

Códigos Turbo para Codificação de Rede na Camada Física sobre Inteiros Gaussianos

Maria Cláudia Castro, Danilo Silva e Bartolomeu F. Uchôa-Filho

Resumo—Codificação de rede na camada física (PNC) é uma técnica de transmissão sem fio na qual nós transmissores transmitem seus pacotes simultaneamente, e um nó intermediário (receptor ou *relay*) decodifica uma combinação linear das respectivas mensagens. Na estratégia computa-e-encaminha, tais combinações lineares são obtidas de acordo com os ganhos dos canais e com base na estrutura algébrica de códigos de reticulados aninhados. A estratégia de decodificação proposta é semelhante à de um sistema de transmissão ponto-a-ponto, independentemente do número de nós transmissores. Recentemente, Feng, Silva e Kschischang propuseram uma abordagem algébrica para PNC, sugerindo o uso de reticulados baseados em anéis de inteiros, ao invés de corpos finitos. Seguindo esta abordagem, neste trabalho projetamos um esquema de codificação/decodificação para PNC baseado em reticulados sobre inteiros Gaussianos obtidos pela Construção A Levantada, fazendo uso de códigos turbo binários. Resultados numéricos comprovam o excelente desempenho do esquema proposto.

Palavras-Chave—Codificação de rede na camada física, códigos turbo, reticulados.

Abstract—Physical-layer network coding (PNC) is a wireless transmission technique in which nodes transmit their packets simultaneously, and an intermediate node (receptor or *relay*) decodes a linear combination of the respective messages. In the compute-and-forward strategy, such linear combinations are obtained according to the channel gains and regarding the algebraic structure of nested lattice codes. The proposed decoding strategy is similar to the one of a point-to-point transmission system, independently of the number of transmit nodes. Recently, Feng, Silva e Kschischang proposed an algebraic approach to PNC, and suggested the use of lattices based on integer rings, instead of finite fields. Following this approach, in this work we design a encoding/decoding scheme for PNC based on lattices over the Gaussian integers obtained via Lifted Construction A, making use of binary turbo codes. Numerical results show the excellent performance of the proposed scheme.

Keywords—Physical-layer network coding, turbo codes, lattices.

I. INTRODUÇÃO

A técnica de codificação de rede tem atraído cada vez mais atenção da comunidade científica, particularmente para os ambientes sem fio. A ideia principal foi proposta inicialmente por Ahlswede *et al.* [1] que mostraram que, se for permitido aos nós intermediários de uma rede combinar as mensagens recebidas, antes de encaminhá-las, o fluxo de informação máxima poderá ser alcançado.

Em 2006, de forma simultânea e independente, alguns pesquisadores em [2], [3], [4] perceberam que, em um am-

biente sem fio, a interferência entre os sinais transmitidos, até então tratada como um fenômeno destrutivo, poderia ser utilizada de forma benéfica possibilitando uma comunicação mais rápida e eficiente. A superposição de sinais, própria do meio sem fio, seria uma forma de codificação de rede que ocorreria naturalmente. Desse modo, o nó intermediário (*relay*) não necessitaria mais conhecer as mensagens individuais dos usuários, e seu papel seria extrair diretamente dos sinais sobrepostos recebidos alguma função das mensagens (por exemplo o XOR). Na literatura, esta estratégia é conhecida como codificação de rede na camada física (PNC, do inglês *physical-layer network coding*) [2], e será a adotada neste trabalho.

Um novo esquema de PNC, desenvolvido por Nazer e Gastpar em [5], atraiu muita atenção da comunidade científica. Os autores propuseram uma nova estratégia de encaminhamento no *relay*, denominada *computa-e-encaminha*, (CF, do inglês *compute-and-forward*). A ideia principal é fazer com que o *relay* decodifique uma combinação linear das mensagens recebidas de acordo com os coeficientes de canal observados. Uma das maneiras mais eficazes de implementar CF é utilizar códigos de reticulados aninhados nos transmissores, assegurando que combinações lineares inteiras de palavras-código também sejam palavras-código. Um aspecto importante de CF é que a decodificação no *relay* é feita de modo semelhante à de um cenário ponto-a-ponto, independentemente do número de usuários, o que torna o esquema escalável.

Recentemente, Feng, Silva e Kschischang apresentaram em [6] uma abordagem algébrica para PNC, denominada *codificação de rede via reticulados* (LNC, do inglês *lattice network coding*), da qual o esquema de Nazer e Gastpar [7] pode ser visto como um caso especial. Foi mostrado em [6] que o uso de códigos de reticulados aninhados com modulações maiores que a binária resulta em ambiguidades na obtenção de uma combinação linear específica com coeficientes em um corpo finito. A solução proposta em [6] foi adotar a estrutura de anéis de inteiros complexos (ao invés de corpos finitos).

Códigos de reticulados vêm sendo desenvolvidos para sistemas de comunicação desde a década de 80 [8]. Em 2003, começaram a surgir classes de códigos de reticulados associados a códigos LDPC [9]. Apenas em 2010 eles começaram a ser associados aos códigos turbo [10]. Com o trabalho de Feng, Silva e Kschischang [6] sobre PNC, a construção de sistemas LNC poderosos foi parcialmente explorada em alguns trabalhos recentes [11], [12]. Em [12], os autores utilizaram códigos LDPC em esquemas LNC sobre anéis de inteiros complexos (os inteiros de Eisenstein), e conseguiram um bom desempenho em canais específicos. A complexidade do processo de decodificação, porém, cresce quando aumenta-se

o número de usuários do sistema.

No presente trabalho, exploramos a abordagem LNC e projetamos códigos de reticulados para PNC contruídos a partir de códigos turbo binários, segundo a Construção A Levantada (para uma rápida referência, ver o artigo “*Codificação de Rede na Camada Física via Reticulados*”, do segundo autor, que encontra-se publicado nestes mesmos anais). Avaliamos através de simulações computacionais o desempenho do algoritmo de decodificação BCJR baseado em uma nova forma de cálculo de métricas, especialmente desenvolvida para o cenário em questão. A vantagem em relação ao processo proposto em [12] reside na complexidade da decodificação, que é independente do número de usuários presentes no sistema.

Este artigo é organizado da seguinte maneira. Na Seção II, descrevemos o modelo completo do sistema, incluindo os modelos estatísticos dos canais e os codificadores. Na Seção III, as principais características da estratégia CF sobre anéis é apresentada. A Seção IV é dedicada à construção do decodificador turbo. Na Seção V, apresentamos os resultados de simulações. Finalmente, na Seção VI, apresentamos as nossas conclusões.

II. MODELO DO SISTEMA

Consideramos um sistema no qual vários nós fonte, S_l , para $l = 1, \dots, L$, desejam transmitir suas mensagens através de um único nó *relay*, R . Quando PNC é empregada, o *relay* recebe sincronamente os sinais das fontes, sobrepostos e corrompidos, e estima uma combinação linear das mensagens originais baseada nos ganhos dos canais. Em seguida, esta combinação linear é codificada e transmitida ao nó destino. Este, após o recebimento de um número suficiente de combinações lineares, poderá resolver um sistema linear e assim obter a sua mensagem desejada. Vamos nos concentrar na recepção simultânea dos sinais no *relay*, por ser este o processo mais crítico do sistema.

Seguindo a abordagem algébrica LNC em [6], consideramos neste trabalho reticulados sobre anéis de inteiros complexos obtidos a partir de códigos turbo binários [13], fazendo uso da *Construção A Levantada*. Seja $\mathcal{C} \subset \mathbb{Z}_2^n$ um código turbo binário. Considere o código levantado $\bar{\mathcal{C}}$ definido por $\bar{\mathcal{C}} \triangleq \{\mathbf{c} + i\mathbf{c}' : \mathbf{c}, \mathbf{c}' \in \mathcal{C}\}$, que é um $\mathbb{Z}_2[i]$ -módulo, sendo $\mathbb{Z}_2[i] = \{0, 1, i, 1 + i\}$ o anel finito de inteiros Gaussianos módulo 2, com $i = \sqrt{-1}$. Defina Λ como sendo o reticulado

$$\Lambda \triangleq \{(2z^1 + \bar{c}_1, \dots, 2z^n + \bar{c}_n) : z^j \in \mathbb{Z}[i], \bar{\mathbf{c}} = (\bar{c}_1, \dots, \bar{c}_n) \in \bar{\mathcal{C}}\} \quad (1)$$

Dessa maneira, os *cosets* da partição $\Lambda/2\mathbb{Z}[i]^n$ são isomorfos às palavras-código de $\bar{\mathcal{C}}$.

O codificador turbo é constituído por dois códigos convolucionais recursivos e sistemáticos (RSC - Recursive Systematic Convolutional) idênticos, operando em paralelo com um entrelaçador entre eles. Para simplificar a exposição, assumimos que o código turbo tem taxa igual a $1/n$. Os nós fonte produzem, de forma independente e paralela, o par de vetores $(\mathbf{u}_l^I, \mathbf{u}_l^Q) \in \mathbb{F}_2^k \times \mathbb{F}_2^k$, representando as componentes em fase e em quadratura da mensagem $\mathbf{u}_l = \mathbf{u}_l^I + i\mathbf{u}_l^Q \in \mathbb{Z}_2[i]^k$.

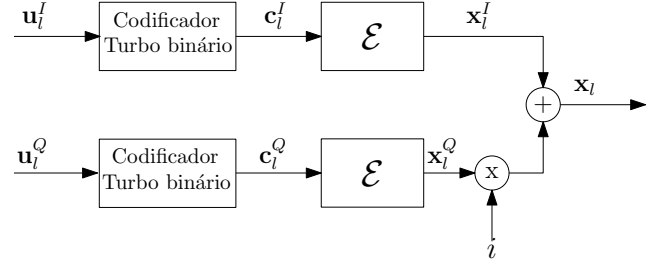


Fig. 1. Modelo do codificador na fonte S_l .

Analogamente, os *cosets* da partição $\mathbb{Z}[i]^k/2\mathbb{Z}[i]^k$ são isomorfos às mensagens $\mathbf{u}_l \in \mathbb{Z}_2[i]^k$.

Para $l = 1, \dots, L$, sejam $\mathbf{u}_l^I = [u_l^I(1), \dots, u_l^I(k)] \in \mathbb{F}_2^k$ e $\mathbf{u}_l^Q = [u_l^Q(1), \dots, u_l^Q(k)] \in \mathbb{F}_2^k$ os dois vetores de mensagem de tamanho k bits cada da fonte S_l . Estes são codificados por dois codificadores turbo independentes, produzindo as respectivas sequências codificadas de tamanho nk bits cada: $\mathbf{c}_l^I = [c_l^I(1), \dots, c_l^I(k)] \in \mathbb{F}_2^{nk}$ e $\mathbf{c}_l^Q = [c_l^Q(1), \dots, c_l^Q(k)] \in \mathbb{F}_2^{nk}$. Cada bloco codificado $\mathbf{c}_l^j(t) = [c_l^{j,1}(t), \dots, c_l^{j,n}(t)]$ é um vetor de n bits, e corresponde à saída do codificador turbo j , com $j \in \{I, Q\}$, considerando a entrada $u_l^j(t)$ no tempo t . Assumimos um codificador sistemático, de tal forma que $c_l^{j,1}(t) = u_l^j(t)$. O reticulado Λ construído via Construção A Levantada derivado deste código é dado pela equação (1).

Cada fonte é equipada com dois moduladores idênticos, $\mathcal{E} : \mathbb{F}_2^{nk} \rightarrow \mathbb{R}^{nk}$, cada um dos quais mapeia \mathbf{c}_l^j em uma palavra-código n -dimensional real $\mathbf{x}_l^j = \mathcal{E}(\mathbf{c}_l^j)$. Para realizar uma transmissão quaternária, o sinal transmitido é representado por $\mathbf{x}_l = \mathbf{x}_l^I + i\mathbf{x}_l^Q \in \mathbb{C}^{nk}$. O processo de codificação das mensagens na fonte S_l é representado na Figura 1.

A potência média de transmissão é dada por

$$P \triangleq \frac{1}{nk} E [||\mathbf{x}_l||^2],$$

e definimos $SNR = P/N_0$.

A taxa de mensagem \mathcal{R}_l de cada transmissor é dada pelo comprimento da sua mensagem normalizado pelo número de usos do canal: $\mathcal{R}_l = 2k/nk \log_2 2 = 2/n$ (medida em bits por símbolo complexo).

Os canais entre os nós fonte e intermediário são modelados como canais com desvanecimento em bloco do tipo Rayleigh. Assim, o sinal recebido pelo *relay* é dado por

$$\mathbf{y} = \sum_{l=1}^L h_l \mathbf{x}_l + \mathbf{z} \quad (2)$$

em que $\mathbf{x}_l \in \mathbb{C}^{nk}$ é o vetor transmitido, $h_l \in \mathbb{C}$ é o coeficiente de desvanecimento do canal entre a fonte S_l e o *relay*, para $l = 1, 2, \dots, L$, e \mathbf{z} é o vetor ruído Gaussiano complexo, com média zero e matriz de covariância $N_0 \mathbf{I}_{nk}$.

Assumimos que o *relay* tem informação completa sobre o estado do canal, ou seja, conhece o vetor h_l . Baseado no sinal recebido \mathbf{y} , nos ganhos h_l , e na SNR, o *relay* tenta obter uma estimativa da melhor combinação linear de mensagens: $\hat{\mathbf{u}}_R = \sum_{l=1}^L a_l \mathbf{u}_l$, em que $a_l \in \mathbb{Z}[i]$ é aquele que maximiza a taxa de transmissão [7], [6]. Este processo será descrito na Seção III.

III. ESTRATÉGIA COMPUTA-E-ENCAMINHA SOBRE ANÉIS

A estratégia CF de Nazer e Gastpar [7] explora a propriedade de que qualquer combinação linear de pontos de um reticulado pertence ao reticulado. Feng, Silva e Kschischang [6] observaram que o uso de CF com modulações maiores que a binária gera ambiguidades na decodificação da combinação linear quando esta é sobre um corpo finito, ao contrário do que acontece quando se considera um anel finito. Esse foi o procedimento adotado na Seção II deste trabalho.

Resumidamente, os nós fonte particionam seu vetor de mensagens $\mathbf{u}_l \in \mathbb{Z}_2[i]^k$, em $\mathbf{u}_l^I \in \mathbb{Z}_2^k$ e $\mathbf{u}_l^Q \in \mathbb{Z}_2^k$, e as mapeiam em palavras-código de \mathcal{C} . Em seguida, para minimizar a energia gasta na transmissão das palavras-código, somam-se vetores *dither*, $\mathbf{d}_l^I \in \mathbb{R}^{nk}$ e $\mathbf{d}_l^Q \in \mathbb{R}^{nk}$, às palavras-código de \mathcal{C} , gerando assim um reticulado deslocado. Os sinais transmitidos são então dados por

$$\mathbf{x}_l = (\mathbf{c}_l^I + \mathbf{d}_l^I) \bmod 2\mathbb{Z} + i(\mathbf{c}_l^Q + \mathbf{d}_l^Q) \bmod 2\mathbb{Z},$$

em que a operação $(x \bmod 2\mathbb{Z})$ retorna o elemento de menor magnitude de $(x + 2\mathbb{Z})$.

O *relay*, após receber o sinal dado pela equação (2), e antes de realizar o processo de decodificação, deve realizar os seguintes passos:

- 1) O sinal recebido é escalonado por um fator α , ou seja, calcula-se $\alpha\mathbf{y}$. O parâmetro α deve ser otimizado, em função dos ganhos dos canais, $\mathbf{h} = [h_1, \dots, h_L] \in \mathbb{C}^L$, do vetor da combinação linear $\mathbf{a} \in \mathbb{Z}[i]^L$, e do valor da SNR, e pode ser interpretado como uma tentativa de aproximar os coeficientes de canal de valores inteiros Gaussianos [6], possibilitando um melhor casamento entre estes coeficientes. O valor ótimo de α é dado pelo teorema que segue.

Teorema 1 ([7], [6]): Para um sistema PNC com vetor de desvanecimento, \mathbf{h} , vetor de coeficientes da combinação linear, \mathbf{a} , e SNR dada por SNR , a seguinte taxa computacional pode ser alcançada

$$R_{comp}(\mathbf{h}, \mathbf{a}) \triangleq \max_{\alpha \in \mathbb{C}} \log_2 \left(\frac{SNR}{\|\alpha\mathbf{h} - \mathbf{a}\|^2 SNR + |\alpha|^2} \right)$$

Esta é maximizada pelo valor ótimo de α , dado por

$$\alpha_{otm} = \frac{\mathbf{a}\mathbf{h}^H SNR}{\|\mathbf{h}\|^2 SNR + 1},$$

que resulta em

$$R_{comp}(\mathbf{h}, \mathbf{a}) = \log_2 \left(\frac{SNR}{\mathbf{a}\mathbf{M}\mathbf{a}^H} \right),$$

em que

$$\mathbf{M} = SNR\mathbf{I}_L - \frac{SNR^2}{SNR\|\mathbf{h}\|^2 + 1} \mathbf{h}\mathbf{h}^H$$

e \mathbf{I}_L é a matriz identidade $L \times L$.

Note que a minimização do fator $\mathbf{a}\mathbf{M}\mathbf{a}^H$, que aumenta a taxa computacional, R_{comp} , é equivalente ao problema de encontrar o menor vetor de um reticulado com matriz Gram \mathbf{M} [6].

- 2) O efeito do *dither* deve agora ser removido, resultando no sinal $\tilde{\mathbf{y}}$, que será a entrada para o decodificador:

$$\begin{aligned} \tilde{\mathbf{y}} &= \alpha\mathbf{y} - \sum_{l=1}^L a_l \mathbf{d}_l \quad (3) \\ &= \alpha \sum_{l=1}^L h_l \mathbf{x}_l + \alpha\mathbf{z} - \sum_{l=1}^L a_l \mathbf{d}_l \\ &= \underbrace{\sum_{l=1}^L a_l \bar{\mathbf{c}}_l \bmod 2\mathbb{Z}}_{\text{palavra-código, } \bar{\mathbf{c}}} + \underbrace{\sum_{l=1}^L (\alpha h_l - a_l) \mathbf{x}_l + \alpha\mathbf{z}}_{\text{ruído efetivo, } \mathbf{n}} \end{aligned}$$

Desse modo, o *relay* pode recuperar a combinação linear desejada, com probabilidade de erro arbitrariamente baixa, se as taxas associadas às mensagens envolvidas (isto é, aquelas com coeficientes diferentes de zero) forem menores do que a taxa computacional, ou seja, $\mathcal{R}_l < R_{comp}(\mathbf{h}, \mathbf{a})$.

Observe que a equação acima é equivalente à de uma transmissão em um canal ponto-a-ponto, na qual as mensagens são codificadas através de pontos de um reticulado e, ao serem transmitidas, são corrompidas por um ruído aditivo, que neste caso não é necessariamente Gaussiano. Note também que não é necessário realizar a decodificação individual das mensagens transmitidas. Na estratégia CF, decodifica-se $\bar{\mathbf{c}} = \sum_{l=1}^L a_l \bar{\mathbf{c}}_l \bmod 2\mathbb{Z}$ como uma palavra-código válida. E, devido às propriedades algébricas do esquema LNC, garante-se a existência de um homomorfismo $\varphi: \Lambda \rightarrow \mathbb{Z}_2[i]^k$, tal que

$$\varphi(\bar{\mathbf{c}}) = \hat{\mathbf{u}}_R = \sum_{l=1}^L a_l \mathbf{u}_l$$

ou seja, a combinação linear desejada é prontamente obtida.

IV. DECODIFICAÇÃO TURBO SOBRE INTEIROS GAUSSIANOS

O processo de decodificação turbo é realizado de forma independente para as componentes em fase e em quadratura do sinal $\tilde{\mathbf{y}}$, conforme apresentado na Figura 2. Depois de algumas manipulações algébricas, chega-se a

$$\tilde{\mathbf{y}}^I = \alpha^I \mathbf{y}^I - \alpha^Q \mathbf{y}^Q - \sum_{l=1}^L (a_l^I d_l^I - a_l^Q d_l^Q) \quad (4)$$

$$\tilde{\mathbf{y}}^I = \mathbf{c}^I + \mathbf{n}^I \quad (5)$$

e

$$\tilde{\mathbf{y}}^Q = \alpha^I \mathbf{y}^Q + \alpha^Q \mathbf{y}^I - \sum_{l=1}^L (a_l^I d_l^Q + a_l^Q d_l^I) \quad (6)$$

$$\tilde{\mathbf{y}}^Q = \mathbf{c}^Q + \mathbf{n}^Q, \quad (7)$$

em que

$$\mathbf{y}^I = \sum_{l=1}^L (h_l^I \mathbf{x}_l^I - h_l^Q \mathbf{x}_l^Q) + \mathbf{z}^I \quad (8)$$

$$\mathbf{y}^Q = \sum_{l=1}^L (h_l^I \mathbf{x}_l^Q + h_l^Q \mathbf{x}_l^I) + \mathbf{z}^Q \quad (9)$$

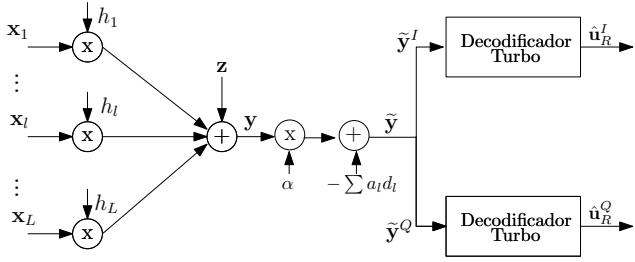


Fig. 2. Modelo do Decodificador.

e

$$\mathbf{c}^I = \left[\sum_{l=1}^L (a_l^I \mathbf{c}_l^I - a_l^Q \mathbf{c}_l^Q) \right] \text{ mod } 2\mathbb{Z} \quad (10)$$

$$\mathbf{c}^Q = \left[\sum_{l=1}^L (a_l^Q \mathbf{c}_l^I + a_l^I \mathbf{c}_l^Q) \right] \text{ mod } 2\mathbb{Z} \quad (11)$$

O processo de decodificação turbo deve ter a capacidade de minimizar a probabilidade de erro do bit $\mathbf{u}_R^j(t) = \sum_{l=1}^L a_l \mathbf{u}_l^j(t)$ no tempo t via decodificação turbo iterativa, para $j \in \{I, Q\}$. Utilizamos o algoritmo padrão de decodificação BCJR [14] para produzir, de forma independente, estimativas melhoradas das probabilidades *a priori* de $\hat{\mathbf{u}}_R^I(t)$ e $\hat{\mathbf{u}}_R^Q(t)$.

Estas estimativas são expressas através do cálculo de duas LLR's *a posteriori*, representando as componentes em fase e em quadratura do sinal, aqui representadas pelo índice j . Dessa forma, a LLR será dada por

$$\Lambda^j(u_R^j(t) | \tilde{\mathbf{y}}^j) = \ln \left(\frac{P(u_R^j(t) = 1 | \tilde{\mathbf{y}}^j)}{P(u_R^j(t) = 0 | \tilde{\mathbf{y}}^j)} \right). \quad (12)$$

O critério de decisão final é o usual, dado por:

$$\hat{u}_R^j(t) = \begin{cases} 0 & \text{se } \Lambda(u_R^j(t) | \tilde{\mathbf{y}}^j) \leq 0 \\ 1 & \text{caso contrário.} \end{cases}$$

A treliça decodificadora será a mesma utilizada pelas fontes. Porém, precisaremos ajustar o valor da variância do ruído efetivo, dado em (3), que não é necessariamente Gaussiano.

Os valores de $P(u_R^j(t) = 0 | \tilde{\mathbf{y}}^j)$ e $P(u_R^j(t) = 1 | \tilde{\mathbf{y}}^j)$ no tempo t são então calculados como

$$P(u_R^j(t) = i | \tilde{\mathbf{y}}^j) = \sum_{(l', l) \in \mathcal{T}_i} P(l', l | \tilde{\mathbf{y}}^j),$$

para $i \in \{0, 1\}$, em que \mathcal{T}_i representa o conjunto de transições de estado, (l', l) , na treliça do decodificador, provocadas por $u_R^j(t) = i$, e $P(l', l, \tilde{\mathbf{y}}^j) = \alpha_{t-1}(l') \cdot \gamma_t(\tilde{\mathbf{y}}^j, l', l) \cdot \beta_t(l)$ para todo $t = 1, \dots, k$. Os valores de α e β do algoritmo BCJR são obtidos da forma padrão [13]. Contudo, o cálculo de γ_t depende da saída atual do canal e das probabilidades de transição da treliça. Com isso, seu valor é dado por

$$\gamma_t(\tilde{\mathbf{y}}^j(t), l', l) = P(u_R^j(t)) \exp \left(- \frac{\sum_{m=1}^n d^2(\tilde{y}^{jm}(t), v^{jm}(t))}{2\sigma^2} \right)$$

em que $v^{jm}(t)$ são os elementos dos vetores dados pelas equações (10) e (11) associados ao rótulo da transição de estado correspondente (l', l) na treliça, $d(a, b)$ é a distância Euclidiana entre os pontos a e b no plano real, e σ^2 é a variância do ruído efetivo dado em (3). A probabilidade *a priori* de $u_R^j(t)$ é inicialmente setada como $P(u_R^j(t)) = \frac{1}{2}$, e é obtida e melhorada na saída do decodificador turbo.

A variância do ruído efetivo é obtida como

$$\sigma^2 = E[|\mathbf{n} - E[\mathbf{n}]|^2]$$

em que $E[\cdot]$ é o operador esperança matemática. O valor de $E[\mathbf{n}] = 0$ pois, como $\mathbf{z} \sim \mathcal{CN}(0, N_0)$ e $\mathbf{x}_l = \{\pm 0.5 \pm i0.5\}$, tem-se que $E[\mathbf{z}] = E[\mathbf{x}_l] = 0$. Dessa forma,

$$\sigma^2 = E[|\mathbf{n}|^2] \quad (13)$$

$$= \frac{1}{2} \sum_{l=1}^L |\alpha h_l - a_l|^2 + |\alpha|^2 N_0 \quad (14)$$

em que $1/2$ é a potência do sinal de dimensão complexa. Podemos ainda rearrumar a equação (14) da seguinte maneira

$$\begin{aligned} \sigma^2 &= N_0 SNR \sum_{l=1}^L |\alpha h_l - a_l|^2 + |\alpha|^2 N_0 \\ &= N_0 \left(SNR \sum_{l=1}^L |\alpha h_l - a_l|^2 + |\alpha|^2 \right) \\ &= N_0 \mathbf{a} \mathbf{M} \mathbf{a}^H \end{aligned}$$

V. RESULTADOS

O desempenho do algoritmo de codificação/decodificação turbo para LNC sobre inteiros Gaussianos foi avaliado através de simulações computacionais. Consideramos um sistema em que duas fontes S_1 e S_2 empregando o mesmo codificador turbo desejam enviar suas mensagens \mathbf{u}_1 e $\mathbf{u}_2 \in \mathbb{Z}_2[i]^k$ para um nó intermediário. Os codificadores convolucionais binários, recursivos e sistemáticos, utilizados para formar o código turbo possuem comprimento de memória $\nu = 2$, matriz geradora $\mathbf{G}(D) = [1 \ (1 + D^2)/(1 + D + D^2)]$ e taxa após punção de $1/2$.

Em conformidade com a Construção A Levantada, foram utilizados em cada fonte dois codificadores turbo em paralelo, um responsável pela codificação da componente em fase e o outro da componente em quadratura do vetor mensagem de tamanho k .

Nas simulações da taxa de erro de frame (FER, do inglês *frame error rate*), o tamanho do vetor mensagem por componente em fase ou em quadratura foi escolhido como 400 bits. As sequências dos coeficientes de canal foram geradas de forma independentes representando variáveis aleatórias Gaussianas complexas de potência unitária.

O número de iterações do decodificador turbo proposto, em todas as simulações realizadas neste trabalho, foi fixado em 6. Nas curvas de desempenho apresentadas nesta seção, foram realizados os devidos ajustes ($SNR \leftrightarrow E_b/N_0$) para os diferentes códigos em relação a suas taxas e às modulações utilizadas, para que, desse modo, uma comparação mais justa fosse realizada.

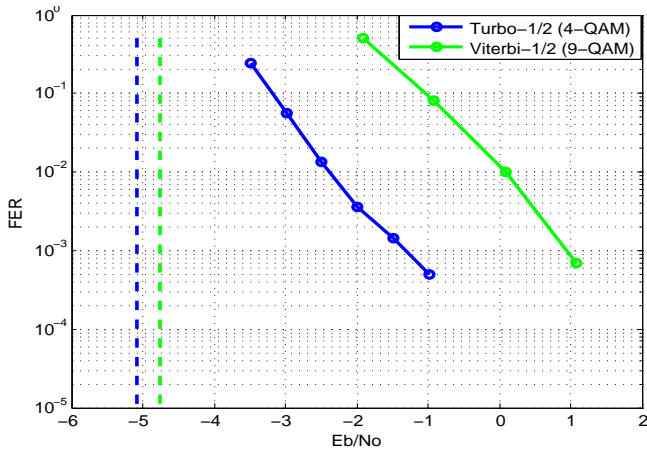


Fig. 3. Comparação de desempenho da taxa de erro de frame (FER) para $h_1 = -1, 17 + i2, 15$ e $h_2 = 1, 25 - i1, 63$.

Na Figura 3, o vetor de ganhos dos canais foi fixado em $h_1 = -1, 17 + i2, 15$ e $h_2 = 1, 25 - i1, 63$, os quais são os mesmos adotados em [15], [12], facilitando assim a comparação. A taxa de mensagem do esquema simulado é de 0,9950 bit/símbolo complexo (o valor um pouco menor do que 1 se deve aos bits de cauda, inseridos para fazerem os codificadores turbo voltarem ao estado zero). Para esta taxa, obtém-se do Teorema 1 que a E_b/N_0 mínima para uma probabilidade de erro arbitrariamente baixa é -5,09 dB. Este limite é indicado na figura por uma linha vertical tracejada azul.

Para fins de comparação, também é mostrada na Figura 3 a curva de FER do esquema LNC em [6], que faz uso de um código convolucional 9-ário de 81 estados e modulação 9-QAM. A taxa de mensagens neste caso é de $\frac{98}{100} \log_2(3)$ bits por símbolo complexo, resultando numa E_b/N_0 mínima (a partir do Teorema 1) de -4,77 dB. Este limite também é indicado na Figura 3 por uma linha vertical tracejada na mesma cor da curva de FER associada a este esquema.

Apesar de os dois esquemas (o aqui proposto e aquele proposto em [6]) não poderem ser comparados diretamente, por possuírem taxas de mensagens distintas, pode-se avaliar, a partir da Figura 3, o grande potencial do esquema LNC envolvendo códigos turbo binários propostos neste trabalho de se aproximar do limite teórico, com uma complexidade de decodificação aceitável.

Na simulação da Figura 4, consideramos mensagens de 400 bits por componente (I e Q), e os canais foram assumidos com desvanecimento em bloco do tipo Rayleigh. A FER para o esquema LNC em [6], denotado por "Viterbi-1/2 (9-QAM)", bem como a FER (probabilidade de *outage*) do esquema de Nazer e Gastpar, ou seja, a probabilidade do evento $\mathcal{R}_{mes} \geq \log_2(SNR/aMa^H)$, para as taxas de mensagem $\mathcal{R}_{mes} = 0,9950$ e $\frac{98}{100} \log_2(3)$ bits por símbolo complexo, também são mostradas na figura para o mesmo modelo de canal. Estas últimas devem servir como limitantes teóricos para a FER. Percebemos que o esquema proposto oferece um ganho em relação ao esquema em [6] de aproximadamente 4 dB para uma FER igual de 0,003, e está bem mais próximo do seu limite teórico do que o esquema em [6] está do seu.

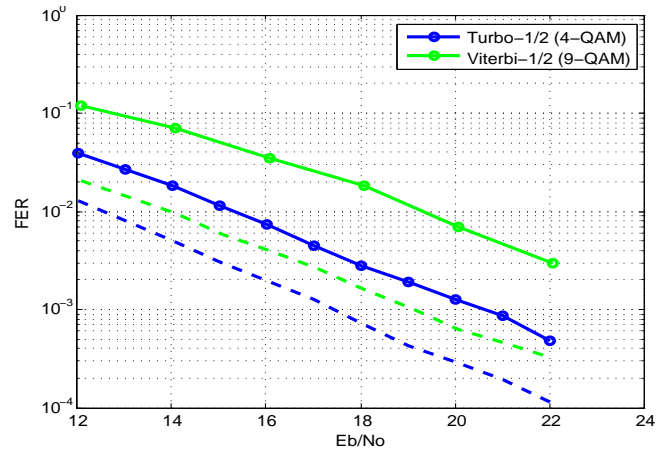


Fig. 4. Comparação de desempenho da taxa de erro de frame (FER) com canais sujeitos a desvanecimento Rayleigh.

VI. CONCLUSÕES

Neste trabalho, projetamos um esquema LNC que usa reticulados sobre inteiros Gaussianos, fazendo uso de códigos turbo binários. Simulações computacionais demonstraram o bom desempenho do esquema proposto, com a vantagem de a complexidade de decodificação ser relativamente baixa e independe do número de usuários presentes no sistema.

REFERÊNCIAS

- [1] R. Ahlswede, N. Cai, R. Li, and R. W. Yeung, "Network information flow," *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1204–1216, Jul. 2000.
- [2] S. Zhang, S. C. Liew, and P. P. Lam, "Hot Topic : Physical-Layer Network Coding," *Proceedings of the 12th annual international conference on Mobile computing and networking*, pp. 358–365, 2006.
- [3] P. Popovski and H. Yomo, "Bi-directional amplification of throughput in a wireless multi-hop network," *IEEE Vehicular Technology Conference*, vol. 2, pp. 588–593, May 2006.
- [4] B. Nazer and M. Gastpar, "Computing over multiple-access channels with connections to wireless network coding," *IEEE International Symposium on Information Theory*, pp. 1354–1358, Jul. 2006.
- [5] —, "Compute-and-forward: Harnessing interference through structured codes," *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6463 – 6486, Oct. 2011.
- [6] C. Feng, D. Silva, and F. R. Kschischang, "An algebraic approach to physical-layer network coding," 2012.
- [7] B. Nazer and M. Gastpar, "Reliable physical layer network coding," *Proceedings of the IEEE*, vol. 99, no. 3, pp. 438–460, Mar. 2011.
- [8] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*, 1998, no. 01.
- [9] M. Sadeghi and D. Panario, "Low density parity check lattices based on construction d cycle-free tanner graph," *DIMACS 2003*, vol. 68, pp. 86–90, 2003.
- [10] A. Sakzad, M. Sadeghi, and D. Panario, "Construction of turbo lattices," *Fiftieth Annual Allerton Conference*, pp. 14–21, Sep. 2010.
- [11] J.-C. Belfiore, "Lattice codes for the compute-and-forward protocol: The flatness factor," *IEEE Information Theory Workshop*, pp. 1–4, 2011.
- [12] N. E. Tunalı, K. R. Narayanan, J. J. Boutros, and Y.-c. Huang, "Lattices over eisenstein integers for compute-and-forward," *Fiftieth Annual Allerton Conference*, pp. 33–40, Oct. 2012.
- [13] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo-codes," *Proc. IEEE International Conference on Communications*, vol. 2, no. 1, pp. 1064–1070, 1993.
- [14] L. Bahl, J. Cocke, F. Jelinek, and J. Raviv, "Optimal decoding of linear codes for minimizing symbol error rate (Corresp.)," *IEEE Transactions on Information Theory*, vol. 20, no. 2, pp. 284–287, Mar. 1974.
- [15] C. Feng, D. Silva, and F. R. Kschischang, "An algebraic approach to physical-layer network coding," *IEEE Inter. Symp. Inf. Theory*, 2010.