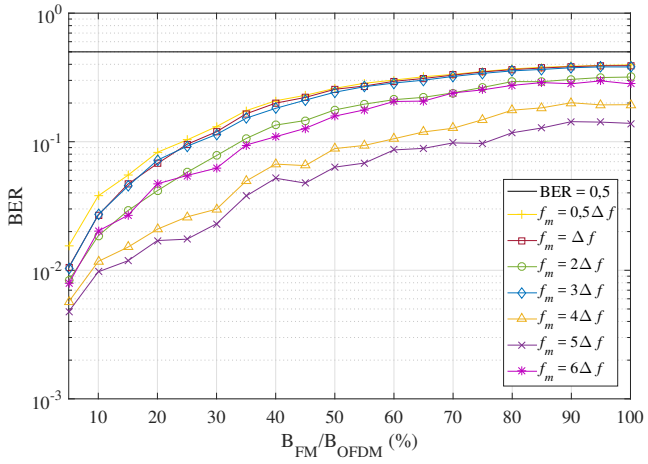

Fig. 6. Taxa de erro de bit em função da banda do sinal interferente (FM) para diferentes valores de f_m.

Conforme dados da Figura 6, as interferências mais eficientes ocorrem quando todos os tons pilotos são interferidos, isso ocorre para k = 1/2, 1 e 3. Quanto mais o valor de k se afasta (k = 4 e 5), pior fica a eficiência da interferência, que volta a melhorar com k = 6, quando apenas tons pilotos estão sendo interferidos. Isso verifica a importância do conhecimento do sistema OFDM a ser interferido para um *jamming* eficiente.

Outro fator que influencia diretamente o desempenho do *jamming* é o desvio de frequência. Um sinal fora de sincronia com o sistema interferido deve ser menos eficiente, pois perde-se a interferência nos tons pilotos. A Figura 7 mostra o desempenho da interferência para diferentes valores de f_Δ para $f_m = \Delta f$ e $f_m = 3\Delta f$, SNR em 15 dB e SNI em 0 dB. Nota-se que a probabilidade de erro de bit pode ser até quatro vezes menor dependendo apenas do desvio de frequência para $f_m = 3\Delta f$. É interessante notar que, quando $f_\Delta = 1,5\Delta f$, isto se deve ao fato das componentes do sinal FM estarem interferindo duas subportadoras simultaneamente e nenhuma delas é um piloto, que equivale a interferir apenas nos tons pilotos. Já para $f_m = \Delta f$, o desvio de frequência não interfere no desempenho da interferência.

Finalmente, para verificar a relação entre a banda do sinal FM e a potência de suas componentes frequenciais, a Figura 8 compara a BER em função da SNI para alguns valores de f_m com $B_{FM} = B_{OFDM}$, $f_\Delta = 0$ e SNR de 15 dB. Novamente, com $f_m = \Delta f$ e $f_m = 3\Delta f$, o sinal FM apresenta o melhor desempenho como *jammer*. Sendo assim, infere-se que é mais importante o modo como as subportadoras OFDM são atacadas que a potência com as quais elas são atacadas.

Ainda na Figura 8, verifica-se que o sinal modulado em frequência proposto neste trabalho pode ser um *jammer* do

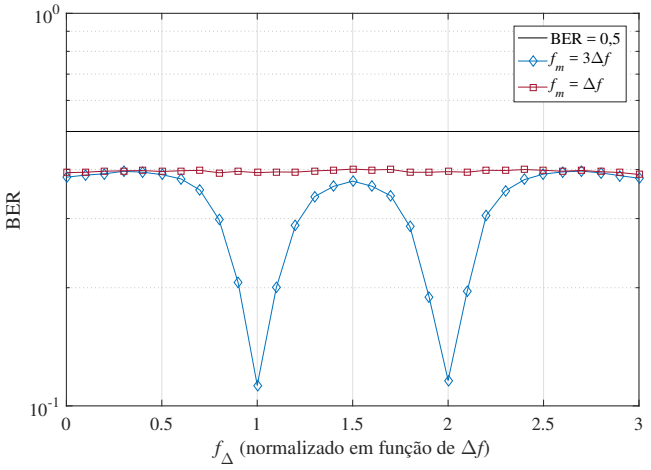

Fig. 7. Taxa de erro de bit em função do desvio de frequência entre o sinal *jammer* (FM) e o sinal OFDM.

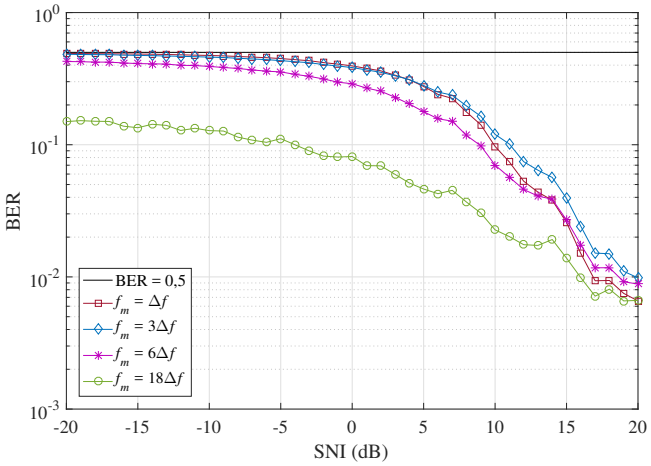

Fig. 8. Taxa de erro de bit em função da relação sinal-interferência.

sistema OFDM, levando este à apresentar taxas de erro de bit de 0,5 quando a SNI é menor que -5 dB utilizando as configurações adequadas. Os resultados encontrados assemelham-se aos encontrados nas técnicas de ataque apresentadas em [5].

V. Conclusões

Este trabalho apresentou um estudo sobre *jamming* de um sistema OFDM utilizando um sinal modulado em frequência. Por meio de simulações, verificou-se a importância dos parâmetros que compõem o sinal FM para que o ataque ao sistema OFDM seja mais eficaz.

O sinal FM, devidamente construído, é capaz de atacar o sistema OFDM com uma técnica chamada *pilot jamming*, que consiste em interferir nos tons pilotos e fazer com que o sistema não seja capaz de estimar corretamente o canal. Esse ataque pode levar o sistema a apresentar taxas de erro de bit de $0,5$, como mostrado nos resultados das simulações.

Fica evidenciado que sistemas OFDM são vulneráveis a ataques de *jamming* de sinais modulados em frequência, sendo que mitigação desses ataques é bastante complexa e, além de

necessitar de uma certa inteligência do sistema atacado, requer sincronização entre transmissor e receptor.

REFERÊNCIAS

[1] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Std 802.11, 2012.

[2] *Evolved Universal Terrestrial Radio Access (E-UTRA); LTE physical layer; General description*, 3GPP TS 36.201, 2017.

[3] Patel, C. S., Stuber, G. L. e Pratt, T. G. "Analysis of OFDM/MC-CDMA under imperfect channel estimation and jamming," *IEEE Wireless Comunnications and Networking Conference (WCNC)*, v. 2, pp. 954-958, Março de 2004.

[4] Mueller-Smith, C. e Trappe, W. "Efficient ofdm denial in the absence of channelinformation," *IEEE Military Communications Conference (MILCOM)*, pp. 89-94, Novembro de 2013.

[5] Clancy, T. C. "Efficient OFDM denial: pilot jamming and pilot nulling," *IEEE International Conference on Communications (ICC)*, pp. 1-5, Junho 2011.

[6] Jakes, W. C. *Microwave Mobile Communications.* John Wiley & Sons Inc. New York, 1975.

[7] Negi, R. e Cioffi, J. "Pilot tone selection for channel estimation in a mobile OFDM system," *IEEE Transactions on Cosumer Electronics*, pp. 1122-1128, Agosto de 1998.