

LAN Sem Fio

Trabalho da disciplina de Fundamentos de Redes de Comunicação

Sinval Nascimento – *sinvalnascimento@uol.com.br*

Ezequiel Pereira – *ezequiel000@yahoo.com*

Daniel Reis – *danieldosreis@yahoo.com.br*

Nicolau Werneck – *nwerneck@cefala.org*

Leonardo Araujo – *leoca@cefala.org*

UFMG — Universidade Federal de Minas Gerais,
Belo Horizonte, MG, Brazil

3 de Fevereiro de 2004

1 Introdução

Durante os últimos anos, o mercado de comunicações sem fio teve um tremendo crescimento. A tecnologia sem fio atinge agora, ou é capaz de atingir, qualquer localidade na superfície do planeta. Centenas de milhões de pessoas estão trocando informações todos os dias utilizando pagers, telefones celulares e outros produtos que fazem uso da tecnologia de comunicação sem fio. Com o enorme sucesso da telefonia e serviços de mensagens sem fio, não é de se surpreender que essa tecnologia, também conhecida como wireless, esteja começando a ser aplicada no campo da computação pessoal e de negócios. Não mais limitadas pelos arreios das redes com fio, as pessoas terão acesso e compartilharão informação numa escala global, em quase todos os lugares onde se aventurarem. Este trabalho trará informações sobre wireless local area networks (wireless LANs) e apresentará uma breve discussão sobre os padrões que vêm sendo desenvolvidos, com ênfase no IEEE 802.11.

As redes sem fio (wireless LANs - WLANs) são um sistema flexível de comunicação que pode ser implementado como extensão ou uma alternativa às redes de comunicação com fio. As WLANs utilizam ondas eletromagnéticas para transmitir e receber dados através do espaço, minimizando assim a necessidade de conexões com fio.

Nos últimos anos as redes sem fio tem ganhado uma grande popularidade. Algumas organizações tem achado que as redes sem fio são indispensáveis devido a possibilidade de mobilidade, realocação, ad hoc networking, e cobertura de locais inaccessíveis aos cabos. Alguns dos mercados onde as WLANs se tornaram mais populares são: saúde, vendas, indústria, armazenamento e meio acadêmico.

1.1 Motivação e Aplicações

Desde o sucesso do projeto Ethernet e outros padrões similares, a tecnologia de local area networks (as LANs) aflorou tanto no setor público como privado. Os protocolos padrão de LAN, que operam a altas velocidades e com hardware de baixo custo, podem levar a intercomunicação digital a praticamente qualquer computador. Atualmente, organizações de todos os tamanhos acessam e disponibilizam informações através de uma rede digital. O poder de compartilhamento e computação distribuída e cooperativa começa agora a ser percebido como uma forte realidade. Todavia, até muito recentemente, as LANs eram limitadas a serem estruturas físicas, fortemente cabeadas dentro de algum edifício. Mesmo com o acesso por telefone, os nodos das redes eram limitados a fazer acesso por linhas de conexão longas e cabeadas. Muitos usuários de rede, especialmente usuários móveis da área comercial, médica, fábricas e universidades, para citar alguns, encontraram enormes benefícios nas capacidades adicionais providas pelas wireless LANs.

O maior benefício e motivação para as wireless LANs é a sua incrível mobilidade. Diferentemente das redes convencionais, usuários de redes sem fio podem se mover quase sem restrição e acessar as LANs de praticamente todos os lugares. Exemplos práticos de uso para as redes wireless ficam a cargo da

imaginação de cada projetista.

Profissionais médicos podem obter não somente dados de seus pacientes como também ter acesso a sinais vitais em tempo real, sem falar outras referências que podem ser acessadas a partir de um leito de hospital, sem depender de consultas a papéis e outras formas físicas de armazenamento de informação. Trabalhadores nas fábricas podem acessar partes e especificações de projetos sem as impraticáveis ou impossíveis redes cabeadas. Conexões sem fio juntamente com sensores em tempo real permitem a um engenheiro diagnosticar e a manter o bom funcionamento de equipamentos, mesmo num ambiente hostil e prejudicial à saúde humana. O controle de estoque em armazéns pode ser feito de forma rápida e efetiva com o auxílio de unidades móveis diretamente conectadas a base de dados central. Até mesmo etiquetas "inteligentes", feitas com tecnologia wireless e completadas com visores de cristal líquido (LCD), permitirão os comerciantes eliminarem discrepâncias entre os preços previstos no gerenciamento de estoque e os preços nas prateleiras. As possibilidades são quase infinitas.

1.2 Histórico

A primeira rede a combinar comutação de pacotes e comunicação de rádio foi desenvolvida no Havaí, EUA, em 1971, para interligar sete campi distribuídos por quatro ilhas com o computador central da ilha de Oahu. Ironicamente, nasceu desta experiência a tecnologia amplamente utilizada em redes locais fixas: Ethernet. Limitações de largura de banda e da tecnologia de transmissão não permitiram que o projeto resultasse na utilização em massa de redes sem fio. Contudo, dois fenômenos consolidados ao longo da última década, miniaturização e comunicações pessoais sem fio, devolveram a redes locais sem fio grande interesse em pesquisa e desenvolvimento, culminando com o aparecimento das primeiras redes sem fio comerciais na primeira metade dos anos 1990.

As primeiras redes locais sem fio de rádio-frequência implementaram ou transmissão spread spectrum ou transmissão infravermelha difusa. A transmissão spread spectrum destas redes utiliza as bandas ISM (Industrial, Scientific and Medical), compostas por três bandas, de 902 a 928 MHz; de 2,40 a 2,4835 GHz e de 5,725 a 5,85 GHz, Todavia, apresentavam baixa interoperabilidade, pois cada rede apresentava um conjunto de características único, já que fabricantes construía suas redes conforme critérios próprios. É possível encontrar, portanto, redes com vazões e alcances diferentes, empregando diversos critérios de segurança e definindo a subcamada MAC (Medium Access Control) com abordagens particulares.

O grupo que criou o padrão IEEE 802.11 (Wireless LAN) foi formado em 1987 para começar uma padronização das WLANs usando tecnologia spread spectrum para utilizar a banda ISM.¹ Apesar do espectro alocado irrestrito e

¹ISM - Industrial Scientific and Medical. Em 1997 o FCC (Federal Communications Commission) alocou 300MHz de faixa de espectro não licenciado na banda de 5.725-5.825GHz para o propósito de dar suporte a um serviço de comunicação spread spectrum de baixa potência e licença livre.

intenso interesse da indústria, o movimento da WLAN não ganhou força até o fim da década de 90 quando a fenomenal popularidade da Internet combinado com a larga aceitação de portáteis, os laptops finalmente fizeram da WLAN um importante segmento de rápido crescimento do mercado moderno das comunicações sem fio. O padrão IEEE 802.11 ficou pronto 1997 e forneceu uma interoperabilidade entre os fabricantes de WLANs usando taxas de transferência de dados de 2Mbps (caído para 1Mbps em condições ruidosas). Com o padrão internacional aprovado, muitos fabricantes começaram a convergir para uma interoperabilidade e o mercado começou a acelera rapidamente. Em 1999, o padrão IEEE 802.11 de alta velocidade (IEEE 802.11b) foi aprovado, fornecendo uma nova capacidade de transmissão para os usuários, agora de 11Mbps e 5.5Mbps além do original 2Mbps e 1Mbps do IEEE 802.11 que foram mantidos.

À medida em que se elaborava o padrão, os fabricantes de rede passaram a formular planos de migração de seus produtos, de acordo com as exigências feita pela norma 802.11. O atraso na elaboração do padrão juntamente com um mercado aquecido, determinou que muitos produtos fossem lançados no mercado, mas com garantias de uma transição suave para as especificações do 802.11.

O último padrão IEEE 802.11a será capaz de fornecer uma taxa de transmissão de até 54Mbps na banda de 5GHz. O padrão IEEE 802.11b utilizando DS-SS (Direct Sequence Spread Spectrum) foi denominado Wi-Fi pela *Wireless Ethernet Compatibility Alliance*, um grupo promoveu a adoção do padrão IEEE 802.11b DS-SS WLAN nos equipamentos e a interoperabilidade entre os fabricantes. O IEEE 802.11g está desenvolvendo o CCK-OFDM (Complementary Code Keying Orthogonal Frequency Division Multiplexing) nas faixas de 2.4GHz (802.11b) e 5GHz (802.11a) e irá suportar capacidade de roaming e utilização de banda dupla para redes WLAN públicas, suportando compatibilidade com a tecnologia 802.11b.

De acordo com um estudo do Giga Information Group, a América Latina, a China e a Índia terão o crescimento mais rápido na adoção da tecnologia móvel sem fio, em três anos. Mundialmente, o crescimento deve ultrapassar 27%, até 2005.

No mercado latino-americano, a adoção da tecnologia móvel wireless deve crescer de 21% em 2002, para 31,8% nos próximos três anos. Neste período, os especialistas do Giga indicam que as iniciativas de mobile business (m-business) serão tão importantes quando o atual e-business.

"Hoje, 141 países permitem a competição móvel, o dobro do número de países que trabalham com a concorrência em linhas fixas", destaca o estudo divulgado em setembro de 2002.

A avaliação também prevê que, até o início de 2003, a maior parte do mercado mundial atuará em "crossover", ou seja, com um número maior de assinantes de serviços móveis do que fixos. Tal comportamento já é observado em oito países latino-americanos, segundo o Giga.

Figura 1: Padrões de WLANs do IEEE

1.3 Vantagens

- **A mobilidade aumenta a produtividade** - as redes sem fio fornecem aos usuários acesso em tempo real a informações em qualquer lugar dentro de suas organizações.
- **Facilidade de Instalação** - a instalação de uma rede sem fio é rápida e fácil, sem a necessidade de puxar cabos através das paredes e telhados.
- **Flexibilidade na Instalação** - a tecnologia sem fio permite a rede se estender a lugares onde eram proibitivos utilizando-se fios.
- **Preço reduzido de manutenção** - embora o investimento inicial seja maior do que para uma rede com fio, a rede sem fio pode ter um custo de ciclo de vida inferior.
- **Escalabilidade** - as redes sem fios podem ser configuradas para diversas topologias para satisfazer aplicações específicas. As configurações são facilmente modificadas.

1.4 Desvantagens

- **Qualidade de serviço:** a qualidade do serviço provido ainda é menor que a das redes cabeadas. As principais razões para isso são a pequena banda passante devido às limitações da radiotransmissão e a alta taxa de erro devido à interferência.

- **Custo:** atualmente, o preço dos equipamentos de redes sem fio são mais altos que os equivalentes em redes cabeadas.
- **Segurança:** intrinsecamente, os canais sem fio são mais suscetíveis a interceptores não desejados. O uso de ondas de rádio na transmissão de dados também pode interferir em outros equipamentos de alta tecnologia, como por exemplo, equipamentos utilizados em hospitais. Além disso, equipamentos elétricos são capazes de interferir na transmissão acarretando em perdas de dados e alta taxa de erros na transmissão.
- **Baixa transferência de dados:** embora a taxa de transmissão das redes sem fio esteja crescendo rapidamente, ela ainda é muito baixa se comparada com as redes cabeadas.
- **Estações Perdidas (hidden node):** Um dos grandes problemas em redes sem fio ocorre quando uma estação fica incomunicável por um período de tempo com o AP. São vários os motivos porque isto ocorre. O desligamento da estação móvel, a saída da estação móvel da área de atuação do ponto de acesso ou entrada da estação móvel em uma área onde as ondas de rádio proveniente de outro lugar não se propagam ou locais com grande degradação de sinal, que pode ser por motivos geográficos ou ambientais (área de sombra).

2 Componentes Físicos de Redes Sem Fio (Hardware)

Os componentes essenciais de LANs sem fio são os mesmos ou similares aos das LANs convencionais (cabeadas). A mudança maior está na substituição de cartões de interface de redes Ethernet e Token Ring pelos seus similares nas LANs sem fio, e a ausência de conectores de cabo, e do próprio cabo, evidentemente.

Os principais componentes são:

- **Cartões de interface de rede NICs (Network Interface Cards):** Este deve ser da forma PCMCIA para notebooks ou cartões padrão ISA para computadores de mesa (PC).
- **Antenas para captar e difundir sinais de rádio:** Diversos tipos de antenas podem ser utilizados.
 - Antenas direcionais que levam sinais de rede para longas distâncias, tais como edifício para edifício. Elas são montadas em postes ou mastros em telhados para assim aumentar o alcance.
 - Antenas onidirecionais que são usadas em sistemas onde as comunicações são baseadas em células.

- **Pontos de acesso ou módulos de controle:** Equipamento com uma porta Ethernet e um slot PCMCIA para placa de rede sem fio, que funciona como bridge (ponte) entre a rede Ethernet tradicional e a rede sem fio, cada ponto de acesso pode atender até 200 estações, sendo recomendável um número de até 50 estações por ponto de acesso de forma a manter adequado o nível de utilização da rede é composta por uma pequena antena opcional para ser utilizada no ponto de acesso quando este é colocado dentro de um rack ou em PCs de forma a aumentar o alcance do sinal. Cria uma célula com raio de até 171m de alcance em ambiente aberto e 53m de alcance em ambiente semi-aberto.

3 Elementos Básicos de uma Wireless LAN

A topologia de uma rede WLAN é composta pelos seguintes elementos principais:

- **BSS - Basic Service Set:** corresponde a uma célula de comunicação wireless.
- **STA - Stations:** são as estações de trabalho que comunicam-se entre si dentro da BSS.
- **AP - Access Point:** funciona como uma bridge entre a rede wireless e a rede tradicional. Coordena a comunicação entre as STA dentro da BSS
- **ESS - Extended Service Set:** consiste de várias células BSS vizinhas que se interceptam e cujos AP estão conectados a uma mesma rede tradicional. Nestas condições uma STA pode movimentar-se de um BSS para outro permanecendo conectada à rede. Este processo é denominado roaming. O roaming entre diferentes células é definido de forma superficial no padrão, deixando para cada fabricante os detalhes de implementação. Desta forma, para tornar possível a interoperabilidade do roaming entre equipamentos de diferentes fabricantes, foi definido o IAPP (Inter-Access Point Protocol) adotado por um grupo de empresas.

4 Topologia de uma Wireless LAN

A maioria das WLANs de hoje em dia são redes com infra-estrutura. Nelas, a transferência de dados acontece sempre entre uma estação e um ponto de acesso. Os APs são nós especiais responsáveis pela captura e retransmissão das mensagens enviadas pelas estações. A transferência de dados nunca ocorre diretamente entre duas estações. O AP também pode agir como uma ponte para outra rede (cabeadas ou sem fio).

Essa estrutura é típica de uma rede com topologia em estrela, onde um elemento central (no caso, o AP) controla o fluxo de toda a rede. Esse tipo de rede pode usar diferentes esquemas de acesso, com ou sem colisão. Colisões

Figura 2: Configuração típica de uma WLAN

podem ocorrer se as estações junto com o AP não são coordenados. Entretanto, quando somente o AP controla o acesso ao meio, nenhuma colisão é possível.

Redes com infra-estrutura perdem um pouco da flexibilidade que as redes sem fio podem oferecer. Por exemplo, elas ficam inutilizadas no caso de um terremoto que provoque a destruição de toda infra-estrutura da rede. As redes de telefonia celular são um caso típico de redes com infra-estrutura. As redes de telefones celulares que funcionam através de satélites também possuem uma infra-estrutura - os próprios satélites. Portanto, uma infra-estrutura não implica necessariamente em uma rede fixa cabeada.

Já as redes Ad Hoc não necessitam de nenhuma infra-estrutura para funcionar. Cada estação se comunica diretamente com outra estação. Nenhum AP é necessário para controlar o acesso ao meio. Uma estação A só pode se comunicar com uma estação B se B estiver dentro do raio de ação de A ou se existir uma ou mais estações entre A e B que possam encaminhar a mensagem. Entenda-se por raio de ação a área de cobertura de uma estação, ou seja, todos os pontos geográficos onde o sinal desta estação chegue com um mínimo de clareza.

Numa rede Ad Hoc, a complexidade de cada estação é alta porque toda estação tem que implementar mecanismos de acesso ao meio, mecanismos para controlar problemas com "estações escondidas" e mecanismos para prover uma certa qualidade de serviço.

As duas variantes básicas de redes sem fio (especialmente WLANs), rede baseada em infra-estrutura e rede Ad Hoc, nem sempre aparecem na sua forma pura. Existem redes que contam com AP e serviços básicos de infra-estrutura (exemplo: controle de acesso ao meio), mas também permitem uma comunicação direta entre duas estações sem fio.

O IEEE 802.11 é uma típica rede com infra-estrutura, mas que pode suportar uma rede Ad Hoc. Entretanto, muitas implementações só funcionam na versão com infra-estrutura. O padrão IEEE 802.11 será apresentado mais adiante com mais detalhes.

5 Camada de Enlace

Redes sem fio impõe restrições ao funcionamento do protocolo de enlace que não existem em rede com fio. Redes com fio foram projetadas sobre as seguintes premissas:

- O grupo de estações compartilha um meio a qual apenas elas tem acesso;
- Todas estações são capazes de se contatar diretamente;
- Não é esperado que estações entrem ou saiam da rede com frequência.

Enquanto isto, nas redes sem fio:

- A topologia é dinâmica e não completamente conectada;
- Não existe certeza absoluta da disponibilidade ou não das estações para receberem quadros, devido tanto à presença da estação no meio quanto à possibilidade das estações entrarem em modo de economia de energia;
- É típico que estações saiam da rede subitamente, ou mudem subitamente seu ponto de operação;
- Não existe a sigilosidade implícita no uso de guias de onda.

O padrão IEEE802.11 foi desenvolvido com os requisitos de que as estações atendidas fossem tanto portáteis quanto móveis. Esta característica de mobilidade forçou que a camada de enlace adquirisse características que não fazem parte de seu papel tradicional.

5.1 Entidades da Rede

No padrão IEEE802.11 define-se uma unidade básica de construção da rede chamada conjunto básico de serviço, ou BSS (*Basic Service Set*). Um BSS é uma espécie de região de operação cujas estações podem se comunicar entre si. Uma rede constituída de um único BSS é conhecida como uma rede *ad hoc* devido à inexistência de um planejamento prévio, inerente a redes com fio. Um BSS seria uma rede local em uma analogia do enlace do IEEE802.11 com o padrão tradicional IEEE802.

Esta associação de estações aos BSS são dinâmicas, e envolvem o uso do serviço de sistema de distribuição.

Sistema de distribuição, ou DS (*distribution system*), é o componente estrutural que interliga diferentes BSS para formar uma única rede lógica em que estações não precisam dividir um mesmo meio físico para se contatar. O padrão IEEE802.11 não especifica o meio físico do sistema de distribuição. Ele pode funcionar tanto sobre uma rede sem fio quanto sobre uma rede Ethernet, por exemplo.

Um ponto de acesso, ou AP (*access point*), é uma estação que provê serviços do sistema de distribuição a outras estações do BSS a que pertence, além de funcionar como uma estação normal.

O conjunto do AP e do DS fazem entre outras coisas o papel de pontes (*bridges*) na analogia citada acima. Eles permitem a definição de um conjunto estendido de serviços, ou ESS (*Extended service set*) unindo diferentes BSS em um único meio lógico (3).

Diferentes BSS e ESS podem se sobrepor de todas as maneiras. Não existem limites lógicos, e redes distintas criadas por diferentes corporações podem funcionar sobre um único meio físico.

Figura 3: Esquema Lógico dos Enlaces

Ainda existe uma entidade chamada portal, que é capaz de conectar logicamente uma rede IEEE802.11 com outras redes IEEE802, emulando um bridge convencional para cada rede.

6 Serviços

As estações e pontos de acesso são caracterizadas pelos serviços que eles atendem. Para o DS, apenas os serviços são especificados, flexibilizando sua implementação ao máximo.

Casos típicos de pontos de acesso incluem:

- AP conectando-se a outro via rede sem fio, promovendo a integração da rede;
- AP conectando-se a uma rede IEEE802.3, funcionando como ponte;
- AP funcionando como gateway de uma LAN, e servindo como comutador tanto a computadores ligados por IEEE802.3 quanto IEEE802.11.

Os serviços disponibilizados por todas as estações são:

- Autenticação;
- Desautenticação;
- Privacidade;
- Entrega de MSDU (*MAC service data unit*, pacotes de informação).

Os serviços relativos ao sistema de distribuição são:

- Associação;
- Disassociação;
- Distribuição;
- Integração;
- Reassociação.

O serviço de distribuição se refere à transferência de pacotes de um BSS para outro do mesmo ESS. O serviço de integração se refere à distribuição de pacotes para redes ligadas através de portais.

Três serviços são relacionados ao gerenciamento de associação de clientes na rede. Associação e reassociação são serviços requisitados por estações para que o sistema de distribuição mantenha atualizada uma espécie de tabela de roteamento que relaciona cada estação com um único ponto de ligação. Disassociação é um serviço que pode ser requisitado por qualquer estação para informar a saída de uma cliente da rede.

Redes com fio, de dependerem de uma conexão maciça, que deve ser habilitada por usuários humanos. Esta característica de redes com fio dotam o sistema de um processo de autenticação e também de um esquema de segurança que são intrínsecos a elas.

Para dotar redes sem fio de semelhantes características, o nível de enlace foi dotado de facilidades básicas de autenticação e criptografia, que são os três primeiros serviços fornecidos pelas estações em geral. O protocolo de encriptação é o chamado WEP, *wireless equivalent privacy*.

7 Quadros de MAC

7.1 Campos

Os quadros de MAC do IEEE802.11 são chamados de unidades de dados de protocolo do MAC, ou MPDU (*MAC protocol data units*).

Existem três diferentes tipos de quadro de MAC neste padrão. Eles são compostos por diferentes campos:

- **Controle de quadro :**

2		2		4			
Versão		Tipo		Subtipo			
1	1	1	1	1	1	1	1
P DS	D DS	MF	R	G	MD	WEP	Or

Versão, Tipo e Subtipo identificam a estrutura do quadro. A seguir encontramos os flags “para DS”, “do DS”, “mais fragmentos”, “retry”, “gerenciamento de energia”, “mais dados”, WEP e “ordenado”.

Os campos relativos ao DS são necessários para se realizar o roteamento de pacotes dentro do sistema de distribuição. Os últimos dois campos são flags que sinalizam o uso de encriptação e a permissão de se desordenar pacotes na transmissão.

- Duração/ID:

Bit 15	Bit 14	Bits 13-0	Usage
0	0-32767		Duração
1	0	0	Sem-contenção
1	1	1-2007	ID de Associação

- Endereço: Existem quatro campos de endereço. Eles podem identificar: BSS, remetente, destinatário, transmissor e receptor.

O campo de identificação do BSS carrega o endereço da estação que é o AP, ou um número aleatório no caso de redes *ad hoc*. Transmissor e receptor se referem às estações intermediárias por onde transita o pacote naquele instante. Estes endereços intermediários serão utilizados quando o sistema de distribuição entra em funcionamento.

- Controle de Seqüência:

4	12
Número do fragmento	Número de seqüência

Estes campos identificam pacotes nos casos de haver necessidade de retransmissão, reordenação ou ou fragmentação.

- Corpo

O corpo do quadro varia de função de acordo com o tipo de quadro, podendo até mesmo não existir. É neste campo que eventualmente irão trafegar dados para camadas superiores. O corpo pode chegar a abrigar até 2312 octetos.

- Checagem de Erros.

Este campo contém um código CRC de 32 bits calculado a partir de todo o resto do quadro.

7.2 Tipos de Quadro

Os tipos de quadros são: gerenciamento, controle e dados. Os campos são unidos de diferentes maneiras para se criar quadros de cada tipo e subtipo.

7.2.1 Controle

Os quadros de controle são utilizados na administração da transmissão de quadros, como para fazer comunicação dentro de um esquema de requisição com confirmação (RTS/CTS/ACK). Este tipo de comunicação não é utilizada em Ethernet, por exemplo, e é mais uma amostra das funcionalidades de camadas superiores do modelo ISO/OSI que se fazem necessárias em redes sem fio.

7.2.2 Dados

O formato dos quadros de dados não variam com o subtipo. Seus campos são:

2	2	6	6	6	2	6	0-2312	4
FC	D/ID	A1	A2	A3	SC	A4	Corpo	FCS

Os campos A1, A2, A3 e A4 são endereços. Seus significados são determinados pelos flags relativos ao sistema de distribuição no campo de controle do quadro.

É estranho para alguém acostumado com Ethernet ver quatro campos de endereço. São precisos mais especificações de endereçamento porque não há certeza de que uma interface da estação esteja ligada a apenas um meio compartilhado pelas outras máquinas da rede. O meio a que uma interface está conectada é todo o volume com que ela consegue trocar dados. Uma única estação pode fazer parte de mais de um BSS que não necessariamente está acessível a outras estações (4).

Figura 4: Estação em diferentes BSS

Assim torna-se necessário que a estação transmissora sempre indique o BSS a que ela está se referindo quando transmite um pacote. A identificação do BSS

é o terceiro campo de endereço nos três casos de transmissão em que há troca de dados entre uma estação e outra, ou entre uma estação e um AP.

O quarto caso é o da transmissão direta entre dois AP, o que permite a criação de um DS usando o próprio protocolo, de forma integrada com o resto da rede. Neste caso os quatro campos são os endereços do remetente original, do destinatário final do pacote, do transmissor instantâneo e do próximo receptor. Estes dois últimos são os AP realmente envolvidos na transmissão deste pacote, cuidando assim do roteamento do pacote dentro do ESS, que é uma espécie de interrede.

O campo de duração é utilizado para determinação de velocidades de transmissão.

Quadros de dados são capazes de desempenhar o papel de alguns quadros de controle.

7.2.3 Gerenciamento

Os quadros de gerenciamento também são invariantes com relação ao subtipo. Sua estrutura é similar à do quadro de dados, mas sem o quarto campo de endereço.

2	2	6	6	4	2	0-2312	6
FC	D/ID	A1	A2	BSSID	SC	Corpo	FCS

O campo de corpo de quadros de gerenciamento são padronizados para cada subtipo. Eles incluem informações necessárias para se realizar os serviços referentes a cada subtipo, como sincronização dos relógios das estações, pedidos de associação e autenticação, e sondagem.

8 Funções de Subcamada

8.1 Acesso ao meio

As duas funções mais fundamentais das subcamadas de MAC são as funções distribuída (DCF, *distributed coordination function*) e pontual (PCF *point coordination function*) de coordenação.

O DCF é um método de controle de acesso ao meio chamado CSMA/CA (*Carrier sense multiple access / collision avoidance*). Ele é similar ao CSMA/CD, exceto que após detectar que o meio está livre, a estação transmissora inicialmente sorteia um tempo de espera antes de iniciar uma transmissão, como faria no caso de uma colisão.

Existem ainda os chamados métodos virtuais de se evitar colisões. Um deles é o uso de um esquema de requisição de transmissão de pacotes (RTS/CTS). O IEEE802.11 é capa de operar sob este método, mas não é requerido que ele seja utilizado. Seu uso depende das condições do meio e da rede.

O outro esquema virtual para evitar colisões é o uso do campo de duração. Este campo carrega o tempo em milissegundo que a estação está alocando para

si. Este tempo leva em consideração quanto tempo será necessário para se transmitir o pacote atual, o tempo necessário entre pacotes, e ainda o tempo de transmissão de um pacote de ACK de resposta. Esta alocação evita que o pacote de cause uma colisão.

A outra função de acesso ao meio é a PCF. Esta função implementa um método centralizado de controle de transmissão das estações em que uma única estação, o coordenador pontual (PC, *point coordinator*), que também deve ser o ponto de acesso do BSS, decide que estações podem transmitir. Este método pode ser usado para colocar a rede em um modo de operação sem contenção por um certo período de tempo. O coordenador pontual também pode utilizar quadros com um espaço entre quadros menor do que o normal, para ganhar prioridade de transmissão sobre todas outras estações.

8.2 Outras funções

As outras funções de subcamadas da camada de enlace são: Fragmentação e Desfragmentação, seleção de taxa de transmissão, restrição de reordenação de pacotes e seqüências definidas de troca de pacotes entre estações.

9 Tecnologias Empregadas

As redes sem fio são geralmente classificadas de acordo com a técnica de transmissão empregada. Todas as atuais redes sem fio caem em uma das seguintes categorias:

- **LANs utilizando Infravermelho (IR)** - um célula de uma IR LAN é limitada a um único ambiente, pois a luz infravermelha não é capaz de atravessar paredes opacas.
- **LANs spread spectrum** - tais LANs utilizam a modulação spread spectrum para transmissão do sinal.
- **Microondas de faixa estreita** - essas LANs operam na frequências de microondas mas não utilizam a modulação spread spectrum.

9.1 Modulação Spread Spectrum

A maioria das redes sem fio utilizam a tecnologia spread spectrum. Esta modulação é uma modulação de banda larga desenvolvida para aplicações militares devido a sua confiabilidade e segurança. A modulação spread spectrum foi feita para trocar a eficiência em largura de banda por confiabilidade, integridade e segurança. Um sistema spread-spectrum espalha o sinal em uma faixa de frequências muito mais larga do que a largura mínima de banda necessária para transmitir a informação. Existem dois tipos de modulação spread spectrum: chaveamento em frequência e seqüência direta.

9.1.1 Modulação Spread Spectrum por chaveamento em frequência

A modulação spread spectrum por chaveamento em frequência (FHSS) é na verdade uma modulação FH-DPSK (Frequency-Hopped Difference Phase-Shift Keying). Esta modulação utiliza uma portadora de banda estreita que muda de frequência seguindo uma seqüência que é conhecida pelo transmissor e pelo receptor. Quando devidamente sincronizados (receptor e transmissor) é possível manter um canal lógico. Um receptor desavisado perceberia o sinal FHSS como um ruído impulsivo de curta duração.

Cada sinal FH-DPSK é um sinal senoidal, de envelope constante, onde em cada intervalo de tempo t_1 a fase é constante. O sinal é dividido então em um número inteiro de intervalos de duração t_1 chamados "chips". Para uma forma de onda de duração $T = Lt_1$, uma específica seqüência de L chips é associada de forma a não haver repetição de frequências em nenhum desses chips. Cada usuário possuirá uma código, que na verdade é a seqüência de L frequências que serão utilizadas nos L chips. Os códigos devem ser tais que em nenhum chip possa haver mais de um usuário utilizando uma dada frequência. O sinal é periódico com período T . A associação de frequências é feita da seguinte forma:

$$f_i^k = f_c + \alpha_i^k f_1$$

onde f_i^k é o deslocamento em frequência em relação a portadora f_c associado ao i -ésimo chip da k -ésima forma de onda. α_i^k é o inteiro do k -ésimo código e f_1 é a frequência fundamental do canal antes do chaveamento. Existem então L sinais distintos, cada um com L chips de tempo e com uma largura de banda de aproximadamente L/t_1 .

A eficiência espectral do sistema pode ser expressa por:

$$\eta = M \frac{R_b}{B}$$

onde M é o número de usuários simultaneamente servidos pelo sistema, B é a banda ocupada para transmissão em apenas uma direção e R_b é a taxa de transmissão de informação definida por:

$$R_b = \frac{\log_2 L}{T} = \frac{\log_2 L}{Lt_1}$$

Cada estação recebe o seu sinal (seqüência de L tons) e também $M - 1$ seqüências interferentes. Assumindo que todos os transmissores estão descorrelacionados e que $M \gg 1$, teremos que a interferência incidente é equivalente a um ruído Gaussiano na largura de banda B do sistema.

9.1.2 Modulação Spread Spectrum de seqüência direta

A modulação spread spectrum de seqüência direta (DSSS) gera um padrão redundante de bits para cada bit a ser transmitido. Cada padrão de bit é chamado de chip (ou código de chip). O quanto mais longo o chip, maior a probabilidade

do dado original poder ser recuperado (e, como consequência, maior a largura de banda necessária). Mesmo que um ou mais bits seja corrompidos durante a transmissão, técnicas estatísticas podem ser utilizadas para recuperar o dado original sem necessidade de retransmissão. Para um observador qualquer que for o alvo da transmissão, o sinal DSSS pareceria com um ruído de banda larga de baixa potência e seria ignorado pela maioria dos receptores de banda estreita.

Existem dois tipos de modulação spread spectrum de seqüência direta: espalhamento antes da modulação pela portadora e modulação após a modulação pela portadora.

No primeiro tipo, o dado $x(t)$ que é transmitido numa taxa R_b é modulado pela portadora f_0 e depois pelo código de espalhamento $G(t)$, formando o sinal DS (seqüência direta), $s_t(t)$, com uma taxa de chips R_c , ocupando uma largura de banda B_{ss} . O sinal $s_t(t - T)$, após um tempo de propagação T , é recebido e passa por um correlacionador que consiste em duas funções: multiplicação e média. O correlacionador utiliza o mesmo código de espalhamento $G(t)$ para "desespalhar" o sinal DS e assim recuperará o sinal original.

A segunda técnica de DS consiste em primeiro espalhar o sinal e depois modular. As duas técnicas DS fornecem o mesmo sinal $s_t(t)$.

Vejamos a análise da primeira técnica.

Seja $x(t)$ o sinal, um fluxo de dados, modulado por um BPSK (binary phase shift keying), de tal forma que:

$$s_t(t) = x(t)\cos(2\pi f_0 t)$$

onde $x(t) = \pm 1$ e a taxa de dados é R_b . No transmissor, a seqüência de espalhamento é $G(t)$ utiliza também um BPSK:

$$G(t) = \pm 1$$

com uma taxa de chip R_c . O sinal espalhado fica então:

$$s_t(t) = x(t)G(t)\cos(2\pi f_0 t)$$

No receptor, após um tempo de propagação T segundos, o sinal $s_t(t - T)$ é recebido. Inicia-se então o processo de "de-espalhamento". O sinal $s_0(t - T)$ que sai do correlacionador é:

$$s_0(t - T) = E\{x(t - T) \cdot G(t - T), G(t - \hat{T})\cos[2\pi f_0(t - T)]\}$$

$$s_0(t - T) = x(t - T) \cdot E\{G(t - T) \cdot G(t - \hat{T})\} \cdot \cos[2\pi f_0(t - T)]$$

onde \hat{T} é o atraso estimado no receptor. Como $G(t) = \pm 1$ e quando $T = \hat{T}$ temos:

$$E\{G(t - T) \cdot G(t - \hat{T})\} = 1$$

Então $s_0(t - T)$ se torna:

$$s_0(t - T) = x(t - T)\cos[2\pi f_0(t - \tau)]$$

O dado $x(t - T)$ pode ser recuperado após uma demodulação usando a freqüência f_0 .

9.2 Modulação de Banda Estreita

Um sistema de rádio de banda estreita transmite e recebe informações em uma frequência específica. Os rádios de banda estreita mantêm o espectro do sinal transmitido o mais estreito possível, o mínimo necessário para transmitir a informação. A interferência entre canais adjacentes é evitada alocando-se cuidadosamente cada usuário em um canal diferente em uma diferente faixa do espectro.

9.3 Diversidade Espacial

O sinal recebido por uma unidade sem-fio é um somatório das diversas ondas que chegam das mais variadas direções. Se o receptor tiver múltiplas antenas, espaçadas suficientemente para que os sinais recebidos sofram atenuações diferentes, podendo serem utilizados num esquema de diversidade na recepção. O espaçamento necessário para obter dois sinais descorrelacionados deve ser determinado. Para mais informações a respeito do coeficiente de correlação entre os sinais e o espaçamento entre as antenas, veja [2] capítulo 6.9.

10 Segurança no 802.11

A forma como o 802.11 tenta assegurar a confidencialidade das suas transmissões de dados é através de um algoritmo chamado WEP.

WEP - Wired Equivalence Privacy. Algoritmo especificado pelo 802.11 que implementa uma segurança equivalente a uma rede com fios.

A confiabilidade depende de um serviço externo de gerenciamento chaves de criptografia. É importante que além da implementação do WEP a rede use o processo de autenticação. (senão ele poderá ser aberto a ameaças).

A implementação do WEP tem as seguintes características:

- Relativamente Forte: imune a ataques de força bruta entre as chaves. Esta característica depende do tamanho e frequência de alteração das chaves.
- WEP é auto-sincronizável: a cada mensagem o sistema se sincroniza.
- Eficiência: pode ser implementado tanto em software quanto em hardware.
- Opcional: seu uso é opcional.

10.1 Teoria de operação do WEP:

A encriptação processa-se da seguinte forma:

1. Checksumming - Em primeiro lugar é necessário verificar a integridade da mensagem M. Para tal executa-se um algoritmo de checksum $c(M)$. Depois é feita uma concatenação entre o resultado do algoritmo e a própria mensagem $P = (M, c(M))$, obtendo-se um resultado (plaintext) que é passado para a fase seguinte.

Figura 5: Processo de encriptação

2. Encriptação - Esta fase encripta o texto vindo do passo anterior, utilizando o algoritmo RC4 (da RSA Data Security). Este algoritmo gera uma seqüência de bytes do mesmo tamanho que a mensagem a ser cifrada (plaintext). Para isto é utilizado a chave de encriptação (k) e um vetor de inicialização (IV) que são concatenados gerando uma semente (seed) esta semente alimenta um gerador de números pseudo-aleatórios (PRNG) que gera uma seqüência de mesmo tamanho que a mensagem. Finalmente é feito um XOR entre a seqüência obtida e a mensagem (plaintext), ficando-se com o resultado final (ciphertext). Então é transmitido o vetor de inicialização e a mensagem encriptada via radio para o destino.
3. Para descriptar a mensagem protegida pelo WEP, o receptor limita-se a reverter o processo. Primeiro gera uma seqüência de bytes com a chave que ele já tem e vetor de inicialização. Depois ele faz um XOR entre esta seqüência e o texto encriptado que foi recebido.

Figura 6: Processo de descriptação

10.2 Formato do Quadro Encriptado

IV vetor de inicialização e identificador da chave.

Figura 7: Tamanho do quadro de encriptado

PDU packet data unit.

ICV integrity check algorithm. (CRC-32bits).

Em relação à chave de encriptação, o 802.11 não especifica como esta deve ser distribuída. Apoia-se antes num mecanismo externo que povoa um array com quatro chaves partilhado por todos os intervenientes da rede. Cada mensagem contem um campo que especifica a posição do array na qual se encontra a chave a ser utilizada. O que se passa na pratica é que a maior parte das instalações usam apenas uma chave para toda a rede, o que obviamente tem um impacto negativo na segurança de todo o sistema.

Existem duas implementações diferentes do protocolo WEP, o standard e uma versão estendida, usada por alguns fabricantes. Estas versões estendidas usam chaves de encriptação mais longas do que as usadas na versão standard. A versão standard especifica chaves com 40 bits de comprimento. Esta opção foi tomada porque na altura da especificação do protocolo, o governo dos Estados Unidos da América impunha restrições à exportação de tecnologia que contivesse sistemas de criptografia.

11 Padrão IEEE 802.15 - Wireless Personal Area Networks

O padrão IEEE 802.15 visa oferecer conexões sem fio com baixa complexidade e baixo consumo de potência e pode ser dividido entre os sub-padrões a seguir:

- 802.15.1 - 1Mbps WPAN/Bluetooth v1.x;

- 802.15.2 - Recomendado para a coexistência de bandas não licenciadas;
- 802.15.3 - 20+Mbps High Rate WPAN para multimídia e imagens digitais;

Entre todos os padrões acima, o 802.15.1 recebeu mais atenção das empresas até o momento, por isso será o nosso objeto de estudo nesta seção. Quem deu início ao seu desenvolvimento foi a Ericsson por volta dos anos 90 e que hoje é a líder do grupo Bluetooth SIG (Special Industry Group), que envolve empresas como Nokia, IBM, Toshiba, Intel, 3Com, Motorola, Lucent e Microsoft.

11.1 Bluetooth

Bluetooth é o nome dado a um novo padrão de tecnologia que tem por objetivo a substituição de cabos em dispositivos eletrônicos utilizando conexões de rádio de pequena distância.

Esse protocolo sem fio já está embutido em diversos equipamentos como telefones celulares, notebooks, câmeras digitais, PDAs, calculadoras, microfones, leitoras óticas, entre outros.

O padrão 802.15.1, também chamado de Bluetooth, define uma estrutura para facilitar a comunicação entre diversos tipos de dispositivos baseando-se em três características fundamentais: baixa complexidade, baixo custo, baixo consumo de potência.

Essa tecnologia tem por objetivo construir uma aceitação global entre dispositivos de tal forma que qualquer um deles, no padrão, possa se comunicar com outro em qualquer lugar desde que estejam dentro da distância limite definida.

Dispositivos eletrônicos com o padrão Bluetooth podem se comunicar entre si através de conexões ponto-a-ponto ou multi-ponto compartilhando, neste último, o mesmo canal.

11.2 Requisitos do Padrão

Bluetooth não é reconhecido apenas como um padrão para substituição de redes com cabos. Várias novas idéias surgiram a partir de sua definição que abriram novas áreas e novas necessidades ao padrão que deve, além das características já citadas:

- Prover conexões baseadas no paradigma da conectividade inconsciente, em que dispositivos próximos conectam-se praticamente sem nenhum comando ou interação;
- Incorporar a capacidade de transmissões multimídia;
- Oferecer o mesmo nível de segurança existente atualmente para a comunicação cabeada.

Como as implementações dos dispositivos envolvem uma ampla variedade de equipamentos e empresas, o padrão foi feito gratuito para utilização. O objetivo dessa decisão foi evitar que empresas monopolizassem sua utilização e inibissem o seu desenvolvimento.

11.3 Arquitetura e Operação

O sistema Bluetooth é constituído, basicamente, por uma unidade de rádio, uma de controle de conexões (link control) e aplicativos em camadas superiores.

A unidade de rádio opera na frequência de 2,4 GHz ISM (Industry, Science and Medicine). Na transmissão, é utilizada uma técnica chamada frequency hopping para diminuir as interferências e aumentar a segurança. Também é utilizada a TDD (Time Division Duplex) para transmissões full-duplex e a modulação usada é a GFSK.

12 Padrão IEEE 802.16 - Wireless Metropolitan Area Networks

Este padrão foi concluído em outubro de 2001 e publicado em 8 de abril de 2002. Ele define a especificação para redes sem fio em áreas metropolitanas (WirelessMAN). Fornece acesso, por exemplo, à rede através de antenas exteriores comunicando com estações rádio base (BS's). A WirelessMAN é uma alternativa para as redes a cabo, como conexões de fibra ótica, sistemas coaxiais usando modems a cabo e DSL's (Digital Subscriber Line). Com a tecnologia WirelessMAN trazendo a rede para dentro, os usuários se comunicarão internamente através de Ethernet ou WLAN's (IEEE Standard 802.11). Entretanto o projeto fundamental do padrão permite uma extensão eficiente dos protocolos da rede WirelessMAN diretamente para cada usuário, com total qualidade de serviço. Com a tecnologia sendo desenvolvida nesta direção é possível que o padrão dê suporte para usuários móveis. O padrão IEEE 802.16 foi projetado para desenvolver um conjunto de interfaces aéreas baseada em camadas de enlace comuns mas com especificações de camadas físicas dependentes do espectro de uso e regulamentos associados. O padrão aprovado em 2001 refere-se a frequências de 10 a 66 GHz, onde o espectro abrangido é atualmente disponível em todo mundo mas no qual os curtos comprimentos de onda apresentam importante desafio de implementação. Um segundo projeto (802.16a), estende o suporte à interface aérea para baixas frequências na faixa de 2-11 GHz incluindo espectro licenciado e não licenciado. Comparando com o de altas frequências esse espectro oferece a oportunidade de alcançar muito mais consumidores com um custo menor, embora geralmente a taxa de transmissão de dados também menores. Isto indica que tais serviços são orientados a usuários residenciais ou empresas de médio porte.

12.1 Arquitetura e Operação

12.1.1 Camada Física (PHY)

A camada física do padrão especifica a faixa de frequências, o esquema de modulação, técnicas de correção de erro, sincronização entre transmissor e receptor, taxas de transmissão e a estrutura do time-division multiplexing (TDM).

Para a transmissão das estações assinantes (Subscriber Stations - SSS) para uma estação base (Base Station - BS), o padrão utiliza a técnica Demand Assignment Multiple Access - Time Division Multiple Access (DAMA - TDMA). DAMA é uma técnica que permite a adaptação às várias mudanças na demanda de várias estações. TDMA é a técnica de dividir o tempo em um canal dentro de uma sucessão de frames, sendo que cada frame consiste em vários slots, e alocar um ou mais slots por frame para formar um canal lógico.

12.1.2 Estrutura de MAC

Sobre a camada física estão as funções associadas com prover serviços aos SSS. Estas funções incluem transmissões de dados em frames e controle de acesso ao meio wireless compartilhado, e se agrupam em uma camada de MAC, cuja estrutura foi projetada para aplicações de banda larga sem fio ponto-multiponto. O acesso e a distribuição dos algoritmos da largura de banda devem permitir centenas de terminais por canal, com terminais que podem ser divididos por múltiplos usuários finais. Conseqüentemente, há necessidade de altas taxa de transmissão, tanto para upload quanto para download. O protocolo de MAC define quando e como uma BS ou SS podem iniciar uma transmissão no canal. Como algumas das camadas sobre a camada de MAC requerem qualidade de serviço (QoS), o protocolo de MAC deve poder alocar capacidade de canal de rádio e aceitar tanto bursty tráfico quanto tráfico contínuo de dados, para satisfazer demandas de serviço.

13 Outras Tecnologias de LANs Sem-Fio

- **HomeRF**: Padrão de redes sem fio que utiliza a faixa dos 2,4 GHz. Utiliza o protocolo Shared Wireless Access, onde as interfaces de rede se comunicam diretamente, sem o uso de um ponto de acesso. Isto diminui o custo da rede mas, por outro lado, compromete o alcance do sinal, que é de apenas 50 m, em condições ideais. A taxa de transmissão é de 1,6 Mbps;
- **HIPERLAN**: Padrão europeu de futuro incerto. Não se sabe se ele será abandonado em nome do IEEE802.11, ou se algumas das vantagens que ele oferece o tornarão o próximo padrão a dominar o mercado.
- **Satélites**: É empregada onde as distâncias são muito grandes. Possui a vantagem de o sinal chegar em qualquer região da superfície terrestre. Dentre as desvantagens relacionadas pode-se citar a demora, o alto custo de instalação e o elevado atraso por enlace, que é de aproximadamente 120 ms (ida e volta) podendo chegar a 1 s, o que inviabiliza algumas aplicações.

14 Conclusões

O crescimento das redes de computadores tem sido uma realidade e vem acontecendo de forma muito rápida. As formas de acesso a dados também têm mudado

radicalmente, na medida em que transações que antes eram feitas de forma fixa e centralizada, hoje podem ser feitas de formas móveis e distribuídas. A cultura de utilização da informação também vem recebendo novas filosofias da era digital.

Uma forte tendência é que os dispositivos computacionais e domésticos usados em residências, empresas, etc. sejam sem fio no contexto das redes locais, substituindo gradativamente as redes tradicionais cabeadas.

Embora ainda haja muitas questões sendo analisadas a respeito das redes sem fio (WLANs), a comunidade científica tem investido de forma significativa no melhoramento dos padrões, objetivando maior alcance, taxas de transmissão mais elevadas, maior segurança e confiabilidade.

A definição de padrões como o Bluetooth (IEEE 802.15) para comunicação entre dispositivos como celulares, teclados, PDAs e, brevemente, geladeiras, televisores e dispositivos de automação residencial, através das WPANs, é essencial para o futuro das comunicações sem fio.

O padrão IEEE 802.16 provê uma plataforma para o desenvolvimento de redes metropolitanas (WirelessMANs), provendo acesso wireless de banda larga. O MAC IEEE 802.16 é poderoso e flexível o bastante para suportar qualquer tecnologia de acesso, fornecendo uma grande oportunidade para os fabricantes de equipamentos, que podem diferenciar seus produtos sem comprometer a interoperabilidade.

Referências

- [1] Stallins, W. – Data & Computer Communications
- [2] Lee, W.C.Y. – Mobile Communication Engineering
- [3] Padrão IEEE 802.11
- [4] Tanenbaum, Andrew S. – Computer Networks, 4th ed.
- [5] Homepage da Wi-Fi Alliance – <http://www.wi-fi.org>
- [6] RSA Security – <http://www.rsasecurity.com>