Revista de Engenharia e Pesquisa Aplicada, Volume 2, Número 1, 2016

Códigos Corretores de Erro Aplicados a Redes de Sensores sem Fio

Aguiar, R. M. D.
Escola Politécnica de Pernambuco
Universidade de Pernambuco
50.720-001 - Recife, Brasil
rodrigodonato@yahoo.com.br

Cunha, D. C.
Escola Politécnica de Pernambuco
Universidade de Pernambuco
50.720-001 - Recife, Brasil
dccunha@upe.poli.br

Resumo *Em comunicações envolvendo redes de sensores sem fio, erros introduzidos devido à natureza ruidosa do canal são comuns. A utilização de códigos corretores de erro tem o objetivo de proteger a informação transmitida contra os erros de canal, proporcionando um melhor desempenho ao sistema. Além disso, o uso de códigos corretores reduz o consumo de energia dos componentes da rede, aumentando a vida útil de sua estrutura física e diminuindo o custo de sua manutenção. O presente trabalho se propõe a analisar alguns esquemas tradicionais de codificação e controle de erros aplicados a redes de sensores sem fio.*

Abstract *On communications by sensor wireless networks, errors introduced due to the noise nature of the channel are usual. The use of error correcting codes is intended to protect the information against channel errors, providing the system a better performance. Moreover, the use of error correcting codes, reduce energy consumption by the network components, increasing its hardware service life and reducing maintenance costs. This work proposes to analyze some major schemes of error control codes applied to wireless sensor networks.*

1 Introdução

Boa parte dos códigos corretores de erros se baseia em um mesmo princípio básico: a adição de redundância à informação com o objetivo de corrigir erros que possam ocorrer no processo de gravação ou transmissão de dados [1]. No contexto das comunicações, a informação transmitida pode ser degenerada pelo ruído ao longo do meio de transmissão. Daí, o receptor deve verificar o quanto esta informação foi afetada e tentar recuperar a informação original. Em geral, quanto mais redundância se adiciona à informação, mais proteção se obtém contra o ruído. Dentre as classes de códigos utilizadas em sistemas de comunicação, os códigos de bloco lineares constituem uma das principais técnicas de codificação e controle de erros. Esta classe de códigos é empregada em diversas modalidades de sistemas de comunicação, como, por exemplo, as redes de sensores sem fio (RSSF) [2].

Uma das formas de se empregar códigos corretores de erros em RSSFs denomina-se codificação cooperativa [3]. Na realidade, o uso de códigos corretores de erros neste contexto aborda apenas uma parte do sistema de comunicação que utiliza uma técnica conhecida como comunicação cooperativa. A idéia básica da comunicação cooperativa consiste no fato de que usuários móveis, portadores de uma antena simples, possam compartilhar suas antenas de tal modo que um ambiente virtual de múltiplas antenas possa ser criado [4].

O objetivo da comunicação cooperativa é fornecer diversidade ao sistema e com isso, permitir a melhoria de desempenho com a redução da probabilidade de erro.

Diante do exposto, o presente trabalho se destina a estudar esquemas de codificação de canal aplicados a sistemas de comunicação cooperativa com o objetivo de propor alguma modificação na intenção de obter melhorias de desempenho frente aos resultados conhecidos na literatura.

2 Redes de Sensores sem Fio

Uma RSSF pode ser definida dentro de contextos diversos. No contexto das comunicações, podemos entendê-la como um conjunto de sensores implantados numa rede *ad hoc*, i.e., uma rede onde os dispositivos são parte da rede somente quanto estão suficientemente próximos de modo que seja possível realizar transmissões entre eles.

Outro modo de entender as RSSF é como um conjunto de nós individuais (sensores) que operam sozinhos, mas que podem formar uma rede com o objetivo de juntar as informações individuais de cada sensor.

A melhoria no desempenho desse tipo de rede é interessante, e tem motivado um volume grande de pesquisas na área, pois pode significar uma redução no consumo de energia dos sensores. Como em muitas aplicações a substituição das baterias dos nós pode ser impraticável, é interessante que a vida útil delas aumente.

Outro aspecto relacionado ao consumo energético por parte dos sensores consiste no número de restransmissões em sistemas de comunicação que utilizam a técnica ARQ (*Automatic Repet reQuest*). Nesses sistemas um nó da rede (sensor) pode receber um pacote de dados corrompido devido ao ruído e decidir descartar a informação e exigir uma nova transmissão.

Diminuir a probabilidade de erros na transmissão de dados nesse tipo de rede é essencial para melhorar a qualidade dos serviços tecnológicos que dependem das mesmas, e a codificação de canal apresenta-se como uma altenativa de baixo custo.

3 Modelos de Canal

O canal, meio físico por onde a transmissão dos dados ocorre, será descrito por um modelo matemático estatístico e nesse caso discreto. A modelagem estatística considera a entrada (sinal enviado) como uma variável aleatória (VA) e a saída (sinal recebido) como uma versão ruídosa da VA da entrada.

O modulador e o demodulador só possuem dois simbolos disponíveis para representar a mensagem, normalmente os símbolos utilizados são “1” e “0”. A emissão destes símbolos, de cada *bit*, é independente, i.e, não depende dos símbolos anteriores. Essa propriedade é que caracteriza o canal como sem memória.

Nesse trabalho são considerados dois tipos de canal, com duas características típicas de sistemas físicos reais. Um canal com ruído AWGN e outro com ruído AWGN e desvanecimento Rayleigh.

3.1 Estilos

O movimento térmico de moléculas, em especial dos elétrons nos elementos dissipadores presentes em um circuito, dá origem a um tipo de ruído muito comum em sistemas de comunicação. Um modelo teórico simples considera que a potência do ruído possui uma distribuição espectral uniforme, ou seja, considera que uma fonte térmica de ruído emana uma quantidade idêntica de potência por unidade de largura da banda.

O modelo matemático que se enquadra nessas caracteristicas é o gaussiano, descrito estatisticamente pela seguinte equação:

$$p(n) = \frac{1}{\sigma\sqrt{2\pi}} exp\left[-\frac{1}{2}\left(\frac{n}{\sigma}\right)^2\right] \quad (1)$$

em que σ_2 é a variância de n.

O comportamento da VA acima pode ser visualizado na Fig.1**,** onde estão plotadas a função densidade de probabilidade (pdf, *probability density function*) definida pela equação (1) e um histograma obtido de uma amostragem feita no computador.

A forma mais simples de considerar o ruído branco gaussiano (branco em analogia à luz branca que possui partes iguais de todas as frequências do espectro visivel da radiação eletromagnética) é a aditiva, onde o ruído é simplesmete adicionado ao sinal. O ruído gaussiano branco aditivo é conhecido pela sua sigla em inglês, AWGN – *Additive White Gaussian Noise*.

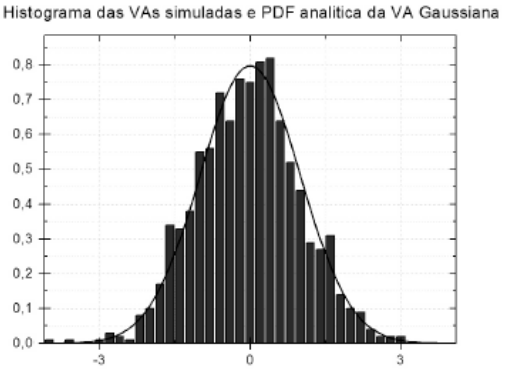

Fig. 1 – Histograma e PDF das VAs Gaussianas.

3.2 Canal com Ruído AWGN e Desvanecimento Rayleigh

Entendido os aspectos básicos do canal com ruído AWGN podemos acrescentar outro aspecto presente em transmissões de dados de uma forma geral. Desvanecimento é um fenômeno comum em transmissões guiadas ou por *broadcast* que significa a perda de potência do sinal na medida em que este se propaga através do canal.

Dentre os modelos de desvanecimento o de Rayleigh foi utilizado, que assim como o ruído gaussiano, possui espectro amplo. O desvanecimento é introduzido no sistema de comunicação simulado como uma atenuação no sinal transmitido.

Na Fig.2 pode-se observar a pdf da distribuição Rayleigh e o resultado de uma amostragem das variáveis simuladas no computador.

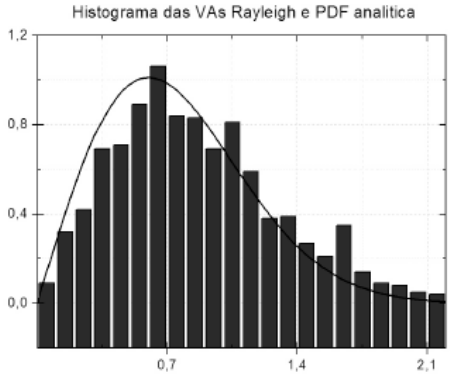

Fig.2 – Histograma e PDF das VAs Rayleigh

4 Esquemas de Codificação

Os códigos corretores de erros são introduzidos para diminuir a probabilidade de erro na transmissão do sinal. A adição de redundância na mensagem é um recurso comumente utilizado para essa finalidade. O codificador de canal (presente no transmissor) aceita bits de mensagem e adiciona redundância de acordo com uma regra bem definida. O decodificador explora a redundância para decidir quais bits foram de fato transmitidos.

A literatura considera basicamente duas classes de codificação: a de bloco e a convolucional [1]. A diferença entre as duas é a presença ou ausência de memória. O estudo se concentrará em códigos de bloco lineares.

Nos códigos de bloco C(*n,k*), o codificador aceita grupos sucessivos de *k bits de mensagem* e adiciona *(n – k) bits de redundância* obdecendo uma regra especifica, que relaciona os (n –k) bits de *mensagem* aos *k* de *paridade*. Cada bloco de *n* bits forma então uma palavra-código. No caso particular onde duas palavras códigos quaisquer puderem ser somadas em aritmética módulo-2 para produzir uma terceira palavra código, este é dito ser linear. A restrição para aritmética módulo-2 se aplica somente a sistemas binários, o essencial a um código de bloco linear é que, escolhida a aritmética, a soma de duas palavras códigos ainda seja uma palavra código do mesmo código.

4.1 Códigos de Hamming

Um dos códigos de bloco mais utilizados é o código de Hamming, que são os códigos que possuem as seguintes características:

$$n = 2^m - 1$$
$$k = 2^m - m - 1$$
$$n - k = m \text{ , } com\ m \geq 3$$

Dessa forma vários códigos podem ser gerados como, por exemplo, C1(7, 4) e C2(15, 11).

De forma resumida, podemos entender o processo até agora da seguinte forma: O codificador utiliza a matriz geradora para construir as palavras código e o decodificador a transposta da matriz de verificação de paridade. Para entender como ocorre a correção de erros o conceito de *síndrome* deve ser introduzido. O vetor de síndrome é definido da seguinte forma:

$$\mathbf{s} = \mathbf{r}\mathbf{H}^{\mathbf{T}}$$

que depende somente do vetor padrão de erro[5]:

$$\mathbf{s} = \mathbf{e}\mathbf{H}^{\mathbf{T}}$$

Outro conceito importante é o de distância mínima que determina a capacidade de correção de um código, que por sua vez depende da introdução dos conceitos de distância de Hamming e Peso de Hamming, que seguem:

-Distância de Hamming: A distância de Hamming é definida entre dois vetores como sendo o número de posições onde os dois vetores diferem.

-Peso de Hamming: É a distância de Hamming entre um vetor qualquer e o vetor nulo.

A distância mínima de um código é então definida como sendo a menor distância de Hamming entre todos os pares de palavras código.

Um código é capaz de corrigir até *t* erros de uma palavra recebida, desde que a distância mínima entre as palavras seja, pelo menos, *2t+1*.

O processo de correção depende do cálculo da construção do *arranjo padrão*, que pode ser entendida como uma tabela onde todos os possíveis vetores **r** são listados numa ordem que permita identificar qual o vetor **x** mais provável. Essa ordenação é determinada pelo cálculo da síndrome e pela capacidade de correção do código em particular.

4.2 Códigos de BCH

Os códigos BCH (*Bose, Chaundhuri e Hocquenghem*) constituem uma importante e poderosa classe de códigos corretores de erro *cíclicos*. Códigos cíclicos podem ser entendidos como uma subclasse de códigos de blocos lineares que possuem a seguinte propriedade: Ao aplicar uma pemutação cíclica em uma palavra código, i.e., deslocar os componentes do vetor palavra código em uma posição, a nova palavra continua sendo uma palavra do código.

Para qualquer inteiro positivo *m* ($m \geq 3$) e *t* ($t < 2^{m-1}$ 1), então existe um código binário BCH com os seguintes parâmetros:

$$n = 2^m - 1$$
$$n - k \leq mt$$
$$d_{min} \geq 2t + 1$$

Este código será capaz de corrigir até *t* erros.

A decodificação de um código BCH tem início de forma idêntica à decodificação de um código de Hamming, ou seja, pelo cálculo da síndrome **s**. No entanto, no caso de códigos BCH, não se obtém uma solução direta para a síndrome e algoritmos de decodificação são utilizados para resolver as equações obtidas.

Outra diferença está na formulação algébrica ao invés da comumente utilizada matricial.

O interesse é em encontrar a síndrome correspondente ao padrão de erro mais provável, que no caso dos códigos BCH é equivalente ao problema de encontrar as raízaes de um polinônimo **σ(X)**, denominado polinômio localizador de erro, numa tradução livre do inglês *error-location polynomial*.

O procedimento mencionado anteriormente pode ser sumariamente descrito como:

i. Calcular a síndrome a partir do polinômio **r(X)** correspondente a mensagem ruidosa recebida.

ii. Determinar o polinômio localizador de erro **σ(X)** a partir das equações obtidas no cálculo da síndrome.

iii. Determinar a localização dos erros através do cálculo das raízaes de **σ(X)**.

O passo ii), de determinar **σ(X),** é o mais complexo e exige o uso de técnicas especiais.

Uma das técnicas mais conhecidas é o algoritmo iterativo de Berlekamp-Massey [5].

5 Resultados

Este trabalho considerou canais com ruído AWGN e desvanecimento Rayleigh, utilizando codificação de Hamming e BCH, verificando-se um melhor desempenho desse último frente ao de Hamming. A modulação utilizada foi BPSK antipodal e para as simulações dos sistemas o método de Monte Carlo.

Na Fig.3 observamos o resultado da simulação do sistema para o canal AWGN com os dois tipos de codificação mencionados anteriormente.

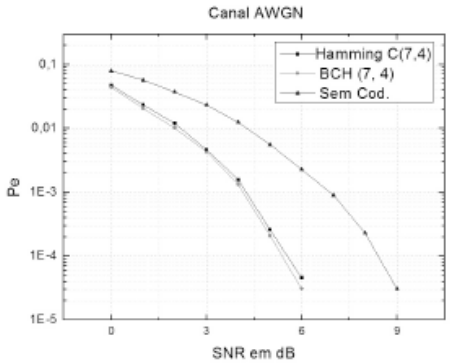

Fig. 3 – Curvas de desempenho para o canal AWGN.

Pela análise da Fig.3 podemos observar a melhora no desempenho dos canais codificados em relação à transmissão não codificada. Entre os dois códigos utilizados observa-se uma sensível superioridade no desempenho do código BCH. Isso se deve ao código escolhido BCH(7,4) que possuí a mesma capacidade de correção do código de Hamming escolhido, C1(7,4).

Na **Fig. 4** podemos observar o comportamento de um canal AWGN com desvanecimento Rayleigh sem codificação e com codificação BCH(7,4).

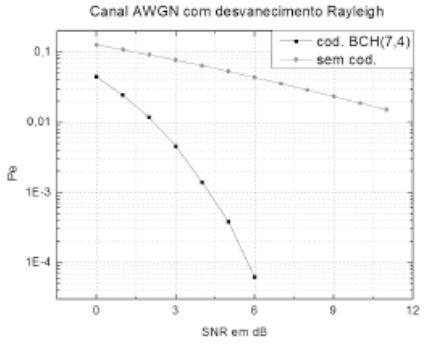

Fig. 4 – Curva de desempenho canal AWGN com desvanecimento Rayleigh

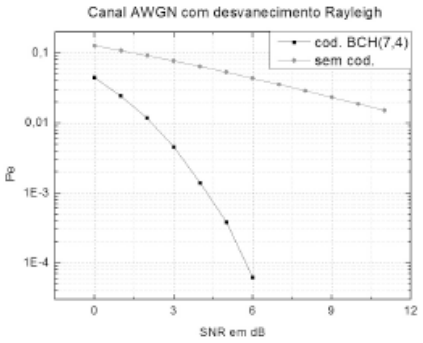

Fig. 4 – Curva de desempenho canal AWGN com desvanecimento Rayleigh

Pode-se observar que com a introdução do desvanecimento Rayleigh a curva de desempenho do canal não codificado exige valores maiores de energia (valores grandes de SNR) para permitir probabilidades de erro baixas.

6 Expectativas

Fundamentada a base teórica, a aplicação de outros esquemas de codificação a RSSFs seguirá com o estudo dos códigos turbo produto e seus algoritmos de decodificação iterativa.

Referências

[1] Zaragoza, R.H.M. *The Art of Error-Correcting Coding*. John Wiley, 2002.

[2] Akyildiz, I. F., SU, W., Sankarasubramanian, Y. and Cayirci, E. "Wireless Sensor Networks: A Survey,"*Computer Networks (Elsevier) Journal*, vol. 38, n. 4, pp. 393- 422, Mar 2002.

[3] Rossi, P. S.; Petropulu, A. P.; Palmieri, F.; Ianello, G. "Distributed Linear Block Coding for Cooperative Wireless Communications". *IEEE Signal Processing Letters*, vol. 14, n. 10, pp. 673 - 676, Out 2007.

[4] Meier, J., Thompson, J. S., "Cooperative Diversity in Wireless Networks". IEE International Conference on 3G and Beyond, Jun 2007.

[5] Lin, S., Costello, D.J. Jr; *"Error Control Coding – 2nd Ed."* Pearson – Prentice Hall, 2004.