INSTITUTO MILITAR DE ENGENHARIA

1º TEN ALEXANDRE AMORIM PEREIRA JÚNIOR

TAXA DE SIGILO DE ENLACES QUE EMPREGAM TÉCNICAS DE MODULAÇÃO ADAPTATIVA EM CANAIS COM DESVANECIMENTO PLANO

Dissertação de Mestrado apresentada ao Curso de Mestrado em Engenharia Elétrica do Instituto Militar de Engenharia, como requisito parcial para obtenção do título de Mestre em Ciências em Engenharia Elétrica.

Orientador: Maj Juraci Ferreira Galdino, D. C.

Rio de Janeiro
2009

INSTITUTO MILITAR DE ENGENHARIA
Praça General Tibúrcio, 80-Praia Vermelha
Rio de Janeiro-RJ CEP 22290-270

P436t Pereira Júnior, Alexandre Amorim
Taxa de Sigilo de Enlaces que empregam Técnicas de Modulação Adaptativa em Canais com Desvanecimento Plano/ Alexandre Amorim Pereira Júnior.
– Rio de Janeiro: Instituto Militar de Engenharia, 2009.
99 p.: il.

Dissertação: (mestrado) – Instituto Militar de Engenharia, Rio de Janeiro, 2009.

1. Sistemas de comunicação sem fio. 2. Modulação Adaptativa. 3. Canal com Desvanecimento Plano. I. Título. II. Instituto Militar de Engenharia.

CDD 621.3845

INSTITUTO MILITAR DE ENGENHARIA

1º TEN ALEXANDRE AMORIM PEREIRA JÚNIOR

TAXA DE SIGILO DE ENLACES QUE EMPREGAM TÉCNICAS DE MODULAÇÃO ADAPTATIVA EM CANAIS COM DESVANECIMENTO PLANO

Dissertação de Mestrado apresentada ao Curso de Mestrado em Engenharia Elétrica do Instituto Militar de Engenharia, como requisito parcial para obtenção do título de Mestre em Ciências em Engenharia Elétrica.

Orientador: Maj Juraci Ferreira Galdino, D. C.

Aprovada em 16 de Dezembro de 2009 pela seguinte Banca Examinadora:

Maj Juraci Ferreira Galdino, D. C. do IME - Presidente

Edmar Candeia Gurjão, D. C. da UFCG

Ernesto Leite Pinto, D. C. do IME

Francisco Marcos de Assis, D. C. da UFCG

Rio de Janeiro
2009

AGRADECIMENTOS

A Deus, por estar sempre presente, principalmente nos momentos mais difíceis.

Aos meus pais Alexandre e Rosangela, meus primeiros mestres, pelo amor que sempre me dedicaram e pelo apoio que sempre me propiciaram.

Ao meu orientador, Maj Juraci Ferreira Galdino, pelos ensinamentos transmitidos, pela disponibilidade e atenção despendida durante esses dois anos de curso e pela confiança no meu trabalho.

Aos professores do programa de pós-graduação em engenharia elétrica, pelo exemplo de mestres que são.

Aos amigos Daniel, Fábio, Humberto, Ingrid, João Paulo, Machado, Rodrigo e Thiago, pela amizade e companherismo nos diversos trabalhos realizados.

As amigas Gisela e Melissa, pela amizade incondicional e por entenderem as prolongadas ausências.

Por fim, a todos que me ajudaram a concluir mais esse desafio.

"A mente que se abre a uma nova idéia jamais voltará ao seu tamanho original."

Albert Einstein

SUMÁRIO

LISTA DE ILUSTRAÇÕES 8

LISTA DE TABELAS 11

LISTA DE ABREVIATURAS E SÍMBOLOS 12

1 INTRODUÇÃO 18

2 A TÉCNICA DE MODULAÇÃO ADAPTATIVA 23
2.1 Introdução 23
2.2 O canal de comunicação variante no tempo 23
2.3 Técnicas de modulação adaptativa 26
2.3.1 Características 26
2.3.2 Modulação adaptativa em canais com desvanecimento plano e lento 31
2.4 Temas atuais de pesquisa 35
2.5 Resumo 38

3 TEORIA DA INFORMAÇÃO E SEGURANÇA NAS COMUNICAÇÕES 39
3.1 Introdução 39
3.2 Conceitos básicos da teoria da informação 40
3.2.1 Entropia - $H(X)$ 40
3.2.2 Informação Mútua - $I(X;Y)$ 41
3.2.3 Capacidade de um canal de comunicação 41
3.2.4 Capacidade de Sigilo (C_s) e Taxa de Sigilo (R_s) 43
3.3 Teoria da informação e segurança nas comunicações 44
3.4 Cenário de estudo 46
3.5 Resumo 48

4 MODULAÇÃO ADAPTATIVA E SEGURANÇA NAS COMUNICAÇÕES 49
4.1 Introdução 49
4.2 Avaliação da Taxa de Erro de Bit do espião 49
4.2.1 Taxa de erro de bit do espião 49
4.2.2 Resultados numéricos e simulações 50

4.3 Informação mútua e Taxa de sigilo das técnicas de modulação adaptativa . 52
4.3.1 Informação mútua e Taxa de sigilo 52
4.3.2 Aproximação para a IM entre o transmissor e o receptor legítimo 54
4.3.3 Limite inferior para R_s dos sistemas de modulação adaptativa 58
4.3.4 Resultados numéricos 63
4.4 Resumo 69

5 PROPOSTAS DE ESTRATÉGIAS DE MODULAÇÃO ADAPTATIVA PARA AUMENTAR A TAXA DE SIGILO 72
5.1 Introdução 72
5.2 Técnicas propostas 72
5.2.1 Técnica I 72
5.2.2 Técnica II 75
5.2.3 Técnica III 77
5.2.4 Técnica IV 78
5.3 Resultados numéricos e simulações 79
5.3.1 Técnicas I e II 79
5.3.2 Técnica III 81
5.3.3 Técnica IV 87
5.4 Resumo 90

6 CONSIDERAÇÕES FINAIS 91
6.1 Conclusões 91
6.2 Propostas para trabalhos futuros 92

7 REFERÊNCIAS BIBLIOGRÁFICAS 94

8 APÊNDICES 97
8.1 Informação Mútua entre S e $\hat{S}$ dado o estado do canal legítimo 98

LISTA DE ILUSTRAÇÕES

FIG.2.1 Desvanecimento em larga escala e desvanecimento em pequena escala. Extraído de (RAPPAPORT, 2002). 24
FIG.2.2 Diagrama dos tipos de desvanecimento. 27
FIG.2.3 Ganho de um canal sujeito as desvanecimento plano e lento. Intervalo de 10s. 29
FIG.2.4 Ganho de um canal sujeito as desvanecimento plano e lento. Intervalo de 20ms. 29
FIG.2.5 Diagrama de blocos em banda base de um sistema de modulção adaptativa. 31
FIG.2.6 BER de sistemas de modulação adaptativa. 36
FIG.2.7 EE de sistemas de modulção adaptativa. 36

FIG.3.1 Relações entre entropia e informação mútua. Extraído de (COVER, 2006). 42
FIG.3.2 Modelo de um sistema simplificado de comunicação. 42
FIG.3.3 Modelo de Wyner - *The wiretap channel*. 45
FIG.3.4 Cenário de comunicação sob investigação. 47

FIG.4.1 BER dos canais legítimo e espião para a técnica de modulação adaptativa e para a modulação fixa 4-QAM. 51
FIG.4.2 Constelação da modulação 64−QAM. 55
FIG.4.3 Taxa de erro de símbolo exata e aproximada para modulações 64-QAM, 256-QAM, 1024-QAM e 4096-QAM em canal AWGN em função da RSR. 56
FIG.4.4 Curvas de $\bar{R}_s$ para limiares que maximizam $\bar{R}_s$. 62
FIG.4.5 Curvas de R_s e $\bar{R}_s$ para limiares que maximizam $\bar{R}_s$ e limiares que atendem $\alpha = 10^{-2}$. 64
FIG.4.6 Curvas de IM analíticas e simuladas em função da RSR média. 66
FIG.4.7 Curvas de capacidade e IM para as estratégias I, II e III em função de P/N_0. 67
FIG.4.8 Curvas de BER média do receptor legítimo para as estratégias I e III em função de P/N_0. 68

FIG.4.9 Curvas de IM do receptor legítimo para as estratégias I e IV em função da RSR média para $\alpha = 10^{-2}$, $\alpha = 10^{-3}$ e $\alpha = 10^{-4}$. 69
FIG.4.10 Curvas de R_s para as estratégias I, III e IV em função da RSR média, considerando $\alpha = 10^{-3}$ e limiares que maximizam I_L. 70
FIG.4.11 Curvas de R_s para a estratégia I com $\alpha = 10^{-3}$ em função de $\bar{\gamma}_L/\bar{\gamma}_E$ para $\bar{\gamma}_E = 10$ dB e $\bar{\gamma}_E = 20$ dB. 71

FIG.5.1 BER dos canais legítimo e espião para a técnica I com $d_{LE} = 0$ e $d_{LE} = 3$ e da técnica de modulação adaptativa. 80
FIG.5.2 EE da técnica I com $d_{LE} = 0$ e $d_{LE} = 3$ e da técnica de modulação adaptativa. 80
FIG.5.3 BER dos canais legítimo e espião da técnica II com m=4 e m=6 e da técnica de modulação adaptativa. 82
FIG.5.4 EE da técnica II para m=4 e m=6 e da técnica de modulação adaptativa. 82
FIG.5.5 Taxa de uso do canal legítimo para a técnica II com m=5 para valores selecionados de RSR média. 83
FIG.5.6 EE da técnica II com m=5 e da técnica de modulação adaptativa considerando, no caso (a), todo o tempo de transmissão e, no caso (b), apenas o tempo em que o canal foi efetivamente ocupado. 83
FIG.5.7 R_s da técnica II com $m = 3$ e $m = 5$ e da técnica de modulação adaptativa convencional. 84
FIG.5.8 Curvas de R_s para as estratégias I, III e IV para limiares que maximizam a EE restritos a $\alpha = 10^{-3}$, limiares que maximizam I_L e limiares que maximizam R_s. 85
FIG.5.9 Curvas de BER_L para as estratégias I, III e IV para limiares que maximizam a EE restritos a $\alpha = 10^{-3}$, limiares que maximizam I_L e limiares que maximizam R_s. 85
FIG.5.10 Curvas de BER_E para as estratégias I, III e IV para limiares que maximizam a EE restritos a $\alpha = 10^{-3}$, limiares que maximizam I_L e limiares que maximizam R_s. 86
FIG.5.11 Curvas de BER para a estratégia IV em função da RSR média dos canais legítimo e espião para constelações rotacionadas. 88
FIG.5.12 Curvas de I_E para a estratégia IV em função da RSR média dos

canais legítimo e espião para constelações rotacionadas. 88
FIG.5.13 Curvas de EE e R_s para a estratégia IV em função da RSR média dos canais legítimo e espião para constelações rotacionadas. 89

LISTA DE TABELAS

TAB.2.1 Condições em que um canal pode ser considerado plano em frequência e lento no tempo. 27
TAB.2.2 Vetor de limiares de adaptação para diversos valores de α. 35

TAB.4.1 Valores mínimos de RSR em que se pode considerar que apenas ocorrem erros entre símbolos adjacentes. 57
TAB.4.2 Complexidade do cálculo da IM. 58
TAB.4.3 Limiares de adaptação utilizados em cada caso. 63
TAB.4.4 Modos de transmissão disponíveis em cada estratégia de transmissão. 64
TAB.4.5 Conjunto de limiares de adaptação. 65

TAB.5.1 Conjunto de limiares de adaptação para as estratégias I, III e IV que maximizam R_s. 84
TAB.5.2 Casos de escolha das sequências de ângulos de rotação. 87

LISTA DE ABREVIATURAS E SÍMBOLOS

ABREVIATURAS

AWGN	-	Additive White Gaussian Noise
BER	-	Bit Error Rate
BPSK	-	Binary Phase Shift Keying
DEP	-	Densidade Espectral de Potência
DFE	-	Decision Feedback Equalizer
EE	-	Eficiência Espectral
END	-	Estratégia Nacional de Defesa
fdp	-	Função Densidade de Probabilidade
IEEE	-	Institute of Electrical and Electronics Engineers
IES	-	Interferência Entre Símbolos
IM	-	Informação Mútua
MIMO	-	Multipli-Input Multiple-Output
M-QAM	-	Multilevel Quadrature Amplitude Modulation
OFDM	-	Orthogonal Frequency Division Multiplexing
pmf	-	Probability Mass Function
QAM	-	Quadrature Amplitude Modulation
RSR	-	Razão Sinal Ruído
SER	-	Symbol Error Rate
TLS	-	Transport Layer Security
v.a.	-	Variável Aleatória
WiMAX	-	Worldwide Interoperability for Microwave Access
WMAN	-	Wireless Metropolitan Area Network

SÍMBOLOS

$\mathcal{A}_i^l$	-	Conjunto dos símbolos adjacentes ao símbolo i da constelação da modulação l
$\mathcal{A}_i^{*l}$	-	União de $\mathcal{A}_i^l$ com o conjunto unitário formado pelo símbolo i
$\overline{BER_E}^l$	-	BER média do espião dado que $c_L = l$
$\overline{BER_l}$	-	BER média dado que $c_L = l$
c	-	Estado do canal avante
c_E	-	Estado do canal espião
c_L	-	Estado do canal legítimo
C	-	Capacidade de informação
C_E	-	Capacidade do canal do espião
C_L	-	Capacidade do canal legítimo
C_s	-	Capacidade de sigilo
d_{LE}	-	Diferença mínima entre c_L e c_E para que ocorra transmissão segundo a técnica proposta I
d_{min_l}	-	Distância mínima entre símbolos da modulação l
$D(p\|\|q)$	-	Entropia relativa entre p e q
erfc	-	Função erro complementar
EE	-	Eficiência espectral média
E_b	-	Energia média do bit
f_0	-	Banda de coerência do canal
f_D	-	Máximo desvio Doppler
$f_{Doppler}$	-	Desvio Doppler
g_k	-	Ganho do canal espião
h_k	-	Ganho do canal legítimo
$H(X)$	-	Entropia de X
I_E	-	Informação mútua do espião
I_{El}	-	Informação mútua do espião dado que $c_L = l$
I_L	-	Informação mútua do receptor legítimo
I_{Ll}	-	Informação mútua do receptor legítimo dado que $c_L = l$
$I(X;Y)$	-	Informação mútua entre X e Y
k	-	Índice do instante de tempo kT considerado

m	-	Estado mínimo para a transmissão segundo a técnica II
Mc_l	-	Número de componentes distintas em fase da constelação do modo de transmissão l
M_l	-	Número de símbolos distintos da constelação do modo de transmissão l
Ms_l	-	Número de componentes distintas em quadratura da constelação do modo de transmissão l
N	-	Número de modulações disponíveis
N_0	-	DEP do ruído aditivo do canal legítimo
$\tilde{N}_0$	-	DEP do ruído aditivo do canal espião
p_{64}	-	Probabilidade de erro de símbolo da modulação 64-QAM
$P_b(\gamma, M_l)$	-	BER da modulação M_l-QAM em canal AWGN com RSR γ
P_E	-	Taxa de erro de bit média do espião
P_L	-	Taxa de erro de bit média do receptor legítimo
$P(\bar{\gamma})$	-	Probabilidade de erro de bit média
$q_l(\gamma)$	-	Probabilidade de erro entre símbolos adjacentes da constelação da modulação l
$Q(\cdot)$	-	Função Q
R	-	Taxa de transmissão
R_s	-	Taxa de sigilo
$\bar{R}_s$	-	Limite inferior para a taxa de sigilo
$R_{s_{nv}}$	-	Parcela de R_s referente aos símbolos não vizinhos
$\bar{R}_{s_{nv}}$	-	Aproximação de $R_{s_{nv}}$
R_{s_v}	-	Parcela de R_s referente aos símbolos vizinhos
$\hat{S}_E$	-	Símbolos detectados no espião
s_k	-	k-ésimo símbolo transmitido
$\hat{S}_L$	-	Símbolos detectados no receptor legítimo
$\mathbf{S}$	-	Símbolos transmitidos
$\hat{\mathbf{S}}$	-	Símbolos detectados
$SER_{aproximada}$	-	Taxa de erro de símbolo aproximada
SER_{exata}	-	Taxa de erro de símbolo exata
T	-	Período de símbolo do sinal transmitido
T_0	-	Tempo de coerência do canal
T_m	-	Máximo atraso em excesso do canal

$u_l(\cdot)$	-	Função degrau unitário
V	-	Velocidade relativa do móvel
W	-	Largura de banda do sinal transmitido
$\mathcal{W}$	-	Mensagem a ser transmitida
X	-	Sinal transmitido
$\mathcal{X}$	-	Alfabeto de símbolos de entrada de um canal discreto
$\mathbf{X}$	-	Vetor de símbolos a serem transmitidos
Y	-	Sinal recebido no receptor legítimo
$\mathbf{Y}$	-	Vetor de símbolos detectados pelo receptor legítimo
$\mathcal{Y}$	-	Alfabeto de símbolos de saída de um canal discreto
y_k	-	k-ésima amostra da observação do sinal na entrada do receptor legítimo
z_k	-	k-ésima amostra da observação do sinal na entrada do espião
Z	-	Sinal recebido no espião
$\mathbf{Z}$	-	Vetor de símbolos detectados pelo espião
α	-	Taxa de erro de bit alvo
γ	-	RSR instantânea
$\bar{\gamma}$	-	RSR média na entrada do receptor
γ_E	-	RSR instantânea na entrada do espião
$\bar{\gamma}_E$	-	RSR média na entrada do espião
γ_k	-	RSR instantânea na entrada do receptor
γ_L	-	RSR instantânea na entrada do receptor legítimo
$\bar{\gamma}_L$	-	RSR média na entrada do receptor legítimo
γ_{min}	-	Valor mínimo de RSR
η_k	-	Ruído aditivo do canal legítimo no k-ésimo intervalo de símbolo
$\tilde{\eta}_k$	-	Ruído aditivo do canal espião no k-ésimo intervalo de símbolo
θ	-	Ângulo entre a direção do movimento e a direção de propagação da onda eletromagnética
λ	-	Comprimento de onda da portadora
$\boldsymbol{\lambda}$	-	vetor de limiares de adaptação
λ_l	-	l-ésimo limiar de adaptação
π_l	-	Probabilidade de $c_L = l$
$\tilde{\pi}_l$	-	Probabilidade de $c_E = l$
$\lfloor \cdot \rfloor$	-	Menor inteiro maior que $\cdot$

RESUMO

Este trabalho aborda o uso das técnicas de modulação adaptativa em sistemas de comunicação cujos canais estão sujeitos ao efeito do desvanecimento plano em frequência e lento no tempo. Tradicionalmente, o emprego das técnicas de modulação adaptativa tem como objetivo o melhor aproveitamento do canal de comunicação variante no tempo, porém nesta dissertação é proposto o uso dessas técnicas como forma de aumentar a segurança das comunicações sem fio. Expressões analíticas para a taxa de erro de bit e para a taxa de sigilo do sistema analisado são apresentadas e seus resultados numéricos são discutidos.

Diversos trabalhos que tratam do sigilo nas comunicações sob o ponto de vista da teoria da informação baseiam-se em sistemas de transmissão hipotéticos, o que faz com que seus resultados produzam limites teóricos para os canais de comunicação, como os limites para a capacidade e capacidade de sigilo desses canais. Uma das contribuições dessa dissertação é justamente a obtenção de expressões de informação mútua, que podem ser comparadas às expressões teóricas de capacidade, e de taxa de sigilo, que tem sua referência na capacidade de sigilo, de sistemas de modulação adaptativa realizáveis na prática.

As expressões aqui apresentadas são obtidas com base em hipóteses comumente adotadas no contexto dos sistemas de comunicações sem fio, como, por exemplo, as suposições empregadas na modelagem estatística do canal de comunicação, do ruído aditivo e da informação transmitida. Além disso, elas são expressas em termos de parâmetros importantes das estratégias de modulação adaptativa, como a razão sinal ruído média dos canais de comunicação envolvidos e outros parâmetros das modulações empregadas.

Várias avaliações e comparações de desempenho são realizadas com base nessas expressões analíticas e em simulações computacionais de Monte Carlo, tendo como figuras de mérito a taxa de erro de bit, a eficiência espectral, a informação mútua e a taxa de sigilo dos sistemas analisados. As simulações realizadas validam as expressões encontradas. Os diversos resultados obtidos, sob variadas condições, indicam que as técnicas de modulação adaptativa, além de propiciarem um melhor aproveitamento do canal de comunicação variante no tempo, têm a capacidade de aumentar o sigilo na transmissão das informações. Os parâmetros dos sistemas de modulação adaptativa foram otimizados de forma a maximizar a sua taxa de sigilo e novas estratégias de transmissão baseadas nas técnicas de modulação adaptativa foram propostas de forma a potencializar o sigilo nas comunicações.

ABSTRACT

This work discuss the use of adaptive modulation techniques in wireless slow flat fading communication systems. Usually, adaptive modulation techniques are employed in order to better explore the instantaneous propagation characteristics of time-varying channels. However, this paper proposes the use of adaptive techniques as a mean to increase the security of wireless transmissions. Analytical expressions for the bit error rate and for the secrecy rate of these systems are presented and its numerical results are analyzed.

Many communication secrecy related works under the information theory point of view presents theoretical results for channel capacity and secrecy capacity of fading channels, since they are based on hypothetical transmission systems. One of the main contributions of this study is the attainment of the mutual information and secrecy rate expressions for the adaptive modulation systems that can be compared to the theoretical results of channel capacity and secrecy capacity.

The expressions presented here are based on commonly assumed hypothesis at the wireless transmission systems context, as, for example, the assumptions employed at the statistical modeling of the channels, of the additive noise and of the information source. Besides, these expressions are expressed in terms of pivotal parameters of the adaptive modulation techniques, as the mean signal to noise ratio of the involved communication channels and others parameters of the employed modulations schemes.

Several performance evaluations and comparisons based on the analytical expressions and via computer simulation are conducted in order to evaluate the bit error rate, the spectral efficiency, the mutual information and the secrecy rate of the analyzed systems. The simulation results validates the presented analytical expressions and many results obtained, upon several different conditions, indicate that the adaptive modulation techniques, besides providing better spectral efficiency with low bit error rate, have the capacity to increase the secrecy at communications under fading conditions. The adaptive modulation parameters were optimized in order to produce the maximum secrecy rate and new transmission techniques based on the adaptive modulation techniques were proposed in order to better explore the secrecy characteristics of adaptive modulation techniques.

1 INTRODUÇÃO

A crescente demanda por serviços multimídia em sistemas de comunicações sem fio ocorrida nas últimas décadas contribuiu com o aumento das pesquisas em diversos setores do conhecimento humano, tais como, processamento digital de sinais, transmissão digital, protocolos de comunicação, eletrônica digital e microeletrônica. Como resultado, as comunicações sem fio ocupam hoje um lugar de destaque na área de transmissão digital face à variedade de aplicações e serviços de grande interesse da sociedade. Atualmente, as redes de comunicação sem fio, além da facilidade de mobilidade propiciada, permitem a transmissão de informações a altas taxas, como, por exemplo, as redes de telefonia móvel 3G que fornecem serviços a taxas que chegam a 2 Megabits por segundo.

Esse aumento na capacidade das redes de comunicação sem fio foi possível por meio do aumento da eficiência espectral (EE) dos sistemas de comunicação que as compõem. Uma alternativa para aumentar a eficiência espectral dos sistemas de comunicações sem fio que vem sendo cada vez mais empregada é o uso das técnicas de transmissão adaptativa. Essas técnicas procuram explorar a variabilidade das condições de propagação dos canais por meio da adaptação dinâmica dos parâmetros do sistema de transmissão, como, por exemplo, a modulação utilizada, a taxa dos códigos corretores de erros e a potência de transmissão. A grande vantagem que essas técnicas possuem em relação às técnicas de transmissão fixa é que, diferentemente dessas últimas, que têm seus parâmetros projetados com base nas condições médias ou nas piores condições de propagação dos canais de comunicação, as técnicas de transmissão adaptativas podem aproveitar os momentos em que o canal encontra-se em boas condições de propagação para aumentar a eficiência espectral do sistema de comunicação por meio da utilização de modulações com mais pontos em suas constelações, ou por meio do uso de códigos corretores de erro com maiores taxas, sem prejudicar os requisitos de desempenho em termos de taxa de erro de bit (BER, do temo em inglês *Bit Error Rate*).

Um exemplo de utilização das técnicas adaptativas é o padrão IEEE 802.16 que veio para consolidar o conceito de rede metropolitana sem fio (WMAN, do temo em inglês *Wireless Metropolitan Area Network)* batizado de WiMAX (do termo em inglês

Worldwide Interoperability for Microwave Access). Esse padrão prevê a adaptação de modulação e de codificação.

As técnicas de modulação adaptativa, que têm recebido grande destaque nos últimos anos (CHATTERJEE, 2003; CONTI, 2005; AL-KEBSI, 2009), constituem um caso particular das técnicas de transmissão adaptativa nas quais se pode variar apenas o esquema de modulação adotado pelo transmissor. A melhoria na eficiência espectral é alcançada pelo uso de modulações com mais pontos em suas constelações nos momentos em que o canal apresenta melhores condições de propagação. Por outro lado, quando o canal de comunicação apresenta desvanecimentos profundos são utilizadas modulações com baixa eficiência espectral a fim de se manter a taxa de erro de bit a níveis aceitáveis para o sistema de comunicação. Dessa forma essas técnicas obtêm alta vazão de dados a custa de variações na sua taxa de transmissão e de uma maior complexidade computacional.

Além da busca de melhoria da eficiência espectral, outra questão de extrema importância para os sistemas de comunicação é a segurança nas comunicações, principalmente nos sistemas que empregam o espaço livre como canal de propagação, que são mais suscetíveis às recepções não autorizadas.

Devido à popularidade e variedade de aplicações das redes de comunicação sem fio, as operações realizadas por meio dessas redes variam desde simples conversas telefônicas até complexas transações bancárias e em diversos casos as informações trafegadas durante essas operações possuem caráter sigiloso e devem ser protegidas contra interceptações e adulterações. Assim sendo, torna-se valioso o desenvolvimento de técnicas que promovam a segurança do conteúdo trafegado em tais sistemas.

No âmbito militar, conforme (C24-18, 1997), o emprego das radiocomunicações constitui o principal meio de comunicação de muitas unidades táticas, sendo utilizada para comando, administração, ligação entre unidades, comunicação entre aviões etc. Por sua alta versatilidade e facilidade de instalação, aliada à crescente capacidade de integração com outros sistemas de comunicação, como redes corporativas ou redes de Comando e Controle, a segurança da informação nos sistemas rádio-móveis constitui tema de elevada relevância para as Forças Armadas, de um modo geral.

Além da evidente importância da segurança das comunicações militares, a sociedade civil também possui grande interesse em mecanismos que promovam a segurança nas comunicações sem fio, pois 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. A preocupação com a segurança das comunicações também está presente na esfera governamental, tanto que em 14 de julho de 2000 foi publicado no Diário Oficial da União o Decreto 3.505 que institui a Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal.

Mais recentemente, em 18 de dezembro de 2008, foi aprovada a Estratégia Nacional de Defesa (END) que objetiva modernizar a estrutura nacional de defesa, atuando em três eixos estruturantes dos quais um refere-se à reestruturação da indústria brasileira de material de defesa tendo como propósito assegurar que o atendimento das necessidades de equipamento das Forças Armadas apóie-se em tecnologias sob domínio nacional. Esta estratégia aponta três setores decisivos para a defesa nacional: o cibernético, o espacial e o nuclear. No que diz respeito ao setor cibernético, as tecnologias de comunicação se incluem como parte prioritária e, de acordo com a própria END, devem ser empregadas de forma a potencializar as capacidades de mobilidade e flexibilidade das Forças Armadas. Sendo assim, o desenvolvimento das tecnologias de comunicações sem fio tornaram-se tema de elevada importância para a defesa nacional.

O conceito de sigilo nas comunicações foi inicialmente introduzido por Shannon (SHANNON, 1949). Segundo ele, uma transmissão é realizada em sigilo absoluto quando um transmissor comunica-se com um receptor legítimo sem que um receptor não autorizado, com recursos computacionais ilimitados, tenha condições de recuperar a mensagem transmitida. A taxa com que se é capaz transmitir em sigilo absoluto é denominada de taxa de sigilo do sistema de comunicação. A importância do sigilo nas comunicações sem fio tem motivado não apenas o emprego de técnicas que garantam o sigilo nas comunicações, como, por exemplo, os códigos criptográficos que são utilizados nos diversos protocolos de comunicação, mas também o desenvolvimento de procedimentos de camada física que propiciem maior segurança nas comunicações.

Pelo crescente emprego das técnicas de modulação adaptativa em sistemas de comunicação cujos canais são modelados pelo efeito do desvanecimento, e pela importância da segurança em sistemas de comunicação sem fio, este trabalho pretende analisar, sob o ponto de vista da teoria da informação, o sigilo nas comunicações sem fio propiciado pela camada física, particularmente quando nelas são empregadas as técnicas de modulação adaptativa. O cenário analisado consiste em um transmissor

que troca informações com um receptor legítimo através de um canal sem fio sujeito a interceptação dos sinais transmitidos por parte de um receptor não autorizado, denominado de espião. A fim de se obter expressões analíticas para as grandezas aqui analisadas considerou-se canais modelados pelo efeito do desvanecimento plano e lento. A suposição de desvanecimento plano não é restritiva pois casos em que o desvanecimento é seletivo em frequência podem ser reduzidos ao caso do desvanecimento plano por meio do uso de técnicas de equalização ou técnicas OFDM (do inglês *Orthogonal Frequency Division Multiplexing*), nas quais este modelo pode ser empregado para caracterizar os canais das sub-portadoras (sub-canais OFDM).

A seguir, são apresentados os objetivos e contribuições principais desta dissertação:

- Provar que as técnicas de modulação adaptativa em canais com desvanecimento plano e lento provêem taxa de sigilo maior que zero nas comunicações;
- Propor técnicas de transmissão, baseadas nas técnicas de modulação adaptativa, de forma a potencializar o sigilo dos sistemas de comunicação sem fio;

A fim de se alcançar o primeiro objetivo, define-se os seguintes objetivos e contribuições secundárias:

- Obter a expressão analítica para a probabilidade de erro de bit de um receptor não autorizado em um sistema de comunicação que emprega as técnicas de modulação adaptativa em canais sujeitos ao desvanecimento plano e lento;
- Obter a expressão analítica para a informação mútua (IM) entre os símbolos detectados no receptor legítimo e os símbolos transmitidos, bem como a IM entre os símbolos detectados no espião e os símbolos transmitidos em sistemas que empregam as técnicas de modulação adaptativa em canais sujeitos ao desvanecimento plano e lento;
- Analisar a taxa de sigilo dos sistemas de comunicação que empregam as técnicas de modulação adaptativa em canais sujeitos ao desvanecimento plano e lento;

Esta dissertação está organizada em seis capítulos, conforme apresentado a seguir:

No Capítulo 2 são apresentados modelos mais comumente utilizados para descrever as variações dos canais empregados nos sistemas de comunicação sem fio. Além disso, são apresentadas as principais características das técnicas de modulação adaptativa, bem como suas vantagens e desvantagens. Diversos temas atuais de pesquisa

relacionados às técnicas de modulação adaptativa são comentados e, por fim, o sistema de modulação adaptativa adotado nesta dissertação é detalhado.

O Capítulo 3 aborda o tema da segurança nas comunicações em canais sem fio sob o ponto de vista da teoria da informação. Inicialmente os conceitos básicos de entropia, informação mútua e capacidade de informação do canal de comunicação são apresentados. Alguns trabalhos sobre o tema são comentados e o cenário sob investigação durante o restante do presente trabalho é descrito.

No Capítulo 4 são derivadas expressões analíticas para a taxa de erro de bit do espião bem como para a IM entre os símbolos detectados no receptor legítimo e os símbolos transmitidos e para a IM entre os símbolos detectados pelo espião e os símbolos transmitidos. A taxa de sigilo é calculada pela diferença entre a IM do receptor legítimo e a IM do espião e simulações são conduzidas com o objetivo de validar tais expressões. Neste capítulo prova-se que as técnicas de modulação adaptativa possibilitam a transmissão de informação em sigilo absoluto por meio do uso de um limite inferior para a taxa de sigilo dos sistemas que as empregam.

No Capítulo 5 são propostas quatro estratégias de transmissão baseadas nas técnicas de modulação adaptativa que visam potencializar o sigilo dos sistemas de transmissão. Duas delas baseiam-se na transmissão de informação apenas em momentos em que as condições de propagação do canal entre o transmissor e o receptor legítimo estão melhores do que as do canal entre o transmissor e o espião. A terceira consiste na otimização dos limiares de adaptação de forma a se maximizar a expressão da taxa de sigilo das técnicas de modulação adaptativa, e a última baseia-se na utilização das constelações das modulações empregadas rotacionadas por um ângulo que é desconhecido pelo espião, dificultando assim a detecção dos símbolos transmitidos.

As conclusões do trabalho e algumas propostas para a sua continuação são apresentadas no Capítulo 6.

2 A TÉCNICA DE MODULAÇÃO ADAPTATIVA

2.1 INTRODUÇÃO

As técnicas de modulação adaptativa apresentam melhores valores de EE em relação às modulações fixas pois elas têm a capacidade de adequar parâmetros da modulação empregada às variações do canal de comunicação. Sendo assim, na Seção 2.2 são apresentados modelos comumente empregados para descrever essas variações e os diversos tipos de distúrbios provocados pelos canais de comunicação sem fio.

Em seguida, na Seção 2.3, são apresentadas as principais características das técnicas de modulação adaptativa, bem como suas vantagens e desvantagens. Ainda nesta seção, é descrito o sistema de transmissão que emprega as técnicas de modulação adaptativa adotado nesta dissertação.

Finalmente, na Seção 2.4, diversos temas atuais de pesquisa são comentados.

2.2 O CANAL DE COMUNICAÇÃO VARIANTE NO TEMPO

O desempenho das técnicas de modulação adaptativa, bem como o de qualquer sistema de transmissão, é diretamente influenciado pelos distúrbios introduzidos pelos canais de comunicação. Dessa forma, a seguir será apresentado um resumo desses distúrbios e as modelagens estatísticas comumente empregadas para descrever o comportamento desses canais.

A Figura 2.1, extraída de (RAPPAPORT, 2002), ilustra a potência recebida no receptor de um sistema de comunicação rádio em ambiente fechado (*indoor*). Observa-se nessa figura que a potência do sinal muda rapidamente para pequenas variações na distância entre o transmissor e o receptor, porém a média local da potência do sinal recebido varia mais lentamente com essa distância. Sendo assim, para fins de análise, o desvanecimento é dividido em dois tipos: o desvanecimento em pequena escala e o desvanecimento em larga escala.

O desvanecimento em larga escala está relacionado às características dos canais de comunicação cujos efeitos são percebidos ao longo de médias e grandes distâncias quando comparadas ao comprimento de onda do sinal transmitido. Ele é consequência das obstruções naturais, como relevo e vegetação, bem como das obstruções oriundas

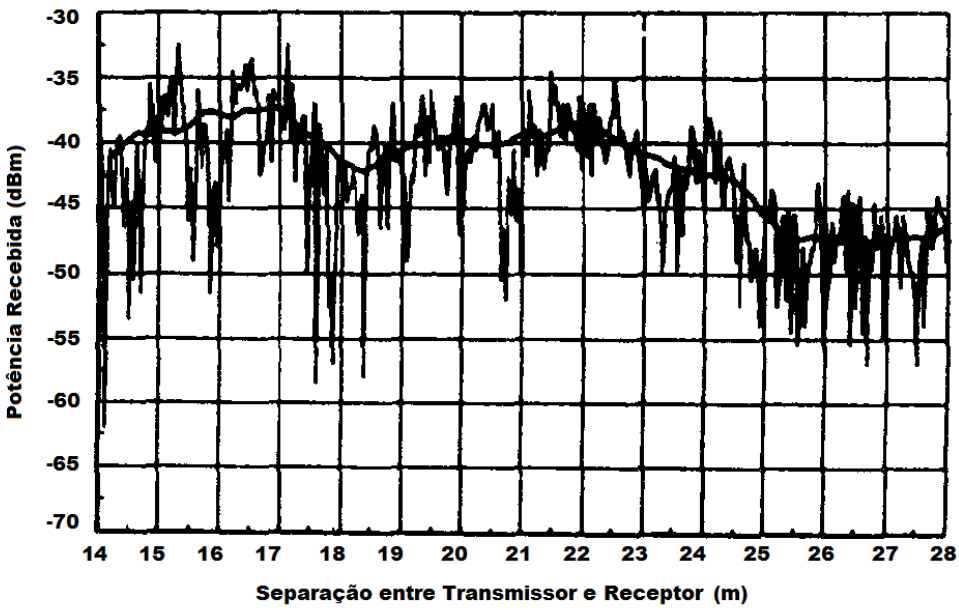

FIG. 2.1: Desvanecimento em larga escala e desvanecimento em pequena escala. Extraído de (RAPPAPORT, 2002).

de construções, como casas e edifícios, ao sinal transmitido. Essas obstruções fazem com que o receptor fique em uma região de "sombra", onde a potência do sinal recebido é bastante reduzida. Por esse motivo, esse tipo de desvanecimento também é chamado de "sombreamento". Em face de sua pequena variabilidade em relação ao desvanecimento em pequena escala ao longo do espaço e do tempo, e por não ser objeto de estudo dessa dissertação, o desvanecimento em larga escala será desconsiderado ao longo do texto.

Já o desvanecimento em pequena escala descreve flutuações "rápidas" das componentes em fase e amplitude do sinal rádio-móvel em um curto período de tempo ou em um pequeno deslocamento no espaço. Esse comportamento é causado pela interferência ente as componentes do sinal que percorrem caminhos distintos, chegando ao receptor com diferentes fases e amplitudes. Os três efeitos mais importantes causados pelo desvanecimento em pequena escala são:

a) Variações rápidas na potência do sinal recebido em pequenos deslocamentos no espaço ou pequenos intervalos de tempo;

b) Modulação em frequência causada pela variação no desvio Doppler sofrido pelas diferentes componentes de multipercurso;

c) Dispersão temporal causada pelos diversos atrasos das componentes de multi-

percurso que podem gerar interferência entre símbolos (IES).

O desvanecimento em pequena escala produz o espalhamento do sinal transmitido tanto no domínio do tempo quanto no domínio da frequência. Devido ao espalhamento temporal, a amplitude do sinal transmitido sofre alterações em suas diversas componentes espectrais. O desvanecimento é dito plano quando essas alterações são praticamente iguais em toda a faixa de frequência do sinal. Caso o sinal sofra modificações distintas para diferentes componentes frequenciais, o desvanecimento é dito seletivo em frequência.

Um dos parâmetros que classifica o desvanecimento como plano ou seletivo em frequência é a banda de coerência (f_0) do canal de comunicação. A f_0 de um canal indica a faixa de frequência em que o canal pode ser considerado plano (SKLAR, 1997). Se f_0 for maior do que a largura de banda do sinal transmitido (W), o desvanecimento sofrido por este sinal será dito plano, caso contrário é dito seletivo em frequência. No desvanecimento plano, apesar de serem preservadas as características espectrais do sinal transmitido, a sua intensidade pode variar devido às mudanças no ganho do canal.

O desvanecimento também pode ser caracterizado quanto ao espalhamento no domínio do tempo. Nesse caso, o espalhamento é dito plano quando o período de símbolo do sinal transmitido (T) é muito maior que o espalhamento provocado pelo canal, que pode ser medido pelo máximo atraso em excesso (T_m) definido a partir do perfil de potência de atraso do canal de comunicação, que consiste em uma média espacial das potências das respostas ao impulso do canal.

Quando o sinal transmitido está sujeito ao desvanecimento seletivo em frequência existe a possibilidade de ocorrer IES. Analisando no domínio do tempo, neste caso, T é próximo ou menor que T_m, o que possibilita a recepção de uma componente de multipercurso de um símbolo passado durante o intervalo de tempo destinado à recepção do símbolo atual, gerando dessa forma a mencionada interferência. No domínio da frequência tem-se que, no caso do desvanecimento seletivo em frequência, o sinal transmitido possui uma largura de banda que se aproxima ou é maior que f_0. Dessa forma, as componentes frequenciais do sinal transmitido que possuírem afastamento maior do que f_0 serão afetadas de forma diferente pelo canal de comunicação.

O espalhamento em frequência pode ser provocado pelo movimento relativo entre o transmissor e o receptor, bem como pelo movimento dos objetos que os circundam. Estes movimentos provocam uma variação nos diversos percursos que as diferentes

componentes do sinal transmitido percorrem. Por sua vez, a variação nos percursos percorridos pelo sinal transmitido gera uma variação aleatória de fase cuja taxa é percebida como uma variação de frequência do sinal recebido em cada percurso, denominada de desvio ou espalhamento Doppler. Esse desvio é diretamente proporcional à velocidade de deslocamento do receptor em relação à direção de propagação da onda, e é expresso por:

$$f_{Doppler} = f_D \times \cos(\theta), \tag{2.1}$$

na qual θ é o ângulo entre a direção do movimento relativo entre o transmissor e o receptor e a direção de propagação da onda eletromagnética e f_D é o máximo desvio Doppler, também denominado de taxa de desvanecimento, dado por:

$$f_D = \frac{V}{\lambda}, \tag{2.2}$$

sendo V a velocidade relativa do móvel e λ o comprimento de onda da portadora.

Definindo-se o tempo de coerência do canal (T_0) como o intervalo de tempo em que a resposta ao impulso do canal de comunicação pode ser considerada invariante, temos que $T_0 \approx 1/f_D$. No domínio do tempo, o desvanecimento é considerado lento quando a duração do símbolo do sinal transmitido é muito menor que o tempo de coerência, ou seja, quando $T \ll T_0$. Caso contrário, o desvanecimento é considerado rápido. Analogamente no domínio da frequência, o desvanecimento é considerado lento quando a largura de banda do sinal transmitido for muito maior que f_D.

Considerando $W \approx 1/T$, pode-se classificar o desvanecimento como lento caso $f_D T \ll 1$ e como rápido caso contrário.

A Figura 2.2 apresenta um diagrama contendo a classificação dos diversos tipos de desvanecimento. Neste trabalho são considerados apenas canais sujeitos ao desvanecimento plano em frequência e lento no tempo. A Tabela 2.1 resume as condições (em termos da comparação entre parâmetros da função de espalhamento do canal e parâmetros do sinal transmitido) que o canal deve atender para ser classificado como plano em frequência e lento no tempo.

2.3 TÉCNICAS DE MODULAÇÃO ADAPTATIVA

2.3.1 CARACTERÍSTICAS

Em canais variantes no tempo, como os descritos na Seção 2.2, as técnicas de transmissão que empregam potência de transmissão, codificação e modulações fixas

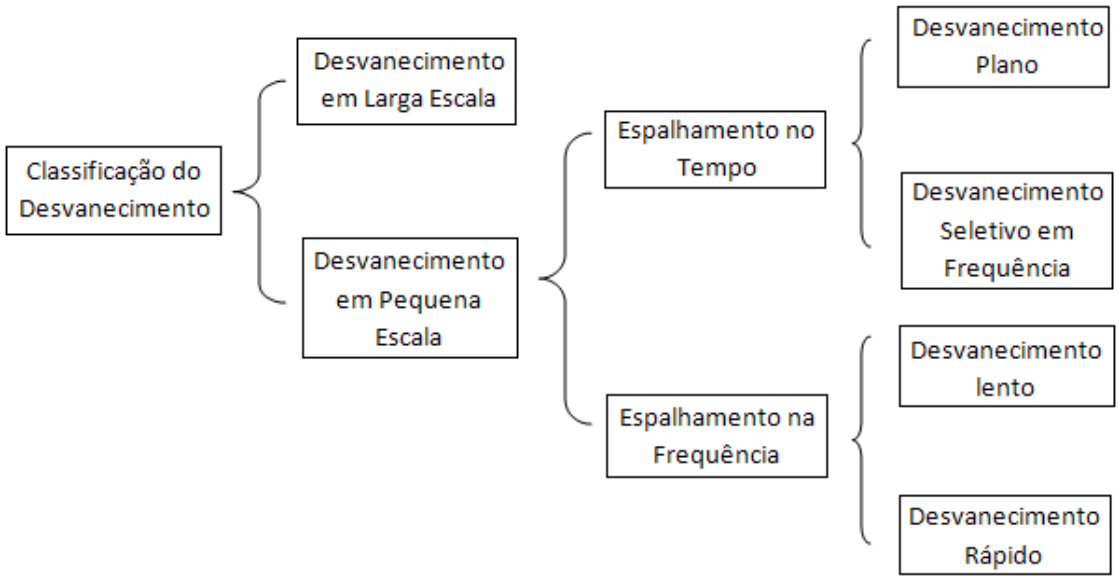

FIG. 2.2: Diagrama dos tipos de desvanecimento.

Desvanecimento	Plano em frequência	Lento no tempo
Domínio do tempo	$T \gg T_m$	$T \ll T_0$
Domínio da frequência	$W \ll f_0$	$W \gg f_D$

TAB. 2.1: Condições em que um canal pode ser considerado plano em frequência e lento no tempo.

enfrentam um sério problema no que diz respeito ao atendimento dos requisitos de desempenho, como os relativos à BER, EE e potência de transmissão. O desempenho desses sistemas depende apenas da razão sinal ruído (RSR) na entrada do receptor, que pode ser expressa em termos da razão entre a potência do sinal que chega no receptor e a potência do ruído que incide sobre este sinal. Em canais modelados apenas pelo efeito do ruído aditivo gaussiano branco, esta RSR oscila em torno da sua média, de acordo com a variância do ruído aditivo do sinal transmitido. Sendo assim, baseado nos valores médios da RSR, é possível a escolha prévia dos parâmetros dos sistemas de transmissão de forma a atender os requisitos desejados.

Porém, como mostrado na Seção 2.2, nos cenários sujeitos ao desvanecimento, mesmo que seja plano em frequência e lento no tempo, o ganho do canal pode apresentar grandes variações como tempo. A Figura 2.3 ilustra o comportamento do ganho de um canal sujeito ao desvanecimento plano e lento durante um intervalo de tempo de 10 segundos que foi normalizado a fim de produzir ganho médio unitário. Observando essa figura, tem-se a impressão que o desvanecimento não pode ser considerado lento, porém nota-se na Figura 2.4, que consiste apenas em uma mudança de escala temporal do gráfico apresentado na Fig. 2.3, que o canal permanece praticamente invariante durante um intervalo de cerca de 20ms. Considerando um transmissor hipotético que emprega uma portadora cuja frequência é de $1850MHz$ e uma velocidade relativa entre o transmissor e o receptor de $60km/h$, usando a Eq. (2.2), temos que $f_D \approx 102,88Hz$. Como nesse caso foi empregado $f_D T = 10^{-3}$, o período do símbolo é de aproximadamente $9,72 \times 10^{-3} ms$. Sendo assim, para o canal ilustrado nas figuras 2.3 e 2.4, em $20ms$ são transmitidos cerca de 2060 símbolos com o ganho do canal praticamente invariante, o que justifica a afirmação de canal com desvanecimento lento.

Apesar disso, pode-se observar que o canal apresenta ganhos em torno de $5dB$ e atenuações próximas de $35dB$, ou seja, uma variação de aproximadamente $40dB$. Nas situações de desvanecimento profundo, a RSR instantânea na entrada do receptor diminui significativamente, o que pode provocar a ocorrência de erros em surto.

A fim de contornar esse problema, as técnicas de transmissão que empregam potência de transmissão, codificação e modulações fixas são projetadas para atender aos requisitos de desempenho, como máxima taxa de erro de bit, nas situações em que o canal apresenta severas condições de propagação, ou nas características médias do canal. Essa abordagem apresenta o incoveniente de fazer uso ineficiente do canal de comunicação, pois na maior parte do tempo o canal pode apresentar boas condições

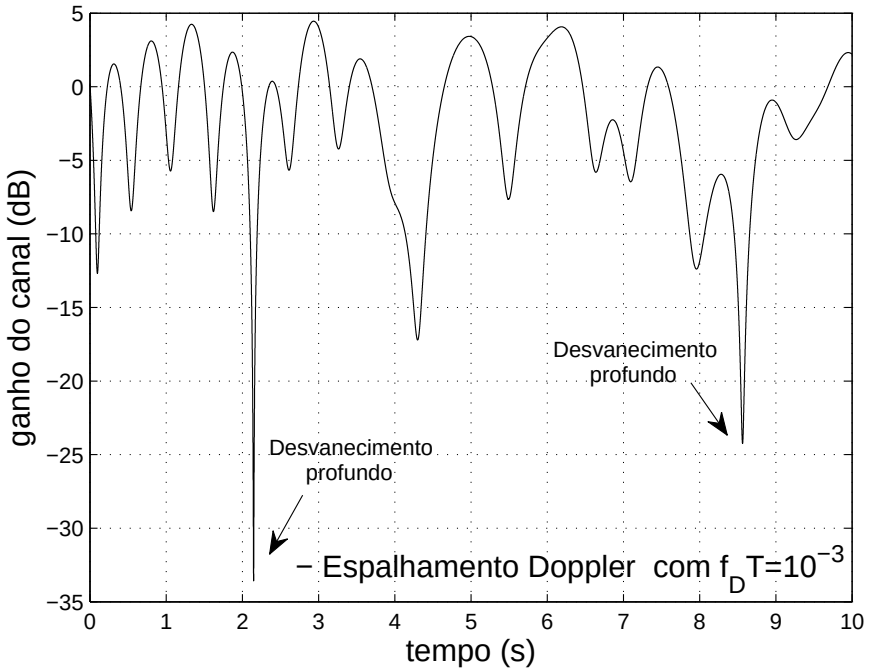

FIG. 2.3: Ganho de um canal sujeito as desvanecimento plano e lento. Intervalo de 10s.

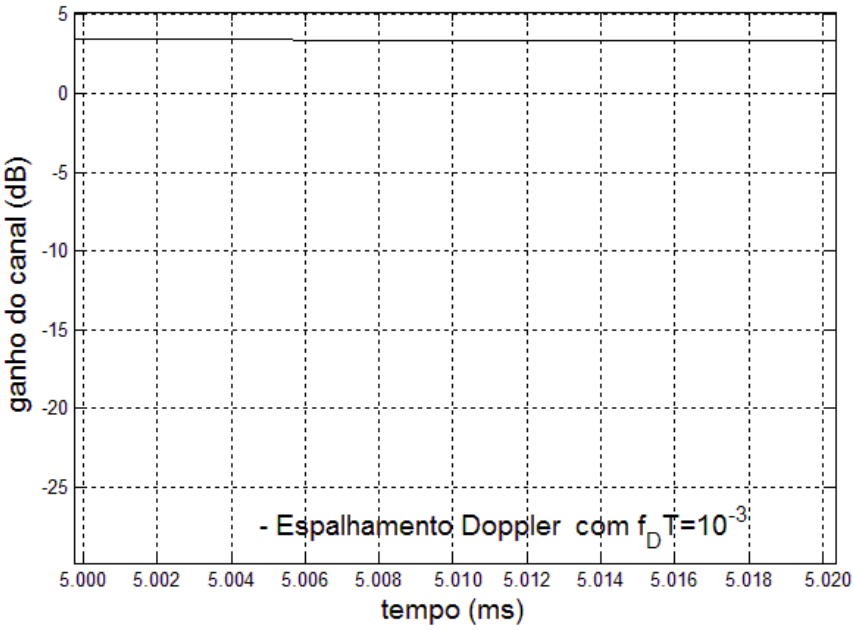

FIG. 2.4: Ganho de um canal sujeito as desvanecimento plano e lento. Intervalo de 20ms.

de propagação que não são exploradas.

As técnicas de transmissão adaptativas surgem como uma alternativa para o melhor aproveitamento do canal de comunicação variante no tempo, como os canais sem fio de telefonia móvel e enlaces via satélite (BUTCHART, 1998; QIU, 1999; ABDER-RAHMANE, 2007). Essas técnicas propõem a adaptação de diversos parâmetros de transmissão, como a potência, a modulação e a taxa dos códigos corretores de erro, da seguinte forma: quando o canal de comunicação apresentar excelentes condições de propagação, é possível atingir taxas de erro menores que os limites de desempenho impostos utilizando códigos corretores de erros com elevada taxa, ou empregando modulações com elevada EE, ou até mesmo com baixa potência de transmissão. Já nos momentos em que o canal apresenta profundos desvanecimentos, deve-se utilizar códigos corretores de erro com baixas taxas, ou modulações com pequena EE, ou aumentar a potência de transmissão de forma a atender aos requisitos de desempenho do sistema.

É nesse contexto que se enquadram os sistemas de comunicação que empregam as técnicas de modulação adaptativa. Nelas, o transmissor adapta apenas o esquema de modulação utilizado de acordo com as condições atuais de propagação do canal de comunicação. Esses sistemas têm se tornado cada vez mais atraentes que aqueles que empregam modulação fixa, pois apresentam melhor compromisso entre BER e EE permitindo economizar dois recursos extremamente valiosos: potência de transmissão e, principalmente, largura de banda.

O ganho em desempenho provido pelas técnicas de modulação adaptativa é acompanhado por um aumento na complexidade dos sistemas que as utilizam em relação aos sistemas que empregam modulação fixa. Nessas técnicas é necessário que haja o conhecimento do estado do canal de comunicação por parte do transmissor antes da transmissão ser realizada. Além disso, também faz-se necessário o conhecimento por parte do receptor da estratégia de modulação que foi empregada na transmissão dos diversos blocos de dados. Sendo assim, o uso das técnicas de modulação adaptativa possui suas limitações de emprego e diversas questões de pesquisa ainda estão em aberto. Por exemplo, devido à taxa de transmissão variável dos sistemas que empregam as técnicas de modulação adaptativa, pode-se citar como limitação de emprego dessas técnicas os sistemas sensíveis a essas variações, como os sistemas de videoconferência.

Normalmente o parâmetro utilizado para a escolha do esquema de modulação,

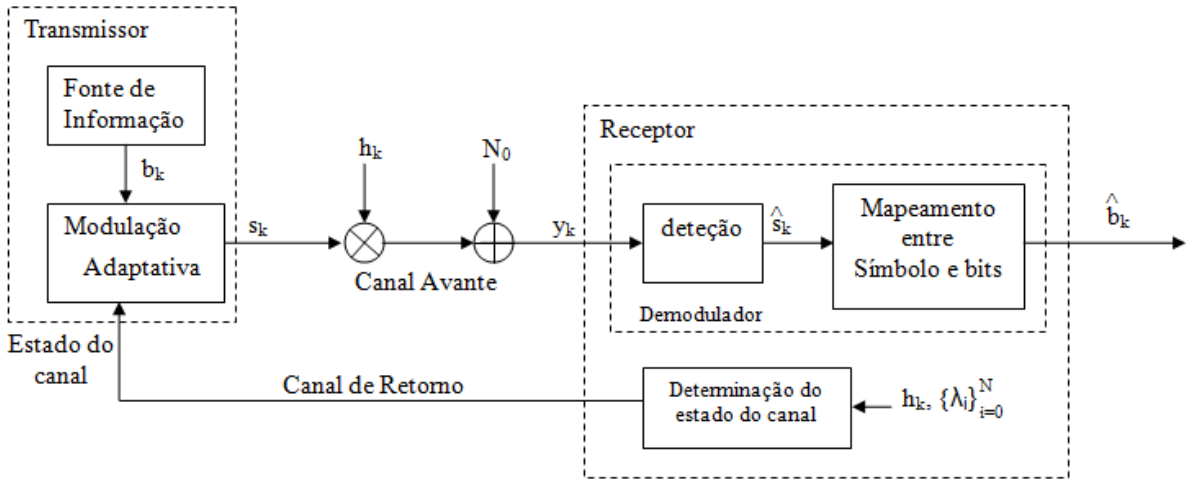

FIG. 2.5: Diagrama de blocos em banda base de um sistema de modulção adaptativa.

como, por exemplo, a RSR instantânea na entrada do receptor, é estimado no receptor e, a informação sobre qual esquema de modulação será empregado é enviada periodicamente ao transmissor por um canal de retorno.

Nesta dissertação, a fim de facilitar a obtenção das expressões analíticas desejadas, o canal de retorno será considerado ideal, ou seja, não introduz erros nem atraso na comunicação entre o receptor e o transmissor. A maioria dos trabalhos apresentados na literatura faz essa consideração com respeito ao canal de retorno, como por exemplo em (TORRANCE, 1996a) e (TORRANCE, 1996b). Ela é baseada na assertiva de que os erros no canal podem ser reduzidos a um nível desejado com a adoção de códigos corretores de erros (LIN, 2004) e o atraso pode ser combatido por meio do uso de preditores (DUEL-HALLEN, 2000) no receptor.

Na Seção 2.3.2 o emprego das técnicas de modulação adaptativa em canais sujeitos ao desvanecimento plano e lento com canal de retorno ideal é descrito em maiores detalhes. São apresentadas também as expressões de EE e BER média para esse sistema.

2.3.2 MODULAÇÃO ADAPTATIVA EM CANAIS COM DESVANECIMENTO PLANO E LENTO

A Figura 2.5 apresenta o diagrama de blocos do equivalente em banda básica do sistema de comunicação que emprega a técnica de modulação adaptativa adotada nesta dissertação.

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:

$$y_k = h_k s_k + \eta_k, \tag{2.3}$$

sendo h_k o ganho do canal avante, modelado por um processo gaussiano complexo de média nula, cujas componentes real e imaginária são estatisticamente independentes e de mesma variância. A densidade espectral de potência (DEP) deste processo é dada pelo espectro de Jakes (PARSONS, 2000), e η_k representa o ruído aditivo modelado por um processo gaussiano complexo branco de média nula e DEP igual a N_0, estatisticamente independente do canal de comunicação e do sinal transmitido. O índice k denota o instante de tempo considerado kT.

Em sistemas de modulação adaptativa, a observação y_k é empregada não apenas para detectar a informação transmitida, mas também para estimar a RSR instantânea na entrada do decisor, γ_k, que para canais sujeitos ao desvanecimento plano representa a qualidade do canal naquele instante, definida da seguinte forma:

$$\gamma_k \triangleq \bar{\gamma}|h_k|^2, \tag{2.4}$$

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.

Em seguida, o valor de γ_k é comparado a limiares de decisão para definir o estado do canal de comunicação. Considerando que a técnica de modulação adaptativa emprega N modos de operação, são definidas N regiões de decisão delimitadas por limiares λ_l, para $l = 0, \cdots, N$, sendo $\lambda_0 = 0$ e $\lambda_N \to \infty$. O estado do canal avante (c) é definido a partir desses limiares de tal forma que:

$$c = l \; se \; \{\gamma_k \in \mathbb{R} | \lambda_l \leq \gamma_k < \lambda_{l+1}\}. \tag{2.5}$$

Neste trabalho, considera-se que γ_k é conhecido no receptor. A informação sobre o estado do canal avante é então 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.

De acordo com a modelagem adotada para o canal de comunicação, $|h_k|$ segue uma distribuição de Rayleigh, e γ_k pode ser modelada por uma variável aleatória

exponencial cuja função densidade de probabilidade (fdp) é dada por:

$$f_{\bar{\gamma}}(\gamma_k) = \frac{1}{\bar{\gamma}} \cdot exp\left\{-\frac{\gamma_k}{\bar{\gamma}}\right\}. \tag{2.6}$$

Sendo assim, a probabilidade de $c = l$, denotada por π_l, é dada por:

$$\pi_l = \int_{\lambda_l}^{\lambda_{l+1}} f_{\bar{\gamma}}(\gamma_k) d\gamma_k = e^{\frac{-\lambda_l}{\bar{\gamma}}} - e^{\frac{-\lambda_{l+1}}{\bar{\gamma}}}. \tag{2.7}$$

Escolhe-se a estratégia de modulação l quando o canal avante estiver no estado l.

Os limiares de adaptação, definido pelo vetor $\boldsymbol{\lambda} = [\lambda_0, \cdots, \lambda_N]$, são obtidos resolvendo um problema de otimização com restrição que geralmente consiste em maximizar a EE média do sistema de comunicação, mantendo a sua probabilidade de erro de bit média ($P(\bar{\gamma})$) menor ou igual a α, ou seja, resolve-se o seguinte problema (TORRANCE, 1996a):

$$\boldsymbol{\lambda} = \max_{\boldsymbol{\lambda}^* \in \mathbb{R}^{N+1}} EE(\bar{\gamma}) \tag{2.8}$$

sujeito a:

$$\lambda_0 = 0, \tag{2.9}$$

$$\lambda_N = \infty, \tag{2.10}$$

$$P(\bar{\gamma}) \leq \alpha, \tag{2.11}$$

e

$$\lambda_i < \lambda_{i+1}. \tag{2.12}$$

A expressão analítica da taxa de erro de bit média desses sistemas pode ser derivada, como feito em (TORRANCE, 1996b), tomando-se a média da razão entre o número médio de bits errados e o número médio de bits transmitidos em cada modo de transmissão:

$$P(\bar{\gamma}) = \frac{1}{EE} \sum_{l=0}^{N-1} \pi_l \log_2(M_l) \overline{BER_l}, \tag{2.13}$$

sendo M_l o número de símbolos distintos da constelação do modo de transmissão l e $\overline{BER_l}$ a BER média dado que foi utilizado esse modo de transmissão.

Por sua vez, o cálculo de $\overline{BER_l}$ é feito por meio do valor esperado da probabilidade de erro de bit ao se utilizar a modulação l em um canal cuja RSR instantânea, γ, segue uma distribuição exponencial de média $\bar{\gamma}$. Sendo assim, $\overline{BER_l}$ é dada por:

$$\overline{BER_l} = \frac{1}{\pi_l} \int_{\lambda_l}^{\lambda_{l+1}} P_b(\gamma, M_l) \frac{1}{\bar{\gamma}} e^{-\frac{\gamma}{\bar{\gamma}}} d\gamma, \tag{2.14}$$

na qual $P_b(\gamma, M_l)$ é o valor da BER do modo de transmissão l em um canal AWGN com RSR igual a γ. Aplicando (2.14) em (2.13) chega-se a:

$$P(\bar{\gamma}) = \frac{1}{EE} \sum_{l=0}^{N-1} \log_2(M_l) \int_{\lambda_l}^{\lambda_{l+1}} P_b(\gamma, M_l) f_{\bar{\gamma}}(\gamma) d\gamma. \tag{2.15}$$

Geralmente, empregam-se nas técnicas de modulação adaptativa modulações M-QAM (do termo em inglês *Multilevel Quadrature Amplitude Modulation*) em razão do bom compromisso entre EE e BER propiciado por tais modulações (PROAKIS, 2001). A expressão fechada de $P_b(\gamma, M_l)$ para as modulações M_l-QAM foi apresentada em (CHO, 2002) e é dada pelas equações seguintes:

$$P_b(\gamma, M_l) = \frac{1}{\log_2 M_l} \left(\sum_{k=1}^{\log_2(Mc_l)} Pc_l(k) + \sum_{w=1}^{\log_2(Ms_l)} Ps_l(w) \right), \tag{2.16}$$

com

$$Pc_l(k) = \frac{1}{Mc_l} \sum_{i=0}^{(1-2^{-k})Mc_l - 1} \left\{ (-1)^{\left\lfloor \frac{i2^{k-1}}{Mc_l} \right\rfloor} \left[2^{k-1} - \left\lfloor \frac{i2^{k-1}}{Mc_l} + \frac{1}{2} \right\rfloor \right] \right.$$
$$\left. \cdot \operatorname{erfc}\left((2i+1) \sqrt{\frac{3\log_2(M_l)\gamma}{Mc_l^2 + Ms_l^2 - 2}} \right) \right\}, \tag{2.17}$$

e

$$Ps_l(w) = \frac{1}{Ms_l} \sum_{j=0}^{(1-2^{-w})Ms_l - 1} \left\{ (-1)^{\left\lfloor \frac{j2^{w-1}}{Ms_l} \right\rfloor} \left[2^{w-1} - \left\lfloor \frac{j2^{w-1}}{Ms_l} + \frac{1}{2} \right\rfloor \right] \right.$$
$$\left. \cdot \operatorname{erfc}\left((2j+1) \sqrt{\frac{3\log_2(M_l)\gamma}{Mc_l^2 + Ms_l^2 - 2}} \right) \right\}. \tag{2.18}$$

Nas equações anteriores, Mc_l e Ms_l denotam o número de componentes em fase e em quadratura distintas do modo de transmissão l, $\lfloor x \rfloor$ representa o maior inteiro menor que x, e $\operatorname{erfc}(\cdot)$ é a função erro complementar, expressa por:

$$\operatorname{erfc}(z) = \frac{2}{\sqrt{\pi}} \int_z^{\infty} e^{-t^2} dt. \tag{2.19}$$

Por sua vez, a EE média do sistema de comunicação que utiliza as técnicas de modulação adaptativa é dada pela média probabilística da EE de cada modo de transmissão, ou seja:

$$EE(\bar{\gamma}) = \sum_{l=0}^{N-1} \log_2(M_l) \cdot \pi_l. \tag{2.20}$$

As Figuras 2.6 e 2.7 mostram os resultados de BER média e EE média para um sistema de modulação adaptativa e para um sistema de transmissão que emprega a

α	λ
10^{-2}	[0 2,20 2,21 5,11 10,08 31,29 110,17 201,10 ∞]
10^{-3}	[0 4,17 4,18 8,52 22,31 59,12 218,50 519,01 ∞]
10^{-4}	[0 6,28 6,31 12,69 36,43 99,22 355,93 894,02 ∞]

TAB. 2.2: Vetor de limiares de adaptação para diversos valores de α.

modulação fixa 16-QAM em função da RSR média do canal avante. Os modos de transmissão disponíveis para o sistema de modulação adaptativo considerado são: BPSK, 4-QAM, 16-QAM, 64-QAM, 256-QAM, 1024-QAM e 4096-QAM, além da opção de não transmitir. Os limiares de adaptação foram calculados para $\alpha = 10^{-2}$, $\alpha = 10^{-3}$ e $\alpha = 10^{-4}$ e são apresentados na Tabela 2.2. Observa-se nessas figuras que mesmo para valores de RSR média pequenos o sistema de modulação adaptativa é capaz de realizar a transmissão de informação respeitando os requisitos de BER alvo estabelecidos, uma vantagem em relação às técnicas de modulação fixa 16-QAM, que para atingir taxas de erro menores que 10^{-2}, 10^{-3} e 10^{-4} deve-se empregar potências de transmissão de forma a produzir RSR maiores que $17dB$, $27dB$ e $37dB$ respectivamente. Outra alternativa dos sistemas de modulação fixa para se atingir tais taxas de erro com menores valores de potência de transmissão é a adoção de uma modulação fixa com menor EE.

Nota-se ainda que para valores mais elevados da RSR média, o sistema adaptativo atinge maiores EEs do que a do sistema que emprega modulação fixa mantendo a BER média dentro dos limites estabelecidos. Por exemplo, o sistema de modulação fixa 16-QAM, cuja EE é de $4bps/Hz$, atinge taxas de erro de bit menores que 10^{-2} somente a partir de valores de RSR média maiores que $17dB$, enquanto que os três sistemas de modulação adaptativa apresentados, para valores de RSR média maiores que $17dB$, apresentam maiores valores de EE com taxas de erro de bit menores que 10^{-2}.

2.4 TEMAS ATUAIS DE PESQUISA

Pelas suas boas características de desempenho, as técnicas de modulação adaptativa têm sido propostas em diversas aplicações. Em (CHATTERJEE, 2003) e (AL-KEBSI, 2009) o uso das técnicas de modulação adaptativa é empregado para melhorar o desempenho de sistemas OFDM utilizados em sistemas de comunicação sem fio 4G.

O OFDM é um sistema de transmissão multi-portadora que divide a largura de banda do sinal transmitido em diversas sub-bandas para a transmissão. Convencionalmente, um sistema OFDM emprega o mesmo esquema de modulação em todas

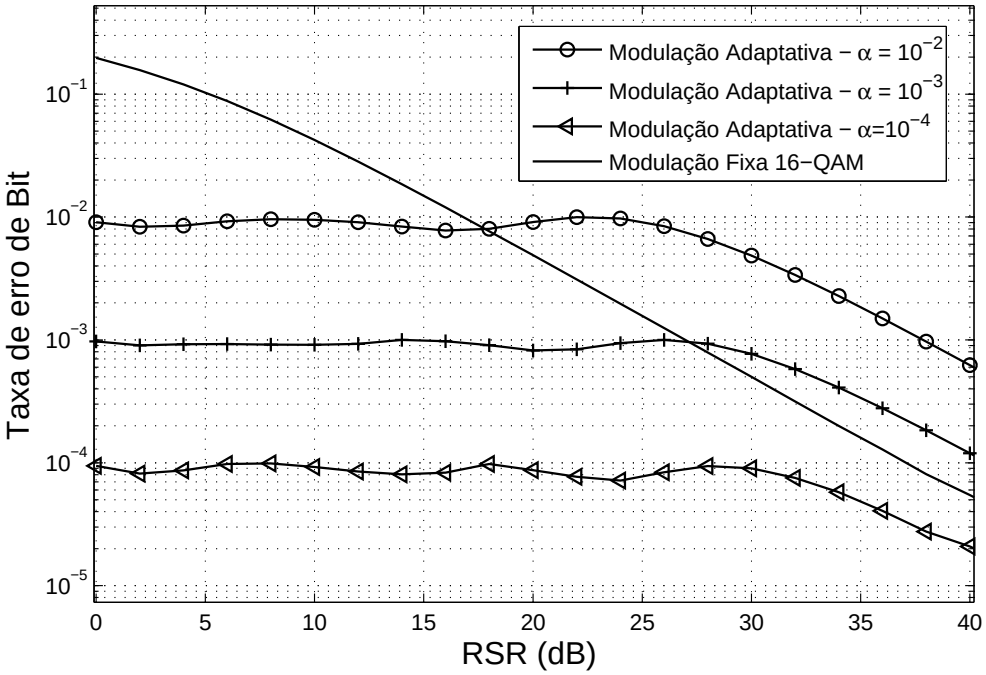

FIG. 2.6: BER de sistemas de modulação adaptativa.

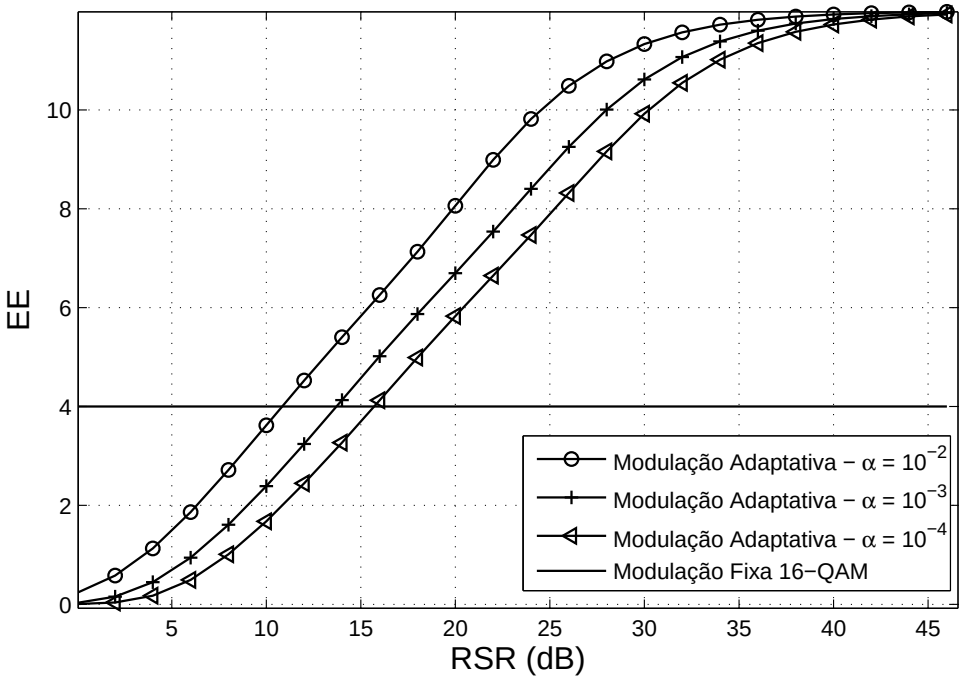

FIG. 2.7: EE de sistemas de modulção adaptativa.

as sub-bandas. Porém, em um canal seletivo em frequência, é possível utilizar modulações diferentes em cada sub-banda de acordo com a sua condição de propagação. As técnicas de modulação adaptativas também podem ser utilizadas em cada sub-banda de forma a melhor explorar o canal de comunicação em cada sub-banda ao longo do tempo. Os sistemas OFDM que empregam essas técnicas são chamados de OFDM adaptativos.

Sendo assim, os sistemas OFDM têm a capacidade de estender a abordagem das técnicas de modulação adaptativa adotada para os canais sujeitos ao desvanecimento plano aos canais com desvanecimento seletivo em frequência por meio da divisão da banda do sinal em diversas sub-bandas nas quais o desvanecimento pode ser considerado plano. Outra forma de utilizar as técnicas de modulação adaptativa em canais seletivos em frequência é proposta em (HANZO, 2000), na qual os autores empregam um equalizador com realimentação de decisão (DFE - do termo em inglês *Decision Feedback Equalizer*) para combater os efeitos da IES. Neste caso, a função do equalizador é tornar o efeito dos filtros de transmissão e detecção combinados aos efeitos do canal de comunicação e do equalizador próximo a um sistema de comunicação sujeito ao desvanecimento plano.

Em (KIM, 2003) as técnicas de modulação adaptativa são empregadas em sistemas MIMO (do termo em inglês *Multiple-Input Multiple-Output*), nos quais procura-se aumentar o desempenho dos sistemas de comunicação por meio do aumento na diversidade espacial.

Apesar da grande aplicabilidade das técnicas de modulação adaptativa, algumas questões ainda estão em aberto, principalmente no que diz respeito ao canal de retorno. Uma questão importante diz respeito ao atraso na comunicação entre o receptor e o transmissor pelo canal de retorno. Se este atraso for elevado, o esquema de modulação escolhido pode não mais ser adequado às condições atuais do canal no momento da transmissão. Em (GOECKEL, 1999), a avaliação da degradação do desempenho das técnicas de modulação adaptativa devido ao atraso no canal de retorno é realizada e, em (DUEL-HALLEN, 2000), são propostas estratégias de predição a fim de mitigar essa degradação. Os erros no canal de retorno também podem degradar significativamente o desempenho das técnicas de modulação adaptativas, criando até mesmo regiões de RSR nas quais não é possível atender aos requisitos de BER para os quais o sistema foi projetado, chamada de região de inviabilidade (EKPENYONG, 2006; MACHADO, 2009). Caso esses erros ocorram, o transmissor utilizará um esquema de

modulação inapropriado às condições de propagação atuais do canal de comunicação, o que poderá acarretar uma violação nos requisitos de desempenho do sistema de comunicação. Em (GALDINO, 2008) propõe-se a redução dessa região por meio da consideração dos erros introduzidos pelo canal de retorno na otimização dos limiares de adaptação.

2.5 RESUMO

Neste capítulo os modelos de canais geralmente adotados em sistemas de comunicação sem fio foram apresentados e as características das técnicas de modulação adaptativa foram comentadas. Além disso, detalhou-se o funcionamento de um sistema de modulação adaptativa em canal sujeito ao desvanecimento plano em frequência e lento no tempo. As principais vantagens e limitações das técnicas de modulação adaptativa foram discutidas e alguns temas atuais de pesquisa foram citados.

No próximo capítulo, a segurança das comunicações sob o ponto de vista da teoria da informação é analisada. Alguns conceitos básicos, como os de entropia, informação mútua e capacidade de canal, são apresentados e diversos trabalhos sobre o sigilo nas comunicações são discutidos. Além disso, o cenário de comunicação considerado na presente dissertação é definido.

3 TEORIA DA INFORMAÇÃO E SEGURANÇA NAS COMUNICAÇÕES

3.1 INTRODUÇÃO

Neste capítulo, é abordada a questão da segurança nas comunicações em canais sem fio, especificamente no que se refere ao sigilo nas comunicações sob o ponto de vista da teoria da informação. Inicialmente, na Seção 3.2 é feita uma breve revisão acerca de alguns conceitos básicos da teoria da informação, que instrumentam as análises feitas neste trabalho. Posteriormente, alguns trabalhos nessa área são comentados na Seção 3.3, de forma a descrever a evolução do estudo do sigilo nas comunicações em meios não confinados, e o cenário considerado durante todo o restante da presente dissertação é apresentado na Seção 3.4.

No que diz respeito à troca de informações, diversas questões relativas à segurança podem ser levantadas, como, por exemplo, a garantia da autenticidade das mensagens transmitidas e a preocupação com a adulteração das informações nelas contidas. Este trabalho, no entanto, é focado no que diz respeito à análise do sigilo das mensagens transmitidas, no sentido das informações contidas nessas mensagens serem obtidas apenas pelos seus destinatários legítimos.

A abordagem mais comumente adotada para o problema da segurança em redes de comunicações é o uso das técnicas criptográficas, principalmente as que utilizam mecanismos de chaves públicas ou privadas (STALLINGS, 2005). Normalmente essas técnicas se propõem a resolver não só o problema do sigilo mas também diversas outras questões relativas à segurança, como é o caso do protocolo criptográfico TLS (do termo em inglês *Transport Layer Security*), baseado na criptografia de chave pública, que provê segurança nas comunicações de redes de computadores como a internet (DIERKS, 2008). Esses protocolos normalmente são empregados em camadas mais elevadas da pilha de protocolos de um sistema de comunicação (TANENBAUM, 2002), e podem ser específicos para cada aplicação. Outra forma de prover segurança na transmissão de dados é adotar mecanismos de transmissão que agem na camada física dificultando a interceptação/interpretação da mensagem transmitida. A grande vantagem desses mecanismos é que eles podem ser utilizados independentemente da aplicação e em conjunto com outras técnicas, como as criptográficas, a fim de melhorar ainda mais a segurança nos sistemas de comunicação.

3.2 CONCEITOS BÁSICOS DA TEORIA DA INFORMAÇÃO

As análises acerca do sigilo nas comunicações realizadas na presente dissertação são baseadas em conceitos oriundos da teoria da informação como os de informação mútua (IM) entre duas variáveis aleatórias (v.a.) e taxa de sigilo (R_s, do temo em inglês *Secrecy Rate*) de canais de comunicação. Sendo assim, nesta seção são apresentados os conceitos de entropia, informação mútua, capacidade, capacidade de sigilo e taxa de sigilo dos sistemas de comunicação (COVER, 2006).

3.2.1 ENTROPIA - $H(X)$

A entropia (H) é uma medida da incerteza de uma variável aleatória. Para uma variável aleatória discreta X com alfabeto $\mathcal{X}$ e função massa de probabilidade (pmf, do temo em inglês *probability mass function*) $p(x) = Pr(X = x)$, $x \in \mathcal{X}$, a entropia H(X) é definida por:

$$H(X) = -\sum_{x\in\mathcal{X}} p(x)\log_2 p(x). \tag{3.1}$$

Como na equação (3.1), geralmente o logaritmo está na base 2 e a entropia é dada em bits. Como $0\log(0) = 0$, a adição de termos com probabilidade de ocorrência igual a 0 não afeta a entropia. Observando a equação (3.1), nota-se que $H(X)$ depende apenas da distribuição de X e não dos valores que a v.a. assume. Sendo assim, a entropia da v.a. X também é denotada por $H(p(X))$.

Outra forma de expressar $H(X)$ é

$$H(X) = -E\left[\log_2\left(p(x)\right)\right] = E\left[\log_2\left(\frac{1}{p(x)}\right)\right]. \tag{3.2}$$

Também pode-se definir a entropia conjunta de duas v.a.s (H(X,Y)) e a entropia condicional de uma v.a. dada outra v.a. (H(Y|X)). A primeira pode ser interpretada como uma medida de incerteza do vetor aleatório (X, Y) e a segunda é o valor esperado em X das entropias das distribuições condicionais $p(y|X = x)$, como se segue:

$$H(X,Y) = -\sum_{x\in\mathcal{X}}\sum_{x\in\mathcal{Y}} p(x,y)\log_2 p(x,y). \tag{3.3}$$

$$\begin{aligned} H(Y|X) &= \sum_{x\in\mathcal{X}} p(x)H(p(y|X=x)) && (3.4)\\ &= -\sum_{x\in\mathcal{X}} p(x)\sum_{y\in\mathcal{Y}} p(y|X=x)\log_2(p(y|X=x)) && (3.5) \end{aligned}$$

$$= -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y)\log_2(p(y|X=x)) \tag{3.6}$$

$$= -E\left[\log_2(p(y|X=x))\right]. \tag{3.7}$$

Das equações (3.1), (3.3) e (3.6) chega-se à seguinte regra em cadeia para entropia:

$$H(X,Y) = H(X) + H(Y|X). \tag{3.8}$$

3.2.2 INFORMAÇÃO MÚTUA - $I(X;Y)$

A informação mútua (IM) entre duas v.a.s, X e Y, é uma medida da quantidade de informação que uma variável possui sobre a outra. Ela pode ser definida como a redução da incerteza de X devida ao conhecimento de Y, ou seja:

$$I(X;Y) = H(X) - H(X|Y) \tag{3.9}$$

$$= \sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y)\log_2\left(\frac{p(x,y)}{p(x)p(y)}\right) \tag{3.10}$$

$$= E\left[\log_2\left(\frac{p(x,y)}{p(x)p(y)}\right)\right] \tag{3.11}$$

A IM também é simétrica, ou seja:

$$I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) = I(Y;X). \tag{3.12}$$

De (3.8) e (3.12), tem-se que:

$$I(X;Y) = H(X) + H(Y) - H(X,Y). \tag{3.13}$$

A Figura 3.1, extraída de (COVER, 2006), ilustra as relações entre entropia e IM.

3.2.3 CAPACIDADE DE UM CANAL DE COMUNICAÇÃO

A Figura 3.2 apresenta um modelo simplificado de um sistema de comunicação. Nele, uma fonte de informação gera uma mensagem a ser transmitida, $\mathcal{W}$, que é transformada em uma sequência de símbolos, descrita pelo vetor de símbolos de N posições $\mathbf{X}$, que constitui a entrada do canal de comunicação. Essa sequência de símbolos induz uma sequência aleatória de símbolos de saída, $\mathbf{Y}$, que depende de $\mathbf{X}$. Cada possível sequência de entrada induz uma distribuição de probabilidade das possíveis sequências de saída do canal. Como duas sequências de símbolos de entrada distintas podem resultar em uma mesma sequência de símbolos na saída, erros

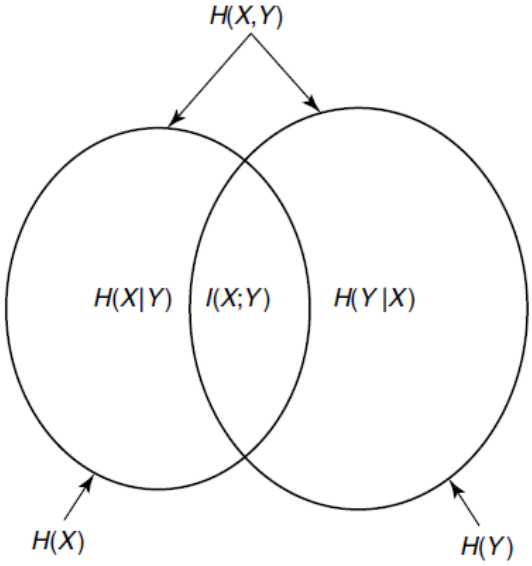

FIG. 3.1: Relações entre entropia e informação mútua. Extraído de (COVER, 2006).

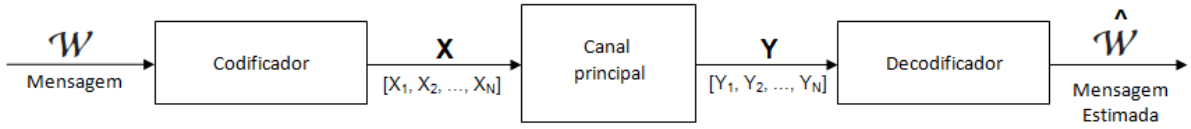

FIG. 3.2: Modelo de um sistema simplificado de comunicação.

podem ocorrer na comunicação. A probabilidade de ocorrência desses erros pode ser arbitrariamente reduzida pela utilização de apenas um subconjunto entre todas as sequências de entrada formado por sequências de símbolos diferentes o suficiente entre si de tal forma que, com alta probabilidade, uma sequência de símbolos de saída seja causada por apenas uma sequência de entrada. A taxa máxima de bits com que se pode realizar essa transmissão é denominada de capacidade do canal de comunicação. Em (SHANNON, 1948), mostrou-se que mensagens podem ser transmitidas com probabilidade de erro arbitrariamente pequena a taxas menores ou iguais a capacidade do canal de comunicação.

Um canal discreto consiste em um sistema que possui um alfabeto de símbolos entrada $\mathcal{X}$, um alfabeto de símbolos de saída $\mathcal{Y}$ e uma matriz de transição de probabilidades $p(y|x)$ que expressa a probabilidade de se observar o símbolo de saída y dado que foi transmitido o símbolo de entrada x. Nesta dissertação os canais envolvidos são considerados discretos.

A capacidade de informação de um canal de comunicação (C) é definida pela máxima informação mútua entre a saída Y e a entrada X entre todas as distribuições de entrada $p(x)$ possíveis (COVER, 2006), ou seja:

$$C = \max_{p(x)}\{I(X;Y)\}. \tag{3.14}$$

3.2.4 CAPACIDADE DE SIGILO (C_S) E TAXA DE SIGILO (R_S)

Neste trabalho, como na maioria dos estudos sobre capacidade de sigilo, a fonte de informação possui alfabeto finito e é considerada estacionária e ergódica. As primeiras k saídas da fonte, $\mathbf{w} = [w_1, \cdots, w_k]$, são codificadas em um vetor de N posições, $\mathbf{x}$, que constitui a entrada dos canais legítimo e espião. O receptor legítimo faz uma estimativa da mensagem transmitida, $\hat{\mathbf{w}}$, baseada na saída do canal legítimo, $\mathbf{y}$. A taxa de erro de bloco é definida então como:

$$P_e = Pr(\mathbf{w} \neq \hat{\mathbf{w}}). \tag{3.15}$$

Sendo $\mathbf{z}$ a saída do canal espião, o espião possui a incerteza residual $H(\mathbf{w}|\mathbf{z})$ após a observação de $\mathbf{z}$. Define-se a taxa de equívoco fracionária, Δ, da seguinte forma:

$$\Delta = \frac{H(\mathbf{w}|\mathbf{z})}{H(\mathbf{w})}. \tag{3.16}$$

Por sua vez, a taxa de transmissão, R, é dada por:

$$R = \frac{H(\mathbf{w})}{N}. \tag{3.17}$$

Sendo assim, diz-se que o par (R^*, d^*) é alcançável se para todo $\epsilon > 0$ existe um par de codificador e decodificador tal que:

$$R > R^* - \epsilon,\ \Delta \geq d^* - \epsilon\ e\ P_e \leq \epsilon. \tag{3.18}$$

A capacidade de sigilo, C_s, é definida então pelo valor máximo tal que $(C_s, 1)$ é alcançável. Dessa forma, ao se operar em taxas menores que a capacidade de sigilo é possível garantir que o espião não obtenha nenhuma informação adicional sobre a mensagem transmitida com a observação $\mathbf{z}$.

Em (LEUNG-YAN-CHEONG, 1978) os autores mostraram que, para canais gaussianos, a capacidade de sigilo de um sistema de comunicação onde a saída do canal entre o transmissor e o espião, aqui denominado de canal espião, é uma versão degradada da saída do canal entre o transmissor e o receptor legítimo, aqui denominado de canal

legítimo, é dada pela diferença entre a capacidade do canal legítimo (C_L) e a capacidade do canal espião (C_E), ou seja:

$$C_s = C_L - C_E. \tag{3.19}$$

A fim de mensurar o sigilo em um sistema de comunicação que opera a taxas menores que a capacidade do canal de comunicação, define-se a taxa de sigilo (R_s) como a diferença entre a IM entre a saída do canal legítimo, Y, e a saída do transmissor, X, e a IM entre a saída do canal espião, Z, e X. Sendo assim, R_s é dada por:

$$R_s = I(X;Y) - I(X;Z). \tag{3.20}$$

3.3 TEORIA DA INFORMAÇÃO E SEGURANÇA NAS COMUNICAÇÕES

Shannon, em um de seus primeiros trabalhos sobre segurança das comunicações sob o ponto de vista da teoria da informação (SHANNON, 1949), apresentou um canal livre de ruído no qual um espião recebe uma versão idêntica de uma mensagem criptografada destinada a um receptor legítimo. Nesta ocasião, o conceito de sigilo absoluto foi introduzido da seguinte forma: uma transmissão é realizada em sigilo absoluto quando ela é feita sem que um suposto espião, com recursos computacionais ilimitados, tenha a capacidade de adquirir qualquer informação através da observação do sinal transmitido. A capacidade de sigilo de um sistema de comunicação seria então a taxa máxima de bits em que se pode transmitir em sigilo absoluto. Neste estudo, foram estabelecidas as condições necessárias e suficientes para a transmissão em sigilo absoluto.

Seja $\mathcal{W}$ uma mensagem que é criptografada empregando-se a chave de criptografia K resultando no criptograma E. O sigilo absoluto é atingido quando o conhecimento da mensagem criptografada não diminui a incerteza da mensagem original, ou seja, quando $H(\mathcal{W}|E) = H(\mathcal{W})$. Dessa forma um espião que porventura observe E, sem o conhecimento da chave K, não obterá nenhuma informação acerca da mensagem transmitida. No trabalho de Shannon, ele provou que o sigilo absoluto nas comunicações apenas poderia ser alcançado se a chave secreta fosse tão longa quanto a própria mensagem a ser transmitida, ou seja, nos casos em que

$$H(K) \geq H(\mathcal{W}). \tag{3.21}$$

Em 1975, Wyner, em (WYNER, 1975), apresentou um modelo de comunicação com interceptação onde o espião recebe uma versão degradada do sinal que chega no

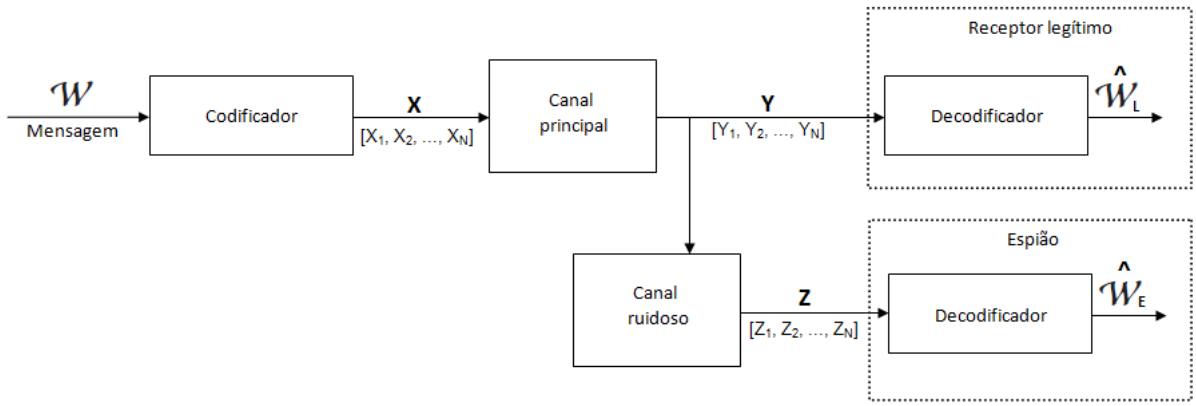

FIG. 3.3: Modelo de Wyner - *The wiretap channel*.

receptor legítimo. Neste modelo o transmissor se comunica com um receptor por meio de um canal que pode ou não introduzir erros, chamado de canal principal, e o espião possui uma cópia da mensagem transmitida por meio de um canal composto pelo canal principal seguido de um canal ruidoso. A Figura 3.3 ilustra o cenário estudado por Wyner. O transmissor codifica cada K símbolos da mensagem, $\mathcal{W}$, no vetor de N posições $\mathbf{X}$ que serve de entrada para o canal principal. O vetor $\mathbf{Y}$ e $\mathbf{Z}$ representam respectivamente a saída do canal principal e a saída do canal do espião. No trabalho de Wyner, ambos os canais foram considerados discretos sem memória, ou seja, a pmf da saída de cada canal depende apenas da sua entrada naquele instante e é independente das entradas e das saídas passadas do canal. O sigilo nesse caso foi definido utilizando a incerteza $H(\mathcal{W}|\mathbf{Z})$ e o sigilo absoluto é atingido quando

$$H(\mathcal{W}|\mathbf{Z}) = H(\mathcal{W}), \tag{3.22}$$

ou seja, a observação do espião $\mathbf{Z}$ não fornece qualquer informação sobre a mensagem transmitida. Wyner neste trabalho apresentou também expressões para a capacidade de sigilo, C_s, deste modelo, de forma que a transmissão em sigilo absoluto é possível ao se operar a taxas menores ou iguais a esta capacidade.

Em (CSISZAR, 1978), os autores estudaram um canal de *broadcast* em um cenário de comunicação constituído de duas mensagens, A e B, e dois receptores, 1 e 2. A mensagem A é destinada para ambos os receptores enquanto que a mensagem B destina-se apenas ao receptor 1. Deseja-se que o receptor 2 tenha o menor conhecimento sobre a mensagem B possível. Nesse trabalho foi mostrado que a capacidade de sigilo é sempre positiva a menos que o canal do espião seja menos ruidoso que o canal

principal. A capacidade de sigilo para esta extensão ao modelo de Wyner é dada por:

$$C_s = \max\left[I(\mathcal{W};\mathbf{Y}) - I(\mathcal{W};\mathbf{Z})\right], \tag{3.23}$$

sendo a maximização realizada sobre todas as possíveis distribuições de $\mathcal{W}$. A Equação (3.23) traduz a idéia de que a capacidade de sigilo consiste na diferença entre a quantidade de informação que o receptor legítimo possui sobre a mensagem transmitida e a quantidade de informação que o espião consegue adquirir.

O modelo de Wyner também foi alvo de estudos em (LEUNG-YAN-CHEONG, 1978), no qual os autores estenderam o referido modelo para canais gaussianos. Nesse caso, de forma similar ao resultado ilustrado na Eq. (3.23), os autores mostraram que a capacidade de sigilo é dada pela Eq. (3.19).

Recentemente, o efeito do desvanecimento no sigilo das comunicações foi objeto de estudo. Em (BARROS, 2006) e (GOPALA, 2008), baseados nos estudos de Wyner, foram desenvolvidas expressões para a capacidade de sigilo de canais sujeitos ao desvanecimento plano 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 maiores que zero. Nesses trabalhos foi mostrado que o desvanecimento, normalmente considerado um fator complicador para as comunicações sem fio, pode ser utilizado de forma a contribuir para o sigilo na transmissão de informação.

Formas de se aumentar a capacidade de sigilo dos sistemas de comunicação vêm sendo estudadas como as propostas em (NEGI, 2005) em que os autores procuram aumentar a capacidade de sigilo do canal de comunicação por meio da inserção de ruído, gerado de forma controlada, no sinal transmitido a fim de degradar o sinal recebido no espião.

3.4 CENÁRIO DE ESTUDO

A Figura 3.4 ilustra o cenário estudado nesta dissertação. Ele consiste em um sistema de comunicação sem fio sujeito à interceptação de informação. Nele, um transmissor comunica-se com um receptor legítimo na presença de um espião.

Considera-se que os canais legítimo e espião são estatisticamente independentes e modelados pelo efeito de desvanecimento plano e lento. A suposição de independência se verifica quando a distância entre o receptor legítimo e o espião é da ordem do comprimento de onda da portadora, o que é uma condição razoavelmente fácil de atingir na prática. A par disso, a modelagem adotada para o desvanecimento não é

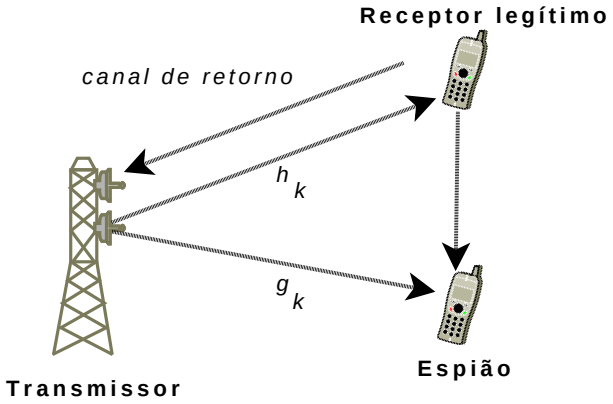

FIG. 3.4: Cenário de comunicação sob investigação.

restritiva, pois cenários que envolvem canais caracterizados pelo efeito de desvanecimento seletivo em frequência podem ser reduzidos ao caso de desvanecimento plano por meio do uso das técnicas OFDM (*Orthogonal Frequency-Division Multiplexing*), nas quais este modelo pode ser empregado para caracterizar os canais das subportadoras (sub-canais OFDM).

Admite-se ainda que o espião conhece as constelações empregadas no sistema de modulação adaptativa bem como o tamanho do bloco de dados. Além disso, considera-se que ele possui acesso irrestrito ao canal de retorno.

O sistema de comunicação emprega as técnicas de modulação adaptativas conforme descritas no Capítulo 2 cujo diagrama de blocos em banda base é apresentado na Figura 2.5. Sendo assim, o sinal recebido na entrada do receptor legítimo e do espião, y_k e z_k respectivamente, em banda base, são dados por:

$$y_k = h_k s_k + \eta_k, \tag{3.24}$$

$$z_k = g_k s_k + \tilde{\eta}_k, \tag{3.25}$$

sendo h_k e g_k modelados por processos gaussianos complexos de média nula, cujas componentes real e imaginária são estatisticamente independentes e de mesma variância. A DEP dos processos estacionários em sentido amplo, h_k e g_k, é dada pelo espectro de Jakes (PARSONS, 2000), e η_k e $\tilde{\eta}_k$ são ruídos aditivos estatisticamente independentes, ambos modelados por processos gaussianos complexos brancos de médias nulas e cujas DEP são expressas por N_0 e $\tilde{N}_0$, respectivamente.

O estado do canal legítimo, c_L, e o estado do canal espião, c_E são definidos da seguinte forma:

$$c_L = l \; se \; \{\gamma_L \in \mathbb{R} | \lambda_l \leq \gamma_L < \lambda_{l+1}\}, \tag{3.26}$$

e

$$c_E = l \; se \; \{\gamma_E \in \mathbb{R} | \lambda_l \leq \gamma_E < \lambda_{l+1}\}, \tag{3.27}$$

nas quais γ_L e γ_E representam as RSR instantâneas do canal legítimo e do canal espião dadas por:

$$\gamma_L \triangleq \bar{\gamma}_L |h_k|^2, \tag{3.28}$$

e

$$\gamma_E \triangleq \bar{\gamma}_E |g_k|^2, \tag{3.29}$$

sendo $\bar{\gamma}_E$ e $\bar{\gamma}_L$ as RSR médias dos canais legítimo e espião. O índice k de γ_L e γ_E foi removido a fim de simplificar a notação.

3.5 RESUMO

Foram apresentados neste capítulo alguns conceitos oriundos da teoria da informação fundamentais para o prosseguimento dos trabalhos realizados na presente dissertação, como os conceitos de entropia, informação mútua e capacidade de sigilo nas comunicações. Em seguida diversos trabalhos na área da segurança das comunicações sob o ponto de vista da teoria da informação foram comentados incluindo os estudos pioneiros de Shannon e Wyner e trabalhos mais recentes que investigam a capacidade de sigilo em canais sujeitos ao desvanecimento. Por fim, na Seção 3.4, o cenário de análise considerado nesta dissertação foi apresentado.

No próximo capítulo será analisado o efeito do uso das técnicas de modulação adaptativa, descritas no Capítulo 2, no sigilo das comunicações em canais sujeitos ao desvanecimento plano e lento. As expressões de taxa de erro de bit do espião, informação mútua do canal legítimo e do canal do espião e taxa de sigilo desses sistemas são apresentadas, e resultados numéricos são comentados.

4 MODULAÇÃO ADAPTATIVA E SEGURANÇA NAS COMUNICAÇÕES

4.1 INTRODUÇÃO

Neste capítulo é analisado o efeito do uso das técnicas de modulação adaptativa na segurança das comunicações em sistemas de transmissão cujos canais estão sujeitos ao desvanecimento plano em frequência e lento no tempo. Na Seção 4.2, a taxa de erro de bits de um espião é analisada a fim de se mostrar que o emprego dessas técnicas propicia uma degradação no desempenho do espião em relação ao receptor legítimo que dificulta a interpretação por parte do espião da mensagem transmitida.

Além disso, na Seção 4.3, expressões integrais para a informação mútua entre os símbolos detectados no receptor legítimo e os símbolos transmitidos e para a informação mútua entre os símbolos detectados no espião e os símbolos transmitidos são obtidas e a taxa de sigilo é calculada pela diferença entre a IM do receptor legítimo e a IM do espião. Diferentemente de outros trabalhos que obtêm expressões de IM baseadas na abordagem *water-filling* (GOLDSMITH, 2005), aqui estas expressões são obtidas a partir da definição de IM, conforme apresentada no Capítulo 3, e são expressas em termos de parâmetros importantes das estratégias de modulação adaptativa. Por meio da consideração de algumas suposições usualmente adotadas no contexto dos sistemas de comunicações sem fio, chega-se a uma expressão simplificada para a IM dos símbolos detectados pelo receptor legítimo e os símbolos transmitidos, e resultados numéricos de IM para diversos sistemas de modulação adaptativa são apresentados. Além disso, nesta seção é proposto um limite inferior para a taxa de sigilo a fim de provar que os sistemas de modulação adaptativa propiciam a transmissão de informação em sigilo absoluto.

Todas as expressões apresentadas são validadas por meio de simulações computacionais e seus resultados numéricos são comparados e discutidos.

4.2 AVALIAÇÃO DA TAXA DE ERRO DE BIT DO ESPIÃO

4.2.1 TAXA DE ERRO DE BIT DO ESPIÃO

Seguindo a mesma metodologia adotada para o cálculo da BER do receptor legítimo apresentada no Capítulo 2, a BER média do espião em um sistema de transmissão

que emprega a técnica de modulação adaptativa, denotada por P_E, pode ser calculada pela média da razão entre o número médio de bits errados e o número médio de bits transmitidos em cada modo de transmissão, e dependerá tanto da RSR média do canal legítimo, $\bar{\gamma}_L$, quanto da RSR média do canal espião, $\bar{\gamma}_E$. Ou seja:

$$P_E(\bar{\gamma}_L, \bar{\gamma}_E) = \frac{1}{EE} \sum_{l=0}^{N-1} \pi_l \log_2(M_l) \overline{BER}_E^l, \tag{4.1}$$

sendo $\overline{BER}_E^l$ a BER média do espião dado que foi utilizado o modo de transmissão l.

Por sua vez, o cálculo de $\overline{BER}_E^l$ é feito por meio do valor esperado da probabilidade de erro de bit do espião ao se utilizar a modulação l em um canal cuja RSR instantânea, γ_E, segue uma distribuição exponencial de média $\bar{\gamma}_E$. Devido à independência estatística dos canais legítimo e espião, diferentemente do caso do receptor legítimo, o uso da modulação l não restringe os valores que γ_E pode assumir. Sendo assim, $\overline{BER}_E^l$ é dada por:

$$\overline{BER}_E^l = \int_0^\infty P_b(\gamma, M_l) \frac{1}{\bar{\gamma}_E} e^{-\frac{\gamma}{\bar{\gamma}_E}} d\gamma, \tag{4.2}$$

na qual $P_b(\gamma, M_l)$ é o valor da BER do modo de transmissão l em um canal AWGN com RSR igual a γ, expressa pelas equações (2.16), (2.17) e (2.18).

Aplicando (4.2) em (4.1), chega-se a expressão para a BER do espião, dada por:

$$P_E(\bar{\gamma}_L, \bar{\gamma}_E) = \frac{1}{EE} \sum_{l=0}^{N-1} \pi_l \log_2(M_l) \int_0^\infty P_b(\gamma, M_l) \frac{1}{\bar{\gamma}_E} e^{-\frac{\gamma}{\bar{\gamma}_E}} d\gamma. \tag{4.3}$$

4.2.2 RESULTADOS NUMÉRICOS E SIMULAÇÕES

Com o intuito de validar as expressões obtidas para a BER do receptor legítimo e do espião das técnicas de modulação adaptativa e avaliar a degradação na BER do espião em relação a BER do receptor legítimo, foram realizadas simulações de transmissões com um receptor legítimo na presença de um espião. O sistema considerado pode utilizar para a transmissão as modulações BPSK, 4-QAM, 16-QAM, 64-QAM, 256-QAM, 1024-QAM e 4096-QAM, além da opção de não transmitir. 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, $f_D T$, é igual a 10^{-4}. Foram utilizados 3 conjuntos de limiares de adaptação, que foram obtidos de forma a atender a um requisito de BER alvo de $\alpha = 10^{-2}$, $\alpha = 10^{-3}$ e $\alpha = 10^{-4}$. Os valores dos limiares utilizados encontram-se na Tabela 4.5. Utilizou-se blocos de 10 símbolos, admitiu-se que o canal é conhecido pelo receptor legítimo e que o canal de

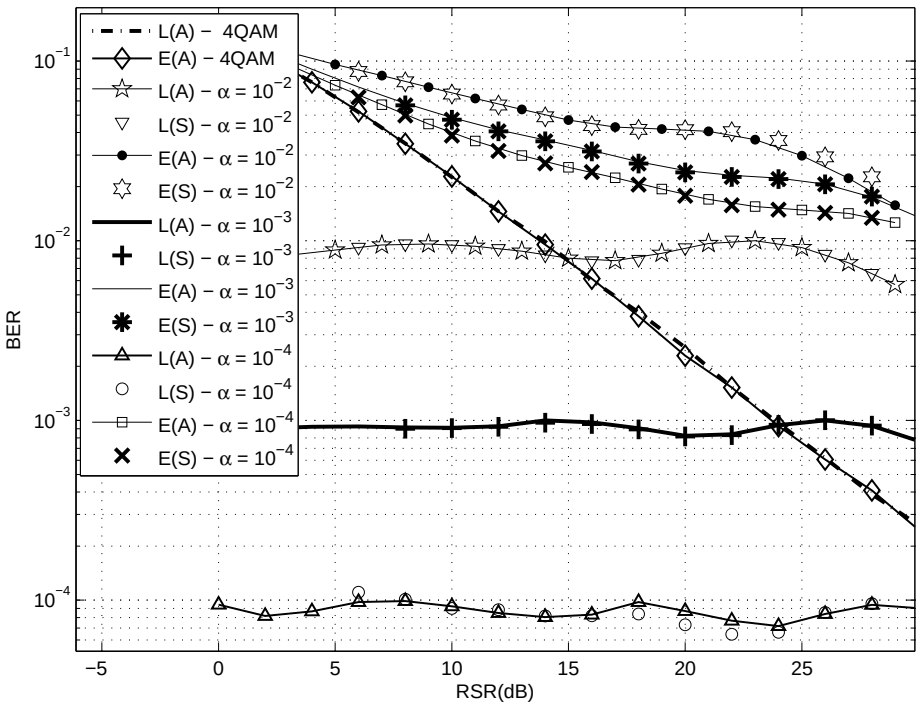

FIG. 4.1: BER dos canais legítimo e espião para a técnica de modulação adaptativa e para a modulação fixa 4-QAM.

retorno é ideal, ou seja, sem erros e atrasos. Em todos os casos, a RSR média dos canais legítimo e espião foram mantidas iguais e realizou-se nas simulações a transmissão de 10^6 símbolos.

A Figura 4.1 apresenta as curvas de probabilidade de erro de bit obtidas das expressões analíticas (A) e suas estimativas oriundas dos sistemas simulados (S) para o receptor legítimo (L) e para o espião (E) , e, para fins de comparação, as curvas de BER do espião e do receptor legítimo para um sistema que emprega a modulação fixa 4-QAM. Em todos os casos, pode ser observado que os resultados de simulação se aproximam bem das curvas analíticas. Vale ressaltar que as curvas de BER para o sistema de modulação fixa para o receptor legítimo e para o espião são bem próximas, pois, como as RSR médias do canal legítimo e do canal espião foram consideradas iguais, os momentos em que o canal espião possui melhores condições de propagação que o canal legítimo são compensados pelas situações em que o canal legítimo possui melhores condições de propagação que o espião.

Nota-se nesta figura que a medida que se reduz α as taxas de erro de bit do espião também adquirem valores menores. Isto ocorre pois o sistema de modulação adaptativa torna-se "menos agressivo" para atender aos requisitos de qualidade de

serviço mais exigentes, empregando modulações com menor EE. Sendo assim, o espião também se beneficia com a diminuição de α. Porém a melhora na BER ocasionada pela diminuição de α percebida pelo espião é bem menor do que a percebida pelo receptor legítimo, o que faz com que a diminuição de α aumente a diferença entre as curvas de BER do receptor legítimo e as do espião. Sendo assim, pode-se concluir a partir dessas curvas que o uso da técnica de modulação adaptativa provoca uma degradação significativa da BER do espião em relação à BER do receptor legítimo, e que esta diferença aumenta com a diminuição de α, o que constitui forte indício de que é possível aumentar a taxa de sigilo do sistema de comunicação por meio do emprego das técnicas de modulação adaptativa.

4.3 INFORMAÇÃO MÚTUA E TAXA DE SIGILO DAS TÉCNICAS DE MODULAÇÃO ADAPTATIVA

4.3.1 INFORMAÇÃO MÚTUA E TAXA DE SIGILO

Nesta seção são analisadas as IMs do canal legítimo e do canal espião, bem como a taxa de sigilo do sistema. Sendo a IM entre duas variáveis aleatórias uma medida da quantidade de informação que uma variável possui acerca da outra, R_s é calculada como:

$$R_s(\bar{\gamma}_L, \bar{\gamma}_E) = I_L(S; \hat{S}_L|\bar{\gamma}_L) - I_E(S; \hat{S}_E|\bar{\gamma}_L, \bar{\gamma}_E). \tag{4.4}$$

onde $I_L(S; \hat{S}_L|\bar{\gamma}_L)$ representa a IM entre os símbolos transmitidos, S, e os símbolos detectados no receptor legítimo, $\hat{S}_L$, dado $\bar{\gamma}_L$, e $I_E(S; \hat{S}_E|\bar{\gamma}_L, \bar{\gamma}_E)$ representa a IM entre S e os símbolos detectados no receptor do espião, $\hat{S}_E$, dado $\bar{\gamma}_L$ e $\bar{\gamma}_E$.

$I_L(S; \hat{S}_L|\bar{\gamma}_L)$ e $I_E(S; \hat{S}_E|\bar{\gamma}_L, \bar{\gamma}_E)$ podem ser calculadas a partir da média probabilística da IM em cada estado do canal legítimo, pois S, $\hat{S}_L$ e $\hat{S}_E$ dependem do modo de transmissão empregado pelo transmissor, que por sua vez depende desse estado. Ou seja,

$$I_L(S; \hat{S}_L|\bar{\gamma}_L) = \sum_{l=0}^{N-1} \pi_l I_{Ll}(S; \hat{S}_L|\bar{\gamma}_L), \tag{4.5}$$

e

$$I_E(S; \hat{S}_E|\bar{\gamma}_L, \bar{\gamma}_E) = \sum_{l=0}^{N-1} \pi_l I_{El}(S; \hat{S}_E|\bar{\gamma}_E). \tag{4.6}$$

sendo $I_{Ll}(S; \hat{S}_L|\bar{\gamma}_L)$ e $I_{El}(S; \hat{S}_E|\bar{\gamma}_E)$ as IMs entre S e $\hat{S}_L$ e entre S e $\hat{S}_E$ dado o estado do canal legítimo $c_L = l$, $\bar{\gamma}_L$ e $\bar{\gamma}_E$.

Para o caso do receptor legítimo, a IM entre S e $\hat{S}_L$ condicionada a $c_L = l$ é dada por:

$$I_{Ll}(S;\hat{S}_L|\bar{\gamma}_L) = \int_{\lambda_l}^{\lambda_{l+1}} \frac{I_l(S;\hat{S}_L|\gamma) f_{\bar{\gamma}_L}(\gamma) d\gamma}{\pi_l}, \tag{4.7}$$

e, por sua vez, a IM do espião condicionada ao estado do canal legítimo é dada por:

$$I_{El}(S;\hat{S}_E|\bar{\gamma}_E) = \int_0^{\infty} I_l(S;\hat{S}_E|\gamma) f_{\bar{\gamma}_E}(\gamma) d\gamma, \tag{4.8}$$

na qual $I_l(S;\hat{S}|\gamma)$ é a IM entre os símbolos de entrada e os símbolos de saída em um sistema de transmissão que utiliza a modulação l em um canal AWGN com RSR γ. Segundo a Equação (3.12), esta IM pode ser calculada por:

$$I_l(S;\hat{S}|\gamma) = \sum_{s=s_1}^{s_{M_l}} \sum_{\hat{s}=s_1}^{s_{M_l}} p(s;\hat{s}|\gamma) \log_2 \left[\frac{p(\hat{s}|s;\gamma)}{p(\hat{s}|\gamma)} \right], \tag{4.9}$$

com

$$p(s_j;s_w|\gamma) = \frac{p(s_w|s_j;\gamma)}{M_l},\ 1 \leq w, j \leq M_l \tag{4.10}$$

e

$$p(s_j|\gamma) = \frac{1}{M_l},\ 1 \leq j \leq M_l. \tag{4.11}$$

Para o cálculo de $p(s_w|s_j;\gamma)$, seja

$$s_j \in \{(x_c, x_s)|1 \leq x_c \leq Mc_l \ e\ 1 \leq x_s \leq Ms_l\}$$

e

$$s_w \in \{(y_c, y_s)|1 \leq y_c \leq Mc_l \ e\ 1 \leq y_s \leq Ms_l\}.$$

Sendo assim:

$$p(s_w|s_j;\gamma) = c_1(x_c, y_c) \cdot c_2(x_s, y_s), \tag{4.12}$$

em que

$$c_1(x_c, y_c) = \begin{cases} 1 - 2Q(\beta(\gamma)),\ para\ x_c = y_c \\ Q(a_c\beta(\gamma)) - Q(b_c\beta(\gamma)),\ cc. \end{cases} \tag{4.13}$$

$$c_2(x_s, y_s) = \begin{cases} 1 - 2Q(\beta(\gamma)),\ para\ x_s = y_s \\ Q(a_s\beta(\gamma)) - Q(b_s\beta(\gamma)),\ cc. \end{cases} \tag{4.14}$$

com

$$a_c = 2|y_c - x_c| - 1, \tag{4.15}$$

$$b_c = 2|y_c - x_c| + 1, \tag{4.16}$$

$$a_s = 2|y_s - x_s| - 1, \tag{4.17}$$

$$b_s = 2|y_s - x_s| + 1, \tag{4.18}$$

na qual

$$\beta_l(\gamma) = \sqrt{\frac{6log_2(M_l)\gamma}{Mc_l^2 + Ms_l^2 - 2}}. \tag{4.19}$$

$Q(\cdot)$ nas equações (4.13) e (4.14) representa a função Q (GOLDSMITH, 2005).

4.3.2 APROXIMAÇÃO PARA A IM ENTRE O TRANSMISSOR E O RECEPTOR LEGÍTIMO

Verifica-se pela expressão de (4.9) que todas as transições de entrada e saída possíveis são consideradas no cálculo de $I_l(S;\hat{S}|\gamma)$. Esta expressão pode ser simplificada para o caso do receptor legítimo ao se considerar que os erros de símbolo apenas ocorrem entre símbolos adjacentes da constelação, ou seja

$$p_l(\hat{s}_j|s_i;\gamma) \approx \begin{cases} 0, \text{ se } \hat{s}_j \notin \mathcal{A}_i^l \\ q_l(\gamma), \text{ se } \hat{s}_j \in \mathcal{A}_i^l \\ 1 - \sum_{w \neq i} p_l(\hat{s}_w|s_i;\gamma), \text{ se } i = j \end{cases}, \tag{4.20}$$

sendo $\mathcal{A}_i^l$ o conjunto formado pelos símbolos adjacentes ao símbolo i da constelação da modulação l e $q_l(\gamma)$ é dada por (PROAKIS, 2001):

$$q_l(\gamma) = \left[Q\left(\beta_l(\gamma)\right) - Q\left(3\beta_l(\gamma)\right)\right]\left[1 - 2Q\left(\beta_l(\gamma)\right)\right]. \tag{4.21}$$

Sabe-se que a probabilidade de se detectar o símbolo adjacente $\hat{s}_j$ dado que foi transmitido o símbolo s_i depende da posição desses símbolos na constelação. Como exemplo, a Figura 4.2 ilustra a constelação da modulação 64-QAM. Observando essa figura nota-se que a probabilidade de se detectar o símbolo 2 dado que foi transmitido o símbolo 1 é diferente da probabilidade de se detectar o símbolo 3 dado que foi transmitido o símbolo 1. Especificamente,

$$p_{64}(\hat{s}_2|s_1;\gamma) = \left[Q\left(\beta(\gamma)\right)\right]\left[1 - 2Q\left(\beta_{64}(\gamma)\right)\right] \tag{4.22}$$

e

$$p_{64}(\hat{s}_3|s_1;\gamma) = q_{64}(\gamma). \tag{4.23}$$

Apesar disso, com o objetivo de se encontrar uma expressão simplificada para $I_l(S;\hat{S}|\gamma)$, considera-se que a probabilidade de se detectar o símbolo adjacente $\hat{s}_j$ dado que foi transmitido o símbolo s_i depende apenas da distância entre os símbolos e é dada por $q_l(\gamma)$ como descrito em (8.2).

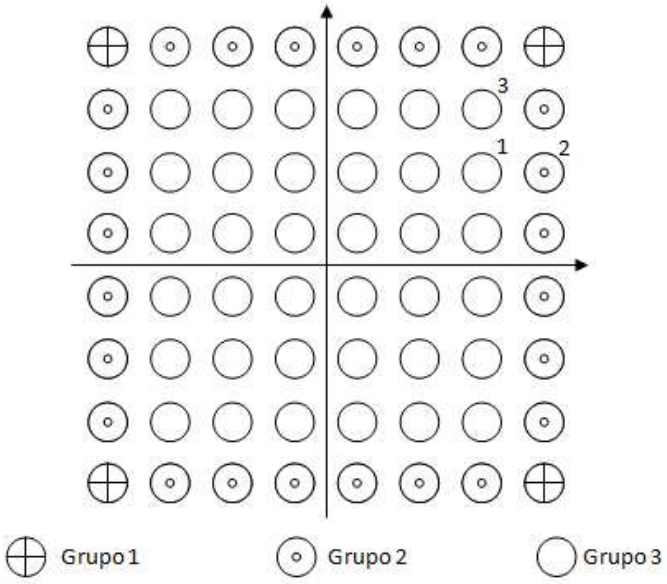

FIG. 4.2: Constelação da modulação 64−QAM.

Devido à geometria das constelações das modulações QAM, os seus símbolos podem ser agrupados de acordo com o número de vizinhos em três grupos distintos, como se segue. O primeiro conjunto é formado pelos 4 símbolos posicionados nos vértices da constelação, que possuem apenas 2 vizinhos separados pela distância mínima da constelação, d_{min_l}. O segundo conjunto é composto por $2(Mc_l + Ms_l) - 8$ símbolos localizados nos lados da constelação e que possuem 3 vizinhos separados por d_{min_l}. Por fim, o terceiro conjunto é constituído pelos $M_l - 2(Mc_l + Ms_l) + 4$ símbolos internos da constelação, os quais possuem 4 vizinhos separados por d_{min_l}. A Figura 4.2 ilustra esse agrupamento para o caso da modulação 64-QAM.

Sendo assim, com base na geometria das constelações M-QAM e considerando as aproximações mencionadas, como feito no Apêndice 8.1, pode-se mostrar que (4.9) reduz-se a:

$$I_l(S;\hat{S}|\gamma) = \log_2(M_l) - \frac{\Phi_l}{M_l}, \tag{4.24}$$

em que

$$\Phi_l = \sum_{j=1}^{4} a_{lj} \log_2 \Big[u(j-2) + (-j)^{u(j-2)} q_l(\gamma) \Big], \tag{4.25}$$

com

$$a_{l1} = (-4M_l + 2(Mc_l + Ms_l))q_l(\gamma), \tag{4.26}$$

$$a_{l2} = 8q_l(\gamma) - 4, \tag{4.27}$$

$$a_{l3} = (6(Mc_l + Ms_l) - 24)q_l(\gamma) - 2(Mc_l + Ms_l) + 8, \tag{4.28}$$

$$a_{l4} = (4M_l - 8(Mc_l + Ms_l))q_l(\gamma) + 2(Mc_l + Ms_l) - 4 - M_l. \tag{4.29}$$

Em (4.25) $u(x)$ representa a função degrau unitário, ou seja, $u(x) = 0$ para $x < 0$ e $u(x) = 1$ para $x \geq 0$.

A Figura 4.3 apresenta curvas da taxa de erro de símbolo (SER, do termo em inglês *symbol error rate*) para estratégias de modulação fixa em canais AWGN. As curvas aproximadas são obtidas considerando apenas os erros entre símbolos adjacentes. Nesta figura também são mostrados os limiares de adaptação para um sistema de modulação adaptativa com $\alpha = 10^{-2}$ que pode empregar na transmissão as modulações BPSK, 4-QAM, 16-QAM, 64-QAM, 256-QAM, 1024-QAM e 4096-QAM, além da opção de não transmitir.

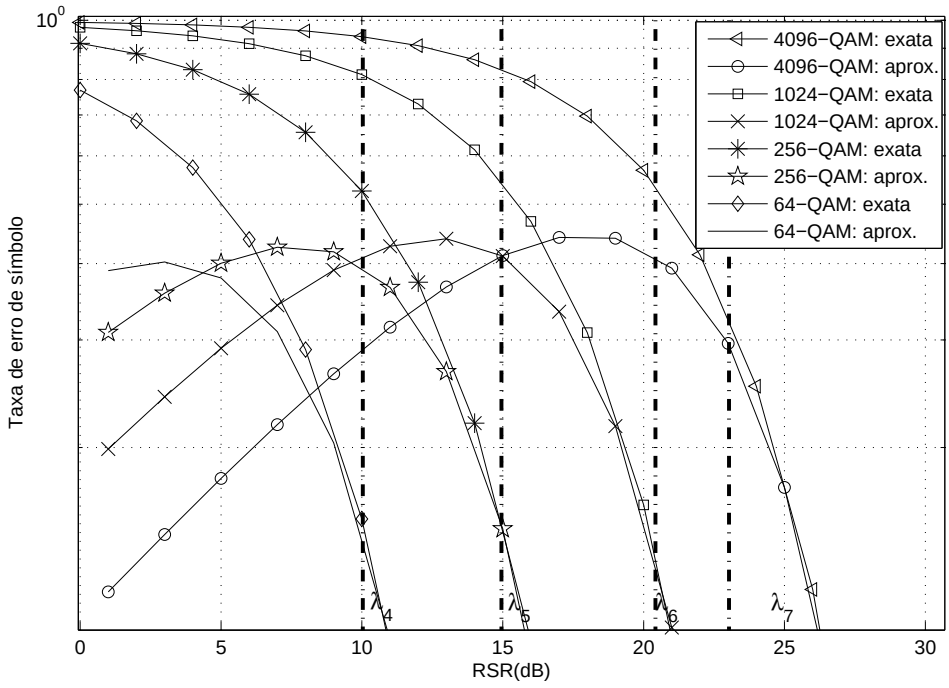

FIG. 4.3: Taxa de erro de símbolo exata e aproximada para modulações 64-QAM, 256-QAM, 1024-QAM e 4096-QAM em canal AWGN em função da RSR.

Conforme pode ser verificado na Figura 4.3, a aproximação é muito boa para valores de RSR maiores que os limiares de adaptação apresentados no gráfico. Sendo assim, para o canal legítimo a consideração realizada acerca dos erros de símbolos é valida, pois a l-ésima modulação apenas é utilizada para valores de RSR instantânea do canal legítimo maiores que o seu respectivo limiar. É claro que esta aproximação

Modulação	$\gamma_{min}(dB)$
4-QAM	$0,1$
8-QAM	$4,1$
16-QAM	$4,1$
32-QAM	$8,1$
64-QAM	$8,1$
128-QAM	$13,1$
256-QAM	$13,1$
512-QAM	$18,1$
1024-QAM	$18,1$
2048-QAM	$24,1$
4096-QAM	$24,1$

TAB. 4.1: Valores mínimos de RSR em que se pode considerar que apenas ocorrem erros entre símbolos adjacentes.

só será válida para o receptor legítimo se os limiares de adaptação forem maiores que um conjunto de limiares críticos, para os quais a aproximação pode ser considerada, visto que para valores baixos de RSR as curvas aproximadas se distanciam das curvas exatas. No exemplo da Figura 4.3 foram destacados os limiares que atendem $\alpha = 10^{-2}$ pois geralmente os sistemas de comunicação não operam a taxas de erro maiores que esse valores de BER alvo. Para valores de α menores, os limiares tendem a possuir valores mais elevados, sendo assim, se a aproximação é valida para o sistema que emprega os limiares que atendem $\alpha = 10^{-2}$, então também será para o sistema que emprega limiares que atendem valores menores de α.

Os valores mínimos (críticos) de RSR, γ_{min}, adotados nesta dissertação para considerar a aproximação válida para o receptor legítimo para cada modulação M-QAM foram encontrados de forma que, para valores de RSR maiores que γ_{min}, a seguinte inequação fosse válida:

$$\frac{SER_{exata} - SER_{aproximada}}{SER_{exata}} < 0,1. \tag{4.30}$$

Os valores de γ_{min} encontrados são apresentados na Tabela 4.1.

Observando a Figura 4.3 pode-se afirmar que a aproximação acerca dos erros de símbolos realizada para o cálculo de $I_l(S;\hat{S}|\gamma)$ não se aplica para o caso do espião. Como o modo de transmissão é escolhido de acordo com o estado do canal legítimo, e como os canais legítimo e espião são independentes, uma constelação com muitos pontos pode ser utilizada mesmo quando o canal espião apresentar valores pequenos de RSR instantânea, o que torna elevada a probabilidade de ocorrência de erros entre símbolos não adjacentes. Apesar disso, a redução da complexidade computacional

	Número de integrais	Número de multiplicações
Cálculo exato	$\sum_{l=1}^{N} M_l^2$	$1 + \sum_{l=1}^{N} 3M_l^2 + 1$
Cálculo aproximado	$5N$	$26N$

TAB. 4.2: Complexidade do cálculo da IM.

propiciada pela adoção desta aproximação (Equação (4.24)) permite que a expressão de $I_l(S;\hat{S}|\bar{\gamma}_L)$ seja usada como função objetivo no problema de busca dos limiares de adaptação das técnicas de modulação adaptativa de forma a maximizar a IM entre os símbolos transmitidos e os símbolos detectados no receptor legítimo, principalmente nos casos em que são utilizadas modulações com elevado número de pontos em suas constelações. Sendo assim, os limiares de adaptação são encontrados resolvendo-se o problema de otimização:

$$\boldsymbol{\lambda} = \max_{\boldsymbol{\lambda}^* \in \mathbb{R}^{N+1}} I_L(S;\hat{S}_L|\bar{\gamma}_L) \tag{4.31}$$

sujeito a:

$$\lambda_0 = 0, \tag{4.32}$$

$$\lambda_N = \infty, \tag{4.33}$$

$$\lambda_i \geq \gamma_{min}^i \tag{4.34}$$

e

$$\lambda_i < \lambda_{i+1}. \tag{4.35}$$

no qual γ_{min}^i representa o valor de RSR mínimo para o qual a suposição de se errar apenas para símbolos vizinhos da constelação da modulação i é razoável. O número de integrais e o número de multiplicações necessárias ao cálculo de $I_l(S;\hat{S}|\bar{\gamma}_L)$ levando em consideração as expressões exatas e a expressão com a aproximação em questão são apresentadas na Tabela 4.2.

4.3.3 LIMITE INFERIOR PARA R_S DOS SISTEMAS DE MODULAÇÃO ADAPTATIVA

Será conduzida nesta seção uma análise da expressão da R_s a fim de se obter um limitante inferior de seu valor que pode ser utilizado para provar que os sistemas de modulação adaptativa propiciam taxas de sigilo maiores que zero, o que permite a transmissão de informação de forma sigilosa. Por meio da obtenção de expressões para esse limitante que possuam complexidade computacional menor do que as das expressões exatas para a taxa de sigilo (4.4), (4.5) e (4.6), é possível resolver o problema

de busca dos limiares de adaptação que maximizam esse limitante a fim de se obter limiares que propiciem limitantes inferiores para a taxa de sigilo maiores que zero, comprovando assim a tese aqui defendida de que as técnicas de modulação adaptativa apresentam taxa de sigilo maior que zero, mesmo quando o espião possui todas as informações sobre o sistema de transmissão, as trocas de modulação e as mesmas condições de recepção que o receptor legítimo.

O limitante assim obtido pode também ser empregado para otimizar os limiares de adaptação no sentido de maximizar a taxa de sigilo ao invés da EE dos sistemas de modulação adaptativa.

A partir das expressões (4.5) e (4.7) para $I_L(S;\hat{S}|\bar{\gamma}_L)$ e das expressões (4.6) e (4.8) para $I_E(S;\hat{S}|\bar{\gamma}_L,\bar{\gamma}_E)$, $I_L(S;\hat{S}|\bar{\gamma}_L)$ e $I_E(S;\hat{S}|\bar{\gamma}_L,\bar{\gamma}_E)$ podem ser reescritas como:

$$I_L(S;\hat{S}|\bar{\gamma}_L) = \sum_{l=1}^{N} \frac{1}{M_l} \sum_{s_l=s_1}^{s_{M_l}} \left\{ \sum_{\hat{s}_l \in \mathcal{A}_i^{*l}} \int_{\lambda_l}^{\lambda_{l+1}} p(\hat{s}_l|s_l,\gamma) \log_2(M_l p(\hat{s}_l|s_l,\gamma)) f_{\bar{\gamma}_L}(\gamma) d\gamma + \right.$$

$$\left. \sum_{\hat{s}_l \notin \mathcal{A}_i^{*l}} \int_{\lambda_l}^{\lambda_{l+1}} p(\hat{s}_l|s_l,\gamma) \log_2(M_l p(\hat{s}_l|s_l,\gamma)) f_{\bar{\gamma}_L}(\gamma) d\gamma \right\} \tag{4.36}$$

e

$$I_E(S;\hat{S}|\bar{\gamma}_L,\bar{\gamma}_E) = \sum_{l=1}^{N} \frac{\pi_l}{M_l} \sum_{s_l=s_1}^{s_{M_l}} \left\{ \sum_{\hat{s}_l \in \mathcal{A}_i^{*l}} \int_{0}^{\infty} p(\hat{s}_l|s_l,\gamma) \log_2(M_l p(\hat{s}_l|s_l,\gamma)) f_{\bar{\gamma}_E}(\gamma) d\gamma + \right.$$

$$\left. \sum_{\hat{s}_l \notin \mathcal{A}_i^{*l}} \int_{0}^{\infty} p(\hat{s}_l|s_l,\gamma) \log_2(M_l p(\hat{s}_l|s_l,\gamma)) f_{\bar{\gamma}_E}(\gamma) d\gamma \right\}, \tag{4.37}$$

na qual $\mathcal{A}_i^{*l} = \mathcal{A}_i^l \cap s_i$. Sendo assim, a taxa de sigilo do sistema, R_s, calculada pela diferença entre (4.36) e (4.37), pode ser separada em duas parcelas, uma referente aos pares de símbolos vizinhos entre si e outra referente aos não vizinhos, como se segue:

$$R_s = R_{s_v} + R_{s_{nv}}\ , \tag{4.38}$$

onde

$$R_{s_v} = \sum_{l=1}^{N} \frac{1}{M_l} \sum_{s_l=s_1}^{s_{M_l}} \sum_{\hat{s}_l \in \mathcal{A}_i^{*l}} \left\{ \int_{\lambda_l}^{\lambda_{l+1}} p(\hat{s}_l|s_l,\gamma) \log_2(M_l p(\hat{s}_l|s_l,\gamma)) f_{\bar{\gamma}_L}(\gamma) d\gamma - \right.$$

$$\left. \pi_l \int_{0}^{\infty} p(\hat{s}_l|s_l,\gamma) \log_2(M_l p(\hat{s}_l|s_l,\gamma)) f_{\bar{\gamma}_E}(\gamma) d\gamma \right\}, \tag{4.39}$$

e

$$R_{s_{nv}} = \sum_{l=1}^{N} \frac{1}{M_l} \sum_{s_l=s_1}^{s_{M_l}} \sum_{\hat{s}_l \notin \mathcal{A}_i^{*l}} \left\{ \int_{\lambda_l}^{\lambda_{l+1}} p(\hat{s}_l|s_l,\gamma) \log_2(M_l p(\hat{s}_l|s_l,\gamma)) f_{\bar{\gamma}_L}(\gamma) d\gamma - \right.$$

$$\pi_l \int_0^{\infty} p(\hat{s}_l|s_l,\gamma)\log_2(M_l p(\hat{s}_l|s_l,\gamma)) f_{\bar{\gamma}_E}(\gamma)d\gamma \Bigg\}. \tag{4.40}$$

Seja uma função $g_l(\gamma)$ tal que:

$$g_l(\gamma) > p(\hat{s}_l|s_l,\gamma)\log_2(M_l p(\hat{s}_l|s_l,\gamma)), \text{ para } \forall\gamma \in \mathbb{R}, \tag{4.41}$$

então:

$$\int_{\lambda_l}^{\lambda_{l+1}} p(\hat{s}_l|s_l,\gamma)\log_2(M_l p(\hat{s}_l|s_l,\gamma)) f_{\bar{\gamma}_L}(\gamma)d\gamma = \int_{\lambda_l}^{\lambda_{l+1}} g_l(\gamma) f_{\bar{\gamma}_L}(\gamma)d\gamma - K_1^l, \tag{4.42}$$

e

$$\int_0^{\infty} p(\hat{s}_l|s_l,\gamma)\log_2(M_l p(\hat{s}_l|s_l,\gamma)) f_{\bar{\gamma}_E}(\gamma)d\gamma = \int_0^{\infty} g_l(\gamma) f_{\bar{\gamma}_E}(\gamma)d\gamma - K_2. \tag{4.43}$$

nas quais K_1^l e K_2 são valores maiores que zero. Dessa forma, $R_{s_{nv}}$ é dada por:

$$R_{s_{nv}} = \bar{R}_{s_{nv}} + \sum_{l=1}^{N} \frac{1}{M_l} \sum_{s_l=s_1}^{s_{M_l}} \sum_{\hat{s}_l \notin \mathcal{A}_i^{*l}} (\pi_l K_2 - K_1^l) \tag{4.44}$$

com

$$\bar{R}_{s_{nv}} = \sum_{l=1}^{N} \frac{1}{M_l} \sum_{s_l=s_1}^{s_{M_l}} \sum_{\hat{s}_l \notin \mathcal{A}_i^{*l}} \left\{ \int_{\lambda_l}^{\lambda_{l+1}} g_l(\gamma) f_{\bar{\gamma}_L}(\gamma)d\gamma - \pi_l \int_0^{\infty} g_l(\gamma) f_{\bar{\gamma}_E}(\gamma)d\gamma \right\}. \tag{4.45}$$

Sendo assim, pelas equações (4.38) e (4.44), temos que

$$R_s = R_{s_v} + \bar{R}_{s_{nv}} + \sum_{l=1}^{N} \frac{1}{M_l} \sum_{s_l=s_1}^{s_{M_l}} \sum_{\hat{s}_l \notin \mathcal{A}_i^{*l}} (\pi_l K_2 - K_1^l) \tag{4.46}$$

Deseja-se utilizar $\bar{R}_s = R_{s_v} + \bar{R}_{s_{nv}}$ como um limitante inferior para a taxa de sigilo do sistema. Dessa forma, $\bar{R}_s$ será um limite inferior de R_s caso $(\pi_l K_2 - K_1^l) \geq 0$ para todo l, s_l e $\hat{s}_l \notin \mathcal{A}_i^{*l}$. Sendo assim, temos que

$$\frac{K_1^l}{K_2} = \frac{\int_{\lambda_l}^{\lambda_{l+1}} erro(\gamma) f_{\bar{\gamma}_L}(\gamma)d\gamma}{\int_0^{\infty} erro(\gamma) f_{\bar{\gamma}_E}(\gamma)d\gamma} \tag{4.47}$$

na qual $erro(\gamma) = g_l(\gamma) - p(\hat{s}_l|s_l,\gamma)\log_2(M_l p(\hat{s}_l|s_l,\gamma))$. Observe que $erro(\gamma) > 0$ para $\forall\gamma \in \mathbb{R}$.

Substituindo a função $erro(\gamma)$ por $inf(erro(\gamma))$, sendo $inf(f(x))$ o menor valor que uma função f apresenta em seu domínio, tanto no numerador quanto no denominador da equação (4.47), temos que:

$$\frac{K_1^l}{K_2} \leq \frac{\int_{\lambda_l}^{\lambda_{l+1}} \inf(erro(\gamma)) f_{\bar{\gamma}_L}(\gamma)d\gamma}{\int_0^{\infty} \inf(erro(\gamma)) f_{\bar{\gamma}_E}(\gamma)d\gamma} = \frac{\inf(erro(\gamma))\pi_l}{\inf(erro(\gamma))} \tag{4.48}$$

$$\pi_l K_2 - K_1^l \geq 0. \tag{4.49}$$

A primeira desigualdade se verifica pois, como $\int_0^\infty f_{\bar{\gamma}_E}(\gamma)d\gamma \geq \pi_l$, a redução causada pela substituição de $erro(\gamma)$ por inf($erro(\gamma)$) no valor de K_2 é maior que a redução causada por esta substituição no valor de K_1^l.

Dessa forma, $\bar{R}_s = R_{s_v} + \bar{R}_{s_{nv}}$ é um limitante inferior de R_s.

O cálculo de $\bar{R}_s$ é realizado pela soma $R_{s_v} + \bar{R}_{s_{nv}}$. Com base nos mesmos argumentos utilizados na Subseção 4.3.2, a equação (4.39) pode ser escrita como:

$$R_{s_v} = \sum_{l=1}^{N} \left\{ \int_{\lambda_l}^{\lambda_{l+1}} \left(\log_2(M_l) - \frac{\Phi_l}{M_l} \right) f_{\bar{\gamma}_L}(\gamma)d\gamma \; - \pi_l \int_0^\infty \left(\log_2(M_l) - \frac{\Phi_l}{M_l} \right) f_{\bar{\gamma}_E}(\gamma)d\gamma \right\}, \tag{4.50}$$

com Φ_l dado por (4.25). O cálculo de $\bar{R}_{s_{nv}}$ dependerá da escolha da função $g_l(\gamma)$ de acordo com (4.41), sendo importante que se escolha uma função que facilite o cálculo das integrais de (4.45).

A fim de se determinar uma função $g_l(\gamma)$ de tal forma que atenda a restrição estabelecida em (4.41), faz-se necessária a análise de $p(s_w|s_j;\gamma)\log_2(M_l p(s_w|s_j;\gamma))$. Partindo das Equações (4.12) a (4.19), para símbolos s_i e $\hat{s}_j$, tem-se que:

$$\begin{aligned} p(s_w|s_j;\gamma)(\gamma)\log_2(M_l p(s_w|s_j;\gamma)) &\leq \left[Q(a_c\beta_l(\gamma))\right]\left[Q(a_s\beta_l(\gamma))\right] \times \\ &\log_2\left(M_l Q(a_c\beta_l(\gamma))Q(a_s\beta_l(\gamma))\right) && (4.51) \\ &\leq \left[\frac{1}{2}\left(e^{\frac{-a_c^2\beta_l^2(\gamma)}{2}}\right)\right]\left[\frac{1}{2}\left(e^{\frac{-a_s^2\beta_l^2(\gamma)}{2}}\right)\right]\log_2\left(M_l\frac{1}{4}e^{\frac{-(a_c^2+a_s^2)\beta_l^2(\gamma)}{2}}\right) && (4.52) \\ &= g_l(\gamma) && (4.53) \end{aligned}$$

onde na segunda desigualdade utilizou-se o seguinte limitante para a função $Q(\cdot)$:

$$Q(x) \leq \frac{1}{2}e^{\frac{-x^2}{2}} \tag{4.54}$$

Usando a função $g_l(\gamma)$ definida anteriormente, temos que:

$$\int_{\lambda_l}^{\lambda_{l+1}} g_l(\gamma)f_{\bar{\gamma}}(\gamma)d\gamma = \frac{\log_2(M_l/4)\Psi_1}{4\bar{\gamma}} - \frac{(a_c^2+a_s^2)\Delta\Psi_2}{8\ln(2)\bar{\gamma}} \tag{4.55}$$

com

$$\Psi_1 = \frac{e^{-\theta(a_c,a_s)\lambda_l} - e^{-\theta(a_c,a_s)\lambda_{l+1}}}{\theta((a_c,a_s)}, \tag{4.56}$$

$$\Psi_2 = \frac{e^{-\theta(a_c,a_s)\lambda_l}}{\theta(a_c,a_s)}\left(\lambda_l + \frac{1}{\theta(a_c,a_s)}\right) - \frac{e^{-\theta(a_c,a_s)\lambda_{l+1}}}{\theta(a_c,a_s)}\left(\lambda_{l+1} + \frac{1}{\theta(a_c,a_s w)}\right), \tag{4.57}$$

$$\theta(v,w) = \frac{(v^2+w^2)\Delta\bar{\gamma}+2}{2\bar{\gamma}} \tag{4.58}$$

$$\Delta = \sqrt{\frac{6log_2(M_l)}{Mc_l^2+Ms_l^2-2}}. \tag{4.59}$$

e

$$\int_0^\infty g_l(\gamma) f_{\bar{\gamma}}(\gamma) d\gamma = \frac{\log_2(M_l/4)\Upsilon_1}{4\bar{\gamma}} - \frac{(a_c^2 + a_s^2)\Delta\Upsilon_2}{8\ln(2)\bar{\gamma}} \tag{4.60}$$

com

$$\Upsilon_1 = \frac{1}{\theta(ac, as)} \tag{4.61}$$

$$\Upsilon_2 = \frac{1}{\theta^2(ac, as)} \tag{4.62}$$

Aplicando (4.55) e (4.60) em (4.45), calcula-se $\bar{R}_{nv}$.

A Figura 4.4 apresenta curvas dos valores de $\bar{R}_s$ para um sistema de modulação adaptativa que pode empregar para a transmissão as modulações 4-QAM, 16-QAM e 64-QAM, além da opção de não transmitir, para limiares de adaptação que maximizam $\bar{R}_s$ para três casos distintos. No primeiro caso as RSRs médias do canal legítimo e do canal espião são mantidas iguais. Já no segundo caso a RSR do espião é mantida igual a $10dB$, enquanto que no terceiro caso adota-se $\bar{\gamma}_E = 20dB$.

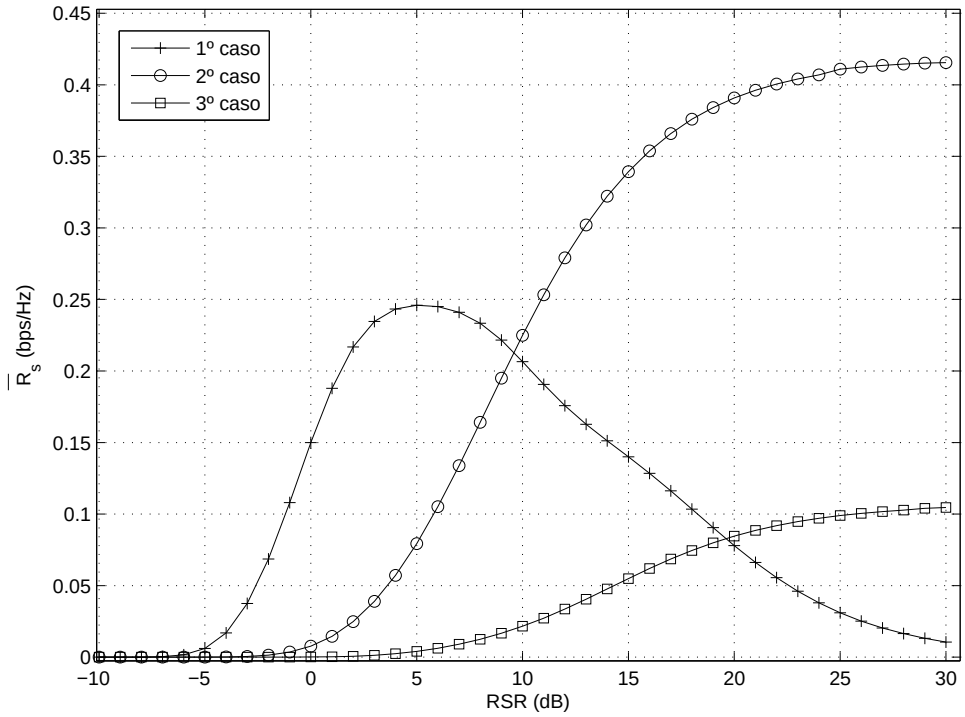

FIG. 4.4: Curvas de $\bar{R}_s$ para limiares que maximizam $\bar{R}_s$.

Observando as curvas ilustradas na Figura 4.4, verifica-se que as técnicas de modulação adaptativa propiciam de fato taxas de sigilo maiores que zero, mesmo em situações em que as condições de propagação do canal do espião são melhores que as

Caso	Vetor de limiares ($\boldsymbol{\lambda}$)
1	$[0 \;\; 1,52 \;\; 7,75 \;\; 34,1 \;\; \infty]$
2	$[0 \;\; 2,52 \;\; 7 \;\; 6600,4 \;\; \infty]$
3	$[0 \;\; 4,89 \;\; 12 \;\; 31,47 \;\; \infty]$

TAB. 4.3: Limiares de adaptação utilizados em cada caso.

do canal legítimo. Vale ressaltar que as curvas apresentadas nessa figura constituem um limite inferior para a taxa de sigilo. Dessa forma, a taxa de sigilo para os sistemas consideradas possui valores mais elevados que os de $\bar{R}_s$. Os limiares utilizados em cada caso são apresentados na Tabela 4.3.

A Figura 4.5 apresentas curvas de R_s e $\bar{R}_s$, de acordo com a função $g(x)$ aqui apresentada, para o mesmo sistema de modulação adaptativa do caso anterior no qual as RSR médias dos canais legítimo e espião foram mantidas iguais. Utilizou-se os limiares de adaptação obtidos por meio da maximização de $\bar{R}_s$ e os obtidos maximizando a EE do sistema restritos a $\alpha = 10^{-2}$. Pode-se observar que a taxa de sigilo do sistema com os limiares que atendem a $\alpha = 10^{-2}$ possui valores mais elevados que a do sistema com os limiares que maximizam $\bar{R}_s$. Sendo assim, conclui-se que o limitante aqui apresentado não é adequado à busca dos limiares que maximizam a taxa de sigilo do sistema de modulação adaptativa. Outras funções $g(x)$ podem ser investigadas de modo que se possa maximizar R_s por meio da maximização de $\bar{R}_s$.

4.3.4 RESULTADOS NUMÉRICOS

Nesta subseção são apresentados alguns resultados numéricos oriundos de simulações e obtidos a partir das expressões integrais de IM e R_s deduzidas nesta dissertação. Esses resultados foram gerados para quatro estratégias de modulação adaptativa, aqui denominadas de estratégias I, II, III e IV, as quais se diferenciam pelos modos de transmissão adotados. A estratégias I pode utilizar para a transmissão as modulações BPSK, 4−, 16−, 64−, 256−, 1024− e 4096−QAM, além da opção de não transmitir. A estratégia III pode transmitir utilizando sete modos de transmissão diferentes sendo compostos pelas modulações 4−, 8−, 16−, 32−, 64− e 128−QAM, além da opção de não transmitir. As estratégias II e IV empregam quatro modos de operação, sendo utilizados na estratégia II os modos: não transmite, 16−, 256− e 4096−QAM, e na estratégia IV os modos: não transmite, 4−, 16− e 64−QAM. Os modos de transmissão disponíveis em cada estratégia são resumidos na Tabela 4.4 e os limiares de adaptação

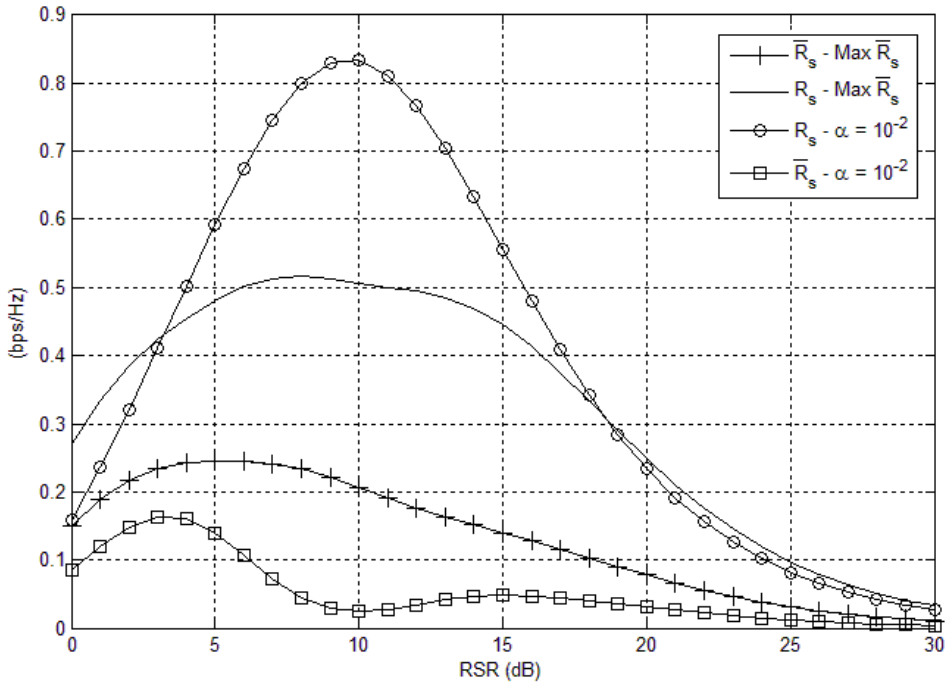

FIG. 4.5: Curvas de R_s e $\bar{R}_s$ para limiares que maximizam $\bar{R}_s$ e limiares que atendem $\alpha = 10^{-2}$.

Estratégia	Modos de transmissão disponíveis
I	não transmite, BPSK, 4-QAM, 16-QAM, 64-QAM, 256-QAM, 1024-QAM, 4096-QAM
II	não transmite, 16-QAM, 256-QAM, 4096-QAM
III	não transmite, 4-QAM, 8-QAM, 16-QAM, 32-QAM, 64-QAM, 128-QAM
IV	não transmite, 4-QAM, 16-QAM, 64-QAM

TAB. 4.4: Modos de transmissão disponíveis em cada estratégia de transmissão.

referente a cada estratégia para os diversos critérios de otimização dos limiares de adaptação analisados são dados na Tabela 4.5.

De forma a validar as expressões integrais obtidas, foram gerados resultados de simulações para sistemas que empregam as quatro estratégias de modulação adaptativa definidas previamente na presença de um espião. Os canais foram simulados de acordo com a técnica de Monte Carlo (GUIMARÃES, 1997). Os canais legítimo e espião são sorteados independentemente, sendo que cada um deles é modelado por um processo estacionário em sentido amplo cuja DEP é dada pelo espectro de Jakes. Em ambos os canais considerou-se $f_D T = 10^{-4}$. O tamanho do bloco utilizado foi de 10 símbolos, o canal de retorno foi considerado ideal e admitiu-se ainda que o receptor

Estratégia	critério de otimização	Vetor de limiares (λ)
I	$\alpha = 10^{-2}$	[0 2,20 2,21 5,11 10,08 31,29 110,17 201,10 ∞]
	$\alpha = 10^{-3}$	[0 4,17 4,18 8,52 22,31 59,12 218,50 519,01 ∞]
	$\alpha = 10^{-4}$	[0 6,28 6,31 12,69 36,43 99,22 355,93 894,02 ∞]
	Max I_L	[0 0,02 1,05 2,65 6,57 20,5 64,63 257,13 ∞]
II	*Max* I_L	[0 2,65 20,5 257,13 ∞]
III	$\alpha = 10^{-3}$	[0 4,47 7,92 9,31 24,12 27,50 55,30 ∞]
	Max I_L	[0 1,06 2,68 2,69 6,49 6,5 20,43 ∞]
IV	$\alpha = 10^{-2}$	[0 2,12 5,11 10,08 ∞]
	$\alpha = 10^{-3}$	[0 4,17 8,52 22,31 ∞]
	$\alpha = 10^{-4}$	[0 6,39 31,56 31,65 ∞]
	Max I_L	[0 1,15 2,63 6,48 ∞]

TAB. 4.5: Conjunto de limiares de adaptação.

conhece o canal avante. Para cada simulação utilizou-se 10^7 sorteios independentes dos canais envolvidos e manteve-se a RSR média do canal espião igual a RSR media do canal legítimo.

Na Figura 4.6 são apresentados resultados de IM em função da RSR média dos canais legítimo e espião, sendo a RSR média expressa em termos de E_b/N_0. Na referida figura são mostradas oito curvas para as estratégias I e IV com limiares que foram obtidos de forma a maximizar a EE do sistema restrito a $\alpha = 10^{-3}$. Para cada estratégia são apresentados os resultados empíricos (E) oriundos das simulações e os analíticos (A) oriundos das expressões integrais. Em todos os casos, pode ser observado que os resultados de simulação se aproximam bem das curvas das expressões integrais. Observa-se ainda que, no caso da estratégia IV, para valores elevados de RSR média as curvas de IM do receptor legítimo e do espião se aproximam, pois nessas condições o sistema adaptativo se assemelha a um sistema de modulação fixa 64-QAM. O mesmo ocorre para a estratégia I, porém para valores bem mais elevados da RSR média. Para valores pequenos da RSR média, a probabilidade de se utilizar modulações com EE mais elevada das disponíveis na estratégia IV diminui, fazendo com que os resultados para a estratégia I se confundam com os apresentados pela estratégia IV.

Na Figura 4.7 o limite da Capacidade do Canal para canais com desvanecimento Rayleigh (GOLDSMITH, 2005) e cinco curvas de IM para o receptor legítimo são apresentadas como função da potência do sinal recebido no receptor, P, sobre N_0 ($P = EE(\bar{\gamma})E_b$)[1]. Duas dessas curvas são relativas às estratégias I e III, com limiares de

[1]Utiliza-se P/N_0 neste caso a fim de possibilitar a comparação das curvas de IM com a de capacidade,

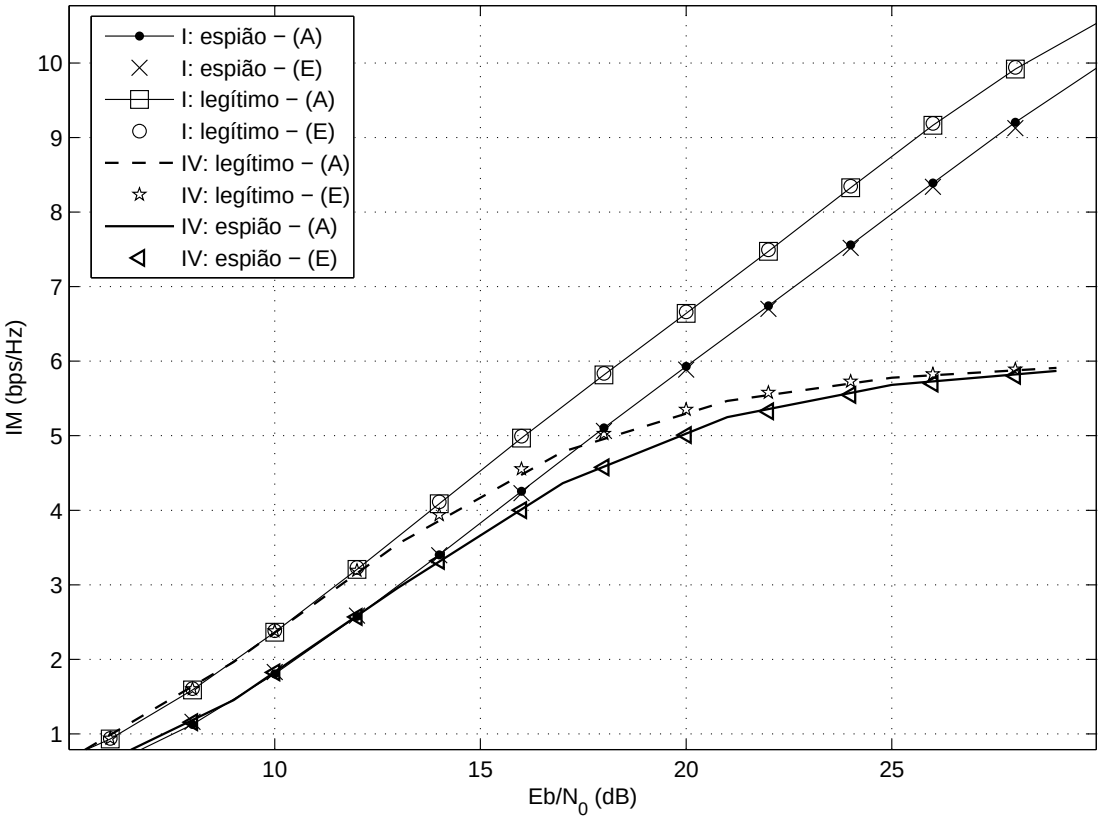

FIG. 4.6: Curvas de IM analíticas e simuladas em função da RSR média.

adaptação obtidos de forma a produzirem $\alpha = 10^{-3}$, e as outras três para as estratégias I, II e III considerando limiares que maximizam (4.5) independentemente de α, desde que se mantenha válida a aproximação relativa aos erros de símbolos utilizada na Subseção 4.3.2. As RSR do receptor legítimo foram mantidas iguais às do espião.

Para as estratégias I e III, os casos em que se maximiza a IM do receptor legítimo, apesar de apresentarem BER do receptor legítimo piores que 10^{-3}, como pode ser observado na Figura 4.8, resultam em melhores valores de IM. Outro aspecto interessante constatado na Figura 4.7 é que se obtém maiores valores de IM ao se utilizar estratégias de transmissão com modulações cujas EE não são muito distintas umas das outras, mantendo-se a mesma restrição. Este fato pode ser observado ao se comparar as curvas de IM referentes às estratégias I, II e III com limiares que maximizam (4.5). Para estratégias com modulações cujas EE são muito distintas, os limiares de adaptação são muito distantes entre si, o que torna a mudança de modo de transmissão menos frequente, prejudicando dessa forma o aproveitamento das condições momentâneas de

visto que esta é independente do modo de transmissão empregado.

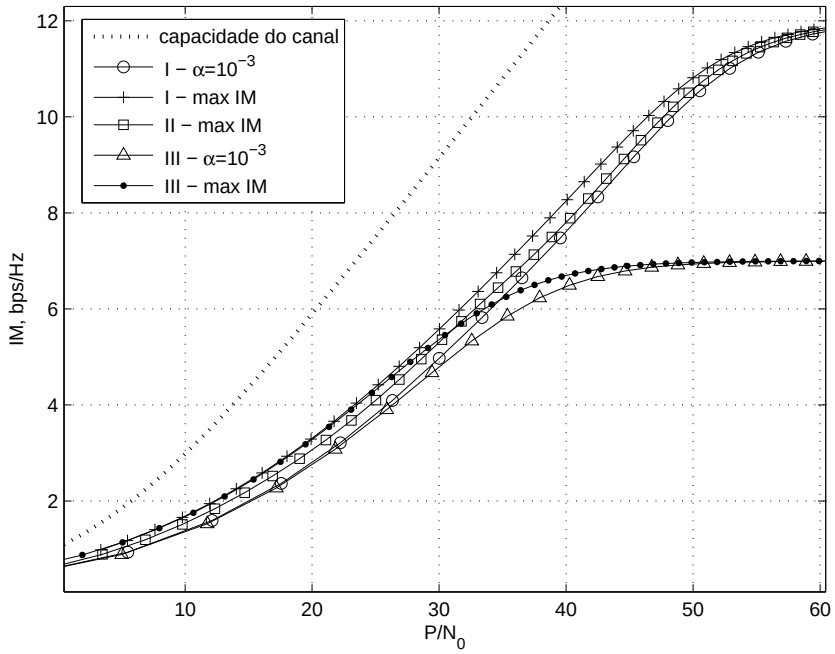

FIG. 4.7: Curvas de capacidade e IM para as estratégias I, II e III em função de P/N_0.

propagação do canal. Este fenômeno também é observado para uma figura de mérito correlata à IM: a Eficiência Espectral. Em (GOLDSMITH, 2005, p.274) é analisada a EE de um sistema de modulação adaptativa em canais com desvanecimento plano. A partir das equações integrais lá obtidas, que se baseiam na abordagem *water-filling*, vê-se que a máxima EE é alcançada ao se utilizar um sistema de transmissão hipotético capaz de adaptar de forma contínua a sua taxa de transmissão.

A Figura 4.9 apresenta as curvas de IM para as estratégias I e IV em função da RSR média do canal legítimo com limiares de adaptação obtidos de forma a produzirem $\alpha = 10^{-2}$, $\alpha = 10^{-3}$ e $\alpha = 10^{-4}$. Observando essas curvas nota-se uma clara degradação da IM com a redução de α. Este resultado, que a princípio pode parecer ilógico, pelo menos para modulações fixas, é coerente quando se trata da modulação adaptativa. Conforme α diminui, $I_{Li}(S;\hat{S}|\bar{\gamma}_L)$ tende a aumentar, porém a probabilidade de se utilizar constelações com maiores EE diminui, reduzindo assim, na média, o número de bits por uso do canal (ver Eq. (4.5)). Ou seja, reduzir α produz dois efeitos conflitantes, que combinados podem resultar na degradação da IM, conforme mostrado nesta figura.

Em seguida, curvas de R_s para as estratégias I, III e IV, para $\alpha = 10^{-3}$ e para limiares de adaptação que maximizam a IM do receptor legítimo são apresentadas na Figura 4.10 como função da RSR média, que foi mantida igual tanto para o receptor legítimo

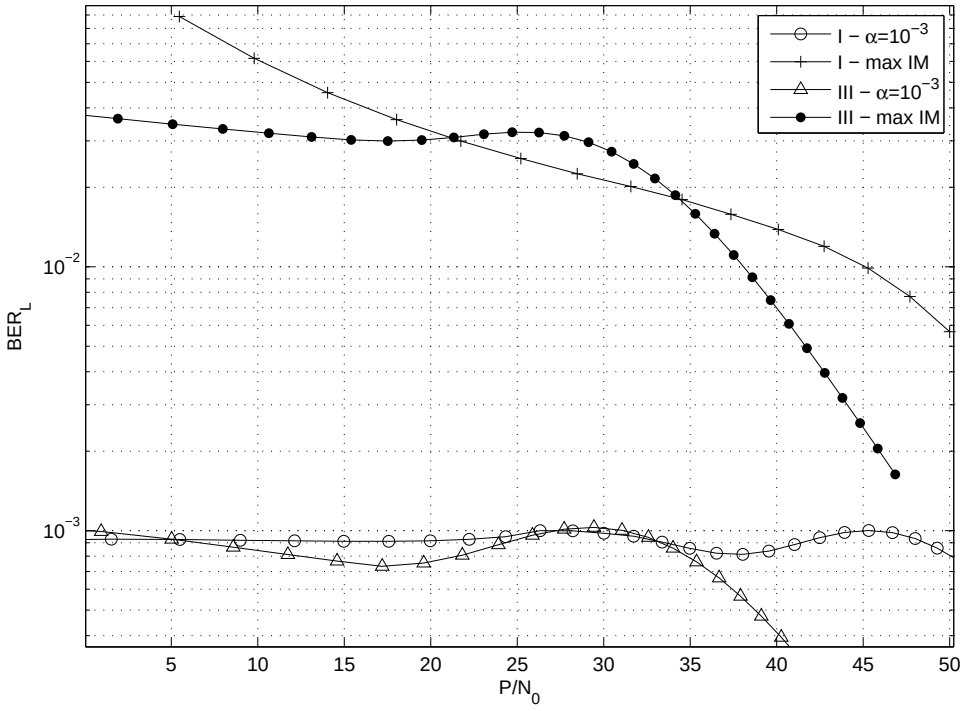

FIG. 4.8: Curvas de BER média do receptor legítimo para as estratégias I e III em função de P/N_0.

quanto para o espião. Observa-se que até um determinado valor de RSR média (em torno de 10 dB), as estratégias empregadas produzem praticamente o mesmo valor de R_s, porém para valores maiores de RSR, a R_s aumenta com o uso de estratégias que possuem constelações com maiores EE. Também pode ser notado o aumento de R_s com o uso de limiares de adaptação que maximizam a IM do receptor legítimo.

Finalmente, são apresentadas na Figura 4.11 curvas de Taxa de Sigilo que foram obtidas com valores de RSR média do canal legítimo e espião distintas. Para obter esses resultados fixou-se $\bar{\gamma}_E$ e variou-se $\bar{\gamma}_L$. Os resultados de R_s são expressos em termos da razão $\bar{\gamma}_L/\bar{\gamma}_E$, e foram obtidos considerando $\bar{\gamma}_E = 10$ dB e $\bar{\gamma}_E = 20$ dB, para a estratégia I e $\alpha = 10^{-3}$. Observa-se nessa figura que mesmo para os casos em que $\bar{\gamma}_E > \bar{\gamma}_L$ temos valores de R_s maiores que zero, o que mostra o efeito positivo do desvanecimento no sigilo das comunicações. Porém, os resultados mais expressivos ocorrem quando $\bar{\gamma}_L > \bar{\gamma}_E$. Vê-se claramente que para uma RSR média do canal legítimo cerca de 10 dB maior do que a RSR média do canal espião é obtida a expressiva taxa de sigilo de 3 bits por uso do canal por Hertz. Assim sendo, o emprego da técnica de modulação adaptativa, em conjunto com técnicas que degradam o desempenho do canal espião, como em (NEGI, 2005), pode propiciar, além de segurança irrestrita, um uso eficiente

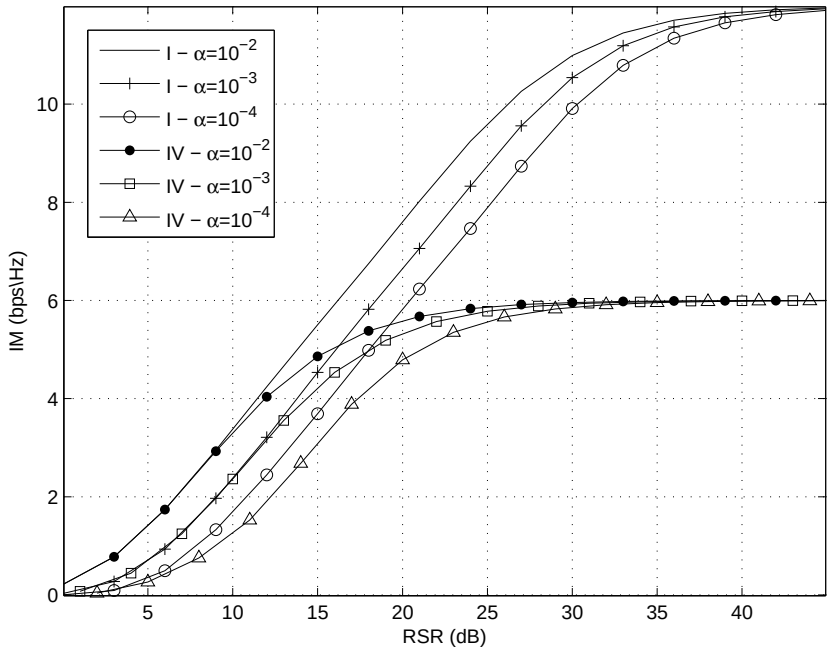

FIG. 4.9: Curvas de IM do receptor legítimo para as estratégias I e IV em função da RSR média para $\alpha = 10^{-2}$, $\alpha = 10^{-3}$ e $\alpha = 10^{-4}$.

do canal de comunicação.

Verifica-se ainda que a partir de certo valor de $\bar{\gamma}_L/\bar{\gamma}_E$ aumentar $\bar{\gamma}_L$ mantendo $\bar{\gamma}_E$ fixo não traz vantagens para a taxa de sigilo. Este fato pode ser explicado analisando as figuras 4.6 e 4.9, e observando que a IM do receptor legítimo é limitada à EE da maior constelação utilizada pela estratégia de modulação adaptativa, pois aumentar $\bar{\gamma}_L$ torna o sistema de modulação adaptativa próximo a um sistema que utiliza apenas essa modulação, além de diminuir a sua probabilidade de erro. Como a probabilidade de erro do espião está relacionada à $\bar{\gamma}_E$, para valores elevados de $\bar{\gamma}_L$, a IM do espião será maior quanto maior for $\bar{\gamma}_E$. Por esse motivo, a curva de R_s para $\bar{\gamma}_E = 10$dB apresenta valores maiores que a curva para $\bar{\gamma}_E = 20$dB ao se considerar valores elevados de $\bar{\gamma}_L$.

4.4 RESUMO

Neste capítulo apresentou-se a expressão da BER do espião ao se utilizar as técnicas de modulação adaptativa. Além disso, foram analisadas a IM entre os símbolos transmitidos e os símbolos recebidos pelo receptor legítimo e a IM entre os símbolos transmitidos e os símbolos recebidos no espião. Expressões integrais para as IMs do receptor legítimo e do espião foram obtidas e a taxa de sigilo do sistema foi calculada

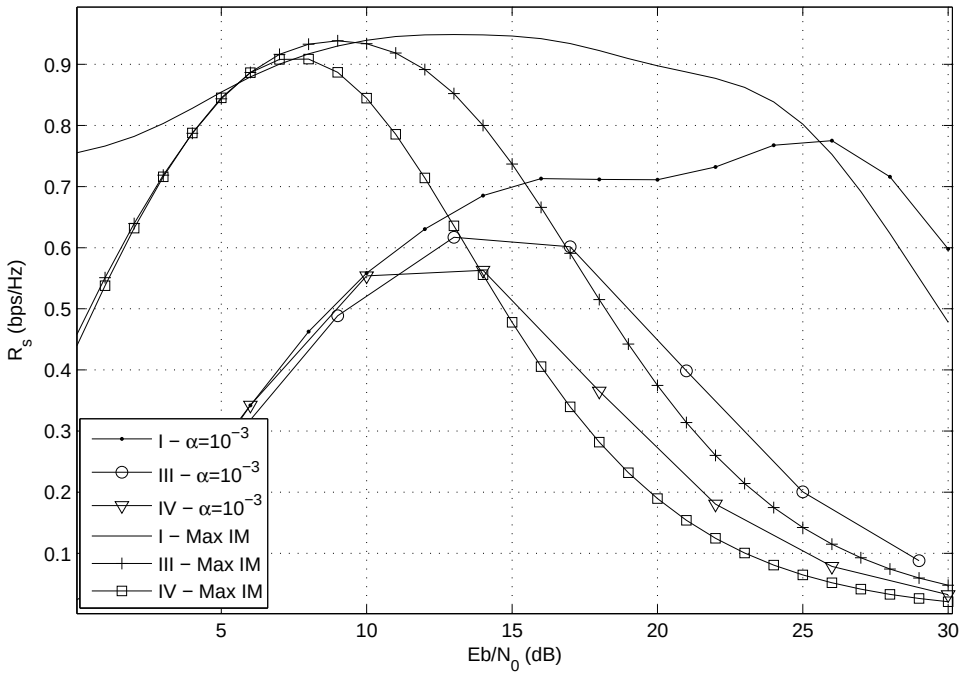

FIG. 4.10: Curvas de R_s para as estratégias I, III e IV em função da RSR média, considerando $\alpha = 10^{-3}$ e limiares que maximizam I_L.

a partir da diferença entre essas IMs.

Simulações computacionais foram realizadas que validaram as expressões apresentadas e os resultados numéricos obtidos foram analisados. Desta análise destaca-se a degradação do desempenho do espião obtida por meio do uso das técnicas de modulação adaptativa e a obtenção de valores positivos para a taxa de sigilo dos sistemas que empregam essas técnicas, especialmente quando se considera o canal espião em piores condições de propagação que o canal legítimo.

Foi apresentada uma metodologia para se obter limitantes inferiores para a taxa de sigilo dos sistemas que empregam as técnicas de modulação adaptativa e um exemplo de limitante foi utilizado para provar que essas técnicas propiciam taxas de sigilo maiores que zero. Devido à alta complexidade computacional do cálculo da taxa de sigilo, originada pela necessidade de se calcular a probabilidade de erro de símbolo entre todos os pares de símbolos das modulações utilizadas pelo sistema de comunicação, considerou-se resolver o problema de busca dos limiares de adaptação que maximizam a taxa de sigilo por meio da maximização do limite inferior apresentado, porém constatou-se que este limitante não é adequado para tal solução. Outras funções $g(x)$ podem ser consideradas a fim de se obter limites inferiores que sejam adequados para a maximização pretendida.

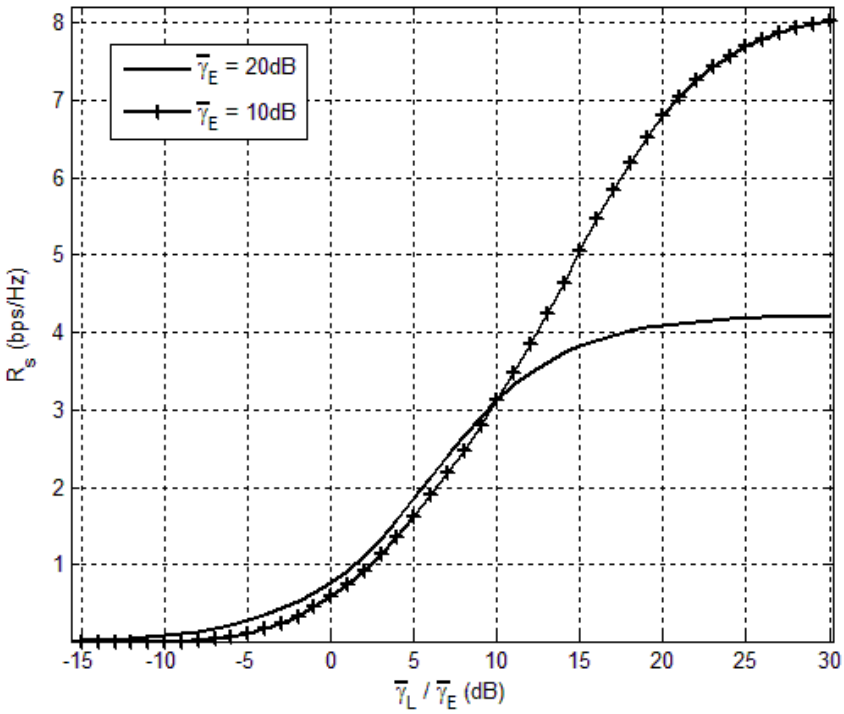

FIG. 4.11: Curvas de R_s para a estratégia I com $\alpha = 10^{-3}$ em função de $\bar{\gamma}_L/\bar{\gamma}_E$ para $\bar{\gamma}_E = 10$ dB e $\bar{\gamma}_E = 20$ dB.

No próximo capítulo serão investigadas formas de se potencializar o sigilo provido pelas técnicas de modulação adaptativa. Serão propostas quatro estratégias de transmissão, baseadas nas técnicas de modulação adaptativa, que visam degradar ainda mais o desempenho do espião.

5 PROPOSTAS DE ESTRATÉGIAS DE MODULAÇÃO ADAPTATIVA PARA AUMENTAR A TAXA DE SIGILO

5.1 INTRODUÇÃO

No Capítulo 4 é mostrado que as técnicas de modulação adaptativa, além de utilizar de forma mais eficiente o canal de comunicação variante no tempo, propiciam segurança aos sistemas de comunicação, diferentemente do que ocorre com as técnicas de modulação fixa para o receptor legítimo e o espião sob as mesmas condições de recepção. Neste capítulo são investigadas estratégias de transmissão baseadas nas técnicas de modulação adaptativa que visam potencializar o sigilo dos sistemas de transmissão.

Inicialmente, na Seção 5.2 quatro técnicas de transmissão são propostas. Duas delas baseiam-se na transmissão de informação apenas em momentos favoráveis para o receptor legítimo. A terceira consiste no emprego das expressões analíticas apresentadas no Capítulo 4 para a determinação de limiares de adaptação que maximizam a taxa de sigilo do sistema de comunicação. Finalmente a quarta técnica proposta utiliza as constelações das modulações disponíveis para a transmissão rotacionadas por um ângulo conhecido apenas pelo transmissor e pelo receptor legítimo, a fim de dificultar a interpretação do sinal recebido no espião, aumentando dessa forma a taxa de sigilo do sistema de comunicação.

Na Seção 5.3 resultados numéricos e de simulação em termos de taxa de erro de bit, informação mútua, EE e taxa de sigilo são apresentados e analisados para as quatro técnicas propostas.

5.2 TÉCNICAS PROPOSTAS

5.2.1 TÉCNICA I

Em (GOPALA, 2008), os autores realizam um estudo sobre a capacidade de sigilo de canais com desvanecimento e propõem uma estratégia de alocação de potência que atinge capacidades de sigilo maiores que zero. Esta estratégia consiste em realizar a transmissão apenas em momentos oportunos, enquanto que nos momentos desfa-

voráveis não se realiza a transmissão. Inspiradas nesse trabalho, as técnicas I e II aqui apresentadas objetivam aumentar a segurança do sistema de comunicação apenas utilizando o canal de comunicação para transmissão de informação em circunstâncias favoráveis para o canal legítimo.

Na primeira delas, admite-se que o transmissor possui informação sobre os estados dos canais legítimo e espião, c_L e c_E. A transmissão de informação é efetuada utilizando estratégias de modulação escolhidas da mesma forma que é realizado nas técnicas de modulação adaptativa nos momentos considerados oportunos. Nos demais momentos não ocorre a transmissão.

Com o conhecimento dos estados dos canais legítimo e espião, a transmissão torna-se oportuna nos momentos em que o canal legítimo encontra-se em melhores condições de propagação do que o canal espião. Sendo assim, esta técnica prevê a transmissão de informação apenas quando a diferença entre o estado do canal legítimo e o estado do canal do espião for maior que d_{LE}, sendo $d_{LE} \in \{\mathbb{N} | 0 \leq d_{LE} < N-1\}$. Denotando-se por ξ_l o evento de haver transmissão utilizando a modulação M_l-QAM, ou seja:

$$\xi_l \triangleq \{c_L > c_E + d_{LE}\} \cap \{c_L = l\}, \tag{5.1}$$

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

$$EE(\bar{\gamma}_L, \bar{\gamma}_E) = \sum_{l=0}^{N-1} \log_2(M_l) \cdot Pr(c_L > c_E + d_{LE} | c_L = l) \cdot \pi_l. \tag{5.2}$$

Para $l \leq d_{LE}$, a probabilidade $Pr(c_L > c_E + d_{LE} | c_L = l)$ é zero, visto que $c_E \geq 0$. Para $l > d_{LE}$, temos que

$$\begin{aligned} &Pr(c_L > c_E + d_{LE} | c_L = l) = \\ &\quad = \frac{Pr(c_E < c_L - d_{LE}, c_L = l)}{Pr(c_L = l)} &(5.3)\\ &\quad = \frac{\int_{\lambda_0}^{\lambda_{l-d_{LE}}} \int_{\lambda_l}^{\lambda_{l+1}} f_{\bar{\gamma}_L, \bar{\gamma}_E}(\gamma_L, \gamma_E) d\gamma_L d\gamma_E}{\int_{\lambda_l}^{\lambda_{l+1}} f_{\bar{\gamma}_L}(\gamma_L) d\gamma_L}. &(5.4) \end{aligned}$$

Devido à independência dos canais legítimo e espião,

$$\begin{aligned} &Pr(c_L > c_E + d_{LE} | c_L = l) = \\ &\quad = \frac{\int_{\lambda_0}^{\lambda_{l-d_{LE}}} f_{\bar{\gamma}_E}(\gamma_E) d\gamma_E \int_{\lambda_l}^{\lambda_{l+1}} f_{\bar{\gamma}_L}(\gamma_L) d\gamma_L}{\int_{\lambda_l}^{\lambda_{l+1}} f_{\bar{\gamma}_L}(\gamma_L) d\gamma_L} &(5.5)\\ &\quad = \sum_{j=0}^{l-(d_{LE}+1)} \int_{\lambda_j}^{\lambda_{j+1}} f_{\bar{\gamma}_E}(\gamma_E) d\gamma_E &(5.6) \end{aligned}$$

$$= \sum_{j=0}^{l-(d_{LE}+1)} \tilde{\pi}_j. \tag{5.7}$$

Ou seja, a probabilidade de $c_L - c_E > d_{LE}$ dado que $c_L = l$ é dada por:

$$Pr(c_L > c_E + d_{LE} | c_L = l) = \begin{cases} \sum_{j=0}^{l-(d_{LE}+1)} \tilde{\pi}_j & , \, l > d \\ 0 & , \, c.c. \end{cases} \tag{5.8}$$

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

$$EE(\bar{\gamma}_L, \bar{\gamma}_E) = \sum_{l=d_{LE}+1}^{N-1} \sum_{j=0}^{l-(d_{LE}+1)} \log_2(M_l) \cdot \pi_l \cdot \tilde{\pi}_j. \tag{5.9}$$

Da mesma forma que o realizado anteriormente para as técnicas de modulação adaptativa, a BER média do receptor legítimo para a técnica I é dada por:

$$P_L(\bar{\gamma}_L, \bar{\gamma}_E) = \frac{1}{EE} \sum_{l=0}^{N-1} \log_2(M_l) Pr(e_L, \xi_l), \tag{5.10}$$

sendo $Pr(e_L, \xi_l)$ a probabilidade de ocorrer um erro no receptor legítimo ao se utilizar o modo de transmissão l. Essa probabilidade pode ser escrita como:

$$\begin{aligned} Pr(e_L, \xi_l) &= Pr(e_L | \xi_l) \cdot Pr(\xi_l) \\ &= Pr(e_L | c_L > c_E + d_{LE}, c_L = l) \cdot Pr(c_l = l) \\ &\quad \cdot Pr(c_L > c_E + d_{LE} | c_L = l) \\ &= \int_{\lambda_l}^{\lambda_{l+1}} P_b(\gamma, M_l) f_{\bar{\gamma}_L}(\gamma) d\gamma \cdot Pr(c_L > c_E + d_{LE} | c_L = l), \end{aligned} \tag{5.11}$$

na qual $f_{\bar{\gamma}_L}$ é a fdp da RSR instantânea do canal legítimo. Utilizando novamente o resultado da equação (5.8), temos que:

$$\begin{aligned} &P_L(\bar{\gamma}_L, \bar{\gamma}_E) = \\ &\quad \frac{1}{EE} \cdot \sum_{l=d_{LE}+1}^{N-1} \sum_{j=0}^{l-(d_{LE}+1)} \tilde{\pi}_j \log_2(M_l) \int_{\lambda_l}^{\lambda_{l+1}} P_b(\gamma, M_l) f_{\bar{\gamma}_L}(\gamma) d\gamma. \end{aligned} \tag{5.12}$$

Para o cálculo da BER média do espião, substitui-se $Pr(e_L, \xi_l)$ por $Pr(e_E, \xi_l)$ na equação (5.10) e observa-se que o evento ξ_l é equivalente ao evento $\{c_E < l - d_{LE}\} \cap \{c_L = l\}$.

Sendo assim tem-se que:

$$\begin{aligned} Pr(e_E, \xi_l) &= Pr(e_E \cap c_E < l - d_{LE} \cap c_L = l) \\ &= Pr(e_E \cap c_E < l - d_{LE}) \cdot Pr(c_L = l) \\ &= \begin{cases} \int_{\lambda_0}^{\lambda_{l-d_{LE}}} P_b(\gamma, M_l) f_{\bar{\gamma}_E}(\gamma) d\gamma \cdot \pi_l & , \text{ se } l > d_{LE} \\ 0 & , \text{ c.c.} \end{cases}, \end{aligned} \tag{5.13}$$

onde na segunda igualdade utilizou-se a independência entre os canais legítimo e espião.

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

$$\begin{aligned} &P_E(\bar{\gamma}_L, \bar{\gamma}_E) = \\ &\quad \frac{1}{EE} \sum_{l=d_{LE}+1}^{N-1} \log_2(M_l) \int_{\lambda_0}^{\lambda_{l-d_{LE}}} P_b(\gamma, M_l) f_{\bar{\gamma}_E}(\gamma) d\gamma \cdot \pi_l. \end{aligned} \tag{5.14}$$

5.2.2 TÉCNICA II

Nesta técnica, admite-se que o estado do canal do espião não é conhecido no transmissor, visto que o primeiro não transmite nenhuma informação ao segundo. Mesmo assim é possível diminuir a probabilidade de ocorrer transmissões em que o canal legítimo se encontra em piores condições de propagação que o canal espião. Neste caso, permite-se a transmissão apenas quando o canal legítimo propicia boas condições de propagação. Sendo assim, a transmissão de informação é realizada quando c_L for maior que um estado mínimo para transmissão, $m \in \{\mathbb{N} | 0 \leq m < N - 1\}$. Quanto maior for o valor de m utilizado, 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:

$$EE(\bar{\gamma}_L) = \sum_{l=m+1}^{N-1} \log_2(M_l) \cdot \pi_l \tag{5.15}$$

Como na equação (5.10), a probabilidade de erro do canal legítimo é dada por:

$$P_L(\bar{\gamma}_L) = \frac{1}{EE} \sum_{l=m+1}^{N-1} \log_2(M_l) Pr(e_L, c_L = l), \tag{5.16}$$

sendo $Pr(e_L, c_L = l)$ dada por:

$$\begin{aligned} Pr(e_L, c_L = l) &= Pr(e_L | c_L = l) \cdot Pr(c_L = l) \\ &= \int_{\lambda_l}^{\lambda_{l+1}} P_b(\gamma, M_l) f_{\bar{\gamma}_L}(\gamma) d\gamma. \end{aligned} \tag{5.17}$$

De (5.16) e (5.17), tem-se que:

$$P_L(\bar{\gamma}_L) = \frac{1}{EE} \cdot \sum_{l=m+1}^{N-1} \log_2(M_l) \int_{\lambda_l}^{\lambda_{l+1}} P_b(\gamma, M_l) f_{\bar{\gamma}_L}(\gamma) d\gamma. \tag{5.18}$$

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

$$P_E(\bar{\gamma}_L, \bar{\gamma}_E) = \frac{1}{EE} \sum_{l=m+1}^{N-1} \log_2(M_l) Pr(e_E, c_L = l), \tag{5.19}$$

sendo

$$\begin{aligned} &Pr(e_E, c_L = l) = \\ &\quad = Pr(e_E | c_L = l) Pr(c_L = l) \\ &\quad = \int_0^{\infty} P_b(\gamma, M_l) f_{\bar{\gamma}_E}(\gamma) d\gamma \cdot \pi_l. \end{aligned} \tag{5.20}$$

Aplicando (5.20) em (5.19), chega-se a:

$$\begin{aligned} &P_E(\bar{\gamma}_L, \bar{\gamma}_E) = \\ &\quad \frac{1}{EE} \sum_{l=m+1}^{N-1} \log_2(M_l) \int_0^{\infty} P_b(\gamma, M_l) f_{\bar{\gamma}_E}(\gamma) d\gamma \pi_l. \end{aligned} \tag{5.21}$$

Observando as expressões de EE, P_L e P_E, nota-se que elas são idênticas às expressões equivalentes para as técnicas de modulação adaptativa excluindo-se os primeiros $m+1$ termos dos somatórios. Esse fato explica-se pois, na verdade, a técnica II consiste no emprego das técnicas de modulação adaptativa, conforme descrito no capítulo 2, sendo que não se realiza a transmissão de mensagens nos momentos em que o canal legítimo encontra-se nos $m+1$ primeiros estados. Sendo assim, as expressões analíticas da IM do receptor legítimo e da IM do espião para esta técnica podem

ser facilmente adaptadas das expressões para as técnicas de modulação adaptativa convencional da seguinte forma:

$$I_L(S;\hat{S}|\bar{\gamma}_L) = \sum_{l=m+1}^{N-1} \pi_l I_{Ll}(S;\hat{S}|\bar{\gamma}_L), \tag{5.22}$$

$$I_E(S;\hat{S}|\bar{\gamma}_L,\bar{\gamma}_E) = \sum_{l=m+1}^{N-1} \pi_l I_{El}(S;\hat{S}|\bar{\gamma}_L,\bar{\gamma}_E), \tag{5.23}$$

com $I_{Ll}(S;\hat{S}|\bar{\gamma}_L)$ e $I_{El}(S;\hat{S}|\bar{\gamma}_L,\bar{\gamma}_E)$ dados por (4.7) e (4.8) respectivamente.

5.2.3 TÉCNICA III

Nesta técnica propõem-se o emprego das expressões integrais obtidas no Capítulo 4 para I_L e I_E na otimização dos limiares de adaptação das técnicas de modulação adaptativas de forma a se maximizar a taxa de sigilo dos sistemas de comunicação que as empregam. Apesar da alta complexidade computacional do cálculo de I_E oriunda da necessidade de se efetuar o cálculo de $\mathscr{S}$ termos (equações (4.6), (4.20) e (4.21)), sendo

$$\mathscr{S} = \sum_{i=0}^{N-1} M_i^2, \tag{5.24}$$

com cada termo composto por 4 funções Q, a resolução deste problema de otimização ainda é viável, pois a integral em (4.20) não depende dos limiares de adaptação e pode ser calculada previamente.

Dessa forma os limiares de adaptação são obtidos por meio da resolução do seguinte problema de otimização:

$$\boldsymbol{\lambda} = \max_{\boldsymbol{\lambda}^* \in \mathbb{R}^{N+1}} R_s(\bar{\gamma}_L,\bar{\gamma}_E) \tag{5.25}$$

sujeito a:

$$\lambda_0 = 0, \tag{5.26}$$

$$\lambda_N = \infty, \tag{5.27}$$

$$\lambda_i \geq \gamma_{min}^i \tag{5.28}$$

e

$$\lambda_i < \lambda_{i+1}. \tag{5.29}$$

sendo γ^i_{min} o valor de RSR mínimo para o qual pode-se considerar que erros de símbolos ocorrem apenas entre símbolos vizinhos da constelação da modulação i, e R_s é dada por:

$$R_s = \sum_{l=0}^{N-1} \int_{\lambda_l}^{\lambda_{l+1}} \left(\log_2(M_l) - \frac{\Phi_l}{M_l} \right) f_{\bar{\gamma}_l}(\gamma) d\gamma - \sum_{l=0}^{N-1} \pi_l \mathscr{C}_l, \tag{5.30}$$

com Φ_l dado por (4.15) e $\mathscr{C}_l$ independente dos limiares de adaptação dado por (4.20). Os valores de γ^i_{min} considerados encontram-se na Tabela 4.1.

5.2.4 TÉCNICA IV

Nesta dissertação, considera-se que o espião possui o conhecimento da modulação empregada na transmissão de todos os blocos de dados, o que o coloca em uma situação favorável para a interceptação da mensagem transmitida. Mesmo neste cenário desfavorável para a transmissão sigilosa da informação, provou-se que as técnicas de modulação adaptativas tem a capacidade de transmitir informações em sigilo absoluto a taxas maiores que zero.

Nesta técnica pretende-se incluir um procedimento no mecanismo de transmissão das técnicas de modulação adaptativa de forma a diminuir o conhecimento do espião sobre o sistema de transmissão. Este procedimento consiste em uma rotação na constelação utilizada para a transmissão por um ângulo distinto em cada bloco transmitido conhecido entre o transmissor e o receptor. Dessa forma, mesmo que o espião saiba que modulação foi utilizada para a transmissão do bloco de dados, ele fará a detecção dos símbolos de acordo com a constelação não rotacionada, o que aumentará a sua probabilidade de erro de símbolo, diminuindo assim a IM entre os símbolos detectados e os símbolos transmitidos. Este procedimento não influencia o desempenho do receptor legítimo, visto que, como tem conhecimento do ângulo utilizado, ele pode desfazer a rotação antes de efetuar a detecção dos símbolos transmitidos em cada bloco.

A sequência de ângulos de rotação utilizada na transmissão pode ser escolhida segundo um procedimento de geração de números aleatórios no qual é empregada a mesma semente tanto no transmissor quanto no receptor de forma a garantir que ambos utilizem sequências idênticas. Esta semente pode ser acordada previamente à comunicação, ou até mesmo no estabelecimento da conexão.

5.3 RESULTADOS NUMÉRICOS E SIMULAÇÕES

5.3.1 TÉCNICAS I E II

Com o intuito de validar as expressões obtidas na Seção 5.2 e avaliar os desempenhos das técnicas I e II propostas, foram realizadas simulações de transmissões com um receptor legítimo na presença de um espião. O sistema considerado pode utilizar para a transmissão as modulações BPSK, 4-QAM, 16-QAM, 64-QAM, 256-QAM, 1024-QAM e 4096-QAM, além da opção de não transmitir. 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, $f_D T$, é igual a 10^{-4}. Os limiares de adaptação foram obtidos de forma maximizar a EE do sistema de comunicação atendendo a um requisito de 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. Em todos os casos, a RSR média dos canais legítimo e espião foram mantidas iguais e realizou-se a transmissão de 10^6 símbolos em cada simulação.

A Figura 5.1 apresenta um gráfico de comparação entre as curvas de probabilidade de erro de bit analíticas, P_L e P_E, e suas estimativas obtidas a partir dos sistemas simulados, BER_L e BER_E, para a técnica I, e, para fins de referência, curvas de P_L e P_E da técnica de modulação adaptativa descrita no Capítulo 2, bem como da estratégia de modulação fixa 4-QAM. Os valores de d_{LE} considerados foram de $d_{LE} = 0$ e $d_{LE} = 3$. Pode-se observar nessa figura que o simples uso da técnica de modulação adaptativa provoca uma degradação significativa da BER do espião em relação à BER do receptor legítimo. Além disso, há um aumento na probabilidade de erro do espião com o aumento de 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, validando assim as expressões obtidas anteriormente. 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, o que pode ser facilmente resolvido por meio da reavaliação dos limiares considerando as expressões de BER média específicas para a técnica I.

Ainda para o mesmo cenário, a Figura 5.2 mostra a comparação entre a EE da técnica de modulação adaptativa e a EE da técnica I. Novamente, os resultados de simulação validam as expressões integrais obtidas. Verifica-se uma degradação da

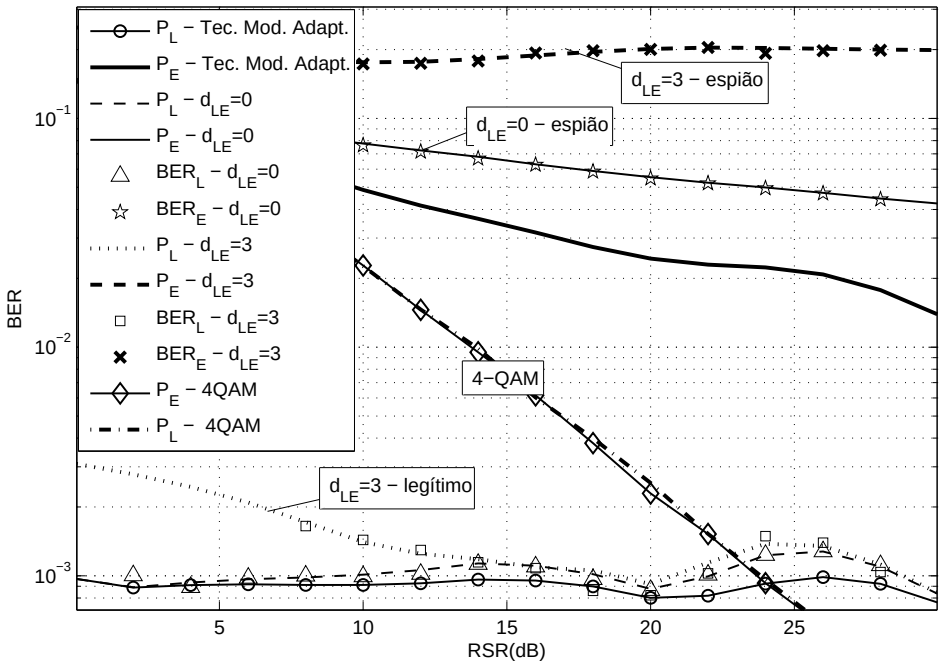

FIG. 5.1: BER dos canais legítimo e espião para a técnica I com $d_{LE} = 0$ e $d_{LE} = 3$ e da técnica de modulação adaptativa.

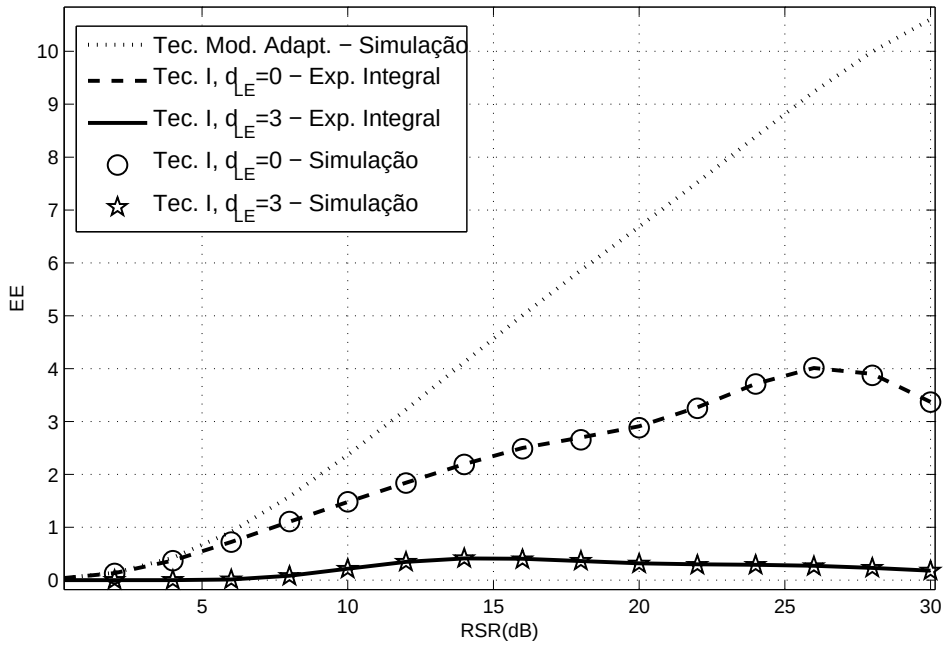

FIG. 5.2: EE da técnica I com $d_{LE} = 0$ e $d_{LE} = 3$ e da técnica de modulação adaptativa.

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, que provoca um aumento na sua capacidade de sigilo, e a EE do sistema de comunicação.

As Figuras 5.3 e 5.4 apresentam os resultados relativos à técnica II, na qual o transmissor não dispõe das informações do estado do canal do espião. Os resultados numéricos das expressões integrais estão de acordo com os resultados simulados obtidos e pode-se observar que mesmo neste caso é possível provocar 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 essas duas técnicas, a degradação observada na EE é resultante de períodos de ociosidade do canal de comunicação. A Figura 5.5 mostra um histograma da utilização do canal legítimo para a técnica II com $m = 5$ 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 5.6 apresenta as curvas de EE considerando todo o tempo de transmissão e a as curvas de EE ao se considerar apenas os momentos em que o canal legítimo é efetivamente ocupado.

Assim sendo, o uso dessas técnicas em conjunto com o emprego de mecanismos que identificam os períodos de ociosidade nos canais de comunicação e os aproveitam, conforme a filosofia dos rádios cognitivos, (HAYKIN, 2009), podem promover o uso global do espectro de forma eficiente enquanto propiciam maior segurança na transmissão de informações sigilosas pelo meio de comunicação sem fio.

Por fim, a Figura 5.7 apresenta curvas de R_s para a técnica II com $m = 3$ e $m = 5$, além da curva de R_s para a técnica de modulação adaptativa convencional. Observa-se que o aumento de m, apesar de aumentar a BER do espião, provoca a diminuição da taxa de sigilo do sistema. Este fato explica-se pois com o aumento de m na técnica II ocorre a diminuição do número de modulações disponíveis, o que torna o sistema de modulação adaptativo mais próximo ao sistema de modulação fixa.

5.3.2 TÉCNICA III

As curvas da taxa de sigilo, BER média do receptor legítimo e BER média do espião em função da RSR média dos canais legítimo e espião para as estratégias I, III e IV,

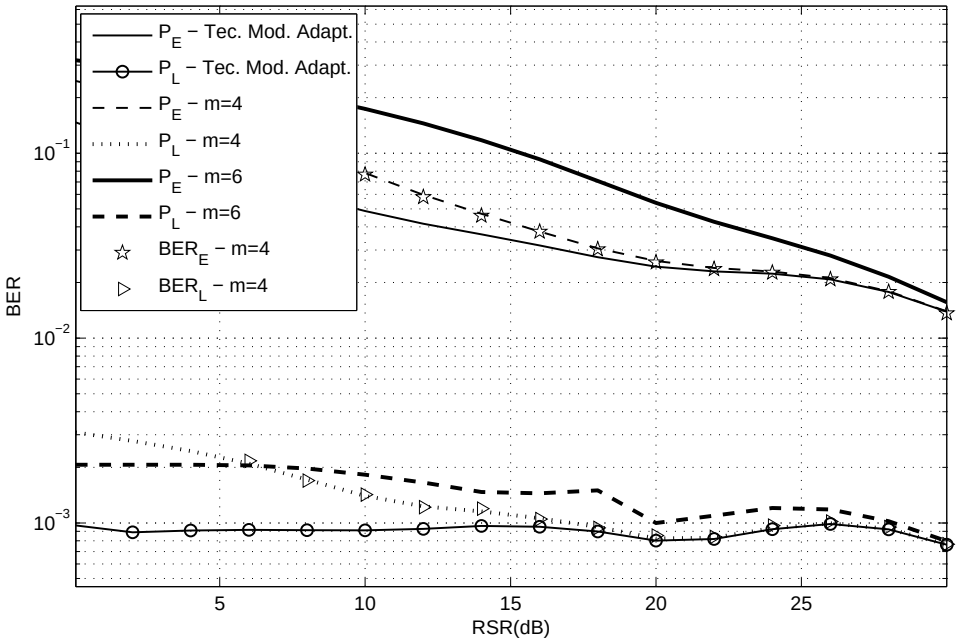

FIG. 5.3: BER dos canais legítimo e espião da técnica II com m=4 e m=6 e da técnica de modulação adaptativa.

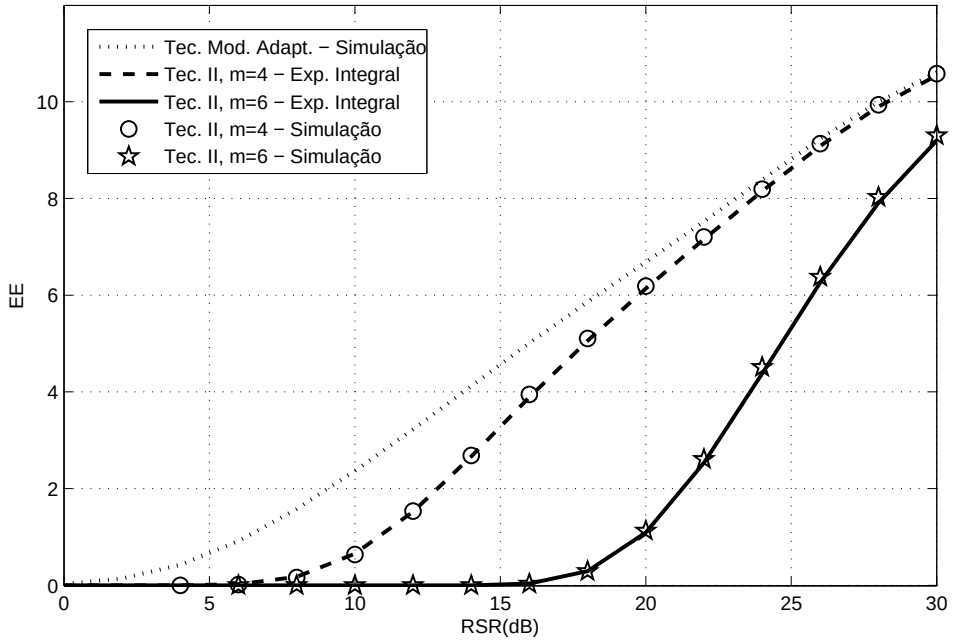

FIG. 5.4: EE da técnica II para m=4 e m=6 e da técnica de modulação adaptativa.

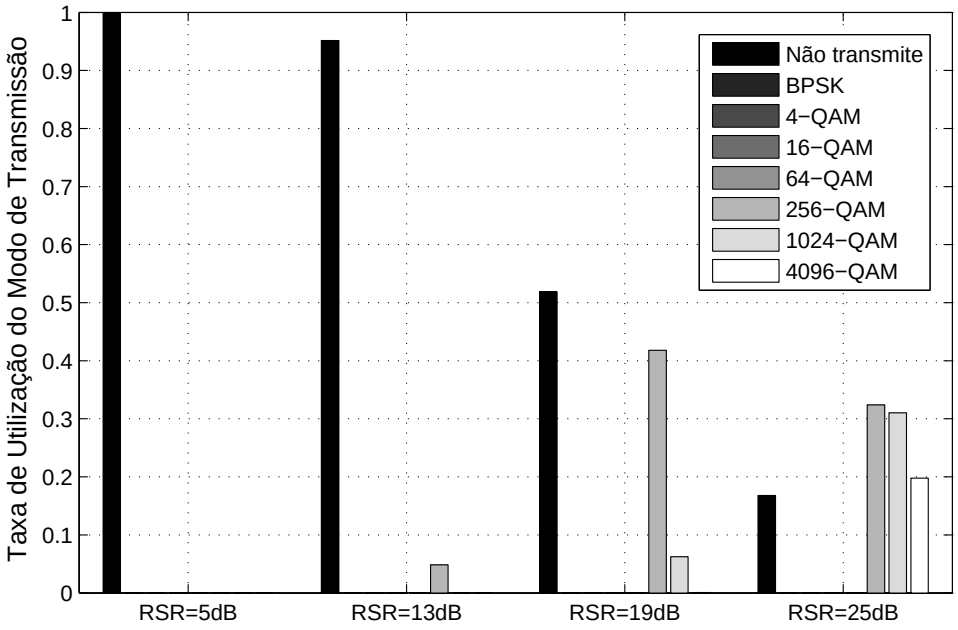

FIG. 5.5: Taxa de uso do canal legítimo para a técnica II com m=5 para valores selecionados de RSR média.

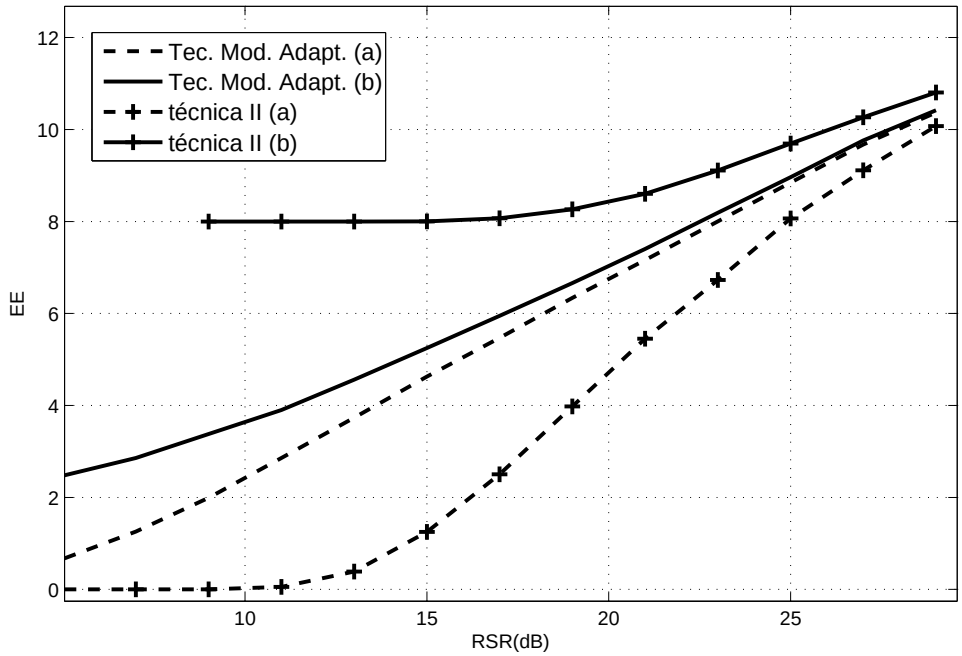

FIG. 5.6: EE da técnica II com m=5 e da técnica de modulação adaptativa considerando, no caso (a), todo o tempo de transmissão e, no caso (b), apenas o tempo em que o canal foi efetivamente ocupado.

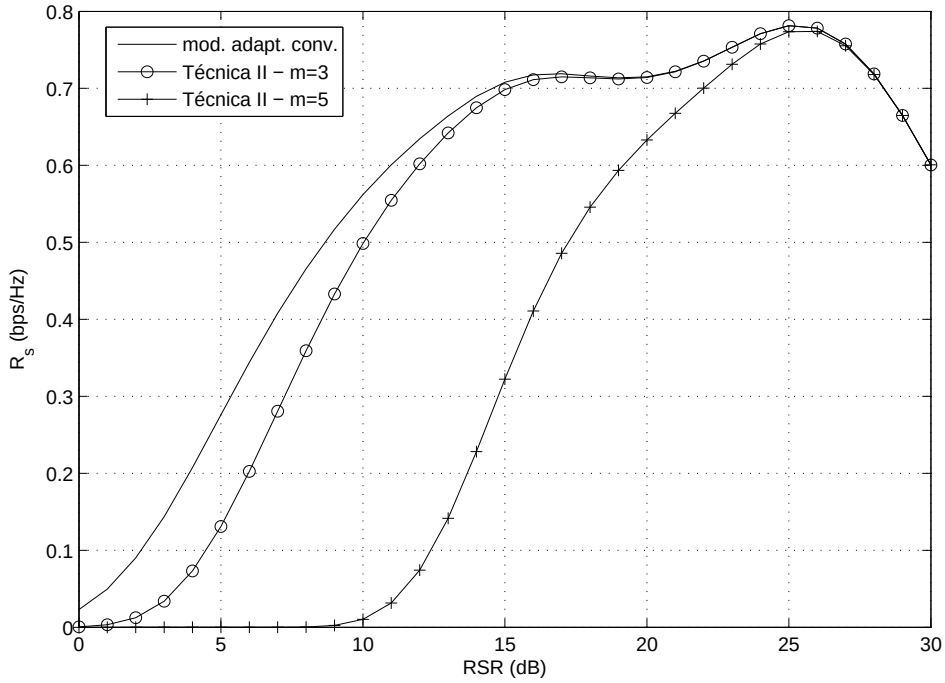

FIG. 5.7: R_s da técnica II com $m = 3$ e $m = 5$ e da técnica de modulação adaptativa convencional.

Estratégia	Objetivo	Vetor de limiares ($\boldsymbol{\lambda}$)
I	*Max* R_s	$[0\ \ 0,27\ \ 2,18\ \ 2,65\ \ 6,57\ \ 21,37\ \ 65,13\ \ 257,13\ \ \infty]$
III	*Max* R_s	$[0\ \ 1,06\ \ 2,68\ \ 2,69\ \ 6,49\ \ 6,5\ \ 20,43\ \ \infty]$
IV	*Max* R_s	$[0\ \ 1,15\ \ 2,63\ \ 6,48\ \ \infty]$

TAB. 5.1: Conjunto de limiares de adaptação para as estratégias I, III e IV que maximizam R_s.

descritas na Seção 4.3.4 do Capítulo 4, são apresentadas nas Figuras 5.8, 5.9 e 5.10. Para cada estratégia, são utilizados limiares que maximizam a EE média do sistema restrito a $\alpha = 10^{-3}$, limiares que maximizam a IM média do receptor legítimo na faixa de RSR considerada e os limiares que maximizam a R_s média. As RSR médias dos canais legítimo e espião foram mantidas iguais e os limiares de adaptação utilizados são apresentados nas Tabelas 4.5 e 5.1.

Observa-se para todas as estratégias que as curvas de R_s obtidas ao se utilizar os limiares que maximizam I_L são bem próximas às curvas obtidas ao se empregar os limiares que maximizam R_s. De fato, exceto para a estratégia I, a resolução do problema de otimização ao se utilizar como função objetivo a expressão de I_L resultou nos mesmos limiares que a resolução desse problema ao se utilizar como função

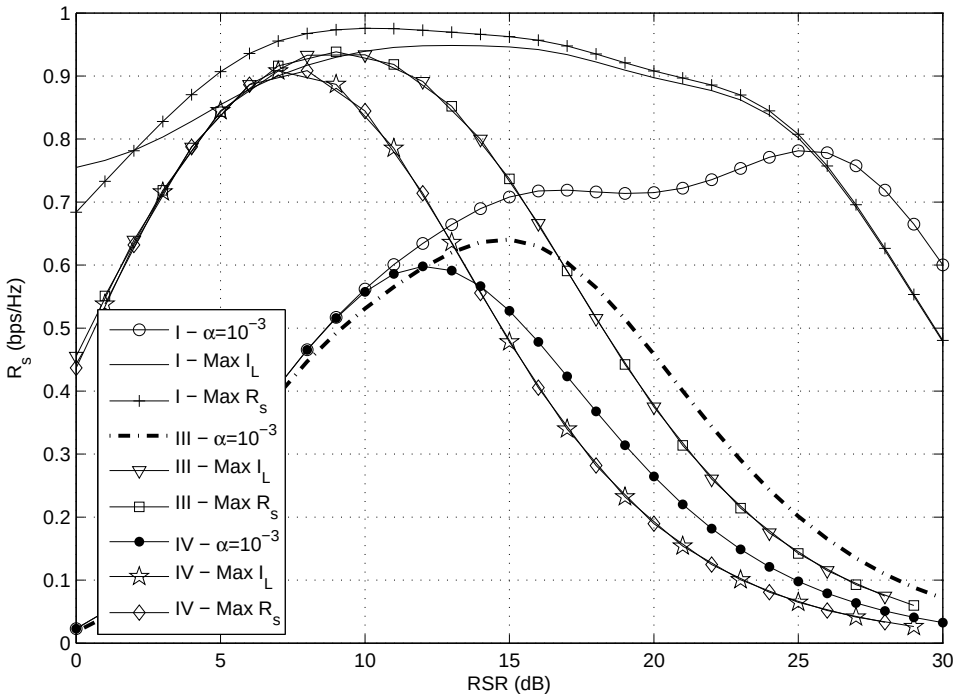

FIG. 5.8: Curvas de R_s para as estratégias I, III e IV para limiares que maximizam a EE restritos a $\alpha = 10^{-3}$, limiares que maximizam I_L e limiares que maximizam R_s.

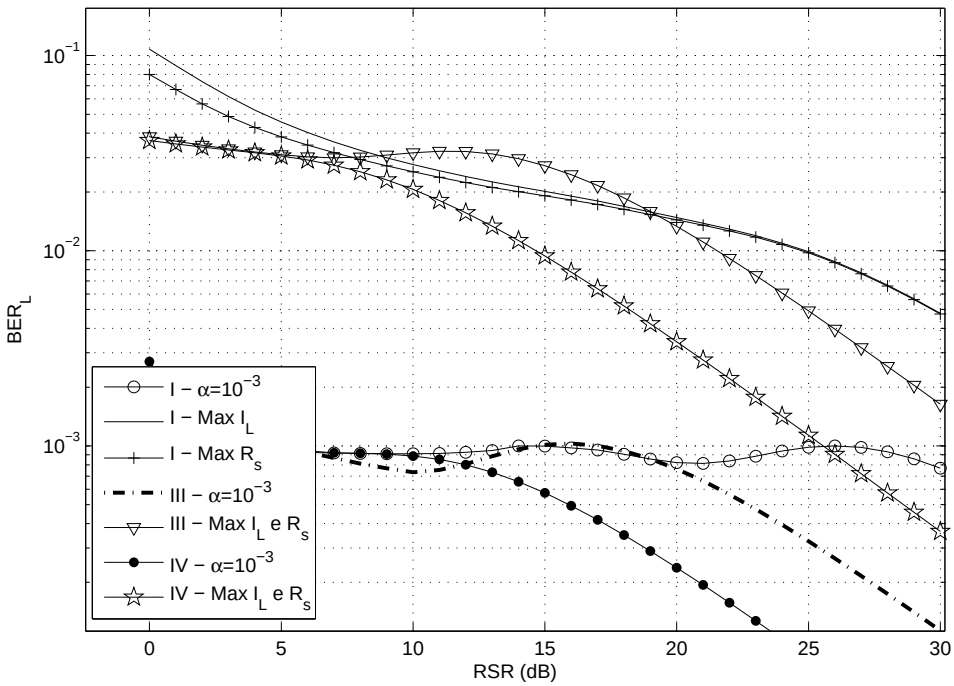

FIG. 5.9: Curvas de BER_L para as estratégias I, III e IV para limiares que maximizam a EE restritos a $\alpha = 10^{-3}$, limiares que maximizam I_L e limiares que maximizam R_s.

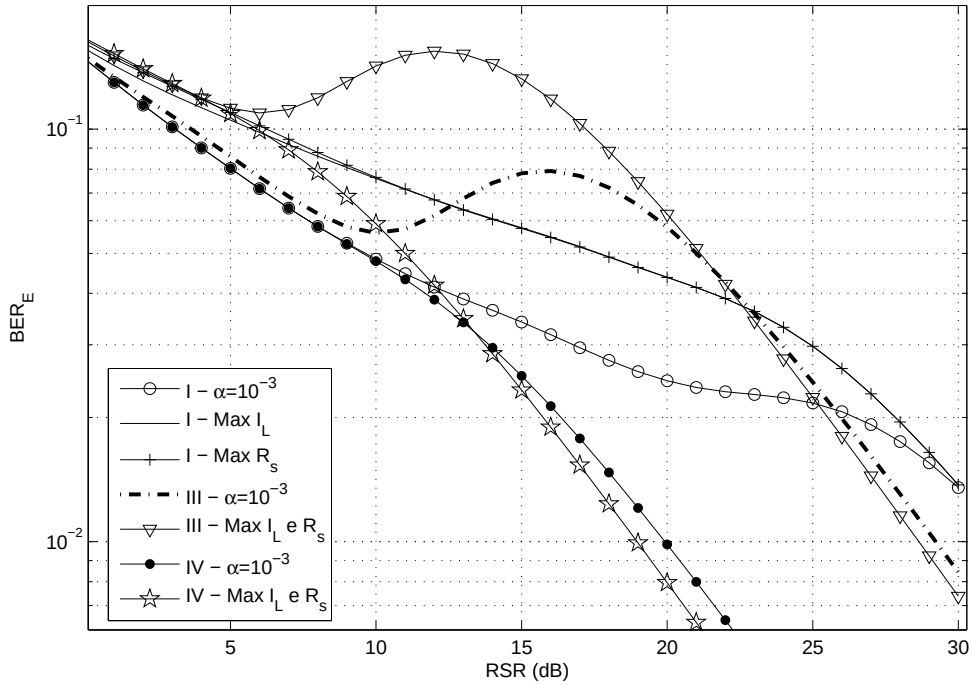

FIG. 5.10: Curvas de BER_E para as estratégias I, III e IV para limiares que maximizam a EE restritos a $\alpha = 10^{-3}$, limiares que maximizam I_L e limiares que maximizam R_s.

objetivo a expressão de R_s (5.30). Este fato pode ser explicado pela independência estatística dos canais legítimo e espião, o que faz com que a variação nos limiares de adaptação cause pequena variação em I_E. Sendo assim, a maximização de I_L acaba gerando também a maximização de R_s. Na Figura 5.8, as curvas de R_s para os limiares sujeitos a $\alpha = 10^{-3}$ atinge valores mais elevados que as outras duas curvas de R_s para cada estratégia pois utilizou-se o mesmo conjunto de limiares para todas os valores de RSR considerados e a busca dos limiares foi realizada no sentido de se maximizar a média entre todos os valores de R_s e I_L obtidos para cada valor de RSR.

Mais uma vez nota-se que apenas a BER não é suficiente para a análise do sigilo nos sistemas de comunicação. Como exemplo, para a estratégia I com uma RSR média de $10dB$, a diferença entre as BERs do receptor legítimo e do espião passa de $0,049$, quando são utilizado os limiares que atendem a $\alpha = 10^{-3}$, para $0,065$, quando são utilizados os limiares que maximizam R_s, ou seja, um aumento de 33%. Porém a taxa de sigilo passa de $0,55$ para $0,97$, o que consiste em um aumento de 76%.

Caso	Distribuição	valores
a)	Uniforme discreta	$\pi/8$, $\pi/4$, $3\pi/8$ e $\pi/2$
b)	Uniforme discreta	$\pi/16$, $\pi/8$, $3\pi/16$, $\pi/4$, $5\pi/16$, $3\pi/8$, $7\pi/16$ e $\pi/2$
c)	Uniforme contínua	entre 0 e $\pi/2$
d)	Uniforme contínua	entre 0 e π
e)	Uniforme contínua	entre 0 e 2π

TAB. 5.2: Casos de escolha das sequências de ângulos de rotação.

5.3.3 TÉCNICA IV

As Figuras 5.11, 5.12 e 5.13 ilustram os resultados de BER, I_E e R_s oriundos de simulações realizadas com o objetivo de verificar o desempenho da técnica IV ao se empregar a referida rotação para os limiares obtidos de forma a maximizar a EE atendendo a $\alpha = 10^{-3}$. Nessas simulações os canais legítimo e espião foram simulados de acordo com a técnica de Monte Carlo (GUIMARÃES, 1997) e sorteados independentemente, sendo que cada um deles é modelado por um processo estacionário em sentido amplo cuja DEP é dada pelo espectro de Jakes. Em ambos os canais considerou-se $f_D T = 10^{-4}$. O tamanho do bloco utilizado foi de 10 símbolos. Para cada simulação foram transmitidos 10^6 símbolos e manteve-se a RSR média do canal espião igual a RSR media do canal legítimo. As estimativas para todas as probabilidades envolvidas foram obtidas por frequência relativa, como, por exemplo, a probabilidade de erro de bit média do receptor legítimo foi estimada pela razão entre o número total de bits errados detectados pelo receptor legítimo e o número total de bits transmitidos.

Cada caso ilustrado nas Figuras 5.11, 5.12 e 5.13 refere-se a uma forma diferente de escolha da sequência de ângulos de rotação. Nos casos a) e b), os ângulos de rotação podem assumir valores discretos com mesma probabilidade, sendo, para o caso a), iguais a $\pi/8$, $\pi/4$, $3\pi/8$ e $\pi/2$, e, para o caso b), iguais a $\pi/16$, $\pi/8$, $3\pi/16$, $\pi/4$, $5\pi/16$, $3\pi/8$, $7\pi/16$ e $\pi/2$. Nos casos c), d) e e), os ângulos foram sorteados segundo distribuições uniformes, sendo no caso c) entre 0 a $\pi/2$, no caso d), entre 0 a π, e, no caso e), entre 0 a 2π. A Tabela 5.2 resume os casos de escolha da sequência de ângulos de rotação.

Ao se observar as curvas de BER presentes na Figura 5.11, nota-se que todos os casos apresentaram resultados semelhantes em relação à BER do espião, que aumentou significativamente em relação ao caso sem rotação. Entretando, verifica-se nas Figuras 5.12 e 5.13 que a IM do espião é afetada de forma diferente em cada caso. Este fato pode ser explicado considerando que a informação mútua diz respeito à quantidade

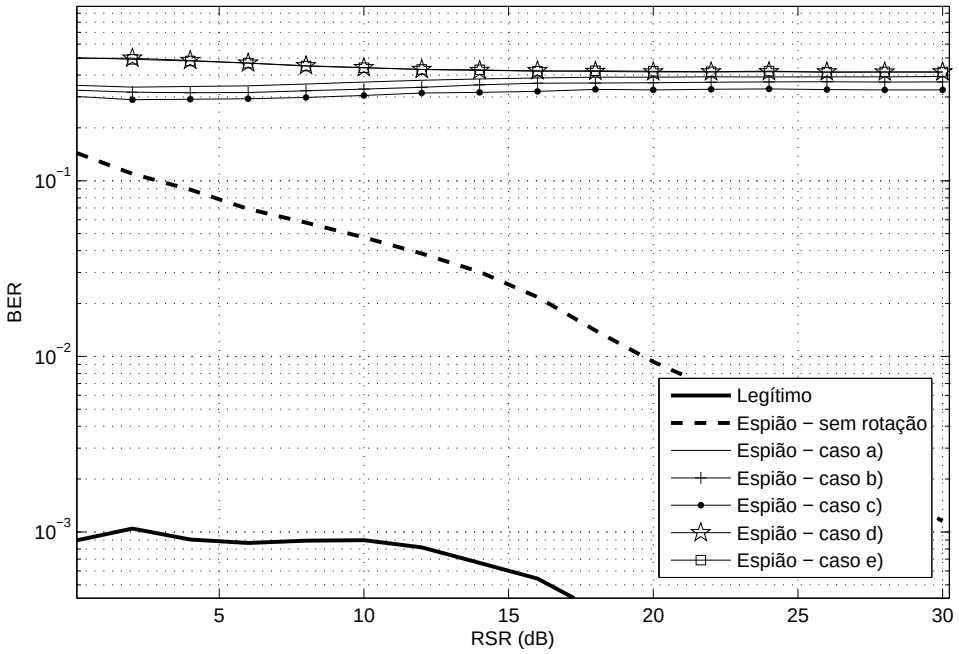

FIG. 5.11: Curvas de BER para a estratégia IV em função da RSR média dos canais legítimo e espião para constelações rotacionadas.

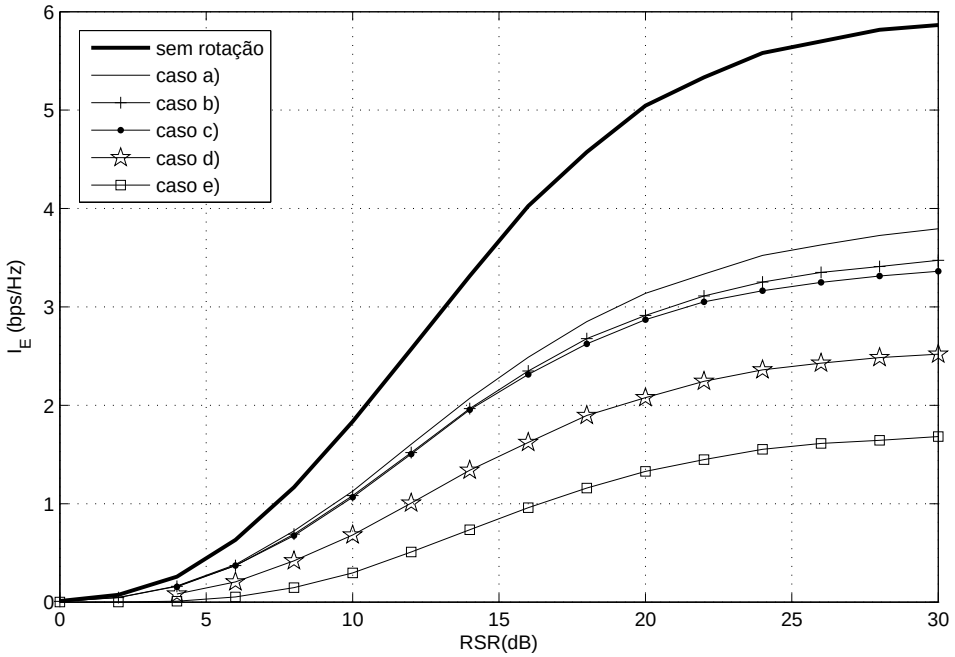

FIG. 5.12: Curvas de I_E para a estratégia IV em função da RSR média dos canais legítimo e espião para constelações rotacionadas.

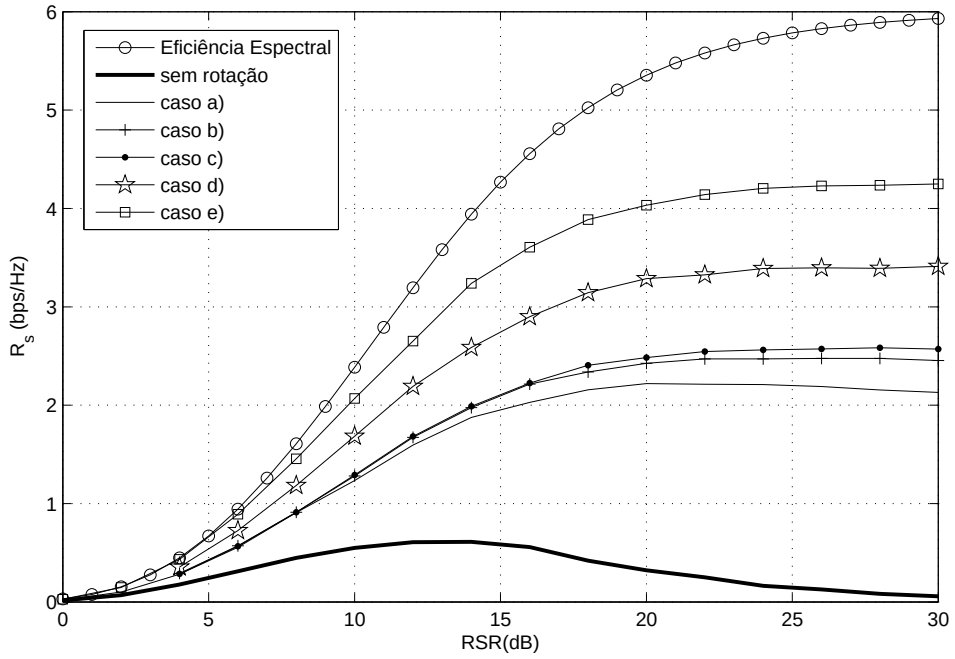

FIG. 5.13: Curvas de EE e R_s para a estratégia IV em função da RSR média dos canais legítimo e espião para constelações rotacionadas.

de informação que uma variável possui sobre a outra e não está relacionada aos valores assumidos por essas variáveis, como é o caso da BER. Por exemplo, se o transmissor utilizasse todas as suas constelações rotacionadas por um ângulo fixo, a BER do espião certamente aumentaria, porém a IM entre os símbolos detectados por ele e os símbolos transmitidos não se alteraria.

Comparando-se os casos a), b) e c) nota-se que a IM do espião diminui com o aumento do número de possíveis ângulos de rotação, pois a incerteza do símbolo transmitido dado o conhecimento do símbolo detectado no espião aumenta com o aumento do número de possíveis ângulos de rotação, o que por sua vez diminui a informação mútua entre os símbolos detectados no espião e os símbolos transmitidos. Pelo mesmo motivo, observa-se pelas curvas c), d) e e) que a IM do espião diminuiu ao se aumentar o máximo ângulo de rotação possível. A Figura 5.13 também apresenta a curva de EE para a estratégia IV. Pode-se observar que, no caso e), obteve-se uma taxa de sigilo relativamente alta, comparada com a curva de EE do sistema de transmissão em questão.

5.4 RESUMO

Neste capítulo quatro estratégias de transmissão baseadas nas técnicas de modulação adaptativa com o objetivo de potencializar o sigilo propiciado por essas técnicas foram propostas e analisadas. Duas delas consistem no aumento do sigilo nas comunicações por meio da transmissão de informação apenas em momentos considerados propícios. Essas técnicas foram capazes de degradar o desempenho do espião no que diz respeito à BER. A terceira estratégia proposta baseia-se na otimização dos limiares de adaptação das técnicas de modulação adaptativas a fim de maximizar as expressões de R_s apresentadas no Capítulo 4. Constatou-se que os limiares obtidos ao se maximizar I_L produzem taxas de sigilo próximas aos limiares que maximizam R_s, sendo assim, conclui-se que a expressão de I_L também pode ser utilizada de forma a maximizar a taxa de sigilo dos sistemas de modulação adaptativa. Por fim, a última estratégia consiste na aplicação de uma rotação nas constelações utilizadas pelos sistemas que empregam as técnicas de modulação adaptativa por um ângulo conhecido apenas pelo transmissor e pelo receptor legítimo de forma a aumentar a taxa de sigilo desses sistemas.

Por meio da análise das expressões apresentadas e via simulações computacionais constatou-se que é possível melhorar ainda mais o desempenho em termos de taxa de sigilo dos sistemas de comunicação em canais sujeitos ao desvanecimento plano e lento através do emprego de estratégias de transmissão baseadas nas técnicas de modulação adaptativa.

6 CONSIDERAÇÕES FINAIS

6.1 CONCLUSÕES

O presente trabalho teve por objetivo o estudo do sigilo nas comunicações em sistemas de modulação adaptativa empregados em canais caracterizados pelo efeito do desvanecimento plano em frequência e lento no tempo. O sistema analisado é constituído por um transmissor e um receptor legítimo que trocam informações e por um espião que possui acesso aos sinais transmitidos na comunicação. Dentre as contribuições apresentadas, destacam-se:

- Dedução de expressões analíticas para a BER do espião, I_L, I_E e R_s;
- Demonstração que o uso das técnicas de modulação adaptativa propicia aos sistemas de comunicação taxas de sigilo maiores que zero, o que possibilita a transmissão sigilosa de informação;
- Proposição de estratégias de transmissão que potencializam o sigilo nas comunicações decorrente do uso das técnicas de modulação adaptativa.

As expressões analíticas apresentadas nesta dissertação foram deduzidas em função das RSRs médias dos canais legítimo e espião, dos limiares de adaptação empregados no sistema de modulação adaptativa, e de outros parâmetros das modulações empregadas na transmissão, como o número de pontos nas suas constelações. Dessa forma foi possível comparar diversos sistemas de modulação adaptativa em termos de BER e R_s. Todas as expressões obtidas foram validadas por meio de simulações nas quais os canais legítimo e espião foram simulados de acordo com a técnica de Monte Carlo.

Observou-se que sistemas que possuem maior capacidade de adequação às condições do canal de comunicação, ou seja, sistemas que podem utilizar um maior número de modulações distintas, além de apresentarem maiores EEs, atingem maiores taxas de sigilo. Além disso, foi mostrado que taxas de sigilo consideráveis podem ser obtidas em cenários em que as condições médias do canal de propagação do espião são piores que as do canal legítimo. Outra importante constatação foi que os sistemas de modulação adaptativa que impõem restrições rígidas à BER alvo tendem a apresentar

menor taxa de sigilo que os sistemas que trabalham a taxas de erros maiores. Deste fato conclui-se que é mais vantajoso para o sistema de modulação adaptativa utilizar limiares de adaptação que produzem taxas de erro mais elevadas aliados a códigos corretores de erro, pois dessa forma, além de se obter maior EE, o sistema possuirá maior taxa de sigilo.

Além de se ter mostrado por meio dos resultados numéricos obtidos nas diversas análises realizadas durante o presente trabalho que os sistemas de comunicação que empregam as técnicas de modulação adaptativa em canais variantes no tempo podem ser utilizados para a transmissão em sigilo absoluto de informações, utilizou-se também um limitante inferior para R_s de tal forma que foi possível provar que tais sistemas atingem valores de R_s maiores que zero, mesmo em situações em que as condições de propagação do canal espião são melhores que as condições de propagação do canal legítimo.

Por fim, a potencialização da taxa de sigilo obtida no Capítulo 5 foi possível por meio do uso de mecanismos que dificultam a recepção por parte do espião dos símbolos transmitidos, o que demonstra o grande potencial das técnicas de modulação adaptativa ao serem combinadas com outras técnicas que visam aumentar a segurança nas comunicações.

6.2 PROPOSTAS PARA TRABALHOS FUTUROS

Nos trabalhos futuros, pretende-se dar continuidade às pesquisas em comunicações digitais e, em especial, à análise do uso das técnicas de modulação adaptativa no aumento da segurança nas comunicações. Dentre diversas opções, apresenta-se a seguir alguns temas para trabalhos:

- Avaliação do impacto das imperfeições do canal de retorno, como erros e atrasos, bem como da inclusão de erros de estimação da RSR instantânea por parte do receptor legítimo no desempenho dos sistemas que empregam as técnicas de modulação adaptativa no que diz respeito ao sigilo nas comunicações;

- Busca de outras funções $g(\gamma)$ de forma a se obter limitantes inferiores para a taxa de sigilo mais adequados a otimização dos limiares de adaptação das técnicas de modulação adaptativa de forma a se maximizar a taxa de sigilo desses sistemas;

- Considerar o espalhamento Doppler nas expressões de IM e de R_s dos sistemas de modulação adaptativa;

- Dedução das expressões analíticas para a taxa de sigilo dos sistemas que utilizam as técnicas de modulação adaptativa com rotação nas constelações apresentado na Seção 5.5.
- Análise do comportamento do sigilo nos sistemas de modulação adaptativa ao se considerar o espião com várias antenas receptoras;
- Avaliação do sigilo nas comunicações em sistemas MIMO e OFDM, com o emprego das técnicas de modulação adaptativa.

7 REFERÊNCIAS BIBLIOGRÁFICAS

ABDERRAHMANE, L. H. e BENYETTOU, M. **Using adaptive modulation in a leo satellite communication system**. *In: Proceedings of the 11th Conference on 11th WSEAS International Conference on Communications*, 11:255–259, 2007.

AL-KEBSI, I. I., ISMAIL, M., JUMARI, K., RAHMAN, T. A. e EL-SALEH, A. A. **A novel algorithm with a new adaptive modulation form to improve the performance of ofdm for 4g systems**. *In: International Conference on Future Computer and Communication*, págs. 11–15, April 2009.

BARROS, J. e RODRIGUES, M. R. D. **Secrecy capacity of wireless channels**. *In: IEEE international symposium on Informarion Theory*, págs. 356–360, July 2006.

BUTCHART, K. e BRAUN, R. **An adaptive modulation scheme for low earth orbit satellites**. *In: Proceedings of the 1998 South African Symposium on Communications and Signal Processing, 1998. COMSIG '98.*, págs. 43–46, Sep 1998.

C24-18. ***Manual de Campanha C24-18 - Emprego do rádio em Campanha***. Ministério do Exército, Estado Maior do Exército, 4 edition, 1997.

CHATTERJEE, S., FERNANDO, W. A. C. e WASANTHA, M. K. **Adaptive modulation based mc-cdma systems for 4g wireless consumer applications**. *In: IEEE Transactions on Consumer Electronics*, 49(4):995–1003, Nov 2003.

CHO, K. e YOON, D. **On the general ber expression of one- and two-dimensional amplitude modulations**. *In: IEEE Transactions on Communications*, 50(7):1074–1080, Jul 2002.

CONTI, A., WIN, M. Z. e CHIANI, M. **Invertible bounds for m-qam in rayleigh fading**. *In: IEEE Transactions on Wireless Communications*, 4(5):1994–2000, Sept 2005.

COVER, T. M. e THOMAS, J. A. ***Elementes of Information Theory***. John Wiley and Sons, 2 edition, 2006.

CSISZAR, I. e KORNER, J. **Broadcast channels with confidential messages**. *In: IEEE Transactions on Information Theory*, 24(3):339–348, May 1978.

DIERKS, T. e RESCORLA, E. **Rfc 5246 - the transport layer security (tls) protocol version 1.2**. *Internet Engineering Task Force Request for Comments*, aug 2008.

DUEL-HALLEN, A., HU, S. e HALLEN, H. **Long-range prediction of fading signals**. *In: IEE Signal Processing Magazine*, 17(3):62–75, May 2000.

EKPENYONG, A. E. e HUANG, Y.-F. **Feedback detection strategies for adaptive modulation systems**. *In: IEEE Transactions on Communications*, 54(10), October 2006.

GALDINO, J. F. e GURJÃO, E. C. **Otimização de limiares para adaptação de modulação diante de erros no canal de retorno**. *In: Anais do XXVI Simpósio Brasileiro de Telecomunicações - SBrT08*, Setembro 2008.

GOECKEL, D. L. **Adaptive coding for time-varying channels using outdated channel estimation**. *In: IEEE Transactions on Communications*, 47(6), Jun 1999.

GOLDSMITH, A. ***Wireless Communications.*** Cambridge University Press, 1 edition, 2005.

GOPALA, P. K., LAI, L. e GAMAL, H. E. **On the secrecy capacity of fading channels**. *In: IEEE Transactions on Information Theory*, 54(10):4687–4698, October 2008.

GUIMARÃES, A. G., PINTO, E. L. e GALDINO, J. F. **Comparação de desempenho de simuladores de canais com desvanecimento rápido - parte 1 - avaliação numérica**. *In: Anais do XV Simpósio Brasileiro de Telecomunicações*, págs. 426–430, 1997.

HANZO, L. e WONG, C. H. **Upper bound performance of a wide band adaptive modem**. *In: IEEE Transactions on Communications*, 48(3):367–369, March 2000.

HAYKIN, S., THOMSON, D. J. e REED, J. H. **Spectrum sensing for cognitive radio**. *In: Proceedings of the IEEE*, 97(5), May 2009.

KIM, Y.-D., KIM, I., CHOI, J., AHN, J.-Y. e LEE, Y. H. **Adaptive modulation for mimo systems with v-blast detection**. *In: Vehicular Technology Conference, 2003. VTC 2003-Spring*, 2:1074–1078, April 2003.

LEUNG-YAN-CHEONG, S. K. e HELLMAN, M. E. **The gaussian wiretap channel**. *In: IEEE Transactions on Informarion Theory*, 24(4):451–456, July 1978.

LIN, S. e COSTELLO, D. J. ***Error Control Coding***. Prentice Hall, 2 edition, 2004.

MACHADO, I. F. C. e GALDINO, J. F. **Erros no canal de retorno em sistemas que empregam modulação adaptativa**. *In: Anais do XXVII Simpósio Brasileiro de Telecomunicações*, 2009.

NEGI, R. e SATASHU, G. **Secret communication using artificial noise**. *In: IEEE 62nd Vehicular Technology Conference*, 3:1906–1910, September 2005.

PARSONS, J. D. ***The Mobile Radio Propagation Channel***. John Wiley, 2 edition, 2000.

PROAKIS, J. G. ***Digital Communications***. McGraw-Hill, 4 edition, 2001.

QIU, X. e CHAWLA, K. **On the performance of adaptive modulation in cellular systems**. *In: IEEE Transactions on Communications*, 47(6):884–895, June 1999.

RAPPAPORT, T. S. ***Wireless Communications - Principles and Practice***. Prentice Hall, 2 edition, 2002.

SHANNON, C. E. **A mathematical theory of communication**. *In: Bell System Tecnical Journal*, 27:379–423, July 1948.

SHANNON, C. E. **Communication theory of secrecy systems**. *In: Bell System Tecnical Journal*, 28:656–715, October 1949.

SKLAR, B. **Rayleigh fading channels in mobile digital communications systems - part i: Characterization**. *In: IEEE Communications Magazine*, 35(7):90–100, July 1997.

STALLINGS, W. ***Cryptography and network security: principles and practice***. Prentice Hall, 4 edition, 2005.

TANENBAUM, A. S. ***Computer Networks***. Prentice Hall, 4 edition, 2002.

TORRANCE, J. M. e HANZO, L. **Optimization of switching levels for adaptive modulation in slow rayleigh fading**. *In: IEEE Electronics letters*, 32(13):1167–1169, June 1996a.

TORRANCE, J. M. e HANZO, L. **Upper bound performance of adaptive modulation in a slow rayleigh fading channel**. *In: Electronics Letters*, 32(32):718–719, April 1996b.

WYNER, A. D. **The wire-tap channel**. *In: Bell System Tecnical Journal*, 54(8):1355–1387, 1975.

8 APÊNDICES

8.1 INFORMAÇÃO MÚTUA ENTRE S E $\hat{S}$ DADO O ESTADO DO CANAL LEGÍTIMO

Neste apêndice será mostrado que a expressão da IM entre os símbolos de entrada e os símbolos de saída em um sistema de transmissão que utiliza a modulação M_l-QAM em um canal AWGN com RSR γ, $I_l(S;\hat{S}|\gamma)$, pode ser simplificada ao se considerar que apenas ocorre erros entre símbolos adjacentes.

De acordo com (4.9), tem-se que esta Informação Mútua é dada por:

$$I_l(S;\hat{S}|\gamma) = \sum_{s=s_1}^{s_{M_l}} \sum_{\hat{s}=s_1}^{s_{M_l}} p(s;\hat{s}|\gamma) \log_2 \left[\frac{p(\hat{s}|s;\gamma)}{p(\hat{s}|\gamma)} \right], \tag{8.1}$$

Considerando que erros de símbolo apenas ocorrem entre símbolos adjacentes da constelação, ou seja

$$p(\hat{s}_j|s_i;\gamma) \approx \begin{cases} 0, \text{ se } \hat{s}_j \notin \mathcal{A}_i^l \\ q_l(\gamma), \text{ se } \hat{s}_j \in \mathcal{A}_i^l \\ 1 - \sum_{w \neq i} p_l(\hat{s}_w|s_i;\gamma), \text{ se } i = j \end{cases}, \tag{8.2}$$

sendo $\mathcal{A}_i^l$ o conjunto formado pelos símbolos adjacentes ao símbolo i da constelação da modulação M_l-QAM e q_l a probabilidade de erro de símbolo entre símbolos adjacentes dessa constelação, pode-se agrupar os símbolos da constelação M_l-QAM em 3 grupos indicados na Figura 4.2.

Sendo assim, eliminando os termos nulos do somatório duplo de (8.1), relativos aos pares de símbolos não adjacentes, esta equação se reduz a:

$$\begin{aligned} I_l(S;\hat{S}|\gamma) = & \\ & 4\left(\frac{(1-2q)}{M_l}\log_2\left([1-2q]M_l\right) + \frac{2q}{M_l}\log(qM_l)\right) + \\ & (2(Mc_l + Ms_l) - 8)\left(\frac{(1-3q)}{M_l}\log_2([1-3q]M_l) + \frac{3q}{M_l}\log_2(qM_l)\right) + \\ & (M_l - 2(Mc_l + Ms_l) + 4)\left(\frac{(1-4q)}{M_l}\log_2([1-4q]M_l) + \frac{4q}{M_l}\log_2(qM_l)\right) \end{aligned} \tag{8.3}$$

Agrupando os termos da expressão acima, tem-se que:

$$\begin{aligned} I_l(S;\hat{S}|\gamma) = & \\ & \log_2(M_l) + \frac{1}{M_l}\Big[(8q + [2(Mc_l + Ms_l) - 8]3q + [M_l - 2(Mc_l + Ms_l) + 4]4q)\log_2(q) + \\ & (4 - 8q)\log_2(1-2q) + (2(Mc_l + Ms_l) - 8 - 6q(Mc_l + Ms_l) + 24q)\log_2(1-3q) + \\ & (1-4q)(M_l - 2(Mc_l + Ms_l) + 4)\log_2(1-4q)\Big] \end{aligned} \tag{8.4}$$

Uma forma mais compacta de se denotar (8.4) é

$$I_l(S;\hat{S}|\gamma) = \log_2(M_l) - \frac{\Phi_l}{M_l}, \tag{8.5}$$

em que

$$\Phi_l = \sum_{j=1}^{4} a_{lj} \log_2 \Big[u(j-2) + (-j)^{u(j-2)} q_l(\gamma)\Big], \tag{8.6}$$

com

$$a_{l1} = (-4M_l + 2(Mc_l + Ms_l))q_l(\gamma), \tag{8.7}$$

$$a_{l2} = 8q_l(\gamma) - 4, \tag{8.8}$$

$$a_{l3} = (6(Mc_l + Ms_l) - 24)q_l(\gamma) - 2(Mc_l + Ms_l) + 8, \tag{8.9}$$

$$a_{l4} = (4M_l - 8(Mc_l + Ms_l))q_l(\gamma) + 2(Mc_l + Ms_l) - 4 - M_l. \tag{8.10}$$

Em (8.6) $u(x)$ representa a função degrau unitário, ou seja, $u(x) = 0$ para $x < 0$ e $u(x) = 1$ para $x \geq 0$.

Livros Grátis

(http://www.livrosgratis.com.br)

Milhares de Livros para Download:

Baixar livros de Administração
Baixar livros de Agronomia
Baixar livros de Arquitetura
Baixar livros de Artes
Baixar livros de Astronomia
Baixar livros de Biologia Geral
Baixar livros de Ciência da Computação
Baixar livros de Ciência da Informação
Baixar livros de Ciência Política
Baixar livros de Ciências da Saúde
Baixar livros de Comunicação
Baixar livros do Conselho Nacional de Educação - CNE
Baixar livros de Defesa civil
Baixar livros de Direito
Baixar livros de Direitos humanos
Baixar livros de Economia
Baixar livros de Economia Doméstica
Baixar livros de Educação
Baixar livros de Educação - Trânsito
Baixar livros de Educação Física
Baixar livros de Engenharia Aeroespacial
Baixar livros de Farmácia
Baixar livros de Filosofia
Baixar livros de Física
Baixar livros de Geociências
Baixar livros de Geografia
Baixar livros de História
Baixar livros de Línguas

Baixar livros de Literatura
Baixar livros de Literatura de Cordel
Baixar livros de Literatura Infantil
Baixar livros de Matemática
Baixar livros de Medicina
Baixar livros de Medicina Veterinária
Baixar livros de Meio Ambiente
Baixar livros de Meteorologia
Baixar Monografias e TCC
Baixar livros Multidisciplinar
Baixar livros de Música
Baixar livros de Psicologia
Baixar livros de Química
Baixar livros de Saúde Coletiva
Baixar livros de Serviço Social
Baixar livros de Sociologia
Baixar livros de Teologia
Baixar livros de Trabalho
Baixar livros de Turismo