4
Redes sem fio

4.1
Redes Locais

As redes locais ou LANs (*Local Area Networks*), são redes privadas utilizadas por corporações para conectar estações de trabalho em escritórios e fábricas possibilitando o compartilhamento de recursos e troca de informações. As LANs podem ser implementadas por diversas tecnologias diferentes de transmissão, que consistem por exemplo de cabos aos quais as estações estão conectadas, caracterizando um meio confinado de transmissão. As LANs convencionais permitem que as informações trafeguem a velocidades de 10 a 100Mbps, com pouco atraso e erros, porém LANs que utilizam tecnologia mais avançada conseguem chegar a velocidades da ordem de Gbps. [1]

4.1.1
O padrão IEEE 802

O Projeto IEEE 802 surgiu com o objetivo de padronizar as redes locais de computadores. Sua origem se deu através do Comitê da IEEE *Computer Society*, onde seu modelo de referência definiu uma arquitetura de 3 camadas apenas, que correspondem às camadas 1 e 2 do modelo OSI apresentado anteriormente. Com relação à camada de enlace, suas funções englobam:

- Fornecer um ou mais SAP (*Service Access Point*) para os usuários de rede;
- Na transmissão, montar os dados a serem transmitidos em quadros contendo campo de endereço e de correção de erros;
- Na recepção, desmontar os quadros, efetuando o reconhecimento de endereço e detecção de erros;
- Gerenciar a comunicação no enlace

O primeiro item é atendido pela subcamada *Logical Link Layer* (LLC) e os demais são tratados em uma subcamada chamada de *Medium Access Control* (MAC). A Figura 4.1 [2] mostra a relação entre os padrões IEEE 802 e o modelo OSI de referência.

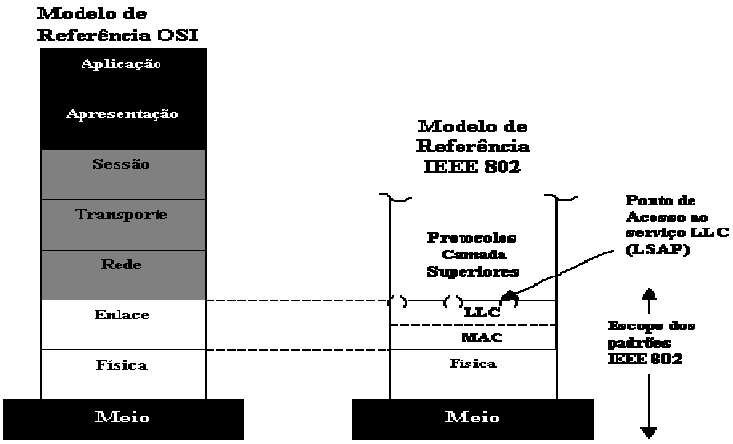

Figura 4.1 - Relação entre os padrões IEEE 802 e OSI

O Padrão 802.1 descreve o relacionamento entre os diversos padrões 802.2 e o relacionamento deles com modelo de referência OSI. Ele contém também as funções de gerenciamento da rede e informações para a ligação entre redes. O padrão IEEE 802.2 descreve a subcamada superior da camada de enlace, chamada de *Logical Link Layer*, que implementa um protocolo de mesmo nome. Os demais padrões especificam diferentes opções de camada física e protocolos de subcamada MAC para diferentes tecnologias de redes locais. Sendo:

Padrão	Tecnologia
802.3	Rede em barramento utilizando CSMA/CD como método de acesso.
802.4	Rede em barramento utilizando Passagem por Permissão como método de acesso.
802.5	Rede em anel utilizando Passagem por Permissão como método de acesso.
802.6	Rede em barramento utilizando o *Distributed Queue Dual Bus* (DQDB) como método de acesso.
802.11	Rede sem fio utilizando o CSMA/CA como método de acesso.

Tabela 4.1 - Padrões de camada física e MAC

4.2
Redes locais sem fio

A rede local sem fio é um sistema de comunicação flexível que pode ser implementado como uma extensão ou como uma alternativa às redes locais montadas a partir do par trançado, cabo coaxial ou ainda a fibra ótica. O conceito básico segue o princípio das células existentes nos sistemas de telefonia móvel. Através da rede *wireless*, os usuários móveis podem ter acesso à informação e a recursos de rede enquanto se deslocam para outros pontos desde que dentro da área coberta. [3]

As WLANs estão sendo empregadas em corporações proporcionando ganhos de produtividade com o uso de *notebooks* e terminais do tipo *hand-held* para transmitir e receber informações em tempo real. Além das empresas, outros

locais como os hospitais, armazéns, fábricas, universidades, aeroportos, restaurantes, centros de convenção, etc. E servem também como rede de *backup* para sistemas de missão crítica. [4]

Os padrões para as WLANs procuram atender aos requisitos básicos impressindíveis para o bom desempenho de aplicações que atuam sobre este diferenciado meio de transmissão. Sendo assim, as redes sem fio devem oferecer confiabilidade, transparência, simplicidade, *throughput*, segurança, dentre outros.

Vale mencionar que a confiabilidade deve ser atendida de forma muito similar às redes cabeadas, com taxas de erro inferiores a 10^{-6}. A transparência deve estar presente no âmbito de coexistência e integração das WLANs com as LANs. Com relação à segurança, talvez uma das maiores preocupações nas WLANs, é necessário proteger as informações trafegadas pois elas estão presentes em ondas eletromagnéticas que percorrem o ar livre e podem ser interceptadas de forma mais fácil que em redes cabeadas.

4.2.1 Tecnologias w*ireless*

Existem várias tecnologias para o estabelecimento de um enlace sem fio entre dois pontos e um quadro como o da Tabela 4.2 [59] sumariza muito bem essas variedades de padrões.

Padrão	Taxa	Modulação	Segurança	Vantagens e Desvantagens
IEEE 802.11	Até 2Mbps na faixa de 2.4GHz	FHSS ou DSSS	WEP e WPA	- Esta especificação foi extendida na IEEE 802.11b
IEEE 802.11a (Wi-Fi)	Até 54Mbps na faixa de 5GHz	OFDM	WEP e WPA	- Produtos que aderem a este padrão são considerados *Wi-Fi Certified* - Oito canais disponíveis - Menor risco de interferência que os padrões 802.11b e 802.11g - Melhor que o 802.11b no suporte a voz, vídeo e imagens em ambientes densamente povoados - Menor cobertura que o 802.11b - Não opera com o 802.11b - Faixa de frequência regulamentada elevando o custo da solução
IEEE 802.11b (Wi-Fi)	Até 11Mbps na faixa de 2.4GHz	DSSS com CCK	WEP e WPA	- Produtos que aderem a este padrão são considerados *Wi-Fi Certified* - Não opera com o 802.11a - Requer menos APs que o 802.11a para cobrir uma mesma região - Oferece acesso a alta velocidade a estações distantes 91m do AP - 14 canais disponíveis na banda de 2.4GHz

Tabela 4.2 – (a) Padrões de redes sem fio

Padrão	Taxa	Modulação	Segurança	Vantagens e Desvantagens
IEEE 802.11g (Wi-Fi)	Até 54Mbps na faixa de 2.4GHz	OFDM acima de 20Mbps, DSSS com CCK abaixo de 20Mbps	WEP e WPA	- Produtos que aderem a este padrão são considerados *Wi-Fi Certified* - Possivelmente estes substituirão o 802.11b - Mecanismos de segurança que são melhores que o 802.11 - Compatível com o 802.11b - 14 canais disponíveis na banda de 2.4GHz
Bluetooth	Até 2Mbps na faixa de 2.45GHz	FHSS	PPTP, SSL ou VPN	- Não oferece suporte nativo ao protocolo IP e por isso não suporta de forma adequada aplicações baseadas em TCP/IP - Não foi criado originalmente para suportar WLANs - Melhor aplicação para conectar PDAs, celulares e PCs por alguns momentos
HomeRF	Até 10Mbps na faixa de 2.4GHZ	FHSS	Dados são encriptados por um algoritmo de 56 bits	- Não está mais sendo assunto de estudo e comércio - Focado em residência e não em empresas - Cobertura até 45m da estação base - Relativamente barato para se configurar e manter - Qualidade de voz é sempre boa pois reserva continuamente uma parcela da banda para estes serviços - Imune a interferências devido à modulação FHSS
HiperLAN 1	Até 20Mbps na faixa de 5GHz	CSMA/CA	Encriptação por sessão e autenticação individual	- Em uso somente na Europa - É totalmente ad-hoc, não necessitando configuração e controladora central - Relativamente caro para operar e manter - Não possui garantia de banda
HiperLAN 2	Até 54Mbps na faixa de 5GHz	OFDM	Fortes *features* de segurança com suporte a autenticação individual e chaves de encriptação por sessão	- Em uso somente na Europa - Desenvolvido para transporter células ATM, pacotes IP, Designed to carry ATM cells, IP packets, e voz digital - Melhor qualidade de service que o HiperLAN/1 - Garantia de banda

Tabela 4.2 – (b) Padrões de redes sem fio

4.2.2
Histórico das redes sem fio

Pode-se dizer que, de acordo com a premissa de comunicação por meio de ondas rádio, o Projeto ALOHANET desenvolvido pela Universidade do Havaí, implementou a primeira rede local sem fio de comunicação, salvo as dimensões envolvidas. A rede surgiu em 1971 e utilizava comunicações via satélite dispostas em topologia estrela, tendo computadores distribuídos entre quatro ilhas que realizavam a comunicação com um computador central na Ilha de Oahu. [6]

Diversos projetos e desenvolvimentos foram tocados durante os anos, até que na década de 90 começaram a surgir os primeiros produtos comercializados utilizando a tecnologia sem fio para comunicação.

Um pouco antes, em 1985, determinadas faixas do espectro de frequências foram liberadas pelo FCC (*Federal Communications Commission*) da necessidade de licença por parte dos órgãos reguladores mundiais para que fossem utilizadas comercialmente para comunicação sem fio. As faixas de 900MHz, 2,4GHz e 5GHz foram as contempladas nesta liberação, e receberam a denominação de Banda *ISM* (*The Industrial, Scientific, and Medicine Frequency Bands*). Esta importante decisão fez com que o interesse por redes *wireless* nestas faixas crescesse de forma bastante acentuada, acendendo o setor.

Com isso, diversos fabricantes desenvolveram suas tecnologias proprietárias obrigando o FCC a solicitar a padronização dessas redes através do IEEE. O padrão desenvolvido portanto ao final desta década, veio a ser chamado de IEEE 802.11, seguindo as mesmas denominações para os padrões que englobam as funções de camada física e de enlace para redes locais. Nessa mesma época, surgiram os primeiros produtos comercializados para a faixa de 2,4GHz.

Ainda assim, a existência de três diferentes tecnologias dentro do padrão vinha provocando a insatisfação por parte dos usuários e fornecedores que buscavam assegurar a interoperabilidade dos dispositivos. Surgiu então a WECA (*Wireless Ethernet Compatibility Alliance*) em 1997. Formada pelas empresas Lucent, Cisco, Nokia, 3Com, dentre outras, a aliança procurou interoperar os diferentes padrões existentes.

Ao final de 1999, outro padrão surgiu, porém interoperável com os demais, apresentando desempenho superior aos existentes até aquele momento, é o chamado IEEE 802.11b. Assim apareceu o termo *Wireless-Fidelity* ou Wi-Fi, como sendo a garantia de interoperabilidade entre os padrões para rede local sem fio dada pela WECA aos dispositivos por ela certificados. [1]

4.2.3 Redes 802.11

Desde a formação dos grupos de estudo no IEEE para o desenvolvimento da tecnologia sem fio, a evolução destas redes nunca ficou estagnada. Novos padrões foram criados de forma a atender aos maiores requisitos da tecnologia. Assim sendo, um resumo dos padrões existentes hoje é apresentado na Tabela 4.3 [7] a seguir:

Padrão	Data de regulamen.	Banda disponível	Freqüência/ técnica	Taxa de transmissão por canal	Modulação
802.11	Julho de 1997	83,5 MHz	2,4 a 2,4835 GHz DSSS, FHSS	2,1 Mbps	DQPSK (2 Mbps DSSS) DBPSK (1 Mbps DSSS) 4GFSK (2Mbps FHSS) 2GFSK (1Mbps FHSS)
802.11a	Setembro de 1999	300,0 MHz	5,15 a 5,35 GHz OFDM 5,725 a 5,825 GHz OFDM	54, 48, 36, 24, 18, 12, 9, 6 Mbps	BPSK (6, 9 Mbps) QPSK (12, 18 Mbps) 16-QAM (24, 36 Mbps) 64-QAM (48, 54 Mbps)
802.11b	Setembro de 1999	83,5 MHz	2,4 a 2,4835 GHz DSSS	11, 5,5, 2, 1 Mbps	DQPSK/CCK (11, 5,5 Mbps) DQPSK (2 Mbps) DBPSK (1 Mbps)
802.11g	Metade de 2003	83,5 MHz	2,4 a 2,4835 GHz DSSS, OFDM	54, 36, 33, 24, 22, 12, 11, 9, 6, 5,5, 2, 1 Mbps	OFDM/CCK (6, 9, 12, 18, 24, 36, 48, 54 Mbps) OFDM (6, 9, 12, 18, 24, 36, 48, 54 Mbps) DQPSK/CCK (22, 33, 11, 5,5 Mbps) DQPSK (2 Mbps) DBPSK (1 Mbps)

Tabela 4.3 – Resumo dos padrões IEEE 802.11

Através deste conjunto de informações, pode-se constatar que o padrão 802.11a apresenta taxas bastante elevadas quando comparadas com o padrão original, devido aos seus métodos de modulação serem bem mais eficientes. Representam o único padrão que atua sobre a faixa dos 5GHz. O padrão seguinte, o 802.11b, consegue alcançar taxas de transmissão maiores que o padrão original, porém não são compatíveis com seu antecessor, o 802.11a. Um novo padrão, que fosse capaz de interoperar com o 802.11a, foi desenvolvido e surgiu em meados de 2003, o chamado 802.11g. Este oferece altíssimas taxas, assim como o 802.11a.

4.2.4
Vantagens e desvantagens das redes sem fio para as cabeadas

Podem-se listar as vantagens das redes locais sem fio sobre as redes cabeadas em [8]:

- Mobilidade
- Portabilidade
- Fácil e rápida instalação e desinstalação
- Baixos custos de implantação
- Escalabilidade

Com respeito à mobilidade, este é um ponto importante e foco principal da tecnologia *wireless*, pois permite que um usuário se conecte à um sistema de rede onde quer que ele esteja desde que sob cobertura de uma rede de acesso *wireless*.

A portabilidade promove a facilidade de transporte dos equipamentos que utilizam esta tecnologia de rede. O desenvolvimento dos comunicadores tais como PDAs, laptops, etc tem proporcionado grande avanço neste item.

A facilidade de instalação é conquistada pois não há necessidade de obras civis e passagem de cabos através de condutores por meio do ambiente em questão. Desta forma, rapidez é alcançada na implantação e desmontagem de uma rede como esta, permitindo que redes temporárias sejam organizadas para atender a eventos tais como convenções, palestras e amostras.

Os baixos custos relacionados com essas redes, está intimamente ligado ao quesito de facilidade de instalação. A não necessidade de que sejam feitas obras no local, muitas vezes interrompendo as atividades ali desenvolvidas, proporciona uma melhor distribuição dos investimentos sobre os equipamentos que oferecerão o acesso propriamente dito, o que permite um bom planejamento de forma a atender todas as necessidades dos usuários.

Um outro fator que culmina na redução de custos é o contínuo desenvolvimento da tecnologia *wireless*, o que batareia cada vez mais seus equipamentos e traz ao mercado formas de acesso cada vez mais rápidas, eficientes e seguras.

Sobre a escalabilidade, os sistemas *wireless* permitem a fácil inserção e remoção de qualquer terminal remoto. Ao contrário das redes fixas, não é preciso habilitar ponto ou passar cabo adicional para que uma estação possa usufruir da rede.

Com respeito às desvantagens, a que mais é discutida dentro do setor, se trata justamente da segurança. A preocupação surge a partir do momento em que as redes sem fio estão enquadradas dentro do que se entende por meios não confinados, onde a energia utilizada para as transmissões não seguem um caminho determinado, ou seja, os sinais não são guiados. O contrário ocorre com as redes cabeadas, onde os sinais elétricos seguem por meio de cabos que confinam a energia e a guiam da origem até o destino em uma comunicação.

Segundo esse entendimento, em uma rede de acesso sem fio, não é possível limitar a cobertura do sinal, e como um usuário somente necessita estar dentro desta área para entrar na rede, fica fácil um invasor agir. Em uma rede cabeada, o invasor precisa se conectar fisicamente a um ponto na rede. Assim sendo, tornou-se necessário o desenvolvimento de técnicas que garantam a segurança em um ambiente como este.

4.2.5
Componentes de *WLANs*

Os componentes presentes nas redes *WLAN* são diferentes daqueles que constituem uma rede cabeada como a Ethernet, por exemplo. Os equipamentos até desempenham as funções básicas bem semelhantes ao modelo tradicional, porém as executam sob uma nova ótica, a da comunicação via rádio. Podem-se listar os principais equipamentos e suas funções como segue.

Access Point

O *Access Point* ou Ponto de Acesso ou ainda AP, exerce a mesma função que um *hub* em uma rede cabeada, mas devem ainda, realizar o controle de potência das estações terminais para fins de economia de bateria, permitir o *roaming* e sincronização. A sincronização é implementada através do envio periódico de quadros *beacon* para as estações, de tal forma que elas possam programar o momento em que devem ligar seu receptor para receber mensagens.

A Figura 4.2 [57] apresenta um AP que serve como um ponto de conexão via rádio das estações, fixas ou móveis, com a rede de serviços. Cada AP possui sua própria área de cobertura e todos os usuários que estiverem cobertos por ele, poderão usufruir os serviços oferecidos pela rede, como servidores de arquivos, impressão, acesso à Internet, etc.

Figura 4.2 – Access Point

Figura 4.3 – Antenas externas

A comunicação via rádio exige portanto que esses tipos de dispositivos detenham antenas instaladas em seus módulos, normalmente em diversidade, e que distribuem os sinais de forma homogênea por todas as direções formando uma esfera de cobertura, são as chamadas antenas isotrópicas. Porém, nem sempre estes tipos de antenas atendem de forma eficiente a demanda de cobertura em um determinado ambiente onde se deseja implantar uma rede *wireless*. Assim sendo, existem diversos tipos de antenas, como as ilustradas pela Figura 4.3 [49], que podem ser acopladas ao AP de forma a proporcionar melhor cobertura do sinal em local específico.

Os APs possuem ainda funcionalidades importantes tais como a regulagem da potência de transmissão, a diversidade de antenas como já mencionado, as saídas cabeadas diversas para conexão com a rede fixa, mecanismos de segurança, etc.

Wireless Bridge

Um outro dispositivo interessante é a *Wireless Bridge*, como a representada pela Figura 4.4 [49] que possui a função de estabelecer, de forma *half-duplex*, a comunicação entre duas ou mais redes. Esta é uma necessidade comum atualmente, quando se deseja interligar dois ambientes em uma mesma rede e estes estão separados por distâncias relativamente grandes como uma rua. Esta conexão é feita entre duas ou mais *Bridges*, configurando assim conexões ponto-a-ponto ou ponto-multiponto.

Como funcionalidades extras, a maior parte das *Bridges* existentes no mercado podem ser configuradas como simples repetidores através do *Repeater mode*. Esta funcionalidade é muito útil para estabelecer comunicação entre

longas distâncias, acarretando, entretanto, diminuição da taxa de transmissão, por ser *half-duplex*.

Estas interligações podem ser muitas vezes temporárias para oferecer mais flexibilidade durante o processo de implantação. Este tipo de equipamento também pode ser configurado como um *Access Point* comum.

Figura 4.4 – Wireless Bridge

***Workgroup Bridge* (WB)**

Uma Workgroup Bridge, como a da Figura 4.5 [49], é similar a uma Wireless Bridge, porém, ela é um dispositivo a ser utilizado no ambiente do usuário, onde se procura fazer uma extensão da rede sem fio através da conexão com um AP. Ou seja, instala-se um AP no ponto de terminação de uma rede cabeada e uma WB no ponto onde se deseja proporcionar cobertura rádio. O AP e a WB se comunicarão por meio de suas antenas permitindo atender àquela determinada região.

Figura 4.5 – Workgoup Bridge

Adaptador cliente

Os adaptadores *wireless* das estações cliente permitem que o usuário final se conecte a uma rede sem fio através de autenticação e associação, por meio de um AP. Estes adaptadores podem ser instalados em microcomputadores convencionais, em *laptops*, ou ainda *palms*. Os dois primeiros estão refletidos na Figura 4.6 [57]. Eles são constituídos por um circuito e antenas omnidirecionais propagando a energia por todas as direções.

Figura 4.6 – Client Adapters

4.2.6
Topologias de *Wireless* LAN

As redes *wireless* possuem o princípio básico de cobertura celular já consagrada pelos sistemas celulares tradicionais. No ambiente WLAN, as células são chamadas de BSA (*Basic Service Area*), onde um grupo de estações são atendidas, formando-se o que se chama de BSS (*Basic Service Set*). O tamanho de uma célula depende das características do ambiente e das unidades transmissoras e receptoras usadas nas estações. Em qualquer ponto dentro desta área de cobertura, um terminal deve ser capaz de usufruir os recursos que a rede proporciona. O equipamento que gera uma célula é o AP, como já dito anteriormente, mas também pode haver comunicação sem a presença de um *Access Point*, quando os terminais conversam diretamente entre si.

A cobertura a ser disponibilizada em um determinado ambiente de trabalho, deve levar em conta diversos fatores imprescindíveis para a boa eficiência da rede local sem fio. É importante se conhecer bem o local que será atendido por esta rede, bem como a quantidade de terminais e de tráfego gerado por cada um deles. A isto deve estar associado à quantidade média de usuários simultaneamente ativos na rede. [5]

As redes *wireless* podem ser dispostas segundo topologias variadas. A primeira delas, chamada de *Peer-to-Peer* ou *Ad-Hoc* pode ser montada por meio de dois terminais de usuário com adaptadores sem fio. Essa topologia é denominada de ponto-a-ponto, pois envolve somente estes dois terminais, sem a presença de um AP. Desta maneira, os recursos de um terminal podem ser acessados pelo outro e vice-versa, configurando-se assim um esquema onde cada um dos terminais pode ser cliente e também servidor. Essa topologia também é conhecida como IBSS (*Independent Basic Service Set*). A Figura 4.7 [1] apresenta bem este modelo de rede.

Figura 4.7 - Rede sem fio ponto-a-ponto

Essa topologia é a única Não-Estruturada, as demais que se seguem são todas do tipo Infra-Estruturadas, pois o AP faz o papel de uma ponte interligando as estações remotas à rede cabeada.

A segunda forma de conexão entre terminais é através de um Ponto de Acesso ou AP que proporciona cobertura em uma determinada região. Também chamada de estrutura Unicelular ou ainda BSS, qualquer estação, fixa ou móvel, desde que autorizada, é capaz de se associar a esta rede sem fio desde que dentro da área coberta por esta BSS, que certamente é maior que a topologia anterior. Como mostra a Figura 4.8 [1], um AP permite que uma estação de usuário se conecte a uma rede cabeada, usufruindo os serviços por ela oferecidos. Porém, existe um limite de acessos a um AP. Os mais novos padrões permitem, por exemplo, que algumas dezenas de dispositivos de clientes se associem a ele.

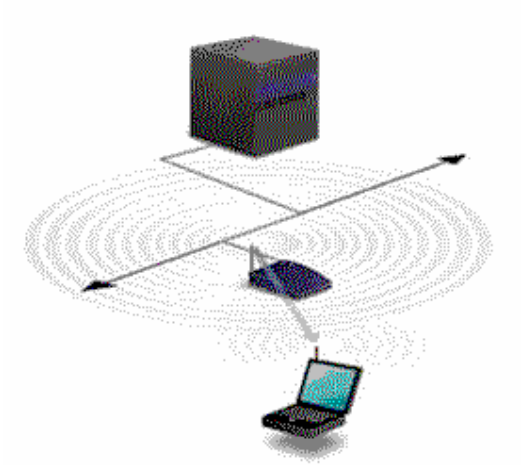

Figura 4.8 - Cliente e Ponto de Acesso

Apesar dos APs proporcionarem uma grande área de cobertura, ela muitas vezes não atende às reais necessidades de um projeto. Para tal, é preciso fazer uso de mais de um Ponto de Acesso, como o da Figura 4.9 [1], interligados por um Sistema de Distribuição (*Distribuition System* ou DS), surgindo assim, a estrutura do tipo ESS (*Extended Service Set*). A área total coberta por estes APs é denominada de ESA (*Extended Service Area*). De acordo com a disposição destes APs, sub-estruturas ou configurações aparecem de forma a procurar atender da melhor maneira possível a demanda local pelos serviços da rede.

Para se verificar a forma como a rede deve ser instalada, é feito o *site survey* e através dele estimam-se os melhores pontos em que os APs devem ser dispostos para que toda a área de interesse seja coberta, não restando espaços mal atendidos. Caso os terminais sejam de usuários móveis, a movimentação

dos mesmos através das diversas células caracteriza o que se chama de *roaming*, não ocorrendo a perda de conexão quando os terminais se movimentam entre as células de cobertura, ou seja, os APs transferem as conexões dos usuários com os outros APs de maneira transparente. [7]

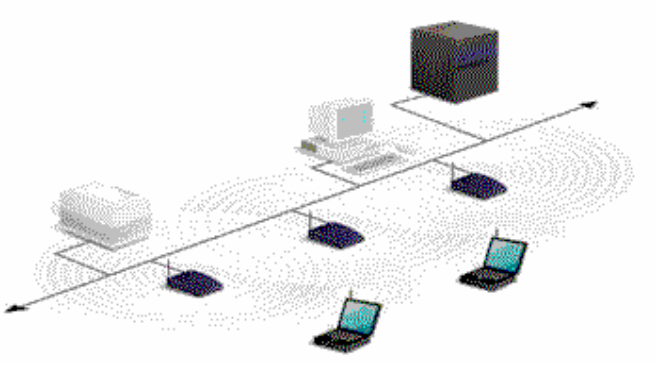

Figura 4.9 - Configuração com superposição celular

O modelo seguinte de topologia possível, faz uso das WBs para proporcionar uma extensão à rede sem fio. As WBs funcionam como Pontos de Acesso, mas elas não estão conectadas à rede cabeada como os APs. Caso a distância entre a WB e o AP for muito grande e não se consiga comunicação com eficiência, podem ser utilizadas antenas externas que devem ser acopladas aos equipamentos para que se consigam melhores resultados. A Figura 4.10 [1] a seguir torna fácil o entendimento.

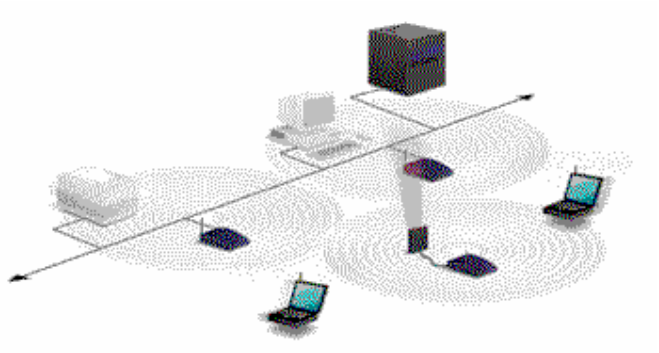

Figura 4.10 - Configuração Multi-Hop

A última topologia comentada é a que faz uso de antenas direcionais, ou seja, que direcionam as ondas eletromagnéticas de forma a concentrar a energia do sinal em uma única direção, proporcionando maior alcance. Este tipo de arquitetura é bastante útil quando se deseja interligar diferentes redes *wireless* distantes entre si como é apresentado na Figura 4.11 [1].

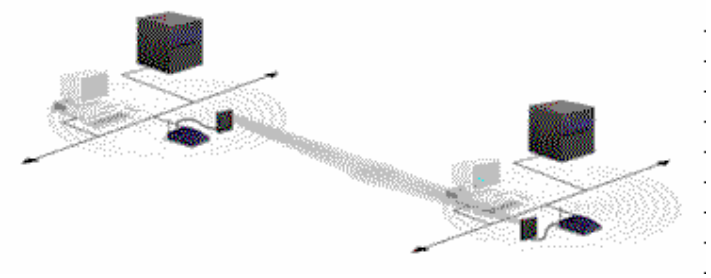

Figura 4.11 - Utilização de Antenas Direcionais

Existe ainda um outro tipo de configuração chamada de Multicelular, representada pela Figura 4.12 [19]. Segundo ela, os APs são posicionados de tal forma que suas células são quase que totalmente sobrepostas. Esta solução aumenta a vazão disponível para os terminais que ali se encontram, porém, cada um dos APs deve estar configurado para operar em uma determinada frequência para evitar interferência. Sempre que houver configuração em que áreas de cobertura são sobrepostas, os terminais poderão se comunicar com mais de um AP.

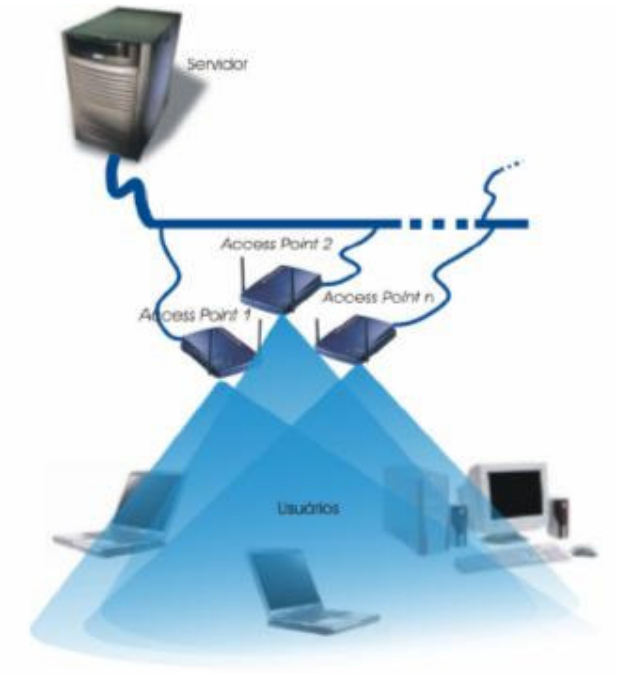

Figura 4.12 – Topologia Infra-estrutura (configuração multicelular)

É importante também comentar que uma rede mista pode ser configurada utilizando-se mais de um tipo de arquitetura, tornando a rede sem fio bastante flexível, uma de suas principais vantagens procura atender às inúmeras necessidades dos usuários. [9]

O Sistema de Distribuição está presente em todas as topologias infra-estruturadas e apesar de sua implementação não ser especificada no padrão

802.11, este padrão especifica os serviços que o DS deve suportar. Esses serviços englobam os Serviços de Estações (*Station Services* - SS) e os Serviços do Sistema de Distribuição (*Distribuition System Service* - DSS).

Dentre os serviços DSS, estão a Associação, Reassociação, Desassociação, Distribuição e Integração. Os serviços de Associação, Reassociação e Desassociação dizem respeito à mobilidade da estação. Assim, se um terminal remoto está se movendo dentro de sua BSS ou está parado, a mobilidade da estação é chamada de Não-Transição. Caso uma estação se mova entre BSSs distintas, porém, dentro da mesma ESS, a sua mobilidade é chamada de Transição-BSS. Se ao invés disso, a estação se move entre ESSs diferentes, ocorre uma Transição-ESS.

Para que uma estação de usuário deseja utilizar os serviços oferecidos pela rede, ela deve se associar a uma BSS, o que é feito através da sua Associação a um Ponto de Acesso. As associações devem ser dinâmicas pois as estações se movem, ligam e desligam, porém, deve-se respeitar a regra de que uma estação só pode se associar a um único AP. Isto assegura que o Sistema de Distribuição sempre saberá onde a estação está. A Associação suporta a Não-transição, mas não é suficiente para suportar a Transição-BSS.

A Reassociação por sua vez, permite que uma estação transfira sua associação de um Ponto de Acesso para outro, e assim como a Associação, é iniciada pelo terminal do usuário. Já a Desassociação ocorre quando a Associação entre uma estação e um AP termina, podendo ser gerada por ambas as partes. Uma estação desassociada não pode enviar ou receber dados, ela está logicamente fora da rede.

Os Serviços de Estações são Autenticação, De-Autenticação, Privacidade, entrega da *MAC Service Data Unit* (MSDU). Com um sistema sem fio, as estações devem estabelecer primeiro sua identidade assegurando que ela é exatamente quem ela diz que é, antes de ser permitido à estação transferir dados. Este procedimento é a chamado Autenticação e em seguida o terminal deve se associar a um AP.

Existem dois tipos de Autenticação oferecidos pelo padrão 802.11. O primeiro deles é a Autenticação de Sistema Aberto (*Open System Authentication*) que permite que qualquer estação se autentique na rede. O segundo tipo é Autenticação por Compartilhamento de Chave (*Key Sharing Authentication*). Para que um terminal se autentique, os usuários devem estar de posse de uma chave compartilhada. Esta chave é implementada com o uso do

algoritmo WEP (*Wired Equivalent Privacy*) e deve ser transferida para todas as estações de forma segura.

A De-Autenticação ocorre quando tanto uma estação quanto um AP quer terminar com a autenticação de um terminal de usuário. Quando isto acontece, a estação é automaticamente desassociada.

A Privacidade é um serviço obtido através de um algoritmo de encriptação, o qual é utilizado de forma que outros usuários do padrão 802.11 não possam "enxergar" o tráfego da rede. O padrão IEEE 802.11 especifica o WEP como um algoritmo opcional para satisfazer a privacidade, e caso ele não seja utilizado, as estações estarão no estado "*clear*" ou "*red*", o que significa que a informação não está encriptada.

Todas as estações começam a transmissão no estado *clear* até que sejam autenticadas. A entrega da MSDU garante que a informação na MSDU seja entregue ao serviço de controle de acesso ao meio dos pontos de acesso.

O WEP é utilizado para proteger as estações autorizadas dos *hackers*. Este algoritmo pode se quebrado e está relacionado diretamente com o tempo que uma chave está em uso. Para contornar este fato, o WEP permite que a chave seja modificada para prevenir ataques fortes ao algoritmo, que pode ser implementado em hardware ou software. A razão pela qual o WEP é opcional se deve ao fato que a encriptação não pode ser exportada dos EUA. Isto permite que o padrão IEEE 802.11 seja um padrão fora dos EUA, embora sem o uso de encriptação. [1]

4.2.7
Segurança em WLANs

O padrão IEEE 802.11 inclui dois métodos de segurança: Autenticação e Encriptação. No método de Autenticação, cada estação que se deseja conectar à rede deve ter sua autorização avaliada. Esta avaliação se dá entre o *AP* e cada estação. A Autenticação pode ser de chave compartilhada (*Shared Key*) ou de Sistema Aberto (*Open System*).

No caso de utilização de Sistema Aberto, uma estação pode obter autenticação conhecendo apenas o nome identificador da rede (*SSID*) e solicitando a autenticação. Num sistema totalmente aberto, os *APs* transmitem seus *SSIDs* em intervalos regulares, permitindo assim a autenticação de qualquer usuário sem qualquer preocupação com a segurança da rede. Uma primeira medida de segurança pode ser implementada inibindo a transmissão aberta dos *SSIDs* o que obriga os usuários a conhecer, pelo menos, o nome da

rede. Os *APs* que recebem a solicitação podem autenticar qualquer estação ou apenas um grupo pré-definido de estações, identificadas pelo seu endereço MAC. Esta técnica é chamada de MAC *Adress Filtering* e corresponde a uma medida adicional de segurança.

No caso do uso de chave compartilhada, apenas as estações que possuem uma chave secreta podem se autenticar na rede. A chave compartilhada pode ser utilizada em combinação ou não com MAC *Address Filtering.*

Mesmo que esta estratégia seja implementada, não é possível evitar que um *hacker* altere o endereço MAC de fábrica por um localmente administrado, escolhendo-o aleatoriamente até que um MAC válido seja encontrado. Outra possibilidade é a utilização de um *sniffer* de rede para identificar o tráfego de usuários ativos e seus respectivos MACs. Utilizando-se deste endereço, o *hacker* pode participar da rede como se fosse um usuário válido. Desta maneira, pode-se concluir que a utilização do endereço MAC como método de autenticação não é aconselhável e seguro.

A Encriptação tem como objetivo elevar o nível de segurança de uma WLAN para que este seja comparável ao de uma rede cabeada. A técnica utilizada no padrão 802.11b, conhecida como *WEP* (*Wired Equivalent Privacy*), utiliza um algoritmo de encriptação chamado de RC4. Este algoritmo foi desenvolvido para prover características tais como ser razoavelmente forte, possuir auto-sincronia, eficiência computacional, ser exportável e opcional.

A técnica de segurança WEP também não fornece um nível de segurança ideal contra invasões à rede por *hackers*. Para tal, o IEEE continua estudando novas medidas de segurança para as redes *wireless*. De fato, existem alguns mecanismos básicos de segurança incluídos na especificação e que podem ser empregados de modo a tornar a rede mais segura, mas mesmo com a adoção desses mecanismos, o potencial risco de invasão continua sendo elevado.

Com o objetivo de melhorar os mecanismos de segurança, o IEEE criou um novo grupo de estudo, denominado 802.1x, cuja especificação foi ratificada em Abril de 2002.

Inicialmente, a intenção era padronizar a segurança em portas de redes *wired* ou cabeadas, mas ela se tornou aplicável também às redes *wireless* [10]. No padrão 802.1x, quando um dispositivo solicita acesso a um AP, este requisita um conjunto de credenciais. O usuário então fornece esta informação, segundo uma política repassada pelo AP para um servidor RADIUS, que efetivamente o autenticará e o autorizará. O protocolo utilizado para informar estas credenciais

chama-se EAP (*Extensible Authentication Protocol*), uma base a partir da qual os fabricantes podem desenvolver seus próprios mecanismos para a troca de credenciais. Existem atualmente cinco tipos diferentes de autenticação: EAP-MD5, EAP-TLS, EAP-CISCO (ou LEAP), EAPTTLS e EAP-PEAP.

Motivado pelas deficiências de segurança e gerenciamento apresentadas pelo WEP desde que foi padronizado pelo comitê 802.11b, o IEEE criou ainda um novo grupo de trabalho, o 802.11i, preocupado principalmente em definir boas práticas de segurança. Apesar de o trabalho ainda estar em andamento, muito já foi feito e alguns novos mecanismos já são fornecidos pelos fabricantes para as redes *wireless* legadas, como o PKIP, MIC e o *Broadcast Key Rotation*.

O padrão 802.11i aborda a utilização de um novo mecanismo de criptografia para as novas redes *wireless* 802.11a e 802.11g de alto desempenho, chamado de AES-OCB (*Advanced Encryption Standard – Operation Cipher Block*). Esta nova técnica de criptografia foi recentemente adotada pelo governo norte-americano em substituição ao 3DES. O objetivo é que o AES-OCB seja muito mais forte do que a combinação WEP/PKIP.

4.2.8 Camada MAC

A Camada MAC desempenha as funções de Controle de Acesso ao Meio e para tal, implementa o mecanismo de criação de quadros ou *frames* para atender às redes sem fio segundo o padrão 802.11 que define vários tipos de *frames* que as estações e os *Access Points* utilizam para suas comunicações. Não é o objetivo deste trabalho detalhar os campos de um quadro MAC [1] e as funções de coordenação utilizadas para controlar o acesso ao meio [22]. Porém, um breve descritivo é interessante de ser feito para informação ao leitor.

Estes quadros surgem com a necessidade de se gerenciar e controlar a comunicação sem fio bem como possibilitar o tráfego da informação em si. Desta forma, o padrão 802.11 especifica os *frames* de gerenciamento (*Management Frames*), os *frames* de controle (*Control Frames*) e os *frames* de transporte de dados (*Data Frames*).

a) *Management Frames*

Permitem que as estações remotas e os APs estabeleçam e mantenham as comunicações ativas. Os sub-tipos de *frames* de gerenciamento mais comuns são:

***Frame* de Autenticação**: A remota inicia o processo de autenticação enviando para o AP este quadro contendo sua identidade e o AP responde com

um único quadro de aceitação ou rejeição. Outras formas de autenticação podem ser empregadas envolvendo criptografia mas não são objeto deste estudo.

***Frame* de Des-Autenticação**: Um AP ou uma estação remota podem enviar este tipo de quadro caso desejem terminar uma comunicação.

***Frame* de Solicitação de Associação**: A associação permite que um AP aloque recursos e se sincronize com uma remota a partir do pedido feito por ela.

***Frame* de Resposta à Associação**: Enviado por um AP em resposta (aceitação ou rejeição) a um pedido de associação.

***Frame* de Solicitação de Reassociação**: Enviado por uma remota quando a mesma se movimenta através de vários APs, saindo do que ela está atualmente associada. O AP reassocia e coordena com o AP anterior o envio dos dados por ele armazenados para este novo AP de forma que eles possam ser encaminhados à remota.

***Frame* de Resposta de Reassociação**: Utilizado quando um AP envia o aceite ou a rejeição da reassociação de um terminal.

***Frame* de Des-Associação**: Uma estação ou um AP podem terminar uma associação e para isto utilizam este quadro.

Frame* de *Beacon: Enviados periodicamente pelos APs para difundir parâmetros de rede sobre sua cobertura. As estações varrem os canais e procuram identificar os *beacons* para que possam escolher dentre os APs presentes, qual oferece melhor qualidade de sinal para que se associem.

Frame* de Solicitação de *Probe: Uma estação ou um AP enviam uma Solicitação de *Probe* para obter informações de outra estação ou AP.

Frame* de Resposta de *Probe: Um AP responderá, por exemplo, com este quadro informando sua capacidade, taxa de dados suportada, etc.

b) *Control Frames*

Estes quadros auxiliam na entrega da informação entre a origem e o destino.

***Frame Request to Send* (RTS)**: Representa uma solicitação de envio de dados por parte do transmissor.

***Frame Clear to Send* (CTS)**: Resposta dada por um receptor a um RTS, permitindo que o transmissor envie os dados.

***Frame Acknowledgement* (ACK)**: Envido pelo receptor ao transmissor informando que os dados foram recebidos com sucesso.

c) *Data Frames*

Representam a informação útil proveniente das camadas superiores que será transportada através do meio físico até alcançar o destino.

Protocolos de Acesso ao meio

a) DFWMAC (*Distributed Foundation Wireless Media Access Control*)

Suporta dois sub métodos de acesso ou Funções de Coordenação. Na Função de Coordenação do tipo distribuída ou DCF (*Distributed Coordination Function*), a decisão de quando haverá transmissão é tomada individualmente por cada nó, o que pode resultar em transmissões simultâneas, gerando conseqüentemente, colisões na rede. Por outro lado, quando a Função de Coordenação é dita pontual ou PCF (*Point Coordination Function*), a decisão de quem deve transmitir é centralizada em um único ponto.

b) *Distributed Coordination Function*

Este é o mecanismo básico de acesso ao meio do DFWMAC e é conhecido como CSMA/CA. Sua implementação é obrigatória para todas as estações e APs.

Resumidamente, a estação escuta o meio para determinar se o mesmo está livre, transmitindo seu quadro. Caso contrário, ela aguarda o final da transmissão que está ocupando o meio. Um modo de alocação de *time slots* é usado e só permite que uma transmissão ocorra por uma remota dentro de seu tempo. Entretanto, se nenhuma remota desejar transmitir, a rede entra em um estado onde um método CSMA comum é utilizado até que outra transmissão ocorra e a rede volte à pré-alocação de intervalos de tempo.

O DFWMAC acrescenta ao método CSMA/CA, um mecanismo opcional que envolve a troca de quadros de controle RTS/CTS (*Request to Send* / *Clear to Send*) antes da transmissão dos dados. Quando uma estação ganha a posse do meio, ela transmite um quadro de controle RTS e a estação receptora, em resposta envia um quadro de controle CTS avisando que está pronta para receber os dados. Somente neste momento, o transmissor envia os quadros de dados, que são respondidos com quadros de reconhecimento (ACK) quando as informações são recebidas corretamente.

Essa troca de quadros é mostrada na Figura 4.13 a seguir:

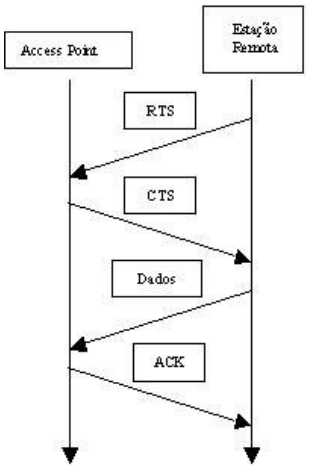

Figura 4.13 – Troca de quadros RTS/CTS

c) *Point Coordination Function*

Esta função é opcional e quando implementada, o DFWMAC divide o tempo em períodos (superquadros): no primeiro, controlado pela PCF, o acesso é ordenado (não ocorrem colisões), no segundo, controlado pela DCF, o acesso baseia-se na disputa pela posse ao meio (podem haver colisões). [2]

4.2.9 Camada Física

A Camada Física das redes sem fio 802.11 especifica duas técnicas de espalhamento espectral, brevemente descritas a frente, denominadas de FHSS (*Frequency Hopping Spread Spectrum*) e a DSSS (*Direct Sequence Spread Spectrum*), que utilizam a faixa de frequência de 2,4GHz chamada de ISM (*Industrial Scientific and Medical*) e juntos com a especificação do infravermelho vão formar as 3 camadas físicas definidas no padrão original. Todas estas técnicas têm o mesmo princípio, que se baseia em espalhar a potência do sinal em uma faixa mais larga do espectro de freqüência, reduzindo a densidade de potência do mesmo em freqüências específicas e, conseqüentemente, reduzindo o efeito de interferências a outros dispositivos que utilizam a mesma faixa. Estas interferências, correspondem àquelas apresentadas por fornos de microondas, por exemplo.

FHSS - *Frequency Hopping Spread Spectrum*

Faz uso de uma portadora de banda estreita que altera a freqüência em operação para valores previamente conhecidos tanto pelo transmissor quanto pelo receptor. A Figura 4.14 [1] apresenta 4 comunicações sendo realizadas simultaneamente, onde se vê que cada uma destas segue um padrão de freqüências distinto e que nunca coincidem no mesmo instante.

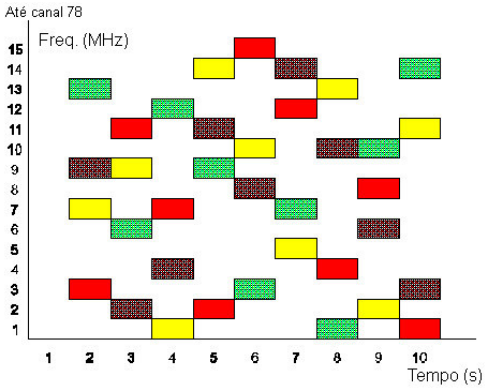

Figura 4.14 – Frequency Hopping Spread Spectrum

Seu funcionamento básico se dá com a estação transmissora enviando e recebendo informação por meio de uma freqüência durante um intervalo muito pequeno de tempo, em seguida salta para outra freqüência, retoma a comunicação e assim por diante.

Apesar dos efeitos das interferências só ocorrerem em pequenos intervalos de tempo, da necessidade do invasor em conhecer a sequência de frequências a seguir para violar a segurança da comunicação e da grande escalabilidade motivada pela diversidade de sequências de saltos em frequência, esta técnica foi praticamente descontinuada com a introdução do 802.11b, que se manteve compatível apenas com a técnica de *Direct Sequence*.

DSSS - *Direct Sequence Spread Spectrum*

Baseia-se em modular o sinal em banda estreita através de um sinal em banda larga de tal maneira que o resultado seja o sinal original espalhado no espectro de frequências. Para tal, é necessário o uso de seqüências PN em conjunto com uma modulação M-PSK, de modo que a fase do sinal modulado varie aleatoriamente de acordo com este código PN (ou *Chipping Code*). A sequência dos procedimentos está representada na Figura 4.15 [1].

O código PN consiste em seqüências finitas de *bits* “1” e “0” (ou *chips*), enviados a uma taxa maior que a taxa dos *bits* de dados. Quanto maior for a sequência de *chips*, mais larga será a banda de transmissão sobre a qual o sinal original é espalhado. A demodulação só poderá ser feita utilizando a mesma seqüência cifrada empregada na modulação. Caso uma seqüência diferente seja utilizada, o sinal obtido será próximo de zero. Assim, para que um "invasor" seja capaz de transpor esta segurança, ele teria que descobrir qual o *Chipping Code* utilizado para espalhar a informação.

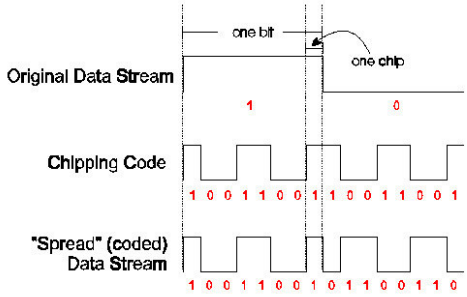

Figura 4.15 – Utilização do Chipping Code

Como resultado da utilização desta técnica, após o espalhamento do sinal, a interferência gerada por outros sistemas é de uma baixa potência em toda a faixa, similar a um ruído branco [14,17,18]. A Figura 4.16 ilustra a influência do sinal interferente (banda estreita) em um sinal espalhado no espectro [18].

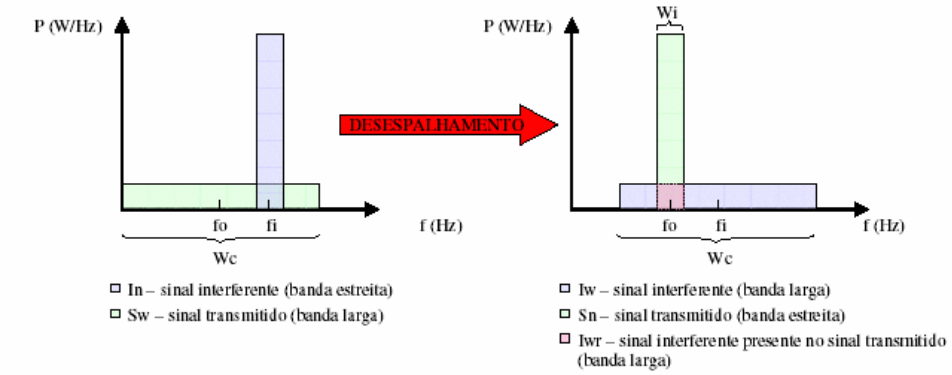

Figura 4.16 – Influência do sinal interferente

Nota-se que o sinal desejado, após “desespalhado” pelo mesmo código utilizado para seu espalhamento, volta a conter a informação original em um sinal banda estreita de alta potência (Wi), enquanto que o sinal interferente, quando espalhado (Wc) por este mesmo código, gera um sinal que interfere no sinal desejado em toda sua faixa, mas com uma densidade espectral de potência baixa.

Canal	Frequência (GHz)
1	2.412
2	2.417
3	2.422
4	2.427
5	2.432
6	2.437

Tabela 4.4 – (a) Canais DSSS

Canal	Frequência (GHz)
7	2.442
8	2.447
9	2.452
10	2.457
11	2.462
12	2.467
13	2.472
14	2.484

Tabela 4.4 – (b) Canais DSSS

Desta maneira, observa-se que até 11 canais de aproximadamente 22MHz podem ser disponibilizados em sistemas DSSS. A Tabela 4.4 mostra estes canais e suas freqüências centrais, onde é possível observar que apenas três canais não são sobrepostos: 1, 6, e 11. Isso faz com que somente três APs podem existir dentro de uma determinada área de cobertura, cada qual com seu canal de comunicação sem que se faça reuso de frequências.

Vale mencionar que nos Estados Unidos, são permitidos os usos dos canais de 1 ao 11, no Reino Unido do 1 ao 13 e no Japão do 1 ao 14.

A Figura 4.17 ilustra uma implementação que utiliza os três canais não sobrepostos discutidos, onde os APs 3 e 4 são configurados no canal 11, os APs 1 e 5 no canal 1 e os APs 2 e 6 no canal 6. É permitido se ter tal configuração em uma rede apenas se os APs que utilizam os mesmos canais não sejam sobrepostos, ou seja, não pode haver intersecção entre eles. A sobreposição de Pontos de Acesso de canais diferentes em um sistema DSSS provê o mesmo balanceamento obtido nos sistemas FHSS.

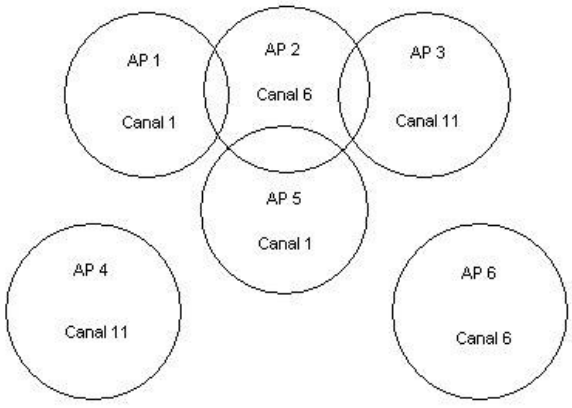

Figura 4.17 – Sobreposição de canais DSSS

Comparação entre FHSS e DSSS

Uma comparação, como a da Tabela 4.5 [1] pode ser feita com relação às particularidades de cada uma destas técnicas. É claro que ambas apresentam pontos fortes e fracos e cabe ao projetista da rede sem fio determinar qual será de melhor valia para seu projeto em particular.

	DSSS	FHSS
Taxa	Acima de 2Mbps	1 ou 2Mbps
Escalabilidade	Baixa	Alta
Densidade de usuários	Baixa	Alta
Custo	Maior	Menor
Processamento de dados	Maior	Menor
Controle de potência	Maior	Menor
Imunidade ao multipercurso	Menor	Maior
Observações	Maiores taxas e distâncias	Menores taxas e distâncias

Tabela 4.5 - Comparativo entre DSSS e FHSS

Em sistemas DSSS não existe a mesma escalabilidade que está presente nos sistemas FHSS, pois, quando utilizam o *Chipping Code* mínimo de 11 *bits*, somente três faixas de freqüências não se sobrepõem em 2.4GHz. Isto resulta em uma limitação de três pontos de acesso co-localizados na mesma área de cobertura. Assim, caso a densidade de usuários de uma determinada região a ser atendida por uma rede WLAN seja alta, a técnica de Salto em Frequência é a mais apropriada.

Uma observação pode ser feita ainda com relação ao controle de consumo de potência. Em sistemas DSSS, as unidades remotas podem confiar mais facilmente na unidade central para determinar quando elas podem entrar no *power safe mode*, o que ocorre de forma contrária em sistemas FHSS que requerem que uma estação de tempos em tempos se preocupe com a necessidade de sincronismo com as demais estações.

Técnicas de Modulação

Diversos fatores devem ser considerados no momento da opção por uma técnica de modulação para uso nas redes locais sem fio. Fatores estes, que envolvem principalmente a Eficiência Espectral que, simplesmente, significa aproveitar ao máximo uma determinada faixa de frequências inserindo nela a maior quantidade possível de canais com condições de comunicação. Esta preocupação é ainda maior em sistemas sem fio, pois o espectro rádio é limitado em faixa, não é infinito. Outro fator que deve ser levado em consideração é a facilidade e custo de implementação da técnica.

O padrão 802.11 original definiu três tipos de camada física diferentes e independentes para as redes sem-fio. Duas delas eram baseadas em técnicas

de espalhamento espectral (*spread spectrum*) conforme já visto, e a terceira baseada no uso de sistemas infravermelho. Todas elas suportam as taxas de transmissão de 1Mbps e 2Mbps especificadas no padrão original. Mais tarde, foram criados novos padrões, como o 802.11a, 802.11b, e o 802.11g. Estes novos padrões visam obter maiores taxas de transmissão, utilizando para isso novas técnicas de modulação.

Esta parte do trabalho procura apresentar de forma resumida as técnicas de modulação utilizadas por estas três camadas, sendo que os novos padrões nas versões “a”, “b” e “g” definem técnicas particulares.

a) Infravermelho - IR

Esta é a camada física menos utilizada atualmente em redes 802.11, talvez por não ter sido difundida e seu uso é bastante restrito.

Seu funcionamento se dá através do uso de comprimentos de onda da ordem do espectro da luz visível e é a mesma faixa espectral utilizada por outros equipamentos eletrônicos comuns, como controles remotos de TVs e aparelhos de som. Diferentemente de outros sistemas infravermelhos, a camada IR do 802.11 não é baseada somente na onda direta, mas principalmente, nas ondas refletidas. E por este motivo é empregado seu uso somente em ambientes fechados, dando-se o nome de Sistema Infravermelho por Difusão.

Uma característica deste tipo de sistema, é que as ondas infravermelhas não ultrapassam paredes ou qualquer outro objeto do gênero, pondendo ser constituída uma rede local em um ambiente fechado, inclusive fazendo fronteira com uma outra sala ao lado. A interferência não existe e a questão da segurança da informação é alcançada com facilidade, ficando a comunicação restrita àquela sala.

Para esta camada física, a modulação utilizada é a PPM (*Pulse Position Modulation*), na Tabela 4.6 [13]. Para 1Mbps utiliza-se o 16-PPM, que faz o mapeamento de 4 *bits* em um símbolo de 16 posições, enquanto para 2Mbps utiliza-se o 4-PPM, mapeando 2 *bits* em um símbolo de 4 posições.

Sixteen-PPM basic rate mapping

Data	16-PPM symbol
0000	0000000000000001
0001	0000000000000010
0011	0000000000000100
0010	0000000000001000
0110	0000000000010000
0111	0000000000100000
0101	0000000001000000
0100	0000000010000000
1100	0000000100000000
1101	0000001000000000
1111	0000010000000000
1110	0000100000000000
1010	0001000000000000
1011	0010000000000000
1001	0100000000000000
1000	1000000000000000

Four-PPM enhanced rate mapping

Data	4-PPM symbol
00	0001
01	0010
11	0100
10	1000

Tabela 4.6 – Mapeamento na modulação PPM

b) IEEE 802.11a

O padrão 802.11a surgiu da necessidade de ser obter taxas de transmissão mais elevadas e utiliza a faixa de freqüências de 5 GHz. Como um dos resultados alcançados com este novo padrão tem-se a redução do nível de interferência, mas apesar disto, problemas surgiram, como a falta de padronização desta faixa de freqüências, de propagação e de incompatibilidade com o padrão original.

A Camada Física destes novos padrões, apresentam uma divisão em outras duas sub-camadas, chamadas de *Physical Layer Convergence Procedure* (PLCP) e *Physical Medium Dependent* (PMD). A sub-camada PLCP na verdade prepara os *frames* (quadros) para transmissão e a sub-camada PMD efetivamente trata da transmissão.

A sub-camada PLCP recebe, portanto, os quadros da camada MAC e monta as chamadas PPDUs (PLCP *Protocol Data Unit*) que serão transmitidas para o meio. Os campos dos quadros PPDUs do 802.11a são os seguintes [21]:

- PLCP *Preamble* – Consiste em 12 símbolos e possibilita o receptor a adquirir um novo sinal entrante;

- *Rate* – Identifica a taxa de dados do quadro conforme Tabela 4.7 [21], porém os campos da PLCP são sempre enviados na mais baixa taxa, ou seja, 6Mbps;

Valor	1101	1111	0101	0111	1001	1011	0001	0011
Taxa	6Mbps	9Mbps	12Mbps	18Mbps	24Mbps	36Mbps	48Mbps	54Mbps

Tabela 4.7 – Valores do campo *rate*

- *Reserved* – Este campo possui valor lógico 0 (zero);
- *Length* – Representa o comprimento do quadro em octetos (*bytes*);
- *Parity* – Baseado nos valores de *Rate*, *Reserved*, e *Length*, este campo fornece a paridade;
- *Tail* - Este campo possui valor lógico 0 (zero);
- *Service* – Consiste de 7 *bits* para sincronismo com o desembaralhador e mais 9 *bits* reservados para uso futuro;
- PSDU – Consiste na informação em si;
- *Tail* – Possui 6 *bits* zerados para funções processadas pelo receptor;
- *Pad Bits* – *Bits* de enchimento.

Neste novo padrão, optou-se por utilizar um esquema de modulação totalmente diferente do anterior, o que causou a incompatibilidade entre as duas especificações. O 802.11a utiliza como técnica de modulação o OFDM (*Orthogonal Frequency Division Multiplexing*), que faz uso de várias sub-portadoras (canal de 20MHz) que permanecem fixas no espectro (não são espalhadas), moduladas em BPSK, QPSK, 16-QAM e 64-QAM. Apesar das mesmas permanecerem fixas em frequência, a técnica é classificada como de Espalhamento Espectral em algumas bibliografias. Também utiliza um código corretor de erros, a *Forward Error Correction* (FEC), com taxas de 1/2, 2/3 ou 3/4. Na sua configuração máxima, o 802.11a pode chegar a 54Mbps, possuindo várias configurações possíveis a partir de 6Mbps. Vale notar que o esquema de modulação também varia conforme for a taxa de transmissão desejada e está ilustrada na Tabela 4.8 [13].

Data rate (Mbits/s)	Modulation	Coding rate (R)	Coded bits per subcarrier (N_{BPSC})	Coded bits per OFDM symbol (N_{CBPS})	Data bits per OFDM symbol (N_{DBPS})
6	BPSK	1/2	1	48	24
9	BPSK	3/4	1	48	36
12	QPSK	1/2	2	96	48
18	QPSK	3/4	2	96	72
24	16-QAM	1/2	4	192	96
36	16-QAM	3/4	4	192	144
48	64-QAM	2/3	6	288	192
54	64-QAM	3/4	6	288	216

Tabela 4.8 – Configurações para o 802.11a

Na técnica FDM da modulação OFDM utilizada por este padrão, o sinal é dividido em partes e cada sub-portadora transmite uma das partes do sinal, sendo a taxa total de transmissão dependente de quantas portadoras são utilizadas. O espaçamento entre os canais (portadoras) deve ser maior que a taxa de símbolos para evitar a sobreposição excessiva dos espectros. No OFDM, as sub-portadoras se sobrepõem, mas são escolhidas sub-portadoras ortogonais, ou seja, que mantém uma certa relação matemática de modo que não haja interferência entre elas. Como elas possuem um espectro do formato [sen(x)/x], colocam-se as sub-portadoras de modo que elas estejam centradas nos zeros das sub-portadoras adjacentes, conforme pode ser observado na Figura 4.18. [13]

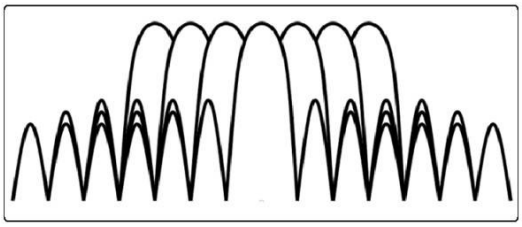

Figura 4.18 – Espectro das sub-portadoras OFDM

De forma a exemplificar as freqüências de operação utilizadas pelo 802.11a, são dispostas abaixo as adotadas pelos Estados Unidos e Japão:

# Canal	Frequência de Operação (MHz)	Domínio Regulatório		Potência Máxima de Transmissão
		Estados Unidos	Japão	
34	5.170		X	40mW
36	5.180	X		
38	5.190		X	
40	5.200	X		
42	5.210		X	
44	5.220	X		
46	5.230		X	
48	5.240	X		
52	5.260	X		200mW
56	5.280	X		
60	5.300	X		
64	5.320	X		
149	5.745			800mW
153	5.765			
157	5.785			
161	5.805			

Tabela 4.9 – Canalização do 802.11a

É importante ainda acrescentar que todos os canais da Tabela 4.9 [21] são restritos para uso em ambientes *indoors* exceto os canais de 52 a 64 nos Estados Unidos que são permitidos também para uso em ambientes *outdoors*.

Levando este conceito para o padrão em questão e sabendo-se que suas sub-portadoras são espaçadas de 312,5KHz, que um símbolo é representado por 48 sub-portadoras de dados, 4 sub-portadoras piloto, mais uma sub-portadora nula, resultando em 53 sub-portadoras, quando estas são multiplicadas pelo espaçamento de 312,5KHz, o resultado apresenta uma banda ocupada de 16,6MHz.

Assim, além de permitir a utilização de baixa potência em cada uma das subportadoras, esta técnica, utilizada no padrão 802.11g e 802.11a, é mais robusta aos efeitos de multipercursos que as técnicas apresentadas [11,14]. Sendo que a versão “a” permite o uso de mais APs sem que haja interferência entre eles do que as versões “b” e “g” (três), aumentando com isso o reuso dos canais.

Uma desvantagem característica deste padrão, é a menor cobertura devido à alta frequência de operação, o que aumenta o custo de implantação de uma rede como esta. O Domínio regulatório de determinadas regiões regula os valores de EIRP e potência máxima, conforme Tabela 4.10 [21].

Domínio regulatório	EIRP máximo	Máxima potência (mW) com antenas de ganho de 6 dBi
Américas	160 mW nos canais 36 a 48	40
Japão	10 mW/MHz	40
Singapura	100 mW	20
Taiwan	800 mW	40

Tabela 4.10 – Níveis de potência do 802.11a

c) IEEE 802.11b

Para se buscar solucionar os problemas de incompatibilidade da versão 802.11a com a versão original, o IEEE desenvolveu um novo padrão, o 802.11b. Basicamente, os campos da PPDU do 802.11b são [21]:

- *Sync* - Este campo procura alternar 1s e 0s de forma a alerter o receptor que um quadro está por vir. O receptor então começa a sincronizar com o sinal;
- *Start Frame Delimiter* - Este campo é sempre “1111001110100000” e define o início do quadro;
- *Signal* - Este campo identifica a taxa de dados do quadro, e seu valor representa a taxa de dados dividida por 100Kbps. Ou seja, este campo valerá “00001010” para 1Mbps, “00010100” para 2Mbps e por aí vai. Porém, os campos do PLCP são sempre enviados na mais baixa taxa (1Mbps) para que o receptor utilize sempre o mecanismo correto de demodulação, pois, este se altera conforme a taxa varia;
- *Service* - Este campo é sempre “00000000” e é reservado para uso futuro;
- *Length* - Representa o comprimento do quadro PPDU;
- *Frame Check Sequence* - Para detecção de erros, utiliza o CRC (16 *bits*);
- PSDU - São os dados propriamente ditos.

Este padrão utiliza a mesma faixa de freqüência de 2,4GHz que o padrão original 802.11 e mantém os modos de operação a 1Mbps e 2Mbps utilizando-se somente o DSSS e colocando o modo FHSS em desuso. A modulação utilizada

para 1Mbps é a DBPSK e para 2Mbps usa-se a DQPSK (similar a anterior porém com 4 fases).

Mas a grande inovação deste padrão foram as taxas alcançadas que chegam a 5,5Mbps e 11Mbps com uma nova técnica de codificação. Diferentemente do 802.11 original, o 802.11b utiliza para estas taxas, ao invés da seqüência de *Barker*, uma técnica de codificação chamada de *Complementary Code Keying* (CCK), que consiste em buscar em uma tabela previamente construída (conjunto de 64 palavras de 8 *bits*) a sequência de espalhamento que corresponde à sequência de *bits* enviada. A técnica CCK funciona somente em conjunto com o DSSS e não funciona em conjunto com o FHSS.

A modulação utilizada é também o DQPSK, para os dois modos, que já faz o mapeamento de 2 *bits* por símbolo. A diferença agora estará no código CCK, que ao invés de mapear um código para um *bit* como fazia o código de *Barker,* irá mapear cada palavra do código em 2 ou 6 *bits*, de acordo com a taxa utilizada, resultando em um total de 4 *bits* por símbolo para 5,5Mbps e 8 *bits* por símbolo para 11Mbps. Um esquema é representado na Figura 4.19 [13].

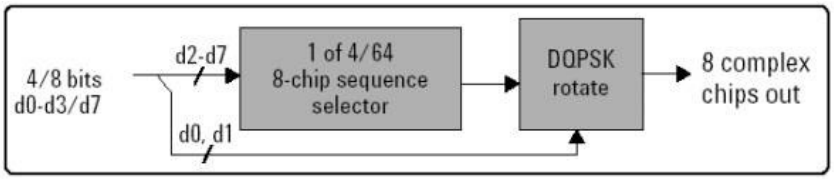

Figura 4.19 – Esquema de modulação 802.11b com CCK

Antes utilizavam-se códigos de 11 *bits*, com taxa de 1 MSps (Mega-símbolo/segundo), resultando em uma taxa de sinalização de 11Mbps. Esta taxa de sinalização é mantida no novo padrão, mas com um novo código de 8 *bits*, teremos uma nova taxa de símbolos de 1,375 MSps. Consequentemente, 5,5Mbps = 1,375 x 4 e 11Mbps = 1,375 x 8. A Tabela 4.11 [13] consolida os valores. Além disto, as Tabelas 4.12 e 4.13 [21] mostram os canais e os níveis de potência para operação em diversos domínios regulatórios.

Data rate	Code length	Modulation	Symbol rate	Bits/Symbol
1 Mbps	11 (Barker sequence)	BPSK	1 MSps	1
2 Mbps	11 (Barker sequence)	QPSK	1 MSps	2
5.5 Mbps	8 (CCK)	QPSK	1.375 MSps	4
11 Mbps	8 (CCK)	QPSK	1.375 MSps	8

Tabela 4.11 – Configurações para o 802.11b

# Canal	Frequência de Operação (MHz)	Domínio Regulatório				
		Américas	EMEA	Israel	China	Japão
1	2.412	X	X		X	X
2	2.417	X	X		X	X
3	2.422	X	X	X	X	X
4	2.427	X	X	X	X	X
5	2.432	X	X	X	X	X
6	2.437	X	X	X	X	X
7	2.442	X	X	X	X	X
8	2.447	X	X	X	X	X
9	2.452	X	X	X	X	X
10	2.457	X	X		X	X
11	2.462	X	X		X	X
12	2.467		X			X
13	2.472		X			X
14	2.484					X

Tabela 4.12 – Canalização do 802.11b

Domínio Regulatório	EIRP Máximo	Ganho da antena (dBi)	Nível máximo de potência (mW)
Américas	4 W	0	100
		2.2	100
		5.2	100
		6	100
		8.5	100
		12	100
		13.5	100
		21	20
EMEA	100 mW	0	100
		2.2	50
		5.2	30
		6	30
		8.5	5
		12	5
		13.5	5
		21	1

Tabela 4.13 – (a) Níveis de potência do 802.11b

Domínio Regulatório	EIRP Máximo	Ganho da antena (dBi)	Nível máximo de potência (mW)
Israel	100 mW	0	100
		2.2	50
		5.2	30
		6	30
		8.5	5
		12	5
		13.5	5
		21	1
China	10 mW	0	5
		2.2	5
		5.2	n/a
		6	n/a
		8.5	n/a
		12	n/a
		13.5	n/a
		21	n/a
Japão	10 mW/MHz	0	50
		2.2	30
		5.2	30
		6	30
		8.5	n/a
		12	n/a
		13.5	5
		21	n/a

Tabela 4.13 – (b) Níveis de potência do 802.11b

d) IEEE 802.11g

O 802.11g é uma evolução do 802.11b e também opera na faixa de 2,4GHz com 30MHz de banda por canal além de manter a compatibilidade com este e a versão “a”. Porém, ele pode ser também visto como uma fusão dos dois padrões, usando o que cada um tem de melhor, sendo a modulação OFDM do 802.11a e a faixa de freqüências do 802.11b. Assim como as vantagens de ambos padrões são postas em conjunto, as desvantagens ou características negativas também se tornam presentes, tais como o limite de 3 APs com canais diferentes em uma área a uma dada potência de operação, como ocorre com o padrão “b”. E as taxas de compatibilidade da versão “b” e “g” são limitadas a 11Mbps.

Além disso, o padrão também define duas técnicas de modulação opcionais, o PBCC (*Packet Binary Convolutional Code*) e o CCK/OFDM, além

das modulações obrigatórias CCK e OFDM. Assim, o padrão 802.11g funcionará identicamente ao 802.11b (1Mbps, 2Mbps, 5,5Mbps e 11Mbps) e também funcionará de modo similar ao 802.11a na faixa de 2,4GHz, possibilitando também todas as suas configurações de velocidade, visíveis na Tabela 4.14 [13].

		802.11b @2.4 GHz		802.11g @2.4 GHz		802.11a @5.2 GHz	
Rate, Mbps	Single/Multi Carrier	Mandatory	Optional	Mandatory	Optional	Mandatory	Optional
1	Single	Barker		Barker			
2	Single	Barker		Barker			
5.5	Single	CCK	PBCC	CCK	PBCC		
6	Multi			OFDM	CCK-OFDM	OFDM	
9	Multi				OFDM, CCK-OFDM		OFDM
11	Single	CCK	PBCC	CCK	PBCC		
12	Multi			OFDM	CCK-OFDM	OFDM	
18	Multi				OFDM, CCK-OFDM		OFDM
22	Single				PBCC		
24	Multi			OFDM	CCK-OFDM	OFDM	
33	Single				PBCC		
36	Multi				OFDM, CCK-OFDM		OFDM
48	Multi				OFDM, CCK-OFDM		OFDM
54	Multi				OFDM, CCK-OFDM		OFDM

Tabela 4.14 – Resumo das configurações para os padrões 802.11

Para manter a compatibilidade com o 802.11b, o 802.11g também suporta todos os seus modos, podendo funcionar normalmente em uma rede 802.11b sem apresentar problemas relacionados às colisões. Uma solução utilizada para contornar este problema são as mensagens RTS/CTS (*Request to Send / Clear to Send*) comentadas neste trabalho. Assim, o AP pode controlar quem irá acessar o meio, evitando colisões entre dispositivos “b” e “g”.

Porém, uma alternativa pode ser implementada com a utilização de uma nova técnica de modulação que é opcional no 802.11g, o CCK/OFDM. Este novo esquema de modulação combina as duas técnicas, onde o cabeçalho dos pacotes é enviado utilizando a modulação CCK e a área de dados (*payload*) é enviada utilizando OFDM. Com isso, os equipamentos 802.11b da rede podem escutar o cabeçalho do pacote e deste cabeçalho podem obter a informação de quanto tempo o pacote vai levar para ser enviado, esperando então este tempo mínimo antes de tentar enviar novamente, evitando-se colisões.

Estes dois tipos de mecanismos para controle de colisões inserem *overhead* adicional à rede, mas que é aceitável diante da necessidade de se obter a compatibilidade com os sistemas atuais.

Quanto ao PBCC, este consiste em uma técnica de uma portadora, com modulação 8-PSK e uma estrutura de código convolucional. Assim como o CCK/OFDM, ele também transmite o cabeçalho do pacote com modulação CCK para manter a compatibilidade com sistemas 802.11b e a máxima taxa de transmissão alcançada fica em 33Mbps.

Como pôde ser visto de forma exemplificada nos padrões 802.11a e 802.11b, as potências dos terminais devem ser limitadas para se evitar ao

máximo as interferências com outros sistemas. Porém, ainda assim, alguns projetistas insistem em utilizar equipamentos com alta potência de transmissão para conseguir uma maior cobertura de sua rede. [23]

Polarização

A polarização é determinada em função da orientação do campo elétrico gerado por uma antena em relação ao solo. No caso de antenas lineares, como as das redes 802.11, o campo elétrico é paralelo ao elemento irradiante e com isso a polarização corresponde à orientação física da antena em relação ao solo, podendo ser definida como "vertical" (antena perpendicular ao solo) ou "horizontal" (antena paralela ao solo). Com base nestes conceitos e de forma a se prover a melhor recepção do sinal possível, a polarização das antenas deve ser sempre a mesma em todos os pontos de comunicação.

Diversidade de antenas

A diversidade de antenas corresponde ao uso de mais de uma antena nos equipamentos de rede sem fio de forma a se alcançar o melhor resultado possível na qualidade da comunicação, procurando-se evitar ao máximo o efeito de multipercurso. Assim, o uso de mais de uma antena permite que se faça uma comparação da intensidade do sinal recebido em cada uma delas e utilizar o mais forte.

Este efeito ocorre quando sinais originados no transmissor, ao se propagarem pelo ar, refletem nos obstáculos encontrados no caminho até o receptor provocando atraso destes sinais com relação aos que sofrem menos espalhamento. Estes atrasos provocam a interferência inter-simbólica que confunde o receptor e provoca erros de leitura da informação. Os receptores então não enviarão os pacotes de reconhecimento (ACKs) e os transmissores retransmitirão os pacotes perdidos o que reduz a vazão da rede.

De forma a exemplificar o problema, valores de atraso da ordem de 50ns (nanosegundos) são encontrados em ambientes residenciais e de escritórios enquanto que valores em torno de 300ns são encontrados em ambientes de fábrica, certamente devido à grande quantidade de objetos metálicos.

Assim, em ambientes onde existe grande quantidade de obstáculos como os ambientes chamados de *indoors* (principalmente em fábricas), o uso da diversidade de antenas é muito útil. Já em ambientes chamados de *outdoors*, esta necessidade se mostra pouco eficaz, bastando uma antena em cada ponto da rede.

Para as redes baseadas em 802.11b o efeito do multipercurso é bastante grande pois este padrão utiliza canais de faixa larga, o que já não ocorre com o

padrões que usam o FHSS devido aos canais de faixa estreita e o salto em frequência e o 802.11a e 802.11g que empregam subcanais de faixa estreita. Com a técnica DSSS, os elementos de mais baixa frequência refletem de forma diferente nos obstáculos do que ocorre com os elementos de mais alta frequência, o que provoca um enorme range de caminhos dos sinais espalhados.

Se durante um *survey* for detectado um número grande de retransmissões, este efeito pode estar presente, mas também pode ser que fontes de interferências externas estejam provocando o mesmo efeito. Atualmente existem no mercado ferramentas que procuram medir o atraso existente em uma rede sem fio auxiliando o projetista. [24]

No maioria das vezes, os equipamentos das redes 802.11, possuem duas antenas que podem ser ativadas ou desativadas pelo próprio usuário, para fins de avaliação de performance. Quando a mesma está desativada, o nível de potência do sinal recebido é muito sujeito a desvanecimento de pequena escala, sendo assim, recomendado seu uso em ambientes *indoors*.

Tráfego

Um fator importante na confecção de uma rede sem fio 802.11, é o dimensionamento do tráfego que será gerado pelos pontos remotos dos usuários. A partir daí, é que se terá condições de definir a quantidade de APs que precisarão ser empregados para cobrir toda a área em questão com a maior eficiência possível.

Cada usuário possui uma demanda de tráfego diferente, mas que dependendo da aplicação pode ser tomada uma média que deve ser multiplicada pela quantidade usuários na rede, obtendo-se etão o *throughput* total gerado em uma área. A capacidade dos APs deve, obviamente ser maior que o *throughput* total gerado pela rede. Porém, um cuidado deve ser tomado quando se considerando o *throughput* nominal dos equipamentos e da regulamentação 802.11, pois não é o valor real a ser consumido pelos usuários. Uma parte deste é destinado à sinalização entre as pontas e com isso, o valor do *trhoughput* real varia em torno de 45% do valor nominal.

Interferências

Por fim, este item procura trazer argumentos que fazem entender a importância que este aspecto possui diante de um projeto de redes sem fio, pois a interferência degrada o sinal e diminui as taxas de transmissão, fazendo com que a rede como um todo perca em performance.

Porém, existem dois tipos de interferência que se fazem presentes: a interferência entre os sistemas e a interferência dentro de um mesmo sistema.

Aquelas relacionadas à sistemas diferentes são provocadas pelo uso de fornos de microondas, telefones sem fio (2.4GHz), aparelhos *Bluetooth* como celulares, PDAs, além, é claro, de outras redes WLAN. Algumas destas interferências já foram comentadas anteriormente neste capítulo.

Segundo [19], os fornos de microondas emitem sinais que variam na faixa de 2450MHz a 2458MHz e como algumas redes Wi-Fi utilizam a faixa de 2412MHz a 2462MHz, elas sofrem interferências destes dispositivos. Os valores de potência próximo de um forno de microondas são muito elevados. Medidas indicam níveis de aproximadamente 18 dBm, a uma distância de 3 metros do aparelho, potência esta, que é equivalente a potência de irradiação máxima de muitos dos *APs* que se encontram no mercado.

Outro fato relevante em relação às interferências geradas por fornos de microondas é que o sinal gerado por este equipamento é emitido em pulsos de aproximadamente 10μs de duração. Como o período de duração de um símbolo no 802.11 é de 1μs, o receptor sofre um surto de erro longo, o que provavelmente inviabilizará a comunicação.

Medidas efetuadas em ambientes com fornos de microondas [20], sugerem que a distância segura entre a rede *WLAN* e o equipamento interferente deve ser de no mínimo 20 metros, considerando que haja visada direta entre a fonte interferente e os equipamentos interferidos.

A interferência entre dispositivos *Bluetooth* e as *WLANs* em um mesmo ambiente é inevitável, pois os equipamentos *Bluetooth* operam na faixa de 2400MHz a 2485MHz. A probabilidade de colisão de pacotes transmitidos em uma rede *WLAN* e pacotes transmitidos por dispositivos *Bluetooth* varia de 48% a 62% [20]. Como as duas tecnologias coexistirão por bastante tempo, a solução para um bom funcionamento de ambas em um mesmo ambiente, é manter terminais *Wi-Fi* a uma distância mínima de terminais *Bluetooth*. Dada a baixa potência dos dispositivos Bluetooth, uma separação de 10 metros talvez seja o suficiente.

Os outros dispositivos que utilizam a mesma faixa de freqüência das *WLANs*, como telefones sem fio e outras *WLANs* próximas são claras fontes de interferência, devendo ser consideradas no processo de planejamento.

Com relação às interferências dentro de um mesmo sistema, estas dizem respeito aos canais utilizados para comunicação, conforme já apresentado neste capítulo e refletido na Tabela 4.15.

ID do canal	Freq. Central
1	2412 MHz
2	2417 MHz
3	2422 MHz
4	2427 MHz
5	2432 MHz
6	2437 MHz
7	2442 MHz
8	2447 MHz
9	2452 MHz
10	2457 MHz
11	2462 MHz

Tabela 4.15 – Canalização do padrão IEEE 802.11 no Brasil (2,4GHz)

Novamente, somente 3 destes canais podem coexistir sem que haja interferência entre eles, como demonstra a Figura 4.20.

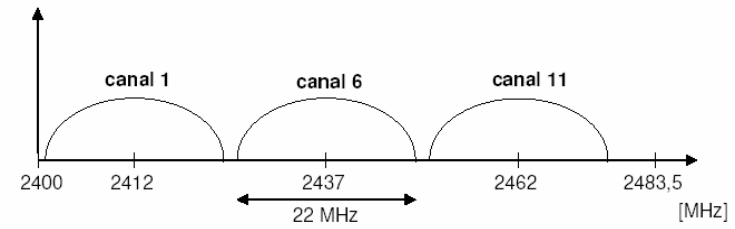

Figura 4.20 – Canalização do padrão IEEE 802.11 no Brasil (2,4GHz)

Portanto, para garantir que não haverá interferência no próprio sistema, é necessário os canais que cobrem áreas em comum não possuam superposição e o reuso dos canais aconteça em áreas onde não há cobertura comum, possibilitando o *roaming* entre as áreas e ao mesmo tempo não causando níveis relevantes de interferência.

Alternativamente, algumas soluções podem ser apresentadas como forma de se tentar reduzir o nível destas interferências, porém, não sendo ainda a melhor alternativa. Pode-se por exemplo, reduzir a potência dos *Access Points*, fazer uso de antenas mais diretivas ou aumentar a distância entre os APs para que as áreas cobertas sejam menores ou afastadas umas das outras, evitando-se com isso, as sobreposições.