

Redes Sem Fio de Sensores

IE708 - Comunicações Móveis

Fernando Contrera - ra085568
Francisco E. de Andrade Leite - ra945242
Pedro Henrique Gomes da Silva - ra024844

22 de julho de 2008

1 Introdução

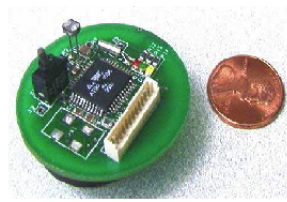
O avanço recente em comunicações sem-fio e eletrônica, principalmente na indústria de semi-condutores que a cada ano permite a redução do tamanho de um chip e aumento da sua capacidade de processamento, efeito da Lei de Moore, levou pesquisadores e indústria a conceber pequenos componentes eletrônicos de capacidade computacional limitada, porém de custo relativamente barato.

Estes componentes, empregando tecnologia MEMS (micro-eletromecanical systems - vide exemplo na figura 1), podem então ser utilizados em larga escala sobre uma área ou fenômeno físico nos quais a realização de algum de tipo de monitoração ou medição se faz necessário. Sua capacidade de processamento e transmissão de dados, aliadas a técnicas de software, permitem a elaboração de uma rede sem fio de sensores cujas características permitem pensar sua aplicação em um vasto campo de atividades, a saber:

- Militar: monitorar e rastrear forças amigas e inimigas, vigiar campo de batalha e fronteiras;
- Médico: monitorar dados de pacientes;
- Vigilância: monitorar pessoas em um prédio ou carros na estrada;
- Ambiental: aviso preliminar de enchentes, monitorar clima e animais;
- Industrial: monitorar inventário;
- Concessionárias: adquirir dados de casas e equipamentos.

Dados as possíveis situações de uso e suas características, podemos pensar que uma rede de sensores é concebida de forma que: sua operação seja desassistida, seu funcionamento seja independente de fonte externa de energia, esteja sujeita às intempéries causadas pelo provável uso em ambientes hostis e seu efeito na capacidade de conectividade da rede. Percebe-se ainda que esta possui uma elevada interatividade com outros nós. Isso cria então uma série de desafios no campo da ciência da informação, que serão tratados mais adiante.

Para melhor elaborar alguns dos problemas e aplicações deste tipo de rede, é importante criar uma definição mais formal do que é uma rede de sensores, que serve como conceito de referência.



UC Berkeley Motes



MIT μ AMPS-I node

- 19.1 Kbps
- 20m Range
- Light Sensing
- Temperature Sensing
- 4 MHz – 3.0 V
- 8 Kbytes –Program Memory
- 512 Bytes – Data Memory
- Available from: CrossBow Inc. \$900 for a complete kit

Figura 1: Exemplo de nó sensor.

1.1 Definição e Arquitetura

Uma rede de sensores é composta de um grande número de elementos de sensoriamento, densamente empregados próximos ou dentro do objeto que se deseja monitorar, cujas características básicas são:

- Emprego aleatório;
- Capacidade de cooperação;
- Sistema auto-organizável;
- Uso limitado de energia.

Neste tipo de rede a comunicação se dá basicamente por saltos: "multihop", situação em que cada nó, potencialmente, participa do roteamento de dados transmitidos por nós próximos ou vizinhos. Assim, a informação que se deseja transmitir vai passando de nó em nó até chegar a um nó coletor, responsável por repassar todos os dados para uma rede externa ou outra rede de nós, conforme se pode observar na figura 2. Dessa forma, podemos perceber que não só uma rede de sensores pode conter nós distribuídos de forma hierarquizada como também tem uma grande semelhança com uma rede Ad Hoc, diferindo, porém desta última em alguns itens, a saber:

- O número de elementos em uma rede de sensores é muito maior do que número de elementos em um rede Ad Hoc;
- Elementos de sensoriamento são empregados de forma a permitir cobertura integral do objeto monitorado;
- São limitados em potência, capacidade computacional e memória;
- Elementos são sujeitos a falhas;
- A topologia de rede de um rede de sensoriamento muda frequentemente;
- Elementos usam comunicação por broadcast;

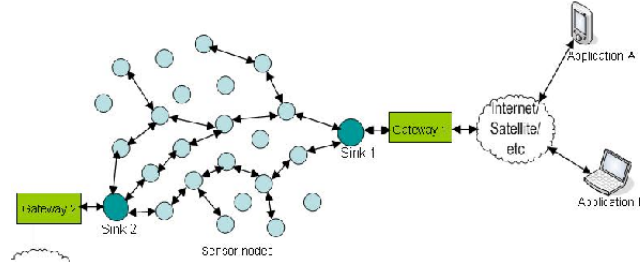


Figura 2: Topologia de uma rede de sensores genérica.

- Não necessitam de um identificador global no sistema, caso em que o sensor é acessado através da medida que se deseja ler, ao invés de um identificador do nó na rede.

A figura 2 ilustra uma topologia genérica para uma rede de sensores, cujo design é influenciado por diversos fatores, dos quais, podemos destacar os seguintes:

- Tolerância a falhas;
- Escalabilidade;
- Emprego da topologia da rede de sensores;
- Ambiente;
- Meio de transmissão (RF ou Infra-Vermelho);
- Consumo de energia;
- Restrições de hardware.

A tolerância a falhas é um requisito que impõe à rede de sensores a necessidade de manter suas funções mesmo que alguns de seus elementos apresentem falhas. Essa tolerância a falha ou confiabilidade de um nó de rede pode ser modelada segundo uma distribuição de Poisson [8].

Uma vez que o número de nós neste tipo de rede é elevado, a consideração sobre seu número é importante para correto dimensionamento, levando-se em consideração o fenômeno que se deseja estudar e o fato de que o excesso de elementos de sensoriamento não necessariamente irão melhorar a qualidade das medições, apesar de que um número excedente de sensores poder prover uma capacidade de backup à rede. [8] menciona uma medição que relaciona o número de sensores total N localizados em um área A , em relação ao número de sensores μ dentro de um raio de transmissão R , nesta área, tal que:

$$\mu = \frac{N\pi R^2}{A} \quad (1)$$

Este valor ainda que resulte aproximado, serve para dar idéia do número de sensores necessários. Valor este útil para se coordenar a comunicação entre nós bem como verificar o custo financeiro de emprego desta rede. Cabe ressaltar

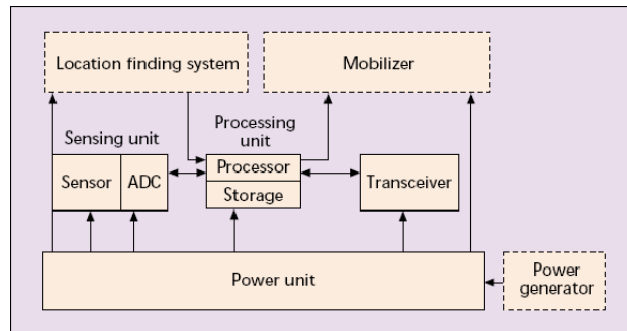


Figura 3: Diagrama de componentes de um nó sensor.

que outras formas mais apuradas de mensurar a densidade e conectividade dos elementos sensores são analisadas em [9].

A própria densidade do número de sensores, em conjunto com as características do ambiente onde a rede será empregada, torna necessário analisar a forma de implantar essa rede e sua gerência, dessa forma, a literatura cita três fases distintas de implantação:

- Fase de pré-distribuição: Sensores podem ser distribuídos em massa ou dispostos uma a um na região de monitoramento;
- Fase de pós-distribuição: Rede de sensores pode mudar com frequência;
- Fase de re-distribuição de sensores: Adição de novos elementos causa uma re-organização da rede.

Conforme já mencionado, a rede de sensores é caracterizada pela limitação de energia de seus nós, cujos componentes que mais afetam o seu consumo são a unidade de processamento, rádio e sensoriamento, mostradas no diagrama da figura 3, que também mostra os demais componentes de hardware de um sensor: bateria, memória e conversos A/D. Adicionalmente, podem ser encontrados componentes responsáveis pela gerenciamento de localização do sensor, movimentação e geração própria de energia (ex. célula fotovoltaica).

Essa questão energética é uma dos itens mais complexos e importantes a serem levadas em consideração no design de uma rede de sensores, uma vez que para otimizar seu uso o tempo de processamento, comunicação [13], potência de envio de sinal [10] e até os protocolos de comunicação tem que ser planejados de forma a causar o menor impacto energético possível.

1.2 Arquitetura de protocolos

Em se tratando de uma rede de elementos de comunicação é necessário definir um modelo de protocolos de referência para transmissão de dados entre seus membros, conforme se observa na figura 4, cuja estrutura de camadas se assemelha ao de uma rede TCP/IP. Há que se considerar que as três primeiras camadas são as mais usadas e implementadas em uma rede de sensores, sendo que a camada de transporte e aplicação passam a ser necessárias quando se deseja integrar essa rede com uma rede externa, IP por exemplo.

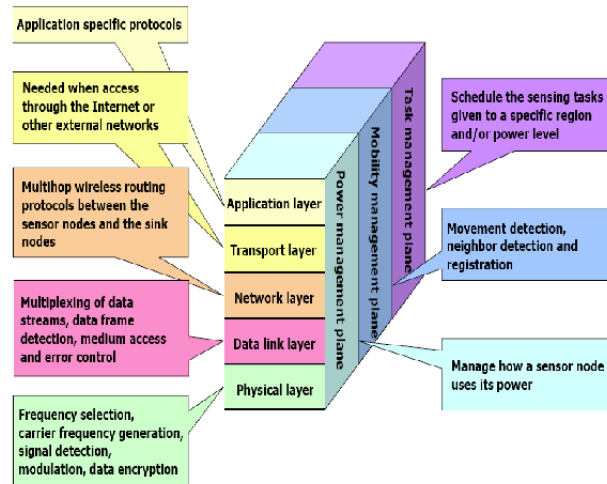


Figura 4: Pilha de protocolos Modelo OSI/ISO.

Antes de passar a uma explicação um pouco mais detalhada das camadas de protocolos cabe notar que este trabalho irá focar mais as três primeiras camadas e sua implementação em padrões de mercado que são o: IEEE802.15.4 e o ZigBee, os quais serão comentados mais adiante. Contudo a figura 4 faz a analogia entre o modelo da camada de protocolos e os padrões citados. Associados aos protocolos, três planos de gerenciamento seriam necessários à rede. A gestão de energia é necessária para por exemplo verificar os momentos em que o sensor pode ser desligado ou emitir uma mensagem de energia baixa, evitando que o sensor participe do "hop" de dados. A gestão de mobilidade ou localização visa manter conhecimento da posição do sensor na rede e a gestão de tarefa, visa a distribuir a ação de sensoriamento de nós vizinhos de forma que apenas um dos nós faça a mesma medição por vez.

1.3 Camada Física (PHY)

Essa camada é responsável pela detecção de sinais, modulação, encriptação de dados, seleção de frequência e geração de portadora. A frequência usada em geral é a da banda ISM (industrial, scientific and medical) 915 Mhz. Sendo responsável pela transmissão, seu gasto de energia deve ser controlada, levando-se em consideração que no emprego de uma rede de sensores, em geral, o coeficiente de perda de percurso está mais próximo de seu valor $\alpha = 4$. Daí que técnicas de multihopping são bastante adequadas para evitar problemas desvanecimento e sombra [8] [13], além de uma modulação eficiente como a binária. Um exemplo ilustrativo de consumo de energia para sensor elaborado em Berkeley (mote) é mostrado na figura 6 para um único ciclo Tx/Rx.

1.4 Camada Acesso ao meio (MAC)

O objetivo desta camada é estabelecer "links" de comunicação confiáveis para transmissão de dados e também o compartilhamento eficiente de recursos de comu-

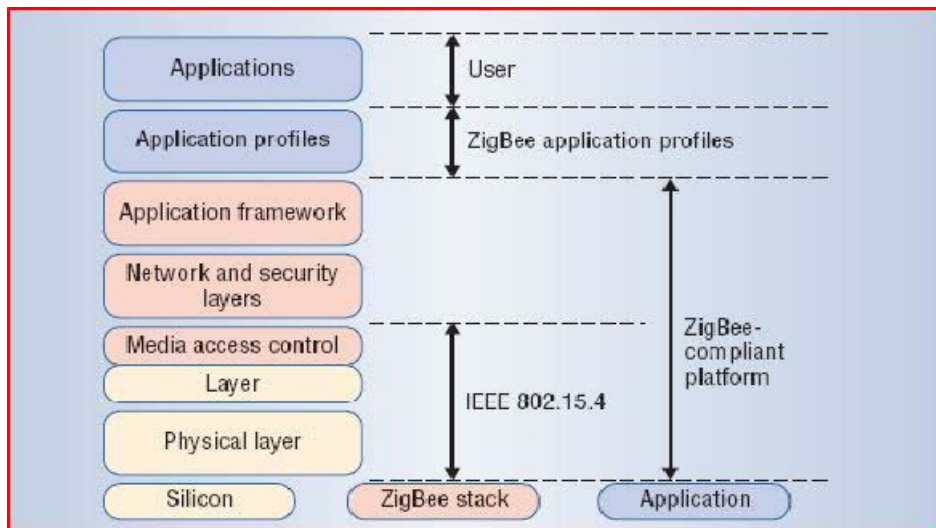


Figura 5: Protocolos de baixo nível.

- $(Q_{TX} + Q_{RX}) / T_{listen}$
- E.g. $(300 \text{ uC} + 200 \text{ uC}) / 10\text{s} = 50 \text{ uA}$

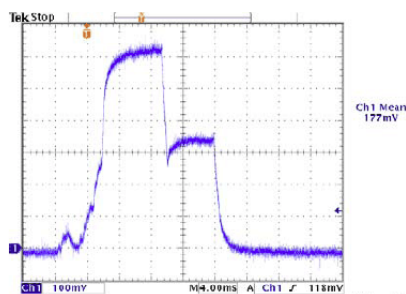


Figura 6: Consumo de energia de um sensor Mote.

nicação entre os nós da rede. O controle de erro é obtido usando mecanismo FEC ou ARQ. Usualmente, protocolos MAC para redes de comunicação sem fio não são compatíveis com redes de sensores uma vez que são voltados para garantir QoS (MANET) ou necessitarem de rádio base (celular), enquanto que em uma rede de sensores a mudança de topologia, elevado número de elementos e baixa potência de transmissão limitam demasiadamente o uso destas técnicas.

Alguns dos protocolos mais propostos na literatura são resumidos na tabela a seguir [8] [10]:

Protocolo	Modo de acesso	Particularidade em relação a rede de sensores.	Conservação de energia
SMACS/EAR	Alocação fixa de frequência e slots de tempo	Explora largura de banda em relação à quantidade de dados enviada	Rádio desligado enquanto "idle" e escuta aleatória do canal
TDMA/FDMA	Divisão por frequência e tempo fixas e direcionadas a uma rádio base, ou a um nó sensor vizinho.	Alocação ótimo do número de canais visando conservação de energia. "Frequency hopping" evita interferências.	Design customizado para eficiência energética, com sincronização de tempos de transmissão.
CSMA	Acesso aleatório por contenção de tempo		Tempo de escuta constante do canal

1.5 Camada de rede

Um protocolo dessa camada usado em redes de sensores requer algumas características básicas: capacidade de auto-configuração, capacidade de manter a rede operando por longos períodos de forma desatendida, ser tolerantes a falhas de nós de comunicação e por fim terem a propriedade de avaliar o gasto e potencial energético de cada nó [11].

Os itens a seguir resumem alguns dos protocolos de rede mencionados na literatura, que podem ser divididos em duas categorias: operação contínua e "query-reply". No primeiro, tão logo o sensor tenha dado a transmitir ele é enviado pela rede, no segundo os dados são enviados a partir de um "request" feito por uma aplicação.

1. SMECN - Cria uma sub-rede dentro da rede de sensores que contem o caminho de menor gasto energético;
2. Flooding - Faz um "broadcast" para todos os nós vizinhos;
3. Gossiping - Seleciona um nó vizinho de forma aleatória e envia o dado para o mesmo;
4. SPIN - Envia dados para um sensor apenas quando este o necessita;
5. SAR - Cria sub-árvores de roteamento cuja nó base está a um hop do nó "sink" e seleciona uma destas árvores de acordo com uma métrica de QoS e eficiência energética;

6. LEACH - Forma clusters para minimizar o gasto energético. Dados dos nós dentro de um mesmo cluster são enviados diretamente para seu master que os repassa para o nó "sink";
7. Directed diffusion - O interesse por uma informação é disseminado na rede (pelo "sink") com uma determinada frequência e armazenado pelo nós juntamente com o caminho de comunicação. Uma vez que um nó contém o dado de interesse, este dado é enviado de volta e a frequência de transmissão entre o "sink" e este nó aumenta.

1.6 Camada de Aplicação e Transporte

O uso destas camadas ainda é bem restrito em redes de sensores, tendo em vista que a camada de transporte é mais comum em situações onde é desejada a conexão com redes em que o controle das mensagens trocadas pelos seus elementos é necessário, já a camada de aplicação visa deixar ou o uso da rede de sensores transparente à aplicações responsáveis por seu gerenciamento. Como exemplo podemos citar os seguintes padrões e protocolos [8] [14].

1. 6LowPan - É um padrão que procura levar a flexibilidade da rede IP às redes de sensores, implementando assim uma camada de transporte. Porém ainda está em fase de definição;
2. SMP - É um protocolo de aplicação que visa prover recursos administrativos à rede de sensores, tais como localização, acesso por atributo, ligar e desligar o sensores, movimentar o sensor, entre outras tarefas;
3. SQDDP - Este protocolo de aplicação visa facilitar a disseminação de mensagem requisitando determinado dado ou informando a disponibilidade na rede de sensores de uma medição de interesse a determinada aplicação.

2 IEEE 802.15

O IEEE (Institute of Electrical and Electronics Engineers) é uma associação de empresas e profissionais na área de engenharia elétrica que, dentre outros diversos trabalhos, desenvolve padrões para redes sem fio que são amplamente adotados pela indústria e academia. O grupo de estudos responsável pelo desenvolvimento de padrões de redes é o grupo 802. São exemplos de padrões desenvolvidos pelo IEEE o 802.3 (Ethernet), o 802.5 (Token-Ring), 802.11 (Wifi) e o 802.16 (WiMax).

O grupo de trabalho 802.15 da IEEE dedica-se ao desenvolvimento de padrões para redes sem fio pessoais (WPAN), ou seja, redes de curto alcance para aplicações específicas. Diferente dos grupos de trabalho 802.11 e 802.16, o grupo 802.15 desenvolve padrões para tecnologias com requisitos distintos e, por isso, apresenta diversas subdivisões, ou subgrupos de trabalho, que possuem enfoques diferentes e desenvolvem padrões para redes sem fio pessoais que podem ser utilizadas em diferentes tipos de aplicações.

O subgrupo 802.15.1 desenvolve a especificação utilizada como base para as redes Bluetooth, de curto alcance e baixa taxa de dados, que tem como objetivo a interconexão de diversos dispositivos pessoais.

O subgrupo 802.15.3 desenvolve o padrão UWB (UltraWide Band) que é utilizado para aplicações multimídia que requerem alta taxa de dados – ordem de Gbps – em curtas distâncias.

Finalmente, o subgrupo 802.15.4 desenvolve padrões para redes sem fio de sensores, que exigem baixas taxas de dados e grande cobertura, além de ser uma rede com diferentes requisitos de consumo, topologia e custo. Os padrões desenvolvidos pelo subgrupo 802.15.4 são utilizados como base para pilhas de protocolos de alto nível largamente difundidas na indústria, como a pilha ZigBee.

3 IEEE 802.15.4

O padrão IEEE 802.15.4 especifica as camadas física (PHY) e controle de acesso ao meio (MAC) do modelo ISO/OSI para redes sem fio pessoais de baixa taxa de dados (low rate wireless personal area network - LR-WPAN). A primeira versão do padrão foi publicada em 2003 (IEEE 802.15.4-2003) e a última e mais atual versão foi publicada em 2006 (IEEE 802.15.4-2006). O padrão 802.15.4 é a base para outros padrões de pilhas de protocolos de alto nível, como o ZigBee e o 6LoWPAN.

A arquitetura provida pelo padrão IEEE 802.15.4 oferece recursos para a implantação de redes de baixíssimo custo, baixa taxa de dados e é focada na comunicação de dispositivos autônomos. São premissas principais desse protocolo o baixo consumo de energia, auto-organização da rede, robustez na comunicação, diversidade de topologias de redes e customização da rede.

A especificação básica das redes 802.15.4 oferece cobertura de 10 metros de raio e 250 kbps. Existem outras taxas e coberturas que são cobertas pelo padrão e podem ser utilizadas de acordo com as necessidades da aplicação a ser implementada.

As redes 802.15.4 funcionam nas bandas ISM (não-licenciadas). O mecanismo básico de controle de acesso ao meio é o CSMA/CA, mas a rede apresenta também garantia de slot times, o que torna possível a implementação de aplicações críticas, como na área médica. Os nós possuem recursos de controle de potência, como a medição da qualidade do link e a detecção de nível de energia na bateria.

3.1 Arquitetura

A pilha de protocolos que o padrão IEEE 802.15.4 se encaixa é exatamente a pilha TCP/IP. Na figura 7 é possível ver que o padrão especifica apenas as camadas inferiores da pilha, mais especificamente as camadas física e de controle de acesso ao meio. A interação com as camadas superiores da pilha TCP/IP pode ser feita através de camadas de convergência e/ou da camada LLC (*Logical Link Control*).

A camada física gerencia a transmissão dos dados no meio RF. Ela define a modulação utilizada, seleção de canal, controle de potência, largura da banda, etc. As faixas de frequência especificadas pelo padrão são mostradas abaixo:

- 868,00 – 868,80 MHz – Europa - possibilita apenas 1 canal;
- 902,00 – 928,00 MHz – América – possibilita até 10 canais, segundo o padrão de 2003; e até 30 canais, segundo o padrão de 2006;

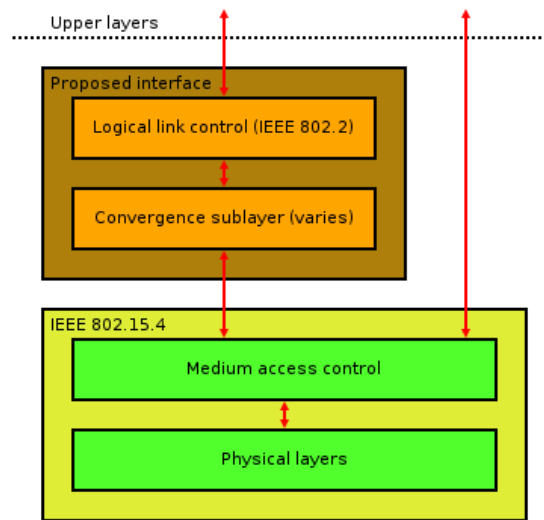


Figura 7: Pilha de protocolos IEEE 802.15.4.

- 2400,00 – 2483,50 MHz – possibilita até 16 canais.

A especificação da camada física sofreu fortes modificações do padrão original, de 2003, para o padrão mais atual, de 2006. O padrão de 2003 especifica duas versões de camada física, ambas baseadas em DSSS (Direct Sequence Spread Spectrum). A primeira versão opera nas faixas de 868/915 MHz com taxas de 20 e 40 kbps; a outra versão opera em 2450 MHz com taxa de 250 kbps.

O padrão de 2006 especifica mais 4 versões de camada física, além de aumentar a taxa das bandas 868/915 MHz para 100 e 250 kbps. As 3 primeiras novas versões de camada física baseiam-se também na abordagem DSSS, sendo as duas primeiras específicas para a banda 868/915 MHz, operando com modulação BPSK e OQPSK; a terceira é especificada para a banda 2450 MHz e opera com a modulação OQPSK. A quarta nova versão de camada física é especificada para a banda 868/915 MHz e opera com uma combinação de modulação binária e modulação por amplitude.

Diversos subgrupos de trabalho estudam a especificação de novas camadas físicas, específicas para países que possuem regulamentações diferenciadas, como a China e o Japão. Em 2007 também foram propostas 2 novas camadas físicas que utilizam Direct Sequence UWB e Chirp Spread Spectrum (CSS). A camada que utiliza Direct Sequence UWB opera em 3 bandas diferentes: abaixo de 1 GHz, entre 3 e 5 GHz e entre 6 e 10 GHz; a camada CSS opera na banda de 2450 MHz.

A camada MAC é responsável pelo controle do uso da camada física. Oferece serviços de transmissão de dados que gerencia o canal físico, garante slot times para transmissão dos dados, organiza a estrutura lógica da rede e oferece serviços de correção e segurança dos dados.

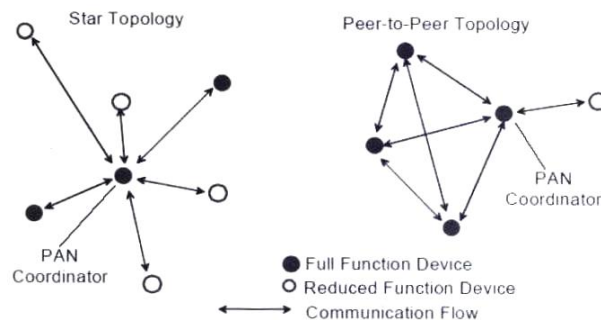


Figura 8: Topologias do padrão 802.15.4.

3.2 Estrutura da rede

Existem dois tipos de nós em uma rede 802.15.4, segundo o padrão. O primeiro tipo de dispositivo é denominado *Full-Function Device* (FFD) e o segundo é denominado *Reduced-Function Device* (RFD). Os dispositivos FFD podem operar em 2 modos: coordenador ou dispositivo da rede. Eles podem se comunicar com qualquer dispositivo da rede e, quando coordenadores, podem fazer a retransmissão de pacotes entre dois dispositivos.

Os dispositivos RFD são muito mais simples, com poucos recursos de memória e processamento; por isso eles podem se comunicar apenas com FFDs e não podem ser coordenadores da rede. Esses tipos de nós funcionam apenas como elementos sensoriais da rede e sempre como nós finais em uma comunicação.

Existem basicamente 2 topologias para as redes 802.15.4: topologia ponto-a-ponto e topologia estrela (figura 8). Na topologia estrela os nós podem se comunicar apenas com o controlador central, ou seja, o coordenador da rede. Os dispositivos da rede podem ser os pontos iniciais ou finais de uma comunicação. O coordenador da rede pode ser o ponto inicial, final, ou apenas um roteador em uma comunicação entre dois dispositivos finais. A topologia estrela pode ser utilizada em ambientes pequenos, onde todos os dispositivos da rede estão na cobertura do coordenador, como em aplicações de automação residencial.

Na topologia ponto-a-ponto qualquer nó pode se comunicar diretamente com outro nó desde que eles estejam no raio de cobertura. Esse tipo de topologia só é suportado por nós FFD, já que todos os nós da rede devem ser capazes de receber e transmitir pacotes para todos os outros nós. Tendo como base a topologia ponto-a-ponto outras topologias lógicas mais complexas podem ser obtidas, como a topologia hierárquica de cluster. A topologia ponto-a-ponto e cluster oferecem recursos para aplicações de sensoriamento agrícola, industrial, rastreamento de inventário, etc. A complexidade de implementação desse tipo de rede é maior, já que a rede precisa ser auto-organizável. Essas redes também precisam implementar algoritmos de roteamento que possibilitem múltiplos saltos para que a cobertura seja expandida. Muitos desses recursos devem ser suportados por protocolos de alto nível e estão fora do escopo do 802.15.4.

O endereçamento dos nós é feito com identificadores de 64 bits ou, em uma versão reduzida de rede, com identificadores de 16 bits. A organização de diferentes redes lógicas em um mesmo local é baseada em um identificador denominado PAN ID, que deve ser criado e gerenciado pelos coordenadores das

```

11011001110000110101001000101110
11101101100111000011010100100010
00101110110110011100001101010010
00100010111011011001110000110101
01010010001011101101100111000011
00110101001000101110110110011100
11000011010100100010111011011001
10011100001101010010001011101101
1000110010010110000001110111011
10111000110010010110000001110111
01111011100011001001011000000111
01110111101110001100100101100000
00000111011110111000110010010110
01100000011101111011100011001001
10010110000001110111101110001100
11001001011000000111011110111000

```

Figura 9: Seqüências PN utilizadas na banda 2,4 GHz.

redes.

3.3 Camada Física

Para que a implantação das redes 802.15.4 tivesse um baixo custo optou-se apenas por especificar camadas físicas que operassem na banda ISM, em 2,4 GHz e em 868/915 MHz. Conforme explicado anteriormente, o padrão de 2003 especifica 27 canais de operação, sendo 1 na faixa de 868 MHz, 10 na faixa de 915 MHz e 16 na faixa de 2,4 GHz. O padrão de 2006 estendeu esses números para 46 canais, especificando 30 canais na faixa de 915 MHz. As freqüências centrais das bandas e a largura dos canais são mostradas a seguir:

- $f_c = 868,3$ MHz, na faixa de 868 – 868,6 MHz
- $f_c = 906 + 2(k-1)$ MHz, $k = 1, \dots, 10$, na faixa de 900 MHz
- $f_c = 2405 + 5(k-1)$ MHz, $k = 11, \dots, 26$, na faixa de 2400 MHz

O padrão 802.15.4 de 2003 especifica 2 tipos diferentes de camadas físicas, ambas baseadas no DSSS. A faixa de 2,4 GHz utiliza modulação 16-ária quase-ortogonal OQPSK. E a faixa 868/915 MHz utiliza modulação binária BPSK.

Na faixa de 2,4 GHz cada 4 bits de informação são transformados em 1 seqüência de códigos PN, que será efetivamente transmitida. A seqüência PN escolhida é transmitida na portadora utilizando a modulação OQPSK (Offset Quadrature Phase Shift Keying). Os chips pares são transmitidos na portadora I e os chips ímpares são transmitidos na portadora Q, sendo que a portadora Q é defasada da portadora I por um tempo equivalente ao período de meio chip. As 16 seqüências PN são apresentadas na figura 9.

A tabela 2 apresenta um resumo das características das camadas físicas especificadas pelo 802.15.4 de 2003.

Tabela 2: Frequências de operação e taxas de dados

Banda	Chip rate	Modulação	Bit rate	Symbol rate
868-868,6 MHz	300 Kchip/s	BPSK	20 Kb/s	20 K
902-928 MHz	600 Kchip/s	BPSK	40 Kb/s	40 K
2400-2483,5 MHz	2 Mchip/s	OQPSK	250 Kb/s	62,5 K

Na faixa de 868/915 MHz a taxa de dados é de 20 kbps e 40 kbps, para as faixas 868 MHz e 915 MHz, respectivamente. A codificação de cada bit é diferencial, assim cada bit, antes de ser transmitido é submetido a uma operação XOR com o bit anterior, e o resultado é codificado em uma sequência PN de 15 chips. Se o resultado da operação XOR for 0, o bit é convertido para a sequência 111101011001000; caso for 1 a sequência é 000010100110111. Cada sequência PN resultante é transmitida com a modulação BPSK.

3.4 Camada MAC

As principais funções da camada MAC do 802.15.4 são gerenciamento de beacons, mecanismos de acesso ao canal, seleção automática de canal, recepção dos frames, reconhecimento de frames (ACK), associação, dissociação e segurança.

O controle de acesso ao meio das redes 802.15.4 pode ser feito de duas formas. Em redes sem o uso de beacons, o controle é feito através do CSMA/CA, semelhante ao mecanismo utilizado pelo 802.11 (Wifi). Em redes com beacons o mecanismo é o CSMA/CA slotado. Nesse esquema de acesso ao meio cada estação que deseja transmitir sente o canal; se o canal estiver livre ela aguarda um número aleatório de slots e começa a transmitir no próximo slot disponível. Os beacons e os ACKs são transmitidos sem o CSMA/CA.

As transmissões entre coordenador e dispositivos da rede depende se a rede é baseada em beacons ou não. Com beacons, o coordenador da rede avisa os dispositivos da existência de dados para os mesmos através dos próprios beacons; após receber a notificação, o dispositivo envia a requisição dos dados. Em redes sem beacons, os dispositivos têm a obrigação de requisitar dados; o coordenador deve manter os dados pendentes até que o destinatário faça a requisição. Em redes ponto-a-ponto, sem coordenador, o mecanismo CSMA/CA deve ser utilizado. O esquema de envio e recepção é diferente de redes convencionais, porque os dispositivos precisam economizar energia e, assim, entram em estado de dormência (sleep mode) periodicamente.

Existem 4 tipos de frames 802.15.4: frame de beacon, frame de dados, frame de ACK e frame comando MAC. Todo frame MAC consiste de um cabeçalho, um payload de tamanho variável e uma sequência de checagem de erro. O cabeçalho compreende informações de controle e endereçamento do frame; os dados são dependentes do tipo de frame e a sequência de erro implementa um código de verificação CRC de 16 bits.

Antes de iniciar a troca de dados a rede deve ser formada. As redes 802.15.4 podem ser formadas apenas por dispositivos FFD. O dispositivo que deseja iniciar uma rede e se tornar um coordenador deve fazer uma varredura passiva ou ativa. Na varredura passiva todos os canais são ouvidos e, quando não existe atividade do canal desejado o dispositivo seleciona um PAN ID adequado e

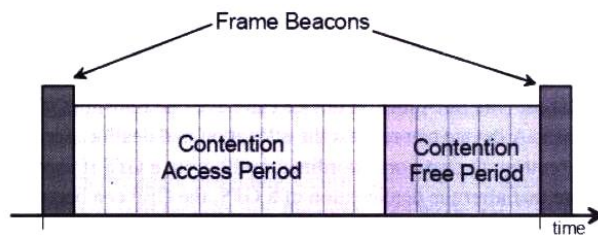


Figura 10: Período de contenção entre os beacons.

torna-se coordenador da rede. Na varredura ativa o dispositivo envia beacons e aguarda respostas de outros coordenadores; na ausência de resposta o canal é considerado vazio e o dispositivo torna-se coordenador de uma rede que passa a operar naquele canal.

Os dispositivos que querem participar de uma rede devem enviar comandos de associação e o coordenador deve verificar a disponibilidade de recursos na rede e aceitar ou não a associação do dispositivo.

O mecanismo de acesso da rede depende da existência ou não de beacons. Os beacons são transmitidos sem CSMA e fornecem informações referentes ao tamanho dos frames permitidos na rede, estado atual do coordenador da rede, tamanho dos períodos de contenção e sem contenção, etc. O período de contenção se inicia imediatamente após os beacons (figura 10). No período de contenção todos os frames, exceto os ACKs, usam o CSMA/CA para acessar o canal.

O CSMA/CA funciona da seguinte forma: a camada MAC faz uma requisição de canal livre para a camada física. A camada física ouve o canal e responde se ele está livre ou ocupado. Se não há atividade o dispositivo pode transmitir. Se existe atividade, o dispositivo deve realizar um procedimento de backoff. É escolhido um número aleatório de slots e durante esse tempo esse contador é decrementado e o meio é ouvido. Quando o contador chega em zero o meio é sentido e, caso esteja livre, a transmissão pode ocorrer. Se houver atividade, o procedimento é reiniciado, e um contador de tentativas é incrementado. Quando esse contador alcança um número máximo a transmissão é considerada falha. Todos frames possuem um bit indicado a necessidade de ACK; caso seja necessário, o nó aguarda o ACK e pode realizar retransmissões, até um número máximo pré-estabelecido.

O padrão 802.15.4 estabelece uma estrutura opcional chamada super-frame (figura 11), onde é possível ter períodos de contenção (CSMA/CA), períodos livres de contenção (baseados em slot times garantidos) e períodos de inatividade. Os períodos livres de contenção devem ser utilizados por dispositivos com requisitos de qualidade de serviço. Os slot times são reservados pelo coordenador e divulgados nos beacons.

3.5 Segurança

Existem basicamente 3 tipos de modos de segurança estabelecidos pelo padrão: modo inseguro, modo ACL (Access Control List – Lista de Controle de Acesso) e o modo seguro. O modo inseguro é mandatório. Os modos ACL e seguro são opcionais, mas qualquer dispositivo que implemente o modo seguro deverá

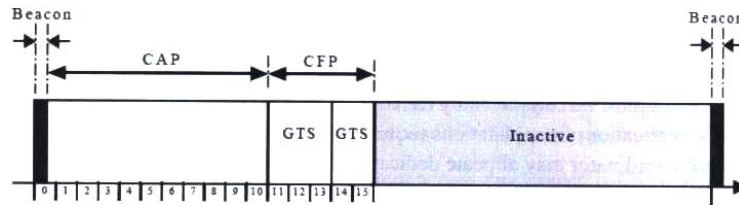


Figura 11: Super-frame 802.15.4.

implementar também o modo ACL. A segurança também pode ser delegada para protocolos de alto nível. O modo inseguro não provê qualquer serviço de segurança. O modo ACL oferece uma lista de identificadores que permite configurar com quais dispositivos é permitida a comunicação. Só são aceitos frames de dispositivos que se encontram na lista de acesso e também só são enviados frames para os dispositivos da lista. Não existem funções de criptografia no modo ACL.

O modo seguro oferece os 4 tipos de serviços de segurança: controle de acesso, criptagem dos dados, integridade dos frames e controle de seqüência de frames. Os serviços de troca e gerenciamento de chaves e autenticação de dispositivos não é incluído no padrão, sendo responsabilidade de protocolos de alto nível. Os 4 serviços de segurança do 802.15.4 são representados por uma "security suite". O padrão propõe 7 "security suites", sendo apenas a AES-CCM-64 mandatória e as outras 6 opcionais. As "security suites" especificam o modo de criptografia simétrica utilizado, o tipo de integridade e o tipo de controle de seqüência de frames. Cada fabricante pode implementar os seus próprios algoritmos de segurança, desde que sejam compatíveis com os requisitos mandatórios do padrão.

4 ZigBee

4.1 Introdução

Os avanços recentes das tecnologias de redes sem fio possibilitaram o surgimento de várias alternativas e padrões de implementação, mas até recentemente a grande maioria tinha como premissa principal prover um conjunto de protocolos que garantissem a qualidade para a transmissão de voz ou de dados com altas taxas de transferência, o que tornava os equipamentos bastante caros e pouco atraentes para outras aplicações mais simples.

Ainda são poucos os padrões de redes sem fio para aplicações em redes locais utilizando sensores e outros dispositivos do controle. O que temos são basicamente sistemas proprietários, desenvolvidos para atender redes específicas, como as redes de automação industrial, por exemplo, onde aplicações com sensores (de temperatura, de umidade, gases, etc) e dispositivos de controle (chaves, relés, etc) não necessitam de uma largura de banda elevada para funcionarem, mas necessitam de uma taxa de transmissão baixa e consumo de energia igualmente baixo para preservar a vida útil das baterias. Nesses casos, os sistemas wireless foram projetados para atenderem às exigências específicas dessas aplicações.

4.2 O padrão ZigBee

Atualmente o foco das redes wireless comerciais se encontra no contexto das redes locais (WLANs), tanto em soluções proprietárias como nos padrões desenvolvidos pelo IEEE, por exemplo. Com a evolução natural das tecnologias das redes sem fio, estas passaram a atender não só as aplicações corporativas mais sofisticadas como também aquelas envolvendo pequenos volumes de dados que exigem baixas taxas de transmissão como, por exemplo, o controle de equipamentos eletroeletrônicos. Além disso, outras tecnologias sem fio têm sido utilizadas também com o objetivo de proporcionar a comunicação pessoal e o controle de dispositivos diversos, são as chamadas redes pessoais (WPANs).

Basicamente, essas tecnologias têm o propósito de permitir o controle remoto de equipamentos domésticos (TVs, videocassetes, geladeiras, etc) e periféricos (teclados, mouse, impressoras, etc), eliminando os cabos e tornando mais prática a operação desses equipamentos pelos usuários.

Uma das tecnologias mais recentes dentro desse grupo de redes para aplicações pessoais e que permite o gerenciamento e controle desses dispositivos é o padrão ZigBee, também conhecido como HomeRF Lite e que corresponde ao IEEE 802.15.4, homologado em maio de 2003.

A tecnologia ZigBee trata-se de um padrão de protocolo para redes de sensores, desenvolvido pela Zigbee Alliance junto ao IEEE. Foi projetado para permitir comunicação sem fio confiável e com baixo consumo de energia e baixas taxas de transmissão.

A Zigbee Alliance é uma associação formada por empresas de diversos segmentos de mercado, como Motorola, Philips, Bosh, Analog Device, Freescale, Siemens etc; com objetivo de pesquisa e geração de novos segmentos de negócio.

O protocolo é definido pelo padrão IEEE 802.15.4 e pertence ao grupo WPAN (Wireless Personal Area Network).

Algumas das aplicações mais comuns das redes de sensores e por consequência do protocolo Zigbee encontram-se na área de monitoramento remoto e controle, dispositivos de localização, periféricos de computadores, sensores médicos, brinquedos e jogos, entre outros. Este documento descreve as interfaces e especificações básicas dos objetos e protocolos que fazem parte do padrão de protocolos Zigbee.

4.3 Arquitetura do protocolo Zigbee

O padrão de protocolo Zigbee para redes de sensores é composto por camadas, formadas por dispositivos. Estão descritas a camada de suporte às subcamadas (APS), o dispositivo de objetos Zigbee (ZDO), o dispositivo de perfis (ZDP), um framework de aplicações, a camada de rede (NWK) e os serviços de segurança. A arquitetura do Zigbee foi desenvolvida em blocos ou camadas. Cada camada executa serviços específicos para servir a camada acima: a entidade de dados provê dados para o serviço de transmissão e a entidade de gerência fornece informação para todos os outros serviços. Cada entidade de serviço expõe uma interface para a camada superior através do ponto de acesso ao serviço (SAP) e cada SAP suporta um número de primitivas de serviço para ativar a funcionalidade solicitada.

A arquitetura do Zigbee, observada na figura 12, segue o modelo de camadas proposto na figura 4, mas define apenas as camadas relevantes para obter a

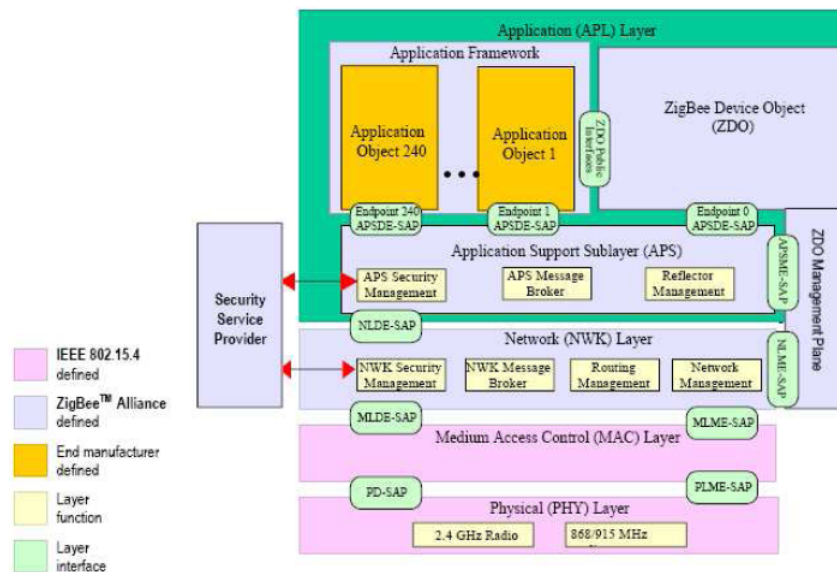


Figura 12: Arquitetura do Zigbee.

funcionalidade desejada. O padrão IEEE 802.15.4-2003 define as duas camadas mais baixas: a camada física (PHY) e a sub-camada de controle de acesso ao meio (MAC). A aliança Zigbee desenvolve sobre essas camadas para provisionar a camada de rede (NWK) e o framework para a camada de aplicação, que inclui a camada de aplicação para suporte às sub-camadas (APS), os objetos de dispositivo Zigbee (ZDO) e os objetos de aplicação definidos pelo fornecedor (Application Object).

Como mostrado anteriormente o padrão IEEE 802.15.4-2003 define duas camadas PHY que operam em duas faixas de frequência distintas: 868/915 MHz and 2.4 GHz. A frequência mais baixa cobre tanto a banda europeia de 868 MHz e a banda usada nos EUA e Austrália de 915 MHz. A frequência mais alta da camada PHY é utilizada virtualmente no mundo inteiro.

A sub-camada IEEE 802.15.4-2003 MAC controla o acesso ao canal de rádio usando o mecanismo CSMA-CA. Sua responsabilidade inclui transmitir frames, sincronização e prover um mecanismo confiável de transmissão.

A camada NWK Zigbee inclui mecanismos usados na conexão e desconexão de dispositivos numa rede, de aplicação de segurança aos frames e roteamento para seus destinos. Adicionalmente, a camada de rede inclui a descoberta e manutenção de rotas entre dispositivos envolvidos na rede NWK. A descoberta e armazenamento da informação da vizinhança pertinente também são feitos na camada NWK. O coordenador da camada NWK é responsável por iniciar uma nova rede, sempre que apropriado e assinalar endereços para os novos dispositivos associados.

A camada de aplicação, como demonstrada na figura 13, do Zigbee é composta pelo APS, pelo framework de aplicações (AF), pelo ZDO e pelos objetos de aplicação definidos pelos fornecedores. A responsabilidade da sub-camada APS inclui a manutenção das tabelas para “binding”, que é a habilidade de combinar dois dispositivos baseado em seus serviços e suas necessidades, enviando mensa-

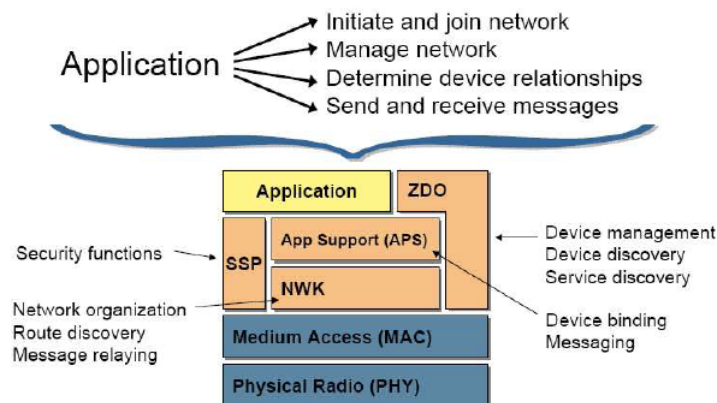


Figura 13: Zigbee stack.

gens entre os dispositivos “combinados”. O ZDO executa a função de definir a regra para o dispositivo na rede (coordenador Zigbee ou dispositivo), iniciando e/ou respondendo às requisições de binding e estabelecendo uma conexão segura na rede. O ZDO também é responsável pela descoberta de dispositivos na rede e pela determinação de que tipos de serviços estes dispositivos provêm.

4.4 Dispositivos ZigBee

Os ZDO (ZigBee device objects) representam uma classe básica de funcionalidades que fornecem uma interface entre os objetos de aplicação, o dispositivo de perfil e o APS. O ZDO está localizado entre o quadro de aplicações e a subcamada de suporte à aplicação. Este objeto atende requisições comuns a todas as aplicações operando no stack ZigBee. Ele é responsável por:

- Inicialização da subcamada de aplicação (APS), da camada de rede (NWK) e especificação dos serviços de segurança (SSS).
- Armazenamento de informação de configuração para as aplicações a fim de determinar e implementar as sub clausulas de “discovery”, manutenção da segurança, gerencia de rede e manutenção de “binding”.

O ZDO possui interfaces publicas para os objetos da camada de aplicação no framework para controle do dispositivo e funcionalidades de rede. O ZDO interage com as camadas baixas do stack Zigbee, no endpoint 0, através do APSDE-SAP para dados e através do APSME-SAP para controle de mensagens. A interface publica fornece gerenciamento de endereços do dispositivo, discovery, binding e funções de segurança na aplicação dentro da camada de framework do protocolo ZigBee. A descoberta (discovery) de um dispositivo é o processo onde um dispositivo ZigBee pode encontrar outros dispositivos ZigBee na rede, através de requisições que são distribuídas por broadcast ou unicast. Existem duas forma de um dispositivo solicitar um “discovery”:

Solicitações de endereços IEEE e solicitações de endereços NWK. A solicitação IEEE é unicast e assume que o endereço NWK é conhecido. A requisição do endereço NWK é broadcast e contém o endereço IEEE como payload. A

gerencia de “discovery” é fornecida para os objetos da aplicação. Quando solicitado, o endereço IEEE dos dispositivos requisitados precisa ser devolvido (se o dispositivo for Zigbee) com o endereço do dispositivo e de todos seus dispositivos associados (se o dispositivo for um roteador ou um coordenador). Isso se refere ao discovery de dispositivo e é utilizado para encontrar os dispositivos ZigBee na rede.

Adicionalmente à descoberta (discovery) do dispositivo, a descoberta de serviços também é fornecida para determinar quais serviços foram oferecidos em cada endpoint ou definidos num dispositivo pelo respectivo objeto de aplicação. Um dispositivo pode descobrir os endpoints ativos em dispositivos individuais ou em todos os dispositivos, e um dispositivo pode descobrir serviços específicos que conferem com um dado critério (identificadores de perfil e de cluster).

A gerencia de “binding” é fornecida para os objetos da aplicação a fim de conectar objetos de aplicações entre dispositivos ZigBee para garantir conexões concisas através de todas as camadas do protocolo e também para as diversas conexões providas pelos nós da rede ZigBee. Tabelas de conexão são construídas e populadas conforme as solicitações e os resultados das conexões. A gerencia de segurança é fornecida pelos objetos da aplicação para habilitar ou desabilitar a parte segura do sistema. Se habilitado, a gerencia de segurança será executada através da gerencia de chaves e autenticação, com objetivo de estabelecer um link seguro.

4.5 Topologias de Rede (NWK)

A camada de rede (NWK) do Zigbee suporta a topologia em estrela, árvore e mesh. Numa topologia do tipo estrela, a rede é controlada por um único dispositivo chamado coordenador Zigbee. Este coordenador é responsável por iniciar e manter os dispositivos da rede e todos os outros dispositivos, conhecidos como “end devices”, diretamente comunicando com o coordenador Zigbee. Nas topologias mesh e estrela, o coordenador Zigbee é responsável por inicializar a rede e pela escolha dos parâmetros chaves da rede, além de que a rede pode ser estendida através do uso dos roteadores Zigbee. Em topologias de árvore os roteadores movem dados e controlam mensagens através do uso da estratégia de roteamento hierárquico.

A função de gerenciamento da rede deve ser implementada pelo coordenador ZigBee, pelo roteador ou dispositivo lógico, conforme a configuração estabelecida via aplicação ou durante a instalação. Se o tipo do dispositivo é roteador ou dispositivo comum, essa função fornece a habilidade de selecionar uma PAN existente para se associar e executar procedimentos que permitam ao dispositivo voltar a se associar com o mesmo coordenador ou roteador se a comunicação na rede for perdida. Essa função será executada pelo Coordenador ou pelo Roteador e tem a habilidade para selecionar um canal que não está em uso para a criação de uma nova PAN. É possível formar uma rede sem que exista um dispositivo pré-designado como Coordenador, onde o primeiro dispositivo de função completa (FFD) ativado assume a função de coordenador.

O processo de gerencia de rede permite a especificação de uma lista de canais para o procedimento de buscas na rede. O padrão é utilizar todos os canais na banda de operação selecionada. Além disso, a gerencia de rede é responsável pelos procedimentos de busca para determinar as redes na vizinhança e a identidade do seu dispositivo coordenador e roteador.

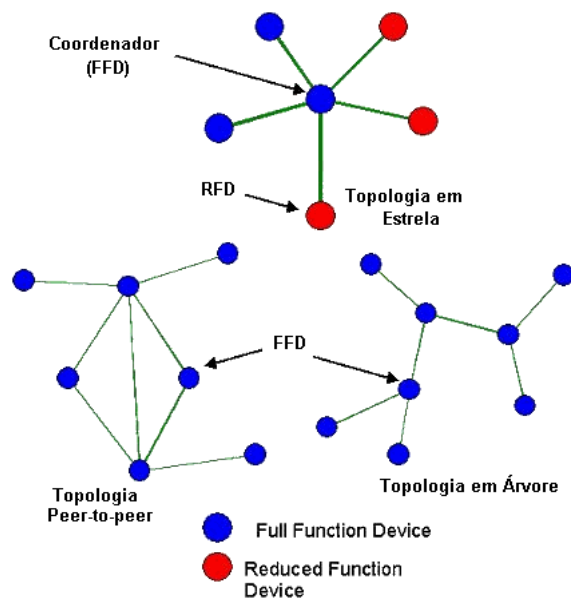


Figura 14: Características básicas de Rede.

Outras funções de gerenciamento de rede implementado nos dispositivos de função completa:

- Permite a seleção de um canal para iniciar uma PAN ou seleção de uma PAN existente para associação;
- Suporte a procedimentos de reassociação na rede;
- Suporta conexão direta e conexão via proxy fornecidos pela camada de rede;
- Deve suportar entidades de gerencia externas, para permitir gerenciamento de rede externo.

4.6 Roteamento

Os dispositivos com função de coordenadores e roteadores provêm as seguintes funcionalidades:

- Envio de frames de dados para as camadas superiores;
- Disponibilizar quadros de dados para outros roteadores ZigBee;
- Participa no discovery para estabelecer rotas para os subseqüentes quadros de dados;
- Participa na descoberta da rota para os dispositivos RFD (reduced function device);
- Participa no reparo de rotas fim a fim;

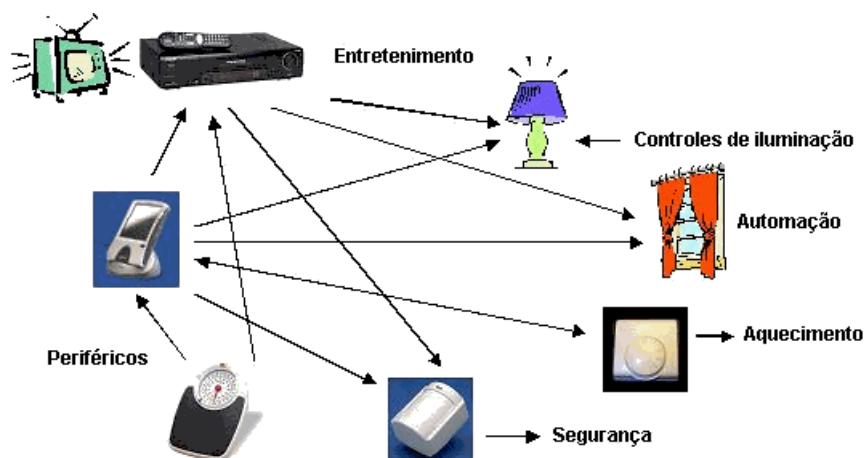


Figura 15: Exemplos de aplicações.

- Participa no reparo das rotas locais;
- Emprega as métricas conforme especificado no discovery e no reparo da rede.

4.7 Aplicações

Aplicações são definidas por conveniência, focando gerenciamento da energia e para toda a conectividade. Algumas das aplicações mais comuns do padrão ZigBee está representado na figura 15 e 16.

- Iluminação;
- Controle de carga, dispositivos On/Off;
- Controle de iluminação residencial;
- Aquecimento, ventilação, ar condicionado (HVAC);
- Sensores de movimento, detectores de fumaça de cigarro

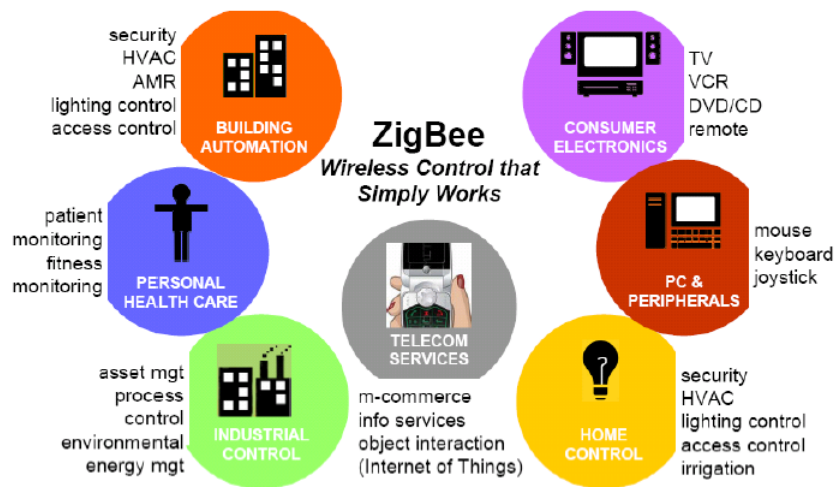


Figura 16: Exemplos de aplicações.

5 Glossário

- MEMS - Micro eletromechanical system
- SMACS - Self Organizing Medium Access Control for Sensor networks
- EAR - Eavesdrop and register algorithm
- SMECN - Small Minimum Energy Communication Network
- SPIN - Sensor Protocol for Information Negotiation
- SAR - Sequential Assignment Routing
- LEACH - Low Energy Adaptive Clustering Hierarchy
- SMP - Sensor Management Protocol
- SQDDP - Sensor Query and Data Dissemination Protocol

Referências

- [1] Wikipedia - IEEE 802.15.4 - http://en.wikipedia.org/wiki/IEEE_802.15.4 - visitado em 02/06/08
- [2] Wireless Communication Standards - A study of IEEE 802.11, 802.15 and 802.16. Todor Cooklev - IEEE Publisher
- [3] Freescale: <http://www.freescale.com/zigbee>
- [4] ZigBee Alliance: <http://www.zigbee.org>
- [5] Tutorial sobre o ZigBee: http://www.teleco.com.br/tutoriais/tutorialzigbee/pagina_2.asp
- [6] Wireless Brasil: <http://www.wirelessbrasil.org>

- [7] COS UFRJ: <http://www.cos.ufrj.br/crismaga/>
- [8] Ian F. Akyildiz, W. S. Weilian, Y. Sankarasubramaniam, and E. Cayirci, “A Survey on Sensor Networks”, *Communication Magazine IEEE*. vol. 40, no. 8, pp. 102-114, Aug. 2002.
- [9] André G. Mignaco, “Análise de Desempenho de Redes de Sensores sem Fio”, Tese mestrado UNICAMP, 2005
- [10] UC Berkeley: Mote and Smart Dust: <http://www-bsac.eecs.berkeley.edu/>
- [11] C. Shen, C. Srisathapornphat, and C. Jaikaeo, “Sensor Information Networking Architecture and Applications,” *IEEE Pers. Commun.*, Aug. 2001, pp. 52–59.
- [12] <http://www.dustnetworks.com/technology/tsmp.shtml>
- [13] Jan M. Rabey, M. Josie Ammer, Julio L. Da Silva Jr, Danny Patel, Shad Roundy, “Pico Radio Supports Ad Hoc Ultra Low Power Wireless Networks”, *IEEE Computer Magazine*, pp. 42-48, July 2000.
- [14] <http://www.archrock.com/downloads/resources/6LoWPAN-tutorial.pdf>