Algumas Aplicações e Resultados Recentes em Codificação de Rede

Bartolomeu F. Uchôa-Filho[1], João Luiz Rebelatto[1,2], Roberto W. Nóbrega[1,3]

[1] Universidade Federal de Santas Catarina, Florianópolis, Brasil
[2] Universidade Tecnológica Federal do Paraná, Curitiba, Brasil
[3] *University of Toronto*, Canadá (doutorado-sanduíche)
{uchoa, jlrebelatto, rwnobrega}@eel.ufsc.br

Introdução

• Em **Codificação de rede** (Ahlswede *et al.* (2000)), os nodos intermediários da rede de dados combinam os pacotes recebidos, ao invés de apenas roteá-los.
• O código de rede é normalmente projetado para uma topologia específica (ver Figura 1), com o objetivo de se alcançar a máxima taxa de transferência de informação da rede, e permanece fixo ao longo do tempo.
• Na maioria dos casos, a codificação de rede é *coerente*, no sentido de que os nodos destino conhecem a topologia e a codificação de rede empregada.
• Neste trabalho, consideramos o cenário não-coerente e outro em que codificação de rede é usada para melhorar o desempenho da rede.

Codificação de Rede para Melhorar o Desempenho da Rede

• Em uma rede sem fio cooperativa de múltiplo acesso em que os usuários possuem informações independentes para transmitir para um destino em comum, pode-se dividir o processo de transmissão em duas fases: a ***fase de difusão***, em que os usuários difundem suas próprias mensagens (normalmente através de canais ortogonais), e a ***fase de cooperação***, em que os usuários retransmitem as mensagens de seus parceiros que foram "ouvidas" durante a fase de difusão.
• Um dos protocolos de retransmissão mais utilizados é o ***decodifica-e-encaminha (DAF — decode-and-forward)*** de Sendonaris *et al.* (2003) e Laneman *et al.* (2004).
• O DAF é ilustrado na Figura 2 para 2 usuários. A ordem de diversidade (de cooperação) é 2.
• Ao invés de simplesmente retransmitir os pacotes do parceiro, os usuários poderiam efetuar combinações lineares destes, caracterizando assim uma codificação de rede.
• Xiao e Skoglund (2010) propuseram os ***códigos de rede de diversidade (DNC)*** e mostraram que combinações lineares não-binárias são requeridas para que a ordem de diversidade do sistema seja aumentada.
• Um DNC sobre $\mathbb{F}_4$ é ilustrado na Figura 3 para 2 usuários. A ordem de diversidade (de cooperação) foi aumentada para 3.
• Rebelatto *et al.* (2010, 2011) perceberam que os pacotes potencialmente recebidos pelo destino, (I_1, I_2, I_1+I_2 e I_1+2I_2), podem ser vistos como uma palavra-código de um código de bloco com matriz geradora

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}$$

Os pacotes de informação I_1 e I_2 serão recuperados pelo destino se no máximo 2 pacotes (dos 4 transmitidos) forem apagados (distância mínima de Hamming 3).
• O ***DNC generalizado (GDNC)*** foi então proposto, através de uma associação entre códigos de rede e teoria da codificação clássica (Reed-Solomon codes): cada usuário transmite k_1 pacotes de informação na fase de difusão e k_2 pacotes (combinações lineares) na fase de cooperação.
• Uma melhor solução de compromisso entre diversidade de cooeperação e taxa de transmissão foi alcançada (ver simulação na Figura 4).

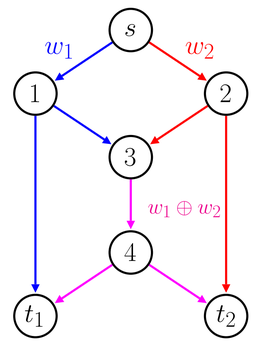
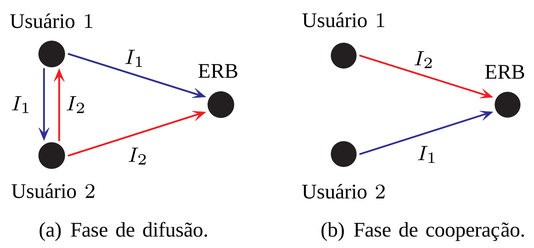
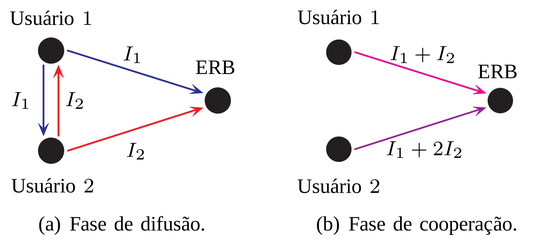


Figura 1: A rede borboleta (com fio).



(a) Fase de difusão. (b) Fase de cooperação.

Figura 2: Rede cooperativa DAF (sem fio) com 2 usuários.



(a) Fase de difusão. (b) Fase de cooperação.

Figura 3: Rede cooperativa (sem fio) com 2 usuários empregando codificação de rede linear sobre $\mathbb{F}_4$.

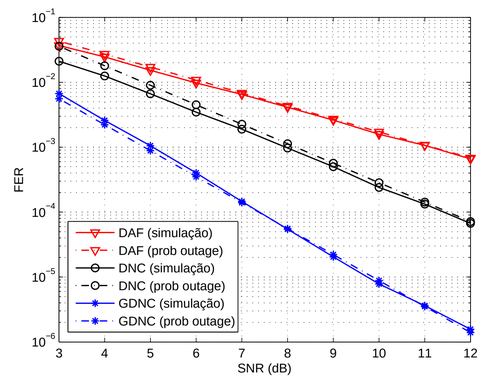


Figura 4: FER versus SNR (dB) para os esquemas DAF, DNC e GDNC ($k_1 = k_2 = 2$), todos com taxa 1/2.

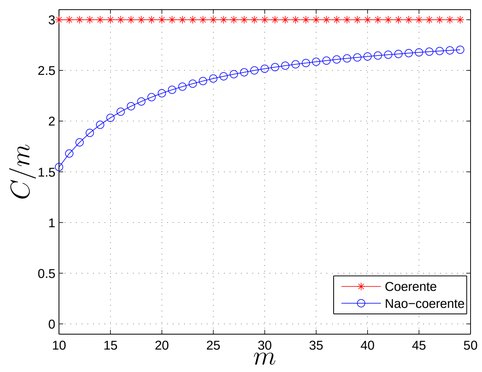


Figura 5: Limitantes (inferior e superior) sobre a capacidade do canal matricial $Y = GX$, para o corpo $\mathbb{F}_2$ e $n = 5$ pacotes injetados na rede, em função do tamanho do pacote m.

Codificação de Rede Não-Coerente e Códigos de Subespaço

Topologia variante no tempo

Problema:
• Nas técnicas DNC e GDNC, a codificação de rede é projetada e mantida fixa para a topologia específica, e é conhecida pelo destino.
• E se a topologia da rede variar com o tempo? Esta abordagem pode se tornar impraticável.
Soluções:
• Chou, Wu e Jain (2003) propuseram uso de um *header*, dando origem à ***codificação de rede não-coerente***.
• Ho *et al.* (2003,2006) propuseram a ***codificação de rede linear aleatória***: nodos realizam combinações lineares escolhendo independente e aleatoriamente coeficientes do corpo.

$$Prob(\text{codigo de rede bem sucedido}) \to 1 \text{ para } q \to \infty$$

• O funcionamento do sistema passa a ser totalmente descentralizado.
• Koetter e Kschischang (2008) propuseram ***codificação de subespaço***: como a rede realiza combinações lineares dos pacotes nela injetados, o subespaço vetorial gerado por tais pacotes é preservado.

Canal Matricial e Códigos de Subespaço

• Os pacotes transmitidos, $X \in \mathbb{F}_q^{n\times m}$, e os pacotes recebidos, $Y \in \mathbb{F}_q^{n\times m}$, (com apagamentos, porém sem erros) se relacionam por: $Y = GX$, em que $G \in \mathbb{F}_q^{n\times n}$ é a *matriz de transferência*, que depende da topologia da rede e do código de rede empregado.
• Koetter e Kschischang (2008) notaram que X e Y constituem duas bases geradoras distintas para o mesmo subespaço vetorial:

$$\langle Y \rangle = \langle GX \rangle = \langle X \rangle$$

em que $\langle A \rangle$ é o subespaço gerado pelas linhas da matriz A.
• A **informação é então associada ao subespaço vetorial**, e não ao conteúdo dos pacotes. Assim, as combinações lineares específicas realizadas pela rede são irrelevantes, e a informação pode ser recuperada no destino sem qualquer conhecimento da topologia ou da codificação de rede realizada.
• Devido a possíveis apagamentos ocorridos nos canais ou a eventuais combinações lineares infelizes, G pode não ter posto completo.
• Um ***código de subespaço*** é um subconjunto não-vazio de $\mathcal{P}(\mathbb{F}_q^m, n)$, o conjunto de todos os subespaços vetoriais de $\mathbb{F}_q^m$ de dimensão n ou menos.

Modelo de erro probabilístico

• Considera-se um canal discreto sem memória:

$$(\mathcal{X} = \mathbb{F}_q^{m\times n}, p_G(\cdot), \mathcal{Y} = \mathbb{F}_q^{m\times n})$$

• **Resultado** [Nóbrega *et al.* (2011)]: Seja $m \geq n$ e $r \triangleq posto(G)$ a variável aleatória que r epresenta o posto de G. Então a capacidade C do canal satisfaz

$$\mathrm{E}\left[\log_q \frac{\begin{bmatrix} m \\ r \end{bmatrix}_q}{\begin{bmatrix} n \\ r \end{bmatrix}_q}\right] \leq C \leq \mathrm{E}\left[mr\right],$$

em que $\begin{bmatrix} n \\ k \end{bmatrix}$ é o coeficiente Gaussiano.
• A Figura 5 mostra os limitantes para $q = 2$, $n = 5$ e $p(r) = (0, \frac{1}{10}, \frac{1}{5}, \frac{2}{5}, \frac{1}{5}, \frac{1}{10})$.