Desempenho de Receptores não Autorizados em Sistemas que usam Modulação Adaptativa

Alexandre Amorim Pereira Júnior e Juraci Ferreira Galdino

***Resumo*— Este trabalho mostra que a técnica de modulação adaptativa, comumente empregada para melhorar as características de desempenho dos enlaces em canais com desvanecimento variante no tempo, pode ser explorada para aumentar a capacidade de sigilo desses enlaces, na medida em que, sob determinadas condições, a probabilidade de erro de um receptor não autorizado (aqui denominado de espião) pode ser bem maior do que a do legítimo. Neste trabalho são apresentadas expressões de probabilidades de erro de bit que demonstram esse fato. A par disso, aqui são propostas duas estratégias de modulação adaptativa com o objetivo de potencializar ainda mais essa característica natural das técnicas de modulação adaptativa clássicas. A primeira dessas técnicas admite o conhecimento dos estados dos canais legítimo e espião no transmissor, ao passo que na segunda considera-se apenas o conhecimento do estado do canal legítimo, uma hipótese geralmente adotada nos sistemas que utilizam modulação adaptativa. Para ambos os casos são apresentadas expressões de eficiência espectral e probabilidade de erro de bit, em particular, estas últimas, indicam que para as técnicas aqui propostas o desempenho do espião é pior do que aquele obtido quando são empregadas as técnicas de modulação adaptativa clássicas.**

***Palavras-Chave*— Modulação adaptativa, segurança das comunicações, desvanecimento plano, probabilidade de erro.**

***Abstract*— In this paper, we show that the adaptive modulation techniques, that are usually adopted to increase the spectral efficiency of digital communication system over flat fading channels, can be employed to increase the secrecy capacity of this communication system, since, under determined conditions, the bit error probability of the eavesdropper can be much larger than the error probability of the receiver. Expressions of bit error probabilities here presented confirm this. In addition, we propose two adaptive modulation schemes in order to improve this natural characteristic of the conventional adaptative modulation technique. The first one assumes the knowledge of channel state information (CSI) of both the receiver and the eavesdropper at transmitter, and the second one assumes only the knowledge of receiver CSI at the transmitter, which is a very common hypothesis in context of adaptive modulation systems. In both cases, we obtain expressions of spectral efficiency and bit error probability. These expressions show a futher degradation at the performance of the eavesdropper in relation to conventional adaptive modulation.**

***Keywords*— adaptative Modulation, communication security, flat-fading channels, error probability.**

I. INTRODUÇÃO

Atualmente, a segurança da informação nas comunicações tem se tornado um fator de extrema importância para qualquer organização na medida que cada vez mais decisões estratégicas são tomadas de forma distribuída por meio de vídeo/teleconferências, estratégias de negócios de grandes empresas são passadas aos seus diversos parceiros distribuídos geograficamente pelas redes de comunicação e transações bancárias são realizadas por essas redes. No âmbito militar, a segurança da informação nas comunicações constitui uma vantagem estratégica indispensável, principalmente nas operações de Comando e Controle. Particularmente nas redes de comunicação sem fio, essa questão se torna ainda mais importante, pois essas redes são mais suscetíveis às recepções não autorizadas.

Devido à sua importância, o assunto em questão se constitui em objeto de investigação de diversos pesquisadores. Em 1949, Shannon introduziu o conceito de capacidade de sigilo nas comunicações para designar a taxa máxima de bits em que um transmissor poderia comunicar-se com o receptor legítimo sem que um receptor não autorizado, denominado de espião, com recursos computacionais ilimitados, pudesse decifrar a mensagem transmitida [1]. Posteriormente, Wyner, em [2], apresentou um modelo em que o espião observa uma versão degradada do sinal capturado pelo receptor legítimo e provou que, nesse caso, é possível atingir capacidades de sigilo maiores do que zero. Em [3] e [4], baseados nos estudos de Wyner, foram desenvolvidas expressões para a capacidade de sigilo de canais sujeitos a desvanecimento e mostrou-se que, mesmo com as condições médias de propagação do canal do espião melhores do que as do canal legítimo é possível se obter capacidades de sigilo diferentes de zero. Em [5], os autores procuram aumentar a capacidade de sigilo do canal de comunicação por meio da inserção de ruído gerado de forma controlada ao sinal transmitido a fim de degradar o sinal recebido no espião.

As técnicas de modulação adaptativa vêm sendo objeto de elevado interesse para emprego em comunicações sem fio. Nelas, o transmissor procura adaptar a estratégia de modulação utilizada de acordo com as condições de propagação do canal de comunicação de forma a aumentar a eficiência espectral (EE) do sistema atendendo a um requisito de máxima taxa de erro, como é o caso do estudo realizado em [6].

Além do uso mais eficiente do canal de comunicação variante no tempo, devido às mudanças de estratégia de modulação utilizada durante a comunicação, este artigo defende a tese de que as técnicas de modulação adaptativa podem aumentar a segurança dos sistemas de transmissão. Este trabalho mostra que tais técnicas podem degradar o desempenho de receptores não autorizados, contribuindo para aumentar a capacidade de sigilo do sistema. Além disso, aqui são propostas duas técnicas de transmissão baseadas nas técnicas de modulação adaptativa para aumentar ainda mais essa capacidade.

O restante deste trabalho está estruturado da seguinte forma. Na Seção II, faz-se uma breve apresentação das técnicas de modulação adaptativa. Na Seção III, o cenário de comunicação

Alexandre Amorim Pereira Júnior e Juraci Ferreira Galdino, Departamento de Engenharia Elétrica, Instituto Militar de Engenharia, Rio de Janeiro, Brasil. E-mail: amorim.alexandre@gmail.com e galdino@ime.eb.br.

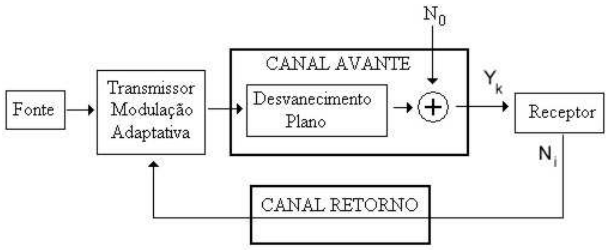

Fig. 1. Diagrama básico de um sistema de comunicação que utiliza a técnica de modulação adaptativa.

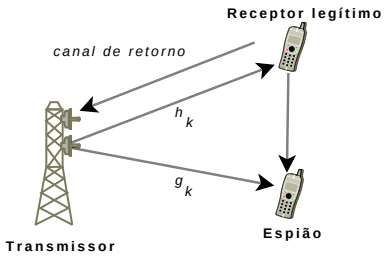

Fig. 2. Cenário em questão. Canais do receptor legítimo e do espião, h_k e g_k, independentes.

sob investigação neste trabalho é apresentado e são propostas e analisadas duas estratégias de modulação adaptativa. Na Seção IV, são apresentados os resultados de simulação que validam a análise de desempenho realizada na Seção III. Por fim, na Seção V, é feita uma breve conclusão.

II. Modulação Adaptativa

As técnicas de modulação adaptativa surgiram como uma alternativa para a utilização de forma eficiente do canal de comunicação cujas respostas ao impulso variam com o tempo. Nesses cenários, essas técnicas apresentam um compromisso entre EE e taxa de erro de bit melhor do que as técnicas de modulação digital clássicas que se caracterizam por empregar apenas um tipo de constelação durante a transmissão da informação.

Nas técnicas de modulação adaptativa a estratégia de modulação é empregada de acordo com as condições do canal. Quando ele apresenta excelentes condições de propagação, geralmente são utilizadas modulações com elevada EE e, mesmo assim, se mantém a probabilidade de erro de bit em níveis aceitáveis. Em contrapartida, quando ele se encontra em um profundo desvanecimento, utilizam-se modulações com baixa EE para não se elevar sobremodo a taxa de erro de bit. Assim sendo, essas técnicas possuem a característica de empregar, a todo o momento, estratégias de modulação que propiciam boa EE sem ultrapassar um limite para a taxa de erro de bit, chamado de taxa de erro de bit alvo.

A Figura 1 apresenta um diagrama em blocos em banda base de um sistema de modulação adaptativa convencional. Como mostrado, o cenário de interesse neste trabalho é caracterizado pela presença de canais sujeitos ao efeito de desvanecimento plano. A fonte de informação gera bits estatisticamente independentes e equiprováveis que são entregues ao transmissor para fins de mapeamento em símbolos, s_k, de acordo com a modulação utilizada no momento. O sinal recebido na entrada do receptor, y_k, em banda base, é dado por:

$$y_k = h_k s_k + \eta_k, \tag{1}$$

sendo h_k o coeficiente de ganho do canal, que é modelado por um processo estacionário em sentido amplo, cuja densidade espectral de potência, neste trabalho, é dada pelo espectro de Jakes [7] e η_k é um ruído aditivo modelado por um processo gaussiano branco de média nula e variância $N_0/2$.

Nos sistemas de modulação adaptativa, y_k é empregado não apenas para detectar a informação transmitida, mas também para estimar a razão sinal ruído, RSR, instantânea na entrada do decisor, que será comparada com limiares de adaptação para definir o estado do canal de comunicação. Essa informação é enviada ao transmissor, através do canal de retorno, onde é empregada para determinar a modulação a ser adotada na transmissão do próximo bloco de dados. Considerando que a técnica de transmissão adaptativa emprega N modos de operação, que são escolhidos de acordo com um conjunto de regiões de decisão delimitadas por limiares λ_i, para $i = 0, ..., N$, sendo $\lambda_0 = 0$ e $\lambda_N = \infty$, escolhe-se a estratégia N_i quando a RSR instantânea, γ_k, que representa a qualidade do canal naquele instante, estiver entre os limiares λ_i e λ_{i+1}, sendo

$$\gamma_k \stackrel{\triangle}{=} \bar{\gamma} \cdot |h_k|^2, \tag{2}$$

em que $\bar{\gamma}$ é a RSR média na entrada do decisor expressa em termos de E_b/N_0, com E_b denotando a energia média do bit. Dessa forma, γ_k pode ser modelada por uma variável aleatória cuja função densidade de probabilidade é dada pela equação seguinte.

$$f_{\bar{\gamma}}(\gamma_k) = \frac{1}{\bar{\gamma}} \cdot exp\left\{-\frac{\gamma_k}{\bar{\gamma}}\right\}. \tag{3}$$

Com base nos limiares de adaptação, o canal de comunicação pode ser classificado em N estados distintos, sendo a probabilidade do canal se encontrar no estado c, π_c, dada por:

$$\pi_c = \int_{\lambda_c}^{\lambda_{c+1}} f_{\bar{\gamma}}(\gamma_k) d\gamma_k = e^{\frac{-\lambda_c}{\bar{\gamma}}} - e^{\frac{-\lambda_{c+1}}{\bar{\gamma}}}, \quad 0 \leq c < N-1. \tag{4}$$

III. Cenário e Técnicas Propostas

A. Cenário

A Figura 2 ilustra um cenário de comunicação sem fio sujeito à interceptação de informação. Assim sendo, o transmissor comunica-se com um receptor legítimo na presença de um espião. Admite-se que os canais do receptor legítimo e do espião, h_k e g_k respectivamente, são estatisticamente independentes e apresentam desvanecimento plano e variante no tempo. A suposição de independência é razoável desde que haja uma separação entre o receptor legítimo e o espião da ordem do comprimento de onda da portadora. A modelagem adotada para o desvanecimento não é restritiva, pois cenários

que envolvam canais caracterizados pelo efeito de desvanecimento seletivo podem ser reduzidos ao caso de desvanecimento plano por meio do uso das técnicas OFDM (*Orthogonal Frequency-Division Multiplexing*) adaptativas, nas quais este modelo pode ser empregado para caracterizar uma das subportadoras. Admite-se ainda que o espião conheça as constelações empregadas no sistema de modulação adaptativa, o tamanho do bloco de dados e possui acesso ao canal de retorno. Ou seja, o espião conhece todos os parâmetros do sistema legítimo e a seqüência de modulações empregada.

Além disso, as variáveis c_L e c_E representam os estados dos canais legítimo e espião, respectivamente e são calculadas da seguinte forma:

$$c_L = i \ se \ \{\gamma_k \in \mathbb{R}|\lambda_i \leq \gamma_k < \lambda_{i+1}\} \quad (5)$$

$$c_E = j \ se \ \{\tilde{\gamma}_k \in \mathbb{R}|\lambda_j \leq \tilde{\gamma}_k < \lambda_{j+1}\}, \quad (6)$$

em que $\tilde{\gamma}_k \stackrel{\triangle}{=} \bar{\gamma}_E \cdot |g_k|^2$ é a RSR instantânea na entrada do receptor do espião no instante k e $\bar{\gamma}_E$ é a sua RSR média. Denota-se por π_i a probabilidade do estado do canal legítimo ser igual a i e por $\tilde{\pi}_j$ a probabilidade do estado do canal do espião ser igual a j.

Além do uso mais eficiente do canal de comunicação, este artigo defende a tese de que as técnicas de modulação adaptativas podem proporcionar um aumento na segurança da transmissão, na medida que a taxa de erro de bit (BER) do espião tende a ser pior do que a do legítimo. A Figura 3 apresenta curvas de BER do espião e do receptor legítimo quando emprega-se a técnica de modulação fixa 4-QAM e modulação adaptativa com oito modos de operação, a saber: não-transmite, B-PSK, 4-QAM, 16-QAM, 64-QAM, 256-QAM, 1024-QAM e 4096-QAM, e cujos limiares de adaptação foram calculados para uma probabilidade de erro de bit alvo de 10^{-3}. Considerou-se ainda a RSR média do espião igual a do enlace legítimo.

Vê-se neste gráfico que as curvas de BER dos receptores legítimo e espião são iguais quando se emprega a modulação fixa, porém observa-se uma severa degradação de desempenho do receptor do espião em relação ao do legítimo quando se emprega a modulação adaptativa. Essa degradação da BER do espião se justifica pela independência dos canais envolvidos. Quando o estado do canal do espião for melhor do que o do legítimo, haverá pequena vantagem da BER do primeiro em relação a do segundo, pois a modulação foi escolhida com base nas condições de propagação do legítimo para atender uma BER máxima, que em geral é pequena. Por outro lado, quando o estado do canal do espião for pior do que o do legítimo, a BER do espião pode ser severamente degradada.

B. Técnicas Propostas

Baseadas nos estudos apresentados em [3], duas estratégias de modulação adaptativa para degradar ainda mais o desempenho do enlace do espião são aqui propostas. Na primeira delas, admite-se que o transmissor conhece h_k e g_k. Na segunda estratégia admite-se apenas o conhecimento de h_k.

- Técnica I

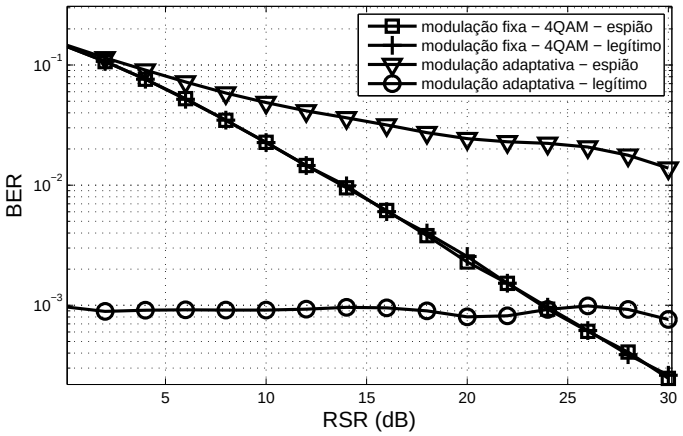

Fig. 3. Comparação entre as curvas de probabilidade de erro de bit do receptor legítimo e do espião ao se utilizar a estratégia de modulação fixa 4-QAM e a técnica de modulação adaptativa.

Neste caso, só ocorre transmissão quando a diferença entre o estado do canal legítimo e o estado do canal do espião for maior que d_{LE}, sendo $d_{LE} \in \{\mathbb{N}|0 \leq d_{LE} < N\}$. Denotando-se por ξ_i o evento de haver transmissão utilizando a modulação N_i, ou seja:

$$\xi_i \stackrel{\triangle}{=} \{c_L > c_E + d_{LE}\} \cap \{c_L = i\}, \quad (7)$$

pode-se mostrar que a eficiência espectral média, EE, do sistema proposto é expressa por:

$$EE = \sum_{i=0}^{N-1} R_i \cdot Pr(c_L > c_E + d_{LE}|c_L = i) \cdot \pi_i, \quad (8)$$

sendo $R_i = \log_2(M_i)$, onde M_i denota o número de símbolos da modulação N_i

Conforme mostrado no Apêndice I, $Pr(c_L > c_E + d_{LE}|c_L = i)$ é igual a 0 para $i \leq d_{LE}$ e, para $i > d_{LE}$, é dada por:

$$Pr(c_L > c_E + d_{LE}|c_L = i) = \sum_{j=0}^{i-(d_{LE}+1)} \tilde{\pi}_j. \quad (9)$$

Sendo assim, temos que a EE da comunicação pode ser expressa por:

$$EE = \sum_{i=d_{LE}+1}^{N-1} \sum_{j=0}^{i-(d_{LE}+1)} R_i \cdot \pi_i \cdot \tilde{\pi}_j. \quad (10)$$

Utilizando o resultado da expressão da probabilidade de erro de bit média para esquemas de modulação adaptativa convencionais [6], a probabilidade de erro de bit no receptor legítimo é dada por:

$$P_L(\bar{\gamma}_L) = \frac{\sum_{i=0}^{N-1} R_i Pe_i}{EE}, \quad (11)$$

sendo Pe_i a probabilidade de erro do canal legítimo condicionada ao uso da modulação N_i. Essa probabilidade pode ser

escrita como:

$$\begin{aligned} Pe_i &= Pr(e_L|\xi_i)\cdot Pr(\xi_i) \\ &= Pr(e_L|c_L > c_E + d_{LE}, c_L = i)\cdot Pr(c_l = i) \\ &\quad \cdot Pr(c_L > c_E + d_{LE}|c_L = i) \\ &= \int_{\lambda_i}^{\lambda_{i+1}} P_b(\gamma, N_i) f_{\bar{\gamma}_L}(\gamma) d\gamma \cdot Pr(c_L > c_E + d_{LE}|c_L = i), \end{aligned} \tag{12}$$

na qual $P_b(\gamma, N_i)$ é a expressão da probabilidade de erro de bit referente ao uso da modulação N_i com uma RSR instantânea na entrada do decisor igual a γ. Utilizando novamente o resultado da equação (23) do apêndice, temos que:

$$P_L(\bar{\gamma}_L) = \frac{1}{EE}\cdot \sum_{i=d_{LE}+1}^{N-1} \sum_{j=0}^{i-(d_{LE}+1)} \tilde{\pi}_j R_i \int_{\lambda_i}^{\lambda_{i+1}} P_b(\gamma, N_i) f_{\bar{\gamma}_L}(\gamma) d\gamma. \tag{13}$$

Para o espião, observa-se que o evento ξ_i é equivalente ao evento $\{c_E < i - d_{LE}\} \cap \{c_L = i\}$. Sendo assim temos:

$$\begin{aligned} Pr(e_E \cap \xi_i) &= Pr(e_E \cap c_E < i - d_{LE} \cap c_L = i) \\ &= Pr(e_E \cap c_E < i - d_{LE}) \cdot Pr(c_L = i) \\ &= \begin{cases} \int_{\lambda_0}^{\lambda_{i-d_{LE}}} P_b(\gamma, N_i) f_{\bar{\gamma}_E}(\gamma) d\gamma \cdot \pi_i & , \; se\ i > d_{LE} \\ 0 & , \; c.c. \end{cases}. \end{aligned} \tag{14}$$

Logo, como o espião possui a mesma EE do receptor legítimo, sua probabilidade de erro de bit pode ser expressa por:

$$P_E(\bar{\gamma}_E) = \frac{\sum_{i=d_{LE}+1}^{N-1} R_i \int_{\lambda_0}^{\lambda_{i-d_{LE}}} P_b(\gamma, N_i) f_{\bar{\gamma}_E}(\gamma) d\gamma \cdot \pi_i}{EE}. \tag{15}$$

- Técnica II

Como comentado inicialmente, para empregar a Técnica I é necessário que o transmissor tenha conhecimento do estado do canal do espião, hipótese pouco realista. A idéia central da referida técnica é realizar a transmissão apenas quando o canal legítimo possuir valores de RSR instantâneas maiores do que os exibidos pelo canal estabelecido entre o transmissor e o espião. Pode-se tentar obter essa condição entre os enlaces legítimo e espião, mesmo quando não se dispõe da informação do estado do canal do espião, realizando a transmissão apenas quando o canal legítimo propicia boas condições de propagação. Admitindo-se que só ocorre transmissão quando $c_l > m$, quanto maior for m, menor será a probabilidade do canal do espião apresentar melhores condições de propagação do que o canal legítimo, contribuindo dessa forma para degradar o desempenho do receptor do espião em relação ao legítimo. Em contrapartida, quanto maior m, menor será a probabilidade de ocorrer a transmissão, o que reduz a EE da técnica.

Da definição da estratégia de transmissão segue que a EE média do sistema é dada por:

$$EE = \sum_{i=m+1}^{N-1} R_i \cdot \pi_i \tag{16}$$

Como na equação (11), a probabilidade de erro do canal legítimo é dada por:

$$P_L(\bar{\gamma}_L) = \frac{\sum_{i=m+1}^{N-1} R_i Pr(e_L \cap c_L = i)}{EE}. \tag{17}$$

A probabilidade $Pr(e_L \cap c_L = i)$ pode ser escrita como:

$$\begin{aligned} Pr(e_L \cap c_L = i) &= Pr(e_L|c_L = i)\cdot Pr(c_L = i) \\ &= \int_{\lambda_i}^{\lambda_{i+1}} P_b(\gamma, N_i) f_{\bar{\gamma}_L}(\gamma) d\gamma, \end{aligned} \tag{18}$$

logo, temos que:

$$P_L(\bar{\gamma}_L) = \frac{1}{EE}\cdot \sum_{i=m+1}^{N-1} R_i \int_{\lambda_i}^{\lambda_{i+1}} P_b(\gamma, N_i) f_{\bar{\gamma}_L}(\gamma) d\gamma. \tag{19}$$

Por seu turno, a probabilidade de erro de bit do espião neste caso é dada por:

$$P_E(\bar{\gamma}_E) = \frac{\sum_{i=m+1}^{N-1} R_i Pr(e_E \cap c_L = i)}{EE}, \tag{20}$$

sendo

$$\begin{aligned} Pr(e_E \cap c_L = i) &= \\ &= Pr(e_E|c_L = i) Pr(c_L = i) \\ &= \int_0^{\infty} P_b(\gamma, N_i) f_{\bar{\gamma}_E}(\gamma) d\gamma \cdot \pi_i. \end{aligned} \tag{21}$$

De (20) e (21), temos que:

$$P_E(\bar{\gamma}_E) = \frac{1}{EE} \sum_{i=m+1}^{N-1} R_i \int_0^{\infty} P_b(\gamma, N_i) f_{\bar{\gamma}_E}(\gamma) d\gamma \pi_i. \tag{22}$$

IV. Resultados de simulação

Com o intuito de validar as expressões obtidas na Seção III e avaliar os desempenhos das técnicas propostas, foram realizadas simulações de transmissões com um receptor legítimo na presença de um espião. Os modos de operação disponíveis para uso na técnica de modulação adaptativa são: não transmite, BPSK, 4-QAM, 16-QAM, 64-QAM, 256-QAM, 1024-QAM e 4096-QAM. Os canais legítimo e espião são estatisticamente independentes e modelados pelo espectro de Jakes, cujo produto da máxima freqüência Doppler pela duração do intervalo de símbolo, $f_D\mathcal{T}$, é igual a 10^{-4}. Os limiares de adaptação foram obtidos de modo que forneçam uma BER alvo de 10^{-3}. Utilizou-se blocos de 10 símbolos, admitiu-se que o canal é conhecido no lado de recepção e que o canal de retorno é ideal, ou seja, sem erros e atrasos.

A fim de se obter os valores de probabilidade de erro de bit analíticas desenvolvidas neste trabalho, foi empregada a equação (14) de [8], que estabelece a probabilidade de erro de bit exata para a codificação de Gray, $P_b(\gamma, N_i)$.

Em todos os casos, a RSR média dos canais legítimo e espião foram mantidas iguais. A Figura 4 apresenta um gráfico de comparação entre as curvas de probabilidade de erro de bit analíticas, PEB_L e PEB_E, e suas estimativas obtidas a partir dos sistemas simulados, BER_L e BER_E,

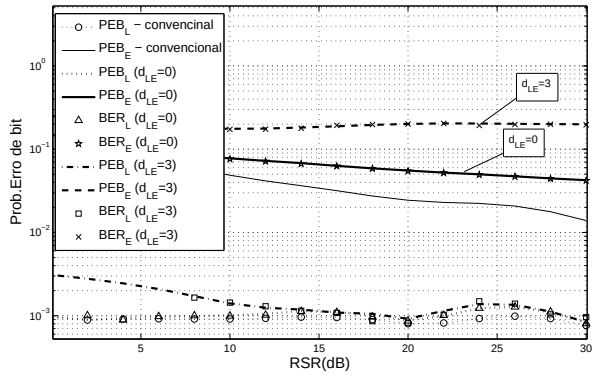

Fig. 4. Curvas de PEB e BER para canais legítimo e espião para $d_{LE} = 0$, $d_{LE} = 3$ e para o sistema de modulação adaptativa convencional. As RSR médias de ambos os canais foram mantidas iguais em todos os casos.

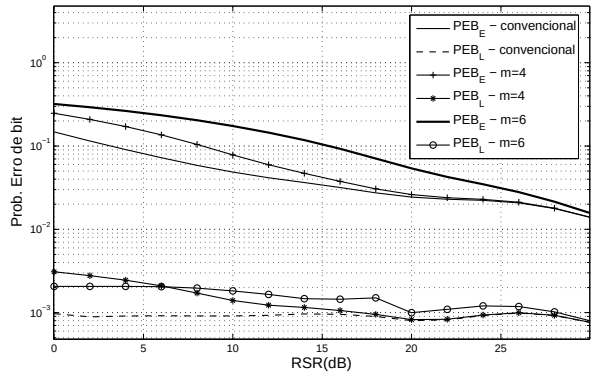

Fig. 6. PEB da técnica proposta II para m=4 e m=6 e do sistema de modulação adaptativa convencional. As RSR médias do canal do espião e do canal legítimo foram mantidas iguais.

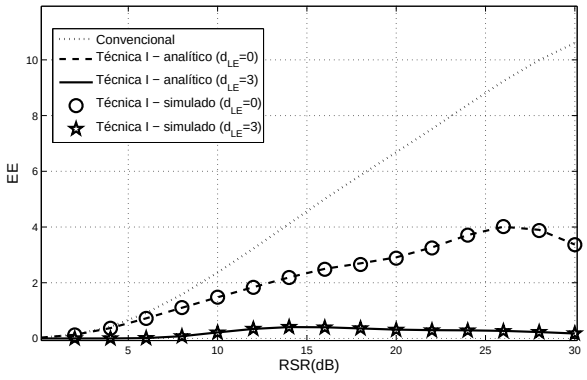

Fig. 5. EE da técnica proposta I para $d_{LE} = 0$ e $d_{LE} = 3$ e do sistema de modulação adaptativa convencional. As RSR médias do canal legítimo e do espião foram mantidas iguais em todos os casos.

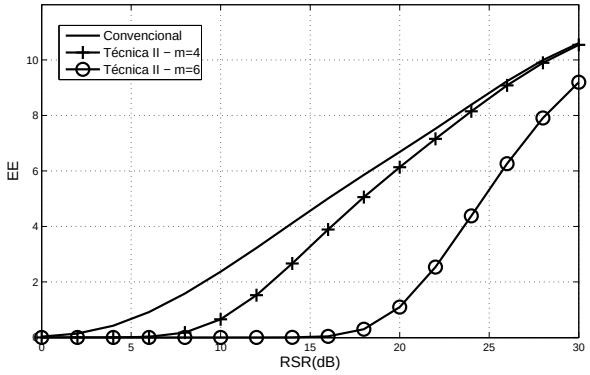

Fig. 7. EE da técnica proposta II para valores selecionados de m e do sistema de modulação adaptativa convencional. As RSR médias do canal legítimo e do espião foram mantidas iguais em todos os casos.

neste caso para a Técnica I, e, para fins de referência, para um sistema que utiliza modulação adaptativa convencional[1]. Nesse caso empregou-se d_{LE} igual a 0 e 3. Pode-se observar nessa figura um aumento da probabilidade de erro do espião com d_{LE} para todos os valores de RSR simulados. Para todos os casos avaliados, as curvas analíticas estão bem ajustadas aos resultados obtidos por simulação computacional, portanto, a partir da Figura 6, foram suprimidas as curvas obtidas por meio de simulação por questões de legibilidade. A violação da BER alvo para o caso de $d_{LE} = 3$ ocorre em razão dos limiares de adaptação terem sido calculados para a técnica de modulação adaptativa convencional, e não para a técnica proposta.

Ainda para o mesmo cenário, a Figura 5 mostra a comparação entre a EE da modulação adaptativa convencional e a da Técnica I. Verificou-se uma degradação da EE com o aumento de d_{LE}. Isso se justifica pela redução da probabilidade de ocorrer transmissão com o aumento de d_{LE}. Ou seja, para esse sistema, existe um compromisso entre a degradação de desempenho do espião (aumento da capacidade de sigilo) e a EE do sistema de comunicação.

[1]Nos sistemas que utilizam a técnica de modulação adaptativa convencional, o funcionamento do transmissor não é influenciado pela presença do espião.

As Figuras 6 e 7 apresentam os resultados relativos à Técnica II, na qual o transmissor não dispõe das informações do estado do canal do espião. As RSR médias do canal legítimo e do espião foram mantidas iguais. Pode-se observar que mesmo neste caso é possível obter um aumento na probabilidade de erro do espião. Da mesma forma que ocorre no caso anterior, esse aumento é acompanhado de uma degradação na EE do sistema.

Vale ressaltar que, para as duas técnicas aqui propostas, a degradação observada na EE é resultante de períodos de ociosidade do canal de comunicação. A Figura 8 mostra um histograma da utilização do canal legítimo para a técnica II com $m = 5$ e para alguns valores de RSR média. Para as RSR médias menores ou iguais a 19dB, o canal legítimo passou a maior parte do tempo ocioso. Observa-se que esse tempo se reduz com o aumento da RSR e que a transmissão, quando ocorre, se dá com elevada EE. A Figura 9 apresenta as curvas de EE considerando todo o tempo de transmissão e apenas os momentos em que o canal legítimo é efetivamente ocupado. Assim sendo, o uso dessa estratégia em conjunto com o emprego de rádios cognitivos [9], os quais se propõem a explorar a ociosidade dos sistemas de comunicações, pode promover o uso global do espectro de forma eficiente.

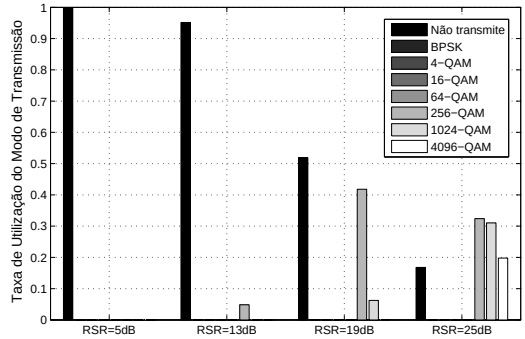

Fig. 8. Taxa de uso do canal legítimo para a técnica II com m=5 para valores selecionados de RSR média.

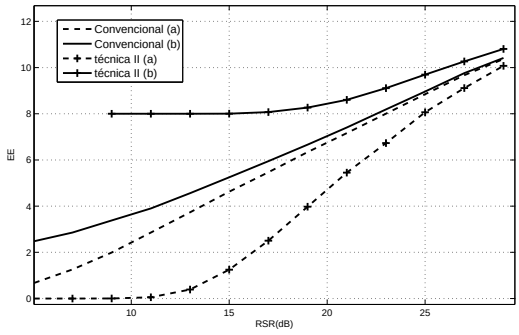

Fig. 9. EE da técnica II com m=5 e do sistema de modulação adaptativa convencional considerando-se, no caso (a), todo o tempo de transmissão e, no caso (b), apenas o tempo em que o canal foi efetivamente ocupado. As RSR médias do canal legítimo e do espião foram mantidas iguais em todos os casos.

V. Conclusão

Neste trabalho mostra-se que existe uma degradação da probabilidade de erro do espião em relação aquela obtida no canal legítimo quando são utilizadas técnicas de modulação adaptativa em sistemas de comunicação cujos canais são sujeitos ao efeito de desvanecimento plano e variante no tempo. Para potencializar essa característica natural dessas técnicas, são propostas duas técnicas de transmissão. As expressões analíticas de probabilidade de erro de bit e EE dessas técnicas são obtidas e validadas por meio de comparação com resultados empíricos obtidos por simulação de Monte Carlo.

Evidencia-se um compromisso entre taxa de erro de bit do espião e EE nas técnicas propostas, no sentido que o aumento na capacidade de sigilo da técnica proposta é acompanhado de uma degradação da EE. Além disso, observa-se que a baixa EE média decorre da existência de períodos de ociosidade do canal. Sendo assim, mensagens não sigilosas podem ser transmitidas nesses períodos. Cabe salientar o aumento da EE nos momentos de efetiva utilização do canal legítimo, o que também contribui para a segurança pois diminui o tempo de tráfego de informações sigilosas no canal de comunicação. Outra característica interessante das técnicas de modulação adaptativa relativa à segurança é a manutenção da probabilidade de erro de bit do receptor legítimo em valores baixos, o que diminui a necessidade de retransmissões dificultando ainda mais o trabalho de interceptação realizado pelo espião.

Vale ressaltar que os resultados aqui apresentados, no que se refere à degradação de desempenho da probabilidade de erro do espião, são pessimistas, pois piores probabilidades de erro para ele podem ser atingidas ao se abandonar a hipótese dele conhecer a todo momento a modulação utilizada pelo transmissor.

Agradecimentos

Os autores desejam agradecer o apoio financeiro prestado pela Capes (Pró-defesa No 01/2008) e aos revisores anônimos por suas valiosas sugestões.

Referências

[1] Shannon, C. E., *Communication Theory of Secrecy systems*. Bell System Technical Journal, vol. 28, pp. 656-715, October 1949.

[2] Wyner, A. D., *The Wire-Tap Channel*. Bell System Technical Journal, vol. 54, No. 8, pp. 1355-1387, 1975.

[3] Gopala, P. K., Lai, L. e Gamal, H. E. *On the Secrecy Capacity of Fading Channels*. IEEE Transactions on Information Theory, Vol. 54, No. 10, pp. 4687-4698, October 2008.

[4] Barros, J. e Rodrigues, M. R. D., *Secrecy Capacity of Wireless Channels*. IEEE international symposium on Information Theory, pp. 356-360, July, 2006.

[5] Negi, R. e Satashu, G., *Secret Communication using Artificial Noise*. IEEE 62nd Vehicular Technology Conference, vol. 3, pp. 1906-1910, September, 2005.

[6] Hossain, Md. J. , Vitthaladevuni, P. K. , Alouini, M. -S , Bhargava, V. K. e Goldsmith, A. J. *Adaptative Hierarchical Modulation for Simultaneous Voice and Multi-Class Data Transmission Over Fading Channels*. IEEE Transactions on Vehicular Technology, vol. 55, No. 4,pp. 1181-1194, July 2006.

[7] Parsons, J. D., *The Mobile Radio Channel*. John Wiley, 1992.

[8] Cho, K. e Yoon, D., *On the General BER Expression of One- and Two-Dimensional Amplitude Modulations*. IEEE Transactions on Communications, Vol. 50, No. 7, July 2002.

[9] Haykin, S., Thomson, D. J. e Reed, J. H., *Spectrum Sensing for Cognitive Radio*. Proceedings of the IEEE, vol. 97, No. 5, May 2009.

Apêndice I

Neste apêndice mostra-se que a probabilidade de $c_L - c_E > d$ dado que $c_L = i$ é:

$$Pr(c_L > c_E + d | c_L = i) = \begin{cases} \sum_{j=0}^{i-(d+1)} \tilde{\pi}_j & , \ i > d \\ 0 & , \ c.c. \end{cases} \quad (23)$$

Para $i \leq d$, essa probabilidade é zero, visto que $c_E \geq 0$. Para $i > d$, temos que

$$Pr(c_L > c_E + d | c_L = i) = \quad (24)$$

$$= \frac{Pr(c_E < c_L - d | c_L = i)}{Pr(c_L = i)} \quad (25)$$

$$= \frac{\int_{\lambda_0}^{\lambda_{i-d}} \int_{\lambda_i}^{\lambda_{i+1}} f_{\bar{\alpha},\bar{\beta}}(\alpha, \bar{\alpha}; \beta, \bar{\beta}) d_\alpha d_\beta}{\int_{\lambda_i}^{\lambda_{i+1}} f_{\bar{\alpha}}(\alpha, \bar{\alpha}) d_\alpha}.$$

Devido à independência,

$$Pr(c_L > c_E + d | c_L = i) = \quad (26)$$

$$= \sum_{l=0}^{i-(d+1)} \int_{\lambda_i}^{\lambda_{i+1}} f_{\bar{\beta}}(\beta, \bar{\beta}) d_\beta \quad (27)$$

$$= \sum_{l=0}^{i-(d+1)} \tilde{\pi}_j. \quad (28)$$