**Eline Alves Santos**

# *Redes de Sensores com Codificação BCH Distribuída*

Campina Grande – PB

Abril / 2009

Universidade Federal de Campina Grande
Centro de Engenharia Elétrica e Informática
Programa de Pós-Graduação em Engenharia Elétrica

**Eline Alves Santos**

# *Redes de Sensores com Codificação BCH Distribuída*

Dissertação apresentada à Coordenação de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Campina Grande para a obtenção do título de Mestre em Engenharia Elétrica

Orientador:

Prof. Dr. Francisco Marcos de Assis

Co-orientador:

Prof. Dr. Edmar Candeia Gurjão

Abril de 2009

**FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL DA UFCG**

S237r
2009 Santos, Eline Alves
Redes de sensores com codificação BCH distribuída / Eline Alves Santos. — Campina Grande, 2009.
49f.

Dissertação (Mestrado em Engenharia Elétrica) – Universidade Federal de Campina Grande, Centro de Engenharia Elétrica e Informática.
Referências.
Orientadores: Prof. Dr. Francisco Marcos de Assis e Prof. Dr. Edmar Candeia Gurjão.

1. Classificação Distribuída. 2. Redes de Sensores sem Fio. 3. Codificação. I. Titulo.

CDU – 621.391:004.772.4(043)

**REDES DE SENSORES COM CODIFICAÇÃO BCH DISTRIBUÍDA**

**ELINE ALVES SANTOS**

Dissertação Aprovada em 13.04.2009

**FRANCISCO MARCOS DE ASSIS, Dr., UFCG**
**Orientador**

**EDMAR CANDEIA GURJÃO, D.Sc., UFCG**
**Orientador**

**BRUNO BARBOSA ALBERT, D.Sc., UFCG**
**Componente da Banca**

**LUIZ FELIPE DE QUEIROZ SILVEIRA, D.Sc., CEFET-RN**
**Componente da Banca**

CAMPINA GRANDE - PB
ABRIL - 2009

*Dedico esta dissertação a meus pais,*
*Obed Santos e Edneuza Alves dos Santos.*

# *Agradecimentos*

Dedico meus sinceros agradecimentos:

– Aos professores Francisco Marcos de Assis e Edmar Candeia Gurjão, pela orientação e incentivo;

– A todos os alunos do Laboratório de Instrumentação e Metrologia Científicas do Departamento de Engenharia Elétrica da UFCG;

– A meu marido Alan, pela compreensão e pela muita paciência;

– Aos funcionários da Universidade Federal de Campina Grande, em especial a Ângela e Suênia;

– Ao Conselho Nacional de Desenvolvimento Científico e Tecnológico, pelo apoio.

# *Resumo*

Redes de sensores sem fio são em geral compostas de uma grande quantidade de nós sensores distribuídos em uma determinada região com o objetivo de detectar e transmitir uma característica física do ambiente. Em um problema de classificação distribuída baseada nas observações de nós sensores, cada nó sensor com base em sua observação envia sua decisão a um nó sensor (centro de fusão) responsável por tomar a decisão final por uma das possíveis classes. As decisões enviadas pelos nós sensores podem ser corrompidas por ruído, uma alternativa para minimizar este problema é utilizar códigos corretores de erro. Em trabalhos anteriores foi proposto um sistema de classificação distribuída utilizando códigos corretores de erro em que para cada uma das $M$ classes ou hipóteses foi associada uma palavra código de comprimento igual a $N$, em que $N$ é o número de sensores, e cada sensor envia apenas um símbolo da palavra código associada à hipótese por ele observada. Para esta abordagem as palavras códigos foram sido obtidas por uma busca aleatória entre todas as palavras de tamanho $N$. Neste trabalho propõe-se o uso de códigos de blocos lineares para obtenção das $M$ palavras código, mais especificamente códigos BCH (Bose, Chaudhuri e Hockquegueim). Esta abordagem permite que a decodificação seja feita utilizando-se algoritmos de decodificação algébrica bem conhecidos. Em particular, com esta nova abordagem é possível evitar uma decodificação exaustiva através do uso de tabela, necessária em trabalhos anteriores, quando o número de hipóteses é muito grande, o que não é possível para palavras código selecionadas aleatoriamente. Foi mostrado através de simulações que esta abordagem baseada no BCH apresenta um desempenho similar à abordagem anterior.

# *Abstract*

Wireless sensor networks are usually composed of a large number of sensor nodes densely deployed to monitor an environment. In a distributed classification problem, each sensor node sends, based on its observation, a decision to the sensor node (fusion center) responsible for making the final classification decision. The decisions transmitted by the sensor nodes may be corrupted by noise, an alternative is to use error correcting codes. In previous works, a distributed classification fusion approach using error correcting codes has been proposed, where each one of the $M$ classes or hypotheses is associated to a codeword with blocklength $N$, where $N$ is the number of sensor nodes, each sensor node sends only a symbol of the codeword associated with the hypothesis that corresponds to its observation. In this approach the codewords are obtained by random search in the set of binary strings of length $N$, where $N$ is the number of sensors. In this work it is proposed the use of classical block codes, more specifically BCH (Bose, Chaudhuri e Hockquegueim) codes, to obtain these codewords. The proposed approach allows tailoring decoding algorithms supported by well known algebraic decoding algorithms. In particular, with the new approach it is possible to avoid a massive table look-up-based decoding for a large number of hypotheses, what cannot be achieved with random selected codewords. It is showed by simulation that algebraic code-based classification performance is similar to the performance of previous random search-based classification.

# *Sumário*

# *Lista de Figuras*

# *Introdução*

O desenvolvimento de pequenos dispositivos de baixo custo dotados de uma unidade de sensoriamento e com capacidades limitadas de processamento e comunicação, os chamados nós sensores, permitiu o surgimento das Redes de Sensores.

Redes de sensores sem fio são em geral compostas de uma grande quantidade de nós sensores distribuídos em uma determinada região com o objetivo de detectar e transmitir uma característica física do ambiente (AKYILDIZ et al., 2002). O leque de aplicações para este tipo de rede é grande indo desde monitoramento ambiental à aplicações militares como vigilância, e por isso têm atraído a atenção de vários pesquisadores, além de apresentar uma grande quantidade de desafios, entre eles o fato destas redes possuírem fontes de energia limitada, este é talvez um dos principais desafios no projeto de uma rede de sensores sem fio.

Outro ponto importante é que muitas vezes as observações realizadas pelos sensores são bastante ruidosas tanto em função da qualidade dos sensores como pelo ambiente em que eles se encontram. Desta forma as redes de sensores devem ser tolerantes a falhas, pois em ambientes hostis alguns nós podem funcionar de maneira inadequada ou mesmo serem danificados completamente (WANG et al., 2005).

Neste trabalho será abordado o problema da classificação de um fenômeno tendo como base as obervações obtidas por uma rede de sensores distribuída em um ambiente ruidoso. Muitos estudos têm sido realizados para o caso em que só existem duas hipóteses, nesse trabalho consideraremos $M$ hipóteses. Quando se faz uma extensão para múltiplas hipóteses frequentemente assume-se que para cada observação local o nó sensor transmite pelo menos $\log_2 M$ bits para serem avaliados no centro de fusão. Entretanto neste trabalho cada sensor envia apenas um bit, e a decisão sobre uma das $M$ hipóteses será feita com base nos bits enviados por todos os sensores.

Em (YAO et al., 2007) propõe-se uma sistema de classificação de múltiplas hipóteses a partir de mensagens binárias de sensores. Considerando o envio dessas mensagens via um canal com ruído aditivo Gaussiano, a tolerância a falhas é conseguida com a utilização de códigos corretores de erro. A idéia consiste em relacionar uma palavra

código a cada hipótese que o fenômeno possa assumir. Então cada nó sensor após realizar sua observação envia um bit da palavra código correspondente à hipótese que ele assumiu como verdadeira.

Este trabalho propõe um sistema de classificação utilizando códigos algébricos para redes de sensores sem fio que seja tolerante a falhas. A motivação para a utilização dos códigos algébricos é que no método de (YAO et al., 2007), onde os códigos utilizados não possuem nenhuma estrutura, a decodificação só pode ser feita por comparação da palavra recebida com as palavras pertencentes ao código enquanto que nos códigos aqui utilizados pode-se obter o mesmo desempenho com a possibilidade de realizar decodificação algébrica, o que facilita o projeto do centro de fusão.

O texto está dividido da seguinte forma, no Capítulo 1 é feita uma introdução sobre redes de sensores, no Capítulo 2 são definidos os códigos corretores de erro dando ênfase aos códigos aplicados no trabalho, no Capítulo 3 é feita uma revisão sobre a aplicação de códigos corretores de erro a redes de sensores, no Capítulo 4 descreve-se o trabalho realizado e os resultados obtidos e finalmente no Capítulo 5 são tecidas conclusões e apresentadas perspectivas para trabalhos futuros.

# 1 Redes de Sensores

## 1.1 Introdução

Avanços tecnológicos nas áreas de Comunicação sem Fio e Eletrônica têm viabilizado o desenvolvimento de pequenos dispositivos com capacidade de sensoriamento, processamento de dados e comunicação, os chamados nós sensores ou ainda sensores "inteligentes". A produção em larga escala destes dispositivos vem barateando o seu custo, sendo possível pensar em aplicações de sensoriamento remoto com centenas ou mesmo milhares de nós sensores (AKYILDIZ et al., 2002).

O conjunto de vários nós sensores densamente distribuídos em uma região de interesse, com o objetivo de coletar, processar, armazenar e transmitir dados acerca de um ambiente, formam uma rede de sensores sem fio (RSSF). Devido ao grande leque de aplicações e desafios a serem superados, as redes de sensores têm despertado o interesse da comunidade científica.

Embora já existam muitos algoritmos e protocolos desenvolvidos para redes sem fio tradicionais, representadas pelas redes de computadores, as redes de sensores sem fio apresentam algumas diferenças com relação às redes tradicionais que impedem a aplicação direta destes algoritmos. As principais diferenças são:

- Topologia Dinâmica
- Alta densidade de nós
- Nós propensos a falha
- Sérias restrições de *hardware* e *software*
- Fontes de energia limitada

Neste capítulo é feita uma revisão sobre as redes de sensores sem fio com ênfase nos componentes, características, aplicações e medidas de desempenho. Para tanto, o

restante deste capítulo está organizado da seguinte maneira: na Seção 1.2 serão descritas as principais características de um nó sensor; na Seção 1.3 serão dados alguns exemplos de aplicações para RSSFs; a Seção 1.4 abordará algumas métricas de avaliação de desempenho de uma RSSF; por fim, na Seção 1.5 serão feitas algumas considerações finais.

## 1.2 O nó sensor

Os nós sensores são dispositivos com capacidades limitadas de sensoriamento, processamento e comunicação, entretanto um esforço colaborativo entre eles permite a realização de uma tarefa maior, como por exemplo monitorar uma grande área geográfica. Para que as redes de sensores sejam viáveis os nós sensores devem apresentar as seguintes características:

- baixo custo, uma vez que uma das vantagens das RSSFs é justamente realizar um sensoriamento distribuído com uma grande quantidade de nós;
- baixo consumo de energia, pois em muitas aplicações a substituição de baterias pode ser inviável tanto em função dos nós se encontrarem em um ambiente hostil quanto pela quantidade de baterias a serem trocadas;
- dimensões pequenas, isto facilita a dispersão dos nós em uma região de interesse e em aplicações militares dificulta a detecção dos nós por inimigos.

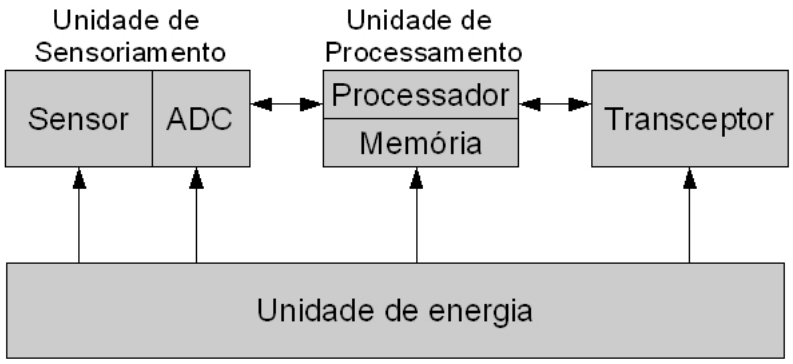


Figura 1: Componentes de um nó sensor

Na Figura 1[1] encontra-se a estrutura básica de um nó sensor: uma unidade de sensoriamento, uma unidade de processamento, um transceptor e uma unidade de energia.

[1]Esta figura foi adaptada de (AKYILDIZ et al., 2002)

A unidade de sensoriamento é composta pelo conversor analógico-digital (ADC, do inglês *Analog to Digital Converter*) e por um ou mais sensores (acústico, sísmico, infravermelho, temperatura, pressão, umidade etc). A unidade de processamento é responsável por tratar os dados recebidos dos sensores e gerenciar as tarefas de colaboração com os outros nós.

O transceptor é o componente do nó responsável pela comunicação. A comunicação sem fio pode ser óptica, por infra-vermelho ou por rádio-frequência (RF). A comunicação óptica requer menor quantidade de energia por bit transmitido que a comunicação por RF e não necessita de área física para instalação de antena, entretanto transmissor e receptor devem estar alinhados e isto é inviável para muitas aplicações. A comunicação por infra-vermelho também não necessita de antena e os transceptores são baratos, porém apresenta baixas taxas de transmissão se comparada a RF e também necessita de visada direta entre transmissores e receptores.

A maioria dos nós sensores utilizam comunicação via RF. Esta tem a vantagem de não necessitar que transmissor e receptor estejam alinhados, mas para o desenvolvimento de nós sensores muito pequenos o tamanho da antena pode tornar inviável o uso de um transceptor RF.

Normalmente, as informações captadas pelos sensores são transmitidas a um elemento da rede que tem maior capacidade de processamento e disponibilidade de energia onde ocorre o processamento dessas informações. Esse elemento é denominado de centro de fusão.

A comunicação da rede de sensores com outras redes é feita utilizando-se nós *gateways*. Estes interceptam as mensagens que percorrem a rede de sensores para encaminhá-las por uma rede como a Internet até um computador que está executando uma aplicação.

A unidade de energia é um dos componentes mais importantes do nó sensor, pois está relacionada com o tempo de vida útil desse nó. Em geral, utilizam-se baterias não recarregáveis como fonte de energia dos nós sensores e como dito antes, a substituição da bateria pode ser inviável. Existem diferentes tecnologias de bateria, a escolha deve ser baseada em características como volume, condições de temperatura e capacidade inicial, de acordo com os requisitos da aplicação a que a rede será destinada. É possível também ter fontes de energias contínuas como células solares e geradores piezoelétricos.

Dependendo da aplicação os nós podem ainda ser equipados com vários outros componentes. Atuadores podem ser necessários para que seja possível controlar parâmetros do ambiente monitorado. Em algumas aplicações e para alguns protocolos de roteamento

a localização do nó sensor pode ser uma informação importante, nesses casos o nó é equipado com um sistema de localização.

As dimensões físicas dos nós sensores irão depender do tipo de aplicação e da tecnologia de fabricação de seus componentes. As RSSFs podem ser homogêneas ou heterogêneas em relação aos tipos, dimensões e funcionalidades dos nós sensores.

Na Figura 2 encontram-se exemplos de alguns nós sensores resultantes de pesquisas em algumas instituições, como o Smart Dust (SMART..., 2009) da Universidade da Califórnia, Berkeley, *μAMPS* (*μ-Adptative Multi-domain Power Aware Sensor*) do Massachusetts Institute of Technology (MIT) (UAMPS, 2009), PushPin também do MIT (PUSHPIN, 2009) e o Micaz comercializado pela Crossbow (CROSSBOW, 2009).

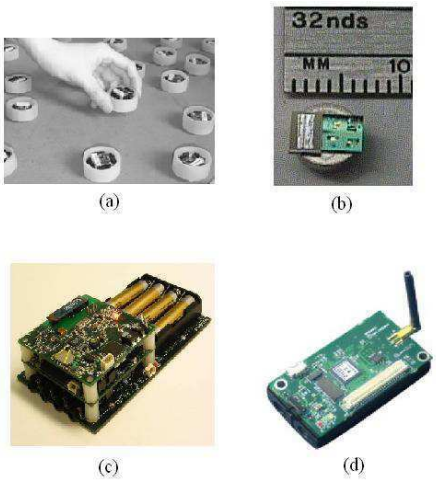


Figura 2: Exemplos de nós sensores. (a) Pushpin, (b) Smart Dust, (c) uAMPS e (d) Micaz.

## 1.3 Aplicações

A possibilidade de realizar um sensoriamento densamente distribuído tornam as RSSFs atraentes a uma grande diversidade de aplicações. As RSSFs são indicadas para monitorar ambientes que sejam de difícil acesso ou perigosos, tais como o fundo do oceano, vizinhanças de atividades vulcânicas, territórios inimigos, áreas de desastres e campos de atividade nuclear.

Segundo (AGRE; CLARE, 2000) algumas das vantagens das RSSFs em relação a sistemas com sensor centralizado, como imagem de satélite e radares terrestre são:

- permitir maior tolerância a falhas através de um alto nível de redundância;

- permitir cobertura de grandes áreas de monitoramento através da união de pequenas áreas cobertas individualmente por cada nó;
- melhor qualidade de sensoriamento utilizando vários tipos de sensores;
- caracterização contínua do fenômeno;
- possibilidade de colocar os sensores muito próximos aos objetos de interesse.

A seguir serão dados exemplos de algumas aplicações. Para efeito de organização agrupamos os exemplos em aplicações ambientais, médicas, militares e outras.[2]

***Aplicações ambientais***

Em aplicações ambientais as RSSFs podem ser utilizadas para monitorar diversas variáveis tais como temperatura, umidade e pressão em ambientes como lagos, rios e florestas, outra possibilidade é o monitoramento e rastreamento de animais. Alguns exemplos são detecção de incêndio em florestas (YU; WANG; MENG, 2005), detecção de enchentes, agricultura de precisão, monitoramento de animais como o projeto ZebraNet da Universidade de Princeton para rastrear o movimento de zebras na África (THE..., 2009). Na Figura 3 tem-se o exemplo de um conjunto de nós sensores desenvolvido pela Crosbow (CROSSBOW, 2009) para aplicações ambientais.

Figura 3: Aplicações ambientais. Fonte: (CROSSBOW, 2009)

***Aplicações militares***

Rápida instalação, auto-organização e tolerância a falhas são características das redes de sensores que as qualificam para serem empregadas em aplicações militares como sistemas militares de comando, controle, comunicações, computação, inteligência, vigilância (YAN; HE; STANKOVIC, 2003), reconhecimento e mira (ILYAS; MAHGOUB, 2005).

Em aplicações militares os requisitos de segurança são fundamentais, é preciso garantir que a informação seja confidencial e que a rede não irá ser descoberta. Algumas medidas

[2]Esta classificação não é rígida e pode ser feita de outra forma.

que podem ser tomadas para alcançar esse objetivo são: codificar as mensagens; diminuir o alcance das transmissões para evitar escutas clandestinas; reduzir as dimensões dos nós sensores e utilizar nós móveis.

***Aplicações médicas***

Algumas das aplicações médicas possíveis para redes de sensores sem fio estão na criação de interfaces para deficientes físicos, monitoramento de dados fisiológicos de pacientes, diagnóstico e administração de drogas para pacientes (AKYILDIZ et al., 2002; ILYAS; MAHGOUB, 2005).

***Outras aplicações***

Algumas aplicações possíveis não citadas anteriormente são em automação doméstica, ambientes inteligentes, monitoramento de tráfego de veículos, entre outras. Na indústria tem-se aplicações na instrumentação das fábricas e no monitoramento da qualidade dos produtos. Na engenharia civil pode ser aplicada ao monitoramento de fadiga de materiais e em estruturas inteligentes com sensores embutidos.

## 1.4 Métricas de desempenho

Esta seção abordará as métricas de avaliação usadas para avaliar o desempenho de uma rede de sensores. Algumas das principais métricas de avaliação são tempo de vida da rede, cobertura, custo e facilidade de implementação, tempo de resposta e segurança (HILL, 2003).

Em geral, existe uma relação de interdependência entre elas, ou seja, muitas vezes é necessário admitir um desempenho pior em relação a uma determinada métrica para se conseguir um desempenho melhor em relação a outra. A aplicação à que a rede se destina é que definirá as métricas mais importantes no momento do projeto e desenvolvimento da rede.

***Tempo de vida da rede***

O tempo de vida esperado é crítico para qualquer rede de sensores. Em algumas aplicações pode ser mais interessante saber o tempo de vida mínimo do que o tempo de vida médio. O principal fator limitante do tempo de vida da rede é a fonte de energia, em geral limitada. Toda a rede deve ser projetada para consumir a menor quantidade de energia possível. Um dos componentes do nó sensor que consome mais energia é o rádio, transmitir 1Kb a uma distância de 100 metros custa tanto em termos de consumo

de energia quanto executar 3 milhões de instruções em um processador de propósito geral (POTTIE; KAISER, 2000).

***Cobertura***

O problema da cobertura esta relacionado à qualidade do monitoramento na área. A área de cobertura de uma RSSF corresponde a região formada pela junção das áreas cobertas pelo dispositivo de sensoriamento de cada nó da rede e o seu cálculo está relacionado com o raio de alcance dos nós que se encontram ativos na rede. Pode-se definir a área de cobertura como uma medida da habilidade da rede em detectar e observar um elemento na área de monitoramento. Para garantir uma maior área de cobertura uma possibilidade é aumentar o número de nós, mas isto também aumenta o custo da rede.

***Custo e facilidade de instalação***

Uma vez que normalmente uma RSSF é formada por uma grande quantidade de nós sensores, o custo de cada nó deve ser baixo para que o custo total da rede não seja maior do que utilizar sensores tradicionais e a rede seja então viável.

Outra característica importante que a rede deve possuir é facilidade de instalação, para que uma pessoa não treinada possa facilmente implementar um RSSF, outro ponto é que o custo de instalação da rede também influi no custo total da rede. Idealmente as RSSFs devem ser autônomas e autoconfiguráveis.

***Tempo de resposta***

O tempo de resposta da rede pode ser crítico em várias aplicações, um alarme deve ser sinalizado imediatamente quando surge um intruso em aplicações de vigilância. Os nós devem ser capazes de responder prontamente quando ocorre um evento importante. Um baixo tempo de resposta conflita com o tempo de vida da rede, uma vez que uma das técnicas para se estender o tempo de vida é permitir que o rádio funcione apenas por breves períodos a cada ciclo de tempo.

***Segurança***

A segurança da informação fornecida pela rede é um requisito importante em aplicações militares, mas não se restringe a elas. Por exemplo, as informações de uma RSSF utilizada para monitorar ambientes domésticos e comerciais pode indicar se há atividade ou não em um ambiente indicando o melhor momento para uma invasão. É importante garantir que as informações sejam confidenciais e que não seja possível a introdução de mensagens falsas, para isso pode-se utilizar técnicas de codificação e autenticação de men-

sagens, mas geralmente isto acarreta em um aumento no número de bits transmitidos e consequentemente no consumo de energia.

## 1.5 Considerações finais

As RSSFs têm grande potencial de aplicação, mas para que se tornem realidade alguns desafios ainda precisam ser vencidos. Um dos desafios é prolongar o tempo de vida da rede. A comunicação via rádio utilizada pelas redes é a principal responsável pelo gasto de energia de um nó sensor, por isso faz-se necessário uma compressão local dos dados nos nós sensores.

Outro questão a ser considerada no projeto de redes de sensores sem fio é a capacidade de tolerância a falhas, alguns nós podem ser danificados ou sofrer interferências do ambiente, entretanto, isto não deve comprometer o funcionamento adequado da rede.

O uso de códigos corretores de erro é uma alternativa interessante para o aumento da tolerância a falhas de uma rede de sensores, neste caso, uma atenção especial deve ser dada às taxas dos códigos utilizados de modo a não comprometer a demanda de energia por bit transmitido.

# 2 Códigos Corretores de Erro

## 2.1 Introdução

Um código corretor de erros é basicamente uma forma de acrescentar de forma controlada redundância à informação que se queira transmitir ou armazenar gerando uma palavra código. Como essa palavra código ao ser transmitida pode sofrer alterações devido às intempéries do meio de transmissão, dependendo do código utilizado, pode-se detectar e até corrigir os erros e recuperar a informação original pela retirada da redundância.

Neste capítulo serão apresentados alguns conceitos sobre codificação para controle de erros, mais especificamente os relacionados à classe dos códigos de bloco, visto que um representante dessa classe de códigos será utilizada no trabalho aqui desenvolvido. Admite-se que o leitor possui conhecimentos prévios de álgebra e aritmética de corpos finitos, para maiores detalhes sobre codificação para controle de erros e sobre álgebra e aritmética de corpos finitos, veja (BLAHUT, 1983; WICKER, 1995).

## 2.2 Códigos de bloco

Considere $\mathbb{F}_q$ um corpo finito de $q$ elementos. Um código de bloco $\mathbf{C}$ consiste em um conjunto de $\mathbf{M}$ sequências $\mathbf{c} = (c_0, c_1, ..., c_{n-1})$, com $c_i \in \mathbb{F}_q$, de comprimento $n$, chamadas de palavras código. Quando $q = 2$ trata-se de um código binário e os símbolos são chamados de bits, quando $q > 2$ o código é dito não binário. Um código de bloco construído desta forma é referido como um código $(n, k)$.

O processo de codificação para esta classe de códigos consiste em mapear univocamente blocos de símbolos de informação de comprimento $k$ em palavras código de comprimento $n$, com $k < n$.

**Definição 1** *A taxa de informação de um código de bloco binário é a relação entre o número de bits de um bloco de informação e o número de bits da palavra código corre-*

*spondente, ou seja:*

$$R = \frac{k}{n}$$

A taxa de um código indica sua eficiência. Quanto maior o valor de $R$, tendo como máximo 1, mais eficiente é o código pois insere-se menos redundância. Entretanto, a afirmativa anterior só é válida se o código tem capacidade de detecção e correção de erros alta.

O *peso de Hamming* $w(c)$ de uma palavra código $c$ é o número de coordenadas não nulas desta palavra. O menor peso de Hamming de todas as palavras de um código, excetuando a palavra código nula (toda de zeros), corresponde ao peso mínimo $w_{min}$ de um código.

**Definição 2** *Dadas duas palavras-código* $\boldsymbol{u}$ *e* $\boldsymbol{v}$ *pertencentes a* $\mathbb{F}_q^n$*, a distância de Hamming d(*$\boldsymbol{u}$*,*$\boldsymbol{v}$*) entre elas corresponde ao número de posições nas quais elas diferem.*

$$d(u, v) = |\{i : u_i \neq v_i, 1 \leq i \leq n\}|$$

A distância de Hamming fornece informação sobre a proximidade entre as palavras do código. Seja um código C, a distância mínima $d$ de C é a menor distância de Hamming entre todas as palavras do código, $d = \min\{d(u, v) : u, v \in C \text{ e } u \neq v\}$.

**Definição 3** *Dado um código* $\boldsymbol{C}$ *com símbolos em* $\mathbb{F}_q^n$*, serão ditos parâmetros do código* $\boldsymbol{C}$ *os inteiros* $(n, k, d)$*, em que k é a dimensão de C, d a distância mínima e n é o comprimento do código.*

A distância mínima de um código é importante para determinar a sua capacidade de detecção e correção de erros. Dado um código $\mathbf{C}$ com distância mínima $d$, então $\mathbf{C}$ pode corrigir até $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ e detectar até $d - 1$ erros (VILLELA, 2002).

Os códigos de bloco podem ser classificados como lineares ou não lineares. Neste trabalho utilizaremos os códigos de bloco lineares, apresentados a seguir.

### 2.2.1 Códigos de bloco lineares

A classe dos códigos de bloco lineares é uma das mais utilizadas na prática, pois contém a maioria dos bons códigos conhecidos. A estrutura imposta pelos espaços vetoriais propiciam meios estruturados para a construção de codificadores e decodificadores.

**Definição 4** *Um código $C \subset \mathbb{F}_q^n$ é um código linear se for um subespaço vetorial de $\mathbb{F}_q^n$.*

Uma vez que um código linear é subespaço vetorial, este é um conjunto de palavras-código (vetores) não vazio que contém a palavra-código nula (vetor nulo), tal que o resultado da soma de duas palavras-código como também o produto por um escalar (elemento de $\mathbb{F}_q$) é uma palavra-código. O peso mínimo de um código linear é igual a distância mínima $d$ do código, $d = w_{min}(c)$ (BLAHUT, 1983).

Sendo $k$ a dimensão do código $\mathbf{C}$, qualquer conjunto de $k$ vetores linearmente independentes formam uma base para o código $\mathbf{C}$. Esses $k$ vetores podem ser usados como linhas para formar uma matriz $G_{k\times n}$, chamada de matriz geradora do código. Qualquer palavra-código $\mathbf{c}$ pode ser representada por uma combinação linear das linhas de $\mathbf{G}$. A operação de codificação de uma palavra $\mathbf{i}$ em uma palavra-código pode ser representada por:

$$\mathbf{c} = \mathbf{i}G$$

Por exemplo, para um código binário (5,3) pode-se ter como matriz geradora:

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

A palavra [1 1 0], por exemplo, é codificada como [0 1 0 0 1].

Através de operações elementares nas linhas e permutações de colunas, pode-se colocar uma matriz geradora $\mathbf{G}$ na *forma padrão* ou *sistemática* $G = [I_k|P]$, em que $I_k$ é a matriz identidade $k \times k$ e $\mathbf{P}$ é uma matriz $k \times (n-k)$. A matriz do exemplo anterior colocada na *forma sistemática* fica como segue.

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Para a matriz geradora $\mathbf{G}$ dada acima, a palavra [1 1 0] é codificada como [1 1 0 1 1]. Note que quando a matriz geradora encontra-se na forma sistemática os primeiros k símbolos da palavra-código corresponde aos símbolos da palavra de informação.

Associado a cada código linear $C(n,k)$, existe um subespaço ortogonal $C^{\perp}$ que contém todos os vetores ortogonais a $\mathbf{C}$. Este subespaço é também um código linear e é chamado de código dual de $\mathbf{C}$. O código dual $C^{\perp}$ tem dimensão $n-k$ e matriz geradora $H_{n-k\times n}$,

denominada matriz de paridade. Assim sendo, as palavras-código de $\mathbf{C}$, são ortogonais as linhas de $H_{n-k\times n}$, ou seja:

$$cH^T = 0$$

A matriz de paridade na forma sistemática é dada por $H = [-P^T|I_{n-k}]$, a matriz de paridade relacionada à matriz geradora $\mathbf{G}$ do exemplo é dada por:

$$H = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Caso uma palavra código $c_1$ seja transmitida e o canal de comunicação insira um erro $e$ a palavra recebida será $r = c_1 + e$. No receptor pode-se fazer

$$r = (c_1 + e)H^T = c_1H^T + eH^T = eH^T \tag{2.1}$$

então pode-se no receptor detectar o erro desde que $w(e) \leq d_{min} - 1$, pois caso $w(e) = d_{min}$ a soma $c_1 + e = c_2$ é uma palavra código, será recebida e considerada como válida, e assim o erro não será detectado.

Existem diversos códigos de bloco lineares conhecidos, dentre eles: o código de Hamming, Reed-Solomon e BCH. Na próxima seção os códigos cíclicos (um caso especial de códigos lineares) serão descritos, e na seção seguinte serão descritos os códigos BCH que pertencem a classe dos códigos cíclicos e que serão utilizados neste trabalho.

### 2.2.2 Códigos Cíclicos

**Definição 5** *Um código linear $C \subset \mathbb{F}_q^n$ será chamado de código cíclico se, para todo $\boldsymbol{c} = (c_0, c_1, ..., c_{n-1})$ pertencente a $\boldsymbol{C}$, o vetor $(c_{n-1}, c_0, ..., c_{n-2})$ pertence a $\boldsymbol{C}$.*

Os códigos cíclicos formam uma classe de códigos lineares que possui bons algoritmos de codificação e de decodificação. Uma importante característica dos códigos cíclicos é a possibilidade de uma representação polinomial, isto será explicado a seguir. Considere a seguinte matriz de paridade para um código de Hamming(7,4):

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Pode-se identificar as colunas de **H** com elementos de $\mathbb{F}_8$. Para uma representação polinomial dos elementos de $\mathbb{F}_8$, faça o primeiro componente de cada coluna corresponder ao coeficiente de $z^0$, o segundo ao coeficiente de $z^1$ e o terceiro ao coeficiente de $z^2$. Considerando que foi utilizado o polinômio primitivo $p(z) = z^3 + z + 1$ para construção de $\mathbb{F}_8$, e $\alpha$ é elemento primitivo, então **H** pode ser reescrita como:

$$H = \begin{bmatrix} \alpha^0 & \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \end{bmatrix}$$

A matriz de paridade **H**, tornou-se uma matriz $1 \times 7$ com elementos em $\mathbb{F}_8$. As palavras códigos podem então ser definidas como um vetor de $\mathbb{F}_2$ que na extensão $\mathbb{F}_8$ o produto $cH^T = 0$.

Este produto pode ser reescrito como:

$$\sum_{i=0}^{6} c_i \alpha^i = 0$$

A expressão acima motiva a representação das palavras códigos como um polinômio do tipo:

$$c(x) = \sum_{i=0}^{n-1} c_i x^i = 0$$

A operação de multiplicação da palavra-código pela matriz de paridade torna-se uma operação de avaliação de $c(x)$ em $x = \alpha$. O polinômio $c(x)$ será uma palavra-código se e somente se $c(\alpha) = 0$.

Generalizando, para uma matriz de paridade **H** de um código linear com símbolos em $\mathbb{F}_q$, $n$ colunas e $n - k$ linhas, cada grupo de $m$ linhas pode ser interpretada como uma única linha com elementos em $\mathbb{F}_{q^m}$, esta matriz passa a ser uma matriz de ordem $r \times n$ com elementos em $\mathbb{F}_{q^m}$ em que $r = (n-1)/m$.

Para o caso especial dos códigos cíclicos a matriz de paridade pode ser escrita como:

$$H = \begin{bmatrix} \gamma_1^0 & \gamma_1^1 & \cdots & \gamma_1^{n-2} & \gamma_1^{n-1} \\ \gamma_2^0 & \gamma_2^1 & \cdots & \gamma_2^{n-2} & \gamma_2^{n-1} \\ \vdots & & & & \vdots \\ \gamma_r^0 & \gamma_r^1 & \cdots & \gamma_r^{n-2} & \gamma_r^{n-1} \end{bmatrix}$$

em que $\gamma_j \in \mathbb{F}_{q^m}$ para $j = 1, 2, ..., r$, e $n = q^m - 1$.

Devido a esta forma especial de $\mathbf{H}$, a equação $cH^T = 0$ pode ser escrita na forma:

$$\sum_{i=0}^{n-1} c_i \gamma_j^i = 0 \quad j = 1, ..., r.$$

Assim, cada palavra-código pode ser vista como um polinômio $c(x)$ com zeros em $\gamma_1, ..., \gamma_r$. O código pode ser definido como o conjunto de polinômios $c(x) = \sum_{i=0}^{n-1} c_i x^i$ de grau menor ou igual a $n-1$ que satisfaz $c(\gamma_j) = 0$ para $j = 1, ..., r$.

Um subconjunto no anel $\mathbb{F}_q[x]/(x^n - 1)$ é um código cíclico $\mathbf{C}$ se e somente se satisfaz as seguintes propriedades (BLAHUT, 1983):

1. $\mathbf{C}$ é um subgrupo de $\mathbb{F}_q[x]/(x^n - 1)$ sobre a adição.
2. Se $c(x) \in \mathbf{C}$, e $a(x) \in \mathbb{F}_q[x]/(x^n - 1)$, então $R_{x^n-1}[a(x)c(x)] \in \mathbf{C}$

em que $R_{d(x)}[b(x)]$ representa o resto ou resíduo de $b(x)$ quando dividido por $d(x)$.

**Definição 6** *O polinômio gerador de um código cíclico $\boldsymbol{C}$ é o polinômio de menor grau $g(x) \in \boldsymbol{C}$*

Um código cíclico é o conjunto de todos os múltiplos do polinômio gerador $g(x)$ por polinômios de grau menor ou igual a $k-1$ (BLAHUT, 1983). Sendo a palavra de informação representada pelo polinômio $i(x)$ com grau menor ou igual a $k-1$ e $g(x)$ o polinômio gerador com grau igual $n-k$. Uma regra simples de codificação é dada por:

$$c(x) = i(x)g(x)$$

**Definição 7** *O polinômio de teste de paridade de um código cíclico com polinômio gerador $g(x)$ é um polinômio $h(x)$ tal que $x^n - 1 = g(x)h(x)$.*

Note que para qualquer palavra código, $h(x)c(x)$ módulo $(x^n - 1)$ é igual a zero.

Existe um código cíclico de comprimento $n$ com polinômio gerador $g(x)$ se e somente se $g(x)$ divide $x^n - 1$ (BLAHUT, 1983). Exemplo, considere os códigos binários de comprimento n=7, para encontrar o polinômio gerador devemos fatorar $x^7 - 1$ em polinômios primos:

$$x^7 - 1 = (x+1)(x^3 + x + 1)(x^3 + x^2 + 1)$$

Qualquer combinação dos polinômios primos obtidos pela fatoração de pode gerar um polinômio gerador, ou seja, existem $2^3 = 8$ polinômios geradores possíveis, desses dois são triviais ($g(x) = x^7 - 1$, com k=0 e $g(x) = 1$ com k=7). Para o exemplo aqui, façamos:

$$\begin{aligned} g(x) &= (x+1)(x^3+x+1) \\ &= x^4+x^3+x^2+1 \end{aligned}$$

O polinômio de paridade será:

$$\begin{aligned} h(x) &= \frac{x^7-1}{g(x)} \\ &= (x^3+x^2+1) \end{aligned}$$

Os parâmetros do código serão $n = 7$, $k = n - deg(g(x)) = 4$, os polinômios de informação serão da seguinte forma:

$$i(x) = i_0 + i_1 x + i_2 x^2.$$

Seja $i(x) = x + x^2$, a palavra código correspondente será:

$$\begin{aligned} c(x) &= (x+x^2)(1+x^2+x^3+x^4) \\ &= (x+x^2+x^3+x^6) \end{aligned}$$

A sequência transmitida será c=(0,1,1,1,0,0,1).

### 2.2.3 Códigos BCH

Os códigos BCH (Bose, Chaudhuri e Hockquegueim) são códigos largamente utilizados que pertencem a classe dos códigos cíclicos. Antes de defini-los, vamos começar lembrando que o polinômio gerador de um código cíclico pode ser expresso como:

$$g(x) = MMC[f_1(x), f_2(x), \ldots, f_r(x)]$$

em que $f_1(x), \ldots, f_r(x)$ são os zeros de g(x) e MMC significa mínimo múltiplo comum.

Seja $c(x)$ a palavra-código transmitida e $e(x)$ o polinômio de erro, a palavra recebida é o polinômio $v(x) = c(x) + e(x) \in \mathbb{F}_q[x]$.

Avaliando-se $v(x)$ em $\mathbb{F}_{q^m}$ para o conjunto de zeros de $g(x)$, $\{\gamma_1, \ldots, \gamma_r\}$, tem-se:

$$\begin{aligned} v(\gamma_j) &= c(\gamma_j) + e(\gamma_j) \\ &= e(\gamma_j) \end{aligned}$$

ou seja,

$$v(\gamma_j) = \sum_{i=0}^{n-1} e_i \gamma_j^i, \ j = 1, 2, ..., r$$

Este conjunto de $r$ equações pode ser resolvido para $e_i$, e então o padrão de erro pode ser determinado. Escolhe-se os $\gamma_j$ de maneira que este conjunto de $r$ equações possa ser resolvido para $e_i$, sempre que o erro tiver no máximo $t$ componentes não nulos.

**Definição 8** *Define-se a j-ésima síndrome da palavra recebida $v(x)$ para um código cíclico com polinômio gerador $g(x)$ que tem $\gamma_1, \ldots, \gamma_r$ como zeros, por*

$$S_j = v(\gamma_j) \ j = 1, 2, ..., r$$

Escolhendo-se $\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{2t}$ como zeros de $g(x)$, em que $\alpha$ é um elemento primitivo, pode-se determinar $t$ erros através das síndromes (BLAHUT, 1983).

Pode-se construir um código BCH com comprimento de bloco $n = q^m - 1$, para algum inteiro $m$ e capacidade de correção de $t$ erros da seguinte forma:

1. Escolha um polinômio primo de grau $m$ para gerar $\mathbb{F}_{q^m}$.
2. Encontre $f_j(x)$, o polinômio mínimo de $\alpha^j$ para $j = 1, ..., 2t$.
3. $g(x) = MMC[f_1(x), f_2(x), \ldots, f_r(x)]$

Códigos BCH construídos desta forma são chamados de código BCH primitivos. Note que os códigos são construídos para valores determinados de $n$ e $t$, o valor de $k$ é conhecido depois que $g(x)$ é encontrado através da relação $\deg(g(x)) = n - k$. Pode-se encontrar na literatura tabelas com polinômios geradores para vários parâmetros de códigos BCH como em (PROAKIS, 1983). Algumas vezes o código BCH assim construído pode corrigir mais que $t$ erros, e então $d = 2t + 1$ é chamada de distância projetada do código, a distância mínima pode ser maior.

A seguir será enunciada uma definição formal e mais geral para os códigos BCH.

**Definição 9** *Sejam dados $q$ e $m$, e seja $\beta$ um elemento de $\mathbb{F}_{q^m}$ de ordem $n$. Então para algum inteiro positivo $t$ e para algum inteiro $j_0$, o código BCH correspondente é o código cíclico de comprimento $n$ com polinômio gerador*

$$g(x) = MMC[f_{j_0}(x), f_{j_0+1}(x), \ldots, f_{j_0+2t-1}(x)]$$

*em que $f_j(x)$ é o polinômio mínimo de $\beta^j$.*

Exemplo: Considere um código BCH com comprimento de bloco igual a 15 e capacidade de correção $t = 2$ erros. Suponha que foi utilizado o polinômio primitivo $p(z) = z^4 + z + 1$ para construir $\mathbb{F}_{2^4}$, então o polinômio gerador é obtido da seguinte forma:

$$\begin{aligned} g(x) &= MMC[f_1(x), f_2(x), f_3(x), f_4(x)] \\ &= MMC[x^4 + x + 1, x^4 + x + 1, x^4 + x^3 + x^2 + x + 1, x^4 + x + 1] \\ &= (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1) \\ &= x^8 + x^7 + x^6 + x^4 + 1 \end{aligned}$$

Como o grau de $g(x)$ é 8, $n - k = 8$ e então $k = 7$.

## 2.3 Considerações Finais

Neste capítulo foram apresentados alguns conceitos sobre codificação para controle de erros, que serão úteis mais adiante. No capítulo seguinte será feita uma revisão sobre uma aplicação de códigos corretores de erro a redes de sensores, e então no capítulo 4 será proposto a utilização de códigos BCH para redes de sensores.

# 3 *Códigos Aplicados a Redes de Sensores Sem Fio*

## 3.1 Introdução

O problema da classificação de um evento ou objeto detectado em uma de suas $M$ classes, baseada nas observações de nós sensores distribuídos no ambiente, é uma aplicação importante das rede de sensores e por isso tem recebido bastante atenção (WANG et al., 2003; CHAMBERLAND; VEERAVALLI, 2003; ALDOSARI; MOURA, 2004).

Frequentemente assume-se que para cada observação o nó sensor transmite pelo menos $\log_2 M$ bits para serem avaliados no centro de fusão. Devido a restrições de energia em RSSFs é importante reduzir a comunicação. Em alguns trabalhos mostra-se que é possível realizar a classificação mesmo quando os nós enviam menos de $\log_2 M$ bits para o centro de fusão (ZHU et al., 2004; ZHANG; VARSHNEY, 2001). No entanto, a redução da sobrecarga de comunicação deve ser conseguida sem prejudicar a capacidade de tolerância a falhas da rede, para tanto pode-se utilizar códigos corretores de erro.

Em (CHEN et al., 2005) e (YAO et al., 2007) propõe-se uma sistema de classificação de múltiplas hipóteses a partir de mensagens binárias de sensores, em que a tolerância a falhas é conseguida com a utilização de códigos corretores de erro. A idéia consiste basicamente em relacionar uma palavra código a cada hipótese que o fenômeno possa assumir, cada nó é responsável por produzir exatamente um bit da palavra código.

As próximas seções irão detalhar melhor a abordagem proposta em (YAO et al., 2007). Na seção 3.2 será detalhado o modelo do sistema adotado; a seção 3.3 discorre acerca do canal gaussiano, modelo de canal adotado neste trabalho; a seção 3.4 abordará os limitantes que avaliam o desempenho do sistema; a Seção 3.5 trata da tolerância à falhas, a Seção 3.6 descreve o projeto da matriz código, descrita na seção 3.2; por fim, na Seção 3.7 serão feitas algumas considerações finais.

## 3.2 Formulação do Problema

O modelo do sistema para a abordagem descrita em (YAO et al., 2007) é mostrado na Figura 4[1]. Considere o problema de classificação de alvos ou eventos em classes. Seja $M$ o número de classes possíveis e $N$ o número de sensores observando o fenômeno. Assume-se que os nós sensores não se comunicam entre si e que não existe realimentação do centro de fusão para os sensores locais.

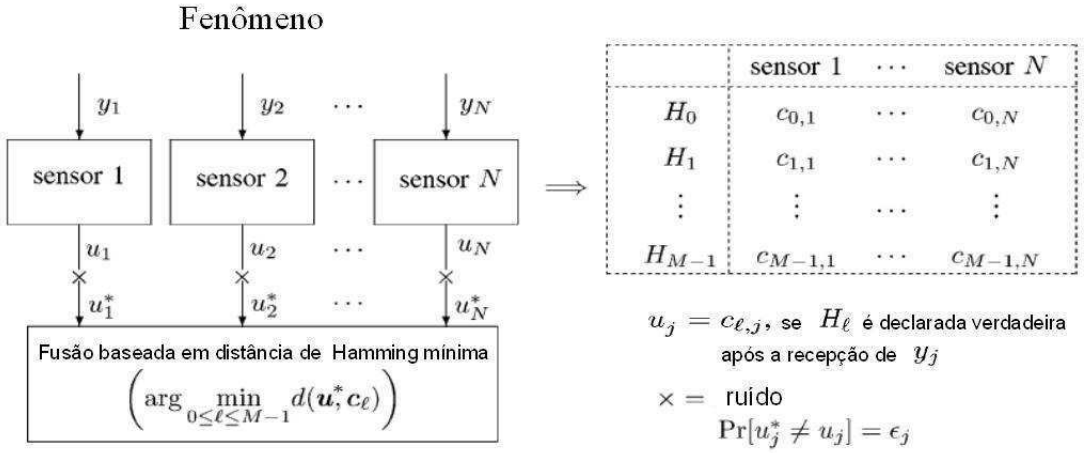


Figura 4: Modelo do Sistema

As observações dos sensores são representadas por $y_j$, em que $j = 1, \ldots, N$. Assume-se que as interferências presentes nos sensores são estatisticamente independentes e então as observações locais $y_j$ são condicionalmente independentes dadas suas hipóteses. A probabilidade do sensor $j$ classificar sua observação como $H_\ell$ dado que $H_i$ é a hipótese verdadeira será representada por $h_{\ell|i}^{(j)}$.

O primeiro passo é projetar uma matriz $\boldsymbol{C_{M\times N}}$, que será chamada de matriz código (não confundir com a matriz geradora do código), com elementos $c_{\ell,j} \in \{0,1\}$, $\ell = 0, \ldots, M-1$. Cada linha de $N$ bits forma uma palavra código que corresponde a uma das $M$ classes, as colunas representam a regra de classificação adotada pelo sensor correspondente. Depois de realizar sua observação, o sensor $j$ transmitirá uma saída binária $u_j$ que corresponderá ao elemento $c_{\ell,j}$ da Matriz $\mathbf{C}$ se a hipótese $H_\ell$ for considerada verdadeira.

Como o canal de transmissão não é perfeito, a palavra $\boldsymbol{u^*} = (u_1^*, u_2^*, ..., u_N^*)$ recebida pelo centro de fusão pode ser diferente da palavra $\mathbf{u} = (u_1, u_2, ..., u_N)$ transmitida. As-

[1]Esta figura foi adaptada de (YAO et al., 2007)

suma que o evento erro no enlace de comunicação é independente para todos os canais de comunicação entre os sensores e o centro de fusão, e também é independente das observações $\{y_j\}_{j=1}^{N}$ e da hipótese verdadeira $H_i$, e sua probabilidade $Pr[u_j^* \neq u_j]$ é $\epsilon_j$.

A regra de fusão é baseada na distância de Hamming mínima, a decisão final será $H_w$ se $w = \arg\min_{0\leq\ell\leq M-1} d(u^*, c_\ell)$, em que $c_\ell \triangleq (c_{\ell,1}, c_{\ell,2}, ..., c_{\ell,N})$ representa a linha de $\mathbf{C}$ correspondente a hipótese $H_\ell$ e $d(x, y)$ é a distância de Hamming entre $\mathbf{x}$ e $\mathbf{y}$. Caso existam mais de uma classe com a mesma distância mínima da palavra recebida, então uma delas é escolhida aleatoriamente.

## 3.3 Canal Gaussiano

No trabalho descrito em (YAO et al., 2007) e também nesta dissertação, adotou-se como modelo para o canal de comunicação, o canal com ruido gaussiano branco aditivo ( AWGN, do inglês *Additive White Gaussian Noise*), neste modelo o sinal $s(t)$ é corrompido por um ruído aditivo $n(t)$ com distribuição gaussiana, como mostrado na Figura 5.

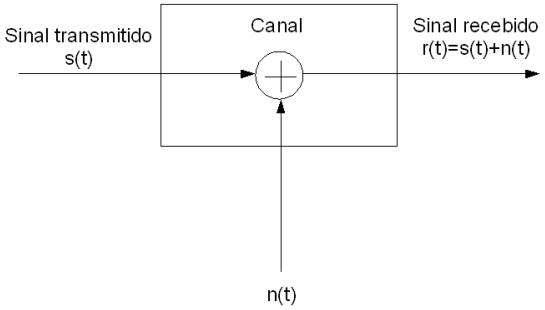


Figura 5: Modelo para um canal AWGN

A função densidade de probabilidade para uma variável aleatória gaussiana com média $m_x$ e variância $\sigma^2$ é dada por:

$$p_X(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{-(x-m_x)^2}{2\sigma^2}}$$

Para um sistema de transmissão binária que emprega modulação BPSK, modelo que será utilizado posteriormente, a probabilidade de erro de bit $P_b$ para um canal AWGN é dada por (PROAKIS, 1983):

$$P_b = Q\left(\sqrt{\frac{2\mathcal{E}_b}{N_0}}\right) \tag{3.1}$$

em que $\mathcal{E}_b/N_0$ é a razão sinal ruído por bit e a função $Q$ é definida por:

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-t^2/2} dt,\ x \geq 0$$

Definindo a função de erro $erf$ e a função complementar de erro $erfc$ como:

$$\begin{aligned} erf(x) &= \frac{2}{\pi} \int_0^x e^{-t^2} dt \\ erfc(x) &= 1 - erf = \frac{2}{\pi} \int_x^\infty e^{-t^2} dt \end{aligned}$$

pode-se redefinir a função $Q$ como $\frac{1}{2} erfc\left(\frac{x}{\sqrt{2}}\right)$.

A equação 3.2 pode ser reescrita como:

$$P_b = \frac{1}{2} erfc\left(\sqrt{\frac{\mathcal{E}_b}{N_0}}\right) \tag{3.2}$$

## 3.4 Análise de desempenho

Para caracterizar o sistema é importante se obter limitantes para a probabilidade de erro do mesmo para uma certa matriz código. Em (CHEN et al., 2005) foi feita uma análise de desempenho quando o número de sensores é suficientemente grande. Em (YAO et al., 2007) os limitantes de probabilidade obtidos são válidos para qualquer quantidade finita de sensores, estes serão expostos a seguir.

O primeiro passo é reescrever a regra de fusão baseada na distância de Hamming da seguinte forma:

$$w = \arg \min_{0 \leq \ell \leq M-1} d(u^*, c_\ell) = \arg \min_{0 \leq \ell \leq M-1} \sum_{j=1}^{N} z_{\ell,j}$$

em que $z_{\ell,j} \triangleq 2(u_j^* \oplus c_{\ell,j}) - 1$ e $\oplus$ representa a operação OU-Exclusivo. Note que a análise de desempenho do sistema está relacionada com as probabilidades dos eventos $[z_{\ell,j} = 1]$ e $[z_{\ell,j} = -1]$. Dado que a hipótese $H_i$ é verdadeira, quanto mais negativo for o somatório $\sum_{j=1}^{N} z_{\ell,j}$ menor é o erro de fusão. A seguir os Lema 1 e 2 fornecerão limitantes de probabilidade para soma de variáveis aleatórias antipodais independentes.

***Lema 1***: Sejam $\{Z_j\}_{j=1}^{\infty}$ variáveis aleatórias antipodais independentes com

$Pr[Z_j = 1] = q_j$ e $Pr[Z_j = -1] = 1 - q_j$.

Defina $\varphi_m(\theta) \triangleq \frac{1}{m} \log E[\exp\{\theta(Z_1 + ... + Z_m)\}]$ e $I_m(x) \triangleq \sup_{\theta \in \Re}[\theta x - \varphi_m(\theta)]$

Então, se $\lambda_m \triangleq E[Z_1 + ... + Z_m]/m < 0$:

$$Pr\{Z_1 + ... + Z_m \geq 0\} \leq \exp\{-m \cdot Im(0)\} = \inf_{\theta \in \Re} \exp\left\{\sum_{j=1}^{m} \log\left(q_j e^{\theta} + (1-q_j)e^{-\theta}\right)\right\}$$

Uma vez que para $\lambda_m < 0$, $I_m(0)$ permanece o mesmo se $I_m(x)$ for redefinido como $\sup_{\theta>0}[\theta x - \varphi_m(\theta)]$, então o Lema 1 pode ser rescrito como:

$$Pr\{Z_1 + ... + Z_m \geq 0\} \leq \inf_{\theta \geq 0} \exp\left\{\sum_{j=1}^{m} log\left(q_j e^{\theta} + (1-q_j)e^{-\theta}\right)\right\} \tag{3.3}$$

***Lema 2***: Se $\lambda_m \triangleq E[Z_1 + ... + Z_m]/m < 0$, então:

$Pr\{Z_1 + ... + Z_m \geq 0\} \leq (1 - \lambda_m^2)^{m/2}$

Baseado no Lema 1, o limitante superior da probabilidade de erro de um sistema de classificação distribuída que usa distância mínima de Hamming como regra de fusão é dado pelo seguinte teorema.

***Teorema 1***: Seja a probabilidade média de erro $P_e$ para fusão baseada em distância de Hamming definida como:

$$P_e \triangleq \frac{1}{M} \sum_{i=0}^{M-1} Pr(\text{detecção após a fusão} \neq H_i | H_i) \tag{3.4}$$

Se para todo $\ell \neq i$:

$$\sum_{\{j \in [1,...,N]: c_{\ell,j} \neq c_{i,j}\}} E[z_{i,j}] = \sum_{j=1}^{N} (c_{\ell,j} \oplus c_{i,j})(2q_{i,j} - 1) < 0 \tag{3.5}$$

em que $0 \leq \ell, i \leq M-1$, $z_{i,j} \triangleq 2(u_j \oplus c_{i,j}) - 1$, e $q_{i,j} \triangleq Pr\{z_{i,j} = 1 | H_i\}$, então:

$$P_e \leq \frac{1}{M} \sum_{i=0}^{M-1} \sum_{0 \leq \ell \leq M-1, \ell \neq i} \inf_{\theta \geq 0} \exp\left\{\sum_{j=1}^{N} \log\left(q_{i,j} e^{\theta} + (1-q_{i,j})e^{-\theta}\right)\right\}^{c_{\ell,j} \oplus c_{i,j}} \tag{3.6}$$

Observe que:

$$\begin{aligned} Pr(z_{i,j}=1|H_i) &= Pr(u_j^* \oplus c_{i,j}=1|H_i) \\ &= Pr(u_j^*=u_j \; e \; u_j \oplus c_{i,j}=1|H_i) + Pr(u_j^* \neq u_j \; e \; u_j \oplus c_{i,j}=0|H_i) \\ &= Pr(u_j^*=u_j)Pr(u_j \oplus c_{i,j}=1|H_i) + Pr(u_j^* \neq u_j)Pr(u_j \oplus c_{i,j}=0|H_i) \\ &= \epsilon_j + (1-2\epsilon_j)\sum_{k=0}^{M-1}(c_{i,j} \oplus c_{k,j})h_{k|i}^{(j)} \end{aligned} \tag{3.7}$$

Baseado no Lema 2 obtém-se um limitante de probabilidade de erro em função da distância de Hamming mínima do código dado pelo seguinte Corolário.

***Corolário 1***: Considere a condição (3.5), a probabilidade média de erro pode ser limitada superiormente por:

$$P_e \leq \frac{1}{M}\sum_{i=0}^{M-1}\sum_{0\leq\ell\leq M-1,\ell\neq i}\left(1-\left(\frac{\sum_{j=1}^{N}(c_{\ell,j}\oplus c_{i,j})(2q_{i,j}-1)}{d(c_\ell,c_i)}\right)^2\right)^{d(c_\ell,c_i)/2} \tag{3.8}$$

$$\leq (M-1)(1-\lambda_{max}^2)^{d_{min}/2} \tag{3.9}$$

Em que:

$$d_{min} \triangleq \; min_{0\leq\ell,i\leq M-1,\ell\neq i}d(c_\ell,c_i)$$

$$\lambda_{max} \triangleq \; max_{0\leq\ell,i\leq M-1,\ell\neq i}\frac{1}{d(c_\ell,c_i)}\sum_{j=1}^{N}(c_{\ell,j}\oplus c_{i,j})(2q_{i,j}-1) \tag{3.10}$$

Pela condição (3.5) $\lambda_{max} < 0$, e $\lambda_{max} \geq \min_{0\leq i\leq M-1,1\leq j\leq N}(2q_{i,j-1}) \geq -1$.

O teorema 2, a seguir, estabelece $\limsup_{N\to\infty}\lambda_{max} < 0$ como uma condição suficiente e necessária para que $P_e$ diminua com o aumento do número de sensores.

***Teorema 2***: se $\limsup_{N\to\infty}\lambda_{max} > 0$, $P_e$ se afasta de zero quando o número de sensores tende ao infinito.

O Corolário 1 e a expressão de $\lambda_{max}$ podem ser bastante simplificados para o caso de um sistema em que os nós sensores tenham mesma precisão e então $h_{k|i}^{(j)} = h_{k|i}$ é o mesmo para todos os sensores e que $\epsilon_j = \epsilon$ para $j = 1, \ldots, N$. Isto será expresso pelo Lema 3 a seguir.

***Lema 3***: suponha que $\epsilon_j = \epsilon$ para $j = 1, \ldots, N$, com $0 \leq \epsilon < 1/2$, e $h_{k|i}^{(j)} = h_{k|i}$ para todos os sensores. Se $\lambda_{max} < 0$ o Corolário 1 pode ser simplificado para:

$$P_e \leq \frac{1}{M}\sum_{i=0}^{M-1}\sum_{0\leq\ell\leq M-1,\ell\neq i}\left(1-(1-2\epsilon)^2\times\left(\frac{\sum_{k=0}^{M-1}h_{k|i}\left[d(c_i,c_k)-d(c_\ell,c_k)\right]}{d(c_\ell,c_i)}\right)^2\right)^{d(c_\ell,c_i)/2} \tag{3.11}$$

$$\leq (M-1)(1-\lambda_{max}^2)^{d_{min}/2} \tag{3.12}$$

em que $\lambda_{max}$ é simplificado para:

$$\lambda_{max} = (1-2\epsilon)\max_{0\leq\ell,i\leq M-1,\ell\neq i}\frac{1}{d(c_\ell,c_i)}\sum_{k=0}^{M-1}h_{k|i}[d(c_i,c_k)-d(c_\ell,c_k)] \tag{3.13}$$

Nesta seção foram apresentados alguns dos limitantes de probabilidades de erro que nos permitem fazer uma análise do desempenho do sistema, e que podem ser usados como função objetivo em algoritmos de busca para a seleção das matrizes códigos. As provas dos teoremas, lemas e corolários aqui expostos foram omitidas, para maiores detalhes ver (YAO et al., 2007).

## 3.5 Tolerância a Falhas

Os nós sensores são propensos a falhas que podem incluir todo tipo de mau funcionamento, tais como falhas aleatórias ou falhas do tipo *stuck-at*. Por falhas aleatórias entenda como a situação na qual o nó sensor envia 0 ou 1 independente da observação realizada. Falhas do tipo *stuck-at-zero* ou *stuck-at-one* ocorrem quando o nó sensor sempre transmite zero ou um respectivamente, negligenciando a observação realizada.

Do limitante (3.10) e da definição de $\lambda_{max}$ em (3.9), observa-se que quanto menor for o valor de $q_{i,j}$ mais negativo $\lambda_{max}$ é, e então menor é o limitante superior de probabilidade (3.10). Quando acontecem falhas nos sensores, $q_{i,j}$ não mais corresponde a equação (3.7), torna-se função de novas estatísticas de $u_j$ próprias do tipo falha que ocorreu, o novo $q_{i,j}$ será representado por $q_{i,j}^{(FS)}$, em que (FS) indica a condição de falha no sensor. Por exemplo, quando acontece uma falha do tipo *stuck-at-one* no sensor $j$, $Pr\{u_j = 1|H_i\} = 1$ para $0 \leq i \leq M-1$, então tem-se:

$$\begin{aligned} q_{i,j}^{(FS)} &= Pr(u_j^* = u_j)Pr(u_j \oplus c_{i,j} = 1|H_i) + Pr(u_j^* \neq u_j)Pr(u_j \oplus c_{i,j} = 0|H_i) \\ &= (1-\epsilon_j)(1-c_{i,j}) + \epsilon_j c_{i,j} \end{aligned}$$

Note que $q_{i,j}^{(FS)}$ não exibe mais nenhuma relação com a precisão dos nós sensores.

Quando a falha é do tipo aleatória, em que $Pr\{u_j = 0|H_i\} = Pr\{u_j = 1|H_i\} = 1$, $q_{i,j}^{(FS)} = 1/2$. O valor de $q_{i,j}^{(FS)}$ pode variar entre $\min\{\epsilon_j, 1-\epsilon_j\}$ e $\max\{\epsilon_j, 1-\epsilon_j\}$. Como a princípio o centro de fusão não possui nenhuma informação a priori do tipo de falhas dos sensores nem quais deles estão com problema, será considerada a capacidade de tolerância à falhas do sistema para o pior caso em que $q_{i,j}^{(FS)} = \max\{\epsilon_j, 1-\epsilon_j\}$. Note que:

$$q_{i,j} = \epsilon_j + (1-2\epsilon_j)\sum_{k=0}^{M-1}(c_{i,j} \oplus c_{k,j})h_{k|i}^{(j)} \leq \epsilon_j + (1-2\epsilon_j) \leq \max\{\epsilon_j, 1-\epsilon_j\} = q_{i,j}^{(FS)}$$

Uma extensão direta do Corolário 1 pode ser usada para caracterizar a capacidade de tolerância à falhas do sistema o que leva ao Corolário 2.

*Corolário 2*: Seja $\boldsymbol{\mathcal{F}}$ o conjunto de índices de sensores com falhas. Então, se $\lambda_{max}(\mathcal{F}) < 0$ e assumindo que $q_{i,j}^{(FS)} = \max\{\epsilon_j, 1-\epsilon_j\}$:

$$\begin{aligned} &P_e \leq \\ &\frac{1}{M}\sum_{i=0}^{M-1}\sum_{0\leq\ell\leq M-1,\ell\neq i}\left(1-\left(\frac{\sum_{j\in\mathcal{F}^c}(c_{\ell,j}\oplus c_{i,j})(2q_{i,j}-1)+\sum_{j\in\mathcal{F}}(c_{\ell,j}\oplus c_{i,j})(2q_{i,j}^{(SF)}-1)}{d(c_\ell,c_i)}\right)^2\right)^{\frac{d(c_\ell,c_i)}{2}} \\ &\leq (M-1)(1-\lambda_{max}^2(\mathcal{F}))^{d_{min}/2} \end{aligned} \tag{3.14}$$

Em que o sobrescrito "c" denota a operação complementar de conjunto e

$$\lambda_{max}(\mathcal{F}) = \max_{0\leq\ell,i\leq M-1,\ell\neq i}\frac{1}{d(c_\ell,c_i)}\times\left(\sum_{j\in\mathcal{F}^c}(c_{\ell,j}\oplus c_{i,j})(2q_{i,j}-1)+\sum_{j\in\mathcal{F}}(c_{\ell,j}\oplus c_{i,j})(2q_{i,j}^{(FS)}-1)\right)$$

Pode-se verificar baseado no corolário acima que:

$$\begin{aligned} \lambda_{max}(F)-\lambda_{max} &\leq \max_{0\leq\ell\leq M-1,\ell\neq i}\frac{1}{d(c_\ell,c_i)}\times\sum_{j\in F}(c_{\ell,j}\oplus c_{i,j})\left(q_{i,j}^{(SF)}-q_{i,j}\right) \\ &\leq 2\max_{0\leq\ell\leq M-1,\ell\neq i}\frac{1}{d(c_\ell,c_i)}\times\sum_{j\in F}|1-2\epsilon_j| \\ &\leq \frac{1}{d_{min}}\sum_{j=1}^{|\mathcal{F}|}|1-2\epsilon_{(j)}| \end{aligned}$$

Para garantir que $P_e$ diminua com o aumento do número de sensores, é suficiente que:

$$\lambda_{max} + \frac{2}{d_{min}}\sum_{j=1}^{|F|}\left|1-2\epsilon_{(j)}\right| < 0 \tag{3.15}$$

Para sistemas em que $\epsilon_j = \epsilon$ para $j = 1, \ldots, N$, esta condição se reduz a:

$$d_{min} > -2\left|1 - 2\epsilon_{(j)}\right| \frac{|\mathcal{F}|}{\lambda_{max}} \geq 2|\mathcal{F}| \tag{3.16}$$

## 3.6 Projeto da Matriz Código

O desempenho desta abordagem está fortemente relacionado com a matriz código escolhida. Em um primeiro momento pode-se pensar que quanto maior for a distância de Hamming mínima entre as palavras códigos da matriz melhor será o desempenho do sistema e em geral é o que acontece. Mas o padrão das colunas da matriz, que está relacionado com o desempenho da classificação que os sensores realizam, também influi no desempenho do sistema como um todo.

Como projetar a matriz é sem dúvida uma questão importante. Definir as regras de decisão para os sensores, ou seja, as colunas da matriz e ao mesmo tempo garantir uma distância mínima entre as linhas suficiente para se obter a capacidade de correção de erros desejada, torna o projeto analítico da matriz muito complicado.

Propõe-se em (WANG et al., 2005) dois algoritmos para o projeto da matriz código, um baseado em substituição cíclica de coluna (*cyclic column replacement*) e outro baseado em *simulated annealing*. O primeiro converge mais rápido, mas pode convergir para um ótimo local dependendo da escolha da matriz inicial. Simulated annealing é mais robusto em relação à matriz inicial e capaz de produzir matrizes melhores.

Em (YAO et al., 2007), para uma rede de $N$ sensores e $M$ hipóteses e para um determinado modelo estatístico, adotou-se o seguinte algoritmo de busca:

1. Inicialização: Para $j = 1, \ldots, N$ e $0 \leq \ell, i \leq M - 1$ determine:

   $h_{\ell|i}^{(j)} = Pr\left\{y_j \in \Gamma_{\ell,j} | H_i\right\}$

   em que $\Gamma \triangleq \{y \in Y : f_{\ell,j}(y) \geq \max_{0 \leq i \leq M-1, i \neq \ell} f_{i,j}(y)\}$ e $f_{\ell,j}(y)$ é a função densidade de probabilidade da observação local no sensor j dado que a hipótese $H_i$ é verdadeira.

2. Encontre utilizando *simulated annealing* o código que minimiza (3.8) sujeito a restrição (3.15) com o objetivo de uma capacidade de tolerância a falhas.

## 3.7 Considerações Finais

Embora a abordagem proposta em (YAO et al., 2007) apresente uma boa tolerância a falhas, os códigos utilizados não possuem nenhuma estrutura e a decodificação só pode ser feita por comparação da palavra recebida com as palavras pertencentes ao código usando uma tabela. Nesta dissertação propõe-se uma abordagem baseada em códigos de bloco lineares, esta será discutida no próximo capítulo.

# 4 Códigos de Bloco Aplicados a RSSF

## 4.1 Introdução

Neste trabalho propõe-se um sistema de classificação baseado em códigos de bloco lineares para redes de sensores sem fio que seja tolerante a falhas. Esta abordagem é similar à proposta em (YAO et al., 2007), mas aqui as palavras código que formam a matriz código formam um sub-código de um código linear. Este sub-código não é linear, mas os parâmetros do código tais como a distância de Hamming mínima do código se mantém.

Com esta abordagem é possível utilizar algoritmos de decodificação algébrica, diferentemente de (WANG et al., 2005) e (YAO et al., 2007) onde os códigos utilizados não possuem nenhuma estrutura e a decodificação só pode ser feita por comparação da palavra recebida com as palavras do código. Isto evita uma decodificação massiva em sistemas em que o número de hipóteses é muito grande.

A principal diferença entre a abordagem proposta aqui e a proposta em (YAO et al., 2007) encontra-se no projeto da matriz código. Será considerado o mesmo modelo de sistema descrito na Seção 3.2, no entanto a seleção das matrizes será baseada em um código BCH (Bose-Chaudhuri-Hochquenghem), isto será detalhado na seção a seguir. Na Seção 4.3 serão apresentados e discutidos os resultados obtidos. Na Seção 4.4 serão feitas as considerações finais.

## 4.2 Projeto da matriz código

Como mostrado na seção (3.6) em (YAO et al., 2007) as matrizes são selecionadas através de *simulated annealing* tendo o limitante (3.8) como função de energia e com a restrição (3.15), para o caso em que $\epsilon_j = \epsilon$ para $j = 1, \ldots, N$ e $h^{(j)}_{k|i} = h_{k|i}$ para todos os

sensores. Nenhuma restrição é imposta às palavras código que compõem a matriz, estas podem ser qualquer bloco de $N$ bits.

Neste trabalho, propõe-se que essas palavras sejam restritas às palavras de um código BCH. Para um código BCH(n,k,d) binário existem $2^k$ palavras-códigos que podem ser combinadas em grupos de M para formar uma matriz código $M \times N$. Em geral o número de hipóteses é menor que a quantidade de palavras código disponíveis, isto resulta em diferentes combinações possíveis para a matriz código, então é necessário selecionar a mais adequada. Em outras palavras, realizar a busca por um subcódigo dentro de um código BCH.

Ao realizar a seleção da matriz código para a abordagem proposta aqui é preciso garantir que as palavras código (linhas da matriz) pertençam ao código BCH escolhido, escolheu-se então utilizar um algoritmo genético (AG) guiado por códigos, este algoritmo é um modificação do algoritmo genético padrão proposto em (ASSIS, 1997, 2000). Algoritmos Genéticos são uma classe particular de algoritmos evolutivos que usam técnicas inspiradas pela biologia evolutiva como hereditariedade, mutação, seleção natural e recombinação. Nos algoritmos genéticos guiados por códigos, a busca é realizada no espaço das sequências de informação, que são depois codificadas em palavras código e então avalia-se a solução, isto garante que todas as palavras da matriz pertençam ao código.

Tanto em um AG padrão quanto em um AG guiado por código, uma população representa um conjunto de soluções aproximadas para o problema, cada indivíduo é uma possível solução, a população é constantemente modificada pelos operadores genéticos (seleção, recombinação e mutação) até evoluir para uma solução ótima ou sub-ótima. Para o algoritmo utilizado neste trabalho os indivíduos são representados por sequências binárias de comprimento $M \times k$, correspondendo a uma matriz com $M$ linhas e $k$ colunas, como ilustrado na Figura 6.

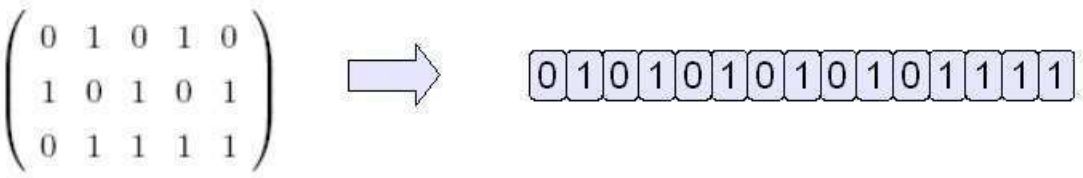


Figura 6: Exemplo de representação das matrizes como indivíduos

A solução é o resultado desta matriz multiplicada pela matriz geradora $\mathbf{G}_{k \times n}$ de um

código BCH $(n, k, d)$, ou seja, uma matriz código $M \times N$. A função objetivo para este algoritmo é o limitante de probabilidade 3.11, não será necessário impor nenhuma restrição quanto a distância mínima, pois esta é previamente conhecida. O pseudo-código para este algoritmo é mostrado a seguir, neste algoritmo $P(t)$ representa uma população com um número $Q$ de indivíduos na geração $t$ e $P'$ é gerada pelos operadores genéticos clássicos de seleção, recombinação e mutação.

**Algoritmo Genético baseado em um BCH $(n, k, d)$**

**Entrada:** função objetivo, matriz geradora $G_{k \times n}$

**Saída:** matriz código $C_{M \times N}$ ótima ou sub-ótima

**Initialização:**

- $t \leftarrow 0$;
- inicializar $p(t) \subset \{0,1\}^{M \times k}$;
- avaliar $P(t)\, G$;

**Iteração:**

**Enquanto** PARE = FALSO **faça**

- $P'(t) \leftarrow$ variação $P(t)$;
- avaliar $P'(t)\, G$;
- $P(t+1) \leftarrow$ selecionar $P'(t)$;
- $t \leftarrow t + 1$;

**Fim**

**Fim**

Para realizar a comparação com a abordagem sem restrições às palavras código, selecionou-se matrizes códigos a partir de um de AG sem restrições às palavras códigos, isto é, as palavras código que formam a matriz podem ser qualquer sequência binária de comprimento $N$. Neste caso, os indivíduos são sequências binárias de comprimento $M \times N$ que corresponde a uma matriz com $M$ linhas e $N$ colunas. O pseudo-código para este algoritmo é mostrado a seguir.

**Algoritmo Genético sem restrição**

**Entrada:** função objetivo

**Saída:** matriz código $C_{M\times N}$ ótima ou sub-ótima

**Initialização:**

- $t \leftarrow 0$;
- inicializar $p(t) \subset \{0,1\}^{M\times N}$;
- avaliar $P(t)$;

**Iteração:**

**Enquanto** PARE = FALSO **faça**

- $P'(t) \leftarrow$ variação$P(t)$;
- avaliar $P'(t)$;
- $P(t+1) \leftarrow$ selecionar$P'(t)$;
- $t \leftarrow t+1$;

**Fim**

**Fim**

É importante ressaltar que não é objetivo deste trabalho fazer uma comparação entre selecionar a matriz código utilizando *simulated annealing* ou algoritmo genético guiado por código, e sim entre fazer uma busca em todo o espaço de soluções e uma busca em um espaço menor, entretanto mais estruturado.

## 4.3 Resultados e Discussões

Nesta seção serão apresentados simulações e resultados numéricos utilizados para comparar o desempenho entre a abordagem baseada no BCH, proposta nesta dissertação, e a abordagem baseada em busca aleatória. Para estas simulações assumiu-se que:

- As observações $\{y_j\}_{j=1}^{N}$ têm distribuição Gaussiana com média $\ell$ e variância $1/\gamma_o$ dado que a hipótese $H_\ell$ é verdadeira.

- Uma hipótese $H_i$ é declarada localmente verdadeira para um determinado nó sensor se $(y_j - i)^2 \leq \min_{0\leq\ell\leq M-1,\ell\neq i}(y_j - \ell)^2$.
- Os *links* de comunicação empregam transmissão antipodal.
- O canal de comunicação entre os sensores e o centro de fusão é um canal com ruído aditivo gaussiano branco.
- A probabilidade de erro no *link* de comunicação $\epsilon_j$ é a mesma para todos os nós sensores. De tal forma que, $\epsilon_j = \epsilon = \frac{1}{2}erfc\left(\sqrt{\gamma_s}\right)$, em que erfc(.) é a função erro complementar, e $\gamma_s$ é a relação sinal-ruído do *link* de comunicação.

Em todas as buscas realizadas tanto para o AG guiado por código quanto para o AG geral utilizou-se uma taxa de cruzamento de 0.6 e uma taxa de mutação de 0.05, a condição de parada foi número máximo de gerações.

Primeiramente consideramos um sistema com quinze sensores ($N = 15$) para classificar oito hipóteses ($M = 8$). De acordo com metodologia descrita na seção anterior, selecionou-se uma matriz baseada no BCH(15,5,7) e comparou-se com uma matriz selecionada sem restrições. As matrizes foram selecionadas considerando $\gamma_s = 0$dB e $\gamma_o = 6$dB.

Foram realizadas simulações para estimar a probabilidade de erro esperada para cada uma das matrizes mantendo-se o valor de $\gamma_s$ em 0 dB e variando o valor de $\gamma_o$, também foi calculado numericamente os valores do limitante (3.11).

Vê-se na Figura 7 que a matriz código baseada no BCH(15,5,7) tem quase o mesmo desempenho que e a matriz obtida sem restrições para valores de $\gamma_o = 0$dB a $\gamma_o = 6$dB, e de $\gamma_o = 6$dB em diante, valor para o qual as matrizes foram otimizadas, a matriz baseada no BCH tem um desempenho superior. As curvas que representam o cálculo numérico do limitante (3.11) apresentam um comportamento similar ao das curvas de simulação.

Também foram feitas avaliações para redes de sensores maiores, com uma quantidade maior de nós sensores. Novamente escolheu-se $\gamma_s = 0$dB e $\gamma_o = 6$dB como razões sinal-ruído alvo durante a seleção das matrizes. Foram avaliados sistemas com $M = 8$ e $N = 511$ e com $M = 16$ e $N = 511$. As matrizes foram selecionadas com base no BCH(511,10,223). Os resultados encontram-se nas Figuras 8 e 9.

Observando os gráficos das Figuras 8 e 9 é possível concluir que as matrizes códigos baseadas no BCH(511,10,223) têm um desempenho tão bom quanto as matrizes obtidas sem nenhuma restrição, com a vantagem de permitir uma decodificação algébrica.

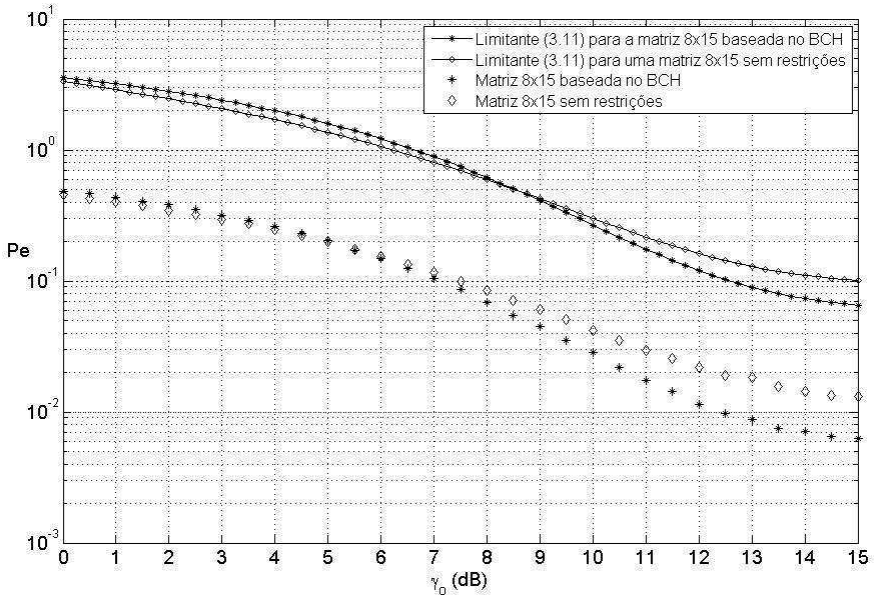


Figura 7: Simulações e cálculo do limitante (3.11) para matrizes 8x15 selecionadas para $\gamma_s = 0$dB e $\gamma_o = 6$dB. As probabilidade de erro foram simuladas para $\gamma_s = 0$dB.

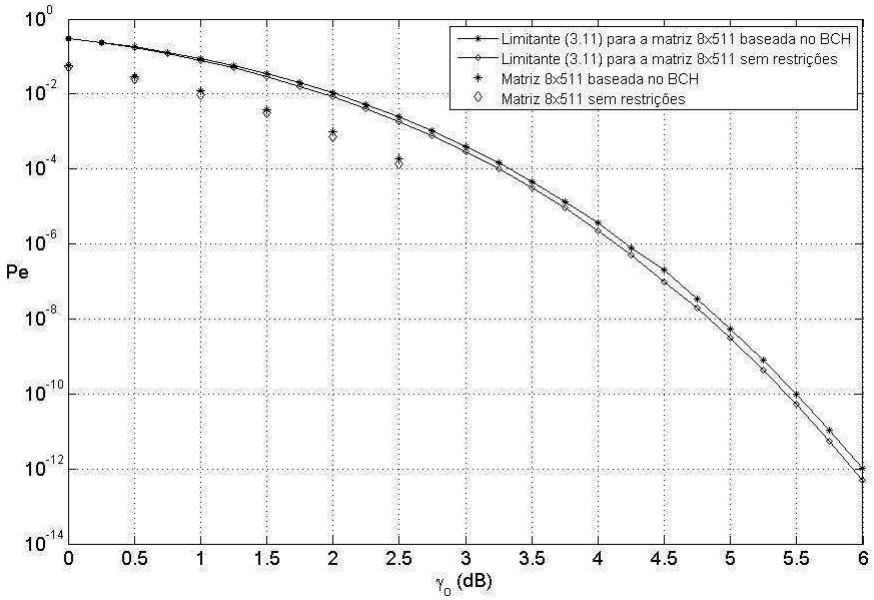


Figura 8: Simulações e cálculo do limitante (3.11) para matrizes 8x511 selecionadas para $\gamma_s = 0$dB e $\gamma_o = 6$dB. As probabilidade de erro foram simuladas para $\gamma_s = 0$dB.

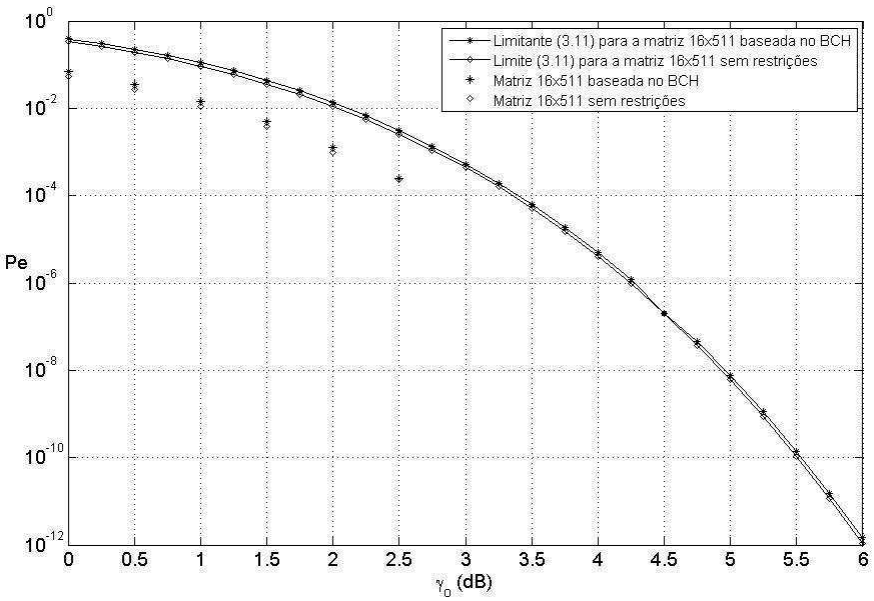


Figura 9: Simulações e cálculo do limitante (3.11) para matrizes 16x511 selecionadas para $\gamma_s = 0$dB e $\gamma_o = 6$dB. As probabilidade de erro foram simuladas para $\gamma_s = 0$dB.

Em todas as seleções as matrizes com código BCH teve um desempenho ligeiramente inferior para baixos valores de $\gamma_o$ e um desempenho melhor para valores mais altos de $\gamma_o$, uma explicação encontra-se no fato das palavras código da matriz baseada no BCH possuírem uma distância mínima.

Quando as matrizes são selecionadas para um valor baixo de $\gamma_o$ pode ser mais interessante que a distância entre palavras vizinhas da matriz (linhas vizinhas) seja pequena, pois quando o nó sensor errar na classificação, tomando como verdadeira uma hipótese adjacente, não ocorrerá erro se o valor binário que ele deve enviar for o mesmo da hipótese verdadeira, para as matrizes selecionadas com base em um código aleatório esse valor da distância não têm um limite mínimo como no caso das matrizes baseadas em um código BCH.

Então quando os valores de $\gamma_o$ aumentam, os erros de classificação do nó sensor diminuem e as matrizes baseadas no código BCH por apresentarem distâncias maiores entre as palavras código passam a ter um desempenho melhor, pois o erro no enlace de comunicação passa a ser mais importante do que erro de classificação do nó sensor.

Por exemplo para o caso de $N = 15$ e $M = 8$, em que as matrizes foram selecionadas para $\gamma_s = 0$dB e $\gamma_o = 6$dB, e o gráfico das simulações encontra-se na Figura 7, a distância mínima para a matriz baseada em código aleatório é 4 enquanto que para a matriz baseada no código BCH é 7, que corresponde a distância mínima do código BCH(15,5,7).

## 4.4 Considerações finais

Embora a abordagem proposta reduza o espaço das possíveis soluções, o novo espaço de busca é mais estruturado e a distância mínima entre as palavras-código é inicialmente conhecida, não sendo necessário avaliar este parâmetro durante o processo de busca da matriz código.

Pode-se concluir que não há uma perda significativa de desempenho quando é usada a abordagem aqui proposta e esta pode ser justificada, pois os códigos usados têm parâmetros bem definidos e existe a possibilidade de realizar a descodificação através de métodos algébricos, o que é particularmente interessante se o número de hipóteses for muito grande.

# 5 Conclusões

Este trabalho desenvolveu um sistema de classificação distribuída tolerante à falhas baseado no uso de códigos BCH. Nesta abordagem as palavras códigos que formam a matriz, que representa as regras de decisão nos nós sensores e no centro de fusão, são obtidas de códigos BCH. Propô-se também o uso de algoritmo genético para a seleção das melhores matrizes.

Foram feitas simulações para verificar o desempenho das matrizes obtidas por busca em código algébrico, e estes resultados foram comparados com o de matrizes selecionadas sem a restrição de suas palavras pertencerem a um determinado código como em (YAO et al., 2007).

Foi mostrado que o desempenho quando é usada a abordagem aqui proposta é tão bom quanto o obtido quando se usa matrizes obtidas de sequências aleatórias. Com a vantagem de um código mais estruturado e um processo de decodificação menos exaustivo.

Alguns pontos para trabalhos futuros são:

- Avaliar a abordagem proposta considerando outros modelos de canais que não o Gaussiano, como por exemplo, o canal com desvanecimento.
- Introduzir um modelo com apagamento no modelo do canal de comunicação.
- Introduzir estratégias de codificação e decodificação por listas, em que uma hipótese seria associada a mais de uma palavra código.

# *Referências*

AGRE, J.; CLARE, L. An integrated architecture for cooperative sensing networks. *Computer*, v. 33, n. 5, p. 106–108, May 2000. ISSN 0018-9162.

AKYILDIZ, I. et al. A survey on sensor networks. *Communications Magazine, IEEE*, v. 40, n. 8, p. 102–114, Aug 2002. ISSN 0163-6804.

ALDOSARI, S.; MOURA, J. Detection in decentralized sensor networks. *Acoustics, Speech, and Signal Processing, 2004. Proceedings. (ICASSP '04). IEEE International Conference on*, v. 2, p. ii–277–80 vol.2, May 2004. ISSN 1520-6149.

ASSIS, F. M. de. Genetic algorithms and packing of block codes. *International Conference on Tele-comunications, Proceedings of the ICT97*, Melbourne, Austrália, v. 3, p. 1045–1048, 1997.

ASSIS, F. M. de. Weight structure of binary codes and the performance of blind search algorithms. *Neural Networks, Brazilian Symposium on*, IEEE Computer Society, Los Alamitos, CA, USA, v. 0, p. 144, 2000. ISSN 1522-4899.

BLAHUT, R. E. *Theory and Practice of Error Control Codes*. [S.l.]: Addison-Wesley, 1983.

CHAMBERLAND, J.-F.; VEERAVALLI, V. Decentralized detection in sensor networks. *Signal Processing, IEEE Transactions on*, v. 51, n. 2, p. 407–416, Feb 2003. ISSN 1053-587X.

CHAMBERLAND, J.-F.; VEERAVALLI, V. Asymptotic results for decentralized detection in power constrained wireless sensor networks. *Selected Areas in Communications, IEEE Journal on*, v. 22, n. 6, p. 1007–1015, Aug. 2004. ISSN 0733-8716.

CHEN, P.-N. et al. Asymptotic performance analysis for minimum hamming distance fusion [wireless sensor network applications]. *Acoustics, Speech, and Signal Processing, 2005. Proceedings. (ICASSP '05). IEEE International Conference on*, v. 4, p. iv/865–iv/868 Vol. 4, March 2005. ISSN 1520-6149.

CROSSBOW. *Homepage da Crossbow*. 2009. Disponível em: <http://www.xbow.com>. Acesso em: fevereiro 2009.

DONTAS, K.; JONG, K. D. Discovery of maximal distance codes using genetic algorithms. *Tools for Artificial Intelligence, 1990.,Proceedings of the 2nd International IEEE Conference on*, p. 805–811, Nov 1990.

HILL, J. L. *System Architecture for Wireless Sensor Network*. Tese (Doutorado) — University of California, Berkeley, 2003.

ILYAS, M.; MAHGOUB. *Handbook of sensor networks: compct wireless and wired sensing systems*. New York: CRC Press, 2005.

POTTIE, G. J.; KAISER, W. J. Wireless integrated network sensors. *Commun. ACM*, ACM, New York, NY, USA, v. 43, n. 5, p. 51–58, 2000. ISSN 0001-0782.

PROAKIS, J. G. *Digital Communications*. New York: McGraw-Hill, 1983.

PUSHPIN. 2009. Disponível em: <http://www.media.mit.edu/resenv/pushpin>. Acesso em: fevereiro 2009.

SCHWIEBERT, L.; GUPTA, S. K.; WEINMANN, J. Research challenges in wireless networks of biomedical sensors. In: *MobiCom '01: Proceedings of the 7th annual international conference on Mobile computing and networking*. New York, NY, USA: ACM, 2001. p. 151–165. ISBN 1-58113-422-3.

SIMON, M. J. et al. A genetic algorithm to design error correcting codes. *Electrotechnical Conference, 2006. MELECON 2006. IEEE Mediterranean*, p. 807–810, May 2006.

SMART Dust. 2009. Disponível em: <http://robotics.eecs.berkeley.edu/ pister/SmartDust/>. Acesso em: fevereiro 2009.

THE ZebraNet Wildlife Tracker. 2009. Disponível em: <http://www.princeton.edu/ mrm/zebranet.html>. Acesso em: fevereiro 2009.

UAMPS. 2009. Disponível em: <http://www-mtl.mit.edu/researchgroups/icsystems/uamps>. Acesso em: fevereiro 2009.

VILLELA, A. H. e M. L. T. *Códigos Corretores de Erros*. Rio de Janeiro: IMPA, 2002.

WANG, H. et al. Target classification and localization in habitat monitoring. *Acoustics, Speech, and Signal Processing, 2003. Proceedings. (ICASSP '03). 2003 IEEE International Conference on*, v. 4, p. IV–844–7 vol.4, April 2003. ISSN 1520-6149.

WANG, T.-Y. et al. Distributed fault-tolerant classification in wireless sensor networks. *Selected Areas in Communications, IEEE Journal on*, v. 23, n. 4, p. 724–734, April 2005. ISSN 0733-8716.

WICKER, S. B. *Error Control Systems for Digital Comunication and Storage*. [S.l.]: Prentice Hall, 1995.

XIAO, J.-J.; LUO, Z.-Q. Decentralized estimation in an inhomogeneous sensing environment. *Information Theory, IEEE Transactions on*, v. 51, n. 10, p. 3564–3575, Oct. 2005. ISSN 0018-9448.

XIAO, J.-J.; LUO, Z.-Q. Universal decentralized detection in a bandwidth-constrained sensor network. *Signal Processing, IEEE Transactions on*, v. 53, n. 8, p. 2617–2624, Aug. 2005. ISSN 1053-587X.

YAN, T.; HE, T.; STANKOVIC, J. A. Differentiated surveillance for sensor networks. In: *SenSys '03: Proceedings of the 1st international conference on Embedded networked sensor systems*. New York, NY, USA: ACM, 2003. p. 51–62. ISBN 1-58113-707-9.

YAO, C. et al. Performance analysis and code design for minimum hamming distance fusion in wireless sensor networks. *Information Theory, IEEE Transactions on*, v. 53, n. 5, p. 1716–1734, May 2007. ISSN 0018-9448.

YU, L.; WANG, N.; MENG, X. Real-time forest fire detection with wireless sensor networks. *Wireless Communications, Networking and Mobile Computing, 2005. Proceedings. 2005 International Conference on*, v. 2, p. 1214–1217, Sept. 2005.

YUAN, Y.; KAM, M. Distributed decision fusion with a random-access channel for sensor network applications. *Instrumentation and Measurement, IEEE Transactions on*, v. 53, n. 4, p. 1339–1344, Aug. 2004. ISSN 0018-9456.

ZHANG, Q.; VARSHNEY, P. K. Decentralized m-ary detection via hierarchical binary decision fusion. *Information Fusion*, v. 2, n. 1, p. 3 – 16, 2001. ISSN 1566-2535.

ZHU, X. et al. Distributed m-ary hypothesis testing with binary local decisions. *Information Fusion*, v. 5, n. 3, p. 157 – 167, 2004. ISSN 1566-2535.