



UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO TECNOLÓGICO
DEPARTAMENTO DE ENGENHARIA ELÉTRICA E ELETRÔNICA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

Técnicas de Forçagem a Inteiros para Canais MIMO de Múltiplo Acesso com Desvanecimento de Bloco

Dissertação submetida à Universidade Federal de Santa Catarina
como parte dos requisitos obtenção do grau de Mestre em Engenharia
Elétrica.

Ricardo Bohaczuk Venturelli
Orientador: Prof. Danilo Silva, Ph.D.

Florianópolis, 24 de outubro de 2016.

RICARDO BOHACZUK VENTURELLI

**TÉCNICAS DE FORÇAGEM A
INTEIROS PARA CANAIS MIMO DE
MÚLTIPLO ACESSO COM
DESVANECIMENTO DE BLOCO**

Dissertação submetida ao Programa
de Pós-Graduação em Engenharia Elé-
trica da Universidade Federal de Santa
Catarina para a obtenção do Grau de
Mestre em Engenharia Elétrica
Orientador: Prof. Danilo Silva, Ph.D.

**FLORIANÓPOLIS
2016**

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Venturelli, Ricardo
Técnicas de Forçagem a Inteiros para Canais MIMO de
Múltiplo Acesso com Desvanecimento de Bloco / Ricardo
Venturelli ; orientador, Danilo Silva - Florianópolis, SC,
2016.
xxii+46 p.

Dissertação (mestrado) - Universidade Federal de Santa
Catarina, Centro Tecnológico. Programa de Pós-Graduação em
Engenharia Elétrica.

Inclui referências

1. Engenharia Elétrica. 2. Forçagem a Inteiros. 3.
Canais MIMO. 4. Desvanecimento de Bloco. I. Silva, Danilo.
II. Universidade Federal de Santa Catarina. Programa de Pós
Graduação em Engenharia Elétrica. III. Título.

TÉCNICAS DE FORÇAGEM A INTEIROS PARA CANAIS MIMO DE MÚLTIPLO ACESSO COM DESVANECIMENTO DE BLOCO

Esta Dissertação foi julgada adequada para a obtenção do título de Mestre em Engenharia Elétrica, área de concentração Comunicações e Processamento de Sinais, e aprovada em sua forma final pelo Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Santa Catarina.

Florianópolis, 28 de setembro de 2016.



Marcelo Lobo Heldwein, Ph.D.

Coordenador do Programa de Pós-Graduação em Engenharia Elétrica

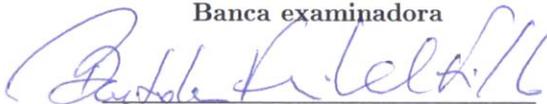


Prof. Danilo Silva, Ph.D.

Orientador

Universidade Federal de Santa Catarina

Banca examinadora



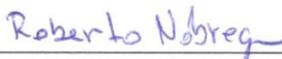
Prof. Bartolomeu Ferreira Uchôa Filho, Ph.D.

Universidade Federal De Santa Catarina



Prof. Carlos Aurélio Faria da Rocha, Dr.

Universidade Federal de Santa Catarina



Prof. Roberto Wanderley da Nóbrega, Dr.

Instituto Federal de Santa Catarina

Dedico esta dissertação a todos que me ajudaram.

Agradecimentos

Desejo expressar meu reconhecimento a todos que, de uma maneira ou outra, colaboraram na realização deste trabalho, em especial

ao professor Danilo Silva, pela dedicação ao trabalho, pela excelente orientação, por todo o incentivo para procurar soluções dos problemas encontrados e pelas críticas, correções e revisões dessa dissertação;

aos professores Bartolomeu Ferreira Uchôa Filho, Carlos Aurélio Faria da Rocha e Roberto Wanderley da Nóbrega, membros da banca examinadora, pela leitura, correções e sugestões para a dissertação que com certeza ajudaram a melhorá-la;

aos professores Leonardo Silva Resende, Raimes Moraes, Djones Lettnin, Eduardo Augusto Bezerra e demais professores do Laboratório de Comunicação e Sistemas Embarcados por todo apoio moral durante os seminários do laboratório;

aos amigos Bruno Fontana da Silva, Juliana Inácio Camillo e Paulo Ricardo Branco da Silva, companheiros para almoço, para o café da tarde e, claro, para discussão da pesquisa, sempre incentivando e propondo novas maneiras de solucionar algum problema;

aos amigos Bruno Seng Chang, Daniel Severo, Pedro Giassi Junior, Gustavo Kasper Facenda, Maria Cláudia Castro e demais colegas e ex-colegas de laboratório que sempre, de alguma maneira, contribuíram para chegar aonde estou;

aos amigos Arthur Zeferino, Bolivar Escobar, Dalton Alexandre P. Vaz, Eduardo Medeiros Schütt, Emygdio Affonso de Faria, Francisco Izzo, Giordano Pivatto, Guilherme Pires, Gustavo Kazuo Hashizume, Luigi Ligocky, Luis Gustavo Aleixo, Marcellus Vinicius, Meg Ganciné, Rafael Soares, Renato Lopes, Shana Ximenes, Thierry D. Freitas e demais amigos dos “Piratas do Quiz” por mostrar que a amizade via internet pode ser duradoura e pelos dias na

Iha do Mel que me ajudou a relaxar em um momento de turbulência;

aos amigos Adelmo Oliveira, Carlos Leite, Janilson Lemos, Marcelo Ferrantini, Vitor Camargo e demais amigos da “Fanáticos por Esportes Internacionais e Associados” que fazem com que assistir jogos de futebol americano seja ainda mais divertido, mesmo estando distantes;

à minha irmã Rafaela Bohaczuk Venturelli Knop e meu cunhado André Felipe Knop, por todo apoio ao longo dos anos;

aos meus pais Ivo José Venturelli e Marly Bohaczuk Venturelli, por todo o suporte que me deram e ainda me dão ao longo da vida;

as demais pessoas que contribuíram para a dissertação mas não foram aqui citadas.

Don't you dare go Hollow. (Laurentius from Dark Souls)

RESUMO

Forçagem a inteiros é um novo método de detecção linear para canais MIMO. Essa técnica é baseada no processamento computa-e-encaminha utilizado em codificação de rede na camada física, o qual tenta recuperar combinações das palavras-código enviadas ao invés de cada palavra-código isoladamente. O método forçagem a inteiros é uma generalização dos métodos tradicionais de detecção linear como o detector com forçagem a zero e de menor erro quadrático médio. Recentemente, a abordagem de forçagem a inteiros foi generalizada para canais com desvanecimento de bloco, nos quais o desvanecimento do canal pode variar durante a transmissão de uma palavra-código. Tal modelo de canal pode ser usado, por exemplo, como uma aproximação para um sistema OFDM com seletividade em frequência. No trabalho de El Bakoury e Nazer são citados dois métodos de decodificação para esse cenário, que são chamados de decodificação via média aritmética (AM) e via média geométrica (GM). Embora com a decodificação GM é possível alcançar taxas maiores do que com a decodificação AM, não se conhece algum algoritmo eficiente para encontrar os coeficientes ótimos das combinações lineares. Essa dissertação tem como objetivo propor um algoritmo sub-ótimo de baixa complexidade para escolher esses coeficientes, assim como validar experimentalmente seu desempenho com códigos de comprimento finito e modulações tradicionais como 2-PAM.

Palavras-chave: Forçagem a Inteiros, Canais MIMO, Desvanecimento de Bloco.

ABSTRACT

Integer forcing is a new approach for linear detection in MIMO channels. This technique is based on the compute-and-forward processing used in physical-layer network coding, which tries to recover linear combinations of codewords rather than individual codewords. The integer-forcing approach generalizes traditional linear detection methods such as zero-forcing and minimum-mean-squared-error detection. Recently, integer forcing was generalized to block fading channels, allowing the fading channel to vary during the transmission of a codeword. This channel model can be used, for example, as an approximation for OFDM systems with frequency-selective fading. In the work of El Bakoury and Nazer, two decoding methods are shown for this scenario, namely arithmetic-mean (AM) and geometric-mean (GM) decoding. Although GM decoding can achieve higher rates than AM decoding, no efficient algorithm is known to find the optimal coefficients of the linear combinations. This thesis has the goal to propose a sub-optimal, low-complexity scheme to find these coefficients, as well as validate its performance with finite-length codes and traditional modulation schemes such as 2-PAM.

Keywords: Integer Forcing, MIMO Channels, Block Fading.

Abreviaturas

Notação	Descrição
AM	Aritmetic mean.
AWGN	Additive white Gaussian noise.
BF	Block fading.
BPSK	Binary phase shift keying.
FER	Frame error rate.
GM	Geometric mean.
IF	Integer forcing.
LDPC	Low density parity check.
LLL	Lenstra-Lenstra-Lovász.
LLR	Log-likelihood ratio.
MIMO	Multiple-input multiple-output.
ML	Maximum likelihood.
MMSE	Minimum mean square error.
OFDM	Orthogonal frequency division multiplexing.
PAM	Pulse-amplitude modulation.
SIC	Successive interference cancellation.
SIF	Successive integer forcing.

Notação	Descrição
SISO	Single-input single-output.
SIVP	Shortest independent vectors problem.
SNR	Signal-to-noise ratio.
SVP	Shortest vector problem.
ZF	Zero forcing.

Lista de Figuras

3.1	Distribuição do ruído efetivo em um canal 2×2 considerando desvanecimento estático.	25
3.2	Distribuição do ruído efetivo em um canal 2×2 com dois blocos. A matriz \mathbf{A} foi escolhida através do método proposto 2. O receptor utiliza o decodificador AM.	25
3.3	Distribuição do ruído efetivo em um canal 2×2 com dois blocos. A matriz \mathbf{A} foi escolhida através do método proposto 2. O receptor utiliza o decodificador GM.	25
3.4	Probabilidade de transição do canal equivalente.	26
4.1	Taxas alcançáveis para uma probabilidade de <i>outage</i> de 1% em um canal 2×2 com um bloco (desvanecimento estático).	30
4.2	Taxas alcançáveis para uma probabilidade de <i>outage</i> de 1% em um canal 2×2 com dois blocos.	31
4.3	Taxas alcançáveis para uma probabilidade de <i>outage</i> de 1% em um canal 2×2 com três blocos.	32
4.4	Taxas alcançáveis para uma probabilidade de <i>outage</i> de 1% em um canal 2×2 com quatro blocos.	33
4.5	Taxas alcançáveis para uma probabilidade de <i>outage</i> de 1%, em um canal 2×2 e com $\text{SNR} = 25$ dB variando o número de blocos (N).	33
4.6	Taxas alcançáveis para uma probabilidade de <i>outage</i> de 1%, em um canal com dois blocos e $\text{SNR} = 25$ dB variando o número de usuários (N_T) e considerando $N_R = N_T$	34

- 4.7 FER para um canal 2×2 com dois blocos, utilizando um código *root*-LDPC com taxa $1/2$ 37
- 4.8 FER para um canal 2×2 com três blocos e $SNR = 25$ dB, utilizando um código *root*-LDPC com taxa $1/3$ 37
- 4.9 FER para um canal 2×2 com quatro blocos e $SNR = 25$ dB, utilizando um código *root*-LDPC com taxa $1/4$. . . 38

Lista de Tabelas

4.1	Probabilidade de <i>outage</i> para um canal 2×2 com $N = 2$ blocos e $\text{SNR} = 10$ dB.	35
-----	--	----

Sumário

1	Introdução	1
1.1	Objetivos	5
1.1.1	Publicações	5
1.2	Organização	5
1.3	Notação	6
2	IF em Canais com Desvanecimento de Bloco	7
2.1	Modelo do Canal	7
2.2	Detector ML	9
2.3	Decodificação Linear Tradicional	9
2.3.1	Método ZF	10
2.3.2	Método MMSE	11
2.4	IF em Canais com Desvanecimento Estático	11
2.4.1	Escolha da matriz \mathbf{A}	14
2.5	Extensão para Desvanecimento de Blocos	15
2.5.1	Decodificador via Média Aritmética	17
2.5.2	Decodificador via Média Geométrica	18
2.5.3	Escolha da matriz \mathbf{A}	18
3	Técnicas Propostas	21
3.1	Escolha Sub-ótima de \mathbf{A} para Decodificador GM	21
3.1.1	Método Proposto 1	22
3.1.2	Método Proposto 2	22
3.2	Códigos Práticos	23

4 Resultados	29
4.1 Taxas Alcançáveis	29
4.2 Taxa de Erro de Quadro (FER)	35
5 Conclusão	39
A Reticulados	41
Referências bibliográficas	43

Introdução

Hoje em dia, a comunicação sem fio é amplamente utilizada em diversas aplicações, por exemplo, a telefonia celular. Um dos motivos do avanço na tecnologia da comunicação sem fio se dá pelo sucesso do padrão da segunda geração (2G) de redes de celular no começo dos anos 90 [1, 2, 3]. A mudança da tecnologia analógica (1G) para digital (2G) permitiu que sistemas de comunicação sem fio alcançassem maiores taxas de transmissão, melhor desempenho e melhor confiabilidade [3].

No começo dos anos 2000, o padrão de terceira geração (3G) foi implementado. Além de serviço de voz, o 3G deveria providenciar altas taxas (na faixa de Mbps) em serviços de internet, jogos interativos, áudio de alta qualidade e vídeos de entretenimento [2].

Atualmente, a tecnologia de transmissão sem fio encontra-se em sua quarta geração (4G), porém, acredita-se que até 2020 a tecnologia de quinta geração (5G) já esteja em uso. Pode-se perceber que dentre os desafios no avanço de uma geração encontra-se o aumento na taxa de transmissão dos usuários.

Uma das maneiras mais populares de aumentar a taxa de transmissão é o uso de múltiplas antenas no transmissor e no receptor, o que é conhecido como tecnologia MIMO (do inglês, *multiple-input multiple-output*) [4]. A principal ideia da tecnologia MIMO é que as antenas do transmissor e do receptor são espaçadas de tal modo que criam diversos canais efetivos em paralelo, aumentando então a taxa, ou seja, o nú-

mero de bits de informação enviados em uma transmissão (conhecido como multiplexação espacial), ou aumentando a qualidade da comunicação, isto é, diminuindo a probabilidade de erro, que é a probabilidade de o receptor não recuperar todos os bits de informação transmitidos (conhecido como diversidade espacial) [5].

A taxa de transmissão e a taxa de erro de quadro (FER, do inglês *frame-error rate*) são duas medidas essenciais para se medir a desempenho de um sistema de comunicação. A taxa de transmissão é definida como a taxa em que os dados (informação) são transmitidos por unidade de banda, enquanto a FER é definida como a probabilidade de o decodificador, no receptor, não recuperar os dados corretamente. A FER é uma função da SNR e da taxa de transmissão. Intuitivamente, sabe-se que para uma taxa de transmissão fixa, aumentar a SNR irá reduzir a FER. Similarmente, para uma FER fixa, o aumento da SNR permite um aumento na taxa de transmissão. Portanto, existe um *trade-off* entre a taxa de transmissão e a FER. Em sistemas MIMO, isso é conhecido como *trade-off* de diversidade-multiplexação, em que diversidade espacial significa redução da FER e multiplexação significa aumento da taxa de transmissão [4].

No escopo desse trabalho, iremos focar apenas na multiplexação espacial. A multiplexação espacial explora o fato que canais MIMO criam múltiplos caminhos entre transmissor e receptor. Com isso, cria-se a possibilidade de que vários usuários transmitam utilizando a mesma frequência, possibilitando um menor uso do espectro de frequências [6]. Diferente de esquemas que focam em diversidade espacial, em esquemas de multiplexação os sinais transmitidos interferem, de modo desconhecido, uns nos outros no receptor. Para que seja possível separar os sinais de forma confiável no receptor é necessário que o número de antenas no receptor seja maior ou igual ao número de antenas transmissoras [4].

O sinal recebido em cada antena do receptor é uma soma dos sinais enviados pelos transmissores, cada sinal com um ganho proporcionado pelo canal, e são acrescido de um ruído. O receptor deve ser capaz de extrair (demultiplexar) cada sinal individualmente através de algum processamento [6].

Uma maneira de inferir os sinais transmitidos é encontrar, a partir do conjunto de sinais recebidos, o conjunto de possíveis sinais transmitidos mais próximos em termos de distância Euclidiana [3, 7]. Esse

esquema é conhecido como detector de máxima verossimilhança conjunta (ML, do inglês *joint maximum-likelihood*). Embora o detector ML forneça maiores taxas do que qualquer outro esquema (inclusive alcançando a capacidade do canal MIMO ponto-a-ponto em algumas situações), sua complexidade é proibitivamente alta, uma vez que ela aumenta exponencialmente com o número de antenas transmissoras e com o comprimento da palavra-código [7]. Para reduzir a complexidade, detectores sub ótimos são utilizados, como por exemplo, receptores com detecção linear.

Receptores com detecção linear, apesar de serem mais simples, são aqueles que apresentam as piores FER [3]. Esse tipo de receptor aplica uma transformação linear (também chamada de equalização) no conjunto de sinais recebidos. Tradicionalmente, dois métodos de equalização são bastante populares: o detector com forçagem a zero (ZF, do inglês *zero-forcing*) e o detector de mínimo erro quadrático médio (MMSE, do inglês *minimum mean square error*).

O detector ZF tenta eliminar qualquer interferência que um sinal transmitido possa ter em outro sinal transmitido. Isso corresponde a retirar a influência do canal, através da inversão da matriz de canal [3, 5, 7]. Note que, por causa dessa inversão de matriz, o ruído pode ser potencialmente aumentado, causando uma FER maior e/ou uma taxa de transmissão menor.

Em contraste, o detector MMSE não tenta eliminar a interferência de outros sinais, e sim minimizar o efeito conjunto da interferência e do ruído [3, 5, 6, 7]. Sabe-se que para alta SNR, o detector MMSE e ZF são equivalentes [5].

Recentemente, foi apresentado outro método de detecção linear conhecido como forçagem a inteiros (IF, do inglês *integer-forcing*) [7]. O método IF generaliza os métodos ZF e MMSE. A abordagem IF vem do processamento computa-e-encaminha [8, 9] em redes com *relays*, em que os receptores tentam extrair uma combinação linear dos sinais recebidos antes de recuperar as mensagens enviadas. Isso só é possível se os sinais transmitidos pertencerem a um código sobre reticulados [7, 10]. Mesmo que sua complexidade seja semelhante aos métodos ZF e MMSE, o desempenho do método IF se aproxima do ML principalmente em canais com desvanecimento de Rayleigh [7].

Os principais resultados sobre IF consideram um canal com desva-

hecimento estático, em que todos os símbolos de uma palavra-código estão sujeitos ao mesmo desvanecimento de canal. Note que, em situações práticas, em que códigos poderosos com comprimento de palavra-código longo são utilizados, pode não ser realista assumir que todos os símbolos possuem o mesmo desvanecimento. Portanto, canais com desvanecimento de bloco (BF, do inglês *block fading*) [11], em que o desvanecimento de canal pode mudar durante a transmissão de uma palavra-código, parecem ser um modelo mais realista.

Em particular, um sistema com tecnologia OFDM (*orthogonal frequency division multiplexing* [6]) pode ser aproximadamente modelado como um canal BF. Para isso, deve-se considerar que a palavra-código é dividida e transmitida por diversas subportadoras, cada uma sujeita a um desvanecimento diferente. Em [12] foi proposta uma abordagem na qual cada palavra-código é transmitida por um subconjunto das possíveis subportadoras (ao invés de uma palavra-código para todas as subportadoras). Entretanto, os resultados obtidos por [12] não conseguiram explorar toda a diversidade oferecida pelo canal.

Em um trabalho recente, El Bakoury e Nazer [13] generalizaram a abordagem IF para canais com desvanecimento de bloco. Eles descreveram dois métodos de decodificação para esse cenário, que são chamados de decodificação via média aritmética (AM, do inglês *arithmetic mean*) e via média geométrica (GM, do inglês *geometric mean*). O método de decodificação AM tenta aproximar o canal com desvanecimento de bloco em um canal com desvanecimento estático. Por outro lado, o método de decodificação GM explora a diversidade do canal e tenta extrair o máximo de informação de cada bloco.

Ambos os métodos podem atingir taxas maiores otimizando a escolha dos coeficientes da combinação linear, com o método GM sempre obtendo taxas maiores que o método AM para a mesma escolha de coeficientes [13]. Entretanto, encontrar a melhor escolha de coeficientes para as combinações lineares do método GM é complexo, já que nenhum algoritmo eficiente é conhecido. Em [13], por exemplo, os coeficientes para as combinações lineares foram escolhidos através de busca exaustiva.

1.1 Objetivos

Essa dissertação tem como objetivo principal propor um método sub-ótimo para escolher os coeficientes para as combinações lineares no método GM. A complexidade do método proposto é comparável com a complexidade para encontrar os coeficientes ótimos do método AM. E, embora o método proposto não consiga atingir as mesmas taxas do método GM utilizando a escolha ótima, ele apresenta um melhor desempenho do que outros métodos com complexidade semelhante.

Os resultados apresentados na literatura consideram códigos de comprimento infinito e modulações com cardinalidade suficientemente grande. Entretanto, cenários mais realistas utilizam códigos com comprimento finito e modulações usuais (como exemplo, PAM ou BPSK). Assim, outro objetivo dessa dissertação foi validar os resultados nesses cenários mais realistas. Para isso, além de considerar modulação PAM, foi necessário utilizar códigos otimizados para canais com desvanecimento de blocos, como os códigos *root-LDPC* [14].

1.1.1 Publicações

Os resultados dessa dissertação também foram apresentados na seguinte publicação:

- R. B. Venturelli e D. Silva, “Low-Complexity Integer Forcing for Block Fading MIMO Multiple-Access Channels”, no XXXIV Simpósio Brasileiro de Telecomunicações e Processamento de Sinais (SBrT’2016), Santarém (PA), Brasil.

1.2 Organização

Essa dissertação é organizada da seguinte maneira. No Capítulo 2 será descrito matematicamente o modelo de canal considerado. Além disso, nesse capítulo serão discutidos os métodos de decodificação conhecidos na literatura tanto para o canal com desvanecimento estático quanto para o canal com desvanecimento de bloco.

Já no Capítulo 3 encontram-se as técnicas propostas nessa dissertação. Primeiramente, são propostos dois novos métodos para escolha de coeficientes das combinações lineares no método GM. Em seguida,

é descrito como é possível utilizar códigos tradicionais, como o LDPC, nesse canal. Em particular, é mostrado como a LLR pode ser calculada.

O Capítulo 4 mostra os resultados obtidos através de simulações. Na primeira parte consideram-se códigos com comprimento infinito e mostram-se as taxas alcançáveis pelos métodos de interesse, já na segunda parte, códigos de comprimento finito são considerados e são mostrados resultados para FER.

Por fim, o Capítulo 5 apresenta algumas conclusões e sugestões para trabalhos futuros.

1.3 Notação

Nessa dissertação, matrizes são denotadas por letras maiúsculas em negrito, e.g. \mathbf{X} . Sejam \mathbf{X}^T e \mathbf{X}^{-1} as matrizes transposta e inversa de \mathbf{X} , respectivamente. A matriz identidade é denotada por \mathbf{I} e suas dimensões são deduzidas pelo contexto. Vetores são denotados por letras minúsculas em negrito, e.g. \mathbf{x} . Assume-se sempre que são vetores-linha e \mathbf{x}^T indica um vetor-coluna. A norma Euclidiana de \mathbf{x} é denotada por $\|\mathbf{x}\|$.

A probabilidade de um evento A qualquer ocorrer é denotada por $\mathbb{P}(A)$ e o valor esperado de uma variável aleatória é denotado por $\mathbb{E}[\cdot]$. O conjunto dos números reais é denotado por \mathbb{R} e o conjunto dos números inteiros é denotado por \mathbb{Z} , além disso \mathbb{Z}_p denota o anel de inteiros módulo p . O conjunto de vetores n -dimensionais com coeficientes reais é denotado por \mathbb{R}^n e o conjunto de matrizes $n \times m$ com coeficientes reais é denotado por $\mathbb{R}^{n \times m}$. Analogamente denota-se o conjunto de vetores e matrizes sobre \mathbb{Z} e \mathbb{Z}_p .

Capítulo 2

Forçagem a Inteiros em Canais com Desvanecimento de Blocos

Neste capítulo, primeiramente será descrito matematicamente o modelo do canal considerado. Além disso, será especificado o objetivo do receptor. Em seguida, serão descritos os métodos de decodificação existentes na literatura, assim como suas taxas alcançáveis tanto para canais com desvanecimento estático como principalmente para canais com desvanecimento de bloco.

2.1 Modelo do Canal

Considere o cenário em que N_T usuários com uma antena cada desejam enviar sua informação através de um canal MIMO de múltiplo acesso com desvanecimento de bloco para um receptor com N_R antenas.

O ℓ -ésimo usuário gera sua mensagem $\mathbf{w}_\ell \in \mathbb{Z}_p^k$ em que p é um número inteiro. Todos os usuários possuem o mesmo codificador $\mu : \mathbb{Z}_p^k \rightarrow \mathbb{R}^n$ tal que $\mu(\mathbf{w}_\ell) = \mathbf{x}_\ell$.

Iremos assumir que cada transmissor enviará sua mensagem com a mesma potência P , e portanto

$$\frac{1}{n} \|\mathbf{x}_\ell\|^2 \leq P.$$

A taxa de cada usuário é definida como

$$R_{\text{mes}} \triangleq \frac{k}{n} \log_2 p.$$

O vetor transmitido é dividido em N blocos de igual comprimento tal que $\mathbf{x}_\ell = \begin{bmatrix} \mathbf{x}_{\ell,(1)} & \mathbf{x}_{\ell,(2)} & \cdots & \mathbf{x}_{\ell,(N)} \end{bmatrix}$, em que $\mathbf{x}_{\ell,(i)} \in \mathbb{R}^{n/N}$ (por simplicidade iremos assumir que n/N resulta em um número inteiro positivo). Seja $\mathbf{X} \in \mathbb{R}^{N_T \times n}$ a matriz em que a ℓ -ésima linha corresponde ao vetor enviado pelo ℓ -ésimo usuário. Note que \mathbf{X} também pode ser dividida em N blocos, tal que $\mathbf{X} = \begin{bmatrix} \mathbf{X}_{(1)} & \cdots & \mathbf{X}_{(N)} \end{bmatrix}$, em que

$$\mathbf{X}_{(i)} = \begin{bmatrix} \mathbf{x}_{1,(i)} \\ \vdots \\ \mathbf{x}_{N_T,(i)} \end{bmatrix}$$

será a matriz de entrada do i -ésimo sub-canal, $i = 1, \dots, N$.

O canal é formado por N sub-canais independentes. No i -ésimo sub-canal, a matriz transmitida será multiplicada pela matriz de coeficientes do canal¹ $\mathbf{H}_{(i)} \in \mathbb{R}^{N_R \times N_T}$ e então somada com a matriz de ruído $\mathbf{Z}_{(i)} \in \mathbb{R}^{N_R \times n/N}$ tal que as entradas de $\mathbf{Z} \in \mathbb{R}^{N_T \times n}$ seguem uma distribuição gaussiana de média nula e variância σ^2 . Assume-se que os transmissores não tenham conhecimento dos valores de $\mathbf{H}_{(i)}$ porém conhecem suas estatísticas. A matriz recebida no receptor pode ser descrita matematicamente como $\mathbf{Y} = \begin{bmatrix} \mathbf{Y}_{(1)} & \cdots & \mathbf{Y}_{(N)} \end{bmatrix}$, em que

$$\mathbf{Y}_{(i)} = \mathbf{H}_{(i)} \mathbf{X}_{(i)} + \mathbf{Z}_{(i)} \quad (2.1)$$

e a j -ésima linha de $\mathbf{Y}_{(i)}$ é o sinal pela j -ésima antena no i -ésimo bloco recebido, $j = 1, 2, \dots, N_R$, $i = 1, 2, \dots, N$.

¹Foi escolhido utilizar um canal em que os coeficientes pertencem aos reais, não apenas por simplicidade, como também para facilitar a comparação com os resultados obtidos na literatura. A extensão para um canal com coeficientes complexos é imediata, além disso, como mostrado em [7] é possível decompor um canal complexo em um canal real com o dobro de antenas tanto nos transmissores quanto no receptor.

Por conveniência define-se a SNR como sendo

$$\text{SNR} \triangleq \frac{P}{\sigma^2}. \quad (2.2)$$

O desafio do receptor é, a partir de \mathbf{Y} e conhecendo os valores de $\mathbf{H}_{(1:N)} = \{\mathbf{H}_{(1)}, \dots, \mathbf{H}_{(N)}\}$ (isto é, CSIR), recuperar todas as mensagens $\mathbf{w}_1, \dots, \mathbf{w}_{N_T}$ através de um decodificador $\mathcal{D} : \mathbb{R}^{N_R \times n} \rightarrow \mathbb{Z}_p^k \times \dots \times \mathbb{Z}_p^k$ tal que $\mathcal{D}(\mathbf{Y}) = (\hat{\mathbf{w}}_1, \dots, \hat{\mathbf{w}}_{N_T})$. Define-se a probabilidade de erro como sendo a probabilidade do receptor não conseguir recuperar alguma das mensagens corretamente, isto é, $\mathbb{P}_{\text{erro}} \triangleq \mathbb{P}((\mathbf{w}_1, \dots, \mathbf{w}_{N_T}) \neq (\hat{\mathbf{w}}_1, \dots, \hat{\mathbf{w}}_{N_T}))$.

Uma taxa R é dita alcançável se dado um $\epsilon > 0$ e $n \rightarrow \infty$ existir algum esquema de codificação e decodificação tal que $\mathbb{P}_{\text{erro}} \leq \epsilon$.

2.2 Detector ML

Detectores ML alcançam melhores desempenho dentre todos os métodos. O detector atua procurando o conjunto de mensagens $(\hat{\mathbf{w}}_1, \dots, \hat{\mathbf{w}}_{N_T})$ mais prováveis [7]. Seja $\mathcal{S} \subseteq \{1, \dots, N_T\}$ um subconjunto e seja $\mathbf{H}_{\mathcal{S},(i)}$ a submatriz de $\mathbf{H}_{(i)}$ cujas colunas são indexadas por \mathcal{S} . A taxa alcançável do decodificador ML é dada por [7, 13]

$$R_{\text{ML}}(\mathbf{H}_{(1:N)}) = \min_{\mathcal{S} \subseteq \{1, \dots, N_T\}} \frac{1}{2N|\mathcal{S}|} \sum_{i=1}^N \log \det \left(\mathbf{I} + \text{SNR} \mathbf{H}_{\mathcal{S},(i)} \mathbf{H}_{\mathcal{S},(i)}^T \right) \quad (2.3)$$

Note que esse valor corresponde à capacidade simétrica do canal de múltiplo acesso [1].

A complexidade desse método cresce exponencialmente com o tamanho do bloco n e com o número de usuários N_T , o que não o torna atrativo em muitas aplicações [7].

2.3 Decodificação Linear Tradicional

Decodificação linear é geralmente utilizada para reduzir a complexidade do sistema. Nesse caso, tenta-se transformar um canal MIMO em vários canais SISO através de uma equalização (transformação linear) do canal [3, 5]. Cada canal SISO é então processado, geralmente em paralelo, de

maneira independente, para recuperar a mensagem de cada usuário.

Após a equalização, um canal efetivo é criado. Esse canal efetivo corresponde à palavra-código transmitida por cada usuário somada com um ruído efetivo. Seja $\mathbf{B}_{(i)} \in \mathbb{R}^{N_T \times N_R}$ a matriz de equalização no i -ésimo bloco. Então o canal efetivo é descrito como

$$\mathbf{Y}_{\text{eff}} = \mathbf{X} + \mathbf{Z}_{\text{eff}} = \begin{bmatrix} \mathbf{Y}_{\text{eff},(1)} & \cdots & \mathbf{Y}_{\text{eff},(N)} \end{bmatrix}$$

em que

$$\mathbf{Y}_{\text{eff},(i)} = \mathbf{B}_{(i)} \mathbf{Y}_{(i)} = \mathbf{B}_{(i)} \mathbf{H}_{(i)} \mathbf{X}_{(i)} + \mathbf{B}_{(i)} \mathbf{Z}_{(i)} \quad (2.4)$$

$$= \mathbf{X}_{(i)} + \mathbf{Z}_{\text{eff},(i)}, \quad (2.5)$$

$$\mathbf{Z}_{\text{eff}} = \begin{bmatrix} \mathbf{Z}_{\text{eff},(1)} & \cdots & \mathbf{Z}_{\text{eff},(N)} \end{bmatrix},$$

$$\mathbf{Z}_{\text{eff},(i)} = (\mathbf{B}_{(i)} \mathbf{H}_{(i)} - \mathbf{I}) \mathbf{X}_{(i)} + \mathbf{B}_{(i)} \mathbf{Z}_{(i)}$$

e $i = 1, \dots, N$,

Tradicionalmente, dois métodos de decodificação linear são amplamente explorados. O primeiro método é conhecido como *forçagem a zero* (ZF, do inglês *zero-forcing*), e o segundo método é conhecido como *mínimo erro quadrático médio* (MMSE, do inglês *minimum mean square error*).

Embora, na literatura, seja comum encontrar esses métodos explicados para um canal com desvanecimento estático, isto é, $N = 1$, a extensão para desvanecimento de bloco é imediata, uma vez que é possível equalizar cada bloco individualmente.

2.3.1 Método ZF

O método ZF tenta transformar o canal MIMO em vários canais SISO invertendo a matriz do canal [3, 6]. Isto é, a matriz de equalização é escolhida como

$$\mathbf{B}_{(i)} = (\mathbf{H}_{(i)}^T \mathbf{H}_{(i)})^{-1} \mathbf{H}_{(i)}^T.$$

Neste caso, o ruído efetivo pode ser escrito como $\mathbf{Z}_{\text{eff},(i)} = \mathbf{B}_{(i)} \mathbf{Z}_{(i)}$. Note que nesse método, a interferência de outra palavra código é completamente eliminada, isso é, a m -ésima linha de \mathbf{Y}_{eff} , $\mathbf{y}_{\text{eff},m}$ depende apenas de \mathbf{x}_m .

Esse método, apesar de ser simples, pode potencialmente amplificar o ruído efetivo [6].

2.3.2 Método MMSE

Essa outra abordagem, ao invés de simplesmente eliminar a interferência, tenta minimizar o erro (quadrático médio) entre o sinal enviado e o estimado [3, 6].

A matriz de equalização é dada por²

$$\mathbf{B}_{(i)} = (\mathbf{H}_{(i)}^T \mathbf{H}_{(i)} + \text{SNR}^{-1} \mathbf{I})^{-1} \mathbf{H}_{(i)}^T.$$

Note que conforme a SNR cresce, o método MMSE se aproxima do método ZF.

Sabe-se que, principalmente para baixa SNR, com o método MMSE é possível atingir taxas maiores do que com o método ZF. Por esse motivo, de agora em diante, não serão mais considerados os resultados com o método ZF, apenas o método MMSE será usado como comparação.

2.4 Forçagem a Inteiros em Canais com Desvanecimento Estático

Forçagem a inteiros (IF, do inglês *integer-forcing*) surge como alternativo aos tradicionais métodos de decodificação linear [7]. A abordagem IF vem do método computa-e-encaminha [8, 15] para codificação de rede na camada física. Ao invés de tentar recuperar cada mensagem isoladamente, o método IF tenta recuperar combinações lineares com coeficientes inteiros das palavras-código transmitidas. Note que para isso é necessário que essas combinações sejam palavras-códigos. Essa é uma característica encontrada em códigos construídos sobre reticulados [10]. Uma maneira simples de construir um código sobre reticulados é utilizar a construção A [16], em que são utilizados um código linear p -ário e uma modulação p -PAM (ou p^2 -QAM se for considerado um canal com coeficientes complexos), em que p é um número primo suficientemente grande [10]. Maiores detalhes sobre reticulados podem ser

²Em alguns textos da literatura é comum encontrar a expressão da matriz de equalização como $\mathbf{B} = \mathbf{H}^T (\mathbf{H} \mathbf{H}^T + \text{SNR}^{-1} \mathbf{I})^{-1}$. Como mostrado em [3] ambas as expressões são equivalentes.

encontrados em [17] ou no Apêndice A.

Após a equalização, um canal efetivo é criado. Esse canal efetivo é dado por combinações lineares das mensagens adicionadas de um ruído efetivo. Seja $\mathbf{B} \in \mathbb{R}^{N_T \times N_R}$ a matriz de equalização. A equação do canal efetivo é dada por

$$\mathbf{Y}_{\text{eff}} = \mathbf{B}\mathbf{Y} = \mathbf{B}\mathbf{H}\mathbf{X} + \mathbf{B}\mathbf{Z} \quad (2.6)$$

$$= \mathbf{V} + \mathbf{Z}_{\text{eff}} \quad (2.7)$$

em que $\mathbf{V} = \mathbf{A}\mathbf{X}$, $\mathbf{A} \in \mathbb{Z}^{N_T \times N_T}$, tal que $\text{posto}(\mathbf{A}) = N_T$ e

$$\mathbf{Z}_{\text{eff}} = (\mathbf{B}\mathbf{H} - \mathbf{A})\mathbf{X} + \mathbf{B}\mathbf{Z}. \quad (2.8)$$

Note que devido as propriedades de códigos sobre reticulados, $\mathbf{v}_m = \mathbf{a}_m\mathbf{X}$ é uma palavra-código, em que \mathbf{v}_m e \mathbf{a}_m são a m -ésima linha de \mathbf{V} e \mathbf{A} respectivamente.

Além disso, se o receptor conseguir inferir a matriz \mathbf{V} corretamente, ele pode recuperar a matriz \mathbf{X} facilmente através de $\mathbf{X} = \mathbf{A}^{-1}\mathbf{V}$.

O método IF generaliza os métodos tradicionais de decodificação [7]. Por exemplo, se $\mathbf{B} = (\mathbf{H}^T\mathbf{H})^{-1}\mathbf{H}^T$ e $\mathbf{A} = \mathbf{I}$, então temos o método ZF. E se $\mathbf{B} = (\mathbf{H}^T\mathbf{H} + \text{SNR}^{-1}\mathbf{I})^{-1}\mathbf{H}^T$ e $\mathbf{A} = \mathbf{I}$ então temos o método MMSE.

É intuitivo que minimizar a potência do ruído efetivo irá maximizar as taxas alcançáveis (esse fato será discutido mais adiante). A m -ésima linha de \mathbf{Z}_{eff} pode ser escrita como sendo $\mathbf{z}_{\text{eff},m} = (\mathbf{b}_m\mathbf{H} - \mathbf{a}_m)\mathbf{X} + \mathbf{b}_m\mathbf{Z}$, em que \mathbf{b}_m e \mathbf{a}_m correspondem a m -ésima linha de \mathbf{B} e \mathbf{A} respectivamente. Note que o receptor tem conhecimento de \mathbf{H} , \mathbf{b}_m e \mathbf{a}_m , assim, é possível encontrar facilmente $\sigma_{\text{eff},m}^2 = \frac{1}{n}\mathbb{E}[\mathbf{z}_{\text{eff},m}\mathbf{z}_{\text{eff},m}^T]$ como sendo

$$\sigma_{\text{eff},m}^2 = \sigma^2 \left(\|\mathbf{b}_m\mathbf{H} - \mathbf{a}_m\|^2 \text{SNR} + \|\mathbf{b}_m\|^2 \right). \quad (2.9)$$

A escolha de \mathbf{b}_m que minimiza $\sigma_{\text{eff},m}^2$ é feita através da estimação MMSE e é dada por [7]

$$\mathbf{b}_{\text{opt},m} = \mathbf{a}_m(\mathbf{H}^T\mathbf{H} + \text{SNR}^{-1}\mathbf{I})^{-1}\mathbf{H}^T$$

e portanto podemos escrever a matriz \mathbf{B}_{opt} como sendo

$$\mathbf{B}_{\text{opt}} = \mathbf{A} (\mathbf{H}^T \mathbf{H} + \text{SNR}^{-1} \mathbf{I})^{-1} \mathbf{H}^T. \quad (2.10)$$

Além disso, quando escolhe-se $\mathbf{B} = \mathbf{B}_{\text{opt}}$, a variância da m -ésima linha de \mathbf{Z}_{eff} pode ser escrita como [15]

$$\sigma_{\text{eff},m}^2 = \sigma^2 (\mathbf{a}_m \mathbf{M} \mathbf{a}_m^T) \quad (2.11)$$

em que

$$\mathbf{M} = (\mathbf{H}^T \mathbf{H} + \text{SNR}^{-1} \mathbf{I})^{-1}. \quad (2.12)$$

A taxa alcançável por um decodificador linear é dada por [7]

$$R_{\text{IF}}(\mathbf{H}, \mathbf{A}, \mathbf{B}) = \min_m \frac{1}{2} \log^+ \left(\frac{P}{\sigma_{\text{eff},m}^2} \right) \quad (2.13)$$

em que $\log^+(x) = \max(\log(x), 0)$. Assim, para maximizar a taxa alcançável é necessário ou aumentar a potência de transmissão ou tentar reduzir a variância do ruído efetivo.

Como sempre iremos considerar que $\mathbf{B} = \mathbf{B}_{\text{opt}}$, é comum omitir esse termo do argumento, desse modo, pode-se escrever

$$\begin{aligned} R_{\text{IF}}(\mathbf{H}, \mathbf{A}) &= R_{\text{IF}}(\mathbf{H}, \mathbf{A}, \mathbf{B}_{\text{opt}}) \\ &= \min_m \frac{1}{2} \log^+ \left(\frac{\text{SNR}}{\mathbf{a}_m \mathbf{M} \mathbf{a}_m^T} \right). \end{aligned} \quad (2.14)$$

Teorema 2.1. [7, 8] *Para qualquer $\epsilon > 0$ e para n e p suficientemente grandes, existe um esquema de codificação e decodificação tal que é possível recuperar m combinações lineares de coeficientes inteiros a partir de \mathbf{Y} com $\mathbb{P}_{\text{erro}} \leq \epsilon$, para qualquer escolha de \mathbf{A} que satisfaça*

$$R_{\text{mes}} < R_{\text{IF}}(\mathbf{H}, \mathbf{A}). \quad (2.15)$$

Embora este teorema seja válido para recuperar qualquer número de combinações lineares dos vetores transmitidos, estamos interessados em recuperar N_T combinações lineares.

2.4.1 Escolha da matriz \mathbf{A}

Embora o teorema seja válido para qualquer escolha de \mathbf{A} , queremos escolher a matriz \mathbf{A} de forma a maximizar $R_{\text{IF}}(\mathbf{H}, \mathbf{A})$.

Note que, se for especificado que $\mathbf{A} = \mathbf{I}$, então o decodificador está utilizando decodificação com estimador MMSE [7]. A taxa alcançável desse método é dada por:

$$R_{\text{MMSE}}(\mathbf{H}) = R_{\text{IF}}(\mathbf{H}, \mathbf{I}). \quad (2.16)$$

Todavia, escolher $\mathbf{A} = \mathbf{I}$ limita as possíveis combinações lineares que podem ser feitas. Aproveitando-se do fato que as palavras-código pertencem a um código sobre reticulado e, portanto, combinações inteiras de palavras-códigos formam outras palavras-código, podemos escolher \mathbf{A} como qualquer matriz com coeficientes inteiros de posto completo [7]. Novamente, para tentar maximizar a taxa alcançável iremos tentar reduzir a variância do ruído efetivo. Mais precisamente, iremos tentar reduzir o maior $\sigma_{\text{eff},m}^2$, $m = 1, \dots, N_T$.

Seja

$$\mathbf{A} = \begin{bmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_{N_T} \end{bmatrix},$$

em que $\mathbf{a}_1, \dots, \mathbf{a}_{N_T} \in \mathbb{Z}^{N_T}$ são linearmente independentes em \mathbb{Z}_p . Pode-se descrever esse problema como

$$\begin{aligned} \mathbf{A}_{\text{opt}} = \begin{bmatrix} \mathbf{a}_{\text{opt},1} \\ \vdots \\ \mathbf{a}_{\text{opt},N_T} \end{bmatrix} &= \arg \min_{\substack{\mathbf{a}_1, \dots, \mathbf{a}_{N_T} \\ \mathbf{a}_1, \dots, \mathbf{a}_{N_T} \sim \text{L.I.}}} \max_{m=1, \dots, N_T} \sigma_{\text{eff},m}^2 \\ &= \arg \min_{\substack{\mathbf{a}_1, \dots, \mathbf{a}_{N_T} \\ \mathbf{a}_1, \dots, \mathbf{a}_{N_T} \sim \text{L.I.}}} \max_{m=1, \dots, N_T} \mathbf{a}_m \mathbf{M} \mathbf{a}_m^T \end{aligned} \quad (2.17)$$

em que \mathbf{M} é definido em (2.12).

Encontrar um único vetor \mathbf{a}_m que minimize $\sigma_{\text{eff},m}^2$ equivale em encontrar o vetor de menor norma do reticulado gerado pela matriz $\mathbf{M}^T \mathbf{M}$, isto é, pela matriz Gram de \mathbf{M} . Esse problema é conhecido na literatura como *problema de vetor de mínima norma* (SVP, do inglês

shortest vector problem) [17, 18].

Note que é necessário encontrar N_T vetores linearmente independentes de mínima norma a partir do reticulado gerado pela matriz Gram de \mathbf{M} . Esse problema é conhecido na literatura como *problema de vetores linearmente independente de mínima norma* (SIVP, do inglês *shortest linearly independent vectors problem*) [19]. Sabe-se que SIVP é um problema NP-hard [19]. Resolver SIVP corresponde em encontrar os *mínimos sucessivos* do reticulado definido pela matriz de Gram \mathbf{M} [17, 19].

Embora os mínimos sucessivos de um reticulado não necessariamente forme uma base [17, 19], na prática, é comum tentar encontrar a base do reticulado como solução do SIVP [15]. Esse problema também é conhecido como redução de base de reticulado ou simplesmente redução de reticulado.

A literatura apresenta alguns algoritmos de redução de base de reticulados, como por exemplo, o algoritmo de Langrange-Gauss [17], que é usado quando $N_T = 2$. Esse algoritmo é ótimo pois, além de encontrar uma base para o reticulado, os vetores encontrados correspondem aos mínimos sucessivos [17].

Outro algoritmo de redução de reticulado utilizado na prática é o Lenstra-Lenstra-Lovász (LLL) [20]. O algoritmo LLL corresponde a uma generalização do algoritmo de Langrange-Gauss para reticulados de ordem maior [17]. Note que o algoritmo LLL não encontra os mínimos sucessivos e sim uma base para o reticulado. Apesar disso, o LLL é um algoritmo eficiente, uma vez que ele pode ser realizado em tempo polinomial [18].

Como abuso de notação, independente se for utilizado o algoritmo de Langrange-Gauss ou LLL, iremos chamar a solução do algoritmo de \mathbf{A}_{opt} . Desse modo, podemos escrever a taxa alcançável como

$$R_{\text{IF}}(\mathbf{H}) = R_{\text{IF}}(\mathbf{H}, \mathbf{A}_{\text{opt}}). \quad (2.18)$$

2.5 Extensão para Desvanecimento de Blocos

De forma similar ao caso com desvanecimento estático, decodificadores lineares são utilizados para reduzir a complexidade de processamento com um desempenho aceitável.

Como se assume que o receptor conhece todos os desvanecimentos, é possível equalizar, multiplicando pela matriz $\mathbf{B}_{(i)}$, cada bloco de maneira distinta [13], assim criando N canais efetivos

$$\begin{aligned}\mathbf{Y}_{\text{eff},(i)} &= \mathbf{B}_{(i)} \mathbf{Y}_{(i)} = \mathbf{B}_{(i)} \mathbf{H}_{(i)} \mathbf{X}_{(i)} + \mathbf{B}_{(i)} \mathbf{Z}_{(i)} \\ &= \mathbf{V}_{(i)} + \mathbf{Z}_{\text{eff},(i)}\end{aligned}\quad (2.19)$$

em que $\mathbf{V}_{(i)} = \mathbf{A} \mathbf{X}_{(i)}$ e

$$\mathbf{Z}_{\text{eff},(i)} = (\mathbf{B}_{(i)} \mathbf{H}_{(i)} - \mathbf{A}) \mathbf{X}_{(i)} + \mathbf{B}_{(i)} \mathbf{Z}_{(i)}.\quad (2.20)$$

É importante ressaltar que a matriz \mathbf{A} deve permanecer a mesma para todos os blocos [13]. Isso é necessário para preservar as propriedades de códigos sobre reticulados. Note que é necessário que \mathbf{v}_m seja uma palavra-código para que a decodificação seja possível, em que \mathbf{v}_m é a m -ésima linha de $\mathbf{V} = \mathbf{A} \mathbf{X} = \begin{bmatrix} \mathbf{V}_{(1)} & \cdots & \mathbf{V}_{(N)} \end{bmatrix}$. Sem essa restrição, não é possível garantir que \mathbf{v}_m seja uma palavra-código, mesmo que códigos sobre reticulados sejam considerados.

Semelhante ao caso com desvanecimento estático, a variância da m -ésima linha de $\mathbf{Z}_{\text{eff},(i)}$ pode ser facilmente calculada. Note que o desvanecimento muda em cada bloco e portanto, cada um possui uma variância diferente. A variância da m -ésima linha de $\mathbf{Z}_{\text{eff},(i)}$ é dada por

$$\sigma_{\text{eff},m,(i)}^2 = \sigma^2 \left(\|\mathbf{b}_{m,(i)} \mathbf{H}_{(i)} - \mathbf{a}_m\|^2 \text{SNR} + \|\mathbf{b}_{m,(i)}\|^2 \right).\quad (2.21)$$

Visando minimizar $\sigma_{\text{eff},m,(i)}^2$ é simples encontrar o valor de $\mathbf{b}_{\text{opt},m,(i)}$, que é dado por

$$\mathbf{b}_{\text{opt},m,(i)} = \mathbf{a}_m \left(\mathbf{H}_{(i)}^T \mathbf{H}_{(i)} + \text{SNR}^{-1} \mathbf{I} \right)^{-1} \mathbf{H}_{(i)}^T$$

e portanto, pode-se escrever $\mathbf{B}_{\text{opt},(i)}$ como

$$\mathbf{B}_{\text{opt},(i)} = \mathbf{A} \left(\mathbf{H}_{(i)}^T \mathbf{H}_{(i)} + \text{SNR}^{-1} \mathbf{I} \right)^{-1} \mathbf{H}_{(i)}^T.\quad (2.22)$$

Novamente, iremos considerar sempre que $\mathbf{B}_{(i)} = \mathbf{B}_{\text{opt},(i)}$. Assim, a variância da m -ésima linha de $\mathbf{Z}_{\text{eff},(i)}$ pode ser escrita como

$$\sigma_{\text{eff},m,(i)}^2 = \sigma^2 \left(\mathbf{a}_m \mathbf{M}_{(i)} \mathbf{a}_m^T \right)\quad (2.23)$$

em que

$$\mathbf{M}_{(i)} = \left(\text{SNR}^{-1} \mathbf{I} + \mathbf{H}_{(i)}^T \mathbf{H}_{(i)} \right)^{-1}. \quad (2.24)$$

Em canais com desvanecimento de blocos conhece-se dois tipos de decodificadores lineares, cada um com uma taxa alcançável diferente [13]. O primeiro tipo tenta aproximar o canal com desvanecimento de blocos em um canal com desvanecimento estático. Isso é feito através da *média aritmética* das variâncias do ruído efetivo, portanto, chamamos esse método de decodificador via média aritmética (AM, do inglês *arithmetic mean*). Já o segundo tipo, explora a diversidade do canal com desvanecimento de bloco e tenta extrair o máximo de informação (bits) de cada bloco. Como será mostrado, isso equivale a fazer *média geométrica* da variância do ruído efetivo e, portanto, chamamos esse método de decodificador via média geométrica (GM, do inglês *geometric mean*). Ambos os tipos serão melhores detalhados, assim como suas respectivas taxas alcançáveis, nas seções seguintes.

2.5.1 Decodificador via Média Aritmética

Decodificadores AM tentam aproximar o canal ao caso com desvanecimento estático, isto é, consideram que o ruído efetivo está sujeito apenas um valor de variância [13]. O valor de variância considerado na m -ésima equação de decodificação é a média aritmética das variâncias de cada bloco. Seja

$$\sigma_{\text{AM},m}^2 = \frac{1}{N} \sum_{i=1}^N \sigma_{\text{eff},m,(i)}^2 \quad (2.25)$$

então, para uma matriz \mathbf{A} , a taxa alcançável do decodificador AM é dada por [13]

$$\begin{aligned} R_{\text{AM}}(\mathbf{H}_{(1:N)}, \mathbf{A}) &= \min_m \frac{1}{2} \log^+ \left(\frac{P}{\sigma_{\text{AM},m}^2} \right) \\ &= \min_m \frac{1}{2} \log^+ \left(\frac{\text{SNR}}{\mathbf{a}_m \mathbf{M}_{\text{AM}} \mathbf{a}_m^T} \right) \end{aligned} \quad (2.26)$$

em que

$$\mathbf{M}_{\text{AM}} = \frac{1}{N} \sum_{i=1}^N \mathbf{M}_{(i)}. \quad (2.27)$$

2.5.2 Decodificador via Média Geométrica

O decodificador via média geométrica (GM) por sua vez, tenta extrair o máximo de informação mútua de cada bloco [13]. Isso equivale a dizer que cada bloco irá considerar sua própria variância do ruído efetivo.

A taxa alcançável por esse método é dada por

$$\begin{aligned} R_{\text{GM}}(\mathbf{H}_{(1:N)}, \mathbf{A}) &= \min_m \frac{1}{2N} \sum_{i=1}^N \log^+ \left(\frac{P}{\sigma_{\text{eff},m,(i)}^2} \right) \\ &= \min_m \frac{1}{2N} \sum_{i=1}^N \log^+ \left(\frac{\text{SNR}}{\mathbf{a}_m \mathbf{M}_{(i)} \mathbf{a}_m^T} \right) \end{aligned} \quad (2.28)$$

$$= \min_m \frac{1}{2} \log^+ \left(\frac{P}{\sigma_{\text{GM},m}^2} \right) \quad (2.29)$$

em que

$$\sigma_{\text{GM},m}^2 = \left(\prod_{i=1}^N \sigma_{\text{eff},m,(i)}^2 \right)^{1/N} \quad (2.30)$$

é a média geométrica dos ruídos efetivos.

Note que devido a desigualdade entre média geométrica e média aritmética [21], tem-se que, para a mesma matriz \mathbf{A} , $\sigma_{\text{GM},m}^2 \leq \sigma_{\text{AM},m}^2$ e portanto o método de decodificação GM alcança taxas maiores que o método AM [13].

2.5.3 Escolha da matriz \mathbf{A}

Semelhante ao caso estático, em ambos os métodos é possível escolher $\mathbf{A} = \mathbf{I}$ [13]. Se o método AM é utilizado então chamaremos de AM-MMSE e caso o método GM seja utilizado então será chamado de GM-MMSE. As taxas alcançáveis pelos métodos AM-MMSE e GM-MMSE são dadas por

$$R_{\text{AM-MMSE}}(\mathbf{H}_{(1:N)}) = R_{\text{AM}}(\mathbf{H}_{(1:N)}, \mathbf{I}) \quad (2.31)$$

$$R_{\text{GM-MMSE}}(\mathbf{H}_{(1:N)}) = R_{\text{GM}}(\mathbf{H}_{(1:N)}, \mathbf{I}) \quad (2.32)$$

respectivamente.

Todavia, sabe-se que escolher $\mathbf{A} = \mathbf{I}$ não é, necessariamente, a melhor opção, uma vez que os elementos da matriz \mathbf{A} podem assumir qualquer valor inteiro.

Como o método AM é uma aproximação do caso estático, pode-se utilizar as mesmas técnicas para encontrar a melhor matriz \mathbf{A} . Nesse caso, utiliza-se a matriz \mathbf{M}_{AM} como entrada do algoritmo de redução de reticulado [13]. Iremos chamar a melhor matriz obtida por este método como \mathbf{A}_{AM} (independentemente se for utilizado o algoritmo de Langrange-Gauss ou LLL para encontrá-la).

Quando matriz \mathbf{A}_{AM} é utilizada, referimos ao método como AM-IF. Sua taxa alcançável é dada por

$$R_{\text{AM-IF}}(\mathbf{H}_{(1:N)}) = R_{\text{AM}}(\mathbf{H}_{(1:N)}, \mathbf{A}_{\text{AM}}). \quad (2.33)$$

Já para encontrar a matriz ótima do método GM, chamada de \mathbf{A}_{GM} , o problema de otimização pode ser descrito como

$$\mathbf{A}_{\text{GM}} = \begin{bmatrix} \mathbf{a}_{\text{GM},1} \\ \vdots \\ \mathbf{a}_{\text{GM},N_T} \end{bmatrix} = \arg \min_{\substack{\mathbf{a}_1, \dots, \mathbf{a}_{N_T} \\ \mathbf{a}_1, \dots, \mathbf{a}_{N_T} \sim \text{L.I.}}} \max_m \left(\prod_{i=1}^N \mathbf{a}_m \mathbf{M}_{(i)} \mathbf{a}_m^T \right)^{1/N}. \quad (2.34)$$

Enquanto no método AM-IF é possível encontrar a matriz \mathbf{A} de forma sub-ótima (ou até mesmo ótima) em tempo polinomial, isso ainda não é possível para o decodificador GM [13]. Entretanto, é possível utilizar outros algoritmos não-eficientes, como por exemplo busca exaustiva para encontrar a \mathbf{A}_{GM} .

Nesse caso, chamamos este método de GM-IF, e sua taxa alcançável é dada por

$$R_{\text{GM-IF}}(\mathbf{H}_{(1:N)}) = R_{\text{GM}}(\mathbf{H}_{(1:N)}, \mathbf{A}_{\text{GM}}). \quad (2.35)$$

Capítulo 3

Técnicas Propostas

Neste capítulo, as propostas dessa dissertação serão discutidas. Primeiramente serão apresentados dois novos métodos sub-ótimos para escolha da matriz \mathbf{A} para o decodificador GM. Em seguida, será discutido como pode ser o processo de decodificação quando códigos práticos (de comprimento finito) são utilizados, em especial, códigos LDPC.

3.1 Escolha Sub-ótima de \mathbf{A} para Decodificador GM

O método GM-IF tem as maiores taxas alcançáveis dentre todos os métodos conhecidos (com exceção do decodificador ML) [13]. Todavia, como não se conhece nenhum algoritmo eficiente para encontrar \mathbf{A}_{GM} , esse método pode não ser atrativo em situações práticas.

As alternativas conhecidas até então são os métodos AM-IF e GM-MMSE. Note que o método AM-MMSE não é interessante, uma vez que as taxas alcançáveis por este método serão sempre inferiores a ambos os métodos AM-IF e GM-MMSE.

Ainda assim, escolher entre os métodos AM-IF e GM-MMSE não é trivial, uma vez que o desempenho de ambos varia com o número de blocos, número de usuários e com a SNR. Sendo que em alguns casos um método tem melhor desempenho do que o outro.

Como nova alternativa para a escolha da matriz \mathbf{A} para o decodificador GM sugerimos dois novos métodos sub-ótimos, detalhados a

seguir.

3.1.1 Método Proposto 1

No primeiro método proposto, o decodificador deve escolher entre a matriz identidade e a a matriz ótima do método AM, isto é, \mathbf{A}_{AM} . Seja $\mathcal{A}_1 = \{\mathbf{I}, \mathbf{A}_{AM}\}$ o conjunto de possíveis escolhas para matriz \mathbf{A} , a matriz que será escolhida pelo método proposto 1 será

$$\mathbf{A}_{\text{prop},1} = \arg \max_{\mathbf{A} \in \mathcal{A}_1} R_{GM}(\mathbf{H}_{(1:N)}, \mathbf{A}) \quad (3.1)$$

e, portanto, a taxa alcançável pelo método proposto 1 é dada por

$$R_{\text{prop},1}(\mathbf{H}_{(1:N)}) = R_{GM}(\mathbf{H}_{(1:N)}, \mathbf{A}_{\text{prop},1}). \quad (3.2)$$

Note que, se a matriz escolhida for \mathbf{A}_{AM} então o método proposto 1 tem um melhor desempenho do que o AM-IF uma vez que o decodificador GM tem taxas alcançáveis maiores que o decodificador AM. Por outro lado, se a matriz \mathbf{I} for escolhida então o desempenho é o mesmo que do GM-MMSE.

Em termos de complexidade, o método proposto apresenta a mesma complexidade que o método AM-IF, uma vez que em ambos o método a complexidade é dominada pelo algoritmo LLL utilizado para encontrar a matriz \mathbf{A}_{AM} . Naturalmente, o método proposto apresenta uma complexidade maior do que o método GM-MMSE, uma vez que no último o algoritmo LLL não é necessário. Ainda assim, a chance de ter uma taxa alcançável maior compensa o aumento da complexidade em relação ao GM-MMSE.

3.1.2 Método Proposto 2

No segundo método proposto ampliamos as possíveis escolhas de \mathbf{A} . Note que para o algoritmo LLL é necessário conhecer apenas a matriz $\mathbf{M}_{(i)}$ que por sua vez depende dos coeficientes do canal $\mathbf{H}_{(i)}$ e da SNR. Desse modo, é possível utilizar o algoritmo LLL N vezes e encontrar as

matrizes $\mathbf{A}_{(i)}$, em que

$$\mathbf{A}_{(i)} = \begin{bmatrix} \mathbf{a}_{(i),1} \\ \vdots \\ \mathbf{a}_{(i),N_T} \end{bmatrix} = \arg \min_{\mathbf{a}_{(i),1}, \dots, \mathbf{a}_{(i),N_T}} \max_m \mathbf{a}_{(i),m} \mathbf{M}_{(i)} \mathbf{a}_{(i),m}^T$$

para $i = 1, \dots, N$. Seja $\mathcal{A}_2 = \{\mathbf{I}, \mathbf{A}_{AM}, \mathbf{A}_{(1)}, \dots, \mathbf{A}_{(N)}\}$ o conjunto de possíveis escolhas. O método proposto 2 irá escolher a matriz tal que

$$\mathbf{A}_{\text{prop},2} = \arg \max_{\mathbf{A} \in \mathcal{A}_2} R_{\text{GM}}(\mathbf{H}_{(1:N)}, \mathbf{A}) \quad (3.3)$$

e a taxa alcançável por esse método é dada por

$$R_{\text{prop},2}(\mathbf{H}_{(1:N)}) = R_{\text{GM}}(\mathbf{H}_{(1:N)}, \mathbf{A}_{\text{prop},2}). \quad (3.4)$$

Note que o método proposto 1 tenta encontrar uma matriz que seja boa para todos os blocos simultaneamente, porém, não necessariamente é a matriz ótima para cada bloco individualmente. Por outro lado, o método proposto 2 encontra, também, a matriz ótima para cada bloco e verifica se, quando utilizada essa matriz, o desempenho dos outros blocos encontra-se em um nível satisfatório.

A complexidade desse método aumenta um pouco em relação ao método proposto 1 (e ao AM-IF), uma vez que é necessário utilizar o algoritmo LLL um total de $N + 1$ vezes. Entretanto, vale lembrar que o algoritmo LLL pode ser executado em tempo polinomial, fazendo com que o método proposto 2 ainda seja viável na prática.

3.2 Códigos Práticos

Os resultados desenvolvidos até então, consideram tanto um código com comprimento infinito e a cardinalidade da modulação suficientemente grande. Nessa seção será descrito como pode ser feito o processo de decodificação para códigos mais tradicionais, como o LDPC. Note que um código p -ário em conjunto com uma modulação p -PAM pode ser interpretado como um código sobre reticulados através da Construção A [16], em que p é um número primo. Maiores informações sobre reticulados encontram-se no Apêndice A.

Suponha que $p = 2$ e a mensagem do ℓ -ésimo usuário pertença ao corpo \mathbb{Z}_2^k , isto é $\mathbf{w}_\ell \in \mathbb{Z}_2^k$. Por sua vez, a mensagem é codificada pelo código $\mathcal{C}(n, k)$ gerando a palavra-código $\mathbf{c}_\ell \in \mathbb{Z}_2^n$, a qual então é modulada no vetor \mathbf{x}_ℓ .

Pode-se mostrar que a m -ésima equação do canal efetivo é dada por[15]

$$\mathbf{y}_{\text{eff},m} = \mathbf{v}_m + \mathbf{z}_{\text{eff},m} \quad (3.5)$$

em que $\mathbf{v}_m = \mathbf{a}_m \mathbf{C}$, $\mathbf{a}_m \in \mathbb{Z}^{N_T}$ e $\mathbf{z}_{\text{eff},m}$ é o ruído efetivo com variância $\sigma_{\text{eff},m}^2$. O receptor tem conhecimento de $\sigma_{\text{eff},m}^2$.

O objetivo do receptor é recuperar a m -ésima combinação linear¹ $\mathbf{u}_m = \mathbf{a}_m \mathbf{C} \bmod 2 \in \mathcal{C}$ a partir de $\mathbf{y}_{\text{eff},m}$.

Note que como \mathbf{v}_m pode assumir qualquer valor inteiro, ele não é uma palavra-código. Em contra-partida, \mathbf{u}_m é uma palavra-código. Assim sendo, será considerado o canal equivalente módulo 2, isto é

$$\begin{aligned} \mathbf{r}_m &= \mathbf{y}_{\text{eff},m} \bmod 2 \\ &= \mathbf{u}_m + \mathbf{z}_{\text{eff},m} \bmod 2. \end{aligned} \quad (3.6)$$

Considera-se que a operação módulo 2 acima pode retornar qualquer valor real entre 0 (incluso) e 2, isto é, $[\cdot \bmod 2] \in [0, 2)$.

Para facilitar a análise no decodificar a seguinte consideração será feita.

Consideração 1. O ruído efetivo $\mathbf{z}_{\text{eff},m}$ é aproximado por uma distribuição gaussiana com média nula e variância $\sigma_{\text{eff},m}^2$.

As Figs. 3.1, 3.2 e 3.3 mostram a distribuição do ruído efetivo e a gaussiana aproximada nos casos de desvanecimento estático, decodificação AM e decodificação GM, respectivamente. A distribuição do ruído efetivo foi obtida através de simulação em um canal 2×2 com coeficientes reais e dois blocos.

Como é possível perceber, a distribuição do ruído efetivo está bem próxima de uma distribuição gaussiana com exceção apenas na Fig. 3.2. Espera-se, portanto, que o erro ao considerar essa distribuição seja pequeno.

¹Considera-se que a operação módulo 2, quando aplicada em um vetor ou matriz, é feita componente a componente.

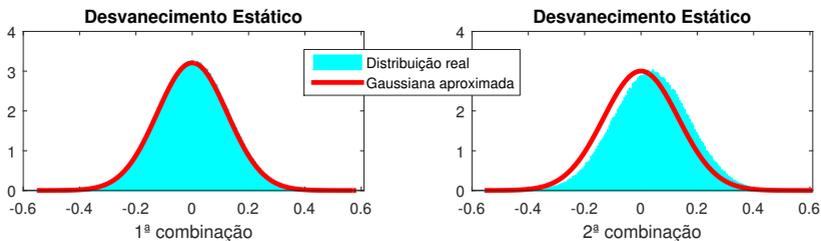


Figura 3.1: Distribuição do ruído efetivo em um canal 2×2 considerando desvanecimento estático.

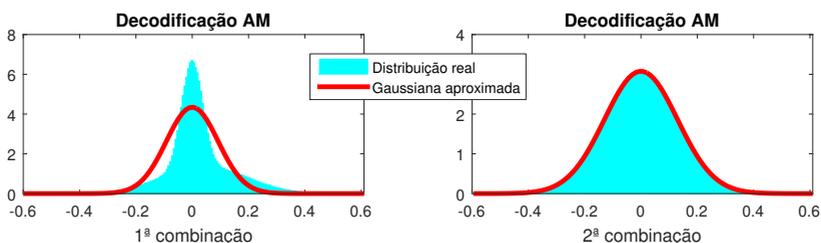


Figura 3.2: Distribuição do ruído efetivo em um canal 2×2 com dois blocos. A matriz \mathbf{A} foi escolhida através do método proposto 2. O receptor utiliza o decodificador AM.

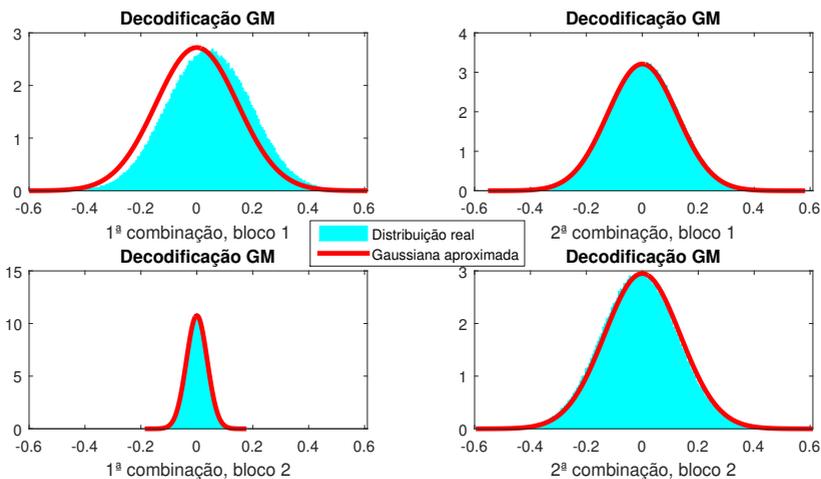
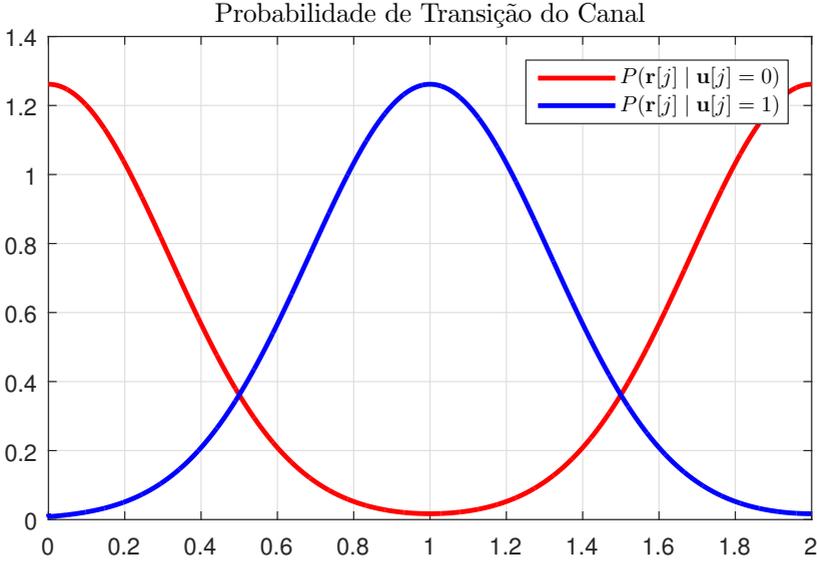


Figura 3.3: Distribuição do ruído efetivo em um canal 2×2 com dois blocos. A matriz \mathbf{A} foi escolhida através do método proposto 2. O receptor utiliza o decodificador GM.



Com essa consideração, o canal descrito na equação (3.6) é um canal AWGN módulo 2. A probabilidade de transição desse canal é mostrada na Fig. 3.4.

Para utilizar um decodificador iterativo de um código LDPC, como por exemplo o *belief-propagation* é necessário informar a LLR de cada componente de \mathbf{r}_m . O cálculo da LLR é definido da seguinte maneira

$$\text{LLR}[j] = \log \frac{\mathbb{P}(\mathbf{r}_m[j] | \mathbf{u}_m[j] = 0)}{\mathbb{P}(\mathbf{r}_m[j] | \mathbf{u}_m[j] = 1)}. \quad (3.7)$$

Note na Fig. 3.4 que para $0 \leq \mathbf{r}[j] \leq 1$ o canal é aproximadamente Gaussiano (sem a operação de módulo 2) e portanto, a LLR pode ser calculada como

$$\text{LLR}[j] = \frac{1 - 2\mathbf{r}_m[j]}{2\sigma_{\text{eff},m}^2}, \text{ para } 0 \leq \mathbf{r}[j] \leq 1. \quad (3.8)$$

Também é possível perceber que para $1 \leq \mathbf{r}[j] < 2$ existe uma reflexão em torno de 1. Nesse caso, pode-se utilizar a equação anterior, porém informando $\mathbf{r}'[j] = -\mathbf{r}[j] \bmod 2$.

Note que, se o decodificador AM for utilizado, então temos que $\sigma_{\text{eff},m}^2 = \sigma_{\text{AM},m}^2$, em que $\sigma_{\text{AM},m}^2$ é definido em (2.25). Por outro lado, se o decodificador GM é utilizado, então é necessário considerar a variância de cada bloco individualmente.

Capítulo 4

Resultados

Neste capítulo serão apresentados os resultados obtidos durante a pesquisa. Os métodos propostos são comparados com os demais métodos existentes, mostrando suas vantagens em diversas situações. Na primeira parte, as taxas alcançáveis de cada método são comparadas variando tanto o número de blocos quanto o número de usuários. Já na segunda parte, é verificado o desempenho de FER quando códigos *root*-LDPC são utilizados.

4.1 Taxas Alcançáveis

A probabilidade de *outage* é uma estimativa da probabilidade de erro (\mathbb{P}_{erro}) e pode ser definida como

$$P_{\text{out}} = \mathbb{P}[R_{\text{mes}} > R]$$

em que R depende do método utilizado. Por exemplo, se for utilizado o método ML, então R é definido como na equação (2.3) e assim por diante.

Dado $\rho > 0$, define-se a *taxa alcançável com outage* ρ ou simplesmente *taxa com outage* ρ como sendo a maior taxa de mensagem tal que a probabilidade de *outage* não seja maior que ρ , ou seja,

$$R(\rho) \triangleq \sup\{R_{\text{mes}} \mid P_{\text{out}} \leq \rho\}.$$

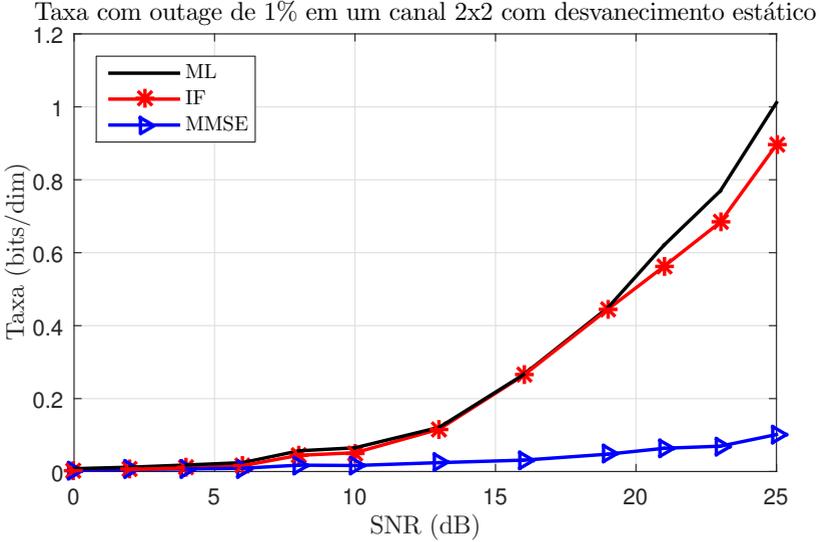


Figura 4.1: Taxas alcançáveis para uma probabilidade de *outage* de 1% em um canal 2×2 com um bloco (desvanecimento estático).

Para cada cenário de nossas simulações, foram feitas 10000 realizações de um canal Rayleigh tal que $h \sim \mathcal{N}(0, 1)$. Em cada realização foi calculado o valor de R para os métodos de interesse. Para determinar o valor de $R(\rho)$ de cada método foi escolhido o $(\rho \cdot 10000 + 1)$ -ésimo maior valor R dentre aqueles obtidos a partir de todas as realizações. Isso faz com que em apenas $\rho \cdot 10000$ realizações tenhamos $R_{\text{mes}} > R$, o que garante $P_{\text{out}} \leq \rho$.

Na Fig. 4.1 mostramos a taxa com outage de $\rho = 0.01$ para diferentes valores de SNR em um canal 2×2 com coeficientes em \mathbb{R} e desvanecimento estático ($N = 1$). O método ML é mostrado como um limitante superior. Note que, nesse caso, os decodificadores AM e GM se tornam essencialmente o mesmo método, e portanto não é necessário fazer uma distinção entre eles.

Na Fig. 4.2 é mostrada a taxa com outage de $\rho = 0.01$ para um canal 2×2 com dois blocos ($N = 2$). O método GM foi obtido através de uma busca exaustiva em todos os vetores inteiros em que a magnitude de

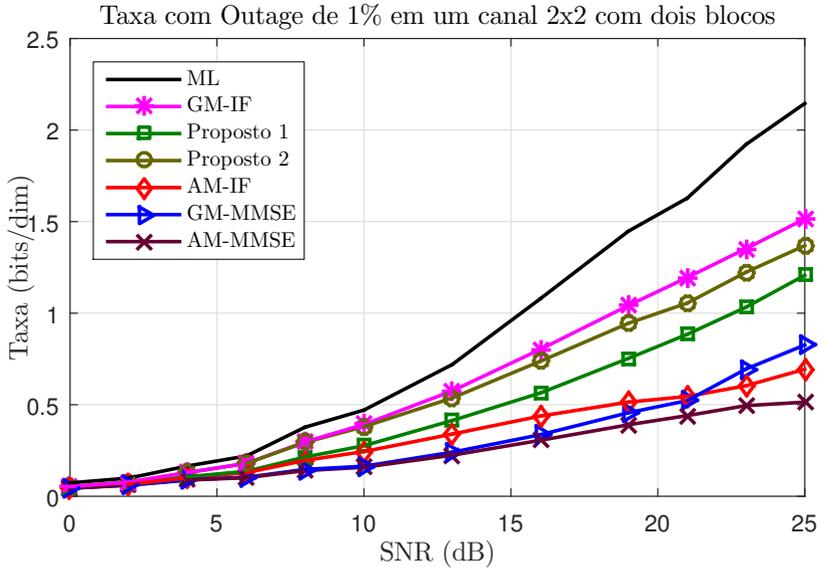


Figura 4.2: Taxas alcançáveis para uma probabilidade de *outage* de 1% em um canal 2×2 com dois blocos.

cada entrada não fosse maior que 10^1 . Nesse cenário é possível perceber uma clara distinção entre os métodos. Como esperado, o método GM-IF alcança as maiores taxas dentre todos os métodos (com exceção do ML). Porém é possível perceber que o método proposto 2 aproxima-se bastante do método GM-IF, perdendo por apenas por 2 dB em alta SNR. Mais do que isso, para baixos valores de SNR o método proposto 2 tem o mesmo desempenho que GM-IF. Já o método proposto 1, apesar de ter um melhor desempenho que os métodos AM-IF e GM-MMSE, fica aquém do método proposto 2 (2 dB em alta SNR) e do método GM-IF (4 dB em alta SNR).

Note que o método AM-MMSE terá o pior desempenho entre todos os métodos. Sabe-se que o método AM-IF será sempre superior ao método AM-MMSE uma vez que o primeiro generaliza o segundo. Além disso, sabe-se que o método GM-MMSE também será superior ao método AM-MMSE devido a desigualdade entre a média aritmética

¹O desempenho do método GM-IF foi testado com limitantes maiores, isto é, permitiu-se que os valores de magnitude não excedessem 12 ou 15. Entretanto, o desempenho do método GM-IF foi o mesmo para esses casos.

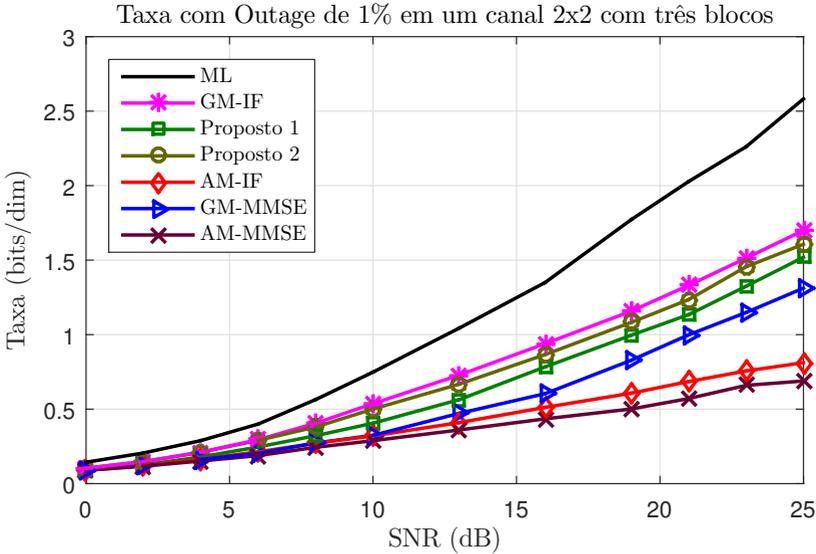


Figura 4.3: Taxas alcançáveis para uma probabilidade de *outage* de 1% em um canal 2×2 com três blocos.

e a média geométrica.

As Figs. 4.3 e 4.4 mostram as taxas alcançáveis em um canal 2×2 com três ($N = 3$) e quatro ($N = 4$) blocos, respectivamente. Nesses cenários, é possível perceber que a diferença entre o método GM-IF e ambos os métodos propostos diminui conforme o número de blocos aumenta. Esse efeito é melhor visualizado na Fig. 4.5 que mostra as taxas alcançáveis em um canal 2×2 com $\text{SNR} = 25$ dB variando o número de blocos. Além disso, o desempenho do método GM-MMSE melhora significativamente, principalmente em comparação ao método AM-IF.

Já a Fig. 4.6 mostra o efeito ao aumentar o número de usuários em uma rede com 2 blocos e $\text{SNR} = 25$ dB para cada usuário (portanto, a potência total de transmissão aumenta conforme o número de usuários). O método GM-IF teve seu desempenho simulado apenas para 2 e 3 usuários devido a sua alta complexidade.

Diferente do que ocorre quando aumenta-se o número de blocos,

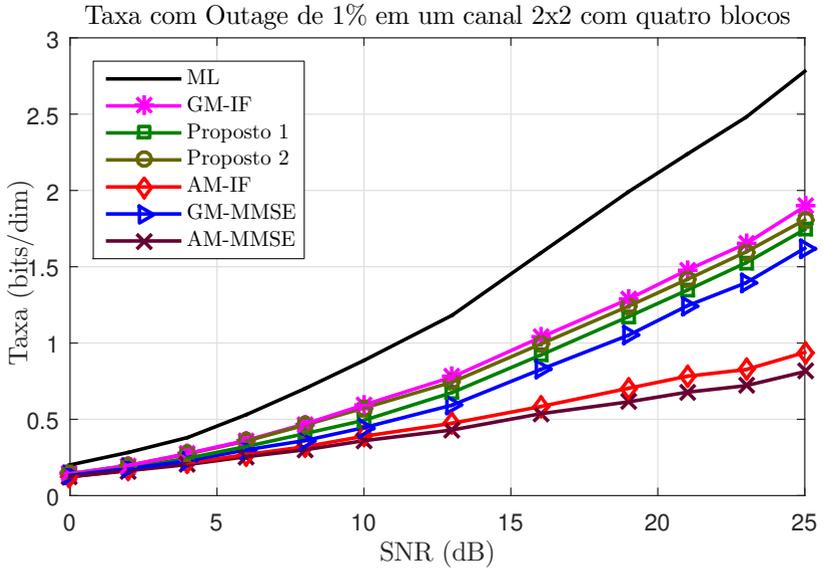


Figura 4.4: Taxas alcançáveis para uma probabilidade de *outage* de 1% em um canal 2×2 com quatro blocos.

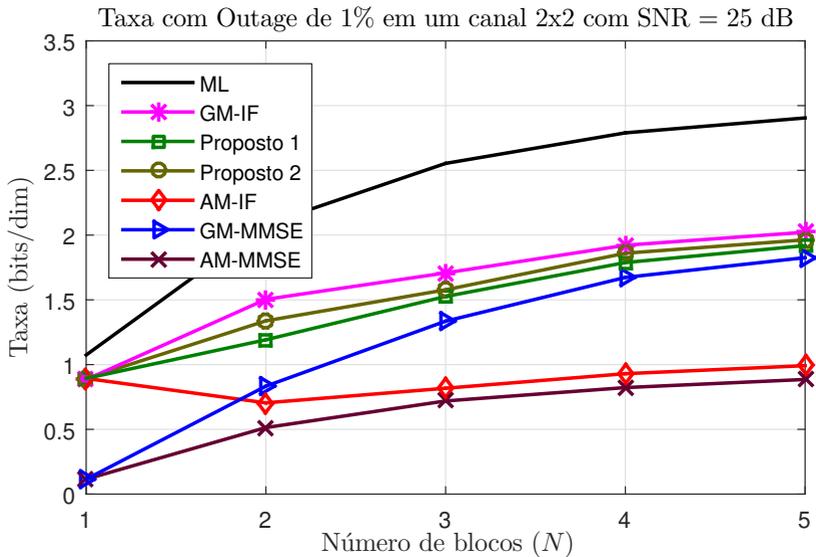


Figura 4.5: Taxas alcançáveis para uma probabilidade de *outage* de 1%, em um canal 2×2 e com SNR = 25 dB variando o número de blocos (N).

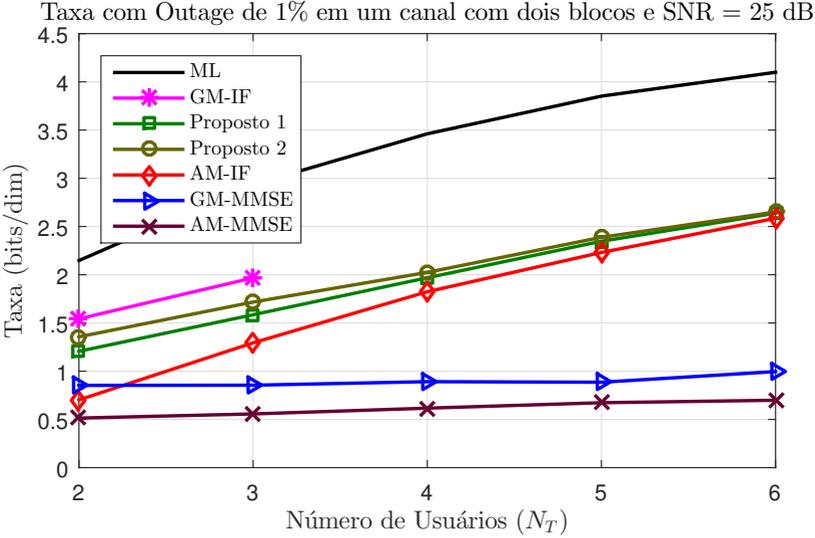


Figura 4.6: Taxas alcançáveis para uma probabilidade de *outage* de 1%, em um canal com dois blocos e SNR = 25 dB variando o número de usuários (N_T) e considerando $N_R = N_T$.

o método AM-IF tem uma melhora de desempenho significativa, enquanto o desempenho do método GM-MMSE é quase constante.

Para melhor compreender a eficiência dos métodos propostos basta perceber que mesmo quando ambos os métodos AM-IF e GM-MMSE falham, os métodos propostos podem ser bem sucedidos. A Tab. 4.1 mostra a probabilidade de *outage* de um canal 2×2 com dois blocos, $R_{\text{mes}} = 0.5$ e SNR = 10 dB. O valor de SNR foi escolhido do modo que os métodos AM-IF e GM-MMSE tenham aproximadamente a mesma probabilidade de *outage* (em torno de 10.1%).

Pode-se pensar que, por exemplo, o método proposto 1 falha quando ambos AM-IF e GM-MMSE falhassem, o que ocorre com uma probabilidade de 6.11%. Entretanto a probabilidade de *outage* desse método proposto é estritamente menor, apenas 4.78%. Isso ocorre pois para a mesma matriz \mathbf{A} o decodificador GM tem um melhor desempenho que o decodificador AM. Assim, quando o método AM-IF alcança melhores taxas que o método GM-MMSE, o método proposto 1 irá alcançar uma taxa ainda maior em relação ao AM-IF. De modo semelhante, temos

Tabela 4.1: Probabilidade de *outage* para um canal 2×2 com $N = 2$ blocos e $\text{SNR} = 10$ dB.

		AM-IF	
		<i>Outage</i>	Sucesso
GM-MMSE	<i>Outage</i>	6.11%	4.02%
	Sucesso	4.03%	85.84%

		<i>Outage</i>	Sucesso
Método Proposto 1		4.78%	95.22%
Método Proposto 2		2.65%	97.35%

que a probabilidade de *outage* para o método proposto 2 é ainda menor, apenas 2.65%.

Os resultados dessa seção mostram que ambos os métodos propostos têm um desempenho melhor que os métodos AM-IF e GM-MMSE independente do número de usuários e/ou blocos. Essa vantagem é ainda mais significativa quando ambos os métodos AM-IF e GM-MMSE tem um desempenho parecido. Mesmo quando há uma disparidade entre esses métodos, o método proposto ainda apresenta melhores taxas, apesar da vantagem não ser tão significativa.

4.2 Taxa de Erro de Quadro (FER)

Nessa seção será mostrado o desempenho dos métodos proposto em um cenário mais realista, em que modulações tradicionais e códigos com comprimento finito são considerados.

É necessário utilizar códigos para canais com desvanecimento de bloco a fim de explorar a máxima diversidade desses canais. Uma família de códigos que garanta essa máxima diversidade são os códigos *root-LDPC* [14].

Como mostrado em [14], para que um código *root-LDPC* tenha máxima diversidade em um canal com desvanecimento de bloco, a taxa do código não pode exceder $1/N$, em que N é o número de blocos. Note que para os decodificadores AM, códigos LDPC tradicionais poderiam

ser utilizados.

Os códigos *root*-LDPC podem ser construídos de maneira similar aos códigos LDPC tradicionais. Algumas referências para construção se encontram em [22, 23, 24, 25]. Em nossas simulações, utilizamos o algoritmo *root*-PEG [23] para construir um código regular, em que cada coluna tem grau 3 (o grau médio das linhas é escolhido de acordo com a taxa de código usada) com comprimento 2016. A taxa do código será diferente em cada cenário para garantir máxima diversidade. Além disso, serão adotadas as considerações citadas na seção 3.2, isto é, será considerado que o ruído efetivo segue uma distribuição Gaussiana para o cálculo da LLR.

Nas figuras a seguir, as curvas teóricas foram obtidas através da comparação da taxa alcançável de cada método com a taxa de mensagem (R_{mes}) em cada cenário, isto é, verifica-se $R_{\text{mes}} > R$. Portanto, as curvas representam um limitante da teoria da informação para a FER.

A Fig 4.7 mostra a FER em um canal 2×2 com dois blocos. O código tem taxa $1/2$ e a modulação utilizada é 2-PAM, portanto, temos que $R_{\text{mes}} = 1/2$. Note que, por exemplo, o método proposto 2 atinge uma FER (teórica) de 1% em torno de 12 dB. Comparando com a Fig. 4.2 temos que para 12 dB a taxa máxima para que o método proposto 2 garanta uma probabilidade de *outage* de 1% é aproximadamente $1/2$, o que confirma as simulações para estimativa de FER.

Como esperado, temos que mesmo em um cenário mais realista, o método proposto 2 apresenta um desempenho melhor que os demais métodos (com exceção dos métodos ML e GM-IF), ganhando em torno de 1 dB do método proposto 1 e em torno de 4 dB dos métodos AM-IF e GM-MMSE.

Já na Fig. 4.8 é mostrada a FER em um canal 2×2 com três blocos. Novamente foi utilizada modulação 2-PAM porém o código tem taxa $1/3$, e portanto, temos que $R_{\text{mes}} = 1/3$. Novamente, note que, por exemplo, a curva teórica do método proposto 2 atinge a FER em 1% em torno de 7 dB. Em comparação com a Fig. 4.3 pode-se perceber que o método proposto 2, com $\text{SNR} = 7$ dB garante uma probabilidade de *outage* de no máximo 1% para uma taxa aproximadamente de 0.4, confirmando mais uma vez as simulações.

O método proposto 2 apresenta um desempenho melhor que os demais métodos, com ganhos próximos ao caso anterior.

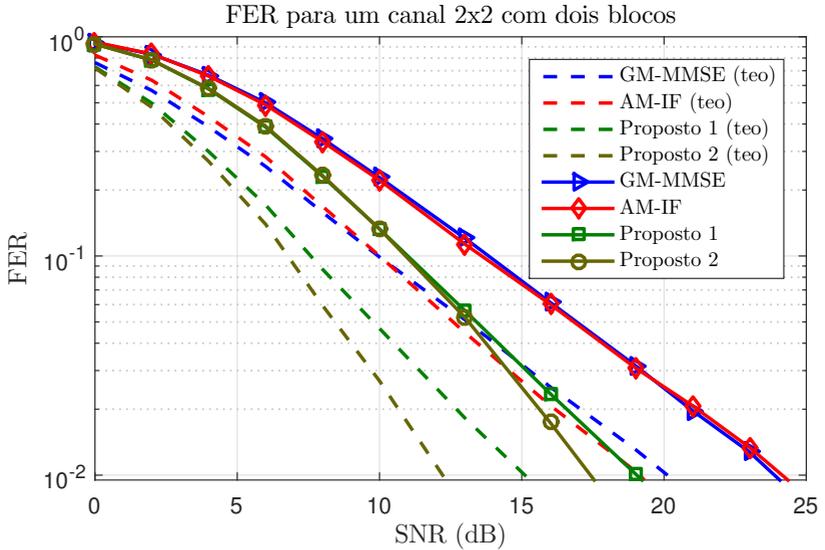


Figura 4.7: FER para um canal 2×2 com dois blocos, utilizando um código *root*-LDPC com taxa $1/2$.

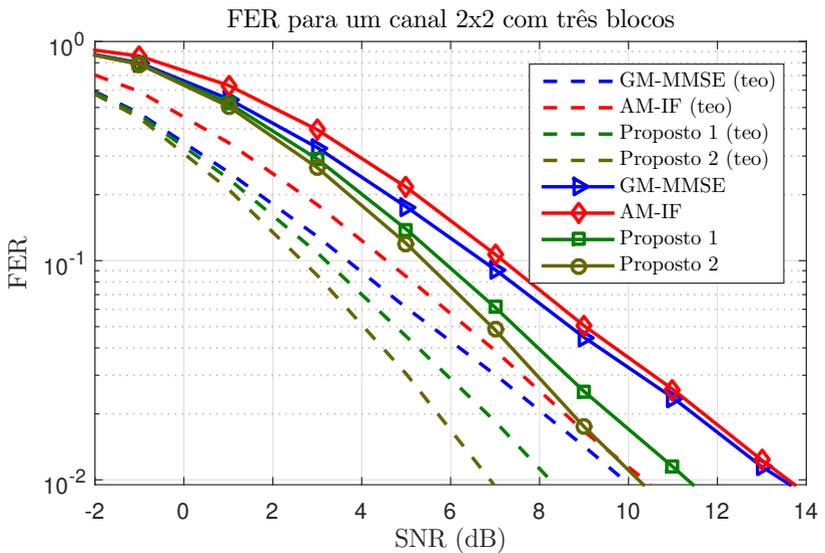


Figura 4.8: FER para um canal 2×2 com três blocos e $\text{SNR} = 25$ dB, utilizando um código *root*-LDPC com taxa $1/3$.

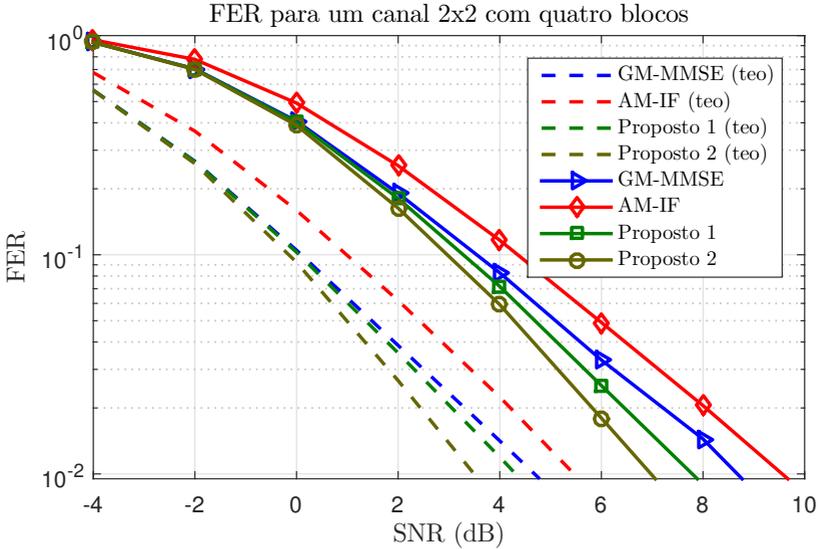


Figura 4.9: FER para um canal 2×2 com quatro blocos e SNR = 25 dB, utilizando um código *root*-LDPC com taxa $1/4$.

Por fim, a Fig. 4.9 mostra a FER para um canal 2×2 com quatro blocos e modulação 2-PAM. O código utilizado tem taxa $1/4$ fazendo com que $R_{\text{mes}} = 1/4$. Se for feita a mesma análise dos casos anteriores, percebe-se que o método proposto 2 alcança a FER de 1% em torno de 4 dB o que coincide com a Fig. 4.4.

Para se aproximar ainda mais das curvas teóricas de FER pode-se utilizar códigos LDPC com outros tipos de construção. Por exemplo, em [14] é mostrado que códigos *root* LDPC irregulares tem melhor desempenho do que códigos regulares. Além disso, outra alternativa para se aproximar dos resultados teóricos é aumentar a R_{mes} . Como a taxa do código está limitada ao número de blocos, nos resta utilizar modulações com maior eficiência espectral, o que exigiria construção de códigos aninhados [26].

Capítulo 5

Conclusão

O método IF suragiu como alternativa aos tradicionais métodos de decodificação linear, como o ZF e MMSE. Mesmo que sua complexidade seja comparável com tais métodos tradicionais seu desempenho fica próximo ao método ML (método ótimo) em diversas situações. O método IF foi originado a partir do algoritmo computa-e-encaminha e já foi bastante explorado na literatura.

Entretanto, apenas recentemente, o método IF foi generalizado para canais com desvanecimento de bloco. Nesse caso, dois métodos de decodificação foram apresentados, o método AM e o método GM. O primeiro tenta aproximar o canal BF em um canal com desvanecimento estático através da variância do ruído efetivo. Já o segundo método, explora a máxima diversidade do canal e tenta extrair o máximo de informação (bits) possível.

Apesar do método GM-IF alcançar as maiores taxas, não se conhece um algoritmo eficiente para encontrar os coeficientes ótimos das combinações lineares. Como alternativa, conhecia-se, até então, os métodos GM-MMSE e AM-IF. Como mostrado nas simulações, em cenários com um número elevado de blocos, o método GM-MMSE apresenta um melhor desempenho do que o método AM-IF. Em contrapartida, em cenários com um número elevado de usuários, o inverso acontece e o método AM-IF apresenta melhor desempenho do que o método GM-MMSE.

Nessa dissertação foram apresentados dois novos métodos de baixa

complexidade para escolher os coeficientes das combinações lineares para o decodificador GM em um canal com desvanecimento de bloco. O primeiro método proposto, mais simples, tem um desempenho melhor que ambos os métodos GM-MMSE e AM-IF em qualquer cenário. Esse método é baseado em uma simples escolha para a matriz \mathbf{A} .

Já no segundo método proposto, aumentamos o número de possíveis escolhas para a matriz \mathbf{A} . Fazendo isso, conseguimos alcançar taxas ainda maiores, aproximando-se das taxas do método GM-IF. Apesar de sua complexidade ser um pouco maior que o primeiro método proposto, esse segundo método ainda pode ser realizado em tempo polinomial.

A fim de consolidar os resultados, testamos a eficiência dos métodos propostos em um cenário mais realista, em que modulações tradicionais e códigos com comprimento finito são usados. Nesse caso, é necessário que o código utilizado tenha máxima diversidade em um canal com desvanecimento de bloco. Portanto, utilizamos os códigos *root*-LDPC em canais com dois, três e quatro blocos, a taxa do código utilizado foi $1/2$, $1/3$ e $1/4$, respectivamente. Em cada um desses cenários, o método proposto 2 apresentou um desempenho melhor que os demais métodos, ganhando 1 dB em relação ao método proposto 1 e até 7 dB em relação aos métodos AM-IF e GM-MMSE.

Os resultados mostrados nessa dissertação nos mostram que as vantagens do método forçagem a inteiros continuam válidas, mesmo em um cenário com desvanecimento de bloco.

Trabalhos futuros

Como futuras linhas de pesquisa, sugere-se o seguinte.

- (i) Explorar métodos alternativos para escolher a matriz \mathbf{A} no método GM;
- (ii) Estudar e avaliar métodos como o cancelamento sucessivo de interferência (SIC) [27] e forçagem a inteiros sucessivo (SIF) [28] em um canal com desvanecimento de bloco;
- (iii) Encontrar códigos com alta eficiência espectral de comprimento finito que atinjam máxima diversidade em canais com desvanecimento de bloco.

Apêndice A

Reticulados

Um reticulado Λ é um subconjunto de \mathbb{R}^n tal que, se $\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2 \in \Lambda$ então para quaisquer $a_1, a_2 \in \mathbb{Z}$ temos que $a_1\boldsymbol{\lambda}_1 + a_2\boldsymbol{\lambda}_2 \in \Lambda$.

Seja $\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_m \in \mathbb{R}^n$ vetores linearmente independentes. Pode-se definir um reticulado como

$$\Lambda = \{\mathbf{a}\mathbf{G}_\Lambda : \mathbf{a} \in \mathbb{Z}^m\} \quad (\text{A.1})$$

em que $\mathbf{G}_\Lambda = \begin{bmatrix} \mathbf{g}_1^T & \mathbf{g}_2^T & \dots & \mathbf{g}_m^T \end{bmatrix}^T$. Note que existe mais de uma matriz \mathbf{G}_Λ capaz de gerar o mesmo reticulado Λ .

Um quantizador é uma função que mapeia $\mathbf{x} \in \mathbb{R}^n$ em um ponto do reticulado $\boldsymbol{\lambda} \in \Lambda$. Em especial, o quantizador de máxima verossimilhança é aquele que mapeia $\mathbf{x} \in \mathbb{R}^n$ no ponto do reticulado mais próximo, em termos de distância Euclidiana, isto é

$$\mathcal{Q}_\Lambda(\mathbf{x}) = \arg \min_{\boldsymbol{\lambda} \in \Lambda} \|\boldsymbol{\lambda} - \mathbf{x}\|^2 \quad (\text{A.2})$$

A região de Voronoi para um dado $\boldsymbol{\lambda} \in \Lambda$ é definido como

$$\mathcal{V}_\Lambda(\boldsymbol{\lambda}) = \{\mathbf{x} \in \mathbb{C}^n : \mathcal{Q}_\Lambda(\mathbf{x}) = \boldsymbol{\lambda}\}. \quad (\text{A.3})$$

Para $\boldsymbol{\lambda} = \mathbf{0}$ chamamos $\mathcal{V}_\Lambda(\mathbf{0})$ de região fundamental de Voronoi. Note que para qualquer $\boldsymbol{\lambda} \in \Lambda$ temos que $\mathcal{V}_\Lambda(\boldsymbol{\lambda}) = \boldsymbol{\lambda} + \mathcal{V}_\Lambda(\mathbf{0})$.

A operação “modulo reticulado” é definida como

$$\mathbf{x} \bmod \Lambda = \mathbf{x} - \mathcal{Q}_\Lambda(\mathbf{x}) \quad (\text{A.4})$$

para qualquer $\mathbf{x} \in \mathbb{R}^n$.

Os reticulados Λ_c e Λ_f são ditos aninhados se $\Lambda_c \subseteq \Lambda_f$. Refere-se ao reticulado Λ_f como reticulado fino e o reticulado Λ_c como reticulado grosso.

Para quaisquer $\mathbf{x}_1, \mathbf{x}_2 \in \mathbb{R}^n$, $\alpha \in \mathbb{Z}$, $\beta \in \mathbb{R}$ e para $\Lambda_c \subseteq \Lambda_f$ temos que

$$(\mathbf{x}_1 + \mathbf{x}_2) \bmod \Lambda_c = ((\mathbf{x}_1 \bmod \Lambda_c) + \mathbf{x}_2) \bmod \Lambda_c \quad (\text{A.5})$$

$$\mathcal{Q}_{\Lambda_f}(\mathbf{x}_1) \bmod \Lambda_c = \mathcal{Q}_{\Lambda_f}(\mathbf{x}_1 \bmod \Lambda_c) \bmod \Lambda_c \quad (\text{A.6})$$

$$(\alpha \mathbf{x}_1) \bmod \Lambda_c = \alpha(\mathbf{x}_1 \bmod \Lambda_c) \bmod \Lambda_c \quad (\text{A.7})$$

$$\beta(\mathbf{x}_1 \bmod \Lambda_c) = (\beta \mathbf{x}_1) \bmod \beta \Lambda_c \quad (\text{A.8})$$

Seja $\Lambda_c \subseteq \Lambda_f$, um código sobre reticulados aninhados $\mathcal{L}(\Lambda_f, \Lambda_c)$ é o conjunto de pontos do reticulado fino Λ_f que estão na região fundamental de Voronoi do reticulado grosso Λ_c . Matematicamente, pode ser definido como

$$\mathcal{L}(\Lambda_f, \Lambda_c) = \Lambda_f \bmod \Lambda_c = \{\boldsymbol{\lambda} \bmod \Lambda_c : \boldsymbol{\lambda} \in \Lambda_f\} \quad (\text{A.9})$$

A taxa desse código é definida como

$$R_{\mathcal{L}} = \frac{1}{n} \log_2(|\mathcal{L}|) = \frac{1}{n} \log_2 \left(\frac{\text{Vol}(\Lambda_c)}{\text{Vol}(\Lambda_f)} \right) \quad (\text{A.10})$$

em que $\text{Vol}(\Lambda_c)$ e $\text{Vol}(\Lambda_f)$ são os volumes da região fundamental de Voronoi dos reticulados Λ_c e Λ_f respectivamente.

Referências bibliográficas

- [1] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*, 1st ed. Cambridge University Press, Jul 2005.
- [2] A. Goldsmith, *Wireless Communications*, 1st ed. Cambridge University Press, Aug 2005.
- [3] M. M. d. Silva and F. A. Monteiro, *MIMO Processing for 4G and Beyond: Fundamentals and Evolution*. CRC Press, Jun 2014.
- [4] E. Biglieri, *MIMO wireless communications*. Cambridge University Press, 2007.
- [5] B. Clerckx, C. Oestges, and C. Oestges, *MIMO wireless networks: channels, techniques and standards for multi-antenna, multi-user and multi-cell systems*, 2nd ed. Academic Press, 2013.
- [6] J. R. Hampton, *Introduction to MIMO communications*. Cambridge University Press, 2014.
- [7] J. Zhan, B. Nazer, U. Erez, and M. Gastpar, “Integer-forcing linear receivers,” *IEEE Transactions on Information Theory*, vol. 60, no. 12, pp. 7661–7685, Dec 2014.
- [8] B. Nazer and M. Gastpar, “Compute-and-forward: Harnessing interference through structured codes,” *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6463–6486, Oct 2011.

- [9] —, “Reliable physical layer network coding,” *Proceedings of the IEEE*, vol. 99, no. 3, pp. 438–460, Mar 2011.
- [10] R. Zamir, *Lattice Coding for Signals and Networks: A Structured Coding Approach to Quantization, Modulation and Multiuser Information Theory*. Cambridge University Press, 2014.
- [11] R. Knopp and P. A. Humblet, “On coding for block fading channels,” *IEEE Transactions on Information Theory*, vol. 46, no. 1, pp. 189–205, Jan 2000.
- [12] B. Fontana da Silva, “Técnicas de codificação de rede no domínio da frequência,” Master’s thesis, Federal University of Santa Catarina (UFSC), 2015.
- [13] I. E. Bakoury and B. Nazer, “The impact of channel variation on integer-forcing receivers,” in *2015 IEEE International Symposium on Information Theory (ISIT)*, Jun 2015, pp. 576–580.
- [14] J. J. Boutros, A. G. i. Fabregas, E. Biglieri, and G. Zemor, “Low-density parity-check codes for nonergodic block-fading channels,” *IEEE Transactions on Information Theory*, vol. 56, no. 9, pp. 4286–4300, Sep 2010.
- [15] C. Feng, D. Silva, and F. Kschischang, “An algebraic approach to physical-layer network coding,” *IEEE Transactions on Information Theory*, vol. 59, no. 11, pp. 7576–7596, Nov 2013.
- [16] J. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed. Springer, Dec 1998.
- [17] P. S. D. Galbraith, *Mathematics of Public Key Cryptography*, 1st ed. Cambridge University Press, Apr 2012.
- [18] E. Agrell, T. Eriksson, A. Vardy, and K. Zeger, “Closest point search in lattices,” *IEEE Transactions on Information Theory*, vol. 48, no. 8, pp. 2201–2214, Aug 2002.
- [19] J. Blömer and J. Seifert, “On the complexity of computing short linearly independent vectors and short bases in a lattice,” in *Proceedings of the Thirty-first Annual ACM Symposium on Theory of Computing*, 1999, pp. 711–720.

- [20] A. K. Lenstra, H. W. L. Jr, and L. Lovász, “Factoring polynomials with rational coefficients,” *Math. Ann.*, vol. 261, no. 4, pp. 515–534, Dec 1982.
- [21] J. M. Steele, *The Cauchy-Schwarz Master Class: An Introduction to the Art of Mathematical Inequalities*. The Mathematical Association of America, Apr 2004.
- [22] D. Duyck, J. J. Boutros, and M. Moeneclaey, “Full diversity random LDPC codes,” in *2011 18th IEEE Symposium on Communications and Vehicular Technology in the Benelux (SCVT)*, Nov 2011, pp. 1–6.
- [23] A. G. D. Uchoa, C. Healy, R. C. d. Lamare, and R. D. Souza, “Design of LDPC codes based on progressive edge growth techniques for block fading channels,” *IEEE Communications Letters*, vol. 15, no. 11, pp. 1221–1223, Nov 2011.
- [24] Y. Li and M. Salehi, “Quasi-cyclic ldpc code design for block-fading channels.” in *IEEE CISS*, Mar 2010, pp. 1–5.
- [25] A. G. Uchoa, C. T. Healy, and R. C. de Lamare, “Structured root-LDPC codes and PEG-based techniques for block-fading channels,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2015, no. 1, Dec 2015.
- [26] P. R. Branco da Silva, “Códigos LDPC multinível para codificação de rede na camada física.” Master’s thesis, Federal University of Santa Catarina (UFSC), 2015.
- [27] P. W. Wolniansky, G. J. Foschini, G. D. Golden, and R. A. Valenzuela, “V-BLAST: an architecture for realizing very high data rates over the rich-scattering wireless channel,” in *1998 URSI International Symposium on Signals, Systems, and Electronics, 1998. ISSSE 98*, Sep 1998, pp. 295–300.
- [28] O. Ordentlich, U. Erez, and B. Nazer, “Successive integer-forcing and its sum-rate optimality,” in *2013 51st Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Oct 2013, pp. 282–292.

