Universidade Federal do Rio de Janeiro

Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais

Laerte de Andrade Arruda

UM ESTUDO SOBRE REDES DE SENSORES SEM FIO

Rio de Janeiro

2013

Laerte de Andrade Arruda

UM ESTUDO SOBRE REDES DE SENSORES SEM FIO

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Orientador:

Claudio Miceli Farias, M.Sc., UFRJ, Brasil

Rio de Janeiro

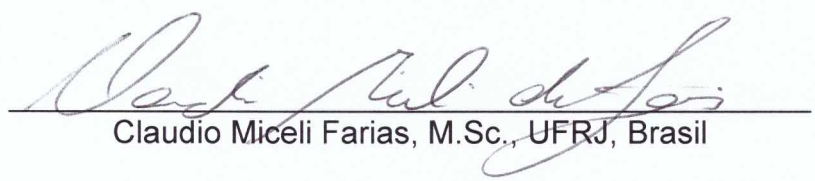
2013

Laerte de Andrade Arruda

UM ESTUDO SOBRE REDES DE SENSORES SEM FIO

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Aprovada em março de 2013.



Claudio Miceli Farias, M.Sc., UFRJ, Brasil

A minha gratidão à Cristine, minha mulher, sempre compreensiva e atenciosa, pelo incentivo e apoio ao meu esforço, e ao meu querido filho Gabriel, pelos sorrisos e carinho que sempre me motivaram a continuar em frente e não desistir, dedico este trabalho.

AGRADECIMENTOS

A Deus, meu Senhor, agradeço pela benção de avançar mais um passo diante de uma grande jornada.

Ao meu orientador Professor Claudio Miceli, agradeço pelo acolhimento, paciência e estímulo, sem os quais eu não teria êxito.

A minha família, por toda a força que me impulsionou para continuar e não desistir nos momentos mais difíceis.

Aos amigos, pela compreensão acerca de todas as horas que passei privada da sua companhia, pela ajuda prestada e pelos momentos de lazer que me permitiram descontrair durante todo este trabalho.

RESUMO

ARRUDA, Laerte de Andrade. **UM ESTUDO SOBRE REDES DE SENSORES SEM FIO**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2013.

Esse trabalho tem como objetivo estudar as redes de sensores sem fio e seu comportamento, apontando seus atributos, áreas de aplicação e desafios.

São tratadas questões relativas à comunicação, padrões utilizados, aplicação dos sensores, mostrando o potencial das redes de sensores sem fio. Também são apresentadas as diferenças e semelhanças que as redes de sensores sem fio possuem com as redes não estruturadas.

ABSTRACT

ARRUDA, Laerte de Andrade. **UM ESTUDO SOBRE REDES DE SENSORES SEM FIO**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2013.

This work aims to study wireless sensor networks and its behavior, pointing out its attributes, application areas and challenges.

Are dealt with issues relating to communication, standards used, applications, showing the potential of wireless sensor networks. It is also presented the main differences and similarities between ad-hoc and wireless sensor networks.

LISTA DE FIGURAS

	Página
Figura 1 – Tipos de Rede Sem Fio de Comunicação de Dados	12
Figura 2 – Exemplo de Rede de Sensores Sem Fio	16
Figura 3 – Unidades Básicas de um Nó Sensor	17
Figura 4 – Exemplo de Nó Sink	18
Figura 5 – Estabelecimento da Rede de Sensores	22
Figura 6 – Fusão de Dados Serial	24
Figura 7 – Fusão de Dados Paralela	25
Figura 8 – Fusão de Dados Híbrida	25
Figura 9 – Transmissão Multi-Hop	30

SUMÁRIO

	Página
1 **INTRODUÇÃO**	10
1.1 MOTIVAÇÃO	12
2 **SENSORES E COMUNICAÇÃO**	13
2.1 USO DE SENSORES EM REDE	13
2.2 USO DE COMUNICAÇÃO	15
3 **REDES DE SENSORES SEM FIO**	17
3.1 ÁREAS DE APLICAÇÃO	18
4 **DESAFIOS DE RSSF**	20
4.1 TOLERÂNCIA A FALHA	20
4.2 ESCALABILIDADE	20
4.3 CUSTO DE PRODUÇÃO	21
4.4 AUTO-ORGANIZAÇÃO	21
4.5 ENDEREÇAMENTO DOS SENSORES OU NÓS	22
4.6 FUSÃO DE DADOS	23
4.7 MOBILIDADE DOS SENSORES	26
4.8 DENSIDADE DE SENSORES	26
4.9 LIMITAÇÃO DA ENERGIA	27
4.10 QUALIDADE DE SERVIÇO EM RSSF	28
4.11 CLASSIFICAÇÃO E ARQUITETURA	29
4.12 SEGURANÇA EM RSSF	31
4.12.1 **Desafios**	31
4.12.2 **Vulnerabilidades**	32
4.12.3 **Ataques Sobre a Topologia da RSSF**	33
4.12.4 **Contramedida de Segurança**	35
5 **CONCLUSÃO**	37
REFERÊNCIAS	39

1 **INTRODUÇÃO**

O avanço tecnológico nas áreas de micro sistemas eletromecânicos (*MEMS – Micro Electro-Mechanical Sistems*), circuitos integrados e comunicação sem fio foram fatores-chave para o desenvolvimento mais acelerado das chamadas redes de sensores sem fio (RSSF) [1]. As RSSF são formadas por um grande número de sensores móveis e pequenos, denominados nós sensores, que são distribuídos numa determinada área ou base para detectar e transmitir características físicas de um ambiente. De uma maneira geral, RSSF podem ser utilizadas na área da segurança, no monitoramento, controle, atuação e manutenção de sistemas complexos, e monitoramento de ambientes internos e externos [2].

As redes de sensores sem fio são compostas por um grande número de nodos (nós sensores), que são elementos computacionais com capacidade de processamento, memória, interface de comunicação sem fio, além de um ou mais sensores do mesmo tipo ou não, que tendem a ser autônomos e necessitam de um alto grau de cooperação dos nós sensores para que possa executar as tarefas definidas para ela. Esses nós sensores são utilizados para as mais variadas situações, como por exemplo, para o monitoramento de abalos sísmicos, verificação de temperatura, pressão, acústica, fenômenos da natureza, etc. Podem ser organizados em grupos (*clusters*) onde um dos sensores deve ser capaz de detectar um evento na região, processá-lo e tomar uma decisão, de divulgar ou não o resultado para outros nodos. [2]

Os nós de uma RSSF possuem recursos bastante limitados, tais como reduzida capacidade computacional, pouca memória e pequena reserva de energia. Além disso, em muitas aplicações, os nós sensores são colocados em áreas remotas, o que não permite facilmente o acesso a esses elementos para

manutenção. Nesse cenário, o tempo de vida da rede depende da quantidade de energia disponível nos nós sensores e, por isso, eles devem balancear seus recursos limitados com o objetivo de aumentar o tempo de vida da rede. Portanto, a conservação de energia é um dos aspectos mais importantes a serem considerados no projeto das RSSF.

Em uma rede de sensores sem fio existem quatro componentes básicos distribuídos:

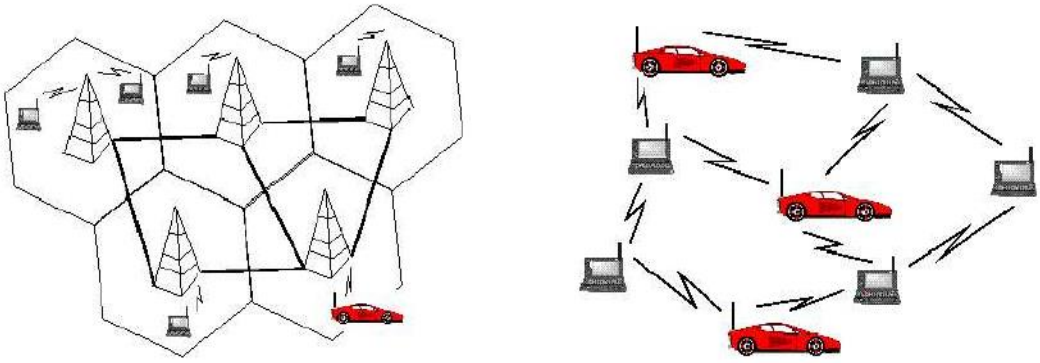
1. Um conjunto de nós sensores distribuídos aleatoriamente ou não;
2. Uma rede de interconexão sem fio;
3. Uma estação central para agrupamento e processamento de informações;
4. Um conjunto de recursos computacionais na estação central para manipular dados, tendência de eventos, solicitações de tarefas, etc.

As redes de sensores podem ser fisicamente estruturadas, onde cada sensor tem posição fixa, tanto lógica quanto física. Neste caso, geralmente os sensores são interligados através de condutores elétricos utilizados para comunicação de dados e alimentação.

Uma rede de sensores é formada pelos nós da rede, que possuem os sensores necessários ao seu funcionamento, que variam conforme a função da rede, e a parte eletrônica, responsável pelo envio dos dados coletados para a central de processamento.

1.1 MOTIVAÇÃO

Numa rede tradicional, a comunicação entre os elementos computacionais é feita através de estações base de rádio, que constituem uma infraestrutura de comunicação, como ilustrado na figura 1a. Esse é o caso da Internet. Por outro lado, numa RSSF os elementos computacionais trocam dados diretamente entre si, como ilustrado na figura 1b.



(a) Rede infra estruturada

(b) Rede não estruturada

Figura 1 – Tipos de Rede Sem Fio de Comunicação de Dados [2]

Com base nas situações apresentadas apresentaremos uma descrição detalhada de aplicações de redes de sensores sem fio, fazendo um comparativo com as redes de sensores tradicionais.

2 **SENSORES E COMUNICAÇÃO**

Neste capítulo será abordado o uso dos sensores descrevendo alguns atributos e padrões de comunicação, associando ao método de utilização de comunicação sem fio.

2.1 USO DE SENSORES EM REDE

Enquanto o ato de gerar dados pelo sensor é razoavelmente bem compreendido pelo emissor, transmitir dados de um sensor para um sistema da monitoração é um desafio, devido ao alto custo e à complexidade de redes de comunicações. Os sistemas cabeados funcionam basicamente assim: sensores ligados via cabos até centrais de coleta de dados, e esses dados são acessados por uma central de controle. Dependendo da distância entre os coletores de dados e o centro de controle, o cabeamento entre eles se torna impraticável, e os dados chegam a ser coletados localmente semanalmente ou em intervalos de tempos maiores.

Em relação às redes sem fio, a falta de padrões da indústria complicou o processo da integração de sensores pela falta de entendimento entre os fabricantes, atrasando a distribuição em grande escala. Assim, enquanto os sensores continuam a ganhar inteligência, eles permanecem incapazes de comunicar seus dados aos sistemas remotos. A maioria de sensores são ligados por fio aos sistemas de monitoração e controle, devido, em parte, à falta de soluções sem fio apropriadas e confiáveis.

Existem ainda os protocolos de comunicações das redes cabeadas, como o *ModBus*, *LonTalk*, ou *DeviceNet*, que fazem um bom trabalho integrando os sensores aos seus ambientes e fornecem altos níveis de confiabilidade e da

segurança. As redes cabeadas são apropriadas sempre que os dados forem tempo-críticos ou missão-críticos.

Os padrões *wireless*, incluindo o *Wi-Fi* [8], *Bluetooth* [18], e *ZigBee* [19], emergiram para fornecer maior flexibilidade do que os sistemas cabeados e para reduzir o risco de integrar comunicações *wireless* proprietárias. Com o *Wi-Fi* e o *Bluetooth* produzindo milhões das unidades anualmente, os custos caíram de valor consideravelmente.

A tecnologia *ZigBee*, foi o primeiro padrão *wireless* projetado especificamente para a monitoração remota e controle, onde pode melhorar significativamente o alcance e a confiabilidade de redes de sensores sem fio. Após a difusão do *ZigBee,* o padrão adotado para as camadas de enlace e física é o padrão 802.15.4 [28].

Associado as premissas de baixo custo, baixo consumo e curto alcance, o padrão 802.15.4 tem um papel diferenciado nas camadas mais baixas da tecnologia em sua pilha de protocolo [14]. Atuando na camada 2 do modelo *OSI* (*Open Systems Interconnection*) o protocolo 802.15.4 é um padrão do *IEEE* (*Institute of Electrical and Electronics Engineers*) que especifica a camada física e efetua o controle de acesso para redes sem fio pessoais de baixas taxas de transmissão. Foi desenvolvido para prolongar a duração da bateria do dispositivo, que necessita de baixo ciclo de trabalho para reduzir o consumo de energia [16]. Esses dispositivos passam pouca parte do tempo em estado ativo, tendo que periodicamente ouvir o canal para saber se existe uma mensagem para ele [14]. Esse mecanismo permite que a aplicação seja balanceada entre o consumo de bateria e a latência das mensagens. Por trabalhar com baixa taxa de transferência, as redes 802.15.4 são conhecidas como *LR-WPAN* (*Low Rate – Wireless Personal Area Network*), trabalhando com taxas de transmissão de até 250kbps [17].

A camada física do *ZigBee* segue o protocolo 802.15.4 e é responsável por permitir a transmissão das *PDUs* (*Protocol Data Units*), unidades de dados, através de ondas de rádio. A camada física utiliza a modulação *DSSS* (*Direct Sequence Spread Spectrum*) que incorpora em cada *bit* de dado um padrão de redundância e os espalha pela largura de banda utilizada. Essa redundância permite não só que o dado seja identificado como pertencente a um determinado nó, como é claro, facilita a detecção de erros[19].

A camada *MAC* (*Media Access Control*) do padrão 802.15.4 é responsável pelo processo do encapsulamento dos dados vindo das camadas superiores preparando-os para serem transmitidos.

2.2 USO DE COMUNICAÇÃO

Uma rede de sensores sem fio (RSSF) pode ser caracterizada pelo uso de uma quantidade grande de nós-sensores com a capacidade de se comunicar. Esses nós podem ser colocados dentro do fenômeno a ser analisado ou próximo a ele, diferentemente das redes de sensores tradicionais. As posições de cada nó não são pré-determinadas ou pré-calculadas, são aleatórias, visto que a implantação de redes de sensores em locais de difícil acesso pode ocorrer pelo uso de helicóptero, apenas "soltando" os nós sobre a região a ser analisada. A comunicação entre estes nós é feita através de uma rede *ad hoc* sem fio, um nó transmitindo a outro nó próximo os valores do sensoriamento (Figura 2). Este próximo nó deve se encarregar de passar os dados para o próximo nó, e assim por diante. A ideia é tirar proveito de dispositivos tão pequenos e (espera-se) baratos que possam ser usados em larga escala.

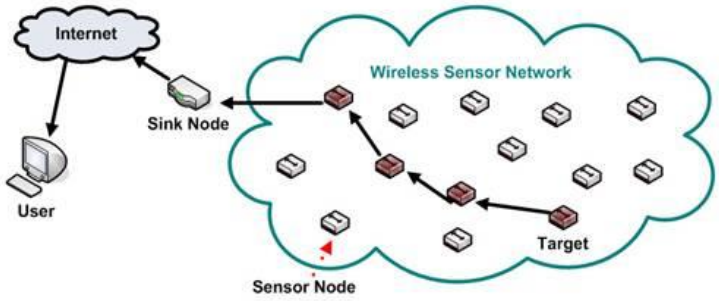


Figura 2 – Exemplo de Rede de Sensores Sem Fio [4]

3 **REDES DE SENSORES SEM FIO**

Rede de sensores sem fio é centrada em dados, diferente das redes tradicionais centradas em endereço. Assim, um nó difunde informações baseadas em atributos. Além disso, os nós-sensores devem atender a requisitos específicos da aplicação, muito comumente os nós focam-se em apenas um atributo, ou um pequeno conjunto de atributos, necessitando então de processamento no interior da rede. As restrições impostas à rede de sensores sem fio implicam em uma série de requisitos para os protocolos de comunicação nunca antes encontrados em tal escala. Como consequência de suas características, os protocolos de comunicação e gerenciamento da rede devem ter capacidades de auto-organização.

Um nó sensor é caracterizado, sobretudo pela sua dimensão reduzida, sendo composto por cinco unidades básicas: unidade dedicada a sensores e/ou atuadores, processamento, memória, fornecimento de energia e outra responsável pelas comunicações. A figura 3 ilustra como estes componentes básicos interagem uns com os outros.

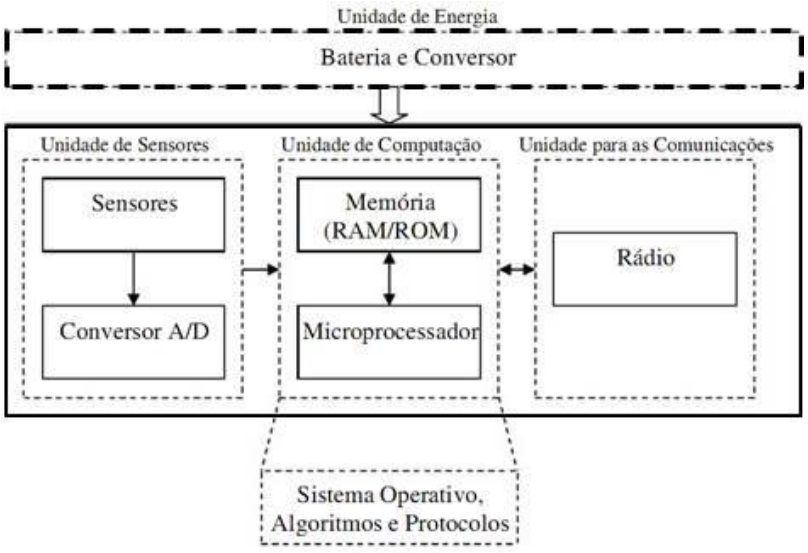


Figura 3 – Unidades Básicas de um Nó Sensor [5]

Os sensores realizam o monitoramento de eventos, enviando os dados coletados, ou recebidos de outro nó, para um dos nós vizinhos. Esta comunicação entre os nós é realizada até que um nó denominado (*sink*) receba as informações. O nó *sink* serve de interface entre a rede e o observador. Este nó é capaz de se comunicar com observador através de um *link* de comunicação, como por exemplo, a internet ou de uma conexão por satélite [6] como ilustra a figura 4.

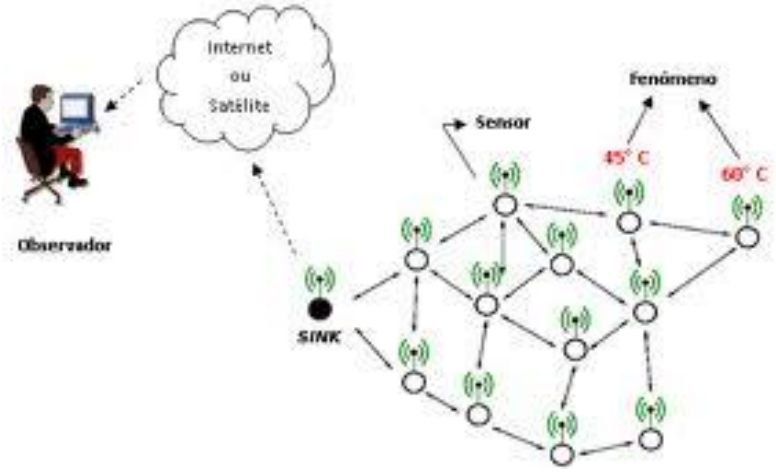


Figura 4 – Exemplo de um Nó *Sink* [7]

3.1 ÁREAS DE APLICAÇÃO

Redes de sensores têm o potencial de serem empregadas em diversas áreas, tais como [3]:

- Aplicações militares – Usadas para detectar movimentos inesperados dos inimigos, presença de algum objeto explosivo ou gases venenosos. O alcance de suas transmissões geralmente é baixo para evitar qualquer tipo de escutas indesejadas, e suas dimensões são reduzidas podendo-se utilizar nós sensores móveis caso venha ser inserido em robôs. As RSSF podem monitorar ambientes internos e externos, no reconhecimento das forças

inimigas, detecção e reconhecimento de ataques químicos, biológicos ou nucleares;

- Aplicações de distribuição de água, energia e gás – Indicar a pressão, temperatura e nível de ambos. Monitorar a extração de petróleo e gás em alto-mar;
- Aplicações ambientais – Este tipo de aplicação serve para monitorar florestas, oceanos, vulcões, desertos e áreas de desastres ambientais, na detecção de incêndios, enchentes, para auxiliar no controle da agricultura (verificação do solo, níveis de poluição no ar, etc.);
- Aplicações médicas e biológicas – Controlar e monitorar o funcionamento dos órgãos do corpo humano ou de animais, indicando ou não problemas biológicos; no diagnóstico e na administração de drogas para pacientes; para criação de interfaces para deficientes físicos; monitoramento de pacientes e médicos em um hospital, etc;
- Aplicações Industriais – Os sensores podem ser enxertados em peças no caso da área industrial, para efetuar testes nos mais diversos processos. Como exemplo, citar as siderúrgicas e refinarias, que usam esses sensores para controlar a temperatura, nível da caldeira, fluxo e pressão, indicando quaisquer tipos de problemas;
- Aplicações domésticas – Sensores embutidos em eletrodomésticos, que criam como consequência uma rede de cooperação entre os aparelhos.

4 **DESAFIOS DE RSSF**

Mesmo que as redes de sensores sem fio possuam algumas semelhanças com as redes convencionais não estruturadas, existem diferenças e desafios específicos a serem observados. A seguir são descritas características deste tipo de redes, onde normalmente não são encontradas nas redes convencionais.

4.1 TOLERÂNCIA À FALHA

Os nós sensores devem ser de baixo custo e pequenos no tamanho, o que acarreta no fato deles serem pouco confiáveis, fazendo com que a rede tenha que ser tolerante a falhas. As falhas podem ocorrer por diversos motivos: falta de energia, falta de visibilidade para outro nó da rede ou algum dano físico, devendo a rede ser capaz de realizar suas tarefas mesmo com a perda de alguns nós.

Os níveis de tolerância à falha vão determinar diferentes algoritmos de controle da rede [3]. O nível de tolerância à falha vai depender do ambiente e da aplicação, dependendo também desses mesmos fatores o algoritmo de controle da rede.

4.2 ESCALABILIDADE

Uma rede de sensores sem fio deve agregar um número de dispositivos significativamente maiores do que em redes convencionais, necessitando de soluções escaláveis. A associação e desassociação de nós sensores são comuns nesta tecnologia e a quantidade destes componentes podem variar inúmeras vezes.

4.3 CUSTO DE PRODUÇÃO

O custo de um único nó sensor é determinante no custo de toda a rede, visto que em redes de sensores sem fio pode ser usado um vasto número de nós sensores. Desta forma, o custo de um nó sensor deve ser mantido baixo, de modo a que o custo de implantação deste tipo de redes seja mais baixo que a estratégia que é aplicada os sensores tradicionais e com recurso a uma rede baseada em fios.

4.4 AUTO-ORGANIZAÇÃO

De forma similar as redes *ad hoc*, as redes de sensores sem fio possuem características de se autoconfigurar, formando uma rede conectada, porem com diferenças significativas em termos de tráfego, de compromisso de energia e de algoritmo de roteamento, entre outras.

Em algumas aplicações, sensores podem ser distribuídos de forma manual, um a um em locais pré-determinados, ou lançados na área que se deseja monitorar (figura 5). Essa ultima forma citada deve ser mais aplicada aos casos em que a rede contém centenas ou até milhares de sensores, em casos em que a área que se deseja monitorar é remota, de difícil acesso ou inóspita.

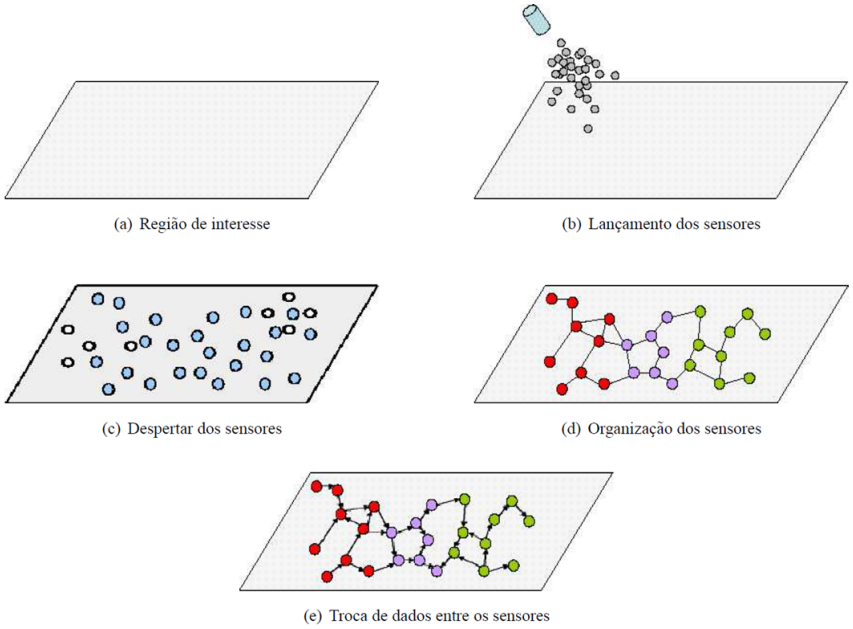


Figura 5 – Estabelecimentos da Rede de Sensores [2]

Uma vez presentes no ambiente, RSSF podem sofrer alterações de topologia devido a vários fatores, tais como: sensores podem ser destruídos pelo ambiente, sensores podem parar de funcionar devido ao esgotamento da bateria, sensores podem ser ligados e desligados para economia de energia, novos sensores podem ser acrescentados à rede e pode-se ter intermitência na comunicação sem fio devido a ruídos ou obstáculos no ambiente.

Assim, pela natureza dinâmica das RSSF, essas redes devem ter a capacidade de se ajustar a possíveis alterações sem interferência humana.

4.5 ENDEREÇAMENTO DOS SENSORES OU NÓS

Dependendo do interesse onde será aplicado cada sensor, é possível endereçá-lo individualmente ou não. Por exemplo, sensores embutidos em peças numa linha de montagem ou colocados no corpo humano devem ser endereçados unicamente caso seja desejado saber exatamente o local de onde o dado está

sendo coletado. Por outro lado, sensores monitorando o ambiente numa dada região externa possivelmente não precisam ser identificados individualmente, já que o ponto importante é saber o valor de uma determinada variável nessa região.

4.6 FUSÃO DE DADOS

Fusão de dados é uma alternativa para pré-processar os dados de uma RSSF de forma distribuída aproveitado a capacidade de processamento dos sensores [20]. Como consequência tem-se a otimização da quantidade e do tamanho das mensagens que trafegam pela rede e do consumo de energia nestas redes. Isso se faz necessário já que um efeito resultante da grande quantidade de sensores é a transmissão de dados redundantes e colisões [21]. Além da capacidade de uma RSSF agregar os dados coletados por esses sensores, esta, comporta o número de informações que precisam ser sumarizadas por ela. Depois de coletados os dados, são feitas junções dessas informações ou mensagens, e estas são enviadas para a estação-base.

Os benefícios dessa fusão são: maior precisão nas leituras, tornando a rede menos vulnerável a falhas e imprecisões de um único sensor; e a economia de energia, visto que a quantidade de mensagens que precisam ser transmitidas é reduzida [22].

Outro objetivo da fusão de dados está diretamente relacionado com o reconhecimento de informações mediante um canal ruidoso. O processo de fusão, neste caso, tenta reconhecer a possibilidade de um determinado evento ter ocorrido mesmo que o sinal sofra uma degradação proveniente do meio [23].

Devido à grande aplicação das redes de sensores sem fio e às características limitadas dos dispositivos sensores, o desenvolvimento de técnicas de fusão de

dados tem sido de grande necessidade para as mais diversas aplicações deste novo tipo de rede.

Considerando a comunicação entre os nodos sensores da rede, a fusão de dados é realizada em aplicações onde o monitoramento colaborativo [24] é realizado, podendo ser de três tipos: serial [25], paralela [26] e híbrida [25][26][27].

A fusão serial faz uso de técnicas de roteamento, por isso os dados são trafegados pelos sensores da origem até o destino. A fusão pode ocorrer em cada nodo sensor por onde o pacote passa. Os dados são coletados ao longo da rede podendo chegar ao destino já condensado, cabendo ao destinatário apenas tomar a decisão final. Nesta técnica, cada sensor fica com a responsabilidade de receber a leitura proveniente de outro sensor, ler, agregar a sua própria leitura e executar um algoritmo de fusão de dados para encaminhar para o nodo seguinte apenas um único pacote contendo apenas uma única leitura resultante da sua fusão de dados.

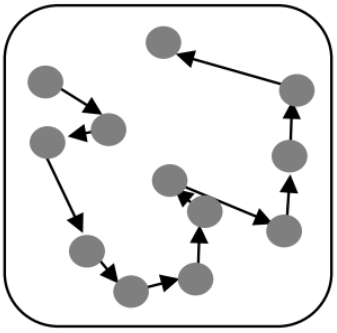


Figura 6 – Fusão de Dados Serial [24]

Na fusão paralela, todos os sensores processam seus dados independentemente e enviam seus dados coletados diretamente para o nodo destino, o qual se encarrega de fazer a fusão destes dados. Neste caso uma grande quantidade de mensagens pode ocasionar um grande número de colisões no nodo destino, porém esta técnica de fusão possibilita com que apenas um único nodo

tenha o poder de processamento necessário para executar a fusão de dados, podendo os demais sensores executarem apenas as atividades de leitura do sinal do ambiente e envio do pacote ao destino e como consequência acabarem apresentando um custo menor.

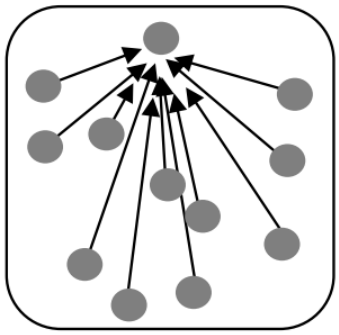


Figura 7 – Fusão de Dados Paralela [24]

A fusão híbrida, também denominada de fusão hierárquica ou em árvore, faz uso da fusão serial e da paralela. A sua formação é composta de um grupo de nodos sensores (um *cluster*) o qual possui um líder denominado *cluster head*. A comunicação dentro do grupo de sensores é exercida de forma paralela. Após o *cluster head* receber as mensagens, encaminha os dados coletados dentro do seu grupo para o *cluster head* raiz, o qual será responsável por tomar a decisão final. O processo de fusão de dados ocorre em cada *cluster head*.

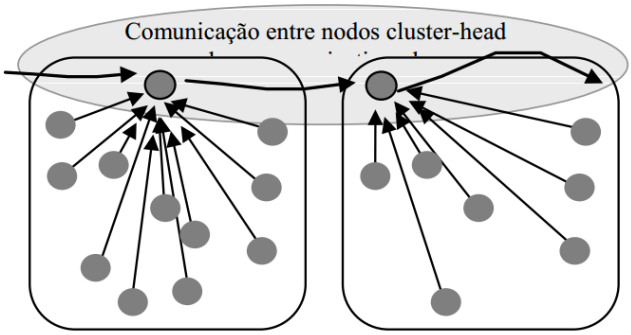


Figura 8 – Fusão de Dados Híbrida [24]

4.7 MOBILIDADE DOS SENSORES

Nós sensores podem ser fixos ou móveis. Por exemplo, sensores colocados numa floresta para coletar dados de umidade e temperatura são tipicamente estáticos, enquanto sensores colocados na superfície de um oceano para medir o nível de poluição da água são móveis. Embora atualmente a grande maioria dos sensores sejam estáticos e grande parte dos trabalhos se baseie em nós estáticos, espera-se que num futuro próximo a mobilidade seja um aspecto importante em RSSF, uma vez que o movimento dos sensores possibilitará um aumento da capacidade de monitoramento e da eficácia da comunicação entre nós e servirá de base para o surgimento de novas aplicações. A mobilidade possibilita que nós inicialmente mal posicionados possam se deslocar para regiões nas quais a eficiência seja maior. Isso é relevante, porque em muitas aplicações os sensores são instalados de forma aleatória, ao invés de terem sido postos em localizações precisas. Nesse caso, se o fenômeno não puder ser bem observado a partir da posição original do nó, este poderá ajustar sua localização de forma a melhorar sua capacidade de sensoriamento. Além disso, para melhorar a qualidade da comunicação, o sensor poderá se mover, ampliando sua conectividade com outros nós e reduzindo a quantidade de energia necessária para a transmissão de dados.

4.8 DENSIDADE DE SENSORES

Descreve qual a quantidade de sensores a serem utilizados para um adequado monitoramento de fenômenos ou ambientes. Para monitorar florestas, oceanos, e vulcões, por exemplo, as redes de sensores sem fio devem conter entre 10 a 100 mil sensores.

4.9 LIMITAÇÃO DA ENERGIA

A dependência da energia é o grande desafio para as redes de sensores sem fio. A energia deve ser controlada para que o seu tempo de duração seja mais prolongado e não haja indisponibilidade da rede.

Os nós que compõem a rede de sensores apresentam recursos muito limitados, sendo um deles a pouca reserva de energia, a qual provém da bateria. O tempo que uma rede de sensores vai funcionar vai depender da quantidade de energia disponível nos nós sensores. Portanto é necessário que os recursos e as funções desempenhadas por elas sejam balanceadas com o intuito de aumentar seu tempo de vida, por isso em um projeto de RSSF deve ser considerado o aspecto da energia, no momento em que está sendo projetada a rede.

Para que se tenha o conhecimento sobre a quantidade de energia, que será usada em cada parte da rede é utilizado um mapa de energia cujas informações auxiliam a prolongar esse tempo de vida da rede. Com a ajuda desse mapa, é possível verificar e determinar em que lugares estão distribuídos os sensores e onde estão ocorrendo as deficiências energéticas [3].

Em virtude desse aspecto fundamental, as aplicações, protocolos e algoritmos que serão aplicados para a rede de sensores não podem ser escolhidos pela elegância ou capacidade, mas, sobretudo, pela questão de seu consumo de energia. Os consumidores de energia são:

- Bateria – É responsável pelo armazenamento de energia do nó sensor e tem uma capacidade finita, assim como uma demanda de consumo específica;
- Rádio – É formado pelos sistemas de transmissão e recepção, amplificador e antena. O consumo de energia depende da operação efetuada. A transmissão de dados consome mais energia que a recepção;

- Processador – É o elemento de processamento central do nó sensor. O consumo depende da frequência do relógio (quanto maior a frequência, maior o consumo);
- Sensores – São os dispositivos de sensoriamento. O consumo depende principalmente do tipo de grandeza medida.

4.10 QUALIDADE DE SERVIÇO EM RSSF

O fator principal que dificulta a provisão de garantia de *QoS (Quality of service*) para RSSF é o consumo de energia. Naturalmente, outros parâmetros como conectividade da rede e quantidade de sensores disponíveis também devem ser considerados. O problema é que quanto maior o número de parâmetros de *QoS* a serem gerenciados, maior o consumo de energia. Além disso, estas redes apresentam os mesmos problemas das redes sem fio tradicionais, ou seja, recursos limitados e canais de comunicação não confiáveis e sujeitos a erros causados por ruído, sombreamento e interferências.

Nos ambientes previstos para utilização das redes de sensores sem fio, a garantia da qualidade de serviços e seu monitoramento são ainda mais difíceis. A reação as violações de *QoS* podem ser tomadas tanto pela aplicação, que fará uma renegociação de novos valores para os parâmetros de interesse, ou pela rede, que se adaptará ao novo cenário sem notificar a aplicação. Esta ultima opção é provável que não seja escolhida nas RSSF já que a rede precisaria conhecer detalhes da aplicação sendo executada para agir de forma apropriada. Qualquer que seja a estratégia usada, a renegociação dos novos níveis de *QoS* devem ser baseados no mapa de energia da rede e de outros parâmetros relevantes.

4.11 CLASSIFICAÇÃO E ARQUITETURA

As diferentes aplicações e os diferentes modos de operação das redes de sensores levam a duas categorias básicas: redes proativas e redes reativas, cada uma levando a diferentes tipos de protocolos de roteamento e modos de distribuir o consumo de energia entre os nós.

Nas redes proativas os nós periodicamente trocam entre si dados coletados. Nas redes reativas cada nó só reage a modificações no ambiente em que estão colocados. Desta maneira, as primeiras parecem adequadas a aplicações que necessitam monitoramento periódico, enquanto as últimas se prestam a aplicações tempo crítico.

Em virtude de suas características peculiares, as RSSF dependem da utilização de alguns protocolos de roteamento especiais. Os protocolos de roteamento dependem do tipo de aplicação que está em desenvolvimento e de como será a organização e desenvolvimento da rede. Existem três tipos de protocolos de roteamento: roteamento plano, roteamento hierárquico e roteamento geográfico [2].

Roteamento Plano: é aplicado em redes planas, que geralmente são homogêneas. Os algoritmos funcionam através de um encaminhamento *multi-hop* (figura 6). Isso se dá em razão da limitação do alcance de transmissão dos nós. A seguir três subclasses de algoritmos:

- Algoritmos reativos – O nó só busca uma rota quando requisitado, economizando energia e banda.
- Proativos – O nó automaticamente atualiza as rotas, o que traz maior gasto de energia e de banda.

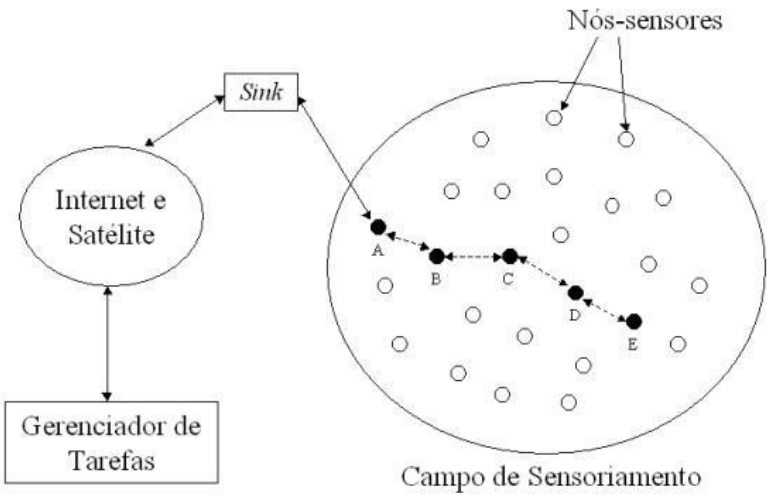


Figura 6 – Transmissão *Multi-hop* [9]

Em ambos existe o processo de descobrimento e de manutenção das rotas, que são controlados por pacotes de sinalização. O próprio descobrimento das rotas é feito por pacotes de sinalização e a manutenção periódica das rotas é feita por tabelas de roteamento e em alguns casos por pacotes de validação.

- Híbridos – Apenas uma parte dos nós faz a atualização periódica.

Roteamento Hierárquico: Os nós podem se dividirem em grupos chamados *clusters* e o mestre (*cluster head*) de cada grupo coordenam as tarefas entre os clusters. Este tipo de roteamento é mais complexo, porém possibilita maior estabilidade e a fusão dos dados coletados.

Roteamento Geográfico: Este tipo de roteamento baseia-se na localização dos nós sensores. Cada nó deve identificar a melhor localização de um grupo de sensores e a partir desta informação determinar o melhor caminho até destino.

4.12 SEGURANÇA EM RSSF

Os recursos muito limitados e as mais variadas necessidades de segurança tornam segurança em RSSF um desafio. Os requisitos para manter a rede segura variam conforme as aplicações, supondo uma aplicação para monitoramento de meio ambientes remotos, não há requisitos de confidencialidade na rede, diferente de uma aplicação em uma indústria, onde os dados de sensores podem ser usados pela concorrência [10]. Os requisitos mais comuns são integridade dos dados, confidencialidade, autenticidade dos nós e de dados, disponibilidade da rede e garantia de que os dados são recentes. A implementação da segurança de uma RSSF torna-se complicada quando levamos em conta os nós com recursos de processamento, armazenamento e energia limitados.

4.12.1 **Desafios**

1. Maximização da segurança x escassez de recursos:

Mecanismos simples para aumentar a segurança de uma rede neste caso devem ser bem observados, a simples criptografia de dados e a adição de assinatura aos pacotes podem arruinar o desempenho de uma RSSF. Visto que o aumento do processamento justificado pelos cálculos de criptografia e de assinatura, em conjunto com o aumento do tamanho de cada pacote, aumentam os gastos de energia e de processamento, normalmente escassos.

2. Topologia de RSSF vulnerável a ataques ao enlace:

Em redes sem fio, em geral, não existe proteção física aos meios de comunicação (sinal), assim ataques de monitoramento do canal (*man in the middle*) [11] e interferência por meio de sinais externos são possíveis. Com um grande

número de nós, atrelado a falta de monitoramento de todos estes e a possibilidade de mobilidade em alguns casos, se torna fácil a captura de nós e substituição por nós comprometidos e a obtenção de informações sobre a rede.

3. Características da comunicação sem fio

As limitações de comunicações sem fio trazem dificuldades. O alcance de transmissão e largura de banda limitada, e enlaces não confiáveis acabam por requerer mecanismos diferentes dos encontrados em redes cabeadas.

4.12.2 **Vulnerabilidades**

As características físicas de comunicação de uma RSSF abrem algumas vulnerabilidades na rede, interferência e destruição de nós [11]. A interferência de um sinal ocorre quando um nó intruso ou uma fonte externa ao sistema gera sinais aleatórios, impedindo a comunicação.

Pelo fato dos nós estarem alocados em locais sem segurança física ou sem monitoramento, assim um intruso pode lesionar um nó, de modo a prejudicar as funções do nó (coleta de informações e roteamento) e da rede por consequência. O nó ainda pode ser substituído por um nó intruso para coleta de informações e/ou ataques na rede. Com a captura de um nó, informações nele contidas podem ser extraídas permitindo ao intruso obter as chaves de criptografia e a autenticação.

Na camada de acesso ao meio encontramos o seguinte problema, ocorrência de um ataque à rede com base na indução de colisões. Os quadros danificados são descartados e retransmitidos, gastando energia e tempo, as retransmissões possuem número máximo de tentativas, ocasionando na perda de alguns quadros. O uso de corretores de erros pode evitar o descarte de um quadro inteiro por colisões

induzidas, porém os corretores para números grandes de bits errados são complexos (como ocorre uma indução de colisões espera-se número de erros por pacote maior que o normal) e comprometem o processamento do nó. Este tipo de ataque pode gerar o esgotamento energético de um nó chave, causando partição da rede e/ou sua negação de serviço (*Deny of Service*).

4.12.3 **Ataques Sobre a Topologia da RSSF**

Outras formas de ataques ocorrem devido à topologia da rede, onde todos os nós são roteadores. Há várias maneiras de atacar uma rede RSSF tirando vantagem deste tipo de configuração.

1. Buracos Negros (*Black or sinkholes*)

Um nó intruso inserido dentro da rede se torna a melhor rota para comunicação entre vários outros nós, possibilitando o descarte e modificação dos pacotes. A disputa por esta rota causará um gasto energético concentrado nos nós próximos ao nó intruso, o que pode levar a uma divisão da rede com o fim da energia destes nós, prejudicando o funcionamento da aplicação como um todo.

2. Inundação da rede (*flooding*)

Um nó intruso inunda a rede com informações falsa, aumentando o tráfego, os gastos com energia e o congestionamento de pacotes.

3. Desvios e *loops*

Um grupo de nós mal intencionados alteram os comandos de roteamento dos pacotes, de forma a criar desvios ou *loops*, criando congestionamento, aumentando o consumo de energia e causando a perda ou atraso na entrega de informações.

4. Buraco de verme (*Wormholes*)

Dois ou mais nós intrusos estabelecem comunicação entre si sem contato com os canais usados pela RSSF, através deste canal são enviados pacotes de uma parte da rede para outra parte causando problemas de roteamento.

5. Sequestro de nós

Vários nós intrusos cercam um nó da rede, recusam os envios de suas mensagens descartando ou inserindo dados falsos nos pacotes.

A morte de nós causa os chamados “buracos de cobertura”, ocorrem quando a densidade de sensores ativos em determinada região é pequena, tornando a análise daquele sistema ruim ou impossibilitada. A densidade de nós ativos varia conforme a necessidade da aplicação.

Um problema que influencia vários aspectos da rede é a geração de pacotes de validação falsos (*Acknowledges ou Ack’s*). A falsificação destas mensagens pode causar inúmeros problemas, tais como aceitar um nó danificado como nó intacto, um caminho de roteamento ser avaliado como bom, no entanto é ruim ou que um nó sem energia está com energia, entre outros.

4.12.4 **Contramedidas de Segurança**

Criptografia:

Uma solução básica para problemas de confidencialidade consiste na encriptação de dados, além disto, previne outros tipos de ataques uma vez que protege as informações de controle e endereçamento dos pacotes. Em RSSF são comumente usadas as chaves simétricas, são distribuídas diferentes chaves a grupos de nós de forma que todos do mesmo grupo possam ler e alterar os dados, e ainda assim manter segurança de uma parte da rede caso um nó seja capturado isoladamente. O uso do par de chaves não é eficiente devido ao alto custo de processamento, limitado nos nós, e por isso não são utilizadas.

Autenticação:

A autenticação em RSSF consiste numa adaptação da autenticação com par de chaves assimétricas, para chaves simétricas. A estação base computa o código de autenticação da mensagem usando uma chave secreta e envia o pacote para os nós. Nenhum inimigo conseguirá alterar o pacote, pois somente a estação saberá a chave secreta, neste momento. Os nós receptores guardarão a mensagem em um buffer. Passado um período de tempo, suficiente para todos os nós receberem os pacotes, a chave secreta é revelada para todos os nós. Quando um nó recebe a chave revelada é fácil conferi-la usando a chave anterior, porque toda chave é gerada por uma função pública unidirecional (função *hash*), conhecida pela base e pelos nós. Cada chave consiste na combinação dos *hash's* da chave anterior. Para autenticação o nó compara a chave revelada com a combinação dos *hash's* da chave anterior, caso esteja correto, o nó verifica o pacote do buffer com a chave

revelada, conferindo o código de autenticação, garantindo que a mensagem não foi alterada.

5 **CONCLUSÃO**

No decorrer de todo o trabalho, foi possível observar o grande potencial que as RSSF possuem e como podem ser de grande utilidade em diversas áreas. No caso de aplicações que necessitam de dados em regiões remotas e/ou perigosas ou aplicações ligadas ao monitoramento de parâmetros biológicos, uma rede de sensores é essencial.

Apesar de apresentarem características comuns às redes móveis *ad hoc*, não podem ser abordadas e tratadas como tais, pois em RSSF, os nós têm baixa capacidade de energia e disponibilidade de memória. Assim, os protocolos de roteamento utilizados para redes *ad hoc* não são apropriados em RSSF, pois geram grandes tabelas de roteamento, memória insuficiente nos nós sensores, além de não apresentarem suporte a agregação de dados e a criação e manutenção de rotas, importante quando se trata da energia dos nós.

Sendo assim, as RSSF trazem novos conceitos e problemas, tais como: capacidade de auto-organização, topologia dinâmica, pouca disponibilidade de energia, fornecimento de informações atuais e corretas do fenômeno, etc. Isto apresenta uma série de novas oportunidades de pesquisa, onde um dos rumos que estão sendo apontados no sentido da pesquisa de RSSF é o surgimento das redes de sensores compartilhadas.

As redes de sensores compartilhadas suportam múltiplas aplicações, de forma dinâmica enviados por diferentes proprietários e, simultaneamente, aplicado sobre uma infraestrutura compartilhada. Nesta visão podemos destacar algumas características:

- A camada de virtualização que está sendo executado em cada nó sensor abstrai o acesso a recursos de sensores e permite a gestão destes recursos através de políticas expressas pelo respectivo proprietário;
- Um ambiente de tempo de execução em cada nó que permite que vários aplicativos sejam executados dentro de cada nó;
- Uma política de implementação de aplicativos baseados que permite aplicação múltipla a ser implantado através da infraestrutura compartilhada.

Como desafio pode-se citar a alocação dinâmica de recursos, onde os proprietários da rede possuem suas políticas sobre o uso de recursos e as exigências de aplicação serão satisfeitas de acordo com esta política; o particionamento de rede flexível para apoiar as redes de sensores virtuais e o compartilhamento seguro dos recursos assegurando a proteção de outras aplicações.

REFERÊNCIAS

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. **Wireless sensor networks: a survey**. Computer Networks, Março 2002.

[2] Loureiro, A. A. F., Nogueira, J. M. S., Ruiz, L. B., Mini, R. A., Nakamura, E. F., Figueiredo, C. M. S. **Redes de Sensores sem Fio. XXI Simpósio Brasileiro de Redes de Computadores (SBRC'03)**, Natal, RN, Brasil. 2003

[3] Portela, M. **Diversidade Cooperativa Adaptativa Aplicada a Redes de Sensores sem Fio**. Paraíba, 2009. Dissertação de Mestrado. Universidade Federal de Campina Grande.

[4] http://monet.postech.ac.kr/research.html. Acesso em 20 Fev 2013.

[5] Vieira, Marcos. A. M., da Silva Junior, D. C., Jr., C. N. C., and da Mata, J. M. (2003). **Survey on wireless sensor network devices. In IEEE Conference on Emerging Technologies and Factory Automation**.

[6] Karl, H.; Willig, A. 2005. **Protocols and Architectures for Wireless Sensor Networks**. John Wiley & Sons.

[7] ARDUINO. http://www.arduinopi.net/2010/10/introducao-redes-de-sensores-sem-fio.html, Acesso em 07 Fev 2011

[8] Ye, W., Heidemann, J., Estrin, D. "**An Energy-Efficient MAC protocol for Wireless Sensor Networks**". In: Proceedings of the IEEE INFOCOM 2002, Junho de 2002

[9] Lemos, P. **Redes de Sensores sem fio**. Rio de Janeiro Universidade Federal do Rio de Janeiro. Disponível em: http://www.gta.ufrj.br/grad/02_2/Redes%20de%20sensores/Redes%20de%20Sensores%20Sem-fio.htm, Acesso em 05 Mar. 2013.

[10] Campista, Miguel., Duarte, O.; **Segurança em Redes de Sensores**. Rio de Janeiro Universidade Federal do Rio de Janeiro. Disponível em: http://www.gta.ufrj.br/seminarios/CPE825/tutoriais/miguel/miguelSensorSeg.pdf. Acesso em 05 Fev. 2013.

[11] Natalia C. Fernandes, Marcelo D. D. Moreira, Pedro B. Velloso, Luís Henrique M. K. Costa e Otto Carlos M. B. Duarte. **Ataques e Mecanismos de Segurança em Redes Ad Hoc**. Rio de Janeiro Universidade Federal do Rio de Janeiro. Disponível em: http://www.gta.ufrj.br/ftp/gta/TechReports/FMVC06.pdf. Acesso em 02 Fev. 2013.

[12] Nakamura, E. Loureiro, A. Frery, **A. Information Fusion for Wireless Sensor Networks: Methods, Models, and Classifications**, 2007

[13] Lins, B.F.de Oliveira. **ADS-Fusion: Fusão de dados para detecção de anomalias baseada na teoria de evidência de Dempster-Shafer**. Pernambuco, Universidade Federal de Pernambuco. Disponível em: http://www.cin.ufpe.br/~tg/2008-2/bfol-proposta.pdf. Acesso em 10 Mar. 2013.

[14] IEEE P802.15.4/D18, **Draft Standard: Low Rate Wireless Personal Area Networks**, Feb. 2003.

[15] IEEE 802.11, Part 11: **Wireless LAN medium access control (MAC) and physical layer (PHY) specifications, IEEE**, Aug. 1999.

[16] E. Shih, S. Cho, et al., **Physical layer driven protocol and algorithm design for energy-efficient wireless sensor networks,** Proc. MOBICOM, 2001.

[17] Jon T. Adams. **An Introduction to IEEE STD 802.15.4**, Freescale Semiconductor, Inc.

[18] MARÇAL, I. S. **Bluetooth e Zigbee Padrões para Redes Pessoais Sem Fio**, 2008

[19] ERGEN, S. C. **ZigBee/IEEE 802.15.4 Summary**, 2004

[20] LIANG, BING; LIU, QUN; **A Data Fusion Approach for Power Saving in Wireless Sensor Networks**. First International Multi-Symposiums on Computer and Computational Sciences, 2006

[21] PATNAIK, M.S.; **Genetic Algorithms: A Survey**. In: IEEE Computer, Vol. 27, 1994.

[22] RIBEIRO, G.M.; LORENA, L.A.N.; **Roteamento de Veículos Dinâmicos Usando Algoritmos Genéticos**, In: XIX ANPET – Congresso de Pesquisa e Ensino em Transportes, Recife, 2005

[23] D'COSTA, A.; SAYEED, A.M.; **Data versus decision fusion in wireless sensor networks**. Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing, 2003.

[24] PINTO, A.; BITENCORT, B.; CABREIRA, U.; RIBEIRO, M.A.; CARLOS, M.; **Fusão de Dados Tempo Real em Redes de Sensores Sem Fio Multimídia. In Webmedia**, Gramado, 2007. Anais do Simpósio Brasileiro de Sistemas Multimídia e Web.

[25] PATIL, S.; DAS, S.R.; NASIPURI, A.; **Serial data fusion using space-filling curves in wireless sensor networks**. First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks. IEEE, 2004.

[26] PINTO, A.R.; BITENCORT, B.R.; MONTEZ, C.; **Uma Abordagem de Fusão de Dados com restrições de Tempo Real em Redes de Sensores Sem**

Fio. In: VIII Simpósio Brasileiro de Automação Inteligente, Florianópolis, 2007

[27] MACHADO, M.V.; GOUSSEVSKAIA, O.; MINI, R.A.F.; REZENDE, C.G.; LOUREIRO, A.A.F; MATEUS, G.R.; NOGUEIRA, J.M.S.; **Data dissemination in autonomic wireless sensor networks**. IEEE Journal on Selected Áreas in Communications, 2005.

[28] Institute of Electrical and Electronics Engineers, Inc., IEEE Std. 802.15.4 – 2003, IEEE Standard for Information Technology – telecommunications and Information Exchange between Systems – Local and Metropolitan Area Networks – Specific Requirements – **Part 15.4: Wireless 83 Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (WPANs)** New York: IEEE Press. 2003.