Tutorial sobre Redes de Sensores

Marluce R. Pereira e Cláudio L. de Amorim
Programa de Engenharia de Sistemas e Computação
COPPE/UFRJ, Brasil
(marluce,amorim)@cos.ufrj.br

Maria Clicia Stelling de Castro
Departamento de Informática e Ciência da Computação
Instituto de Matemática e Estatística-CTC
Universidade do Estado do Rio de Janeiro, Brasil
clicia@ime.uerj.br

Resumo

Na computação móvel é desejável se obter acesso contínuo as informações através de uma comunicação sem fio. As redes sem fio vêm sendo utilizadas nas mais diversas áreas. Como exemplo desta diversidade podemos citar as áreas militar, de turismo, educação, médica entre outras.

O objetivo deste trabalho é apresentar os vários aspectos de uma rede de sensores e suas aplicações no mundo real. Portanto, buscamos enfocar as definições existentes, as principais características de uma rede de sensores, as métricas de desempenho, a arquitetura, os modelos de comunicação e envio de dados existentes, os protocolos, a segurança entre outros pontos relevantes. Apresentamos também alguns exemplos de sensores e suas aplicações no mundo real.

1. Introdução

As redes móveis sem fio estão sendo utilizadas nas mais diferentes áreas como a militar, de turismo, educação, controle de estoque, descoberta de desastres ecológicos, emergência médica entre outras.

Na computação móvel sem fio o usuário tem acesso contínuo às informações através de uma rede de comunicação sem fio. Este tipo de rede é apropriado para situações onde não se pode ter uma instalação com fios e que requer acesso imediato à informação.

As tabelas 1 e 2 [20] apresentam características de várias tecnologias sem fio e suas aplicações. Cada uma das aplicações potenciais de diferentes serviços sem fio estão abordadas a seguir.

As aplicações de sistemas celulares permitem conectar um computador portátil via uma rede sem fio a uma *LAN* (*Local Area Network*) para carregar dados atuais de um determinado documento ou de um banco de dados.

As aplicações baseadas em *WLAN* (*Wireless LAN*) são sistemas de comunicação de dados flexíveis implementados como uma extensão de uma *LAN* com fio. As ondas eletromagnéticas transmitem e recebem dados do ar, minimizando a necessidade de conexões com fio.

Aplicações baseadas em *GPS* (*Global Positioning Systems*) são sistemas de posicionamento via rádio que

Tabela 1. Tecnologias sem fio e características associadas

Tecnologia	**Serviços/ Características**	**Área de Cobertura**	**Limitações**	**Exemplos de Sistemas**
Celular	Voz e dados através de telefones portáteis	Contínua	Largura de banda muito baixa	Telefones celulares, *PAD´s* e *Palm Pilots*
WLAN	*LAN* tradicional com interface sem fio	Somente ambientes locais	Alcance limitado	*NCR´s Wave LAN* e ALTAIR
GPS	Determina posição tridimensional e velocidade	Qualquer lugar do mundo	Custo elevado	GNSS, NAVSTAR e GLONASS
PCS por satélite	Principalmente para mensagens	Quase todo o mundo	Custo elevado	Iridium e Teledesic
Redes *ad hoc*	Grupo de pessoas que compartilham dados	Similar a *LAN*	Alcance limitado	Bluetooth
Redes de sensores	Sensores pequenos sem fio	Pequena	Alcance limitado	Aplicações de defesa civil e militar

Tabela 2. Aplicações potenciais de diferentes serviços

Tecnologias sem fio	Celular	*WLAN*	*GPS*	*PCS*	Redes *ad hoc* e de sensores
Área de Aplicação	serviços no campo, segurança pública, controle de estoque, transportadoras e atividades de linhas aéreas	lojas varejistas, serviços de saúde, tele-diagnósticos, estudantes, restaurantes, escritórios, indústria manufatureira e estoque	pesquisa, agência de aluguel de carros e esportes	*GPS*, Multimídia e Telemetria	Sensores de ambiente, máquinas de prognóstico, detecção de pontes quebradas, condições das estradas e sensores biológicos

funcionam 24 horas, informando posições em três dimensões, velocidade e tempo para usuários com equipamento apropriado em qualquer lugar na superfície da terra. O sistema NAVSTAR, operado pelo Departamento de Defesa Americano é o primeiro sistema *GPS* que permite localização e navegação inteligente de veículos. Além disso, tem muitas aplicações militares, como detecção de minas e localização de alvos [20].

O *Personal Communications System* (*PCS*) descreve uma nova classe de serviços de comunicação sem fio. Eles utilizam toda a tecnologia digital para transmissão e recepção de dados. O projeto Iridium, criado pela Motorola, é um consórcio de tecnologia para *PCS*. Os satélites enviam sinal contínuo para qualquer lugar da terra, suprindo telefones com opções convencionais sem fio e *pagers* com mensagens de texto.

Uma rede *ad hoc* é uma *WLAN* onde os dispositivos móveis são parte da rede somente quando eles estão suficientemente próximos, de forma que seja possível realizar transmissões. Não há infra-estrutura fixa e a informação é passada ponto a ponto usando roteamento *multihop* (múltiplas rotas). Um exemplo de aplicações militares para redes *ad hoc* é o compartilhamento de informações por um grupo de soldados em seus *notebooks*, numa determinada distância, através de sinais de rádio freqüência (*RF – Radio Frequency*). Outra forma de conectar muitos dispositivos é utilizar a tecnologia Bluetooth [2] e conectar telefones celulares a *laptops*, impressoras, *PDAs* (*Personal Digital Assistant*), fax, *joysticks* entre outros periféricos.

Uma rede de sensores pode ser definida sob diferentes enfoques. Uma definição encontrada na literatura para rede de sensores é a de uma rede sem fio formada por um grande número de sensores pequenos e imóveis plantados numa base *ad hoc* para detectar e transmitir alguma característica física do ambiente. A informação contida nos sensores é agregada numa base central de dados [20].

Sob o enfoque de sistemas distribuídos, para Heidemann *et al.* [13], uma rede de sensores pode se definida também como uma classe particular de sistemas distribuídos, onde as comunicações de baixo nível não dependem da localização topológica da rede. Desta forma, possui características particulares como a utilização de recursos restritos de energia, topologia de rede dinâmica e uma grande quantidade de nós. Estas características dificultam a reutilização de alguns algoritmos desenvolvidos para outros tipos de sistemas distribuídos. As soluções para estes problemas, como a sincronização da rede, a eleição de um líder e a aquisição de informações que representam o estado da rede devem considerar também características como a precisão, eficiência e o custo das operações.

Outro enfoque que se pode ter de redes de sensores é de um conjunto de nós individuais (sensores) que operam sozinhos, mas que podem formar uma rede com o objetivo de juntar as informações individuais de cada sensor para monitorar algum fenômeno. Estes nós podem se mover juntamente com o fenômeno observado. Por exemplo, sensores colocados em animais para observar seu comportamento. Ao observar o conjunto de sensores estaria monitorando toda a manada.

Sensores podem ser vistos como pequenos componentes que combinam energia computacional, capacidade de computação sem fio e sensores especializados [29]. Estes componentes ou nós podem ser utilizados de forma eficiente, mesmo que sejam milhares, para alcançar uma missão comum.

Os sensores podem ser usados para monitorar ambientes que sejam de difícil acesso ou perigosos, tais como o fundo do oceano, vizinhanças de atividades vulcânicas, territórios inimigos, áreas de desastres e campos de atividade nuclear. Eles, também, podem ser usados para tarefas interativas, como encontrar e detonar minas dos inimigos, buscar sobreviventes de desastres naturais ou conter e isolar óleo derramado, para proteger a costa marítima.

A nova tecnologia de sensores cria um conjunto diferente de desafios provenientes dos seguintes fatores: (i) os nós encontram-se embutidos numa área geográfica e interagem com um ambiente físico; (ii) são menores e menos confiáveis que roteadores de redes tradicionais; (iii) geram (e possivelmente armazenam) dados detectados ao contrário de roteadores de rede e (iv) podem ser móveis.

Dada a diversidade de fatores e desafios é necessário um novo conjunto de ferramentas de software e protocolos para habilitar a programação e o uso efetivo de tais sistemas de computação embutida em redes [29].

Apesar dos desafios encontrados para se construir uma rede sensores existem muitas vantagens na sua utilização: (i) diminui o custo do sistema, a utilização comercial de tecnologias de rede (ATM, Ethernet, fibra ótica) em sistemas de sensores tradicionais reduz o custo da rede e aumenta o desempenho; (ii) permite a monitoração de alvos de difícil detecção (alvos que possuem baixa atividade sonar atravessando seções, ruídos de baixa radiação são difíceis de detectar e classificar. Utilizando uma combinação de sensores é possível obter informações de número, tipo e localização do alvo monitorado) e (iii) redução de erros (a combinação de sensores de diferentes freqüências melhora a precisão das medidas. Para isso, requer sincronização e posição precisa dos sensores).

Em ambientes inteligentes futuros, as redes de sensores sem fio serão importantes em detectar, coletar e disseminar informações de determinados fenômenos. Aplicações de sensores representam um novo paradigma para operação de rede, que têm objetivos diferentes das redes sem fio tradicionais.

Tilak *et al.* [31] classificaram redes de sensores de acordo com diferentes funções de comunicação, modelos de envio de dados, dinamismo da rede, métricas de desempenho e arquitetura. Esta taxonomia pode ajudar na definição apropriada de infra-estruturas de comunicação para diferentes sub-espaços de aplicações de redes de sensores, permitindo que projetistas de redes escolham o protocolo de arquitetura que melhor se adapte com os objetivos de sua aplicação. Além disso, esta taxonomia habilita novos modelos de redes de sensores para serem definidos para futuras pesquisas nesta área [31].

As seções seguintes apresentam esta taxonomia e alguns trabalhos relacionados a redes de sensores. Na Seção 2 são descritas as características das redes de sensores, com a definição de sensor, observador e fenômeno. Na Seção 3 as métricas de desempenho são ilustradas: vida útil, latência, precisão, tolerância a falha e escalabilidade. A arquitetura de redes de sensores é apresentada na Seção 4, onde são definidos a infra-estrutura, o protocolo de rede entre a aplicação e o observador. Os modelos de comunicação, envio de dados e os modelos dinâmicos de rede são descritos na Seção 5. Na Seção 6 é realizada uma análise dos protocolos de roteamento existentes para redes de sensores. Na Seção 7 são apresentados os problemas de segurança relacionados a redes de sensores e soluções possíveis apresentadas na literatura. A Seção 8 apresenta alguns projetos relacionados a redes de sensores. Finalmente, na Seção 9 são apresentadas algumas considerações finais.

2. Características das redes de sensores

Nesta seção são apresentadas as principais características de redes de sensores, segundo a taxonomia de Tilak *et al.* [31]. As redes de sensores possuem como características principais: o sensor, o observador e o fenômeno, que estão definidos a seguir.

O **sensor** é o dispositivo que implementa a monitoração física de um fenômeno ambiental e gera relatórios de medidas (através de comunicação sem fio). Um sensor produz uma resposta mensurável a mudanças em condições físicas, tais como temperatura, campo magnético e luz [22]. Os dispositivos de detecção, geralmente, têm características físicas e teóricas diferentes. Muitos modelos de complexidade variada podem ser construídos baseados na necessidade da aplicação e características dos dispositivos. Na maioria dos modelos de dispositivos sensores a habilidade de detecção diminui com o aumento da distância do sensor ao fenômeno e melhora com o aumento do tempo que o sensor fica exposto para coletar informações [22]. Um sensor, tipicamente, consiste de cinco componentes: detector de hardware, memória, bateria, processador embutido e transmissor-receptor.

O **observador** é o usuário final interessado em obter as informações disseminadas pela rede de sensores em relação a um fenômeno. Ele pode indicar interesses (ou consultas) para a rede e receber respostas destas consultas. Além disso, podem existir, simultaneamente, múltiplos observadores numa rede de sensores.

O **fenômeno** é a entidade de interesse do observador, que está sendo monitorada e cuja informação potencialmente será analisada/filtrada pela rede de sensores. Além disso, múltiplos fenômenos podem ser observados concorrentemente numa rede.

Numa aplicação, o observador está interessado em monitorar o comportamento do fenômeno sob algum requisito de desempenho específico (por exemplo, precisão ou retardo).

Numa rede de sensores típica, os sensores individuais apresentam amostras de valores locais (medidas) e disseminam informação, quando necessário, para outros sensores e eventualmente para o observador. As medidas realizadas pelos sensores são amostras discretas do fenômeno físico, sujeito a medidas precisas do sensor individual, assim como a localização com respeito ao fenômeno.

3. Métricas de desempenho

As principais métricas para avaliar protocolos de redes de sensores são: eficiência de uso da energia e vida útil do sistema, latência, precisão, tolerância a falhas, escalabilidade e exposição dos sensores.

3.1 Eficiência de energia e vida útil do sistema

Como os nós sensores são operados por baterias, os protocolos devem ser eficientes na utilização de energia para maximizar a vida útil do sistema.

A vida útil do sistema pode ser medida por parâmetros genéricos, como o tempo de nós ativos ou tempo de envio de informações à aplicação. Como exemplo destes tempos podemos citar o tempo até que metade dos nós estejam ativos ou o tempo em que a rede pára de suprir a aplicação com a informação desejada sobre o fenômeno.

Considerando o problema de eficiência na utilização da energia, foi criado o protocolo *S-MAC* (*Sensor-Medium Access Control*) [34]. Este protocolo de controle de acesso ao meio para redes de sensores sem fio foi implementado visando redes de sensores com nós individuais que permanecem por longos períodos de tempo inativos. A idéia é que os sensores tornem-se rapidamente ativos quando algum fenômeno é detectado. Este protocolo usa três novas técnicas para reduzir o consumo de energia e suporta auto-configuração. Os nós permanecem inativos periodicamente para reduzir o consumo de energia. Os nós vizinhos formam *clusters* virtuais para auto-

sincronizar em escalonamentos *sleep*. Além disso, o protocolo *S-MAC* programa o rádio para ficar inativo durante transmissões para outros nós. *S-MAC* aplica passagem de mensagens para reduzir a latência de contenção para aplicações de redes de sensores que requerem processamento *store-and-forward* com movimento de dados através da rede.

3.2 Latência e precisão

O observador está interessado em estudar o fenômeno dentro de um dado espaço de tempo (latência). Portanto, a semântica precisa de latência é dependente do fenômeno e da aplicação sobre o fenômeno.

Obter informação de precisão é o objetivo principal do observador, onde a precisão é determinada pela aplicação dada.

Há um compromisso entre precisão, latência e eficiência de energia. A infra-estrutura dada deve ser adaptativa tal que a aplicação obtenha a precisão e retardos desejados com uso mínimo de energia. Por exemplo, a aplicação pode requerer disseminação mais freqüente de dados dos mesmos nós sensores ou pode direcionar a disseminação de dados dos mesmos nós sensores com a mesma freqüência.

3.3 Tolerância a falhas

Os sensores podem falhar devido as más condições físicas ou quando sua bateria acaba. Pode ser difícil a troca dos sensores existentes. A rede deve ser tolerante a falhas. É desejável que falhas não catastróficas sejam transparentes para a aplicação. A tolerância a falhas pode ser alcançada através da replicação de dados. Entretanto, a replicação de dados por si própria requer energia. Há um compromisso entre replicação de dados e eficiência de energia usada.

Como exemplo de replicação de dados podemos citar os protocolos *SPIN* (*Sensor Protocols for Information via Negotiation*) [14]. Eles compreendem uma família de protocolos adaptativos para disseminação de informação em redes de sensores. Os nós que estão executando o protocolo de comunicação *SPIN* nomeiam seus dados usando descritores de dados de alto nível, denominados meta-dados. Eles usam transmissões de meta-dados para eliminar a transmissão de dados redundantes através da rede. Além disso, os nós podem basear suas decisões de comunicação no conhecimento de dados específicos da aplicação e de recursos disponíveis. Isto permite aos sensores distribuir dados, mesmo tendo uma quantidade de energia limitada.

Em [18] são avaliados quatro protocolos *SPIN* específicos: *SPIN-PP* e *SPIN-EC*, que são otimizados para redes ponto-a-ponto e *SPIN-BC* e *SPIN-RL*, que são otimizados para uma rede *broadcast*.

Os resultados encontrados em [18], da comparação dos protocolos *SPIN* com outros possíveis mecanismos, indicam que os protocolos *SPIN* podem enviar 60% mais dados para uma certa quantidade de energia que mecanismos convencionais, em redes ponto-a-ponto e 80% numa rede *broadcast*. Além disso, a taxa de disseminação e de uso de energia dos protocolos *SPIN* ficam próximas do ótimo teórico em ambas as redes.

Os nós em redes de sensores podem falhar por diferentes causas: a bateria pode estar com carga baixa, podem ser acidentalmente ou propositalmente destruídos ou incapacitados. Os sensores tipicamente realizam o roteamento de medidas para a estação base como se fosse uma rede conectada em forma de árvore. A raiz da árvore corresponde à estação base. Assim, a falha de um único nó pode resultar na interrupção da transmissão numa porção da rede (isto é, a estação base pára de receber medidas de um ramo da árvore). Então a rede não consegue completar sua função [28].

Se a interrupção na rede for devido à destruição de um grande conjunto de nós, é difícil para a estação base conseguir alguma informação - falha recuperável ou nós destruídos. No primeiro caso, a rede precisa adotar uma nova topologia de roteamento, contornando a rota em torno de um pequeno conjunto de nós inativos. No segundo caso, a estação base deve emitir um aviso de que a propriedade de funcionamento da rede de sensores não pode mais ser garantida.

Para distinguir entre os dois casos, a estação base precisa de um *trace* de todos os nós inativos. Isto é, para cada nó na rede é necessário determinar se ele está em funcionamento ou não.

Na literatura alguns trabalhos de roteamento em redes de sensores (protocolos *SPINS* [23]) defendem a re-execução do protocolo de descoberta de rota para este propósito. Porém, esta solução requer o envio de mensagens adicionais, o que pode ser muito custoso.

3.3.1 Roteamento em múltiplas rotas

Na tentativa de resolver problemas de falta de confiabilidade de sensores individuais, Ganesan *et al.* propuseram algoritmos de roteamento de redes de sensores sobre múltiplas rotas [11]. Eles consideram a construção de dois tipos de múltiplas rotas para permitir a recuperação de falhas pela rota mais curta entre um nó fonte e um destino.

Baseado no trabalho de [11], Servetto *et al.* [27] estudaram o problema de roteamento na presença de diferentes tipos de dinâmicas: (i) nós que não se movem, mas que alternam entre estados ativos e (ii) nós inativos em tempos aleatórios. Eles estudaram o comportamento dos sensores com energia renovável, tais como células solares ou ambientes vibratórios. O problema de roteamento correspondente foi formalizado como um problema de construção apropriadamente restrito para caminhos aleatórios em

grafos dinâmicos aleatórios. Os caminhos aleatórios devem ser projetados de forma que sua distribuição invariante resultante alcance uma certa propriedade de balanceamento de carga.

Foram propostos algoritmos distribuídos simples para computar os parâmetros locais para os caminhos aleatórios que alcancem o comportamento desejado. Estes algoritmos são capazes de rotear mensagens por todas as rotas possíveis entre um nó fonte e um destino, sem desempenhar computações de descoberta/reparo de rotas explícitas e sem manter o estado da informação explícito sobre rotas disponíveis dos nós.

Scaglione e Servetto [25] realizaram um trabalho sobre roteamento em redes de sensores *multihop*. Eles consideraram um problema de *broadcast* de comunicação numa rede de sensores *multihop* em que instâncias de dados de um campo aleatório são coletadas de cada nó da rede e o objetivo é obter para todos os nós uma estimativa do campo inteiro dentro de um valor de distorção prescrito. A idéia principal do trabalho é juntar a compressão de dados, gerados por diferentes nós, com a informação de viagem sobre os múltiplos *hops* para eliminar a correlação do campo.

3.4 Escalabilidade

A escalabilidade para redes de sensores é também um fator crítico. Para redes de larga escala, é comum que a localização de interações através de hierarquia e agregação são críticas para assegurar a escalabilidade do sistema.

3.5 Exposição dos sensores

As redes de sensores têm o potencial de prover a interface entre o mundo físico e a Internet, atingindo um grande número de usuários. Para este cenário, a qualidade de serviço deve ser expressa em termos de precisão e/ou latência de se observar eventos e o estado global do mundo físico. Conseqüentemente, um dos problemas fundamentais em redes de sensores é a medida da habilidade de detectar objetos com sensores.

A exposição pode ser definida como a medida de quão bem a rede de sensores pode observar um objeto, movendo-se num caminho arbitrário, num determinado período de tempo. Megerian *et al.* [22] desenvolveram um algoritmo para calcular a exposição em redes de sensores, especificamente para encontrar caminhos de exposição mínima. O algoritmo pode ser aplicado para qualquer distribuição e modelos de sensores, sensibilidade, e características da rede.

4. Arquitetura

Uma rede de sensores é uma ferramenta para medir e passar informação sobre o fenômeno para o observador dentro do limite de desempenho desejado e com melhor custo/benefício possível. Para tal, a rede deve ser organizada da seguinte forma: infra-estrutura, protocolo de rede e de aplicação/observador.

A **infra-estrutura** consiste de sensores e da forma como utilizá-los. Mais especificamente, a infra-estrutura é influenciada pelo número de sensores, pelas características deles (precisão de detecção, tamanho de memória, vida útil da bateria, extensão da transmissão) e estratégia de utilização (quantidade, localização e mobilidade do sensor).

O **protocolo de rede** é responsável por criar caminhos e realizar comunicação entre os sensores e o(s) observador(es).

Na **aplicação/observador** o interesse de um observador no fenômeno é expresso através de consultas realizadas a respeito do fenômeno. Para responder as consultas os dados distribuídos que os sensores são capazes de monitorar são aproximados. Estas consultas podem ser estáticas (os sensores são programados para reportar dados de acordo com um padrão específico) ou dinâmicas. A rede pode participar na sintetização da consulta. Por exemplo, filtrando alguns dados dos sensores ou fundindo diversas medidas num valor. As otimizações nestes três níveis são possíveis para melhorar o desempenho .

O protocolo numa rede de sensores é responsável por dar suporte a toda comunicação, entre os próprios nós sensores e entre os nós sensores e os observadores. O desempenho do protocolo pode ser altamente influenciado pelo dinamismo das redes, assim como pelo modelo construído de envio de dados específicos. Para determinar como o protocolo de rede comporta-se para diferentes cenários é importante classificar estas características.

Intuitivamente, para um dado tipo de sensor, aumentar o número de sensores no campo deveria resultar num melhor desempenho na rede, considerando que: (i) a precisão da monitoração deveria aumentar, já que há mais sensores numa posição para relatar sobre o fenômeno; (ii) a disponibilidade de energia dentro da rede aumentaria e (iii) a densidade do sensor adicional ofereceria o potencial para uma rede melhor conectada com caminhos mais eficientes entre os sensores e os observadores.

Entretanto, aumentar o número de sensores resulta num número maior de sensores reportando seus resultados na unidade de tempo. Se o aumento de carga excede a capacidade da rede em termos de acesso ao meio sem fio compartilhado, e gera congestionamento nos nós intermediários, um aumento do número de nós ativos pode afetar o desempenho da rede.

Com relação à capacidade, o problema pode ser visto em termos de colisão e congestionamento. Para evitar colisões, sensores que estiverem na extensão de

transmissão de cada um dos outros sensores, estes não devem transmitir simultaneamente.

Nem todos os sensores são iguais em termos de precisão: dependendo da localização, um sensor específico pode ter uma melhor qualidade de dados ou uma combinação de sensores pode prover uma precisão maior do que outra.

Da perspectiva da rede a precisão depende de fatores como localizações geográficas dos sensores que geram relatórios, tamanho do *buffer* e tempo de processamento de pacotes.

Em relação à perspectiva da aplicação o valor da informação monitorada pelo sensor precisa, também, ser considerada. Se um sensor está fornecendo alguma informação única sobre alguma característica do fenômeno, então a aplicação deve requerer que o sensor reporte independentemente da sua localização.

A aplicação no nível de informação deve ser usada na determinação de que sensores devem gerar relatórios e quando encontrar métricas de desempenho da aplicação.

Em redes de sensores, a infra-estrutura em termos de capacidade de detecção do sensor, número de sensores e estratégia de uso eficiente mostram uma significante influência na determinação do desempenho da rede. Em [32] são estudados os efeitos de infra-estrutura de dois tipos de modelos de envio da rede (fenômeno contínuo e controlado) e diferentes protocolos de rede (*DSR – Dynamic Source Routing, DSDV – Destination Sequenced Distance Vector* e *AODV – Ad Hoc On Demand Distance Vector*). É mostrado o desempenho em termos da eficiência da rede, precisão da aplicação e demandas de latência.

4.1 Compromissos de infra-estrutura para redes de sensores

Em [32] são estudados os efeitos das decisões de infra-estrutura sobre o desempenho de uma rede de sensores. Este trabalho avaliou o efeito da infra-estrutura para diferentes protocolos de rede (*DSR*, *DSDV* e *AODV*) e dois tipos de modelos de envio de dados: fenômeno discreto (a aplicação de monitoração de animais num *habitat*) e contínuo (monitoração de temperatura).

Além disso, foram considerados dois cenários no nível da aplicação: (i) atualização contínua: os sensores periodicamente reportam suas medidas locais ao observador e (ii) orientado pelo fenômeno: sensores reportam suas medidas ao observador periodicamente, mas somente se eles têm dados de interesse para reportar. Neste caso, o fenômeno discreto está dentro da extensão de monitoração. O desempenho é avaliado em termos de eficiência da rede e demanda de precisão e latência da aplicação.

Os experimentos foram realizados da seguinte forma. Primeiro, eles aumentaram sistematicamente a densidade dos sensores, a taxa de relatórios requerida e observaram o desempenho da rede. Quando a carga de sensores oferecida para a rede excedeu a capacidade da rede, o desempenho caiu de acordo com as métricas (precisão, latência entre outros), no nível da aplicação e da rede. O simples acréscimo de mais sensores pode prejudicar muito o desempenho da rede. Isto mostra a necessidade de um gerenciamento inteligente, no nível de infra-estrutura do protocolo da rede de forma a evitar o congestionamento. O protocolo de rede deve balancear a carga oferecida para a rede e a precisão requerida pelo observador.

A tarefa de uma rede de sensores pode ser vista como um processo de comunicação coletiva redundante dos sensores para o observador. É redundante porque múltiplos sensores podem reportar informações correlatas ou informação com um nível de precisão maior do que o requerido pela aplicação. O mecanismo para evitar o congestionamento deve convergir numa taxa de relatórios/disciplina que é suficiente para encontrar os requisitos de desempenho do observador. O protocolo de rede pode acoplar isto reduzindo a taxa de relatórios por sensor, desativando alguns sensores e/ou juntando informações para otimizar a operação de comunicação coletiva.

5. Modelos de comunicação, envio de dados e dinâmicos de redes de sensores

Esta seção apresenta os modelos de comunicação, modelos de envio de dados e modelos dinâmicos existentes para redes de sensores.

5.1 Modelos de comunicação

Há diversas maneiras para uma rede de sensores alcançar seus requisitos de precisão e atraso. Uma rede bem projetada atinge estes requisitos otimizando o uso da energia dos sensores e provendo tolerância a falhas. Estudando os padrões de comunicação, o projetista de uma rede pode ser capaz de escolher a infra-estrutura e os protocolos de comunicação que provêem a melhor combinação de desempenho, robustez, eficiência e menor custo possível.

Conceitualmente, a comunicação numa rede de sensores pode ser classificada em duas categorias: aplicação e infra-estrutura. O protocolo de rede deve suportar estes dois tipos de comunicação.

A comunicação da aplicação relaciona-se à transferência do dado monitorado (ou informação obtida dele) com o objetivo de informar ao observador sobre o fenômeno. Dentro da comunicação da aplicação, há dois modelos: o cooperativo e o não-cooperativo. No modelo de sensor cooperativo os sensores comunicam-se para atender o interesse do observador. Esta comunicação está além da função *relay* (ligação) necessária para fazer o roteamento. Por

exemplo, num protocolo *clustering* um *cluster-head* e os nós sensores comunicam-se para disseminação de informação relacionada ao fenômeno real.

A infra-estrutura de comunicação refere-se à comunicação necessária para configurar, manter e otimizar a operação. Mais especificamente, devido à natureza *ad hoc* das redes de sensores, eles devem ser capazes de descobrir caminhos para outros sensores de interesse para si próprios e para o observador, desconsiderando a mobilidade ou falha do sensor.

A infra-estrutura de comunicação é necessária para manter a rede funcional, assegurando robustez da operação em ambientes dinâmicos, e otimizando o desempenho global.

Além disso, a infra-estrutura de comunicação é altamente influenciada pelos interesses da aplicação, já que a rede deve ser auto-reconfigurável para melhor satisfazê-los. Como a infra-estrutura de comunicação representa o *overhead* do protocolo, é importante minimizar esta comunicação, assegurando que a rede possa suportar a comunicação da aplicação de forma eficiente.

Em redes de sensores é necessária uma fase inicial da infra-estrutura de comunicação para realizar a configuração da rede. Se os sensores são restritos quanto a energia haverá comunicação adicional para reconfiguração. Similarmente, se os sensores são móveis e o observador tem interesse dinâmico, uma comunicação adicional é necessária para descobrir ou reconfigurar caminhos. A infra-estrutura de comunicação é usada para otimizações da rede.

Nas redes de sensores a quantidade de comunicação requerida, também, é altamente influenciada pelo protocolo de rede. A comunicação da aplicação é otimizada pelos relatórios de medidas de taxa mínima que satisfarão às medidas de precisão e retardo dos dados pelas habilidades dos sensores e qualidade dos caminhos entre os sensores e o observador.

A infra-estrutura de comunicação é gerada pelo protocolo de rede em resposta às requisições da aplicação ou eventos na rede. Investir em infra-estrutura de comunicação pode reduzir o tráfego da aplicação e otimizar a operação na rede.

5.2 Modelos de envio de dados

As redes de sensores podem ser classificadas em relação ao envio de dados requeridos pelo interesse da aplicação (observador). Elas podem ser classificadas como: contínua, orientada a evento, iniciada pelo observador e híbrida. Estes modelos governam a geração do tráfego da aplicação e estão descritos a seguir.

No **modelo contínuo** os sensores comunicam seus dados continuamente numa taxa pré-especificada. No **modelo de dados orientado a eventos** os sensores reportam informação somente se um evento de interesse ocorre. Neste caso, o observador está interessado na ocorrência de um fenômeno específico ou conjunto de fenômenos. No **modelo iniciado pelo observador** (ou *request-replay*) os sensores somente reportam seus resultados em resposta a uma requisição explícita do observador (ou diretamente, ou indiretamente através de outros sensores). No **modelo híbrido** as três estratégias co-existem na mesma rede.

O envio de dados, também, pode ser tratado da perspectiva da aplicação ou do fluxo de pacotes de dados reais entre os sensores e o observador. Estas perspectivas não são o foco deste trabalho. Este é um problema do roteamento sujeito ao protocolo de rede.

Nos modelos citados, os roteamentos são classificados como: *flooding* (baseado em *broadcast*), *unicast*, ou *multicast/other* e estão descritos a seguir.

Utilizando uma estratégia de *flooding*, os sensores realizam *broadcast* de sua informação para seus vizinhos, que realizam novo *broadcast* deste dado até alcançar o observador. Esta estratégia pode causar alto *overhead*, mas é imune a mudanças dinâmicas na topologia da rede.

Alternativamente, os sensores podem comunicar-se com o observador diretamente ou com um *cluster-head*, usando uma mensagem *unicast.* Na estratégia *multicast*, sensores formam grupos de acordo com a aplicação e usam *multicast* para comunicação entre membros do grupo. O observador pode comunicar com qualquer membro do grupo para obter o dado desejado. A maior desvantagem do *flooding* ou *broadcast* é a necessidade de um complexo protocolo na camada de rede para roteamento, endereçamento e gerenciamento de localização.

A técnica de agregação de dados pode ser usada para reduzir o *overhead* gerado pelo *broadcast* [14, 17]. Alternativamente, os sensores podem comunicar-se com o observador diretamente (possivelmente utilizando um protocolo de roteamento *multihop*) ou comunicar-se com um *cluster-head* usando *unicast*.

Na estratégia *multicast* os sensores formam grupos orientados pela aplicação e usam *multicast* para a comunicação entre membros do grupo.

O observador pode comunicar com qualquer grupo para obter o dado desejado.

A interação entre o modelo de envio de dados da aplicação e o modelo de roteamento construído pelo protocolo de rede causa um impacto significante no desempenho da rede.

Considere um cenário onde uma rede de sensores é construída para detecção de intrusos. Neste caso, o modelo de envio de dados é orientado a evento, que corresponde à entrada de um intruso na área monitorada. Se o modelo de roteamento no nível da rede é baseado em *flooding*, os sensores que estiverem fisicamente próximos perceberão o intruso ao mesmo tempo e tentarão enviar dados para o observador simultaneamente.

Estas comunicações concorrentes na vizinhança podem gerar contenção no meio de comunicação, aumentando: a probabilidade de perda de informação crítica e a latência em reportar o evento.

5.3 Modelos dinâmicos de rede

Uma rede de sensores forma um caminho entre o fenômeno e o observador. O objetivo do protocolo na rede de sensores é criar e manter este caminho ou múltiplos caminhos sob condições dinâmicas. Além disso, deve encontrar requisições da aplicação de energia e latência baixas, alta precisão e tolerância a falhas. Sem perda de generalidade esta discussão assume um único observador. Múltiplos observadores podem ser suportados com múltiplas instâncias de um único observador. Protocolos mais sofisticados podem, também, apresentar melhor vantagem na presença de múltiplos observadores para convergir para interesses relacionados e/ou comunicação otimizada.

As diferenças entre ativar caminhos para disseminação de informação numa rede de sensores e o problema de roteamento em redes *ad hoc* são: (i) os sensores não são endereçados individualmente, o interesse está no conjunto de sensores que estão numa posição para contribuir para os interesses do observador ativo. Os sensores podem ser endereçados pelos atributos dos sensores (capacidade) e/ou pelo fenômeno (os sensores próximos a um leão na monitoração de *habitat*) e (ii) nós ao longo do caminho podem ter uma função ativa na disseminação e processamento de informação. Neste aspecto, as redes de sensores são semelhantes às redes ativas [30], já as redes *ad hoc* são redes passivas tradicionais.

Há diversas estratégias para construir e manter um caminho entre o observador e o fenômeno, que diferem dependendo das dinâmicas da rede. Estas são classificadas como: redes de sensores estáticas e redes de sensores móveis. A mobilidade, a falha do sensor e a mudança do interesse do observador são fontes de condição dinâmica. As diferenças entre as redes de sensores estáticas e dinâmicas estão descritas a seguir.

5.3.1 Redes de sensores estáticas

Neste tipo de rede não há movimento entre os sensores que estão se comunicando, o observador e o fenômeno. Um exemplo é um grupo de sensores espalhados para monitorar temperatura. Para estes tipos de rede de sensores, estudos anteriores mostraram que algoritmos locais podem ser usados de maneira efetiva [17]. Os sensores nos algoritmos locais se comunicam com os nós na sua localidade. Um nó eleito transmite um resumo de observações locais para o observador, podendo ser implementado através de um ou mais níveis de hierarquia. Estes algoritmos estendem a vida-útil de uma rede de sensores porque apresentam um compromisso para computação local. Neste tipo de rede, os sensores requerem uma configuração de infra-estrutura de comunicação inicial para criar o caminho entre o observador e os sensores com o tráfego restante, exclusivamente para comunicação da aplicação.

5.3.2 Redes de sensores dinâmicas

Em redes de sensores dinâmicas, os sensores por si próprios, o observador e/ou o fenômeno são móveis. Sempre que qualquer dos sensores associados ao caminho corrente do observador para o fenômeno se move, o caminho pode falhar. Neste caso, o observador ou o sensor deve iniciar a construção de um novo caminho. Durante a fase de configuração inicial o observador pode construir múltiplos caminhos entre ele e o fenômeno e colocá-los em *cache*, escolhendo um que seja mais benéfico naquele momento como caminho corrente. Se este caminho falha, um outro caminho que estiver em *cache* pode ser usado. Se todos os caminhos em *cache* são inválidos, então o observador deve construir novos caminhos. A estratégia iniciada pelo observador (*observer-initiated*) é uma estratégia reativa, onde a ação de recuperar o caminho somente é realizada depois de observar um caminho com falha. Outro modelo para reconstruir novos caminhos do observador para o fenômeno é uma estratégia iniciada pelo sensor (*sensor-initiated*).

Num procedimento de recuperação de caminho iniciado pelo sensor, o caminho recuperado é iniciado por um sensor que naquele momento faz parte do caminho lógico entre o observador e o fenômeno, e que está planejando sair daquele caminho. O sensor pode desempenhar algum procedimento para construir um novo caminho realizando *broadcast* de uma requisição de participação para um dado fluxo lógico para todos os sensores vizinhos. Qualquer um deles pode enviar uma mensagem de resposta de participação para o sensor iniciador indicando espontaneamente disponibilidade para participar e tornar-se parte do caminho requisitado. Se nenhum dos sensores vizinhos responder, o sensor pode por *default* enviar uma requisição de invalidação de caminho para o observador. Assim, o observador pode começar a construir o caminho. Este estratégia iniciada pelo sensor é uma estratégia pró-ativa onde operações de recuperação de caminho são iniciadas em antecipação a uma futura falha de caminho.

As redes de sensores dinâmicas podem ser classificadas segundo o movimento dos componentes. Este tipo de movimento é importante do ponto de vista de comunicações. Isto porque o grau e tipo de comunicação são dependentes das dinâmicas na rede.

Para cada um dos componentes (observador, sensor, fenômeno) móveis são necessárias diferentes infra-estruturas, modelos de envio de dados e protocolos. A

seguir descrevemos as situações em que cada um destes componentes encontram-se móveis.

O observador pode ser móvel em relação aos sensores e ao fenômeno. Um exemplo deste paradigma é a utilização de sensores numa área nada hospitaleira para monitoração ambiental. Como exemplo, podemos citar um avião que voa sobre um campo periodicamente para coletar informação de uma rede de sensores. Entretanto, o observador no avião está em movimento em relação aos sensores e ao fenômeno no chão.

No caso de sensores móveis, eles estão se movendo com relação aos demais sensores e ao observador. Por exemplo, considere a monitoração do tráfego implementado para agrupar sensores para táxis. Como os táxis movem-se, os sensores agrupados continuamente comunicam-se uns com os outros sobre suas próprias observações das condições do tráfego. Se os sensores forem cooperativos, o paradigma de comunicação impõe restrições adicionais tais como detecção dos endereços da camada de ligação de seus vizinhos e construção da localização e informação de estruturas de disseminação de informação. Em [17], os autores mostraram que existe *overhead* para se manter um único identificador do sensor num modo hierárquico como num endereço IP (*Internet Protocol*). Além disso, é caro e desnecessário. Ao invés disso, os sensores devem se comunicar somente com seus vizinhos com o endereço MAC da camada de ligação. Nestas redes, o algoritmo pró-ativo, com modificações locais para reparar um caminho, pode ser usado tal que a informação sobre o fenômeno esteja sempre disponível para o observador, preservando, assim, a mobilidade dos sensores individuais.

No caso de um fenômeno móvel o fenômeno se move em relação ao observador ou aos sensores. Um exemplo típico para este paradigma é de sensores utilizados para monitoração de animais. Neste caso a comunicação no nível de infra-estrutura deve ser orientada a eventos. Dependendo da densidade do fenômeno, pode ser ineficiente se todos os nós sensores estiverem ativos o tempo todo. Somente os sensores na vizinhança do fenômeno podem ser determinados pelos objetivos específicos da aplicação, tais como precisão, latência e eficiência de energia.

O efeito da mobilidade em redes de sensores é fundamentalmente diferente do efeito em redes sem fio tradicionais. Em redes *ad hoc* a mobilidade tem sido tratada do ponto de vista da movimentação de um ou mais nós durante a comunicação. A rede de sensores deve adaptar sua operação para continuar a refletir os interesses do observador na presença de mobilidade. A mobilidade dos sensores deve ser tratada de maneira diferente das redes *ad hoc*. Por exemplo, um nó que está se movendo longe do fenômeno pode escolher fazer *hand-off* da responsabilidade de monitoração para um nó vizinho quando aumentar muito a distância.

É possível implementar uma rede de sensores para um fenômeno específico de diferentes maneiras. Considere o problema de monitoração de um tornado. Uma opção seria aviões sobrevoarem para capturar informações sobre o tornado (fenômeno móvel, sensores móveis e contínuo envio de dados). Outra opção seria ter um *grid* de sensores estaticamente colocados no chão e gerar relatórios de dados quando o tornado passar por eles (fenômeno móvel, sensores estáticos e contínuo envio de dados). Uma terceira maneira seria atirar sensores mais finos e leves no tornado (fenômeno estático, sensores móveis e contínuo envio de dados).

6. Análise de protocolos existentes para redes de sensores

Esta seção apresenta uma análise de protocolos existentes para redes de sensores no contexto da taxonomia apresentada por Tilak *et al.* [31].

Os protocolos de roteamento *ad hoc* podem ser usados como protocolos para redes de sensores. Entretanto, estes protocolos, geralmente, não são bons candidatos para redes de sensores pelas seguintes razões: (i) sensores têm baixa carga de bateria e baixa disponibilidade de memória; (ii) o tamanho da tabela de roteamento cresce com o tamanho da rede; (iii) estas redes são projetadas para comunicação fim a fim e reage inapropriadamente havendo movimentação; (iv) suas requisições de endereçamento podem ser inapropriadas para redes de sensores e (v) protocolos de roteamento para redes *ad hoc* não suportam disseminação cooperativa. Mais especificamente, protocolos de roteamento *multihop* suportam a criação e manutenção de caminhos para roteamento de pacotes da fonte para o destino [37]. Como protocolos de roteamento *ad hoc* não suportam agregação ou fusão de dados, eles podem não ter bom desempenho em aplicações de redes de sensores.

De uma perspectiva operacional, é interessante comparar o protocolo de roteamento *ad hoc* e a taxonomia de redes de sensores. Aparentemente, protocolos pró-ativos são mais apropriados para continuar o envio de dados, já que eles mantêm caminhos através da rede. A função de atualização do estado do *link* nestes protocolos pode ser vista como uma forma de continuidade de envio de dados.

Os protocolos reativos parecem ser mais portáteis para disseminação de informação orientada a evento ou baseada em consulta. Os protocolos como LEACH, *DD*, *publisher-subscribe*, estão descritos a seguir.

LEACH é um protocolo eficiente em energia para redes de sensores projetadas com mecanismo de envio de dados contínuo e sem mobilidade [15]. LEACH usa uma arquitetura *clustering* onde os nós membros enviam seus dados para o *cluster-head* local. *Cluster-*

heads agregam dados de cada sensor e envia esta informação para o nó observador. LEACH usa rotação do *cluster-head* para distribuir carga de energia. Uma vez que os *clusters* são formados, os membros do *cluster* usam TDMA para comunicar com o *cluster-head*. Entretanto, LEACH é portátil para redes onde todo nó tem dado para enviar em intervalos regulares. Entretanto, ele precisa ser estendido para modelos orientados a evento bem como para sensores móveis.

Directed Diffusion (*DD*) é um protocolo *data-centric*, onde os nós não são endereçados por seus endereços na rede, mas sim pelos dados que monitoram [17]. Os dados são nomeados por pares de atributo-valor. No *Directed Diffusion* o interesse é expresso pelos nós observadores em termos de uma consulta que se difunde pela rede usando interações locais. Uma vez que um nó sensor que satisfaz a consulta (nó fonte) é alcançado, aquele nó começa a transmitir dados para o nó sumidouro, novamente usando interações locais. A ausência de noção de um identificador global (por exemplo, um endereço IP) torna a difusão orientada eficiente para redes com mobilidade. O protocolo *DD* é aplicável para redes orientadas a eventos e orientadas a consulta. As interações localizadas permitem ao protocolo ser escalável para redes grandes. O protocolo *DD* escala como uma função do número de interesses ativos presentes na rede.

O modelo *publish/subscribe* foi proposto para redes móveis por Huang e Garcia-Molina [12]. Neste modelo a comunicação é tipicamente anônima, inerentemente assíncrona e *multicast* por natureza. Do ponto de vista da aplicação, o modelo *publish/subscribe* captura o relacionamento entre o observador e o fenômeno para algumas aplicações. Neste modelo a comunicação não é fim a fim, mas anônima com formação de grupo *multicast* específico da aplicação. Em relação à implementação, a comunicação assíncrona ajuda a preservar energia e aumentar a vida útil da rede.

Ratnasamy *et al.* [24] apresentam uma classificação alternativa de redes de sensores baseada no modelo de disseminação de dados. Eles propõem que a disseminação de dados possa ser feita no mínimo de três formas: armazenamento **externo**, onde passa todos os dados para o observador e o deixa processar esta informação; armazenamento **local**, onde a informação sobre o evento é armazenada localmente pelos sensores e armazenamento **orientado a dados**, onde os dados são armazenados pelo nome e consultas são direcionadas pelo nome para o sensor correspondente. A escolha do modelo influencia os padrões de comunicação dentro da rede.

7. Segurança em redes de sensores

Para que uma rede de sensores forneça dados com segurança é necessário que os requisitos a seguir sejam cumpridos.

Confidencialidade dos dados: uma rede de sensores não deve deixar que informações sejam transmitidas para redes vizinhas. Em muitas aplicações os nós comunicam os dados obtidos com muita freqüência. A estratégia padrão para manter os dados secretos é criptografar os dados com uma chave secreta que somente o receptor possua, garantindo confidencialidade.

Autenticação de dados: autenticação de mensagens é importante para muitas aplicações em redes de sensores, principalmente para funções administrativas, como por exemplo, reprogramação de rede. O receptor precisa assegurar que os dados usados em qualquer processo de decisão se originam de fonte correta.

No caso de comunicação em duas partes, a autenticação dos dados pode ser alcançada através de um mecanismo simétrico, onde o emissor e o receptor compartilham uma chave secreta para computar um código de autenticação de mensagem (*MAC-Message Authentication Code*) de todo dado comunicado. Quando uma mensagem com um código de autenticação de mensagem correto chega ao receptor, ele conhece o emissor que enviou a mensagem. Este estilo de autenticação não é seguro para ser aplicado com *broadcast* [23].

Integridade de dados: em comunicação, integridade de dados assegura ao receptor que o dado recebido não foi alterado durante seu trânsito. Em [23], a integridade de dados é alcançada pela autenticação dos dados.

Dados recentes: Garantir que os dados são recentes implica em assegurar que não houve interferência de mensagens antigas. Isto pode ser garantido através da ordenação parcial das mensagens, mas sem acarretar atraso da informação (utilizado para medida de sensores) ou pela ordem total de um par requisição-resposta, que permite estimar o atraso (utilizado para sincronização de tempo dentro da rede).

Para atender às condições de segurança para redes de sensores, Perrig *et al.* [23] apresentam um conjunto de protocolos de segurança para redes de sensores - *SPINS* (*Security Protocols for Sensor Networks*). Os protocolos *SPINS* têm dois blocos construídos: *SNEP* (*Secure Network Encryption Protocol*) e *µTESLA* (a versão micro do *Timed, Efficient, Streaming, Loss-tolerant Authentication Protocol*). O protocolo *SNEP* provê confidencialidade dos dados, autenticação dos dados em dois grupos e dados atuais. Um problema particularmente difícil é prover autenticação de *broadcast* eficiente, que é um mecanismo importante para redes de sensores. *µTESLA* é um novo protocolo que provê *broadcast* autenticado para diversos ambientes de recursos restritos. Os autores implementaram estes protocolos e mostraram que eles funcionam mesmo para uma rede de hardware mínimo. Porém, podem ser usados para construir protocolos de um nível mais elevado.

As pesquisas sobre redes de sensores geralmente assumem um ambiente real. Porém, em muitas aplicações de redes de sensores, a rede pode estar numa situação onde um intruso pode ser motivado a alterar a função da rede. Um intruso pode ser capaz de posicionar diversos nós dentro da rede e usá-los para transmitir falsas mensagens, ou até mesmo comprometer o funcionamento de um nó da rede e conseguir acesso as suas principais informações. Em [16] é tratado o caso onde um intruso deseja corromper a informação que está sendo produzida pela rede de sensores. É apresentado um protocolo que provê um mecanismo de agregação segura para redes de sensores, dentro dos limites de consumo de energia e memória.

A agregação de mensagem pode reduzir significantemente o *overhead* de comunicação, mas dificulta a segurança. Cada nó intermediário pode modificar, forjar ou descartar mensagens, ou simplesmente transmitir valores de agregação falsos. Dessa forma, um nó comprometido pode ser capaz de significantemente alterar o valor final da agregação.

Não se pode criptografar mensagens com uma única chave compartilhada entre cada dispositivo e a estação base, já que cada nó intermediário precisa entender as mensagens recebidas para realizar a agregação. Além disso, não se pode armazenar a mesma chave em todo dispositivo para permitir criptografar ou fazer autenticação, já que um intruso que descobrir a chave de um dispositivo poderá controlar a rede inteira. Por isso, foi desenvolvido um protocolo com mecanismos para detectar nós com comportamento errado (modificando ou forjando mensagens, transmitindo valores agregados falsos). Com este mecanismo, uma estação base é capaz de garantir que os dados transmitidos sejam corretos, mesmo com nós falsos introduzidos ou que ele descubra as informações importantes de um único nó. No trabalho de [16] foram implementadas duas idéias: agregação e autenticação atrasadas. Ao invés da agregação das mensagens ser realizada na próxima rota, as mensagens são passadas para a rota seguinte, sem alterações, onde são agregadas. Isto aumenta o custo da transmissão mas garante integridade para redes onde dois nós consecutivos não estão comprometidos. As mensagens são autenticadas com um atraso, mas isto permite que as chaves sejam simétricas e reveladas para o autenticador depois que o tempo de atraso tenha expirado. Estas estratégias aumentam a confidencialidade na integridade de leituras de sensores sem perder a oportunidade de agregar resultados intermediários na rede.

8. Projetos relacionados a redes de sensores

Esta seção apresenta alguns projetos relacionados a redes de sensores, citados no *site* da Universidade de Virgínia [29], além de citar alguns projetos que estão em desenvolvimento em diferentes universidades ou centros de pesquisa: Programming the Swarm, University of Virginia [10]; Amorphous Computing, MIT [1]; TinyOS, UC Berkeley [4]; SCADDS: Scalable Coordination Architectures for Deeply Distributed Systems, Information Science Institute [8, 9]; CoSense: Collaborative Sensemaking of Distributed Sensor Data for Target Recognition an Condition Monitoring, Xerox Parc [33]; Sensor Webs, UC Berkeley; Dynamic Declarative Networks, MIT Lincoln Laboratory; Self-Organizing Sensor Networks, Auburn University [19]; Active Sensor Networks, Columbia University; Cougar: Flexible Decision Support in Device-Saturated Environments, Cornell University [5]; Multi-resolution Data Fusion, Duke University; Distributed Services for Microsensor Networks, Rockwell Center; Webdust, Rutgers University; Reactive Sensor Networks, Pennsylvania State University [3]; Sensor Networks for Network-centric Warfare, Planning Systems Incorporated Engineering Center [35]; Wireless Networks of Biomedical Sensors; Wayne State University Detroit [7]; Scalable Real-Time Negotiation Toolkit, University of Massachusetts at Amherst e Wireless Sensor Networks for Habitat Monitoring, Intel Research Laboratory, Berkeley Intel Corporation, University of California at Berkeley e College of the Atlantic Bar Harbor. Nas seções seguintes são detalhados alguns destes projetos e apresentados os projetos em andamento.

8.1 Programming the Swarm

Programming the Swarm é um projeto que enfoca o desenvolvimento de métodos para criar, entender e validar propriedades de programas que executam sobre uma agregação (*swarms*) de dispositivos que realizam computação. Uma forma seria construir programas combinando primitivas. O comportamento funcional e não funcional de uma primitiva é descrito usando notações formais. Neste projeto, estão sendo investigadas técnicas baseadas em métodos experimentais e analíticos para previsão de propriedades funcionais e não funcionais de composições de primitivas de agregação [10].

8.2 SCADDS

SCADDS (*Scalable Coordination Architectures for Deeply Distributed Systems*) [8] é um projeto de pesquisa, desenvolvido pela *University of Southern California no Information Sciences Institute,* que explora arquiteturas de coordenação escalável para sistemas distribuídos e dinâmicos como as redes de sensores sem fio.

Os nós nestes sistemas são heterogêneos, tendo uma variação de sensibilidade, atuação e capacidade de comunicação. Muitos sistemas distribuídos requerem

nós que são pequenos, de baixa energia, móveis e sem fio. Em tais sistemas, os nós perdem sua individualidade. Ao invés disso, os dados gerados por estes dispositivos devem ser o foco de toda a comunicação, independente de que nó coletou o dado originalmente e que nós atualmente o armazenam. Este trabalho enfoca os seguintes tópicos de pesquisa: *directed diffusion*, fidelidade adaptativa, localização, sincronização de tempo, *Sensor-MAC*(*S-MAC* [36]) e *Radio Communication Stack on Motes* [8].

8.2.1 Algoritmos de Fidelidade Adaptativa

O projeto SCADDS explora algoritmos de fidelidade adaptativa, onde a qualidade (fidelidade) de resposta pode estar relacionada à vida útil da bateria, largura de banda ou número de sensores ativos. A fidelidade resultante deve estar dentro de limites aceitáveis.

A fidelidade adaptativa é aplicada ao roteamento em redes com energia limitada, *ad hoc* e sem fio. Nós que estiverem executando os algoritmos de fidelidade adaptativa possuem um compromisso entre dissipar energia e a qualidade de envio de dados de acordo com as requisições da aplicação. Estes algoritmos trabalham sobre protocolos de roteamento sob demanda existentes sem modificá-los. Um dos algoritmos é para desligar o rádio para reduzir o consumo de energia com o envolvimento da informação no nível da aplicação e o uso adicional de ajuste de densidade dos nós para adaptativamente ajustar a fidelidade de roteamento a fim de estender a vida útil da rede.

8.2.2 Sincronização de Tempo

A sincronização de tempo é uma parte crítica da infra-estrutura de qualquer sistema distribuído. As redes de sensores sem fio distribuídas fazem um uso extensivo de tempo sincronizado. Porém, freqüentemente têm requisitos únicos no escopo, vida útil e precisão da sincronização alcançada, bem como do tempo e energia requerida para alcançá-lo. Os métodos de sincronização de tempo existentes precisam ser estendidos para encontrar estas novas necessidades. Em [6] é apresentada uma implementação do esquema de sincronização de tempo em redes de sensores, denominado sincronização *post-facto*. Este método combina a disciplina do oscilador de freqüência, provido pelo *NTP* (Ne*twork Time Protocol*), com uma correção de fase instantânea, provida por um sinal de sincronização simples enviado por um *beacon*[1].

8.3 CoSense

Num ambiente de energia limitada e de alvos de difícil observação, *arrays* de sensores distribuídos é uma maneira atrativa para detectar, trilhar e identificar alvos. Alcançar uma estratégia tática usando sistemas descentralizados requer mover-se além do processamento de sinais tradicionais para a identificação de estruturas dentro de coleções de fluxos de sinais distribuídos temporariamente no espaço. O desafio técnico crítico é agregar, representar e manter a informação no nível da estrutura, vinda dos dados dos sensores numa rede com limitação de recursos, dinâmica e irregular. O objetivo principal deste projeto [33] é habilitar aplicações, tal como conhecimento tático, desenvolvendo abordagens de interpretação de dados novos em harmonia com técnicas baseadas em modelos e estatísticas. As idéias novas são: identificar eventos de baixa observação pela análise de sinal colaborativo multinível; focos de sensores múltiplos orientados através do gerenciamento de hipóteses do alvo distribuído e detecção rápida em ambientes com limitação de energia aliado a análise de nível estrutural e de sinalização.

8.4 COUGAR

O projeto Cougar [5] investiga um novo mecanismo de banco de dados distribuído para unir os requisitos de escalabilidade e de flexibilidade em mineração e monitoração do mundo físico. No projeto está sendo construída uma infra-estrutura de gerenciamento de dados distribuída, que escala com o grau de interconectividade e poder computacional existente.

Cougar é uma plataforma para testar técnicas de processamento de consultas sobre redes de sensores *ad-hoc*. Ele possui três camadas: a *QueryProxy*, um pequeno componente de banco de dados que executa sobre nós sensores para interpretar e executar consultas e um componente *front-end*. O *front-end* é um *QueryProxy* mais poderoso, que permite conexões para fora da rede de sensores e possui uma interface gráfica para o usuário, onde estes podem realizar consultas na rede de sensores. O componente de processamento de consultas trata as consultas para os dispositivos distribuídos num gerenciador inteligente.

8.4.1 Arquitetura do sistema

O *QueryProxy* consiste de três partes: o gerenciador do dispositivo, a camada do nó e a camada do líder. Os nós sensores são capazes de atuar como líderes ou nós normais de processamento de sinal/consulta. Quando a rede é configurada são formados grupos e eleitos líderes dos nós nos grupos. O sistema *QueryProxy* tem uma estrutura hierárquica, com o *front-end* comunicando com os nós que atuam como líderes do grupo, e com líderes do grupo comunicando-se com o *front-end* e com os outros nós sensores em seus grupos. A camada do nó gerencia a execução das consultas no nó sensor e interage com os sensores via o gerenciador

[1] Sinal de rádio de alta freqüência.

de dispositivos. Este código está ativo sobre todos os nós. Num membro do *cluster*, quando uma consulta está para ser processada, a primeira camada do nó requisita as tuplas pedidas do gerenciador de dispositivo. Então, a consulta é processada usando as tuplas e os resultados enviados ao líder do grupo. O líder do grupo tem uma camada de processamento de líder ativa, além da camada do nó, que recebe tuplas de outros membros do grupo. As tuplas recebidas são enviadas a cada consulta que ele recebeu do *front-end* que precisa delas. A camada do líder, então, processa as consultas, usando as tuplas recebidas e envia as respostas ao *front-end* que iniciou a consulta. Quando conveniente as tuplas são agregadas antes de serem enviadas.

O *front-end* informa as consultas que ele recebeu da *GUI* (*Graphic User Interface*) para o software *QueryProxy* que está sendo executado sobre os sensores. Ele mantém, também, o caminho das consultas que estão sendo executadas atualmente nas *GUI's* executando sobre o sistema e recebe mensagens dos nós que são líderes de grupo.

O líder envia cada tupla para as consultas requeridas. Em seguida, realiza algum processamento das tuplas e envia uma resposta à *GUI* que iniciou a consulta. O *front-end* pode também receber comandos da *GUI* instruindo-a a começar ou parar consultas. O *front-end* pode, também, ser tuplas de saída para um banco de dados *MySQL* sendo executado no mesmo dispositivo.

8.5 Self Organizing Sensor Networks

As redes de sensores auto-organizáveis [19] podem ser construídas a partir de nós sensores que possuem a capacidade de espontaneamente criar redes, montar a rede por si próprios, dinamicamente adaptar a falha de dispositivos e degradação, gerenciar movimentos de nós sensores e reagir ao desafio em tarefas e requisições da rede. Nós sensores auto-organizáveis permitem que dispositivos sensores sejam auto-suficientes, auto-reconfiguráveis e autônomos.

Os principais benefícios destas características são: (i) suporte a aplicações táticas e de vigilância usando nós de redes de sensores reconfiguráveis que são capazes de formar redes, sendo realizadas de forma incremental e montadas automaticamente sem administração central; (ii) provê capacidades para redes de sensores se adaptarem dinamicamente a falhas e degradação de dispositivos e mudarem requisições em tarefas e na rede e (iii) integra vários serviços de rede específicos da aplicação e serviços do sistema provido por tipos mistos de nós sensores e aplicações de defesa.

8.5.1 Reactive Sensor Networks (RSN)

O objetivo do projeto de redes de sensores reativos (*RSN*) [3] é construir um sistema para agregação e um processamento ágil de informação de sensores em redes de sensores distribuídos. A necessidade de dados, a disponibilidade e o tráfego de rede são características conhecidas.

Os sensores, as redes de sensores e os *links* estão sujeitos a falhas desconhecidas e degradação de serviço. O uso de um repositório de código móvel e técnicas de otimização de recursos limitados permite à rede adaptar-se ao ambiente caótico.

Os processos são alocados a recursos baseados em sua utilização de recursos corrente. O sistema faz estas escolhas usando as informações disponíveis e considerando somente o futuro imediato.

A maior parte do projeto deriva e implementa novos métodos para agregação de dados. De muitas maneiras este é um tipo de problema *anycast*, o problema de *multicasting dual*. Além disso, o problema implementa métodos de multi-resolução que resolvem este problema usando código móvel.

8.6 Wireless Networks of Biomedical Sensors

As redes de sensores biomédicos sem fio na medicina, compostas de sensores inteligentes, que são criados para combinar materiais sensíveis com circuitos integrados, têm sido considerados por diversas aplicações biomédicas, como um monitor de nível de glicose ou uma prótese de retina.

Estes dispositivos possuem a capacidade de se comunicar com um computador externo (estação base) via uma interface sem fio [26].

A energia limitada e as capacidades computacionais de um sensor inteligente baseado em implantes biológicos apresentam desafios em diversos aspectos de redes sem fios. Isto se deve à necessidade de obter uma bio-compatibilidade, tolerância a falhas, eficiência no uso da energia e projeto escalável. Entretanto, sensores embutidos em seres humanos necessitam de requesitos adicionais. Por exemplo, as soluções de redes de sensores sem fio devem ser muito seguras e confiáveis, funcionar sem problemas, em diferentes localizações geográficas e requerer manutenção mínima. Estas necessidades de soluções específicas da aplicação são vastamente diferentes de soluções tradicionais.

Em [26], os autores descrevem o potencial de sensores inteligentes para a biomedicina. Eles explicam os desafios para o funcionamento de redes sem fio de *arrays* de sensores inteligentes embutidos em seres humanos e a estratégia preliminar para uma rede sem fio de uma prótese de retina. O objetivo é motivar pesquisas nesta área ilustrando a necessidade de mais estratégias novas e específicas da aplicação, afim de

desenvolver soluções de redes sem fio para sensores inteligentes implantados em seres humanos.

8.7 Wireless Sensor Networks for Habitat Monitoring

Mainwaring *et al.* [21] apresentam um estudo da aplicação de redes de sensores para a monitoração de *habitat* do mundo real. A aplicação apresenta uma coleção de requerimentos, restrições e linhas de direcionamento que servem como uma base para uma arquitetura de redes de sensores geral para muitas aplicações semelhantes. Ela descreve o hardware e plataformas de sensores, redes distintas envolvidas, sua interconexão e facilidades de gerenciamento de dados. O projeto e implementação de redes essenciais, incluem o gerenciamento de energia, comunicações, re-execução de tarefas e gerenciamento de nós. É apresentada uma instância da arquitetura para monitoração do comportamento de pássaros marinhos. A rede consiste de 32 nós numa pequena ilha da costa de Maine, com dados ao vivo na *Web*.

9. Considerações finais

As redes de sensores formam um campo que está sendo muito pesquisado atualmente.

Utilizando redes de sensores é possível monitorar ambientes de difícil acesso, como campos de batalha, regiões do oceano, florestas. Além disso, podem ser utilizados na área biomédica, na monitoração de tráfego, enfim, pode ser utilizada pelos mais diversos campos de atividades.

Os sensores podem ser móveis ou imóveis, sendo que no segundo caso as redes apresentam características de redes móveis *ad hoc*. Portanto, em redes de sensores, problemas como segurança e tolerância a falhas devem ser observados. Para resolver, ou pelo menos amenizar estes problemas, uma fonte de pesquisa são os protocolos de comunicação que prevêem falhas e tentam evitá-las. Além disso, existem protocolos que tentam evitar que inimigos coloquem informações incorretas na rede de sensores.

Uma rede de sensores pode ser vista como um caso especial de redes móveis, onde os nós têm baixa capacidade de energia e disponibilidade de memória. Porém, os protocolos de roteamento utilizados para redes *ad hoc* não são apropriados para redes de sensores, porque podem gerar tabelas de roteamento muito grandes. Elas exigem uma capacidade de memória que não existe em um sensor, não suportam agregação ou fusão de dados, nem a criação e manutenção de rotas. Os protocolos precisam ser adaptados.

As redes de sensores auto-organizáveis propõem uma outra forma de funcionamento de uma rede composta de sensores, pois os sensores por si próprios formam a rede. Este tipo de rede deve ser capaz de se adaptar para problemas como falhas de dispositivos. Além disso, devem gerenciar os movimentos dos nós sensores e atender a consultas na rede.

O desafio físico encontra-se em se ter um sensor com capacidade de armazenamento de tamanho razoável e que a rede funcione sem falhas, fornecendo informações atuais e corretas do fenômeno observado.

Desta forma, podemos dizer que as redes de sensores possuem características próprias relevantes que devem ser cuidadosamente observadas. Isto para que sejam propostos novos protocolos de comunicação, de gerenciamento de tolerância a falhas, entre outros pontos, para tornar mais concreto e viável a utilização destas redes.

Referências

[1] H. Albelson, D. Allen, D. Coore, C. Hanson, E. Rauch, G.J. Sussman e R. Weiss, ”Amorphous Computing”, Communications of the ACM, 2000, disponível em (2003) http://www.swiss.ai.mit.edu/projects/amorphous/cacm2000.html.

[2]Bluetooth special interest group, disponível em (2003) http://www.bluetooth.com.

[3] R.R. Brooks, “Reactive sensor networks”, Applied Research Laboratory, Pennsylvania State University, disponível em (2003) http://strange.arl.psu.edu/RSN.

[4] D. Culler, J. Hill, N. Lee, P. Levis, S. Madden, J. Polastre, R. Szewczyk, K. Whitehouse e A. Woo, “TinyOS Project”, University Berkeley, disponível em (2003) http://webs.cs.berkeley.edu/tos.

[5] A. Demers, J. Gehrke, J. Shanmungasundaram, M. Calimlim, M. Riedewald e N. Trigoni, Cournel Database Group, disponível em (2003) http://www.cs.cornell.edu/database/cougar/index.htm.

[6] J. Elson e D. Estrin, “Time Synchronization for Wireless Sensor Networks”, University of California, Los Angeles; and USC/Information Sciences Institute, disponível em (2003) http://www.circlemud.org/~Ejelson/writings/timesync.

[7] D. Estrin, R. Govindan, J. Heidemann e S. Kumar, “Next century challenges: scalable coordination in sensor networks”, In Proceedings of the Fifth Annual ACM/IEEE International Conference on Mobile Computing and Networking, Seattle, Washington, USA, ACM Press, ISBN 1-58113-142-9, 1999, pp 263-270, disponível em (2003) http://doi.acm.org/10.1145/313451.313556.

[8] D. Estrin, R. Govindan, J. Heidemann, “SCADDS: Scalable Coordination Architectures for Deeply Distributed Systems”, Information Sciences Institute, University of Southern California, disponível em (2003) http://www.isi.edu/div7/scadds.

[9] D. Estrin, R. Govindan, J. Heidemann, “Wireless Sensor Network Testbed @ USC/ISI”, Information Sciences Institute, University of Southern California, disponível em (2003) http://www.isi.edu/scadds/pc104testbed.

[10] D. Evans, “Programming the Swarm”, Department of Computer Science, University of Virginia, disponível em (2003) http://swarm.cs.virginia.edu.

[11] D. Ganesan, R. Govindan, S. Shenker e D. Estrin, “High-resilient, energy-efficient multipath routing in wireless

sensor networks, ACM Mobile Computing and Communications Review, vol. 5, pp 11-29, 2001.
[12] H. Garcia-Molina e Y. Huang, "Publish/Subscribe in a mobile environment", In International Workshop on Data Engineering for Wireless and Mobile Access, 2001, pp 27-34.
[13] J. Heidemann, F. Silva, C. Intanagonwiwat, R. Govindan, D. Estrin e D. Ganesan, "Building efficient wireless sensor networks with low-level naming", In Proceedings of the Eighteenth ACM Symposium on Operating Systems Principles}, Banff, Alberta, Canada, ACM Press, 2001, pp 146-159.
[14] W.R. Heinzelman , J. Kulik e H. Balakrishnan, "Adaptive protocols for information dissemination in wireless sensor networks", In Proceedings of the Fifth Annual ACM/IEEE International Conference on Mobile Computing and Networking, ACM Press, 1999, pp 174-185.
[15] W. Heinzelman, "Application-specific protocol architectures for wireless networks", Ph.D. Thesis, Massachusetts Institute of Technology, 2000.
[16] L. Hu e D. Evans, "Secure aggregation for wireless networks", In Workshop on Security and Assurance in Ad hoc Networks, January 2003, disponível em http://www.cs.virginia.edu/~evans/pubs/wsaan-abstract.html.
[17] C. Intanagonwiwat, R. Govindan e D. Estrin, "Directed Diffusion: a scalable and robust communication paradigm for sensor networks", In Proceedings of the Fourth International Conference on Mobile Computing and Networking, ACM Press, 2000.
[18] J. Kulik, W. R. Heinzelman e H. Balakrishnan, "Negotiation-based protocols for disseminating information in wireless sensor networks, In Proceedings of the Fifth Annual ACM/IEEE International Conference on Mobile Computing and Networking, Kluwer Academic Publishers, vol. 8, 2002, pp 169-185.
[19] A. Lim, "Self-configurable sensor networks", Computer Science and Engineering, Auburn University, disponível em (2003) http://www.eng.auburn.edu/users/lim/sensit.html.
[20] R. Malladi e D. P. Agrawal, "Current and future applications of mobile and wireless networks", Communications of the ACM, ACM Press, ISSN 0001-0782,vol. 45, no. 10, pp 144-146, 2002, disponível em (2003) http://doi.acm.org/10.1145/570907.570947.
[21] A. Mainwaring, D. Cullerand, J. Polastre, R. Szewczyk e J. Anderson, "Wireless sensor networks for habitat monitoring", In Proceedings of the First ACM International Workshop on Wireless Sensor Networks and Applications, ACM Press, 2002, pp 88-97.
[22] S. Megerian, F. Koushanfar, G. Qu, G. Veltri e M. Potkonjak, "Exposure in wireless sensor networks: theory and practical solutions", Wireless Networks, Kluwer Academic Publishers, ISSN 1022-0038, vol. 8, no. 5, 2002, pp 443-454.
[23] A. Perrig, R. Szewczyk, V. Wen, D. Culler e J. D. Tygar, "SPINS: security protocols for sensor networks", In Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking, Rome, Italy, ACM Press, 2001, pp 189-199.
[24] S. Ratnasamy, D. Estrin, R. Govidan, B. Karp, S. Shenker, L. Yin e F. Yu, "Data-centric storage in sensornets", In Submitted for review to SIGCOMM'02, Febrary 2002.
[25] A. Scaglione e S.D. Servetto, "On the interdependence of routing and data compression in multihop sensor networks, In Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking, Atlanta, Georgia, USA, ACM Press, 2002, pp 140-147.
[26] L. Schwiebert, S.K.S. Gupta e J. Weinmann, "Research challenges in wireless networks of biomedical sensors", In Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking, ACM Press, 2001, pp 151-165.
[27] S.D. Servetto e G. Barrenechea, "Constrained random walks on random graphs: routing algorithms for large scale wireless sensor networks", In Proceedings of the First ACM International Workshop on Wireless Sensor Networks and Applications, Atlanta, Georgia, USA, ACM Press, ISBN 1-58113-589-0, pp 12-21, 2002, disponível em (2003) http://doi.acm.org/10.1145/570738.570741.
[28] J. Staddon, D. Balfanz e G. Durfee, "Efficient tracing of failed nodes in sensor networks", In Proceedings of the First ACM International Workshop on Wireless Sensor Networks and Applications, Atlanta, Georgia, USA, ACM Press, 2002, pp 122-130.
[29] J. A. Stankovic, "A network virtual machine for real time-coordination", The Real-Time Computing Laboratory, University of Virginia, disponível em (2002) http://www.cs.virginia.edu/nest.
[30] D. Tennenhouse, J. Smith, W. Sincoskie, D. Wetherall e G. Minden,"A survey of active network research", IEEE Communications Magazine, vol. 35, no. 1, pp 80-86, January 1997.
[31] S. Tilak, N.B. Abu-Ghazaleh e W. Heinzelman, "A taxonomy of wireless micro-sensor network models", In Proceedings of the ACM Workshop on Wireless Security, ACM Press, 2002, pp 28-36.
[32] S. Tilak, N.B. Abu-Ghazaleh e W. Heinzelman, "Infrastructure tradeoffs for sensor networks", In Proceedings of the First ACM International Workshop on Wireless Sensor Networks and Applications, Atlanta, Georgia, USA, ACM Press, ISBN 1-58113-589-0, pp 49-58, 2002, disponível em http://doi.acm.org/10.1145/570738.570746.
[33] F. Zhao, P. Cheung, L. Guibas, J. Liu, J.J. Liu e J. Reich, "CoSense: collaborative sensemaking of distributed sensor data for target recognition and condition monitoring", Palo Alto Research Center, disponível em (2003) http://www2.parc.com/spl/projects/cosense.
[34] W. Ye, J. Heidemann e D. Estrin, "An energy-efficient MAC protocol for wireless sensor networks", In Proceedings of the 21st International Annual Joint Conference of the IEEE Computer and Communications Societies, September 2001, disponível em (2003) http://www.isi.edu/scadds/projects/smac.
[35] J. Walrod, "Sensor networks for network-centric warfare", Planning Systems Incorporated Engineering Center, Long Beach, MS, USA, disponível em (2003) http://www.plansys.com/Content/NavigationMenu/Products/Sensor_Network_and_Data_Acquisition_Products_White_Papers/Default507.htm .
[36] W. Ye, J. Heidemann e D. Estrin, "Medium access control with coordinated, adaptive sleeping for wireless sensor networks", University of Southern California, Technical Report, no. ISI-TR-567, January 2003, disponível em http://www.isi.edu/scadds/publications.html.
[37] Y. Xu, J. Heidemann e D. Estrin, "Adaptive energy-conserving routing for multihop ad hoc networks", Research Report 527, USC/Information Sciences Institute, October 2000.