UFMG - ICEx
DEPARTAMENTO DE CIÊNCIA DA COMPUTAÇÃO

UFMG
UNIVERSIDADE FEDERAL DE MINAS GERAIS

UMA TAXONOMIA PARA PROTOCOLOS DE CONTROLE DE ACESSO AO MEIO EM REDES DE SENSORES SEM FIO

RT.DCC.005/2005

LUIZ H. A. CORREIA
DANIEL F. MACEDO
ALDRI L. DOS SANTOS
JOSÉ M. S. NOGUEIRA
ANTONIO A. F. LOUREIRO

ABRIL
2005

Uma Taxonomia para Protocolos de Controle de Acesso ao Meio em Redes de Sensores Sem Fio *

Luiz H. A. Correia[1,2], Daniel F. Macedo[1], Aldri L. dos Santos[1],
José M. Nogueira[1], Antonio A. F. Loureiro[1].

[1]Dept. de Ciência da Computação
Universidade Federal de Minas Gerais
Belo Horizonte-MG, Brasil

[2]Dept. de Ciência da Computação
Universidade Federal de Lavras
Lavras-MG, Brasil

{lcorreia,damacedo,aldri,loureiro,jmarcos}@dcc.ufmg.br

Resumo

Diversos protocolos de controle de acesso ao meio (MAC) para redes de sensores sem fio têm sido recentemente propostos na literatura. A maioria das implementações levam em conta a especificidade das aplicações em redes de sensores sem fio (RSSF), sendo as abordagens e os mecanismos desenvolvidos nesses protocolos são diferentes para cada aplicação. É proposta uma taxonomia para classificar os protocolos MAC em RSSF, baseado em atributos comuns dessas redes e nas características diferenciadas da aplicação, como capacidade de adaptação e qualidade de serviço. Uma visão dos principais transceptores em RSSF é apresentada, mostrando o impacto dos eventos de comunicação no consumo de energia. A taxonomia proposta considera decisões de projeto tipicamente utilizadas por protocolos MAC, tendo como objetivo nortear o desenvolvimento de novos protocolos. Baseado nessa taxonomia, classificamos os principais protocolos existentes. Por fim, são discutidas questões sobre segurança e os desafios nos protocolos MAC.

1 Introdução

As Redes de Sensores Sem Fio (RSSF) são compostas de centenas ou milhares de nós sensores utilizados para monitorar eventos em uma determinada área. Os nós sensores, ou elementos de rede, possuem processador, memória, transceptor, um ou mais sensores e bateria, estabelecendo um sistema autônomo. Outro componente do nó sensor é o software executado em seu processador, ou seja, o componente lógico do nó [Loureiro et al., 2003]. A interligação desses sistemas autônomos estabelece uma rede de sensores sem

Nas RSSF a comunicação entre os nós sensores é realizada de maneira ad hoc, sendo estabelecida diretamente entre os nós origem e destino (*single hop*), ou indiretamente através de nós intermediários por uma comunicação multi-saltos (*multihop*). Os dados coletados pelos nós sensores são encaminhados para um ponto de acesso, também conhecido como estação base, nó sorvedouro (*sink*) ou *gateway*. O ponto de acesso (PA) é o elemento de rede que interliga uma RSSF com um ou mais observadores. O observador é uma entidade da rede ou usuário final que deseja obter informações sobre os dados coletados pelos nós sensores [Meguerdichian et al., 2001, Ruiz et al., 2003]. A comunicação entre os nós é feita por transceptores, que utilizam sinais de rádio freqüência, ópticos ou infravermelho.

O hardware empregado em nós sensores deve ser compacto e de tamanho reduzido, implicando na limitação de seus recursos: memória de pequena capacidade, transceptor de curto alcance, processador com dezenas de MHz e bateria com capacidade reduzida. Dessa forma, as RSSF possuem limitações no seu tempo de vida, suas distâncias de transmissão e sua conectividade.

O projeto de uma RSSF é influenciado por requisi-

*O presente trabalho foi realizado com apoio do CNPq, uma entidade do Governo Brasileiro voltada ao desenvolvimento científico e tecnológico. Processo 55.2111/2002-3.

tos que incluem tolerância a falhas, escalabilidade, ambiente operacional, topologia da rede, meio de transmissão e restrições de hardware e consumo de energia, que são devidos à miniaturização e ao baixo custo dos nós. Os nós sensores muitas vezes são lançados de maneira aleatória em regiões inóspitas ou de difícil acesso, situações onde não existem procedimentos para a recarga das baterias. Mesmo em ambientes mais acessíveis agressivos a troca das baterias dos nós, realizadas por um operador humano muitas vezes é inviável devido ao grande número de nós existentes. Assim, um dos grandes desafios em uma RSSF é aumentar o tempo de vida da rede.

Algumas aplicações em RSSF podem utilizar fontes alternativas de energia, tais como células de energia solar, conversores de campo eletromagnético ou vibrações em energia [Pottie and Kaiser, 2000]. As dimensões reduzidas dos nós e as limitações específicas de cada aplicação, entretanto, podem restringir o uso dessas fontes alternativas. Assim, o problema de restrição de energia para o nó sensor pode persistir. Esta restrição, em conjunto com as limitações de hardware apresentadas anteriormente, inviabilizam o emprego de protocolos desenvolvidos para as redes ad hoc sem fio (*WLAN - Wireless Local Area network*), já que essas redes não possuem limitações tão severas de energia.

Nas arquiteturas de protocolos das RSSF, uma das camadas de maior relevância é a de controle de acesso ao meio (MAC - *Medium Access Control*). Os métodos empregados no controle de acesso ao meio influenciam fortemente no consumo de energia dos elementos de rede, na otimização de roteamento visando a conservação de energia e na forma como as aplicações são concebidas. Logo, os protocolos acima da camada MAC (aplicação, transporte e rede) devem se adaptar ao método de controle de acesso ao meio para proporcionar uma maior economia de energia [Polastre et al., 2004].

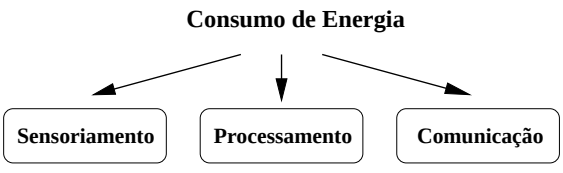

Figura 1: Funções consumidores de energia dos nós sensores.

O consumo de energia dos nós sensores está relacionado aos seus componentes de hardware, que realizam funções de sensoriamento, processamento e comunicação (figura 1).

No sensoriamento os dispositivos sensores consomem ao capturarem dados do ambiente, tais como luminosidade, intensidade de campo magnético, posição geográfica, temperatura, etc. No processamento o consumo é função do tipo e quantidade de instruções executadas pelo processador do nó sensor. Na comunicação o consumo de energia no envio e recepção de dados pelos dispositivos transceptores está relacionado à potência de transmissão, aos modos de operação e aos modos de acesso ao canal de transmissão.

Ao contrário das tradicionais redes ad hoc sem fio, as RSSF são desenvolvidas para um propósito específico, com características de tráfego altamente dependentes da aplicação. Muitos protocolos desenvolvidos para essas redes RSSF tendem a atender somente a uma classe de aplicações. Essas classes são caracterizadas pela forma de coleta de dados, pelo tipo de fenômeno observado ou pelo modo de comunicação entre os nós. Logo, não existe um protocolo de acesso ao meio que seja adequado a todas as aplicações [Langendoen and Halkes, 2005]. Assim, vários protocolos têm sido propostos, empregando diferentes abordagens para reduzir o consumo de energia e aumentar o tempo de vida da rede.

Este artigo propõe uma taxonomia adequada aos protocolos MAC em RSSF, considerando os atributos comuns das RSSF e as características diferenciadas da aplicação, como capacidade de adaptação e qualidade de serviço. O objetivo dessa taxonomia é classificar os protocolos MAC existentes.

O restante do artigo está organizado como se segue. A seção 2 apresenta uma visão dos principais transceptores empregados nas atuais plataformas de RSSF, sendo descritos aspectos relacionados aos eventos que ocorrem durante a comunicação e as técnicas empregadas na redução do consumo de energia. A seção 3 define uma taxonomia para os protocolos MAC considerando os requisitos comuns às RSSF, como alocação de canais e técnicas de comunicação, e características da aplicação como mensagens de notificação, capacidade de adaptação aos requisitos da rede e técnicas de qualidade de serviço. Na seção 4, os principais protocolos MAC encontrados na literatura são discutidos e classificados de acordo com a taxonomia proposta. Na seção 5 são descritos aspectos de segurança em RSSF e apresentados os componentes de segurança dos pro-

tocolos TinySec e IEEE 802.15.4. Uma discussão sobre os principais desafios nos protocolos de controle de acesso em RSSF é apresentada na seção 6. Finalmente, a seção 7 apresenta as considerações finais sobre os protocolos MAC em RSSF.

2 Comunicação e consumo de energia

Esta seção identifica os elementos de hardware do nó sensor que mais consomem energia. É mostrado como a comunicação afeta o consumo de energia nas RSSF e os principais tipos de transceptores empregados. São caracterizados os eventos responsáveis pelo consumo de energia durante a comunicação, utilizando transceptores em rádio freqüência. Os métodos para redução do consumo de energia são apresentados, classificados e discutidos, tendo como base a redução da quantidade de quadros transmitidos, a melhoria da organização da rede e sincronização de dados.

2.1 Consumo de energia dos componentes de hardware

Uma arquitetura tipicamente usada em RSSF é a Mica Motes [Crossbow, 2004], cujo consumo de seus componentes de hardware é mostrado na tabela 1. Dentre os componentes, o maior consumidor de energia é a memória *flash*. Apesar do alto consumo de energia durante os ciclos de gravação e leitura, a utilização da memória *flash* não é essencial na manutenção da conectividade ou na formação de uma RSSF. Em geral essa memória é empregada para armazenar dados lidos pelos sensores, tabelas de roteamento e outras informações específicas de cada aplicação. O uso de estratégias genéricas para economizar energia na utilização da memória *flash* não seria eficiente.

Dessa forma, o transceptor é o maior consumidor de energia dentre os componentes de hardware que são essenciais para a manutenção da conectividade e formação das RSSF. Mesmo quando está ligado escutando o meio de transmissão (modo *idle*) ou em repouso (modo *sleep*), o transceptor consome energia. Os transceptores nas RSSF utilizam o espectro eletromagnético para comunicação sob a forma de laser, infravermelho ou rádio freqüência.

Componente	Corrente
Processador	
Operação em carga	8 mA
Repouso	8 μA
Transceptor (0 dBm)	
Recepção	8 mA
Transmissão	12 mA
Repouso	2 μA
Memória Flash	
Escrita	15 mA
Leitura	4 mA
Repouso	2 μA
Sensor	
Ativo	5 mA
Inativo	5 μA

Tabela 1: Consumo no Mica Motes2. Fonte: [Crossbow, 2004]

Os nós que utilizam transceptores ópticos ou laser consomem menor quantidade de energia por bit transmitido e não necessitam de antena, mas devem ser alinhados de maneira que exista visada direta (LOS - *Line Of Sight*) entre os nós origem e destino. Essa característica impossibilita o uso desses transceptores em redes que não possuem uma topologia planejada, como em redes lançadas de maneira aleatória. Na plataforma Smart Dust vários tipos de transceptores podem ser acoplados, entre eles um transceptor óptico de comunicação passiva, realizada por um *Corner Cube Reflector* (CCR) com dimensões 0,5 $\times$ 0,5 $\times$0,1 mm^3 [Dust, 2004]. Esse transceptor óptico transmite a uma taxa de 10 kbps, consumindo 1 μW de energia e com alcance de transmissão de até 1 km.

Outra opção no Smart Dust é o transceptor laser com transmissão ativa, com dimensões de 1,0$\times$ 0,5 $\times$ 0,1 mm^3. Esse transceptor transmite a 1 Mbps, com consumo de 10 mW de energia e alcance de até 10 km. O volume total de um nó sensor Smart Dust chega a 1,5 mm^3 e a massa total a 5 mg, dimensões que tornam inviável o uso de transceptores que utilizem antenas [Dust, 2004]. Um dos projetos que utiliza esse transceptor é o MALT (*Motorized Active Laser Transceiver* [Hubert, 2004].

Os transceptores infravermelhos possuem as mesmas restrições de alinhamento dos transceptores laser, com o agravante de serem suscetíveis às variações de temperatura e umidade do meio de transmissão. Para resolver estes problemas são empregadas lentes para corrigir o desalinhamento, buscando ajustar o foco do sinal para o receptor [Agilent Technologies, 2004]. No

entanto, essas lentes não funcionam adequadamente em dias nublados.

Transceptor	Óptico ou laser	Infravermelho	Rádio freqüência
Alcance máximo	10Km	1,5m	≈ 100m
Consumo médio	10mW	≈ 7,5mW	15mW
Banda passante	1Mbps	1-4Mbps	10-250Kbps
Restrições	Precisa de linha de visada	Suscetível às condições do ambiente	Baixo alcance

Tabela 2: Transceptores e suas características.

A maioria dos projetos em nós sensores usam transmissão em rádio freqüência (RF) devido às restrições impostas por outros tipos de transceptores. Exemplos de plataformas que empregam RF são: Medusa [CENS, 2004], Smart Dust [Dust, 2004], SensoNet [GATECH, 2004], JPL [JPL, 2002], Millennial [Millennial Net, 2004], Mica Motes [Motes, 2002], μAMPS [μAMPS, 2002], PicoRadio [Pico, 2003], BEAN [Vieira, 2004] e WINS [WINS, 2003].

As especificações de cada tipo de transceptor, alcance de transmissão, consumo e taxa de transmissão estão sumariados na tabela 2. Devido à quantidade e popularidade das plataformas que empregam transceptores em rádio freqüência, nestes artigo são abordados somente os protocolos que empregam esse tipo de transceptor.

Os transceptores de rádio freqüência empregados nas RSSF são de ultrabaixa potência (mW ou μW) e de baixa tensão (de 3 a 5 V) [CC 1000, 2004, TR 1000, 2004]. A faixa de freqüência utilizada por estes rádios é livre, sendo conhecida como ISM/SRD (*Industrial, Scientific and Medical band/Short Range Device*). Os rádios podem utilizar freqüências que variam nas faixas de 315, 433, 868, 915 MHz e 2,4 GHz, dependo da plataforma e do país. Nessas faixas de freqüências são empregadas diversas técnicas de modulação, tais como ASK (*Amplitude Shift Keying*), FSK (*Frequency Shift Keying*) e DSSS (*Direct Sequence Spread Spectrum*), que influenciarão na propagação dos sinais no meio de transmissão. A arquitetura de nós sensores Mica Motes, por exemplo, emprega vários tipos de rádios, cujas especificações são apresentadas na tabela 3.

Os rádios empregados em RSSF operam em *half-duplex*, ou seja, a comunicação é bidirecional e não simultânea [Coelho and Agarwal, 2002, Tanenbaum, 2003]. Dessa forma, o rádio pode somente transmitir ou receber informações a cada instante de tempo. Do ponto de vista de uma pilha de

Transceptores RF			
Parâmetros	**CC1000 Mica Motes 2**	**TR1000 Mica Motes**	**CC2420 MicaZ**
Freqüência	915 MHz	915 MHz	2,4 GHz
Transmissão (0 dBm)	49,5 mW	36 mW	52,2 mW
Recepção	11,4 mW	13,5 mW	59,1 mW
Ocioso	10,5 mW	40,5 mW	1,3 mW
Repouso	2,1 μA	15 μW	3 μW
Banda	76,4 kbps	19,2 kbps	250 kbps
Modulação	FSK	ASK	DSSS

Tabela 3: Consumo dos transceptores. Fonte: [Crossbow, 2004]

protocolos, as características do rádio estão relacionadas às funções da camada física, isto é, tipos de modulação, esquemas de codificação de sinais, técnicas de transmissão e alocação de canal.

O controle dos modos de operação do rádio está relacionado ao protocolo de controle de acesso ao meio (MAC - *Medium Access Control*). Os protocolos MAC são responsáveis pelo método de alocação de canal e pelo controle dos parâmetros do rádio, tais como potência de transmissão, período de escuta e período de repouso.

As operações do rádio consomem grande quantidade de energia e são determinadas pelo protocolo MAC, mas existem outros eventos que consomem energia que devem ser tratados pelo protocolo. Esse tratamento muitas vezes implica em negociar parâmetros de latência, vazão e *fairness* em detrimento da economia de energia.

2.2 Eventos de comunicação e consumo de energia

O protocolo de acesso ao meio deve considerar eventos que consomem energia durante a comunicação. Muitos desses consomem energia desnecessariamente e podem ser evitados ou minimizados de acordo com o modo de operação escolhido. Os eventos durante a comunicação são discutidos abaixo de acordo com o método de alocação de canal utilizado:

Colisão: quando dois ou mais nós transmitem simultaneamente para um mesmo destino haverá colisão no receptor, sendo necessária a retransmissão dos quadros e incrementando o consumo de energia. Os protocolos MAC que empregam métodos de contenção estão sujeitos a colisões e portanto consomem energia desnecessária com quadros não entregues, enquanto os

protocolos MAC baseados em reserva ou alocação de banda não estão sujeitos a colisões (ver seção 3.1).

Overhearing: cada nó mantém seu rádio ligado na escuta de quadros transmitidos não destinados a ele. Para os protocolos MAC baseados em contenção, o período de escuta pode ser minimizado desligando-se o rádio por um período de tempo, ao verificar que o quadro não é endereçado a ele. Os protocolos baseados em alocação de banda não possuem esse problema, já que os nós somente operam em intervalos de tempo reservados ou em freqüências alocadas para cada nó.

Overhead: quadros de controle são utilizados para reserva do canal de comunicação, confirmação de recebimento de quadros de dados, sincronização e outras operações. Os quadros de controle aumentam o tráfego da rede e não transportam dados da aplicação, aumentando o consumo de energia e reduzindo a largura de banda do canal. Os protocolos baseados em contenção utilizam quadros de controle para reserva de canal e confirmação. Nos protocolos baseados em alocação estática de banda o *overhead* está relacionado ao tamanho do seu quadro de sincronização, quanto maior o quadro mais energia irá consumir até a transmissão de seus dados.

Idle listening: o nó escuta o meio de transmissão mesmo quando não existe tráfego na rede. Nos protocolos baseados em contenção esse problema pode ser minimizado estabelecendo períodos de escuta e de repouso, ou seja ajustando-se o modo de operação do transceptor. Nos protocolos baseados em alocação de banda, este problema é minimizado desligando-se o rádio quando o meio está ocioso durante o seu *slot* de tempo.

Sincronização de eventos: quando um evento ocorre em determinada região da rede sendo percebido por mais de um sensor, existe alta probabilidade de transmissão simultânea de informações, o que aumenta o número de colisões e o tráfego da rede [Woo and Culler, 2001]. Essa sincronização pode ser minimizada por agregação ou supressão de dados, já que os dados referentes a um mesmo evento carregam a mesma informação. Nos protocolos baseados em contenção, podemos utilizar algoritmos de *backoff* para atrasar o envio dos quadros. Os protocolos baseados em alocação estática são imunes a esse tipo de sincronização, já que cada nó somente transmite dentro da banda alocada.

O consumo de energia está relacionado à quantidade de quadros transmitidos e ao ciclo de operação do rádio. Algumas técnicas de redução do consumo de energia podem ser empregadas, como gerenciamento dos modos de operação do rádio e tratamento dos dados a serem transmitidos. A seção seguinte descreve os métodos empregados para economia de energia durante a comunicação dos nós na rede.

2.3 Métodos de economia de energia na comunicação

Os métodos para a economia de energia na comunicação são baseados na redução da quantidade de quadros transmitidos, na melhoria da organização da rede e nos métodos de sincronização de dados. A figura 2 classifica os métodos empregados para economizar energia durante o estabelecimento da comunicação entre os nós nas RSSF que são detalhados em seguida.

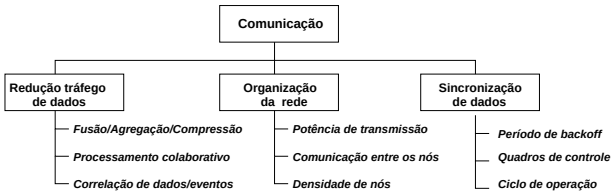

Figura 2: Operações para redução do consumo de energia.

Redução do tráfego de dados

A quantidade de informação transmitida pelo transceptor pode ser reduzida por métodos de fusão, agregação e compressão de dados,pelo processamento colaborativo e pelo emprego de técnica de correlação de dados.

Fusão: um nó sensor ao receber pacotes de outros nós vizinhos concatena esses pacotes em um único pacote de dados. Esse método diminui o *overhead* de tráfego de mensagens de controle na rede.

Agregação: um nó da rede ao receber pacotes de seus vizinhos realiza um processamento dos dados recebidos, e envia o resultado do processamento aos seus vizinhos em um único pacote, reduzindo o tráfego de dados e de quadros de controle.

Compressão: o nó sensor codifica seus dados de maneira a inseri-lo em um único pacote diminuindo o tráfego de dados na rede.

Processamento colaborativo: nós monitorando o mesmo evento podem apresentar medidas díspares. O processamento dos dados pode ajudar na calibração das medidas dos nós, evitando que medidas errôneas trafeguem na rede.

Correlação de dados: a ocorrência de eventos em uma determinada região faz com que sensores próximos transmitam informações semelhantes sobre o evento monitorado. Métodos como supressão, filtragem e outros podem ser usados para reduzir o tráfego de dados na rede.

Organização da rede

A economia de energia por organização da rede se aplica à potência de transmissão do transceptor, ao modo de comunicação entre os nós e à densidade de nós na rede.

Potência de transmissão: o ajuste da potência de transmissão do transceptor está relacionado ao alcance de comunicação. Quanto maior a potência de transmissão, maior será a área de cobertura do transceptor e maior o consumo de energia. A redução da potência de transmissão pode diminuir a probabilidade de terminais escondidos [Agarwal et al., 2001, Karn, 1990, Monks, 2001] e o número de colisões na rede, reduzindo o consumo de energia.

Comunicação entre os nós: a comunicação nas RSSF pode ser direta entre o nó e o ponto de acesso, conhecida como comunicação *single hop*, ou indireta entre os nós da rede até alcançar o ponto de acesso, conhecida como *multihop*. Segundo Heinzelman et al. o emprego de comunicação *multihop* na transferência de mensagens economiza energia [Heinzelman et al., 2000].

Densidade de nós: a alta densidade da rede aumenta a precisão dos dados coletados e também apresenta um esquema de tolerância à falhas. Segundo[Tilak et al., 2002] o aumento da densidade de nós poderá contribuir para o aumento de colisão de quadros na rede. Dessa forma, é necessário ajustar a densidade de nós na rede obtendo precisão dos dados e baixa taxa de colisão de dados.

Sincronização de dados

Os métodos empregados na sincronização de dados podem influenciar no consumo de energia. A comunicação pode ser sincronizada por intervalos de *backoff*, quadros de controle, e ciclo de operação do transceptor.

Período de backoff: na ocorrência de eventos em uma determinada região, nós próximos transmitirão seus quadros sincronizadamente com alta probabilidade de colisões na rede. Os nós ao detectarem um evento devem aguardar um período de tempo aleatório para transmitirem seus quadros, diminuindo a probabilidade de colisões na rede e desincronizando a transmissão com seus vizinhos.

Quadros de controle: a sincronização da transmissão é feita por quadros de controle, que definem escalas de tempo em que os nós podem transmitir e receber quadros. O tráfego dos quadros de sincronização aumenta o consumo de energia dos nós.

Ciclo de operação: os transceptores podem operar nos modos de transmissão, recepção, escuta e repouso. A redução do consumo de energia pode ser obtida alternando o ciclo de operação do rádio em períodos de escuta e repouso. No período de repouso o rádio consome apenas alguns μW enquanto que no modo de escuta consome algumas dezenas mW. O aumento do período de repouso acarreta redução do consumo, mas aumenta a latência de transmissão.

As técnicas para redução do consumo de energia são empregadas nos diversos protocolos MAC propostos na literatura, que além disso apresentam outras características como métodos de alocação de canais, notificação de transmissão, técnicas de comunicação, adaptabilidade do nó sensor ao ambiente da rede e qualidade de serviço. Essas características permitem a elaboração de uma taxonomia para protocolos MAC, apresentada na próxima seção.

3 Taxonomia de protocolos MAC

Esta seção define uma taxonomia para protocolos de controle de acesso ao meio em RSSF, considerando tanto as características comuns dos protocolos MAC quanto a sua capacidade de adaptação aos requisitos das aplicações e aos mecanismos de qualidade de serviço empregados.

Langendoen & Halkes apresentam um estudo sobre questões importantes no projeto de protocolos MAC para RSSF [Langendoen and Halkes, 2005]. Nesse es-

tudo é proposto um esboço de uma classificação para os protocolos MAC considerando três questões de projeto dos protocolos: tipos de alocação e quantidade de canais, grau de organização dos nós e tipo de notificação recebida pelos nós. No entanto, esse estudo não considera outros aspectos como a diversidade das aplicações em RSSF, a dinâmica do ambiente e aspectos de QoS. Por se tratarem de redes de propósito específico, os protocolos devem ser otimizados para cada cenário, e devem ser configuráveis para se adaptarem às características da aplicação e do ambiente. Além disso, a rede deve prover um serviço com a confiabilidade desejada pela aplicação e no tempo determinado. Para tanto, são necessárias políticas que garantam a qualidade do serviço da rede.

Portanto, além das questões mencionadas anteriormente, nossa taxonomia também inclui uma classificação quanto à capacidade de adaptação dos protocolos e quanto aos requisitos de qualidade de serviço. A figura 3 sumariza a taxonomia empregada na classificação dos protocolos MAC.

3.1 Alocação de canais de transmissão

Um elemento de rede com transceptor em rádio freqüência propaga o sinal em difusão para todos os elementos da rede que estão dentro de seu alcance de transmissão. Outros elementos de rede ao tentarem transmitir seus sinais no mesmo intervalo de tempo, poderão causar problemas à comunicação, como distorção do sinal propagado ou colisões dos quadros transmitidos. Para evitar os problemas de mistura de sinais a comunicação entre os elementos da rede deve seguir uma disciplina para controlar a transmissão e recepção. As disciplinas de controle de acesso ao meio empregam dois métodos de alocação de canais: estática ou dinâmica. O canal de comunicação deve adequadamente colocado para as entidades comunicantes, de maneira dinâmica ou estática.

Alocação estática de canal

A alocação estática de canal (ou síncrona) divide a largura de banda em N partes, alocadas para cada nó da rede. Esses nós estarão livres de colisões de sinais e de disputas pelo meio de transmissão, já que cada nó só transmite ou recebe quadros somente dentro de seu espaço alocado. Várias técnicas de multiplexação são empregadas na divisão da banda: divisão de tempo - TDMA (*Time Division Multiplex Access*), divisão de freqüência - FDMA (*Frequency Division Multiplex Access*) e divisão de código - CDMA (*Code Division Multiplex Access*).

As técnicas FDMA e CDMA requerem rádios com múltiplos canais, que em termos de consumo de energia é desaconselhável para RSSF [Ye et al., 2002, Dewasurenda and Mishra, 2004]. O emprego da divisão da banda usando CDMA é computacionalmente caro para ser usada em RSSF, já que os receptores devem possuir canais separados para decodificar o sinal recebido. O método FDMA requer mais componentes de hardware para organizar a alocação do canal, o que aumenta o consumo de energia [van Hoesel et al., 2003].

Os protocolos em RSSFs que empregam alocação estática de canal usam em geral as técnicas TDMA. Essas técnicas de alocação estática de canal necessitam de sincronização para que cada nó da rede identifique seu intervalo de tempo. A sincronização pode ser centralizada ou distribuída:

Centralizada: uma entidade da rede (nó sensor ou nó sorvedouro) é responsável por enviar um sinal para sincronização dos intervalos de tempo dos nós. Essa técnica é inapropriada para redes sem fio devido às características da rede como o atraso de propagação do sinal e perdas freqüentes de quadros.

Distribuída: cada nó ou grupo de nós gera sua própria escala de operação. O uso de diferentes escalas de sincronização na rede pode causar um escorregamento de relógio (*clock drift*), levando a perda de sincronismo. Desta forma, ajustes locais e periódicos devem ser realizados para minimizar este escorregamento de relógio. Apesar dos problemas encontrados neste tipo de alocação de canal, existem alguns protocolos para redes sem fio que empregam esta técnica, mas assumem que o intervalo de tempo reservado para o quadro transmitido é muito maior que o tempo de um possível escorregamento de relógio.

Por causa dos problemas de sincronização encontrados nas técnicas com alocação estática de canal, outro método de alocação dinâmica tem sido usado e pesquisado.

Alocação dinâmica de canal

Na alocação dinâmica de canal não existe atribuição fixa de largura de banda. Os nós disputam o acesso ao meio, existindo a probabilidade de colisões no envio dos dados. Isto ocorre por que os rádios são *half-duplex*, não podendo escutar o meio para verificar se algum outro nó está tentando transmitir ao mesmo tempo ou se ocorreu uma colisão. Dessa forma, métodos de detecção de portadora no meio de transmissão, como o CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*), não podem ser empregados.

As redes sem fio empregam um protocolo de contenção CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) que utiliza quadros de controle para estabelecer um diálogo de comunicação entre as estações. Existem variações nos esquemas empregados no estabelecimento dos diálogos de comunicação entre os nós. As requisições podem ser iniciadas tanto pelo emissor quanto pelo receptor.

Requisição iniciada pela emissor: o nó transmissor envia requisição ao receptor informando que tem dados a transmitir, e aguarda resposta do receptor para estabelecer a comunicação.

Requisição iniciada pelo receptor: o nó receptor envia requisição aos nós da rede informando que está pronto para receber dados. O nó que tem dados para transmitir responde a requisição, estabelecendo a comunicação.

Os métodos de alocação de canais de forma estática ou dinâmica proporcionam a utilização de algumas técnicas de comunicação entre os nós da rede, descritas a seguir.

3.2 Coordenação da comunicação entre nós

Os protocolos de controle de acesso ao meio para RSSF empregam técnicas de comunicação entre os nós que seguem os modelos descritos abaixo:

Aleatórios: os protocolos baseados em alocação dinâmica de canais seguem os modelos de contenção CSMA (*Carrier Sense Multiple Access*), que são aleatórios. Os nós transmitem seus quadros sem seguir qualquer escalonamento.

Escalonados: os protocolos com alocação estática do canal (TDMA) transmitem seus dados em momentos determinados, evitando colisões. A coordenação da transmissão é definida por uma entidade ou nó da rede conhecido como escalonador.

Híbridos: são protocolos baseados em contenção, mas que utilizam escalonadores para que cada nó saiba quando seu vizinho está pronto para receber dados. Alguns protocolos para RSSF como o S-MAC e T-MAC, seguem um modelo híbrido de comunicação entre os nós [van Dam and Langendoen, 2003, Ye et al., 2002].

Para transmitir um quadro, o nó deve aguardar até que o receptor esteja pronto para a recepção de dados. Dessa forma, algum método de notificação deve ser empregado no estabelecimento da comunicação entre os nós. A seguir são descritos os métodos de notificação empregados em RSSF.

3.3 Notificação da existência de dados no canal

Para que a transmissão ocorra, o receptor deve estar pronto para receber dados no momento da transmissão. Dessa forma, o nó deve ser notificado da existência de transmissão de dados no canal. Pelas características dos protocolos de controle de acesso ao meio, podemos classificar as notificações como:

Reserva: os protocolos para RSSF baseados em alocação estática de canal (TDMA) reservam um intervalo de tempo (*slot*) para a transmissão de quadros ou para a escuta do canal. Nesses protocolos o nó mantém seu rádio ligado somente durante períodos reservados de escuta e transmissão. São exemplos deste método de notificação os protocolos TRAMA e DE-MAC [Rajendran et al., 2003, Kalidindi et al., 2003].

Acordar sob demanda: os nós receptores mantêm seus rádios desligados, que somente são ligados (acordados) quando recebem uma notificação dos transmissores. Essa notificação é feita por um sinal ou tom enviado à rede (*beacon*) pelo transmissor. Os nós utilizam dois rádios, um de maior potência para transmitir e receber quadros e outro de ultra baixa potência que fica escutando o meio aguardando uma notificação. O rádio de menor potência desperta o segundo rádio ao receber uma notificação. Esse método é empregado por protocolos projetados para

redes *ad hoc*, como por exemplo o STEM, PCMA e PicoRadio [Bambos and Kandukuri, 2000, Pico, 2003, Schurgers et al., 2002].

Escuta do canal: nos protocolos baseados em contenção não existe uma reserva de tempo definida para cada nó da rede transmitir ou receber quadros. Uma alternativa é manter o receptor ligado aguardando uma transmissão, mas isso consome muita energia. O ideal é que o rádio fique ligado somente no momento da recepção para evitar períodos de escuta ociosa, estabelecendo-se um ciclo de operação. Portanto, a escuta do canal pode ser feita de maneira:

- *Síncrona*: os nós seguem um ciclo de operação, definindo períodos de repouso e atividade, que são determinados localmente pela troca de quadros de sincronização. Dessa forma, o transmissor aguarda até que o receptor esteja em atividade para enviar seus quadros. Protocolo que utilizam esse método são o S-MAC e o T-MAC.
- *Assíncrona*: o nó periodicamente escuta o canal, seguindo o seu próprio ciclo de operação, para verificar se existe alguma transmissão em progresso. Um esquema conhecido como LPL (*Low Power Listening*) é utilizado pelo nó transmissor, que envia um preâmbulo de tamanho superior ao tempo de repouso, garantindo a escuta. Esse método é usado no protocolo B-MAC [Polastre et al., 2004].

Além das notificações propostas para que os nós da rede possam receber dados, é necessário que o nó se adapte às características da aplicação e das condições do ambiente na formação da rede. Essa capacidade de adaptação é apresentada a seguir.

3.4 Capacidade de adaptação

As características de uma RSSF são influenciadas pela aplicação e pela variabilidade das condições do ambiente. Além disso, a estrutura da rede tende a se modificar durante o seu tempo de vida, seja por falha ou desvanecimento de energia dos nós. Logo, os protocolos de controle de acesso ao meio devem possuir mecanismos que permitam seu ajuste à variabilidade do ambiente a fim de otimizar seu funcionamento e economizar energia. As características desses protocolos podem ser subdividas quanto ao modo de adaptação em:

Estático: não permitem à aplicação ajustar os parâmetros de configuração dos protocolos em tempo de execução. Os parâmetros são definidos no momento de compilação do código ou durante a programação do nó, se mantendo inalterados durante todo o tempo de vida da rede. Os parâmetros estáticos são simples de programar e em geral demandam menos recursos de memória e processamento, permitindo seu uso em ambientes com restrição severa de recursos. Os parâmetros podem ser estáticos devido a uma decisão de projeto ou limitações de hardware, como por exemplo freqüência e potência de transmissão do rádio. Além disso, o emprego de parâmetros estáticos limita a aplicabilidade do protocolo a um tipo de rede ou cenário específico.

Reconfigurável: permitem a mudança de parâmetros pelo operador ou pela aplicação em tempo de execução. A mudança dos parâmetros pode ser desencadeada pela aplicação ou por recebimento de um comando do operador. A reconfiguração aumenta a aplicabilidade do protocolo a vários cenários. Para isto a aplicação deve adicionar uma lógica que ajuste os parâmetros em tempo de execução às condições da rede. Outra forma de reconfiguração é o envio de comandos do operador, permitindo a tomada de decisão fora da rede, utilizando algoritmos mais complexos. Essa abordagem demanda mais recursos de hardware e está sujeita a falhas, como por exemplo erros na programação da aplicação ou da transmissão do comando do operador ([Pradhan, 1996]).

Auto-configurável: permitem a mudança automática dos parâmetros, ajustando-se à variabilidade do ambiente sem a influência do operador. Esses ajustes são realizados por uma lógica interna pré-definida no protocolo. Caso essa lógica seja modificada durante o tempo de execução, consideramos que o protocolo é reconfigurável e auto-configurável. A auto-configuração permite ao protocolo se ajustar às condições adversas do ambiente e à múltiplas configurações em pontos distintos da rede. Para tanto o código é mais complexo e geralmente necessita de mais recursos em comparação com a reconfiguração, pois deve levar em conta todos os estados possíveis de operação. A auto-configuração pode ser baseada em algoritmos distribuídos, portanto os nós estarão sujeitos a falhas bizantinas decorrentes de problemas de sincronização [Avizienis et al., 2004].

Para garantir que o serviço da rede opere dentro de parâmetros de qualidade especificados, os protocolos MAC podem utilizar técnicas de QoS. Essas técnicas são sumarizadas a seguir.

3.5 Técnicas de QoS em RSSF

As RSSF tradicionalmente são desenvolvidas para serem eficientes em energia. Entretanto, devemos também considerar aspectos de qualidade de serviço (QoS) durante o projeto da rede. Redes para resposta a situações de risco e redes de monitoração de intrusão são exemplos de RSSF onde a qualidade de serviço deve ser considerada.

Em RSSF o acesso ao meio de comunicação é determinante para a qualidade de serviço (QoS - *Quality of Service*) [Lu et al., 2002]. Os protocolos são projetados para aplicações específicas e necessitam de mecanismos internos para prover requisitos de qualidade. Além disto, os sinais e dados que trafegam no meio sem fio são utilizados tanto para coordenar as atividades dos nós quanto para a transmissão das leituras recebidas. Desta forma, em RSSF a QoS é obtida por meio da implementação de políticas de priorização das funções de rede e não da aplicação. As técnicas de qualidade de serviço são geralmente aplicadas nas camadas física, enlace, rede e aplicação da pilha de protocolos.

Camada física: esta camada busca evitar a interferência com outras redes ou fontes naturais de radiação, modificando a modulação e freqüência de operação para diminuir o nível de sinal-ruído (SNR), como acontece no HiperLAN [Walke et al., 2001] e nos padrões de redes domiciliares HomePlug e HomePNA [Velloso et al., 2004]. Em RSSF, com exceção do padrão IEEE 802.15.4, a modulação e a freqüência de operação normalmente são fixas, para simplificar o projeto do rádio e dos protocolos. Desta forma, os transceptores das RSSF atuais não permitem ajuste de parâmetros de QoS na camada física.

Camada de enlace: nesta camada o escalonamento do acesso ao meio e a ordem dos quadros a serem enviados são modificados para atender os requisitos de QoS. Estas modificações podem ser obtidas pela reordenação de quadros e por políticas de priorização e controle de admissão de dados. Por fim, é possível ajustar a quantidade de dados de controle enviados para aumentar a QoS de um pacote. Cada uma dessas alternativas são descritas na seção 3.5.1.

Camada de rede: como ocorre na camada de acesso ao meio, podemos também utilizar a priorização de pacotes. Em redes tradicionais, priorizamos dados por fluxo ou individualmente, utilizando políticas de enfileiramento de pacotes como o *token bucket* e WFQ (*Weighted Fair Queuing*) [Peterson and Davie, 2003], entre outras . Em RSSF, geralmente não existe a noção de fluxo, portanto temos uma priorização por pacote. Devido à variabilidade da qualidade dos enlaces, a quantidade de cópias enviadas e o número de rotas distintas de um mesmo pacote podem ser ajustadas de acordo com a sua importância [Bhatnagar et al., 2001].

Camada de Aplicação: as aplicações de áudio e vídeo em redes tradicionais utilizam técnicas de compressão adaptativa, que se ajustam às condições da rede diminuindo a banda de passagem utilizada [Peterson and Davie, 2003]. Da mesma forma, e, RSSF a camada de aplicação pode ajustar a periodicidade do envio de dados [Sankarasubramaniam et al., 2003].

Em redes tradicionais, a qualidade de serviço se baseia em métricas como banda, latência e jitter. Em RSSF, entretanto, encontramos vários desafios que não se apresentam em redes tradicionais:

Energia escassa: para prolongar o tempo de vida da rede, os protocolos devem considerar a energia residual dos nós. Assim, métricas de QoS em sensores também devem considerar o consumo de energia da transmissão de dados [Younis et al., 2004].

Correlação de dados: os dados transmitidos por nós sensores tendem a ser correlatos, sendo assim muitos deles podem ser descartados [Sankarasubramaniam et al., 2003], ou passíveis de fusão ou agregação dos dados [Younis et al., 2004].

Desligamento de nós: nós sensores alternam períodos de atividade e inatividade, como forma de economia de energia [F. Dai and J. Wu, 2004]. Os protocolos de QoS devem adaptar-se dinamicamente ao estado dos nós.

Limitações de hardware: como ocorre em qualquer aplicação ou protocolo proposto para RSSF, a limitação de recursos imposta aos nós sensores limita as opções de projeto de políticas de QoS a soluções simples e de baixo consumo de banda e memória.

Alta taxa de erro de bits: característica de redes sem fio, a alta taxa de erro de bits no canal deve ser considerada nas políticas de QoS, pois afeta o número de retransmissões e a taxa de entrega. Além disto, esta taxa pode definir se será utilizado um código de de-

tecção de erros (CRC) ou um código de correção de erros (FEC) na transmissão de dados, de acordo com a importância da informação transmitida.

Tendo em vista estes fatores, as métricas de QoS em RSSF devem considerar, além dos parâmetros tradicionais, a energia e a taxa de entrega [Younis et al., 2004]. Além disto, a corretude da visão do ambiente sensoriado, medida como a diferença das leituras observadas após o processamento dos dados recebidos em relação ao fenômeno real, também pode ser considerada como uma métrica de QoS [Sankarasubramaniam et al., 2003].

Devido à emergência de propostas de QoS para RSSF, optamos por mesclar técnicas utilizadas em redes tradicionais guiadas e em redes sem fio com propostas correntes de RSSF, uma vez que acreditamos que várias soluções utilizadas em redes tradicionais podem ser adaptadas para RSSF.

3.5.1 QoS na Camada de Acesso ao Meio

As técnicas de QoS no acesso ao meio podem ser divididas em quatro categorias:

Reordenação de quadros: são políticas de reordenação da fila de pacotes a serem enviados, utilizadas para que os dados que possuem maior prioridade fiquem menos tempo na fila. O IEEE 802.11e utiliza esta técnica dividindo a fila por classes, que são definidas pelas camadas superiores [Xiao, 2004]. O RAP (*Real-Time Architecture Protocol*) é um exemplo de protocolo que emprega reordenação de quadros em RSSF [Lu et al., 2002].

Priorização do acesso ao meio: utilizada em protocolos de acesso ao meio baseados em contenção, como no IEEE 802.11e no modo EDCF [Xiao, 2004]. Consiste em aumentar a chance de pacotes de maior prioridade ganharem acesso ao meio, utilizando políticas de *backoff* e tempos de espera diferenciados para cada classe de dados.

Controle de admissão: são algoritmos que controlam a quantidade de dados que um nó pode enviar em um dado período de tempo. É utilizado no IEEE 802.11e, onde o ponto de acesso determina quantos bytes uma estação pode enviar a cada *superframe* [Xiao, 2004], e em redes ATM, onde um novo fluxo de dados é aberto somente se o enlace pode prover a QoS requisitada [Peterson and Davie, 2003].

Overhead de controle: consiste em utilizar seletivamente quadros de controle, como reserva de canal (diálogo RTS/CTS do IEEE 802.11, por exemplo) e quadros de confirmação de recebimento (ACK) por quadro ou por grupo de quadros transmitidos. Assim, garantimos uma maior taxa de entrega ao custo de uma menor banda efetiva e maior consumo de energia. As mensagens que necessitariam de uma maior garantia de recebimento (como mensagens de reprogramação, por exemplo) utilizariam quadros de controle, enquanto mensagens comuns seriam enviadas sem sinalização ou confirmação [Bhatnagar et al., 2001].

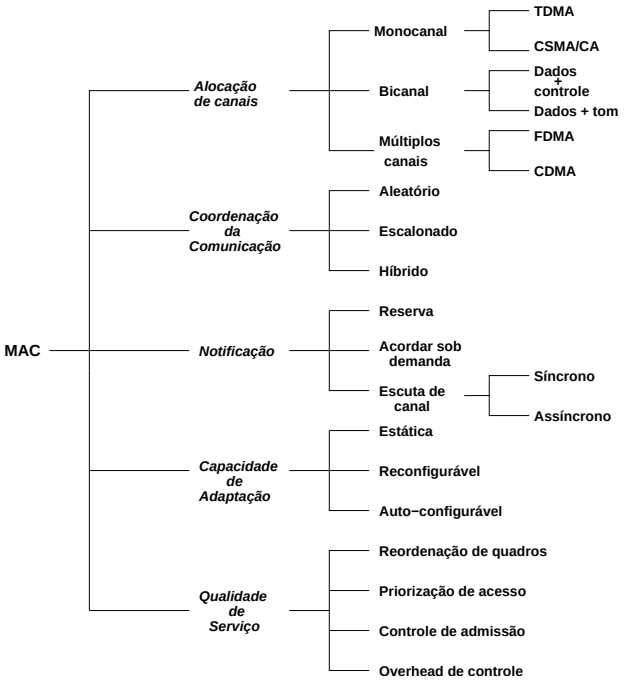

Figura 3: Taxonomia para classificação de protocolos MAC.

Na seção seguinte descrevemos os principais protocolos MAC para RSSF e os classificados segunda a taxonomia proposta.

4 Descrição e classificação de protocolos MAC

Os protocolos de acesso ao meio para RSSF são diferentes dos empregados em redes *ad hoc* sem fio. As características da aplicação influenciam os requisitos do MAC, assim os protocolos são especializados para certos tipos de rede. Além disso, os pacotes possuem algumas dezenas de bytes, devido à baixa largura de banda e ao tamanho dos dados gerados pelos sensores. Outra característica das RSSF, é que seus elementos de rede não possuem hardware adicional para detecção de portadora, detecção de colisão, enquadramento de dados ou balanceamento de energia. Para caracterizar as aplicações em RSSF um conjunto de métricas deve ser utilizado:

- Energia residual: quantidade de energia presente no elemento de rede naquele instante de tempo.
- Escalabilidade: quanto a rede pode crescer em número de nós.
- Adaptabilidade: o nó pode se autoconfigurar ao ser inserido em uma rede já existente ou em uma rede em formação.
- Justiça (*fairness*): é a distribuição de recursos da rede de maneira uniforme para todos os nós da rede, esses recursos são vazão e tempo de acesso ao canal.
- Vazão: quantidade de informação propagada no meio por um intervalo de tempo.
- Latência: atraso na transmissão de mensagens.

A comparação de protocolos MAC em RSSF não é uma tarefa trivial. A maioria dos protocolos projetados para essas redes negociam métricas como energia em detrimento do aumento da latência ou justiça. Além disso, esses protocolos são projetados para ambientes e aplicações específicas. A seguir são descritos os principais protocolos de controle de acesso ao meio para RSSF.

4.1 Protocolo S-MAC

O primeiro protocolo de controle de acesso desenvolvido especificamente para RSSF foi o S-MAC (*Sensor-MAC*) [Ye et al., 2002]. Esse protocolo de controle de acesso ao meio é baseado em alocação dinâmica de canal, mas utiliza sincronização para coordenação dos modos de operação do rádio. O S-MAC é destinado a aplicações dirigidas a eventos, insensíveis a latência e com baixa taxa de envio de mensagens. A comunicação entre os nós segue um fluxo *broadcast* ou um fluxo *unicast*. Considera os requisitos de uma rede densa e homogênea (nós com hardware idêntico) para ser eficiente em energia e permitir a autoconfiguração dos nós da rede.

O S-MAC procura ser eficiente em energia reduzindo o consumo dos principais eventos responsáveis pelo desperdício de energia:

- *Colisões*: todos os nós desejam transmitir ao mesmo tempo para um mesmo destino. Para resolver o problema de colisão o S-MAC emprega um diálogo de comunicação *RTS-CTS-DATA-ACK* para a detecção de portadora física e um vetor de alocação de rede (NAV - *Network Allocation Vector*) para detecção de portadora virtual, como no IEEE 802.11. Este diálogo de comunicação evita colisões e problemas de terminal escondido. Caso ocorra colisão, utiliza um algoritmo para aguardar um tempo aleatório, o BEB (*Binary Exponential Backoff*).
- *Overhearing*: os nós escutam transmissões de quadros destinados a outros nós. O S-MAC desliga o rádio do nó ao verificar que o quadro não é destinado a ele.
- *Overhead*: quadros de controle são utilizados para reserva do canal de comunicação, reconhecimento de quadros de dados, sincronização e outros. Estes quadros de controle aumentam o tráfego da rede e não transportam dados úteis. O S-MAC reduz o tamanho dos quadros de controle para diminuir o *overhead*.
- *Idle listening*: o nó fica escutando o meio de transmissão mesmo quando não existe tráfego na rede. O S-MAC utiliza um ciclo de operação com tempos fixos de atividade (*listen*) e de repouso (*sleep*). O tempo de atividade é menor que o tempo de repouso (cerca de 10%).

A sinalização para os quadros de controle e de sincronização é feita dentro do canal, enviando um pacote SYNC (*synchronization*) em *broadcast* para todos os seus vizinhos. O S-MAC aplica a técnica de

message passing para reduzir a latência durante a contenção em aplicações que requerem armazenamento de informações para processamento na rede (*in-network*). Esta técnica permite a transmissão de mensagens longas, que são divididas em pequenos fragmentos e enviadas em rajada. Este protocolo obtém considerável redução do consumo de energia, prolonga o tempo de vida da rede e encontra-se implementado na plataforma Mica Motes [Motes, 2002].

4.2 Protocolo ARC

O protocolo ARC (*Adaptive Rate Control*) tem como metas a alocação de largura de banda, justiça (*fairness*) e eficiência em energia para condições de alto e baixo tráfego na rede [Woo and Culler, 2001].

É um protocolo de controle de acesso ao meio baseado em alocação dinâmica de canal, destinado a aplicações dirigidas a eventos. A ocorrência de um evento físico em uma determinada região de uma RSSF pode fazer com que todos os nós daquela região transmitam sincronizadamente, evento que pode se repetir periodicamente. Essa transmissão sincronizada leva à colisão na transmissão dos dados coletados pelos nós. O ARC propõe um mecanismo para atrasar e desincronizar a transmissão dos nós na ocorrência de um evento físico na rede. Um atraso inicial, denominado de *backoff* inicial, é introduzido antes da transmissão dos nós, atuando como uma fase de deslocamento da periodicidade da aplicação.

A relação entre o tráfego originado e o tráfego de passagem pelo nó (*traffic thru*) tem um impacto direto em encontrar justiça na transmissão, já que eles competem pela mesma banda de passagem. Para aumentar a probabilidade dos dados chegarem ao ponto de acesso, o ARC controla a taxa de dados repassados utilizando um mecanismo de sinalização. O mecanismo de sinalização indica ao nó para aumentar sua taxa de dados se ao inserir dados na rede ele obtém sucesso e paradimunuir a taxa se houve falha. O nó pai é responsável por sinalizar ao nó filho sobre as condições de tráfego na rede.

O ARC utiliza quadros de controle para evitar o problema do terminal escondido e fornece efetivo controle de acesso ao meio. O ARC proporciona justiça e mantém razoável largura de banda, sendo eficiente em energia para situações de baixo tráfego.

4.3 Protocolo T-MAC

O protocolo Time-out-MAC (T-MAC) é baseado em contenção [van Dam and Langendoen, 2003], foi desenvolvido para aplicações dirigidas a eventos que possuem baixa taxa de entrega de mensagens, insensíveis a latência e com transmissão contínua ou periódica de dados. A meta do T-MAC é ser eficiente em energia, considerando as limitações do hardware do nó e os padrões de comunicação entre seus vizinhos e a estação base.

A proposta do T-MAC é reduzir o tempo de *idle listening*, sendo utilizados ciclos de atividade e repouso para diminuir o consumo de energia do nó. O controle do tempo ativo é feito pelo temporizador T_A, (*time-out*) que ao seu término coloca o rádio em repouso, conforme mostrado na figura 4. As mensagens recebidas durante o tempo de repouso são armazenadas e transferidas em rajadas de tamanho variável, no início do tempo ativo.

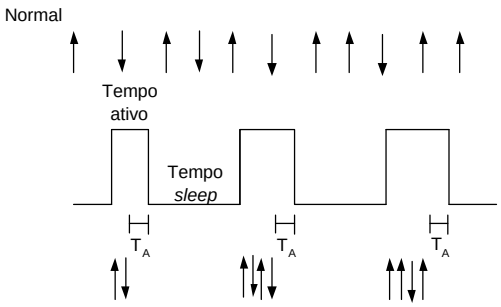

Figura 4: Ciclo adaptativo do protocolo T-MAC.

O nó escuta a rede, transmite e recebe dados durante seu tempo ativo. O temporizador determina o final do tempo ativo quando não ocorrem eventos durante um tempo T_A.

O rádio pode ser religado na ocorrência de eventos, como: início periódico de quadro, recepção de dados no rádio, final da transmissão de seus vizinhos, final da transmissão de seu próprio quadros de dados, recebimento de *ACK* ou detecção de sinal no rádio (RSSI - *Received Signal Strenght Indicator*).

Os nós utilizam o diálogo *RTS-CTS-DATA-ACK* para evitar colisões e obter transmissão confiável. De maneira semelhante ao S-MAC, o T-MAC utiliza agrupamentos virtuais para sincronizar seu ciclo de operação. Os nós transmitem suas escalas para os seus

nós vizinhos através de pacotes SYNC.

A recepção de pacotes *RTS-CTS* renovam o tempo T_A, tempo suficiente para receber um pacote *CTS*. O mecanismo de *backoff* é baseado em um número aleatório de intervalo fixo, calculado em função da carga máxima.

Os protocolos baseados em contenção, como o T-MAC, estão sujeitos ao problema de dormir cedo (figura 5). Este problema ocorre quando um nó dorme enquanto um outro nó ainda tem mensagem para ele. Este problema pode ser resolvido de duas formas:

- Na primeira, um nó ao escutar um pacote *CTS* destinado a outro nó envia imediatamente aos seus vizinhos um pacote designado de *FRTS* (*Future RTS*), que evita que os nós vizinhos entrem em modo de repouso.

- A outra forma é usar um esquema de priorizar o esvaziamento do *buffer* quando eles estiverem perto de sua capacidade limite. Um nó ao receber um *RTS* ao invés de responder com um *CTS*, transmite as mensagens armazenadas em seu *buffer* para o nó de destino.

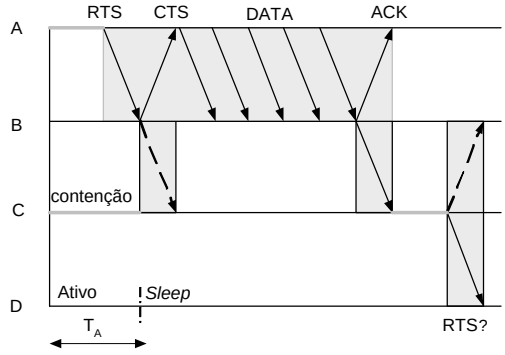

Figura 5: O nó D dorme antes de C enviar um RTS.

O T-MAC consegue ser mais eficiente em energia que o S-MAC, mas é extremamente limitado em largura de banda e o seu algoritmo não é aplicável para grandes transferências de dados, como por exemplo reprogramação [Polastre et al., 2004].

4.4 Protocolo B-MAC

O protocolo B-MAC foi projetado para RSSF de monitoramento ambiental. É um protocolo baseado em alocação dinâmica do canal que apresenta um novo método para evitar colisões na rede por julgamento do estado do canal. Esse método consiste em obter amostras de ruído do meio de transmissão e determinar se o canal está sendo usado. O protocolo permite a reconfiguração de seus parâmetros pelos serviços da aplicação em função das condições do enlace, do número de vizinhos e do tráfego da rede [Polastre et al., 2004]. O B-MAC encontra-se implementado nas arquiteturas de nós sensores que utilizam o sistema operacional TinyOS. As metas do B-MAC são de obter um protocolo MAC reconfigurável para RSSF que seja simples, funcional, com pequeno tamanho de código, que suporte vários tipos de tráfego e que aumente o tempo de vida da rede.

Para evitar colisão de quadros na rede o B-MAC utiliza uma heurística para verificar se existe atividade no canal, ou julgamento de canal, conhecida como CCA (*Clear Channel Assistment*). Essa heurística é baseada em amostrar a força do sinal recebido do meio de transmissão quando não existe tráfego na rede. A partir destas amostras, o valor máximo de ruído do meio é determinado, sendo denominado de ruído base. Quando um nó deseja transmitir ele amostra o nível de sinal do meio e o compara com o ruído base. Quando um nó deseja transmitir ele amostra o nível de sinal do meio e o compara com o ruído base. Se o valor da amostra for próximo ao ruído base, é estimado que o meio está livre para a transmissão, caso contrário, o meio está ocupado e o nó não poderá transmitir. A heurística CCA provê um método de detecção de portadora antes da transmissão pelo nó, não necessitando de sincronização entre os nós vizinhos ou reserva de canal.

Os períodos de *idle-listening* são minimizados utilizando um ciclo de operação. O nó periodicamente amostra o canal para verificar se existe alguma transmissão em progresso. Se alguma transmissão é identificada, o nó entra em modo de recepção e pesquisa um preâmbulo no sinal recebido. Os preâmbulos emitidos pelo transmissor devem ser ajustados de maneira que seu tempo de transmissão seja superior ao intervalo de tempo de repouso dos nós para garantir a sua escuta. Esse método é conhecido como LPL *Low Power Listening*).

O B-MAC não utiliza quadros para reserva de canal (*RTS/CTS*) nem mecanismos de sincronização, de maneira a reduzir e simplificar o código. Para o B-MAC a energia consumida pelo nó consiste da energia consumida pelo receptor, pelo transmissor, pela amostragem de sinais no canal do rádio com LPL e do período de repouso. Dessa forma, o tempo de vida da rede é função do intervalo de amostragem, do tamanho do preâmbulo e do tempo de repouso do nó.

O tamanho do preâmbulo está relacionado com o tempo de repouso do nó, de maneira que seja possível que o nó detecte o preâmbulo a ciclo de operação. No protocolo B-MAC o tamanho do preâmbulo é calculado dinamicamente em função do tempo de repouso, de modo a minimizar o custo da transmissão do preâmbulo.

O B-MAC permite aos serviços da aplicação controlar adaptativamente seus parâmetros como habilitar ou desabilitar o CCA, configurar períodos de *backoff* para negociar vazão e *fairness*. Permite também configurar um serviço confiável de enlace por meio de quadros de controle de mensagem recebida (ACK), o serviço pode escolher entre retransmitir quadros perdidos e reconfigurar os parâmetros de LPL.

4.5 Protocolo DE-MAC

O protocolo DE-MAC (*Distributed Energy aware MAC*) trata do gerenciamento e balanceamento de energia em RSSF [Kalidindi et al., 2003]. É um protocolo que emprega alocação estática de canal TDMA, sendo assim livre de colisões e de *overhead* de pacotes de controle.

O DE-MAC utiliza um algoritmo distribuído para balanceamento de carga na rede. Este algoritmo estabelece que os nós em estado de baixa energia devem ser tratados diferentemente e usados com menor freqüência no roteamento. Para isso o DE-MAC realiza um procedimento local de eleição. A eleição é usada para escolher o nó com mais baixa energia de todos os nós da rede, que ficará mais tempo em repouso (modo *sleep)* que seus vizinhos. Como o protocolo é baseado em TDMA, e a eleição é integrada com o tempo alocado para cada nó (*slot* TDMA). O DE-MAC assume sincronização dos quadros TDMA e a eleição dos nós com mínima energia garante o balanceamento de energia na rede.

4.6 Protocolo TRAMA

O protocolo TRAMA (*TRaffic Adaptive Multiple Access*) é baseado em alocação estática de canal TDMA [Rajendran et al., 2003]. É projetado para aplicações dirigidas a eventos com coleta contínua ou periódica de dados em RSSF. A meta principal deste protocolo é ser eficiente em energia e o método de acesso ao canal garante que não existirão colisões em comunicações *unicast*, *broadcast* ou *multicast*.

O TRAMA se adapta ao tipo de tráfego utilizando um algoritmo distribuído de eleição. Este algoritmo determina qual nó pode transmitir em determinado intervalo de tempo (*time-slot*) e não faz reserva para os nós sem tráfego de envio. O algoritmo de eleição é baseado em informações de tráfego de cada nó e seleciona receptores baseados em escalas anunciadas pelos transmissores. As escalas são obtidas pela troca de informações locais de sua vizinhança de dois *hops* e especificam quais nós serão os respectivos receptores de seu tráfego em ordem cronológica.

O TRAMA alterna entre acessos aleatórios e escalonados para acomodar mudanças de topologia, suportando a adição e falha de nós. Consiste de três componentes:

- NP (*Neighbor Protocol*) - responsável pela propagação e atualização de informações sobre seus vizinhos de um *hop*. As atualizações são incrementais e permitem determinar o conjunto de vizinhos que serão adicionados ou removidos.
- SEP (*Schedule Exchange Protocol*) - permite que os nós troquem informações da vizinhança de suas escalas de dois *hops*.
- AEA (*Adaptive Election Algorithm*) - utiliza as informações da vizinhança e de suas escalas para selecionar transmissores e receptores para o intervalo de tempo atual, enquanto os outros nós selecionem o modo de repouso (*sleep*).

O protocolo TRAMA assume possuir uma visão global da rede pela troca de mensagens locais e de sua vizinhança de dois *hops*. Assume também, que não existe problema de escorregamento de relógio. Mesmo com todas essas considerações as simulações realizadas com esse protocolo mostraram que ele é adequado para aplicações insensíveis à latência e que requeiram alta taxa de entrega.

4.7 IEEE 802.15.4

O IEEE 802.15.4 é uma padronização das camada física e de acesso ao meio para dispositivos de baixo custo, que possuem limitações severas de energia e que enviam dados a baixas taxas [Jianliang Zheng and Lee, M.J., 2004]. O IEEE 802.15.4 é uma alternativa ao Bluetooth, pois aumenta o número de dispositivos suportados, e possui implementação mais simples e de menor custo. Foi desenvolvido para aplicações de automação doméstica e industrial, monitoração ambiental e entretenimento, além de RSSF. São permitidos até 2^{64} dispositivos na rede, distribuídos em uma ou mais redes, coexistindo até 2^{16} redes em uma região.

O padrão especifica duas freqüências de operação: 2.4 GHz com banda total de 250 kbps, e 868/915 MHz operando a 20/40 kbps, respectivamente. A freqüência de operação também determina outras características, como área máxima de cobertura do sinal, interferência e modulação [Callaway et al., 2002]. A banda é dividida em canais, sendo todos estes utilizados por padrão, mas que podem ser selecionados dinamicamente por outras camadas, como uma forma de atenuar interferências com outras redes ou evitar canais com ruído alto.

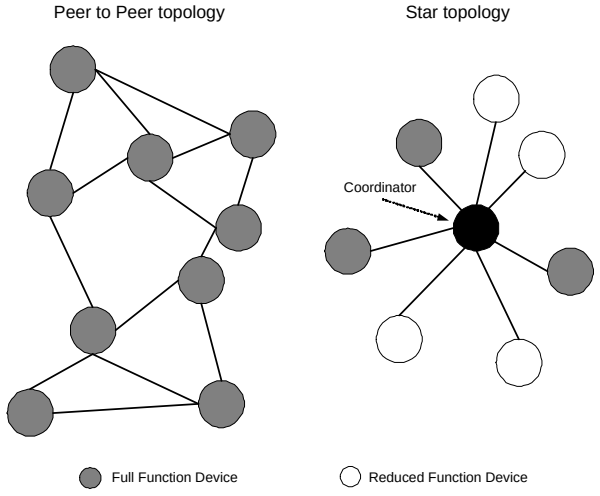

Figura 6: Organizações de uma rede no padrão IEEE 802.15.4.

O padrão foi desenvolvido para duas topologias: estrela e multi-saltos, definidos pela camada de controle de acesso ao meio, ilustradas na figura 6. A configuração da rede permite o uso de dispositivos mais simples, permitindo assim redes de baixo custo, como detalhamos a seguir.

Redes em estrela: as redes em estrela são apropriadas para aplicações onde um nó com grande capacidade (chamado de *Full Function Device*, ou FFD) controla a comunicação entre vários dispositivos restritos (*Reduced Function Devices*, ou RFDs) ou de grande capacidade, formando uma topologia em estrela. São aplicações que se beneficiam dessa topologia: sistemas domésticos de alarmes ou de substituição de cabos. Nestas redes o controlador da comunicação é denominado coordenador, e toda a comunicação é feita por meio deste. As topologias em estrela podem operar em CSMA/CA sem *slots* ou com *slots* (chamado de *beacon-mode*).

Redes multi-saltos: nestas redes todos os dispositivos são FFDs, e se comunicam diretamente ou utilizando uma comunicação multi-salto. São redes onde os dispositivos formam uma rede ad hoc, como em redes de sensores. O método de acesso ao meio empregado é o CSMA/CA.

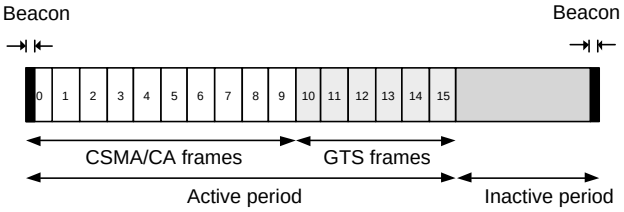

Figura 7: Estrutura de *superframe* utilizada no 802.15.4 em *beacon-mode*.

As redes em estrela possuem mecanismos adicionais para poupar energia. Um deles é o *beacon-mode*. Neste modo de operação, o coordenador estabelece uma janela chamada de *superframe*, mostrada na figura 7, que divide o tempo em intervalos (ou *slots*). Periodicamente o coordenador envia uma mensagem de sincronização chamada de *beacon*, que determina o início de um *superframe*, tamanho e número de *slots*. O acesso ao *slot* é por contenção, utilizando o método CSMA/CA, ou alocados para um nó específico, chamado de *Guaranteed Time Slot* (ou GTS). O GTS permite qualidade de serviço no controle de acesso ao meio. O *beacon-mode* também determina um período de inatividade, onde todos os nós desligam o seu rádio. Por fim, o coordenador pode estabelecer uma forma indireta de comunicação, permitindo ainda maior economia de energia pelos dispositivos escravos. Neste modo, o coordenador anuncia a cada início de *super-*

Protocolos	Data	Projetos/ Universidades	Plataforma	Alocação de canais	Técnicas Comunicação	Notificação	Capacidade Adaptação	QoS
S-MAC	2001	SCADDS/ USC-IS	Mica Motes	M - CSMA/CA	H	ESC-S	AUTO	não
ARC	2001	University of California Berkeley	Mica Motes	M - CSMA/CA	ALT	ESC-S	AUTO	não
T-MAC	2003	University of Technology The Netherlands	EYES	M - CSMA/CA	H	ESC-S	AUTO	não
B-MAC	2003	UCLA/USC/UCB/IR	Mica Motes	M - CSMA/CA	ALT	ESC-A	RECON	não
DE-MAC	2003	Louisiana State University	Simulação	M-TDMA	ESN	RES	EST	não
TRAMA	2003	i-NRG/UC Santa Cruz	Simulação	M-TDMA	ESN	RES	AUTO	não
IEEE 802.15.4	2004	IEEE/Zig Bee Alliance	Mica Motes	M-CSMA/CA	H	RES	AUTO	sim

Tabela 4: Classificação dos protocolos.

frame uma lista de dados pendentes, utilizando uma mensagem de *beacon*. Os dados são armazenados até que o nó requisite explicitamente o seu recebimento, permitindo assim que os dispositivos liguem o rádio esporadicamente para consultar se existem quadros a serem recebidos.

O padrão IEEE 802.15.4 também especifica mecanismos de auto-organização da rede, que permitem a um dispositivo detectar as redes presentes e ajustar a sua operação, além de prever extensões de segurança (detalhadas na seção 5).

Zheng e Lee analisaram o desempenho do IEEE 802.15.4 [Zheng and Lee, 2004]. Neste estudo verificou-se que, apesar de não utilizar reserva de canal, o 802.15.4 possui uma degradação de desempenho ocasionada pelo problema do terminal escondido, mas que é negligenciável para redes com baixas taxas de dados. O estudo mostra que a utilização do meio sem reserva anterior permite uma diminuição na latência, apesar do aumento das colisões. Verificou-se que, mesmo com *superframes* muito longos, que permitem ao nó desligar o rádio por períodos prolongados, a perda de sincronização é rara, e quando acontece o nó rapidamente se associa novamente à rede.

O IEEE 802.15.4 define um padrão a ser adotado por vários fabricantes. Atualmente existem poucas implementações, mas seu uso tende a aumentar devido ao seu emprego na arquitetura ZigBee [Zigbee Alliance, 2005], apoiada por vários fabricantes de dispositivos embutidos.

4.8 Classificação dos protocolos em RSSF

Os protocolos descritos na seção anterior são classificados de acordo com a taxonomia apresentada. A tabela 4 apresenta essa classificação em ordem cronológica de publicação [1].

5 Segurança em RSSF

O aspecto de segurança é crítico para todos os tipos de redes, e isso não é diferente para as RSSF. As aplicações nas áreas de segurança pública, militar, monitoração da saúde pública, ou mesmo em sistemas de resposta a situações de emergência como em ataques terroristas, necessitam de características como autenticidade e confidencialidade das informações trafegadas [Wood and Stankovic, 2002]. Estas funções somente podem ser implementadas com o uso de protocolos seguros.

Por se tratarem de redes que se comunicam utilizando enlaces sem fio, e que geralmente são depositadas em locais onde os nós sensores podem ser facilmente capturados, a segurança em RSSF é uma tarefa mais árdua que a segurança de redes sem fio tradicionais. O uso de técnicas de criptografia de chave pública em RSSF é proibitivo, devido ao seu custo computacional e de memória. Apesar das RSSF também estarem sujeitas à lei de "Moore"[Patterson and Hennessy, 1998], a capacidade computacional dos nós tende a se manter a mesma nos próximos anos, o que implica que as soluções de segurança sejam leves e consumam pouca memória.

A limitação de recursos conjugada com outras características das RSSF faz com que a segurança nessas redes possua características peculiares. Os principais fatores que devem ser considerados nos mecanismos de segurança das RSSFs são:

[1] **(M-CSMA/CA)** - Monocanal-CSMA/CA; **(H)** - Híbrido; **(ALT)** - Aleatório; **(ESN)** - Escalonado; **(ESC-S)** - Escuta de canal síncrona; **(ESC-A)** - Escuta de canal assíncrona;**(RES)** - Reserva;**(AUTO)** - Autoconfigurável; **(RECON)** - Reconfigurável; **(EST)** - Estático

Segurança física do nó sensor: ao contrário das redes tradicionais, onde os elementos de rede podem ser completamente confiáveis, em RSSF um inimigo pode facilmente capturar um nó sensor e assim obter as chaves e outras informações sigilosas armazenadas. As soluções desenvolvidas devem considerar que qualquer nó da rede pode estar comprometido.

Mecanismos de segurança "leves": devido às restrições severas dos nós sensores, geralmente são utilizados algoritmos de chave simétrica, com chaves menores que as utilizadas correntemente na Internet [Perrig et al., 2001]. Além disto, a adição de alguns bytes nos quadros enviados pode diminuir a vazão da rede, o que impossibilita o uso de soluções tradicionais como WEP, IEEE 802.11i, IPSEC e outros [Karlof et al., 2004]. Para não onerar o nó sensor, protocolos seguros devem ser configuráveis tal que as aplicações utilizem apenas o nível mínimo de segurança necessário [Law et al., 2003]. Por fim, a quantidade de dados armazenada pelos sensores deve ser minimizada, justificando o uso de chaves de grupos ou um conjunto de chaves selecionadas aleatoriamente [Chan et al., 2004]. O uso dessas estratégias limita a conectividade dos nós.

Fusão e agregação de dados: para que o nó realize a agregação de dados é necessário que estes sejam decriptografados a cada hop da comunicação. Como discutido por Karlof et al., esse mecanismo impede o uso de criptografia fim-a-fim [Karlof et al., 2004]. Assim, soluções de criptografia ponto a ponto são preferíveis.

Restrições de energia e banda: a transmissão de dados falsos ou indesejáveis até o PA consome recursos da rede. Logo, a detecção de informação falsa deve ser feita o mais breve possível para evitar o consumo de tais recursos [Karlof et al., 2004]. Dessa forma, as soluções de criptografia devem ser distribuídas e aplicadas em cada salto da comunicação, estratégia oposta à empregada em outras redes.

Os dois últimos mecanismos de segurança mostram a importância do uso de soluções de segurança na camada de enlace. Essa camada deve prover confidencialidade e autenticação dos dados, enquanto camadas superiores se preocupam com outras questões de segurança, como a gerência de chaves[Karlof et al., 2004, Sastry and Wagner, 2004].

As principais funções empregadas nas soluções de criptografia são: transmissão segura de dados unicast [Karlof et al., 2004, Sastry and Wagner, 2004], multicast e broadcast seguros [Perrig et al., 2001] e gerência de chaves [Eschenauer and Gligor, 2002]. Os aspectos relacionados à primeira solução são geralmente abordados no controle de acesso ao meio. As demais soluções são em geral, implementadas nas camadas de rede e aplicação. Os principais protocolos que implementam segurança na camada de enlace em RSSF são o TinySec e o IEEE 802.15.4.

5.1 TinySec

O protocolo TinySec é a solução mais popular de segurança em controle de acesso ao meio [Karlof et al., 2004], sendo atualmente implementado na plataforma Mica Motes. Esta solução provê garantias de integridade e confidencialidade de dados unicast, sendo modular e configurável. O TinySec permite a troca do algoritmo criptográfico utilizado, e também permite que a aplicação envie mensagens com apenas integridade ou confidencialidade e integridade. Além disto, esta solução pode ser usada com qualquer protocolo de gerência de chaves, aumentando assim a sua flexibilidade.

O TinySec emprega chaves de 64 bits [2], e utiliza algoritmos criptográficos compatíveis com nós sensores, selecionados de forma a reduzir consumo de energia. O protocolo mostrou-se extremamente eficiente, aumentando o tamanho de pacote em somente 3 bytes, e requerendo custo adicional de 10% de energia.

5.2 IEEE 802.15.4

O padrão IEEE 802.15.4 especifica um protocolo de controle de acesso ao meio com solução integrada de segurança para redes sem fio de baixo consumo de energia.

O mecanismo de segurança é bastante inovador e utiliza criptografia AES[3] embutida no próprio rádio, com suporte a chaves de 32, 64 e 128 bits [Sastry and Wagner, 2004]. A implementação de criptografia no próprio rádio desonera o microcontrolador,

[2] Também é empregado um IV (parâmetro da função de criptografia) de 64 bits para cada chave, construído com informações do pacote enviado e um contador de 16 bits

[3] O AES é o padrão recomendado atualmente pelo governo americano como o mais seguro para criptografia de chave simétrica

e permite que o usuário tenha apenas que se preocupar com a gerência das chaves.

Além do modo sem segurança, o padrão especifica três modos seguros de operação fornecendo confidencialidade, integridade ou ambos. O IEEE 802.15.4 ainda especifica listas de controle de acesso (ACL), permitindo que o nó se comunique com até 255 configurações diferentes de criptografia, variando desde as chaves utilizadas até o modo de operação. Esse padrão também permite o uso de um contador em cada pacote, evitando ataques de *replay* (reenvio de uma mensagem verdadeira, na tentativa de burlar o sistema).

Apesar de ser um padrão robusto que emprega métodos de criptografia de última geração, Sastry e Wagner mostraram problemas na especificação do padrão e na sua implementação nos rádios atuais [Sastry and Wagner, 2004]. Tais problemas levariam a potenciais falhas na segurança, sendo propostas algumas soluções pelos autores.

6 Desafios em MAC para RSSF

Muitos desafios e necessidades devem ser tratados para prover tanto um bom funcionamento quanto desenvolvimento de aplicações em RSSF. Alguns desses desafios devem ser previstos no projeto dos protocolos MAC, no desenvolvimento de novos hardware e de novas aplicações. Uma breve discussão sobre esses desafios é apresentada a seguir, focando os aspectos de hardware, software e ferramentas de simulação.

Sensores: a monitoração de fenômenos naturais, químicos e biológicos dependem do desenvolvimento de novos sensores que possuam tamanho reduzido e menor consumo de energia. Aplicações médicas no monitoramento de pessoas, por exemplo, necessitam de sensores intrusivos. Logo, nas próximas gerações, os sensores deverão ser extremamente pequenos, não tóxicos e oferecer uma alta precisão nas medidas. Essa precisão irá modificar o tráfego da rede, mudando os métodos de tratamento de fusão e agregação de dados, o que impacta diretamente no projeto de protocolos MAC.

Atuadores: inúmeras aplicações em RSSF além de monitorar eventos necessitam atuar e intervir no ambiente. Em aplicações médicas, por exemplo, um paciente monitorado a distância que necessite de alguma medicação poderia ser medicado via atuadores. Nesse caso, os dados obtidos pelos nós sensores deverão oferecer alta precisão, confiabilidade, baixa latência a comandos, além de não produzirem falsos alarmes. Em particular esses aspectos implicam diretamente no projeto de protocolos MAC.

Rádios reconfiguráveis: rádios reconfiguráveis permitirão um ajuste fino de parâmetros de rede como freqüência de operação, largura de banda, número de canais e técnicas de modulação. Estes parâmetros permitirão ao nó sensor uma maior adaptabilidade ao ambiente. Para tanto, é necessário que os protocolos de comunicação, em especial o MAC, possuam mecanismos de negociação de parâmetros entre nós, bem como algoritmos de autodiagnóstico que identifiquem quando e como os parâmetros do rádio devem ser alterados.

Protocolos: qualidade de serviço e segurança são requisitos que os novos protocolos MAC necessitam prover além da economia de energia. Protocolos projetados para redes dirigidas a eventos e que utilizem atuadores devem prover mecanismos para tomada de decisão. Para tal, os nós sensores terão propriedades autonômicas, sendo capazes de realizar autoconfiguração, autogerenciamento e promoverem a autonegociação de parâmetros na rede. Controlar a qualidade do enlace na comunicação por meio de variação de potência do rádio é uma abordagem interessante a ser considerada nos novos protocolos MAC.

Ferramentas de simulação: simuladores que reflitam os conceitos reais das RSSF, de fato, ainda não existem. A representação das características do meio de transmissão, como por exemplo ruídos na propagação de sinais, não estão integradas nas ferramentas de simulação. Tais características viabilizam a percepção do funcionamento de protocolos MAC em cenários reais.

Caracterização da carga de uma RSSF em diversos cenários: por não existir uma caracterização da carga em RSSF, o projeto de protocolos para estas redes se torna um desafio. O projetista deve definir um conjunto de premissas em relação ao tráfego da rede, para que possa avaliar ou desenvolver o seu protocolo. Muitas dessas premissas podem ser inválidas em RSSF reais, impedindo a aplicação prática do protocolo. Com a caracterização do tráfego de um conjunto de aplicações, um projetista pode, a partir do cenário alvo, desenvolver protocolos que são otimizados para um cenário, sem para tanto recorrer as premissas do

comportamento da rede. Para gerar esta caracterização é necessário a análise de um grande número de RSSF em produção. Isto será possível somente com o aumento dessas redes instaladas, que atualmente são poucas.

7 Conclusões

O consumo excessivo de energia no elemento de rede ainda é uma grande restrição na implementação de RSSF. Pesquisas têm sido realizadas para o desenvolvimento de novos dispositivos eletrônicos que consumam menos energia, utilizando modos de gerenciamento de energia e variação de potência do sinal transmitido. Das tarefas de um nó sensor, a comunicação é a que consome maior energia , sendo que os protocolos MAC em especial influenciam fortemente no consumo. Assim, os protocolos MAC tem como meta a economia de energia, obtida as custas de negociar vazão e latência por energia.

O consumo de energia, entretanto, não é o único requisito a ser considerado. Aplicações podem demandar da rede um serviço confiável, impondo requisitos de segurança, qualidade de serviço, tolerância a falhas, escalabilidade e autoconfiguração. Para nortear o desenvolvimento de protocolos que sigam estas características, apresentamos uma taxonomia de protocolos MAC que considera esses requisitos.

A taxonomia, baseada em técnicas propostas para protocolos em redes sem fio, categoriza os protocolos de acordo com os mecanismos de alocação do canal, coordenação da comunicação, notificação de envio dos dados, adaptabilidade e qualidade de serviço. Utilizamos esta taxonomia para classificar os protocolos existentes.

É importante observar que não existe um protocolo MAC que atenda às necessidades de todas as aplicações, portanto novos mecanismos serão desenvolvidos nos próximos anos. A evolução do hardware permitirá o emprego de rádios reconfiguráveis e de outras tecnologias tais como CDMA e UWB (Ultra Wide Band) também irão contribuir para modificar os métodos empregados em protocolos de controle de acesso bem como a taxonomia proposta.

Referências

[Agarwal et al., 2001] Agarwal, S., Krishnamurthy, S., Katz, R., and Dao, S. (2001). Distributed power control in ad hoc wireless networks. In *Personal and Indoor Mobile Radio Communication – (PIMRC)*, volume 2, pages 59–66. IEEE.

[Agilent Technologies, 2004] Agilent Technologies (2004). Data Sheet Agilent Technologies Infrared Products. http://cp.literature.agilent.com/litweb/pdf/5989-0281EN.pdf.

[Avizienis et al., 2004] Avizienis, A., Laprie, J.-C., Randell, B., and Landwehr, C. E. (2004). Basic concepts and taxonomy of dependable and secure computing. *IEEE Trans. Dependable Sec. Comput.*, 1(1):11–33.

[Bambos and Kandukuri, 2000] Bambos, N. and Kandukuri, S. (2000). Power Controlled Multiple Access (PCMA) in Wireless Communication Networks. In *Proceedings of the IEEE International Conference on Computer Communication*, pages 386–395.

[Bhatnagar et al., 2001] Bhatnagar, S., Deb, B., and Nath, B. (2001). Service differentiation in sensor networks. In *Proceedings of the Fourth International Symposium on Wireless Personal Multimedia Communications*.

[Callaway et al., 2002] Callaway, E., Gorday, P., Hester, L., Gutierrez, J., Naeve, M., Heile, B., and Bahl, V. (2002). Home networking with IEEE 802.15.4: a developing standard for low-rate wireless personal area networks. *IEEE Communications Magazine*, 40(8):70–77.

[CC 1000, 2004] CC 1000 (2004). Chipcom corporation. CC1000 low power FSK transceiver. http://www.chipcom.com.

[CENS, 2004] CENS (2004). CENS Center for Embedded Networked Sensing. Medusa Project. http://www.cens.ucla.edu/Project-Descriptions/Sensor_Node_Platforms/.

[Chan et al., 2004] Chan, H., Perrig, A., and Song, D. (2004). Key distribution techniques for sensor networks. In *Wireless sensor networks*, pages 277–303. Kluwer Academic Publishers.

[Coelho and Agarwal, 2002] Coelho, C. M. and Agarwal, D. P. (2002.). *Mobile Ad Hoc Networking*, chapter 3, pages 125–186. SBRC 2002.

[Crossbow, 2004] Crossbow (2004). Mica2: Wireless Measurement System. http://www.xbow.com.

[Dewasurenda and Mishra, 2004] Dewasurenda, D. and Mishra, A. (2004). Design Challenges in Energy-Efficient Medium Access Control for Wireless Sensor Networks. In Ilyas, M. and Mahgoub, I., editors, *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*, volume 1, chapter 28. CRCPress LLC., Flórida, FL, USA. ISBN 0-8493-1968-4.

[Dust, 2004] Dust, S. (2004). Smart Dust: Autonomous sensing and communication in a cubic millimeter. http://robotics.eecs.berkeley.edu/∼pister/SmartDust.

[Eschenauer and Gligor, 2002] Eschenauer, L. and Gligor, V. D. (2002). A key-management scheme for distributed sensor networks. In *Proceedings of the 9th ACM conference on Computer and communications security*, pages 41–47. ACM Press.

[F. Dai and J. Wu, 2004] F. Dai and J. Wu (2004). Energy-Efficient Coverage Problems in Wireless Ad Hoc Sensor Networks. *Journal of Computer Communications on Sensor Networks*.

[GATECH, 2004] GATECH (2004). Sensonet project: Protocols for sensor networks. http://users.ece.gatech.edu/ weilian/Sensor/index.html.

[Heinzelman et al., 2000] Heinzelman, W. R., Chandrakasan, A., and Balakrishnan, H. (2000). Energy-Efficient Communication Protocol for Wireless Microsensor Networks. In *IEEE Proceedings of the Hawaii International Coference on System Sciences*, pages 4–13.

[Hubert, 2004] Hubert, S. (2004). MALT - Motorized Active Laser Transceiver. http://www-bsac.eecs.berkeley.edu/∼ mattlast/research/laser_turret.html.

[Jianliang Zheng and Lee, M.J., 2004] Jianliang Zheng and Lee, M.J. (2004). Will IEEE 802.15.4 make ubiquitous networking a reality?: a discussion on a potential low power, low bit rate standard. *IEEE Communications Magazine*, 42(6):277–288.

[JPL, 2002] JPL (2002). JPL Sensor Webs. http://sensorwebs.jpl.nasa.gov/.

[Kalidindi et al., 2003] Kalidindi, R., Ray, L., Kannan, R., and Iyengar., S. (2003). Distributed Energy Aware MAC Layer For Wireless Sensor Networks. In *International Conference on Wireless Networks*, Las Vegas, Nevada.

[Karlof et al., 2004] Karlof, C., Sastry, N., and Wagner, D. (2004). TinySec: a link layer security architecture for wireless sensor networks. In *Proceedings of the 2nd international conference on Embedded networked sensor systems*, pages 162–175. ACM Press.

[Karn, 1990] Karn, P. (1990). A New Channel Access Protocol for Packet Radio. In *American Radio Relay League – 9thComputer Networking Conference*.

[Langendoen and Halkes, 2005] Langendoen, K. and Halkes, G. (2005). *Embedded Systems Handbook*. R. Zurawski - a ser publicado.

[Law et al., 2003] Law, Y. W., Etalle, S., and Hartel, P. H. (2003). Assessing Security-Critical Energy-Efficient sensor networks. In Gritzalis, D., di Vimercati, S. D. C., Samarati, P., and Katsikas, S. K., editors, *18th IFIP TC11 Int. Conf. on Information Security, Security and Privacy in the Age of Uncertainty (SEC)*, pages 459–463, Athens, Greece. Kluwer Academic Publishers, Boston.

[Loureiro et al., 2003] Loureiro, A. A. F., Nogueira, J. M. S., Ruiz, L. B., de Freitas Mini, R. A., Nakamura, E. F., and Figueiredo, C. M. S. (2003). Redes de sensores sem fio. In *Simpósio Brasileiro de Redes de Computadores*, pages 179 – 226.

[Lu et al., 2002] Lu, C., Blum, B. M., Abdelzaher, T. F., Stankovic, J. A., and He, T. (2002). RAP: A real-time communication architecture for large-scale wireless sensor networks. In *Proceedings of the Eighth IEEE Real-Time and Embedded Technology and Applications Symposium*, page 55. IEEE Computer Society.

[Meguerdichian et al., 2001] Meguerdichian, S., Koushanfar, F., Qu, G., and Potkonjak, M. (2001). Exposure in wireless ad-hoc sensor networks. In *MobiCom '01: Proceedings of the 7th annual international conference on Mobile computing and networking*, pages 139–150. ACM Press.

[Millennial Net, 2004] Millennial Net (2004). Millennial net: Wireless sensor networks. http://www.millennial.net.

[Monks, 2001] Monks, J. P. (2001). *Transmission Power Control for Enhancing the performance of wireless packet data networks.* Doctor of philosophy, University of Illinois at Urbana-Champaign.

[Motes, 2002] Motes, M. (2002). The commercialization of microsensor motes. http://www.sensorsmag.com.

[μAMPS, 2002] μAMPS (2002). μAMPS Projet. http://www-mtl.mit.edu/research/icsystems/uamps.

[Patterson and Hennessy, 1998] Patterson, D. A. and Hennessy, J. L. (1998). *Computer Organization and Design (2nd ed.): the hardware/software interface.* Morgan Kaufmann Publishers Inc.

[Perrig et al., 2001] Perrig, A., Szewczyk, R., Wen, V., Culler, D., and Tygar, J. D. (2001). SPINS: security protocols for sensor networks. In *Proceedings of the 7th annual international conference on Mobile computing and networking*, pages 189–199. ACM Press.

[Peterson and Davie, 2003] Peterson, L. L. and Davie, B. S. (2003). *Computer Networks: A Systems Approach, 3rd Edition.* Morgan Kaufmann Publishers Inc.

[Pico, 2003] Pico (2003). Pico Radio. http://bwrc.eecs.berkeley.edu/Research.

[Polastre et al., 2004] Polastre, J., Hill, J., and Culler, D. (2004). Versatile low power media access for wireless sensor networks. In *Proceedings of the 2nd international conference on Embedded networked sensor systems*, pages 95–107. ACM Press.

[Pottie and Kaiser, 2000] Pottie, G. J. and Kaiser, W. J. (2000). Wireless integrated network sensors. *Communications of the ACM*, 43(5):51–58.

[Pradhan, 1996] Pradhan, D. K., editor (1996). *Fault-tolerant computer system design.* Prentice-Hall, Inc.

[Rajendran et al., 2003] Rajendran, V., Obraczka, K., and Garcia-Luna-Aceves, J. J. (2003). Energy-efficient collision-free medium access control for wireless sensor networks. In *Proceedings of the first international conference on Embedded networked sensor systems*, pages 181–192. ACM Press.

[Ruiz et al., 2003] Ruiz, L. B., Nogueira, J. M. S., and Loureiro, A. A. F. (2003). Functional and Information Models for the MANNA Architecture. *Colloque Francophone sur la Gestion de Reseaux et de Services*, pages 455–470.

[Sankarasubramaniam et al., 2003] Sankarasubramaniam, Y., Özgür B. Akan, and Akyildiz, I. F. (2003). ESRT: event-to-sink reliable transport in wireless sensor networks. In *Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing*, pages 177–188. ACM Press.

[Sastry and Wagner, 2004] Sastry, N. and Wagner, D. (2004). Security considerations for IEEE 802.15.4 networks. In *Proceedings of the 2004 ACM workshop on Wireless security*, pages 32–42. ACM Press.

[Schurgers et al., 2002] Schurgers, C., Tsiatsis, V., Ganerival, S., and Srivastava., M. (2002.). Optimizing sensor networks in the energy-latency-density space. In *IEEE Transactions on Mobile Computing, 1(1):*, pages 70–80.

[Tanenbaum, 2003] Tanenbaum, A. S. (2003.). *Computer networks.* Prentice Hall PTR, 4 ed. edition.

[Tilak et al., 2002] Tilak, S., Abu-Ghazaleh, N. B., and Heinzelman, W. (2002). Infrastructure Tradeoffs Sensor Networks. In ACM, editor, *First International Workshop on Wireless Sensor Networks and Applications*, Electrical and Computer Engineering.

[TR 1000, 2004] TR 1000 (2004). ASH Tranceiver TR1000 data sheet. http://www.rfm.com.

[van Dam and Langendoen, 2003] van Dam, T. and Langendoen, K. (2003). An Adaptive Energy-efficient MAC protocol for wireless ensor networks. In *Proceedings of the first international conference on Embedded networked sensor systems*, pages 171–180. ACM Press.

[van Hoesel et al., 2003] van Hoesel, L., Chatterjea, S., and Havinga., P. (2003). An energy efficient medium access protocol for wireless sensor networks. In *ProRisc Workshop.*

[Velloso et al., 2004] Velloso, P., Cunha, D., Junior, A. A., Rubinstein, M., and Duarte, O. C. M. B. (2004). Redes Domiciliares: Princípios e Desafios das Tecnologias sem Novos Fios. In *22nd Simpósio Brasileiro de Redes de Computadores*, pages 221 – 268.

[Vieira, 2004] Vieira, M. A. M. (2004). Embedded system for wireless sensor network. Master's thesis, Departamento de Ciência da Computação, Universidade Federal de Minas Gerais, Belo Horizonte-MG, Brasil.

[Walke et al., 2001] Walke, B., Esseling, N., Habetha, J., Hettich, A., Kadelka, A., Mangold, S., Peetz, J., and Vornefeld, U. (2001). IP over Wireless Mobile ATM - Guaranteed Wireless QoS by HiperLAN/2. *Proceedings of the IEEE*, 89:21–40.

[WINS, 2003] WINS (2003). Wireless Integrated Network Sensors (WINS). http://www.janet.ucla.edu/WINS/.

[Woo and Culler, 2001] Woo, A. and Culler, D. E. (2001). A transmission control scheme for media access in sensor networks. In *Mobile Computing and Networking*, pages 221–235.

[Wood and Stankovic, 2002] Wood, A. D. and Stankovic, J. A. (2002). Denial of service in sensor networks. *Computer*, 35(10):54–62.

[Xiao, 2004] Xiao, Y. (2004). IEEE 802.11e: A QoS Provisioning at the MAC layer. *IEEE Wireless Communications*, 11(3):72–79.

[Ye et al., 2002] Ye, W., Heidemann, J., and Estrin, D. (2002). An Energy-Efficient MAC protocol for Wireless Sensor Networks. In *Proceedings of the IEEE International Conference on Computer Communication*, pages 1567–1576, New York, NY, USA. USC/Information Sciences Institute, IEEE.

[Younis et al., 2004] Younis, M., Akkaya, K., Eltoweissy, M., and Wadaa, A. (2004). On handling qos traffic in wireless sensor networks. In *Proceedings of the 37th Annual Hawaii International Conference on System Sciences - Track 9*, page 90292.1. IEEE Computer Society.

[Zheng and Lee, 2004] Zheng, J. and Lee, M. J. (2004). A Comprehensive Performance Study of IEEE 802.15.4.

[Zigbee Alliance, 2005] Zigbee Alliance (2005). ZigBee Alliance Reaches Major Milestone Toward A Global Interoperable Standard. http://www.zigbee.com.