UNIVERSIDADE FEDERAL DE ALFENAS
INSTITUTO DE CIÊNCIAS EXATAS
BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

Bruno Cesar Da Ré Guerra

REDES DE SENSORES SEM FIO – APLICAÇÕES E MODELOS DE SENSORES

Alfenas, 08 de Dezembro de 2011.

UNIVERSIDADE FEDERAL DE ALFENAS
INSTITUTO DE CIÊNCIAS EXATAS
BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

REDES DE SENSORES SEM FIO – APLICAÇÕES E MODELOS DE SENSORES

Bruno Cesar Da Ré Guerra

Monografia apresentada ao Curso de Bacharelado em Ciência da Computação da Universidade Federal de Alfenas como requisito parcial para obtenção do Título de Bacharel em Ciência da Computação.

Orientador: Prof. Msc. Tomás Dias Sant'Anna

Alfenas, 08 de Dezembro de 2011.

Bruno Cesar Da Ré Guerra

REDES DE SENSORES SEM FIO – APLICAÇÕES E MODELOS DE SENSORES

A Banca examinadora abaixo-assinada aprova a monografia apresentada como parte dos requisitos para obtenção do título de Bacharel em Ciência da Computação pela Universidade Federal de Alfenas.

Prof. Msc. Flávio Barbieri Gonzaga

Universidade Federal de Alfenas

Prof. Dr. Nelson José Freitas da Silveira

Universidade Federal de Alfenas

Prof. Msc. Tomás Dias Sant' Ana (Orientador)

Universidade Federal de Alfenas

Alfenas, 08 de Dezembro de 2011.

AGRADECIMENTO

Agradeço à minha família. Sem seu apoio e incentivo, certamente este trabalho jamais teria acontecido. Agradeço especialmente aos meus pais, Tânia e Cesar, e a minha irmã, Flávia.

Agradeço a todos amigos de graduação, pelos quatro anos e meio de incontáveis conversas, trabalhos, idéias e tantas outras experiências, mas especialmente aos grandes amigos: Luís Felipe, Diego, Karim, Tardioli, Luiz Paulo, Arthur, Júlio, Thiago, entre tantos outros.

Aos professores de toda minha graduação, em especial ao Professor Tomás, por acreditar neste projeto, quando tantos outros relutaram em acreditar.

E aos demais amigos, especialmente os da academia Bien Hoo, que mesmo sem saber, contribuíram de forma incomparável para minha formação, entre eles: Zé, Erik, Cristiano, João, Gustavo, Isabela, Antônio, Matheus, Thiago, Pietra, Arlete, Lao Shi Flávio, e tantos outros.

"A alegria está na luta, na tentativa, no sofrimento envolvido e não na vitória propriamente dita."

Mahatma Gandhi

RESUMO

Nos últimos anos houve um grande avanço tecnológico nas áreas de sensores e comunicação sem fio, que levou a criação de redes de sensores sem fio. Este tipo de rede pode ser aplicada no monitoramento, rastreamento, coordenação e processamento em diferentes contextos. Pode-se, por exemplo, interconectar sensores para fazer o monitoramento e controle das condições ambientais numa floresta, oceano ou no planeta. A interconexão de sensores através de redes sem fio, com a finalidade de executar uma tarefa de sensoriamento maior, é capaz de revolucionar a coleta e o processamento de informações. O objetivo deste trabalho é elucidar as vantagens do uso de redes deste tipo, mostrando os modelos de sensores existentes e as aplicações das Redes de Sensores Sem Fio.

Palavras-Chave: Redes, Modelos, Sensores Sem Fio

ABSTRACT

In the last years there's been a huge technological advance in the sensors and wireless communication field, which led to the creation of the wireless sensor networks. That kind of network can be applied to monitoring, tracking, coordination and processing in different contexts. For example, you can interconnect sensors to monitor and control environmental conditions in a forest, an ocean or even the planet. The interconnection of sensors through wireless networks, with the goal to fulfill a task of major sensing, is capable of revolutionize the gathering and processing of information. The purpose of this paper is to elucidate the advantages of the use of this kind of networks, showing the existents sensor models and the applications of the Wireless Sensor Networks.

Keywords: Networks, Models, Wireless Sensors

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIAÇÕES

SPINS	*Security Protocols for Sensor Network* (Protocolos de Segurança para Redes Sensores)
ICA	*Inter Cluster Routing Algorithm* (Algoritmo de Roteamento entre Agrupamento de Nós)
SNEP	*Secure Network Encryption Protocol* (Protocolo de Codificação de Segurança de Redes)
uTESLA	*Micro Timed Efficient Stream Loss-tolerant Authentication* (Autenticação micro cronometrada de fluxo eficiente com tolerância a falhas)
RSSF	Redes de Sensores Sem Fio
GPS	*Global Positioning System* (Sistema de Posicionamento Global)
RF	Radio Freqüência
kHz	*KiloHertz*
mHz	*MegaHertz*
TEEN	*Threshold sensitive Energy Efficient sensor Network* (Rede de Sensores sensível ao Limiar Eficiente de Energia)
ST	*Soft Threshold* (Limiar Flexível)
HT	*Hard Threshold* (Limiar Rídigo)
PEGASIS	*Power-Efficient Gathering in Sensor Information Systems* (Sistema de Agrupamento de Informações Enérgico-Eficiente)
Wi-Fi	*Wireless Fidelity* (Fidelidade Sem Fio)
SIG	*Special Interest Group* (Grupo de Interesse Especial)
PDA	*Personal Digital Assistant* (Assistente Pessoal Digital)
Mbps	Mega bits por segundo
Kbps	Kilo bits por segundo
ISM	*Industrial, Scientifical and Medical* (Industrial, Científico e Médico)
gHz	*GigaHertz*
Km	Quilômetros
DARPA	Agência de Projeto e Pesquisa Avançada de Defesa
DSN	Redes de Sensores Distribuídos

MIT	*Massachusetts Institute of Technology* (Instituto de Tecnologia de Massachusetts)
WMTS	*Wireless Medical Telemetry Services* (Serviços de Telemetria Médica Sem Fio)
LUSTER	*Light Under Shrub Thicket for Environmental Research* (Luz Sobre o Arbusto no Matagal para Pesquisa Ambiental)

SUMÁRIO

1 Introdução

Neste capítulo será apresentada uma visão geral sobre o tema que será tratado neste trabalho. Na seção 1.1 são apresentadas as justificativas e a motivação do trabalho. Na seção 1.2 é discutido o problema que envolve o tema proposto e na seção 1.3 são mostrados os objetivos os quais este trabalho se propõe a realizar.

Uma Rede de Computadores consiste de dois ou mais computadores e outros dispositivos conectados entre si de modo a poderem compartilhar seus serviços. Com o advento da Internet, atualmente o conceito de Redes de Computadores é altamente disseminado, pois a Internet nada mais é do que uma grande rede de computadores mundial,ou seja, ela interliga milhões de computadores e equipamentos de computação que estão espalhados pelo mundo todo (KUROSE, 2006). Ainda segundo Kurose (2006, pág.3) "... o termo Redes de Computadores esta começando a soar um tanto desatualizado, dados os muitos equipamentos não tradicionais que estão sendo conectados a Internet...". Entre estes equipamentos estão os dispositivos de sensores sem fio, pois devido ao grande avanço tecnológico ocorrido nas áreas de sensores sem fio, circuitos integrados e comunicação sem fio, permitiu-se a criação das Redes de Sensores (Loureiro, et al., 2003).

Uma rede de sensores consiste de um ou mais grupos de dispositivos de sensoriamento ou de aquisição contínua de dados, interligados em rede, a qual é utilizada para disseminar os dados coletados de um determinado ambiente. Uma especificidade de uma rede de sensores trata-se das Redes de Sensores Sem Fio (Meira, 2007).

Redes de Sensores Sem Fio diferem de Redes de Computadores em vários aspectos. Normalmente essas redes possuem um grande número de sensores (nós) distribuídos, apresentam restrição de energia e devem possuir mecanismos para auto-configuração e adaptação devido a problemas com falhas de comunicação e perda de sensores. Uma Rede de Sensores Sem Fio tende a ser autônoma e requer um alto grau de cooperação para executar as tarefas definidas para a rede. Isto significa que algoritmos distribuídos tradicionais, como protocolos de comunicação, devem ser revistos para esse tipo de ambiente antes de serem usados diretamente. Os desafios e

considerações de projeto de Redes Sensores Sem Fio vão muito além das Redes de Computadores tradicionais (Loureiro, et al., 2003).

1.1 Justificativa e Motivação

Embora extremamente vantajosa, o uso de Redes de Sensores Sem Fio não é amplamente disseminado, como são as Redes de Computadores tradicionais. Com a tecnologia atual, no mundo hoje existe uma gama de aplicações onde o uso de uma Rede de Sensores Sem Fio seria extremamente vantajoso.

Voltada para as mais diversas áres, uma Rede de Sensores Sem Fio pode ser útil de várias formas, como por exemplo: detecção de movimento, análise de propriedades do solo, da água e até mesmo do ar, aplicações militares, ou ainda o projeto de segurança alimentar, proposto pela União Européia em 1999, prestes a se tornar uma realidade, onde o a importação de grãos de um país só poderá ser realizada mediante ao rastreamento da qualidade do produto de origem agrícola desde a colheita até seu consumo (*European Union. Food Safety: From the Farm to the Fork*).

Neste sentido, o objetivo deste trabalho é realizar o levantamento sobre os atuais Sensores Sem Fio, e a viabilidade de seu uso nas mais diversas áreas de aplicação, e como isto vem acontecendo.

1.2 Problematização

É viável a implantação ou ainda passível de melhoramento, em caso de existência prévia, de Redes de Sensores Sem Fio voltadas para diversas áreas de aplicação no Brasil?

1.3 **Objetivos**

1.3.1 Gerais

Elencar aplicações e modelos encontrados para o uso de Redes de Sensores Sem Fio.

1.3.2 Específicos

- Criar uma base de conhecimento sobre Redes de Computadores, voltada para Redes de Sensores Sem Fio, para uso posterior neste, e em demais trabalhos acadêmicos voltados para esta área;
- Estudar Redes de Sensores Sem Fio e seus diversos usos;
- Verificar a viabilidade de aplicação das Redes de Sensores Sem Fio em diversas áreas onde seu uso possa ser aplicado;
- Elaborar a monografia resultante com os resultados das pesquisas.

2 Fundamentação Teórica

Este capítulo apresenta algumas das possíveis aplicações de Redes de Sensores Sem Fio em diversas áreas e uma revisão bibliográfica sobre o tema abordado no Trabalho de Conclusão de Curso (TCC).

2.1 Aplicações de Redes de Sensores Sem Fio

2.1.1 Considerações Iniciais

As Redes de Sensores Sem Fio (RSSFs) podem ser vistas como um tipo especial de rede móvel ad hoc[1] (MANET - *Mobile Ad Hoc Network*) e como uma das vertentes da computação ubiqua[2]. Uma RSSF pode ser utilizada para monitorar e, eventualmente, controlar o ambiente no qual se encontra. Este tipo de rede é tipicamente formada por centenas ou milhares de dispositivos autonômicos chamados nós sensores. Os principais componentes de um nó sensor são: transceptor para realizar a comunicação sem fio, fonte de energia, dispositivos sensores, memória e processador. Os nós sensores tendem a ser projetados com pequenas dimensões, e esta limitação de tamanho impõe restrições aos recursos dos nós, tais como as capacidades da fonte de energia, transceptor e processador. O componente lógico de um nó sensor é o software que executa em seu processador. Apesar do fato de que os nós individualmente possuem pequenas capacidades de energia e computacional, a cooperação entre eles permite a execução de tarefas maiores. (SILVA et.al.,2003)

Segundo (Cabrini, 2006), os principais fatores que afetam o desempenho de uma RSSF são:

- Fenômenos atmosféricos;
- Fontes móveis de interferência;

xvixvi

[1] Redes Ad Hoc: Tipo de rede que não possui um nó especial (ponto de acesso) para o qual todas as comunicações convergem e que as encaminha para os respectivos destinos.

[2] Computação Ubíqua: Tem como objetivo tornar a interação pessoa-máquina invisível, ou seja, integrar a informática com as ações e comportamentos naturais das pessoas.

- Desastres naturais;
- Quebra acidental;
- Bloqueio do processador;
- Falhas maliciosas;
- Interferências eletromagnéticas;
- Posicionamento dos nós.

Tais falhas podem ser classificadas como sendo permanentes ou transitórias. (Cabrini, 2006)

2.1.2 Histórico

Segundo (Lima, 2010): “Apesar do crescente interesse pelas RSSFs observado em publicações científicas, esta tecnologia não é recente. Desde 1980, na época da Guerra Fria, já havia projetos para a utilização de redes de sensores no controle e detecção do movimento de tropas inimigas e monitoramento prévio de ambientes hostis. Neste período, sistemas de detecção de sons empregavam os conceitos destas redes. Um grande número de sensores acústicos foram inseridos no fundo do oceano, visando detectar submarinos soviéticos. Ainda durante a Guerra Fria, redes usando sensores foram utilizadas nos sistemas de defesa aérea desenvolvidos para proteção dos Estados Unidos e Canadá. Redes de sensores mais modernas começaram a ser desenvolvidas quando a Agência de Projeto e Pesquisa Avançada de Defesa (DARPA) introduziu o projeto DSN (Rede de Sensores Distribuídos). Este projeto identificou os componentes tecnológicos necessários, que incluíam sensores acústicos, protocolo para comunicação, algoritmos e técnicas de Redes de Sensores processamento e software distribuído. A rede foi imaginada de forma distribuída e esparsa, na qual seus nós teriam baixo custo e realizariam um roteamento eficiente transmissão de dados.”

Deve-se lembrar que nesse tempo havia muitas limitações tecnológicas para construir um módulo sensor como a inexistência de computadores pessoais, modens atingindo taxas de transmissão baixíssimas. Então, os pesquisadores decidiram criar um sistema que identifica um objeto por meio do som. O MIT (*Massachusetts Institute of Technology*), desenvolveu um sistema

capaz de detectar e seguir um objeto analisando e comparando sinais, usando um conjunto de microfones. No final dos anos 80, este sistema foi testado através do programa DNS, que possibilitou detectar e seguir o movimento de um avião a baixa altitude, usando uma rede de sensores e um processamento centralizado. Nessa época, as RSSFs eram arcaicas e havia grande dependência da rede com os operadores humanos. As redes de sensores atuais exploram tecnologias que não existiam há duas décadas atrás e executam funções que não eram possíveis no passado. Atualmente, sensores, processadores e dispositivos para comunicação sem fio se tornaram menores e mais baratos, o que possibilitou o avanço das redes de sensores. Comparando os sensores desenvolvidos nos anos 80/90 com os atuais pode-se perceber uma evolução na topologia da rede e arquitetura do nó sensor. Inicialmente a sensorização, o processamento e a comunicação eram separados. Hoje, estes três processos estão integrados. O tipo de alimentação, consumo de energia e a longevidade das baterias contribuíram de maneira significativa para o desenvolvimento das RSSFs. (Lima, 2010)

Segundo (Winkler, et. al, 2008), de forma similiar à evolução da tecnologia de celulares, é possível descrever a evolução dos dispositivos sensores militares em termos de gerações:

- **Primeira geração de redes sensores:** Redes de sensores consistem de dispositivos individuais de sensores. A colocação é realizada de forma manual. A rede é totalmente pré-configurada. O acesso à informação através de forma manual do dispositivo em si, ou *links* de comunicação ponto-a-ponto de longo alcance;
- **Segunda geração de redes sensores:** Sensores trabalham de forma colaborativa para cobrir a área. A rede é tipicamente um agrupamento de um pequeno número de sensores (3 ou 4) comunicando com o nó controlador. São tipicamente posicionados manualmente, dependendo pesadamente da pré-configuração;
- **Terceira geração de redes sensores:** A última geração de sensores engloba a auto organização, a flexibilidade e a escalabilidade das redes. Sensores se comunicam entre si para dois propósitos: serviços de comunicação e processamente interno da rede. Redes de sensores podem conter dezenas e até centenas de nós e o posicionamento pode

ser realizado manualmente ou remotamente através de dispositivos aéreos. Os sensores são aptos para estabelecer e, se necessário, publicar e fazer uso de sua própria localização geográfica, baseada no GPS.

2.1.3 Áreas de Aplicação

Segundo (SILVA et.al., 2003) uma RSSF pode ser utilizada nas mais diversas áreas de aplicação, como por exemplo:

- **Monitoração de Espécies:** É possível que um grupo de cientistas deseje ou precise aprender sobre uma espécie animal específica e/ou também sobre um grupo formado por eles. Neste caso, uma RSSF contendo dispositivos sensores de temperatura, aceleração, luminosidade, dentre outros, pode ser espalhada dentro do habitat natural destes animais. O uso desta tecnologia permitiria um alto grau de observabilidade, proximidade e veracidade, uma vez que não seria necessária a presença de nenhum ser humano ou de grandes equipamentos para a realização da monitoração;
- **Qualidade do ar:** Uma RSSF contendo dispositivos sensores de temperatura e gases tóxicos é capaz de controlar a qualidade do ar de um edifício, uma praça, um bairro, ou até mesmo de uma cidade inteira, com precisão e rapidez, tratando e disseminando instantaneamente os dados coletados. A presença humana é eliminada;
- **Monitoração industrial:** Existem diversas aplicações que podem ser aplicadas as necessidades de cada um dos tipos de indústria. Uma RSSF seria capaz de monitorar qualidade do ar e temperatura de um galpão ou forno, além de controlar os bens produzidos e o maquinário complexo e condições do sistema de uma determinada fábrica;
- **Aplicações para o exército:** O exército é uma entidade que está sempre procurando ou mesmo desenvolvendo novas tecnologias de alta qualidade, as quais podem ser utilizadas em diversas situações de guerra. Uma RSSF é uma destas tecnologias, e pode ser utilizada para a monitoração dos movimentos de inimigos, gases tóxicos, além de

preservação de fronteiras e escuta e interferência de transmissões de inimigos. (SILVA et.al., 2003)

- **Aplicações médicas:** Quando os nós sensores das RSSFs se tornarem dispositivos menores, mais baratos e específicos, será possível utilizá-los em aplicações complexas, como por exemplo, aplicações médicas. No futuro, será possível se colocar nós sensores dentro do corpo de um animal ou até mesmo de um ser humano, permitindo que eles formem uma RSSF que poderá monitorar vários aspectos como níveis de oxigênio, insulina ou colesterol, além do volume e tamanho dos órgãos.

2.2 **Redes de Sensores Sem Fio**

2.2.1 Nós Sensores

Um sensor é um dispositivo tecnológico com capacidade de detectar eventos ou determinadas condições físicas em ambientes ou substâncias, gerando um sinal elétrico em resposta ao sensoriamento realizado. Um sensor inteligente tem a capacidade de traduzir este sinal elétrico em informação digital e realizar algum tipo de processamento sobre ele para, em seguida, enviar a informação gerada através de uma rede, para ser utilizada por uma aplicação. (Meira, 2007)

Os principais componentes de um nó sensor são: unidade de comunicação sem fio, unidade de energia, unidade de sensoriamento, unidade de computação. O componente lógico de um nó sensor é o *software* que executa na unidade de computação. Os nós sensores tendem a ser projetados com pequenas dimensões e esta limitação de tamanho acaba impondo limitações nos recursos dos nós, tais como capacidade da fonte de energia, processador e transceptor. Apesar dos nós possuírem individualmente pouca capacidade computacional e de energia, um esforço colaborativo entre os mesmos permite a realização de uma tarefa maior. Em alguns casos, uma RSSF também pode ser composta de dispositivos atuadores que permitem ao sistema controlar parâmetros do ambiente monitorado. (SILVA et.al., 2003) Dependendo da arquitetura implementada ou das necessidades das aplicações usuárias, os nós sensores também podem contar com componentes adicionais, a exemplo de sistema para localização do nó, como GPS (*Global Positioning*

System), sistema de mobilidade do dispositivo e gerador autônomo de energia. (Meira, 2007).

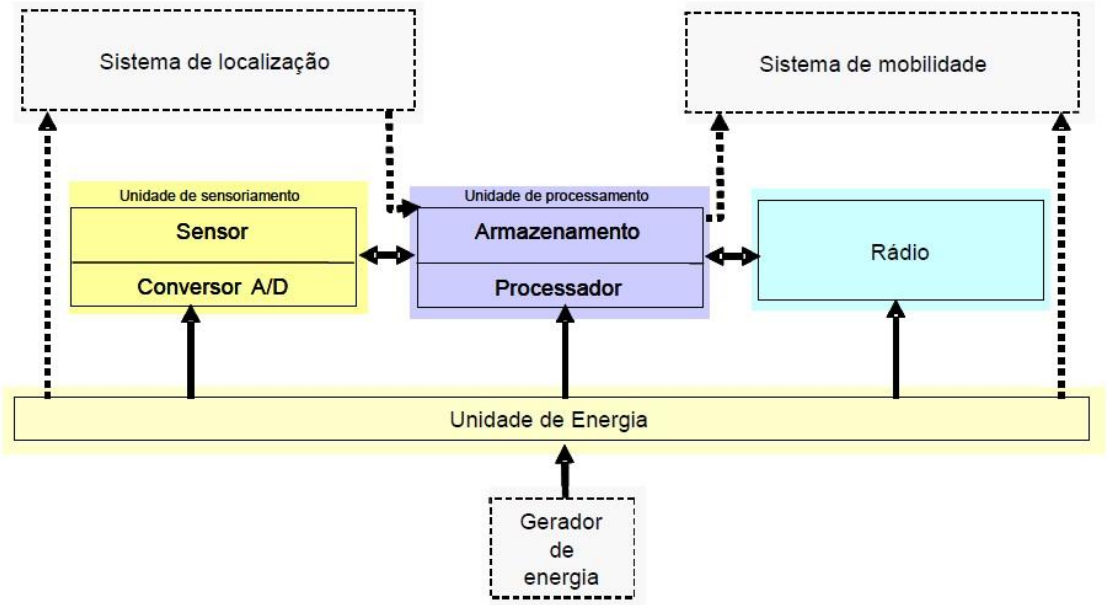

Figura 1 – Componentes de um nó sensor. (Meira,2007)

2.2.1.1 Unidade de Energia

Em geral, baterias de energia finita são utilizadas como fontes de energia dos nós sensores. Existem diferentes tecnologias de fabricação, referindo-se ao consumo de energia. A escolha da bateria a ser utilizada nos nós sensores deve considerar algumas características como volume, condições de temperatura e capacidade inicial. Os tipos mais comuns de bateria dos nós sensores são: linear simples, lítio NR e lítio *Coin Cell*. (SILVA et.al., 2003)

Para RSSFs, uma fonte de energia contínua e disponível no ambiente é de grande importância. Por exemplo, células solares podem contribuir com 15 mWatts por centímetro quadrado se expostas diretamente ao sol e 0,15 mWatts em dias nublados. Para algumas aplicações, como em ambientes fechados, este tipo de fonte pode não ser suficiente. Outros tipos de fontes de energia, como por exemplo a vibração (fricção) e/ou através de sons (acústico), podem então ser utilizados. (SILVA et.al., 2003)

O bloco de fornecimento de energia consiste em uma bateria e um conversor de corrente contínua que tem o propósito de fornecer energia ao

dispositivo, já que o nó sensor necessita de energia para monitorar o ambiente. Pode ser possível aumentar o tempo de vida de um nó sensor ao se extrair energia do ambiente, como por exemplo luz, vibração e rádio-frequência. Hoje em dia, transitores *CMOS* e arranjos células solares podem ser co-fabricados. O processo Icarus combina células solares, *CMOS* de alta voltage e silicone em isolador – Estruturas *MEMS* no mesmo molde. Com a adição de trincheiras de isolamento, dispositivos e estruturas *MEMS* podem ser elétricamente isolados, e células solares podem podem ser empilhadas para fornecer altas voltagens. (Vieira, 2003)

Baterias fornecem energia para nós sensores. É importante escolher o tipo de bateria, já que isso pode afetar o projeto do nó sensor. Circuito de Proteção de Bateria para evitar sobrecarga e/ou grande descarga, regulador de voltagem e outros components podem ser acrescentados aos nós sensores. Existem vários tipos de baterias sendos utilizadas em uma grande variedade de aplicações. Baterias podem ser dividias em primárias (não recarregáveis) e secundárias (recarregáveis). Elas também podem ser classificadas de acordo como o material eletro-químico utilizado para eletrodo, como NiCd, NiZn, AgZn, NiMh, e *Lithium-Ion*. O tipo de bateria dependerá da aplicação. Se não há fonte de energia aproveitável, baterias não recarregáveis são uma boa escolha, já que baterias não recarregáveis possuem densidade energática mais alta. Entre as baterias recarregáveis, baterias baseadas em Lítio aparecem como a melhor escolha. Entretanto, existem outras considerações e a escolha adequada da tecnologia da bateria não é uma escolha óbvia sem um exame detalhado do perfil operacional da aplicação. Por exemplo, em um cenário de pulso de descarga, uma bateria de Lítio teria uma péssima performance, enquanto uma bateria de Níquel-Cádmio possuiría uma boa performance devido às grandes diferenças na resistência interna desses tipos de baterias. Além disso, baterias de Lítio possuem alto custo. Entre os tipos de bateria recarregáveis, a de hidreto metálico de Níquel (NiMH) é a única não agressiva ao meio ambiente. Sua densidade energética só é menor do que a das baterias de Lítio e ela pode ser recarregada a qualquer momento sem experimentar perda de voltagem. A desvantagem é que este método precisa de proteção contra sobrecarga e grande descarga. (Ibidem)

Existem dois esquemas de economia de energia principais, gerenciamento de energia dinâmico (*DPM - dynamic power management*) e

agendamento de voltagem dinâmico (*DVS - dynamic voltage scheduling*). A idéia básica por trás do *DPM* é o desligamento de dispositivos quando não são necessários e seu religamento quando necessários. Desligar alguns componentes fornece uma boa economia de energia, mas em vários casos, não é sabido antecipadamente quando ligar ou desligar um dispositivo em particular. A solução é uma análise estocástica para prever eventos futuros. Um sistema operacional embutido capaz de suportar *DPM* também é necessário. Para esta abordagem, o microcontrolador deve ter os estados: ativo, dormir e inativo. Contudo, é importante considerer que transitar entre estes modos operacionais envolvem despesas gerais de energia e latência. A idéia principal por trás do *DVS* é carregar energia suficiente para a carga de trabalho, evitando ciclos inativos. *DVS* reduz a energia consumidapelo processador reduzindo sua voltagem operacional. Variando a voltagem junto com a frequência, é possível obter uma redução quadrática no consume de energia. O problema é o fato de que cargas de trabalho futures não são determinísticas. Para esta abordagem, o microcontrolador deve permitir a troca de seu fornecimento de energia. A escolha tem sido *StrongARM* SA-1100 que pode variar sua voltagem e frequência de 59MHz/0.79V para 251 MHz/1.65V. (Ibidem)

2.2.1.2 Unidade de Comunicação

A unidade de comunicação inclui todo o sistema de transmissão e recepção, amplificador e antena. Segundo (SILVA et.al.,2003), os dois tipos de comunicação mais utilizados nas arquiteturas de nós sensores são: comunicação por *laser* (ótica) e Rádio Frequência (RF).

Segundo (Vieira, 2003), nós sensores devem se comunicar entre eles e também com uma estação base usando um canal de comunicação sem fio. As principais possibilidades são ótica, infra-vermelho e rádio-frequência (RF).

As vantagens das comunicações óticas, segundo (Vieira, 2003), são:

- Gastar menos energia que RF;
- Segurança, já que não há transmissão *broadcast* e se o canal for incerteceptado o sinal será interrompido;
- Sem necessidade de antenas.

Ainda segundo (Vieira, 2003), as desvantagens são:

- Precisa de linha de visão (*LOS – Line of Sight*), já que o raio *laser* do dispostivo transmissor deve ser alinhado ao recebedor ótico;
- Sensível às condições atmosféricas;
- A comunicação é directional e já que o sensor sera posicionado, isto não é uma solução atrativa.

A comunicação infra-vermelho é normalmente direcional. Já que nós sensores serão posicionados, uma boa solução adotada pelo projeto *PushPin* é usar um difusor feito de um tubo de policarbonato jateado para criar um alcance de comunicação mais omnidirecional. A principal desvantagem do infra-vermelho é o pequeno alcance de apenas 1 metro. Sua vantagem éque o uso de uma antena é desnecessário. (Vieira, 2003)

Comunicação RF é baseada em ondas eletromagnéticas. Um dos desafios mais importantes nos dispostivos de comunicação RF é o tamanho da antena. Para otimizar a transmissão e a recepção, uma antenna deve ser pelo menos λ/4, onde λ é o comprimento de onda da frequência do portador. Assumindo o rádio de um nó sensor com um quarto de comprimento de onda como sendo 1mm, a frequência do portador RF teria de ser de 75 GHz, o que é um pouco fora do alcance de eletrônicos RF de baixo consumo de energia. Também é necessário reduzir o consume de energia com modulação, filtragem, demodulação, etc. As vantagens da comunicação RF são a facilidade de uso, integralidade e um Mercado bem estabelecido, o que o faz uma plataforma de testes ideal para nós sensores. Vários aspectos afetam o consumo de energia de um rádio, incluindo o tipo de modulação, esquema usado, taxa de dados, potência de transmissão. Em geral, rádios podem operar em 4 modos de operação distintos: transmitir, receber, inativo e dormir. A maioria dos rádios operand no modo inativo resultando em um grande consume de energia, quase equivalente o modo de recebimento, deste modo, é importante desligar o rádio. (Vieira, 2003)

2.2.1.3 Unidade de Computação

A memória e o processador estão envolvidos nas atividades de computação realizada pelo nó. Quanto maior a freqüência do processador,

maior o consumo de energia. O consumo do processamento pode ser medido pelo número de ciclos de relógio para diferentes tarefas como o processamento de sinais, verificação de código de erro, etc. Algumas das características dos processadores utilizados em nós sensores são: operam em baixa freqüência (a maioria utiliza processadores de 4 MHz), possuem um baixo custo com energia e baixa capacidade de armazenamento, por exemplo 4 e 128 KB. (SILVA et.al., 2003)

Já que se espera que o nó sensor seja capaz de comunicar, de processor e de colher dados, nós sensores devem possuir unidades de processamento. A unidade central de processamento de um nó sensor determina em um alto grau tanto o consume de energia quanto as capacidades computacionais de um nó sensor. Existe um grande número de microcontroladores , microprocessadores e Arranjos de Portas Programáveis em Campos (*FPGAs – field programmable gate arrays*) comercialmente disponíveis, que permitem uma grande flexibilidade para a implementação de *CPUs*. (Vieira, 2003)

Hoje em dia, *FPGAs* apresentam duas grandes desvantagens. Embora existam no mercado *FPGAs* de baixo consumo de energia como o *CoolRunner-II CPLDs*, seu consumo não é baixo o suficiente como deveria ser para um nó sensor. Por exemplo, *CoolRunner-II* operando a 1.8V e 20MHz necessita de um fornecimento de energia de 17.22 mA. Outra desvantagem é que não é possível desligar blocos separados de *FPGAs*. Somando ao fato de consumirem mais energia, os *FPGAs* não são compatíveis com metodologias de programação tradicional (por exemplo, não possui compilador C). Isso não significa que os *FPGAs* não serão uma boa solução em um futuro próximo. Talvez com o desenvolvimento de *FPGAs* de baixíssimo consume de energia, eles serão uma boa solução para um nó sensor monitorando um planeto, já que eles possuem as vantagens de serem reprogramáveis e reconfiguráveis, eliminando gastos com posicionamento em aplicações espaciais. (Ibidem)

Atualmente, microcontroladores incluem não só memória e processador, como também memória não volatile e interfaces como contadores e timers. Neste caso, el epode iterar com sensores e dispositivos de comunicação como rádios de curto alcance para compor um nó sensor. Existem vários tipos de microcontroladores, de 4 a 32 bits, variando o número de timers, consume de energia e etc. Embora microcontroladores Atmel AVR sejam normalmente

usados, existem melhores alternativas para nós sensores. PIC é usado para propósitos educacionoais, mas não aplicável onde energia é crucial. 8051 é disponível para qualquer um em qualquer lugar, mas possui baixa performance, sendo utilizado somente por razões históricas. O Microcontrolador MSP430F149 é uma boa opção para nós sensores, já que é um *MIPS* de 16 bits, fornecendo grande poder computacional, além de baixíssimo consumo de energia. É equipado com com um conjunto completo de processadores digitais e analógicos. Ele possui depuração embutida e é suportado por diversas ferramentas de desenvolvimento, incluindo o gcc. (Ibidem)

2.2.1.4 Unidade de Sensoriamento

Um dispositivo sensor é um dispositivo que produz uma resposta mensurável para uma mudança na condição física (e.g., temperatura, pressão, campo magnético, estresse mecânico, presença ou ausência de movimento, áudio, vídeo). Dispositivos sensores geralmente têm características físicas e teóricas diferentes. Assim, numerosos modelos de nós sensores de complexidade variável podem ser construídos baseado nas necessidades das aplicações. (SILVA et.al., 2003)

2.2.2 Funcionamento

O funcionamento de uma Rede de Sensores Sem Fio será adaptado de acordo com aplicação para a qual ela for requisitada, ou seja, de acordo com as características da aplicação e dos dados a serem coletados, a RSSF terá que identificar o maior número de requisitos e adaptar-se a eles. Para auxiliar esta tarefa existe um conjunto de passos a serem seguidos, como veremos nos tópicos abaixo. (Loureiro et.al.,2003)

2.2.2.1 Estabelecimento da Rede

Independentemente do tipo de aplicação e dados a serem coletados, o estabelecimento da rede envolve a distribuição dos nós. Ao distribuir os nós para a formação da rede, é necessário levar-se em conta fatores como a localização e os possíveis obstáculos que eles possam vir a enfrentar. (Loureiro et.al.,2003)

2.2.2.2 Sensoriamento

A tarefa de sensoriamento está relacionada com a coleta de dados e a percepção do ambiente em si. De acordo com o tipo de aplicação e os dados que deverão ser coletados pela rede, vários fatores devem ser levados em conta como por exemplo distância do alvo, amostragem, ruídos do ambiente, etc.. (Loureiro et.al., 2003)

Outro fator a observar é a existência de áreas de intersecção entres os sensores. Caso existam dois sensores que tenham uma intersecção em sua área de monitoramento, pode se levar em conta a possibilidade de desativar um sensor e deixar apenas um fazendo o monitoramento. Em caso de falhas, seja ela por falta de energia ou destruição do nó sensor, é necessário avaliar se o número de nós que cobrem a área do nó afetado serão suficientes para fazer o monitoramento. (Loureiro et.al., 2003)

2.2.2.3 Coleta de Dados

O objetivo da RSSF é coletar informações a respeito de uma área de observação especifica. A atividade de coleta leva em consideração o cálculo da área de cobertura e a exposição dos sensores em relação ao alvo. (Loureiro et.al., 2003). O modo como os dispositivos realizam as coletas de dados dependem, por definição, da aplicação para a qual eles servem (Meira, 2007). Ainda segundo (Meira, 2007), este aspecto classifica a RSSF conforme seu método de sensoriamento, da seguinte forma:

- **RSSF de Tempo Real:** os nós sensores coletam os dados no momento em que a atividade associada acontece, buscando realizar maior amostragem possível dos dados num menor intervalo possível exigida pela aplicação. São utilizados por aplicações que envolvem risco para vidas humanas ou aplicações onde a rapidez da disponibilização do dado coletado é importante na tomada de decisão e definição de estratégias. Exemplos: monitoração de áreas sujeitas a desastres naturais e aplicações militares;
- **RSSF Periódica:** os nós sensores coletam dados sobre os fenômenos em intervalos regulares e pré-definidos. Um exemplo são as aplicações que monitoram animais em florestas. A coleta de dados é feita durante o período em que a espécie monitorada

estiver em atividade, e são desligados durante o período em que os animais estiverem repousando;

- **RSSF Contínua:** os nós sensores coletam os dados continuamente, sem interrupção. Um exemplo são as aplicações de exploração interplanetária ou sondas espaciais que coletam dados continuamente, até a extinção da atividade do dispositivo, contribuindo para a formação de base de dados para pesquisas;
- **RSSF Reativa:** os nós sensores coletam dados em resposta ao disparo de eventos pré-programados ou quando solicitado pela aplicação de monitoração. Exemplos são as aplicações de detecção de presença ou gatilhos para determinadas condições ambientais, a exemplo de detectores de calor ou fumaça;
- **RSSF Híbrida:** rede que adota mais de uma abordagem para coleta de dados, sendo que a aplicação implementada avalia em que circunstância o método mais adequado será utilizado.

2.2.2.4 Processamento

O processamento em uma rede de sensor pode ser dividido em processamento de suporte e processamento de informação. O processamento de Suporte é um processamento gerencial, que verifica o estado da RSSF. (Loureiro et.al., 2003)

O processamento de Informação é o processamento que deverá ser feito sobre a informação coletada, como por exemplo, criptografia, compressão, etc. (Loureiro et.al., 2003)

2.2.2.5 Comunicação

A comunicação entre os nós é estabelecida de acordo com o protocolo que estiver sendo utilizado. Outros fatores que devem ser levados em conta na comunicação é o fato que os nós podem ter mobilidade. (Loureiro et.al., 2003)

Em relação a forma de entrega dos dados para a aplicação alvo da RSSF, essas redes podem ser classificadas, segundo (Meira, 2007), como:

- **Contínuas:** os nós sensores coletam dados e enviam à aplicação destino de forma contínua, durante todo o tempo de vida dos nós;
- **Sob demanda:** os nós sensores coletam dados e enviam à aplicação destino em resposta a uma consulta dessa aplicação;

- **Orientadas a eventos:** os nós sensores podem coletar e enviar dados quando detectam eventos que podem ocorrer no ambiente monitorado, ou conforme determinados critérios pré-estabelecidos na aplicação;
- **Híbridas:** quando mais de uma abordagem coexistem na mesma rede.

É Importante notar que a adoção de abordagens de envios contínuos de dados faz o consumo de energia crescer rapidamente, o que influencia negativamente no tempo de vida dos nós sensores. (Meira, 2007)

2.2.2.6 Manutenção

A manutenção tem como objetivo principal prolongar a vida útil da RSSF, corrigindo imprevisibilidades e verificando se a aplicação esta correspondendo aos requisitos especificados. (Loureiro et.al., 2003)

2.3 Protocolos de Comunicação e Segurança

A sessão a seguir retrata os principais protocolos utilizados por RSSFs e uma série de considerações sobre a segurança das mesmas.

2.3.1 Protocolos

Um protocolo especifica detalhes para os aspectos da comunicação entre computadores, incluindo ações a serem tomadas quando erros ou situações inesperadas ocorrem. Um dado protocolo pode especificar detalhes de baixo nível, como por exemplo, a voltagem e/ou sinais a serem utilizados, ou ainda detalhes de alto nível, como o formato das mensagens que os programas da aplicação trocam entre si. (COMER, 2009)

Protocolos para Redes *Ad-Hoc* como o *Bluetooth* podem ser utilizados para se realizar a comunicação em uma RSSF. Porém, protocolos dos gêneros não representam as melhores soluções para os problemas específicos os quais as RSSFs visam resolver. Para isso, protocolos de comunicações especiais

foram criados para as aplicações que se utilizam de Redes de Sensores Sem Fio. (ARAÚJO et. al., 2007)

Embora o protocolo mais utilizado seja o *ZigBee*, o protocolo mais popular, no sentido de que a maioria dos demais protocolos se basearam nele, é o protocolo LEACH (*Low Energy Adaptive Clustering Hierarchy* – Hierarquia de Clusterização Adaptativa de Baixa Energia). (YASSEIN et. al., 2008)

Em seguida, além do protocolo LEACH, trataremos de outros protocolos utilizados em RSSF's.

2.3.1.1 Leach

O *Leach* é um protocolo eficiente em energia para redes sem mobilidade. O *Leach* usa uma arquitetura baseada em *clusters*, onde os nós que fazem parte de um cluster enviam seus dados apenas para o nó raiz desse cluster, o *cluster-head*. Nesse *cluster-head* há a agregação dos dados de cada sensor do cluster, havendo o tratamento de informações redundantes, e o envio desses dados para a estação base. (ARAÚJO et. al., 2007)

Para resolver o problema da falta de energia, há uma rotação dos *cluster-heads*, ou seja, a atribuição no tempo de diferentes nós como *cluster-heads* de um dado cluster, havendo um gasto de energia mais uniforme entre os nós e evitando também que a perda de um *cluster-head* leve à inutilização da rede. A comunicação entre os nós e o *cluster-head* é feita através de TDMA. (ARAÚJO et. al., 2007)

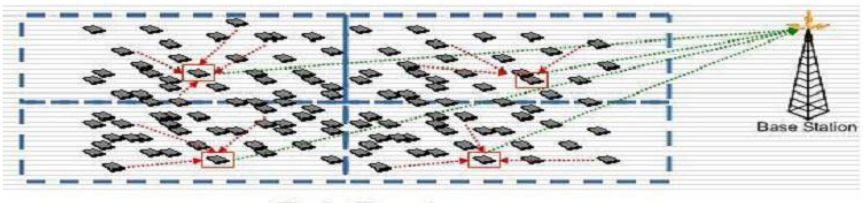

Figura 2 – Clusterização
(http://alkautsarpens.wordpress.com/2008/12/01/leach-pegasis-bcdcp/)

2.3.1.2 Leach-C

O *LEACH-C* é uma variação do *LEACH* que centraliza as decisões de formação dos grupos na estação base. A maior vantagem desta abordagem

centralizada é a criação e distribuição mais eficiente de grupos, na rede. Cada nó, na fase de inicialização da rede, envia sua posição geográfica e energia disponível para a estação base. Baseando-se nesta informação, a estação através de processos de *simulated annealing* (pareamento simulado), determina os grupos de forma centralizada. (RUIZ et. al., 2004)

Quando os grupos e seus líderes são determinados a estação base envia uma mensagem que contém o identificador do líder (*cluster-head*) para cada nó. Após esta fase, os nós agem como no *LEACH* original comunicando-se apenas com seu líder. (RUIZ et. al., 2004)

2.3.1.3 *Direct Difusion* (Difusão Direta)

Na difusão direcionada, o nó que deve transmitir informações nomeia os dados usando um par de atributos, que descrevem a tarefa a ser desempenhada. A estação base (*sink*), propaga seus interesses, ou seja, quais atributos quer receber. Os nós vizinhos propagam essa informação, que, ao passar pelos nós, preenchem um campo de gradiente, ou seja, a distância percorrida, e, ao chegar em um nó que contenha o atributo de interesse, este o envia através do caminho do gradiente até a estação base, não havendo identificação prévia dos nós na rede. Abaixo é exibido o esquema da difusão direta. (ARAÚJO et. al., 2007)

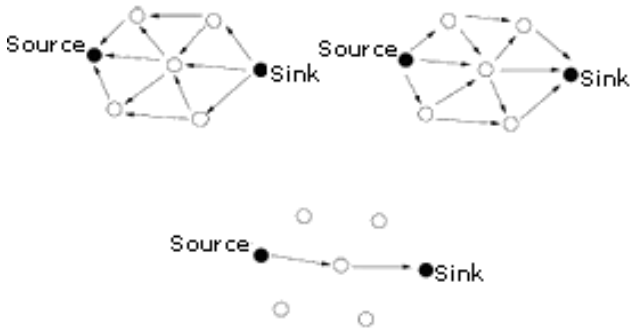

Figura 3 – Esquema de Difusão Direta

2.3.1.4 TEEN (Threshold sensitive Energy Efficient sensor Network)

O *TEEN* (*Threshold sensitive Energy Efficient sensor Network*) (Manjeshwar, 2001) é protocolo de roteamento hierárquico similar ao LEACH exceto pelo fato de que os nós sensores podem não possuir dados a serem transmitidos de tempos em tempos. Os autores deste protocolo propõem classificar as redes de sensores em redes pró-ativas e redes reativas. (ARAÚJO et. al., 2007)

Uma rede pró-ativa monitora o ambiente continuamente e possui dados a serem enviados a uma taxa constante. Em uma rede reativa os nós somente enviam dados quando a variável sendo monitorada se incrementa acima de um certo limite. (ARAÚJO et. al., 2007)

TEEN utiliza a estratégia de formação de líder do *LEACH*, mas adota uma estratégia diferente na fase de transmissão de dados. Ele faz o uso de dois parâmetros chamados *Hard Threshold* (HT) e *Soft Threshold* (ST) para determinar a necessidade de transmissão do dado coletado. Se o valor exceder HT pela primeira vez, ele é armazenado em uma variável e transmitido durante o intervalo (*slot*) de tempo alocado a transmissão do nó. Em seguida, se o valor monitorado exceder o valor armazenado por uma magnitude de ST o nó transmite o dado imediatamente. O valor enviado é armazenado para comparações futuras. (ARAÚJO et. al., 2007)

2.3.1.5 Pegasis (Power-Efficient Gathering in Sensor Information Systems)

O PEGASIS (*Power-Efficient Gathering in Sensor Information Systems*) é um protocolo para RSSF baseado no conceito de correntes. Cada nó troca informações apenas com os vizinhos mais próximos formando uma corrente entre os nós, e apenas um nó é escolhido a cada momento para transferir as informações coletadas ao nó *gateway*. Portanto, o número de trocas de mensagens será baixo e a comunicação será realizada entre nós próximos uns dos outros. (ARAÚJO et. al., 2007)

Espera-se com isso que a energia gasta seja menor, se comparada a outros protocolos que requerem muitas trocas de mensagens para eleger

líderes e formar grupos, e protocolos em que os nós constantemente trocam mensagens com o nó *gateway* de forma direta (o *gateway* geralmente se encontra distante dos nós). Isto implica um tempo de vida maior para cada nó e um consumo menor da largura de banda da rede. (ARAÚJO et. al., 2007)

O PEGASIS assume o seguinte:

- O nó *gateway* (estação base) situa-se estacionado à uma distância fixa da rede;
- Os nós são capazes de transmitir dados diretamente para o nó *gateway* e para qualquer outro nó;
- Cada nó possui informação de localização dos outros nós;
- Os nós são homogêneos e com o nível de energia uniforme;
- Os nós não são móveis. A cada round um nó é escolhido para transmitir a informação à estação base. (Ruiz et al., 2004)

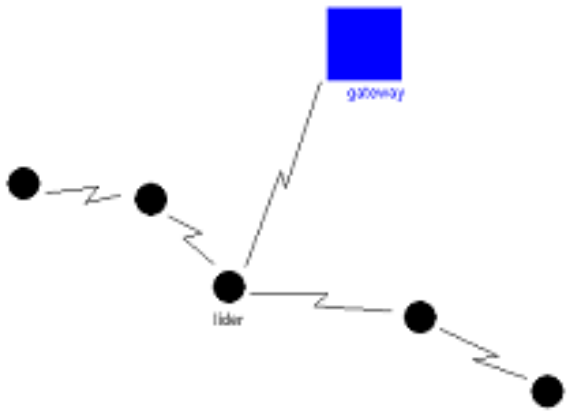

Figura 4 – Protocolo PEGASIS (Ruiz et al., 2004)

2.3.1.6 ICA (Inter Cluster Routing Algorithm)

O protocolo ICA (*Inter Cluster Routing Algorithm*) é baseado no *LEACH*, sendo idealizado para aumentar o tempo de vida e o número de pacotes enviados na rede. O ICA inicia com a estaçãao rádio base enviando um broadcast para todos os nós informando sua posição geográfica. Após esta

fase, os nós sabem a posição geográfica da estação base e é assumido que também sabem suas próprias posições. (ARAÚJO et. al., 2007)

No ICA os nós são agrupados em clusters que seguem as mesmas regras de formação do *LEACH*, a não ser pela decisão de qual *cluster* os nós vão participar. Esta informação é dada pela proximidade dos nós aos *cluster-heads*. O nó vai estar ligado sempre ao cluster-head mais próximo. (ARAÚJO et. al., 2007)

O processo de formação de clusters dissemina a informação da formação de clusters pelos *clusters* vizinhos. No ICA, ao contrário do *LEACH*, os *cluster-heads* tentam não enviar as mensagens diretamente para a estação base. Ao invés disto eles, em uma abordagem gulosa, enviam as mensagens para o *cluster-head* mais próximo, na direção da estação base. O objetivo é economizar energia enviando as mensagens ponto a ponto para nós que estão a uma distância menor que a estação base. Desta forma, a quantidade de energia consumida por cada nó da rede diminui e a quantidade de energia total da rede aumenta. (ARAÚJO et. al., 2007)

Para evitar o problema da morte prematura dos nós perto da estação base, os *cluster-heads* no ICA podem se recusar a retransmitir mensagens de outros *clusters* para a estação base. Isto ocorre quando o *cluster-head* percebe que está ficando sem energia. Para evitar que não possa enviar as mensagens do seu próprio *cluster* ele para de rotear mensagens de outros *clusters* para a estação base. (ARAÚJO et. al., 2007)

Quando ocorre uma recusa em retransmitir dados, o *cluster-head* que requisitou o serviço de roteamento envia a mensagem diretamente a estação base, da mesma forma como ocorre no *LEACH*. Esta abordagem tenta impedir o aparecimento de áreas descobertas perto da estação base. Isto deveria ocorrer rapidamente uma vez que todas as mensagens da rede veriam passar por estes nós antes de chegar à estação base. (Ruiz et al., 2004)

2.3.1.7 Wi-Fi (Wireless Fidelity)

Wi-Fi, abreviatura de "*wireless fidelity*" e também conhecida como *Wireless* LAN (WLAN), é marca registrada pertencente à *Wireless Ethernet Compatibility Alliance* (WECA). Trata-se de uma rede local sem fio padronizada pelo IEEE 802.11. (Rodrigues, 2008)

Segundo (Rodrigues, 2008), redes WLAN têm como principais aplicações:

- Redes locais internas de residências, empresas, lojas e escritórios, complementando ou até mesmo substituindo redes que utilizam cabeamento, seja por praticidade ou necessidade, visto que a instalação de cabos e fios é dificultosa em certos locais;
- Redes públicas de acesso à internet são mais conhecidas pelo nome de Wi-Fi.

As redes *Wi-Fi* possuem como principais vantagens, de acordo com (Rodrigues, 2008):

- Possui taxas de transferência relativamente altas, principalmente se for levado em consideração o novo padrão 802.11n que supera com facilidade o padrão Ethernet de 10Mbps e até mesmo o Ethernet de 100Mbps;
- Possui um alcance médio. No padrão g é possível atingir em campo aberto algo em torno de 200 metros, enquanto em campo fechado se alcança no máximo um raio de 50 metros. Antenas podem ser agrupadas ao sistema para aumentar essa distância, porém além de se tornar mais custoso ainda elevaria bastante o consumo de energia;
- Através do antigo protocolo *WEP,* e o mais recente chamado *WPA*, que surgiu para suprir as limitações de *WEP*. A segurança em redes *Wi-Fi* se encontra em um nível satisfatório, porém devido a seu alto uso em situações críticas, como transações financeiras por exemplo, muito ainda precisa ser pesquisado.

E como principais desvantages, também de acordo com (Rodrigues, 2008):

- Apesar de não haver custos para a utilização do padrão Wi-Fi, os custos de aquisição dessa tecnologia ainda é um pouco alta, devido a sua taxa de transferência ser relativamente grande;
- Apresenta um consumo de energia bastante relevante devido a sua alta banda. Isso torna inviável a alimentação por baterias.

2.3.1.8 Bluetooth

Bluetooth é uma tecnologia de comunicação sem fio de baixo custo que começou a ser desenvolvida em 1994 pela Ericsson, e a partir de 1998 pelo *Bluetooth Special Interest Group* (SIG), consórcio estabelecido inicialmente pela Ericsson, IBM, Sony, Toshiba, Intel e Nokia. Atualmente esse consórcio inclui mais de 2000 empresas e tem sua maior utilização na comunicação entre pequenos dispositivos, telefones celulares, *Pocket PCs*, *PDAs*. Também é

utilizado para a comunicação de periféricos, como scanners, impressoras, e qualquer dispositivo que possua um *chip bluetooth*. A tecnologia opera dentro da faixa aberta de 2,4 GigaHertz com alcance variável dependendo da categoria e da especificação. A comunicação entre dispositivos *bluetooth* de classe 1 pode atingir até 100 metros. Enquanto que a transmissão entre dispositivos de classe 2 dificilmente ultrapassa 10 metros. (Rodrigues, 2008)

Cada dispositivo *bluetooth* é dotado de um número único de 48 bits utilizado na identificação. São possíveis conexões de até 8 dispositivos, desde que um deles seja mestre (dispositivo principal) e os outros escravos. A faixa de freqüência do *bluetooth* é dividida em 79 portadoras espaçadas de 1 MegaHertz, dessa forma cada dispositivo pode transmitir em 79 diferentes frequências, minimizando as interferências.(Rodrigues, 2008)

O dispositivo principal depois de sincronizado com os demais pode mudar as freqüências de transmissão dos dispositivos escravos, até 1600 vezes por segundo (isso é conhecido como *frequency hopping* ou saltos de freqüência). A tecnologia possui uma banda teórica de 2Mbps e efetiva de 721 Kbps. (Rodrigues, 2008)

As vantagens, segundo (Rodrigues, 2008), são:

- A tecnologia *bluetooth* oferece transmissão criptografada de seus dados utilizando o protocolo *WEP*;
- Apresenta um consumo relativamente baixo se comparado ao *Wi-Fi*, principalmente quando se encontra no modo *standby*. Porém, no momento em que está enviando ou recebendo dados, o consumo chega a se equiparar;
- Com a difusão cada vez maior de dispositivos *bluetooth* no mercado, o custo dessas interfaces torna-se cada vez menor;
- Por ser uma tecnologia ponto a ponto de curto alcance, onde os dados só trafegam entre o dispositivo que iniciou a

conexão e o outro dispositivo onde ele está conectado, a utilização do *bluetooth* é isenta de custos.

Ainda de acordo com (Rodrigues, 2008), as desvantagens:

- O alcance dos dispositivos *bluetooth* é limitado a uma distância de 100 metros no caso de dispositivos de classe 1, entretanto devido ao alto consumo de energia dos dispositivos que atendem a esse padrão, a maioria dos dispositivos móveis utiliza interfaces *bluetooth* de classe 2, limitando o alcance a apenas 10 metros;
- Possui uma taxa de transferência razoável, aproximadamente 1Mbps. Essa banda pode permitir até mesmo streaming de vídeo (de baixa qualidade);
- A especificação do protocolo *bluetooth* permite apenas 7 usuários conectados a 1 dispositivo principal.

2.3.1.9 ZigBee

No final de 2004, um conjunto de empresas de diferentes segmentos do mercado chamada *ZigBee Alliance* (Aliança ZigBee) definiu o padrão *ZigBee*. Mais de 200 empresas fazem parte hoje da aliança como Philips, Motorola, Siemens, Bosch e etc. Trata-se de um protocolo para redes de sensores, projetado para permitir comunicação sem fio confiável e com baixo consumo de energia. (Rodrigues, 2008)

Baseada no padrão IEEE 802.15.4, o *ZigBee* opera em três bandas de rádio conhecidas como ISM (*Industrial, Scientifical and Medical*), as quais estão isentas de licenciamento. A taxa de transmissão possível varia com a banda: nos Estados Unidos, com uma banda de 915Mhz podem ser obtidos até 40Kbps, com 10 canais de comunicação; na Europa tem-se uma banda de 868Mhz, com uma taxa de 20Kbps, e apenas 1 canal; já em todo o resto do mundo, a banda é de 2.4Ghz, que pode atingir até 250Kbps, com 16 canais. (Rodrigues, 2008)

Segundo (Rodrigues, 2008) as principais características são:

- O *ZigBee* apresenta um ciclo de trabalho muito baixo, ou seja, a fração de tempo em que ele está ativo é mínimo. Isso possibilita maior autonomia quando alimentado por baterias;
- Suporta dois estados de operação: inativo ("*Sleep Mode*") e ativo, sempre com fluidez na passagem de um para o outro;

- Permite que os dispositivos permaneçam em "*Sleep Mode*" sem necessidade exigente de sincronização;
- Oferece suporte a topologias de rede tanto estáticas e dinâmicas, sejam elas em estrelas, em árvores ou em malhas;
- Recurso de encriptação de 128 bits;
- Como a comunicação ocorre entre módulos que suportam *ZigBee*, a utilização é gratuita;
- Possibilidade de utilização de redes com até 65535 nós para cada nó coordenador, procurando garantir sempre baixa latência;
- O seu alcance depende diretamente da potência dos equipamentos que implementam o protocolo *ZigBee*, podendo chegar até a 1,6Km. Logo, quanto maior o alcance maior também a potência necessária, aumentando assim o consumo de energia;
- Possui uma baixa taxa de transferência, aproximadamente 200kbps;
- Por ser uma tecnologia mais recente que as demais, o custo de aquisição de um dispositivo *ZigBee* ainda está relativamente alto;
- A pilha protocolar de implementação do *ZigBee* é pequena em termos de complexidade, exigindo menores recursos nos dispositivos que a utilizem. Porém, isso conduz a interfaces de baixo custo.

Comparando-se *Wi-Fi, Bluetooth e ZigBee*, obtemos o seguinte gráfico:

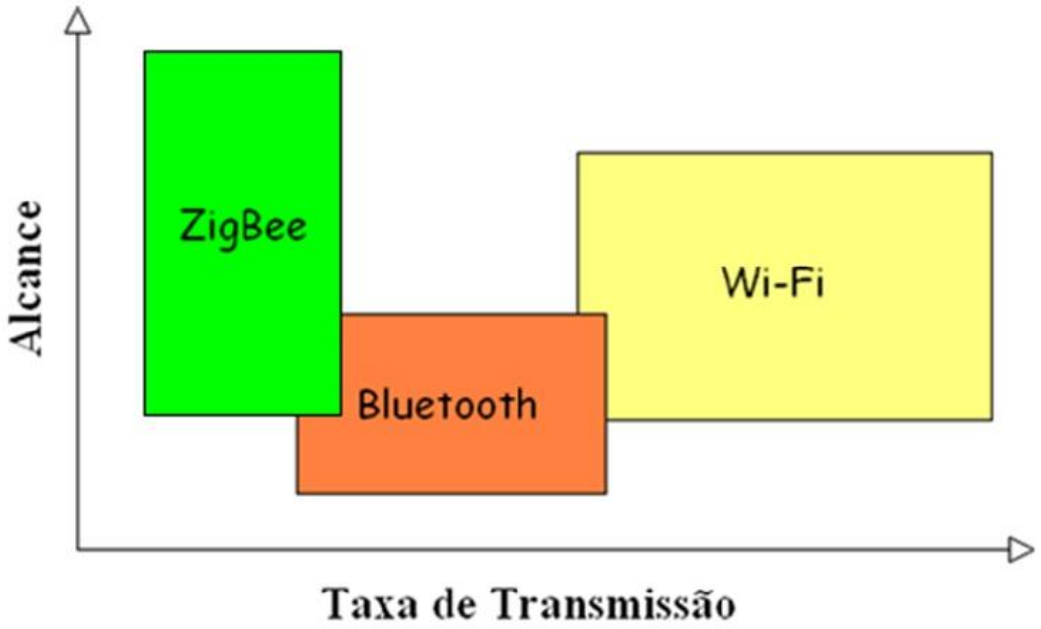

Figura 5: Representação gráfica da taxa de transmissão X alcance (Rodrigues, 2008)

2.3.2 Considerações Iniciais sobre Segurança

Devido às diversas áreas em que pode ser aplicada, quando o assunto é segurança da rede devemos levar em conta vários aspectos. Para alguns tipos de rede, a integridade dos dados coletados e transmitidos é importante, não tendo muito importante a confidencialidade do mesmo. Para outros, alem da integridade, a confidencialidade é muito importante e deve ser levada em consideração. (Cíntia et.al., 2009)

Em alguns casos, a confidencialidade e a autenticidade dos dados são levadas em conta. Porém, além de levarmos em conta os quesitos de segurança, devemos garantir também que os dados entregues sejam recentes. A segurança de uma rede pode ser garantida com o uso de chaves, e neste caso também é necessária a garantia de que as chaves em uso são recentes, pois chaves antigas podem ser obtidas através de algum nó comprometido. (Cíntia et.al., 2009)

Conforme citado anteriormente, o funcionamento destas redes se baseiam em nós com capacidades de processamento, armazenamento, comunicação e energia limitadas. Dito isso, os maiores desafios na

implementação de mecanismos de segurança são em relação à dificuldade de conciliar a máxima segurança com o mínimo consumo de recursos; além disso, a topologia da rede pode facilitar ataques e a comunicação sem fio pode ter um alcance limitado. A seguir serão explicadas essas dificuldades e as formas sugeridas para contornar estes problemas. (Cíntia et.al., 2009)

2.3.3 Problemas Encontrados

2.3.3.1 Máxima segurança x Economia de Energia

Ciclos de *CPU*, memória, codificação de chaves e criptografia de dados gastam recursos (energia) do sensor. Quando as mensagens enviadas pela rede, o calculo dos códigos de autenticação e a criptografia precisam ser executadas tanto no nó de origem quanto no nó de destino. Portanto tanto o mecanismo de criptografia assim como o mecanismo de estabelecimento e distribuição de chaves precisam ser otimizados para que consumam o mínimo de recurso possível. (Cíntia et.al., 2009)

2.3.3.2 Topologia de Rede x Comunicação Sem Fio

Como as RSSFs normalmente se encontram em áreas abertas, ataques como monitoramento de canal ou produção de interferência são possíveis de ocorrer. Outro fator é que como normalmente estas redes possuem uma grande quantidades de nós, alguns com possibilidade de mobilidade, fica difícil monitorar todos eles. (Cíntia et.al., 2009)

Por conta disto, nós podem ser capturados e através deles se obter informações restritas à rede ou então estes nós capturados podem ser substituídos por nós maliciosos. A comunicação da rede pode ter um alcance limitado, e se a topologia não for favorável, essa comunicação pode ser prejudicada ainda mais. (Cíntia et.al., 2009)

Grande parte da vulnerabilidade da rede e dos ataques em uma RSSF se da pelo fato de sua comunicação sem fio e pelos sensores não serem monitorados e por vezes sem encontrarem em áreas sem nenhuma segurança física. (Cíntia et.al., 2009)

2.3.4 Vulnerabilidades

2.3.4.1 Vulnerabilidades na Camada Física do modelo OSI

2.3.4.1.1 Ataques por Interferência

Ataques desta forma ocorrem quando um nó malicioso gera sinais aleatórios para prejudicar a comunicação em determinada área da RSSF. Uma alternativa para contornar essa vulnerabilidade é o uso de espalhamento espectral[1] para a codificação dos sinais, porém os rádios com suporte a este tipo de codificação são mais complexos de se utilizar e consome mais energia, o que pode inviabilizar seu uso em uma RSSF. (Cíntia et.al., 2009)

2.3.4.1.2 Ataques por nós maliciosos ou danos físicos

Devido ao fato dos nós ficarem muitas vezes em locais sem segurança ou monitoramento, uma forma de atacar a RSSF seria simplesmente danificar um nó sensor para que este não execute mais suas funções e assim prejudicar o funcionamento da rede. Outra forma de ataque seria substituir o nó por um nó malicioso para capturar as informações que são transmitidas na rede ou gerar ataques contra ela ou ainda seria possível apenas capturar um nó e obter a acesso às informações nele contidas como chaves de criptografia ou autenticação por exemplo. (Cíntia et.al., 2009)

Uma forma de proteger a RSSF destes tipos de ataque é utilizar mecanismos de proteção aos dados, capas de proteção ou selos. (Cíntia et.al., 2009)

2.3.4.2 Vulnerabilidades na Camada de Rede

2.3.4.2.1 Buracos Negros

Um nó malicioso indica aos nós da rede que a melhor rota é a rota que passa por ele. Assim o nó malicioso terá controle sobre os pacotes que trafegam pela rede, podendo alterá-los ou descartá-los. (Cíntia et.al., 2009)

xlixli

[1] Espalhamento Espectral: é uma técnica de modulação em que a largura de banda usada para transmissão é muito maior que a banda mínima necessária para transmitir a informação. Dessa forma, a energia do sinal transmitido passa a ocupar uma banda muito maior do que a da informação.

2.3.4.2.2 Inundação da Rede

Um nó malicioso dispara mensagens falsas na rede, causando um congestionamento e um consumo excessivo de energia pelos nós sensores. (Cíntia et.al., 2009)

2.3.4.2.3 Desvios e Loops

Um nó malicioso modifica a rota dos pacotes, direcionando o trafego para nós com pouca energia ou congestionados. Assim, ou os pacotes terão atrasos em sua entrega, ou serão descartados. (Cíntia et.al., 2009)

2.3.4.2.4 WormHoles

Neste tipo de ataque dois nós maliciosos em diferentes partes da rede, criam um túnel de comunicação entre si utilizando uma freqüência de radio diferente da rede. Assim fazem com que nós que estão em diferentes partes da rede, acreditem ser vizinhos o que certamente causará erro no roteamento de pacotes. (Cíntia et.al., 2009)

2.3.4.2.5 Seqüestro de Nós

Para realizar este tipo de ataque é necessário que um grupo de nós maliciosos cerquem um nó sensor da rede. Assim, eles descartam os pacotes enviados por este nó ou injetam pacotes inválidos para este sensor. (Cíntia et.al., 2009)

2.3.4.2.6 Nós Irmãos

Neste caso, um nó malicioso é capaz de assumir múltiplas identidades, que podem ser fabricadas ou roubadas. (Cíntia et.al., 2009)

2.3.4.3 Vulnerabilidades na Camada de Aplicação

Um tipo de vulnerabilidade comum na Camada de Aplicação é conhecida como Buracos na Cobertura. Os buracos ocorrem quando não são distribuídos nós suficientes em uma dada região, ou se vários nós de uma dada região morrerem, buracos na comunicação irão surgir nesta rede. (Cíntia et.al., 2009)

Outro ponto que deve ser considerado é o envio de mensagens de conhecimento falsas. Muitos protocolos de RSSF utilizam mensagens de reconhecimento e recebendo mensagens falsas pode fazer com que o nó acredite que um vizinho sem energia esta funcionando corretamente, por exemplo. (Cíntia et.al., 2009)

Logo, este breve estudo sobre as vulnerabilidades em uma RSSF permite concluir que os principais ataques se dão através de captura de nós, negação de serviço ou manuseio indevido dos mesmos.

2.3.5 Arquiteturas de Segurança

Para garantir as necessidades de segurança em uma RSSF, existem algumas arquiteturas propostas. Entre as principais, pode-se citar: *SPINS, TinySec, MiniSec* e o padrão *IEEE 802.15.4*. Vale recordar que os nós sensores possuem recursos limitados, logo as técnicas de segurança empregadas devem ser compatíveis com as limitações do nó sensor.

2.3.5.1 SPINS

O *SPINS* (*Security Protocols for Sensor Network*) é um conjunto de protocolos de segunraça para RSSF. Basicamente podemos dividi-lo em dois blocos: *SNEP* (*Secure Network Encription Protocol*) e o υ*TESLA (Micro Timed Efficient Stream Loss-tolerant Authentication).* (Cíntia et.al., 2009)

O *SNEP* é responsável por garantir confidencialidade, autenticação e integridade da mensagem além de evitar ataques de repetição. Para isso ele utiliza criptografia e códigos de autenticação de mensagem, o custo disso são 8 *bytes* a mais por mensagem. Para garantir a segurança semântica, um contador é incrementado a cada mensagem, e a autenticação dos dados é obtida através de criptografia. (Cíntia et.al., 2009)

O *uTESLA* é responsável por emular assimetria através da disponibilização atrasada de chaves simétricas, alem de funcionar como o serviço de autenticação de broadcasts para o *SNEP*. (Cíntia et.al., 2009)

2.3.5.2 TinySec

Segundo seus autores, a motivação principal para desenvolver este projeto foi a de que o *SPINS* não foi projetado nem implementado. Sendo assim, o *TinySec* se tornou uma das arquiteturas de segurança mais conhecida quando o assunto é RSSF. O único porém desta arquitetura é o fato de ter seu nível de segurança afetado por não possuir mecanismos de gerenciamento e estabelecimento de chaves, sendo assim uma única chave é utilizada para toda a rede. (Cíntia et.al., 2009)

Esta arquitetura permite dois modos de funcionamento: o *TinySec-Auth* e o *TinySec-AE*. Com relação ao conjunto de algoritmos, o modo utilizado pelo *TinySec* é o CBC e para garantir a autenticação e integridade das mensagens, o *TinySec* utiliza o algoritmo CBC-MAC. (Cíntia et.al., 2009)

2.3.5.3 TinySec-AE

Neste modo de funcionamento, os campos dos pacotes são constituídos por: destino, controle de camada de rede, tamanho da mensagem transmitida, origem, contador, dados e *MAC*. O campo contador tem a função de controlar que não ocorram envio de mensagens duplicadas. A combinação de todos os campos tornam o TinySec mais complexo e por conseqüência, menos previsível. (Cíntia et.al., 2009)

2.3.5.4 TinySec-Auth

O *TinySec-Auth* faz uso dos campos destino, controle de camada de rede, tamanho da mensagem transmitida, origem e *MAC*. Neste caso, o *MAC* fica responsável pela detecção de erros de transmissão de mensagem. (Cíntia et.al., 2009)

2.3.5.5 MiniSec

O *MiniSec* utiliza uma abordagem muito semelhante ao *TinySec*, porém se propõe a resolver alguns pontos fracos presentes na arquitetura vista anteriormente. Para resolver estes problemas, o *MiniSec* passa a utilizar o *OCB (Offset Codebook)* como modo de operação de cifra de bloco. Neste modo de operação a mensagem cifrada tem o mesmo tamanho da mensagem

original, economizando assim na transmissão de *bytes*. Outro benefício trazido pelo *OCB* é calcular o texto cifrado e o *MAC* conjuntamente, visto que no CBC é necessário uma execução para cifrar a mensagem e outra execução para efetuar o calculo do *MAC*. (Cíntia et.al., 2009)

Esta arquitetura também provê proteção contra ataques e repetição através de mecanismos de sincronização e estruturas de dados para armazenar contadores de mensagens. Esse mecanismo é interessante, mais se um nó sensor receber mensagens de muitos nós diferentes, essas estruturas podem ocupar uma grande quantidade de *bytes* da memória. Existe a tendência de aumento no espaço de memória nos nós sensores, enquanto as fontes de energia permanecem restritas, o que torna viável o aumento do consumo de memória em favor da economia de energia. (Cíntia et.al., 2009)

2.3.5.6 Padrão IEEE 802.15.4

Segundo (Cíntia et.al., 2009), esta arquitetura provê os seguintes serviços de segurança na camada de enlace: controle de acesso, integridade da mensagem, confidencialidade da mensagem e proteção contra repetição. Para isso, se utiliza de um dos oito conjuntos de segurança definidos no padrão. No entanto, a configuração padrão é de nenhum serviço habilitado. (Cíntia et.al., 2009)

O segundo modo fornece somente criptografia, utilizando o *AES* no modo *CTR*, enquanto o terceiro provê somente autenticação (*AES-CBC-MAC*). O quarto modo fornece criptografia e autenticação, utilizando o *AES-CCM*. Vale observar que o código de autenticação gerado pode ter 128,64 ou 32 *bits*, permitindo assim os oito modos de operação. (Cíntia et.al., 2009)

3 Aplicações e Modelos

Este capítulo representa o objetivo principal deste trabalho: elencar o estado atual das RSSFs apresentando exemplos de aplicação onde as RSSFs são fundamentais hoje em dia, além de apresentar modelos de sensores disponíveis no mercado.

3.1 **Introdução**

3.1.1 Aplicações

As redes de sensores sem fio possuem muitas aplicações possíveis, o que as torna um atrativo para as pesquisas. A cada dia, a tendência é que estas redes sejam utilizadas em diferentes lugares, surgindo mais aplicações para seu uso. A utilização mais comum das RSSFs é na medição de condições ambientais, como temperatura, umidade, pressão e condições do clima ou do solo. No entanto, estas redes também são bastante empregadas para monitorar movimentos, controlar velocidades e na detecção de materiais perigosos. Enfim, as RSSF estão sendo aplicadas em diversas áreas como no meio militar, industrial, ambiental, aviação, tráfego, segurança, medicina e controle. (Lima, 2010)

3.1.1.1 Medicina

Na medicina e biologia, sensores sem fio estão sendo empregadas para medir e acompanhar sinais vitais de pacientes (pressão, temperatura, glicemia, etc), além de monitorar o funcionamento de órgão como o coração, detectar a presença de substâncias que indicam o surgimento de um problema biológico, seja em animais ou no corpo humano. (Lima, 2010)

Avanços em RSSFs abriram novas oportunidades no sistema de cuidado de saúde. O futuro verá integração da abudância de tecnologia médica existente com redes sem fio pervasivas. Elas coexistirão com infraestrutura instalada, aumentando a coletada de dados e a resposta em tempo real. Exemplos de áreas em que os sistemas médicos do futuro podem se beneficiar

ao máximo de RSSFs são em assistência doméstica, enfermagens inteligentes, testes clínicos e aumento das pesquisas. Enquanto a população mundial envelhece, aqueles que sofrem com doenças da idade irão aumentar. Redes pervasivas domésticas podem auxiliar os residentes, providenciando a melhora da memória, aplicações de controle da casa, observações de dados médicos e comunicação de emergência. O uso de sensores não obstrutivos permitirão a coleta de dados e seu uso para os testes clínicos das próximas gerações. Dados serão coletados e reportados automaticamente, reduzindo o custo e a inconveniência de visitas regulares ao médico. Consequentemente, muito mais participantes dos estudos podem ser envolvidos, beneficiando pesquisas nas áreas biológicas, farmacêuticas e médicas. (Stankovic, et.al., 2005).

Esta é uma área de desenvolvimento crítica e ainda segundo (Stankovic, et.al., 2005) é necessária a disponibilização das seguintes tecnologias para os dispostivios médicos futuros:

- Interoperabilidade: Como um resultado de um sistema heterogêneo, a comunicação entre dispositivos podem ocupar múltiplas bandas e usar diferentes protocolos. Por exemplo, *motes* usam bandas não licenciadas para telemetria geral. Dispositivos médicos implantados podem utilizar uma banda licenciada alocada para aquele propósito. Para evitar interferência na crescente multidão de bandas não licenciadas, dispositivos biomédicos podem utilizar a banda WMTS (*wireless medical telemetry services*). A rede de cuidado doméstico deve fornecer interoperabilidade entre os dispositivos, e suportar relações únicas entre os mesmos, como os implantes e seus controladores externos;
- Aquisição e análise de dados em tempo real: A taxa de coleta de dados é maior nesse tipo de rede do que na maioria dos estudos ambientais. Comunicação e processamento eficiente será essencial. Ordenação de eventos, sincronização e respostas rápidas em situações de emergência serão todas necessárias;
- Confiabilidade e robustez: Sensores e outros dispositivos devem operar com confiabilidade suficiente para garantir dados de alta-confiança para diagnóstico e tratamento médico. Já que a rede não será mantida em um ambiente controlado, os dispositivos devem ser robustos;

- Novas arquiteturas de nós: A integração de diferentes tipos de sensores pode necessitar de novas e modulares arquiteturas de nós.

Ainda, (Stankovic, et.al., 2005) elenca modelos e requisitos dirigidos para a prática médica, como:

- Privacidade e segurança de dados e registros: Dados coletados pela rede são sensíveis, e problemas de propriedade nem sempre são claros. É provável que aquele que providência os cuidados de saúde seja o dono do sensor e dos dispositivos de rede, ainda que os dados pertençam ao paciente. Dados devem estar disponíveis durante emergências, mas o acesso deve deixar uma "trilha" não repudiável, para que abusos possam ser detectados. Qualquer mecanismo que ignore prioridades deve ser cuidadosamente projetados;
- Controle e delegação de acesso baseado em papéis em tempo real: Médicos podem delegar privilégios de acessos para outros médicos e enfermeiras; membros da família podem querer monitorar a qualidade do cuidado dos residentes de enfermagem domiciliar. O sistema pode ter autorizações como, por exemplo: "ler, mas não copiar" ou "ver, mas não salvar". Além disso, pacientes podem ler, mas não escrever dados, para evitar qualquer tipo de fraude;
- Operação não obstrutiva: "Camuflagem" é desejável, particularmente para aplicações de cuidados domiciliares, onde tecnologia intrusiva não seria tolerada. Sensores "invisíveis" são socialmente mais aceitáveis (atraem menos atenção, mais dignos) e mais perigosos (vigilância indesejada).

3.1.1.2 Militar

Segundo (Winkler,et.al.,2008), os casos de uso militares para RSSFs são diversos. Eles englobam aplicações como:

- Monitoramente de atividade militar em áreas remotas de interesse específico (estradas, vilas);
- Proteção de força (garantir que prédios que foram evacuados mantenham-se vazios de infiltrações de adversários).

Um caso de uso proeminente que recebeu grande atenção e interesse dos militares é a proteção de base, um caso específico de proteção de força. Tendo distribuído o quartel general em uma área de constantes ataques, é essencial evitar que a base seja atacada. O terreno que o envolve pode ser ondulante ou montanhoso ou pode ser potencialmente obscurecido em árvores e vegetação. Um ataque poderia ocorrer em formas de um grupo militante a pé, ou em veículos motorizados. Para facilitar uma detecção precoce o perímetro apresentado na figura cobriria um cinturão no campo de até 4 Km. (Winkler,et.al., 2008)

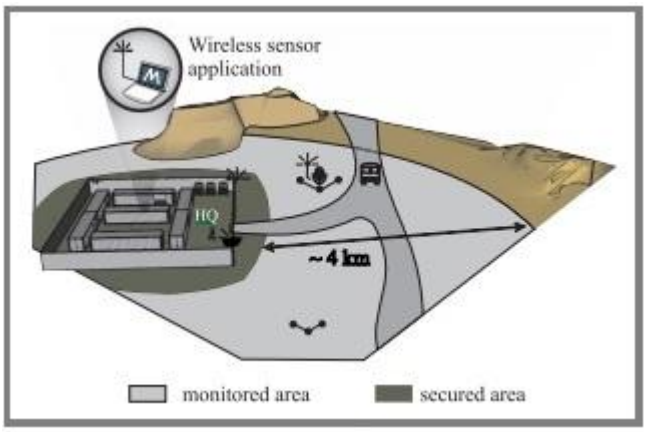

Figura 6 – RSSF usada em proteção de base (Winkler,et.al.,2008)

Segundo (Winkler,et.al.,2008) existem algumas aceitações típicas na área de pesquisa. Aplicações militares representam um uso primário de RSSFs e são melhores servidas por pesquisas informadas que evitam fazer suposições que são baseadas em requisitos militares presumidos. Várias pesquisas propõem algoritmos para redes com milhares de nós sensores e até mais. É aceito que nós sensores serão extremamente pequenos, leves e baratos, além da longevidade da bateria. Essas suposições levaram as pesquisas aos seguintes requisitos:

- Protocolos de roteamento e transporte específicos são necessários;
- Pequenas distâncias entre os nós (apenas alguns metros) são necessárias;
- Sistemas operacionais específicos são requeridos.

Na prática, essas suposições são mais desafiadoras do que o que é realmente utilizado nas atuais necessidades militares enquanto outros aspectos, como resistência a interferência não são suficientemente estudados. (Winkler,et.al.,2008)

Ainda de acordo com (Winkler et.al., 2008), existem certos requisitos que o exército deve cumprir para facilitar uma operação significativa de uma RSSF para propósitos militares de curto a médio prazo:

- **Capacidade física:** É provável que os nós sensores possam ser posicionados manualmente durante o avanço de uma operação. Eles podem ser transportados para a área de posicionamento através de veículos, apesar do tamanho e do peso de um sensor não serem suas maiores restrições. Embora desejável, um nó sensor do tamanho de uma caixa de fósforos não é atualmente esperado e um sensor de 20 a 30 centímetros seria aceitável. Em certos casos, até mesmo através de lançadores de foguetes ou transportes aéreos os sensores poderiam ser posicionados;
- **Auto configuração após o posicionamento:** Nós sensores devem ser capazes de rapidamente identificar vizinhos em seu alcance de comunicação e se configurar em uma rede *ad hoc*. É provável que a rede se mantenha razoavelmente estática e não é provável que os nós sejam movidos durante a operação. A rede deve ser capaz de lidar com uma falha de nó e a reconfiguração da rede deve ocorrer sem intervenção manual;
- **Tamanho da rede:** Para a maioria de operações a área a ser coberta pela rede deve ser entre 5 e 20 Km^2. Geralmente o alcance de comunicação entre nós entre 250 e 500m seria aceitável. Isso acarretaria que uma rede com menos de 100 nós seria necessária. Em casos ocasionais, o alcance da comunicação maior que 1 Km seria desejável;
- **Fluxo de Informação:** Inicialmente, comunicações mono direcionais podem ser suficiente, isto é, da rede de sensores para o *gateway* da RSSF e além. Isso é suficiente para atingir uma noção situacional aumentada tanto para o soldado quanto para o comandante. Na média, algum grau de controle dentro da rede

seria benéfico, como por exemplo, a capcidade de se controlar câmeras. Isso seria necessário para comunicações bi-direcionais. Essa necessidade para comunicações bi-direcionais deve ser refletida no conceito de segurança da rede para evitar o vazamento de informação entre um sensor e o núcleo da rede militar ao qual ele está ligado;

- **Duração de uso:** Algumas redes são simplismente necessárias para operar durante períodos de dias, embora períodos de um a dois meses podem ser visto como razoáveis para redes militares de sensores. No exemplo de proteção de base uma troca de baterias é prática e poderia extender a duração ainda mais. Em alguns casos, a rede não necessita ser funcional o dia todo (as vezes necessária somente durante a noite) ou a transmisão de dados da RSSF pode ser necessária durante somente duas ou três vezes durante o dia;
- **Tipo de dados:** Até mesmo quantidades limitadas de dados (menor do que 30 *bytes*) podem ajudar a garantir a superioridade da informação através da identificação de um incidente e providenciando um relatório do local. Isso significa que a taxa de transmissão de dados não necessita de ser alta. De qualquer forma, comandantes são propícios a requerir imagens e vídeos (tempo real ou não) no futuro;
- **Confiabilidade de dados:** Em vários casos é vital garantir que o dado tenha sido recebido com sucesso pelo usuário final, e técnicas para garantir a entrega devem ser incluídas. Dados também devem ser recebidos de uma forma segura, sem a oportunidade de uma interceptação por qualquer intruso;
- **Negação de Serviço:** Qualquer rede deve ser apta a reagir contra um ataque de negação de serviço por um adversário, pelo menos fornecendo meios para reportar o incidente de um ataque;
- **Custos:** De forma que informação relevante pode ser obtida pelo uso de redes com algumas dezenas de sensores, e o “resgaste” de sensores depois de seu uso pode ser desejável (por

segurança, por exemplo), o preço de um único nó normalmente não é crítico como a tecnologia *Bluetooth* civil.

RSSFs atuais podem fazer uso de vários anos de pesquisas em redes *ad hoc*, roteamente energicamente eficiente e áreas relacionadas. Consequentemente, os casos de uso citados vão ao encontro de uma grande extensão de tecnologias já existentes. Os desafios chaves para o posicionamento de RSSFs são mais problemas práticos de engenharia do que de pesquisa, e (Winkler,et.al., 2008) os lista:

- Clara identificação de vários eventos simultâneos, e uma correlação confiável de informação de nós vizinhos;
- Classificação de objetos e eventos em adição de sua detecção pura. Uma identificação e classificação automática de objetos suportaria uma reação rápida e apropriada e melhoraria o uso para propósitos militares;
- Integração melhorada de diferentes tipos de sensores para melhor confiabilidade de informação. Vários eventos possuem um grande número de efeitos simultâneos;
- Comunicações de radio para uso de sensores sem fio em que, especialmente, guerras urbanas providenciam maiores desafios como a possibilidade de forte interferência de várias fontes, como sombreamento de prédios com vários caminhos de transmissão e ao mesmo tempo ter que atingir cobertura suficiente e eficiência energética com poucas antenas e padrões eletromagnéticos;
- Miniaturização de sensores permitindo um rápido e automatizado posicionamento de redes;
- Robustez de sensores para posicionamento de aviões ou lança-foguetes;
- Não acontecimento de *loops* de dados em grandes redes de sensores;
- A otimização de sensores de redes para providenciar a mais eficiente cobertura de uma área geográfica; considerando os *trade-offs* como custo, alcance do sensor, alcance da

comunicação, tamanho do dispositivo, peso, autonomia e mecanismos de posicionamento;

- Concordância em formatos comuns e padrões para dados de sensores e troca de comunicação.

3.1.1.3 Motes

Mote é um sensor pequeno, embora não tão pequeno que costuma ser comparado a um grão de areia, como a ideal inicial sugerida propôs. *Motes* são tipicamente projetados em camadas empilháveis. O núcleo de um *mote* é um computador pequeno, barato e de baixo poder. O computador monitora um ou mais sensores e conecta com o mundo exterior através de uma conexão à rádio. Para economizar energia, os *motes* ficam cerca de 99% do tempo no modo de espera. Várias vezes por segundo, o dispositivo "conversa" com seu rádio para checar a existência de mensagens recebidas, mas se não há nenhuma, o rádio é desligado dentro de milissegundos. De forma similar, os sensores normalmente fazem suas leituras somente uma vez a cada vários minutos. Dados só são transmitidos quando a memória está cheia. O sistema operacional dos *motes, TinyOS*, força os programas do *mote* a desligar exceto quando certos eventos que garantem ação ocorrem. O sistema operacional também é altamente modular. Se o programa necessita somente de certas funções do *TinyOS,* as partes não-essenciais do sistema operacional são automaticamente removidas do *mote.* Essa abordagem modular garante que o código do programa preencha o mínimo de memória possível, deixando mais espaço para os dados do sensor. Módulos também realçam a robustez dos dispositvos limitando como as partes distintas do *software* interagem. Sensores separados em uma "placa-filha" podem ser conectados ao *mote.* Sensores disponíveis incluem temperatura, aceleração, luz, som e magnetismo. (Girão, 2007)

3.1.1.4 Meio Ambiente

O uso de RSSFs em pesquisa ecológica representa um grande desafio. Frequentemente, a RSSF tem de ser posicionada em ambientes extremos, onde a rede precisa sobreviver a uma série de elementos da natureza e funcionam por longos períodos de tempo sem nenhum acesso, por até vários

meses. Como exemplo, temos as áreas polares, áreas que só são acessíveis por poucos meses do ano. Mesmo sem a presença humana, a RSSF deve continuar a funcionar, mesmo que uma parte da mesma apresente alguma falha. A necessidade de uma RSSF tão confiável e à prova de falha levou à criação de alguns projetos, como por exemplo o LUSTER (*Light Under Shrub Thicket for Environmental Research* – Luz Sobre o Arbusto no Matagal para Pesquisa Ambiental). Segundo (Selavo et.al., 2007) o LUSTER é capaz de de preencher as seguintes necessidades:

Posicionamento rápido: Posicionar um grande número de sensores é uma tarefa que consome muito tempo. O LUSTER possui um sistema que se auto-organiza;

Garantia de posicionamento: Como o sistema deve "sobreviver" por muito tempo, o LUSTER oferece ferramentas que validam o tempo de posicionamento, verificando o estado de cada um dos nós regularmente;

Confiança: O LUSTER oferece tolerância ao atraso de transmissão, acesso online aos dados (evitando gargalos na RSSF), alta capacidade de armazenamento e sensores heterogêneos;

Desafios do ambiente: Sabe-se que cada ambiente representa uma situação. Por exemplo, em uma área insular onde pequenas criaturas mordiam os sensores foi usada uma pintura especial, feita com a pimenta *jalapeño,* possuídora de um forte gosto, afastando as criaturas.

3.1.1.5 Automação Domiciliar

Combinando-se sensores que atuam no ambiente baseado nas leituras dos dados obtidos, é possível realizar uma grande variedade de aplicações na área de automação domiciliar. Esta é uma das áreas mais propícias para o uso de RSSFs, tornando-se já um campo estabelecido do mercado, oferecendo grande variedade de soluções comerciais para os setores profissionais e privados. Soluções nessa área estendem-se desde controle de luzes até sistemas de segurança. (Gauger et.al., 2008)

Ainda segundo (Gauger et.al., 2008), o uso de RSSFs para o aprimoramento desta tecnologia é altamente atrativo. Primeiro, o uso de RSSFs reduz o número de fios e controles, e por consequência, acarreta uma redução de custos. E segundo, a capacidade de auto-organização das RSSFs

simplifica a configuração do sistema de automação domiciliar, reduzindo consideravelmente o esforço para instalação e configuração.

O principal desafio encontrado na área de automação domiciliar é como o sistema deve reagir em caso de decisões de controle conflitantes, onde múltiplas entidades determinam ações de controle visando otimizar o seu próprio objetivo. Por exemplo, quando dois nós sensores próximos recebem "ordens" conflitantes: enquanto um recebe a ordem de acender a luz, o outro recebe a ordem de apagar a mesma luz. Outro desafio latente neste contexto, é a segurança da RSSF, um desafio ainda maior neste caso do que em uma RSSF "pura", já que o fenômeno observado possui influência direta no comportamento do sistema, ao invés de se tornar apenas um dado armazenado. Uma possível solução, embora ainda complexa, é a existência de uma hierarquia entre os sensores do ambiente. (Gauger,et.al.,2008)

3.1.1.6 Agropecuária

Enquanto o uso de RSSFs na área de automação domiciliar já encontra-se em situação plena, seu uso na agropecuária é a área que atualmente apresenta a maior evolução. Segundo (Corke, et.al., 2010), suas principais aplicações na agropecuária são:

Monitoramento de gado: Usando a tecnologia de *motes* com capacidade de energia solar em coleiras dos animais do rebanho que transmitem a posição de cada animal através do uso de GPS;

Monitoramento da qualidade da água: Uma pequena RSSF, de apenas 9 sensores, mas que trabalham praticamente o tempo todo sem apoio humano, e que tem de se comunicar em grandes distâncias, de até 1Km. Possuem um carregador solar controlado por *software* é capaz de desconectar as células solares para evitar sobrecarga;

Cerca virtual: Além do uso de GPS, conta com a presença de sensores de inércia (compasso, giróscopio e acelerômetros). Devido a complexidade, foi necessário o desenvolvimento de um sistema operacional próprio, além da preocupação com os requisitos éticos para o uso de cercas virtuais.

3.1.2 Cenário Atual

As RSSFs encontram-se em pleno desenvolvimento no meio científico e estão ganhando espaço também no meio comercial. Atualmente, sensores cada vez menores estão sendo desenvolvidos, utilizando sistemas micro-eletromecânicos (*MEMS*) e processadores embarcados de baixa potência. Estas tecnologias empregadas na construção dos nós sensores estão tornando as aplicações em Redes de Sensores mais confiáveis e adequadas ao uso cotidiano. No entanto, o consumo de energia é considerado o principal fator restritivo de uma RSSF, pois seus dispositivos sensores foram desenvolvidos levando em consideração que é inviável (ou impossível) a substituição de suas baterias. Este problema motiva pesquisas em diferentes áreas, como otimização, projeto de protocolos e engenharia de hardware, visando o desenvolvimento de estratégias para o aumento da vida de uma rede de sensor. Uma dessas estratégias, na qual o conhecimento sobre a quantidade de energia disponível em cada parte de uma RSSF (chamado mapa de energia) pode auxiliar a prolongar o tempo de vida da rede. Os autores defendem a idéia que os nós sorvedouros devem estar presentes em em áreas com maior quantidade de energia disponível, pois estes gastam mais energia que os nós folhas, devido ao seu uso frequente. (Lima, 2010)

Outra estratégia interessante que busca o equilíbrio e o aumento do tempo de vida da rede está ligada ao desenvolvimento de protocolos de roteamento *power-saving*. Um algoritmo de roteamento otimizado pode fazer um melhor uso das reservas de energia se este seletivamente escolher rotas que utilizam nós sensores com maior quantidade de energia disponível, de tal forma que partes da rede com poucas reservas de energia possam ser preservadas. Entretanto a criação de um protocolo de roteamento eficiente é complexa, por abordar vários aspectos, sendo alguns deles conflitantes. Estes algoritmos devem trabalhar de forma a garantir um número mínimo de nós ativos na rede para cobrir uma área de monitoramento determinada. Porém, é preciso também garantir a conectividade entre os nós sensores ativos e evitar interferências e congestionamento de pacotes. Muitos estudos estão sendo realizados em RSSF com relação à adaptação em caso de falhas. Sabe-se que existe um alto grau de falhas nestas redes, que podem ser ocasionados por danos físicos ao nodo sensor, término da energia armazenada pelo sensor, ou

mesmo interferência do ambiente. Assim, a rede deve se reorganizar, para que continue a exercer a sua função, economizando o máximo de energia possível. Uma solução para este problema é a exploração da redundância de nós sensores presentes em RSSF densas, prolongando assim o tempo de vida de todo o sistema. (Lima, 2010)

A tabela abaixo demonstra algumas das propriedades que sensores sem fio são capazes de monitorar hoje:

	Medida	**Princípios Transdutores**
Propriedades Físicas	Pressão	Capacidade, Piezo-Resistência
	Temperatura	Termo-mecânica
	Umidade	Reistência, capacidade
	Fluxo	Mudança de Pressão
Propriedades de Movimento	Posição	GPS
	Velocidade	Efeito Doppler
	Velocidade Angular	Codificador Ótico
	Aceleração	Fibra Ótica
Propriedades de Contato	Tensão	Piezo-Resistência
	Força	Piezo-Resistência
	Torque	Piezo-Resistência
	Atrito	Torque duplo
	Vibração	Ultrassom
Presença	Contato	Troca de contato
	Proximidade	Magnetismo, efeitos sísmicos
	Distância/Alcance	Sonar, Radar, Tunelamento
	Movimento	Vibração
Bioquímico	Agentes Bioquímicos	Transdução bioquímica
Identificação	Características Pessoais	Visão
	Identificação Pessoal	Scan de Retina, de Impressão Digital

Tabela 1 – Medidas realizadas por RSSFs (Lewis, 2004)

3.2 **Mercado**

Existem algumas empresas que se destacam nesta área. No Brasil, pode-se citar a Bosch (Robert Bosch *GmbH*) e também a Falker, empresas abrangentes, na área de tecnologia (Bosch) e automação agrícola (Falker). Mundialmente, merecem destaque as empresas *Infineon Technologies AG*, a *Freescale Semiconductor, Inc*. e, a de maior destaque, a *Moog Crossbow*.

3.2.1 SMART (Scalable Medical Alert Response Technology – Tecnologia de Resposta Escalonável de Alerta Médico)

Monitoramento contínuo de pacientes desacompanhados é desejável em uma série de configurações onde pacientes não podem ser bem monitorados após a triagem. Uma dessas configurações é um departamento de emergência lotado, onde sempre a preocupação de que o paciente na área de espera pode sofrer de um mau súbito, que passe despercebido ao atendente. Similarmente, em um local de desastre, onde o número de pacientes é muito maior que o número de atendentes, algum monitoramento de pacientes pós-triagem poderia ser muito útil. Nestas situações, é desejável que se possua um sistema para monitorar o estado e a localização do paciente, e alertar um ou mais atendentes de eventos significativos de forma eficiente. (Curtis, 2008)

Ainda segundo (Curtis, 2008), construir um sistema de monitoramente contínuo para uma sala de emergência lotada ou um local de desastre possui vários desafios:

- Selecionar sensores de localização e de sinais vitais que sejam baratos, consumam pouca energia e sejam passíveis de comunicação com outros componentes;
- Selecionar uma plataforma leve e de baixo custo que incorpore comunicações sem fio, possa ser integrada com sensores e possua uma bateria com longa vida útil;
- Elaborar um acondicionamento dos sensores e da plataforma que seja aceitável para os pacientes e conveniente de se lidar.
- Garantir que o sistema sem fio possa monitorar de forma concorrente um grande número de pacientes;
- Analizar os dados dos sensores e de alertas presentes e dados para apropriar atendentes de forma que não os sobrecarregue;
- Integrar estes componentes em um sistema trabalhável que possa ser rapidamente posicionados em um local de desastre, que seja familiar a atendentes preparados para desastres, e que os escalonará para monitorar um grande número de pacientes.

Dado o objetivo de fornecer monitoramento tanto em salas de emergência quanto em locais de desastre, foi desenvolvido o SMART (*Scalable*

Medical Alert Response Technology – Tecnologia de Resposta Escalonável de Alerta Médico) para lidar com os desafios supracitados. O sistema SMART integra monitoramento sem fio de pacientes, geoposicionamento, processamento de sinais, alertamento direcionado e uma interface sem fio para atendentes. (Curtis, 2008)

Uma implementação protótipa do SMART foi realizada na área de espera do departamento de emergência do hospital de Brigham com 145 pacientes pós-triagem. Aspectos de posicionamento do sistema foram avaliados durante um exercício de simulação de desastre em oito pacientes. Devido às limitações da Comissão de Revisão Interna (*IRB – Internal Review Board*), integração completa com protocolos de departamentos de emergência não foi testada. (Curtis, 2008)

Figura 7 – Sensor SpO_2 (Curtis, 2008)

3.2.2 Automação Fabril (IndraMotion for Handling)

> "Desenvolvido para o mercado de automação, o *IndraMotion for Handling* é uma solução *turn key*[1] para controle de sistemas cartesianos baseada em IEC 61131 e PLC Open, que permite o controle de até 3 eixos principais e 3 eixos de orientação por cinemática. Para os fabricantes de máquinas o equipamento propicia o rápido comissionamento com configuração simples e fácil detecção de erros, além de alta flexibilidade por ter uma plataforma ampla e ser um sistema aberto (*Open Source*). Já para os usuários finais, os benefícios são a interface de IHM já pronta e testada, definição de coordenadas através definição direta e programação dos movimentos com instruções similares a robôs. O *IndraMotion for Handling* contribui ainda na melhoria dos processos de produção no que diz respeito à redução do nível de ruído e na alta precisão no posicionamento. Dentre suas aplicações pode-se destacar: sistemas de manipulação em processos automatizados (injetoras, logística, montagem), paletizadores, sistemas *Pick and Place*, automação em laboratórios e *retrofittings*. Com o objetivo de proporcionar alto nível de segurança ao mercado de máquinas com classificação elevada de risco, a Bosch Rexroth desenvolveu as válvulas monitoradas para sistemas hidráulicos de segurança." (Oliveira, 2010)

As válvulas são acionadas por bobinas elétricas e o deslocamento do êmbolo interno tem a sua posição indicada pelo sistema de monitoramento. O cliente pode aplicar este tipo de sistema onde é requerido alto nível de segurança. Estas válvulas podem ser aplicadas em injetoras, prensas, máquinas operatrizes e em aplicações especiais. Este produto atende as normas de segurança nacionais e internacionais para máquinas e equipamentos. (Oliveira, 2010)

lxlx

[1] Solução que contempla todas as etapas do processo de construção (conceituação, planejamento, desenvolvimento, estabilização e distribuição) e todos os serviços referentes à operação (configuração de infra-estrutura, monitoração, hospedagem, transmissão de dados, entre outros), entregando ao cliente uma solução completa pronta para uso.

3.2.3 ParkPilot URF6

A Bosch introduziu recentemente no mercado o brasileiro, após ser utilizado na Europa, o *ParkPilot* URF6. Trata-se de um sensor de esacionamento e aproximação, de aplicação universal, isto é, para todos os veículos.

> "Dirigir um veículo com o sensor de estacionamento Bosch é ainda mais seguro porque o *ParkPilot* supre confiavelmente, durante as manobras de estacionamento, os pontos cegos dos retrovisores dos carros sinalizando ao condutor a presença de qualquer obstáculo fora do seu alcance de visão, tais como: carrinhos de supermercado, floreiras, pequenos postes de estacionamento, portões, colunas e paredes dos estacionamentos de prédios e muito mais. Tanto em manobras em espaços reduzidos ou na presença de veículos com engates já estacionados, o *ParkPilot* reconhece qualquer obstáculo de forma exata sinalizando-os visual e acusticamente." (Bosch, 2011)

Segundo (Bosch, 2011), as principais vantagens oferecidas pelo *ParkPilot* incluem:

- Disponível à todas as marcas e modelos de veículos: O novo *ParkPilot* URF6 é um sistema universal e por isso, ele pode ser instalado independente da marca ou modelo do veículo. A montagem do *ParkPilot* é rápida e fácil, pois existem anéis de contorno com ângulos diferenciados que proporcionam ampla aplicabilidade no mais diversos design de veículos e pára-choques;
- Design: O sensor é instalado no pára-choque do carro proporcionando um excelente acabamento e tornando o visual discreto. O sistema possui uma solução única no mercado para fixação e acoplamento dos sensores ao pára-choque do veículo;
- Segurança confortável e confiável: Com a melhor eficiência sobre o raio de alcance dos sensores e com uma cobertura homogênea (não há pontos cegos), o *ParkPilot* é o sistema de sensoriamento de obstáculos mais confiável existente na atualidade. A partir de 150 cm obstáculos baixos como jardineiras, carrinhos de supermercado, vasos de flores, cerca de arame, postes e até engates de carros são detectados.

Os sensores minuciosamente projetados, são capazes de compensar alteração climática entre frio e calor e ruídos ambientes;

- Diagnóstico rápido: Sempre ao ligar a ignição do veículo o sistema faz o auto-teste para estabelecer as condições ambientais e informa ao condutor do veículo se há alguma anomalia no sistema. Além disso, o Parkpilot pode ser interligado ao sistema de bordo eletrônico para veículos que possuam a solução original Bosch;
- Vale a pena: Reparar danos ou arranhões em pára-choques, sejam eles provocados pelo encosto de engates ou colisões, é mais oneroso do que o sistema que os previne - *ParkPilot*. Portanto, o investimento no *ParkPilot* vale a pena – não haverá mais acidentes;
- Montagem rápida e fácil, com manual de instalação totalmente detalhado;
- Auto-diagnóstico;
- Confiabilidade de funcionamento;

3.2.4 Motores Automotivos

No Brasil, o mercado de automação residencial ainda é pequeno, embora seja talvez a área mais desenvolvida no país ao se tratar de RSSFs, mas segundo a Associação Brasileira de Automação Residencial (Aureside), a tendência é de crescimento. Apostando nisto, a Bosch oferece uma linha de motores elétricos que também podem ser aplicados em sistemas de automação residencial. Entre as soluções em automação residencial que a empresa oferece estão os sistemas para abrir e fechar cortinas, portas, portões, toldos, abaixar ou elevar o encosto do sofá ou da cama, ajuste da TV de *LCD*, do monitor do computador e da mesa do escritório, tudo com apenas o toque do controle remoto. (Bosch, 2010)

> "Um exemplo de utilização residencial é o motor limpador de parabrisa, que pode ser aplicado em sistemas de abertura e fechamento de portões e portas residenciais. O grande diferencial do portão automatizado com o motor limpador de parabrisa tipo CEP Bosch é a vantagem de continuar trabalhando mesmo sem energia elétrica. Por se tratar de um motor de corrente contínua, o sistema pode ser alimentado por bateria na falta de energia, oferecendo maior segurança e comodidade ao

> usuário. Já o motor, que originalmente é utilizado para levantar os vidros do carro, pode ser aplicado janelas residenciais. Com este sistema, o usuário pode programar aberturas e fechamentos de vidros ou basculantes (os sensores detectam a presença ou ausência de luz natural para ordenar ao motor abertura ou fechamento de janelas). Com esta automatização também é possível a integração com outros sistemas de segurança eletrônica." (Bosch, 2010)

Estes motores elétricos ainda podem ser aplicados em automação de móveis, como cadeira de conforto, ajuste elétrico de camas e mesas, e em outras comodidades, como automação de varal, toldos, cortinas, entre outras. Por serem fabricados para utilização originalmente em sistemas automotivos, os motores elétricos Bosch são submetidos a testes rígidos de qualidade e desempenho, e seu processo de fabricação exige alta tecnologia. (Ibidem)

3.2.5 AURESIDE (Associação Brasileira de Automação Residencial)

O nicho de mercado crescente de automação industrial, intimamente relacionado às Redes de Sensores Sem Fio, possui um órgão regulamentador. Segundo (Aureside, 2011), os principais sistemas de automação residencial são os seguintes:

- Segurança: alarmes, monitoramento, circuito fechado de TV, controle de acesso;
- Entretenimento: *home theater*, áudio e vídeo distribuídos. TV por assinatura;
- Controle de iluminação;
- *Home Office*: telefonia e redes;
- Ar condicionado e aquecimento;
- Portas e cortinas automáticas;
- Utilidades: bombas e limpezas de piscinas, controle de sauna;
- Irrigação automática e aspiração central à vácuo;
- Infraestrutura: cabeamento dedicado, cabeamento estruturado, painéis e quadros de distribuição;
- Controladores e centrais de automação;

- *Softwares* de controle de integração.

> "Atualmente, podemos definir três níveis de interação: Sistemas Autônomos, Integração de Sistemas, e a Residência Inteligente. Nos Sistemas Autônomos podemos ligar ou desligar um subsistema ou um dispositivo específico de acordo com um ajuste pré-definido. Porém, neste esquema, cada dispositivo ou subsistema é tratado independentemente, sem que dois dispositivos tenham relação um com o outro. A Integração de Sistemas é projetada para ter múltiplos subsistemas integrados a um único controlador. A limitação deste sistema está em que cada subsistema deve ainda funcionar unicamente na forma a qual o seu fabricante pretendia. Esta integração já permite uma ampla gama de benefícios aos usuários e lhe garante a máxima eficiência no aproveitamento dos recursos utilizados. Na Residência Inteligente o produto manufaturado pode ser personalizado para atender às necessidades do proprietário. O Integrador de Sistemas em conjunto com o proprietário delinearão instruções específicas para modificar o uso do produto. Assim, o sistema torna-se um gerenciador ao invés de apenas um controlador remoto. Os sistemas residenciais inteligentes dependem de comunicação de mão-dupla e *feedback* de *status* entre todos os subsistemas para um desempenho acurado." (Aureside, 2011)

Para tomar vantagem da tecnologia mais recente, os proprietários têm uma expectativa maior quanto aos construtores fazerem as coisas de modo diferente do que antes faziam. Os construtores, de forma a participar deste lucrativo novo mercado, precisam educar a si próprios e treinar ou contratar indivíduos para atuar como Integradores e Instaladores de sistemas residenciais. A comunicação entre o construtor e/ou Integrador e Instaladores com os proprietários é a chave para o sucesso. Segundo também (Aureside, 2011), um bom projeto de Automação Residencial resulta numa interface amigável para o usuário final, que dele poderá obter variados benefícios, dos quais merecem ser destacados: economia, segurança, comodidade, conforto, entretenimento, confiabilidade, velocidade e interatividade.

3.2.6 Produtos Crossbow Inc.

Uma das maiores empresas do mercado, a *Moog Crossbow* possui vários nós sensores disponíveis no mercado. Entre eles merecem destaque:

- MICA2 e MICA2DOT: Estes dispositivos foram desenvolvidos pela Universidade de *Berkeley* e são comercializados pela *Crossbow Technology Inc.* O microcontrolador de 8 bits utilizado é o ATMega 128L e o sistema de rádio frequência é baseado no chip CC1000 da Chipcon, que trabalha com baixa potência e baixos níveis de tensão, operando na faixa ISM e SRD (*Short Range Device* – Dispositivo de Curto Alcance). A banda de frequência situa-se nos 315, 433, 868 e 915 MHz. Este sistema de rádio utiliza a modulação FSK (*Frequency Shift Key* – Chave de Troca de Frequência), que permite atingir taxas de transmissão da ordem de 76.8Kbps. O chip é alimentado com tensões que podem variar entre 2.1V e 3.6V, permitindo que o sistema de rádio trabalhe com o mínimo de recursos energéticos. Na figura 8 observa-se o kit que a marca disponibiliza para monitorização. A Crossbow disponibiliza diversas placas de sensores e aquisição de dados, que sã independentes da placa de processamento e rádio, mas que juntas formam um sensor completo, que poderá medir por exemplo: temperatura e CO2. Além disto, a empresa desenvolve uma placa para a estação base receber a informação da rede. (Gouveia, 2009)

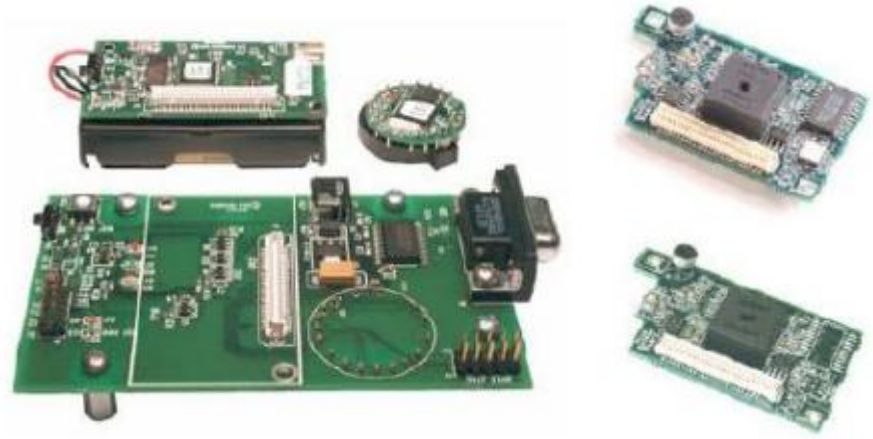

Figura 8 – Dispositivos MICA2 e MICA2DOT (Gouveia, 2009)

- Mica Z: O Mica Z é um módulo *wireless* de baixo consumo para redes de sensores. Segue o protocolo IEEE 802.15.4, funcionando na banda dos 2,4GHz. Utiliza a técnica DSSS que é resistente a interferência, proporciona segurança de informação e taxas de transferências de 250Kbs. Utiliza na sua arquitetura o mesmo microcontrolador utilizado na plataforma Mica e trabalha com o sistema de rádio CC2420 desenvolvido pela Chipcom. Este dispositivo é compatível com o sistema operacional *TinyOS* e com a maioria das aplicações desenvolvidas para a plataforma Mica2 e Mica2dot. Na figura 9 observa-se um destes nós. A Crossbow, empresa que comercializa estes módulos, oferece uma variedade de placas de aquisição de dados, isto é, módulos sensoriais, para o módulo Mica Z. Qualquer uma dessas placas pode ser conectadas ao Mica Z através de um conector de 51pins. (Gouveia, 2009)

Figura 9 – Dispositivo Mica Z (Gouveia, 2009)

- *Tmote Sky*: O *Tmote Sky* é um módulo de comunicação *wireless* de baixo consumo, para utilização em redes de sensores e aplicações de monitorização. É desenvolvido pela *Crossbow Inc* e utiliza a tecnologia *ZigBee* para a comunicação por rádio frequência. Este tipo de dispositivo utiliza o chip CC2420 desenvolvido pela Chipcom, e o rádio trabalha com a modulação QPSK através do DSSS. O módulo utiliza o microcontrolador MSP430 da empresa *Texas Instruments*, de 16bits que trabalha a uma frequência de 8MHz. Um dos pontos fortes deste nó sensor é a utilização da interface *USB* (*Universal Serial Bus*), que facilita a programação dos dispositivos e a troca de

informações com a estação base. Na figura 10 mostra-se um exemplar desta marca. O *Tmote Sky* é alimentado por duas baterias AA, sendo que essas duas baterias garantem uma tensão entre 2.1 e 3.6V. A alimentação é fornecida pela porta USB, sempre que o módulo está conectado a esta, sendo neste caso uma alimentação de 3V. Este módulo comunica para o exterior usando uma antena integrada no circuito que tem um alcance de 50 metros em locais fechados e alcance de 125 metros em locais abertos, sendo uma vantagem para a rede de sensores. Ao nível sensorial, o dispositivo tem embutido três sensores: umidade, temperatura e luminosidade. Os sensores de temperatura e umidade são fabricados pela Sensirion de modelo SHT11 ou SHT15. O sensor de luminosidade é fabricado pela *Hamamatsu Corporation* de modelo S1087-01. O preço deste módulo aproxima-se dos 80 euros, já com os sensores incluídos. (Gouveia, 2009)

Figura 10 – Dispositivo Tmote Sky (Gouveia, 2009)

3.3 **Universidade**

Atualmente, várias universidades no mundo possuem centros de pesqusa voltadas para a área de Redes de Sensores Sem Fio. No Brasil, destacam-se principalmente a UFMG (Universidade Federal de Minas Gerais, grupo de pesquisa WINET) e a UFPR (Universidade Federal do Paraná, grupo de pesquisa NR2). Porém, mundialmente, a universidade que mais se destaca é a Universidade da Califórnia, *Berkeley*, nos Estados Unidos. Neste capítulo,

serão citadas algumas das principais pesquisas realizadas no âmbito das universidades.

3.3.1 Monitoramento de Usinas Nucleares utilizando RSSFs com capacidade de auto-manutenção

Detectar uma falha de um nó sensor é a parte mais importante de um sistema de RSSF com capacidade de auto-manutenção. É impossível estimar uma falha observando-se somente o dado de um sensor. Nós não podemos dizer se o dado irregular é causado por um dano relativo ao sensor ou ao local que o sensor monitora. O sistema com decisão acertada de falhas em nós é requerido para evitar um falso-positivo ou um falso-negativo. Neste sistema, a detecção de danos nos sensores é baseada no raciocínio de que “nós próximos devem possuir alguma relação”. Falhas podem ser verificadas comparando-se os valores de um sensor com seus vizinhos. Em outras palavras, a confiabilidade do sensor é determinada através do compartilhamento de informações de cada sensor e lidando com essas informações através de uma rede composta por sensores. Consequentemente, consideramos que o sistema será capaz de detectar a falha dos sensores através de um parâmetros “indíce de confiabilidade” de cada um dos nós. (Fujiwara, 2008)

Quando um sensor quebrado é detectado, o sistema excluirá o sensor da rede e a reorganizará somente com os sensores “saudáveis”. Essa função permite a minimização dos danos de uma rede após uma falha parcial. Sem esta função, o nó sensor danificado causará colisão de pacotes e isso vai afetar toda a rede. Um novo monitor “saudável”, seguido por um grande número de sensores e esta capacidade de auto-manutenção, permite uma forma inovadora e eficiente de se gerenciar usinas nucleares. (Ibidem)

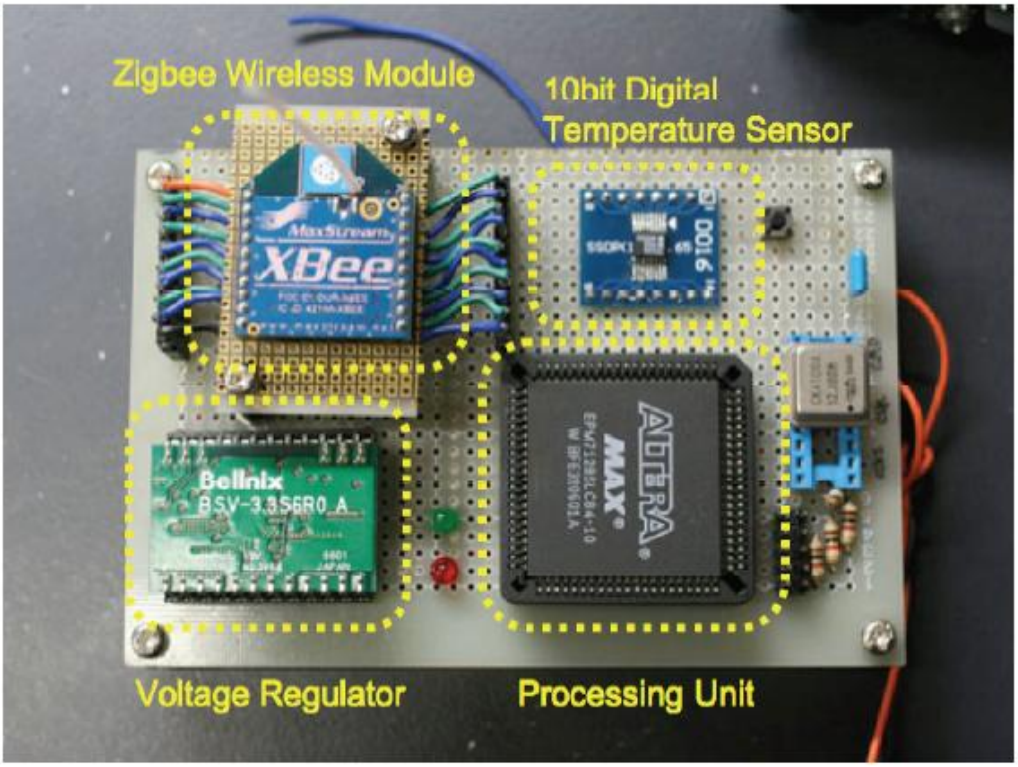

Figura 11 – Dispositivo RSSF (Fujiwara, 2009)

3.3.2 Aumento do desempenho de RSSFs utilizando "dicas" de sensores

Com mais de 172 milhões de dispositivos vendidos em 2009, smartphones representam uma mercado de crescimento acelerado. Alguns analistas preveêm que *smartphones* e *tablets* superarão as vendas de *PCs* até o fim de 2011. Com o atual crescimento, estes dispositivos podem se tornar a forma dominante de acesso à internet em um futuro próximo. Além disso, tratando-se destes dispositivos móveis, é comum o uso de protocolos de redes sem fio para lidar com uso estático e móvel em um curto período de tempo. Considere por exemplo um usuário de smartphone em um supermercado que alterna entre ficar parado em frente a uma vitrine de produtos e se movimentando entre as ilhas de produtos, isto enquanto a rede sem fio interna da loja disponibiliza áudio por stream ao aparelho. A mobilidade introduz grandes problemas que protocolos de redes sem fio devem superar para obter uma boa performance. Em meio ao movimento, os caprichos da comunicação

sem fio tornam-se mais visíveis: qualidade do canal varia rapidamente, perdas se tornam mais notáveis, e avaliaçõs da qualidade dos canais são rapidamente desatualizados. Por isso, nós não devem manter longas histórias, já que a rápida troca de condições dos canais e da topologia de rede os tornaria rapidamente inválidos. Tabelas de roteamento também devem se adaptar mais rapidamente às trocas de vizinhos, e o próximo salto ótimo pode depender da direção e velocidade de movimento. De qualquer forma, estratégias que compensam essas dificuldades relacionadas a mobilidade dificilmente serão ótimas em casos estacionários. Quando os nós são estáticos, eles podem possuir uma estimativa média da qualidade do canal, observar seus vizinhos, e computar rotas durante longas escalas de tempo, cuidadosamente obtendo e atualizando observações de vários pacotes. Fazendo isto, eles podem corretamente evitar reagir as variações inevitáveis que até mesmo redes sem fio estáticos encontram. (Ravindranath, 2011)

Trabalhos anteriores geralmente não fizeram distinção entre estes modos, ao invés disso tentando adaptar livremente através dessas diferenças extremas condições de redes. A chave neste trabalho é que os nós podem usar “dicas” externas de sensores para melhorar a performance dos protocolos de redes sem fio. A abordagem é prática e prontamente implementada, pois praticamente todos os smartphones e tablets atuais possui um vasto conjunto de sensores, como: *GPS*, acelerômetro e compassos, entre outros. Estes sensores são usados por aplicativos, mas são sumariamente ignorados pela pilha de rede e seus protocolos. É mostrado como dados destes sensores podem fornecer “dicas” para os protocolos, sobre o modo de mobilidade do dispositivo. Por “modo de mobilidade” pode-se entender atributos como se o dispositivo começou a se mover, ou está estático, sua velocidade de movimento, posicionamento e a direção do movimento, todos fatores que afetam a performance do protocolo de redes sem fio. Procolos podem explicitamente adaptar seu comportamento e parâmetros para o atual modo de mobilidade. As dicas de sensores podem ser usados de formas diferentes em protocolos diferentes. Quando um nó gera uma dica localmente, ou recebe uma dica de um nó vizinho, ele pode se adaptar em resposta a isto. A adaptação pode ser contínua (atualizar parâmetros de protocolos) ou discreta (mudar de um protocolo otimizado estático para um otimizado móvel). (Ravindranath, 2011)

3.3.3 Monitoramento e Automação de Irrigação utilizando RSSFs

> "O sensor capacitivo FDR utilizado neste trabalho foi desenvolvido no Departamento de Engenharia Agrícola (DENA), mais especificamente no Laboratório de Eletrônica e Mecânica Agrícola (LEMA). Este sensor já foi utilizado em campo e mostrou-se eficiente ao monitorar a irrigação, acompanhando de forma precisa a umidade em tempo real, possibilitando o perfeito fracionamento da distribuição de água. O sensor capacitivo FDR é confeccionado na forma retangular em placas de circuito impresso (fibra de vidro, com uma fina camada de cobre em um dos lados), com espessura, largura e tamanho aproximados de 0,2 cm, 3 cm e 15 cm, respectivamente. Suas placas são posicionadas paralelamente, definindo os eletrodos do capacitor, separadas em 0,5 cm e cobertas por um verniz, tanto para evitar oxidação das placas de cobre, devido o contato com o solo, como para eliminar o efeito da condutância elétrica da carga através do dielétrico. A área da placa que constitui o campo elétrico é de 25,48 cm2. Este sensor é composto de um oscilador, cuja freqüência é definida pelo capacitor que pode variar o dielétrico e por um resistor fixo. Toda a área correspondente ao circuito é encapsulada por material composto de resina industrial." (Cruz, 2009)

Ainda segundo (Cruz, 2009), para a estratégia do manejo de irrigação foi implementado um sistema de rede de sensores sem fio. Seu desenvolvimento derivou da necessidade de se economizar água e energia em campos agrícolas no semi-árido através de melhorias nos métodos atuais de administração da irrigação. O módulo sensor é composto pelo rádio sensor, contendo a unidade de processamento, e os sensores capacitivos FDR. O módulo sensor desenvolvido e utilizado é composto pelos seguintes elementos: transceptor (banda de 1 Kbit/s a 1Mbit/s); memória (128 kbytes a 1 Mbyte); microcontrolador; sensor de umidade; bateria de 12 volts e conexão com outras redes através de *gateways*. Para o fornecimento de energia deste módulo sensor foi escolhida uma bateria de 12 volts da marca *HAZE POWER*, cuja mesma é recarregável e constituída de chumbo, ácido sulfúrico e polipropileno, de fácil acesso no mercado. Para o processamento dos comandos do módulo sensor foi utilizado o microcontrolador PIC 18F4550 da Microchip, ideal para baixo consumo de energia e para aplicações de monitoramento que requer

conexão periódica com um computador pessoal para transferência de dados, possuindo grande quantidade de memória *RAM*. O rádio transceptor utilizado foi o modelo TRF 2.4 GHz da Laipac, com alcance, segundo o fabricante, de 150 metros utilizando taxa de transmissão de 1 Mbps. Ele opera em banda de freqüência ISM de 2.4 GHz com espalhamento espectral e não necessita de licença da Anatel. Sua escolha decorreu de suas características, que permite alcançar distâncias satisfatórias, possuindo taxa de transmissão de dados compatível com as variáveis a ser monitoradas, proporcionando baixo consumo de energia, além da sua disponibilidade no comércio oferecendo custo de compra reduzido.

> "O rádio sensor é composto por duas unidades. Uma de processamento do circuito e outra destinada aos sensores capacitivos FDR. Entretanto, vale considerar o uso alternativo de outros tipos de sensores já que a unidade de sensores é removível. Neste protótipo o controle suporta a conexão de até três sensores capacitivos FDR. A unidade foi confeccionada no método de foto revelação positiva, em placa de fenolite de uma camada. As placas do rádio sensor foram confeccionadas na forma circular com o objetivo de moldar o protótipo de forma compacta para ser acondicionado em peças de PVC. O uso dos tubos de PVC como compartimento do circuito traz várias vantagens, a começar pelo fácil manuseio com ferramentas simples, comprovada resistência às intempéries de umidade e radiação do meio rural e ainda garantir uma relativa estética ao produto final. A modularização do circuito prevê ainda a conexão de mais camadas de placas, onde outros sensores, além dos já testados, poderão ser adicionados ao módulo e multiplexados por sua unidade de processamento." (Ibidem)

> "O sistema foi desenvolvido com base numa arquitetura distribuída em que cada unidade remota (módulo sensor) comunica-se via rádio frequência com uma unidade central (Módulo mestre) por rádio frequência. Esta, por sua vez, comunica-se via cabo serial com um computador pessoal que tem a função de supervisionar o arquivo dos dados coletados. Cada módulo sensor envia os dados de resposta do sensor capacitivo FDR e tensão da bateria. O microcontrolador PIC18F4550 possibilita desligar a alimentação de todo o circuito do módulo e minimizar o seu consumo quando no

> modo “dormir”. Cada módulo sensor possui um conjunto de parâmetros que possibilita o seu reconhecimento pela estação base, quando configurado para funcionar. A estação base tem a função de recolher todos os dados recebidos dos módulos sensores e enviá-los para um computador pessoal. O transceptor utilizado nesta estação é idêntico ao utilizado nos módulos sensores.” (Ibidem)

(Cruz, 2009) ainda ressalta que uas etapas foram realizadas para definir o processo de envio e recepção do pacote de dados dos módulos sensores. A primeira consistiu no controle do transceptor, onde foram desenvolvidas pequenas rotinas para a contagem de pacotes enviados e recebidos. Nesta etapa foi definido o protocolo de comunicação entre o módulo mestre e os módulos sensores. Foi investido em um protocolo que relacionasse a limitação de energia com o alcance e banda de freqüência. Em seguida, realizou-se o processamento do código dos módulos sensores, os quais foram escritos em C++. O desenvolvimento do programa, em linguagem C, foi feito através dos compiladores *CCS*, *Source Boost* e de um emulador. Segundo os autores, este kit de desenvolvimento é formado por um compilador e placas dotadas de vários recursos baseadas no microcontrolador 8051, especificamente o modelo AT89S8252 DIP 40 da Atmel com clock de 11 MHz. A segunda etapa foi destinada ao controle das ações de transmissões dos módulos sensores em situações de campo, que se dividem em controle, aquisição e comunicação dos dados. O módulo sensor, uma vez colocado para funcionar, permanecerá em um ciclo de comandos de dormir e acordar. Na condição deste último, o módulo sensor verifica se está no instante de realizar a leitura e após a obtenção dos dados volta a dormir. Se não for o momento a memória do processador é atualizada e configurada para o modo recepção, onde o módulo sensor aguarda algum comando de pedido do módulo mestre. Caso isto não ocorra, ele ainda continua acordado escutando o módulo mestre até que este intervalo de tempo seja finalizado e a partir daí volta ao modo dormir. Mas, se o módulo mestre solicitar algum tipo de comando, durante o intervalo de tempo que o módulo sensor encontra-se acordado, o mesmo responderá de acordo com o tipo de tarefa a cumprir, como, por exemplo, enviar os dados ou servir de multihop para conseguir dados de outro módulo sensor. Os comandos solicitados pelo módulo mestre são definidos através da interface de comunicação. Esta interface de controle e aquisição foi implementada em

linguagem C para realizar a comunicação entre o módulo mestre e um computador pessoal do tipo IBM-PC ou compatível, possibilitando a configuração dos módulos remotos via rádio e o armazenamento dos dados adquiridos. O software *Borland Builder* foi utilizado para elaborar a interface de comunicação.

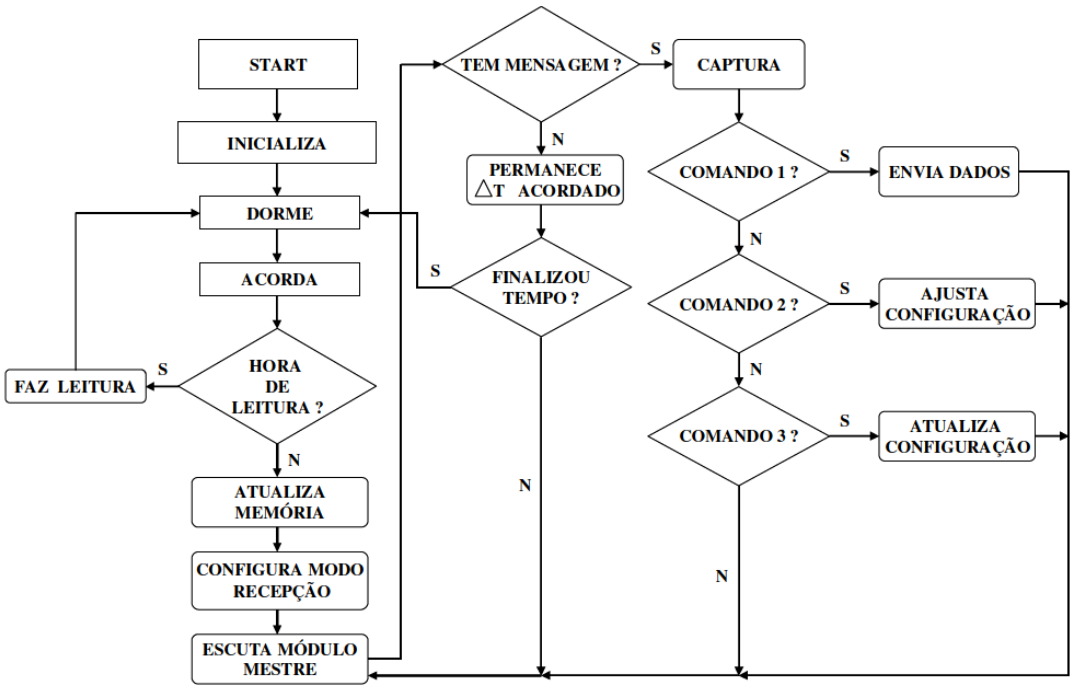

Figura 12 – Fluxograma do programa de comunicação dos módulos sensores. (Cruz, 2009)

3.3.4 UrbanSensorDB

> "Os ambientes urbanos estão cada vez mais complexos tanto pelo aumento do número de pessoas na cidade quanto pela redução das áreas verdes, sendo muitas vezes possível a percepção de diversos micro-climas ocorrendo ao mesmo tempo numa mesma cidade. Tais características têm um impacto na qualidade de vida do seres humanos e na sua saúde. Através do acompanhamento desses ambientes, é possível a aplicação de políticas de ações a serem tomadas em cada circunstância, como por exemplo, no aconselhamento da população a evitar determinadas áreas em razão de altas temperaturas ou qualidade do ar.

> As alterações de temperatura em uma cidade podem impactar no aumento de diversas doenças, na taxa de mortalidade, no consumo de energia, entre outros. As ilhas de calor são um fenômeno cada vez mais comum nas grandes cidades, onde há regiões em que a concentração de prédios criou regiões de sombra quase permanentes, ou seja, regiões em que dependendo da estação do ano não há incidência alguma de sol. A cobertura da rede também é um problema devido às construções e também a interferência de outros dispositivos que utilizem ondas de rádio para comunicação.” (Santos, 2010)

“Contudo, com a popularização dos micro-controladores, as redes de sensores sem fio têm se difundido, e o sensoriamento urbano é uma das aplicações que tem despertado bastante interesse nos últimos anos. O monitoramento da temperatura em uma grande cidade exige o emprego de muitos dispositivos para garantir a cobertura de toda a área de interesse. Os sensores, por estarem imersos em ambiente urbano, podem ser supridos de energia constantemente, possibilitando que o provimento de dados e informações de forma eficiente seja o foco principal de estudo. Este projeto tem como objetivo desenvolver um modelo de armazenamento e disseminação de dados para redes de sensores sem fio urbanas. O modelo proposto busca explorar a similaridade na extração contínua de dados de dispositivos comumente encontrados nos ambientes urbanos. A aplicação de um esquema de agrupamento baseado em similaridade possibilita que se obtenham os valores significativos de qualquer dispositivo de sensoriamento que pertença a uma dada região consultada. A conjectura é que esta estratégia possibilite a obtenção eficaz dos dados sensoriados, e consequentemente uma tomada de decisão mais rápida.” (Ibidem)

Segundo (Santos, 2010), os resultados do projeto, se implantados em uma rede urbana de sensores sem fio de larga escala, podem ser utilizados para prover informações essenciais para a adoção de políticas de saúde pública para garantir a qualidade de vida de seus habitantes, tais como conforto térmico e qualidade do ar. Além disso, diversas áreas e aplicações que se utilizem de redes de sensores sem fio urbanas poderão se beneficiar desse modelo.

O projeto UrbanSensorDB pertence ao grupo de redes sem fio e redes

avançadas (NR2) que desenvolve pesquisas nas áreas de roteamento e gestão eficaz de energia, segurança, confiabilidade e gerência de sistemas.

3.3.5 OpenWSN

A Internet das Coisas (*Internet of Things*[1]) permite várias aplicações, como dispositivos de rastreamento de tempo real ou lares auto-suficientes em energia. Com estas redes ganhando maturidade, órgãos de padronização começaram a trabalhar para padronizar como estas redes de pequenos dispositivos se comunicam. (Berkeley, 2011)

O objetivo do projeto OpenWSN, da Universidade da Califórnia, Berkeley, é fornecer implementações de código aberto de uma pilha completa de protocolos baseada nos padrões a serem finalizados da Internet das Coisas, em uma grande variedade de plataformas de hardwares e softwares. Esta implementação pode então ajudar tanto universidades quanto indústrias a verificar a aplicabilidade desses padrões para a Internet das Coisas, para que estas redes se tornem realmente ubíquas. (Ibidem)

3.3.6 CIA2 – Construindo Cidades Inteligentes: da Instrumentação dos Ambientes ao desenvolvimento de Aplicações

> "Um projeto de pesquisa envolvendo 19 instituições nacionais e quase 30 pesquisadores definirá propostas para construir cidades inteligentes. O projeto, denominado CIA2 - Construindo Cidades Inteligentes: da Instrumentação dos Ambientes ao desenvolvimento de Aplicações, tem como meta estabelecer uma infraestrutura de instrumentação, computação e comunicação para viabilização das cidades. O projeto abrange desde a aquisição dos dados urbanos brutos por meio de tecnologias de redes de sensores e internet das coisas, a comunicação, o armazenamento e o acesso a esses dados por meio de diferentes tecnologias e protocolos de redes sem fio. E vai até a construção de

lxxvilxxvi

[1] A Internet das coisas é uma revolução tecnológica que representa o futuro da computação e da comunicação e cujo desenvolvimento depende da inovação técnica dinâmica em campos tão importantes como os sensores wireless e a nanotecnologia.

> aplicações que se beneficiem de toda essa infraestrutura, suportando uma melhor gestão pública e do meio ambiente e agregando valor ao cidadão. O projeto tem apoio financeiro do Ministério de Ciência e Tecnologia pelo Centro de Pesquisa e Desenvolvimento em Tecnologias Digitais para Informação e Comunicação (CTIC) da Rede Nacional de Ensino e Pesquisa (RNP) no valor de R$ 1,8 milhão e é coordenado pelo professor do Departamento de Informática da UFPR, Aldri Luiz dos Santos, um dos professores lideres do grupo de pesquisa em Redes Sem Fio e Redes Avançadas (NR2).” (CIA2, 2011)

Os pesquisadores das instituições envolvidas reuniram oito propostas sobre o assunto e criaram uma rede de estudos. O projeto ainda está no começo e o que eles pretendem é por meio da instrumentação e integração das tecnologias de comunicação e de informação possibilitar que soluções inteligentes sejam criadas para apoiar os diferentes desafios encontrados nas cidades, como trânsito, vigilância, atendimento de emergência, monitoramento ambiental, saúde, educação e inclusão digital, bem como colaborar para uma maior eficiência e transparência na gestão pública. Essa primeira etapa, proposta pelos pesquisadores, terá a duração de dois anos. Os pesquisadores trabalham em três vertentes, que integradas possibilitarão a instrumentação de serviços para as cidades inteligentes. A primeira é a proposta das ações em comum, depois o sensoriamento de ambientes, implantando a rede de comunicação e, por fim, dar tratamento às informações pela internet. Ele explica também que a preocupação está em criar ferramentas para que o setor público possa usufruir.

Além da Universidade Federal do Paraná (UFPR), fazem parte da rede de pesquisas as universidades federais de Rio de Janeiro, Fluminense, Espírito Santos, Minas Gerais, Ouro Preto, São João Del Rey, Rio Grande do Sul, Santa Catarina, Alagoas, Rio Grande do Norte, Goiás, Pará, e PUC-Rio, USP, Unicamp, UNB, Universidade de Fortaleza. (Ibidem)

3.3.7 Sensor de Umidade do Solo

Atualmente, na Universidade Federal de Alfenas, Unifal-MG, está sendo desenvolvido um projeto na área de RSSFs, pelo discente Karim Costa Maluf de Paula, orientado pelos professores Tomás Dias Sant’Ana e Célio

Wisniewski. Atualmente o projeto se encontra em fase de experimentação de outros sensores, no caso os dispositivos Falker HFM2010 e WRambo Kits v3.

Figura 13 – Sensor Falker HFM2010.

Figura 14 – Sensor WRambo Kits v3.

4 Conclusões

Este capítulo apresenta as conclusões desta monografia.

A pesquisa realizada para a elaboração deste trabalho, demonstrou o crescente uso de RSSFs para as mais diversas áreas de aplicação. Através deste estudo pode-se perceber que tanto o mercado quando as universidades estão investindo pesadamente em pesquisa e desenvolvimento à cerca desta área, e que a tendência é o aumento do incentivo para tal.

É uma tendência que se consolida cada vez mais, o uso de RSSFs para tratamentos médicos, proteção militar, automação fabril e até mesmo para o uso no dia-a-dia, unindo as propostas de praticidade e baixo custo.

A monografia resultante da pesquisa serve como grande referência bibliográfica para pesquisas futuras, contendo informações de fontes importantes e atuais.

Entre as dificuldades encontradas, podemos citar especialmente o encontro de fontes atuais, imparciais e de alta qualidade, evitando encontrar artigos que faziam propagandas de produtos específicos, especialmente em se tratando dos dispositivos encontrados no mercado.

Através desta pesquisa também foi possível concluir que embora gradativamente as RSSFs comecem a aparecer no mercado mundial, existe um grande nicho de mercado a ser explorado, especialmente no Brasil, onde a concorrência ainda não é consolidada, e oportunidades surjam em diversas áreas.

Como uma proposta futura, é sugerida a criação de um grupo de pesquisa na área na instituição, oferecendo estrutura suficiente para a criação de dispositivos de qualidade e de baixo custo, necessidades primárias para o desenvolvimento e a pesquisa na área.

5 Referências Bibliográficas

ARAÚJO F. C., ANDERSON F., SANTOS K. F.. Avaliação de Estratégias e Construção de Software para a Medição do Nível de Energia em Sensores de Redes de Sensores Sem Fio (RSSF). II CONNEPI, 2007.

BÖHM, A., *State of the Art on Energy-Efficient and Latency-Constrained Networking Protocols for Wireless Sensor Networks*, 2007

Berkeley: OpenWSN. Disponível em: openwsn.berkeley.edu. Acessado em: 07 de Novembro de 2011.

Bosch oferece ao Mercado de reposição automotiva o sensor de estacionamento *ParkPilot* UFR6. Disponível em: http://www.bosch.com.br/br/negociosindustriais/produtos/sensor/pg/default.asp. Acessado em: 07 de Novembro de 2011.

Bosch mostra na Feicon 2010 como os motores automotivos ganham aplicações em residências. Disponível em: http://www.bosch.com.br/Imprensa/Releases/Detalhes.aspx?idRelease=6828. Acessado em: 07 de Novembro de 2011.

CABRINI F. H., KOFUJI S. T.. Introdução as Redes de Sensores Sem Fio, 2006.

CIA2: Universidades criam rede de pesquisas para desenvolver cidades inteligentes. Disponível em: http://www.nota10.com.br/noticia-detalhe/8852_Universidades-criam-rede-de-pesquisas-para-desenvolver-cidades-inteligentes-. Acessado em: 07 de Novembro de 2011.

COMER, D.. *Computer Networks and Internets*, 2009, 5ª Edição.

CORKE, P., et. al., *Environmental Wireless Sensor Networks*. *Proceedings of the IEEE*, 2010.

CURTIS, W. D., PINO, E. J., et. Al., SMART – *An Integrated Wireless System for Monitoring Unattended Patients*. *J Am Med Inform Assoc*., 2008.

FUJIWARA T., TAKAHASHI H., *Study on a Sensor Network System with a Self-Maintenance Function for Plant Monitoring System*. *Joint International Workshop: Nuclear Technology and Society – Needs for Next Generation*, 2008.

GAUGER M., et. al., *Prototyping Sensor-Actuator Networks for Home Automation*. REALWSN, 2008.

GIRÃO, P. S., ENACHE, G. A., *Wireless Sensor Networks: State of the art and future trends*. Metrologia e Inovação, 2ª Conferência Nacional, 2007.

GOUVEIA, B. A. T., Dispositivos de Monitoração e Controlo Automático de factores climáticos de museus, 2009.

KUROSE, J.F., ROSS, K.W.. Redes de Computadores e a Internet: Uma Abordagem Top-Down, 2006, 3ª Edição, pág. 3.

LEWIS, F. L., *Wireless Sensor Networks*, 2004.

LIMA, M. P., Redes de Sensores Sem-Fio: histórico, tipos, aplicações e cenário atual, 2010.

LOUREIRO, A.A.F.,Nogueira, J.M.S., Ruiz, L.B.,Mini, R.A.F..Redes de Sensores Sem Fio. XXI Simpósio Brasileiro de Redes de Computadores, 2003.

MANJESHWAR, AGRAWAL. TEEN: *A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks*. *Parallel and Distributed Processing Symposium*, 2001.

MARGIL, Cintia Borges, JUNIOR, Marcos Simplício, BARRETO, Paulo, CARVALHO, Tereza. Segurança em Redes de Sensores Sem Fio, 2009.

MEIRA D. M.. Um Mecanismo de Processamento de Consultas Distribuído em Redes de Sensores Sem Fio, 2007.

OLIVEIRA G. C., *Securing Your Future With* Rexroth, 2010

RAVINDRANATH, L.,et.al., *Improving Wireless Network Performance Using Sensor Hints*. *8th USENIX Syposium*, 2011.

RODRIGUES R. M.. Disponibilização de Informações Sensoriais Sem Fio Via UpnP, 2008.

RUIZ, Linnyer B., CORREIA, Luiz H., VIEIRA, Luiz F., e outros (2004). Arquitetura de redes de sensores sem fio. Pág. 167–218. Capítulo 4 do livro texto de mini-cursos do XXII Simpósio Brasileiro de Redes de Computadores (SBRC). Gramado, RS, Brasil. ISBN 85-88442-81-7.

RUIZ L. B., et. al. Arquiteturas para Redes de Sensores Sem Fio, 2004.

SANTOS, A. L.,et.al., UrbanSensorDB – Provimento Eficaz de Agrupamento de Dados em Redes Urbanas de Sensores sem Fio. Disponível em: http://www.nr2.ufpr.br/UrbanSensorDB/. Acessado em: 07 de Novembro de 2011.

SELAVO, L.et. al., LUSTER: *Wireless Sensor Network for Environmental Research*. SenSys, 2007.

SILVA, F. A., BRAGA, T. R. M., RUIZ, L. B., NOGUEIRA, J. M. S. "Tecnologia de Nodos Sensores Sem Fio". Relatório Técnico DCC/006, Departamento de Ciência da Computação da Universidade Federal de Minas Gerais, 2003.

STANKOVIC, J. A., et. al., *Wireless Sensor Networks for In-Home Healthcare: Potential and Challenges*. *Systems* (HCMDSS) *Workshop*, 2005.

VIEIRA, M. A. M., JUNIOR, D. C. S., *Survey on Wireless Sensor Network Devices*. *Emerging Technologies and Factory Automation*, 2003.

WINKLER, M., et. al., *Theoretical and practical aspects of military wireless sensor networks*. *Journal of Telecommunications and Information Technology*, 2008.

YASSEIN M. B., AL-ZOU'BI A., KHAMAYSEH Y., MARDINI W.. *Improvement on LEACH Protocol of Wireless Sensor Network* (VLEACH). *JDCTA: International Journal of Digital Content Technology and its Applications*, 2008.