Protocolos de Roteamento em Redes Ad Hoc

Bruno Vieira Fernandes

Trabalho Final de Mestrado Profissional

Instituto de Computação
Universidade Estadual de Campinas

Protocolos de Roteamento em Redes Ad Hoc

Bruno Vieira Fernandes

Dezembro de 2003

Banca Examinadora:

- Prof. Dr. Nelson Luis Saldanha da Fonseca (Orientador)
- Prof. Dr. Célio Cardoso Guimarães
  Instituto de Computação - UNICAMP
- Prof. Dr. Omar Carvalho Branquinho
  Faculdade de Engenharia Elétrica – Universidade São Francisco
- Prof. Dr. Edmundo Roberto Mauro Madeira (Suplente)
  Instituto de Computação - UNICAMP

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP

Fernandes, Bruno Vieira

V673p Protocolos de roteamento em redes AD HOC / Bruno Vieira Fernandes - - Campinas, [S.P. :s.n.], 2003.

Orientador : Nelson Luis Saldanha da Fonseca.

Co-Orientador: Otto Carlos Muniz Bandeira Duarte.

Trabalho final (mestrado profissional) - Universidade Estadual de Campinas, Instituto de Computação.

1.Redes de computação - Protocolos. 2. Sistemas de comunicação sem fio. 3. Sistemas de transmissão de dados. I. Fonseca, Nelson Luis Saldanha da. II. Duarte, Otto Carlos Muniz Bandeira. III. Universidade Estadual de Campinas. Instituto de Computação. IV. Título.

Protocolos de Roteamento em Redes Ad Hoc

Este exemplar corresponde à redação final do Trabalho Final devidamente corrigida e defendida por Bruno Vieira Fernandes e aprovada pela Banca Examinadora.

Campinas, 19 de dezembro de 2003.

Prof. Dr. Nelson Luis Saldanha da Fonseca

(Orientador)

Prof. Dr. Otto Carlos Muniz Bandeira Duarte

(Co-orientador)

Trabalho Final apresentado ao Instituto de Computação, UNICAMP, como requisito parcial para a obtenção do título de Mestre em Computação na área de Engenharia de Computação.

Protocolos de Roteamento em Redes Ad Hoc

Este exemplar corresponde à redação final do Trabalho Final devidamente corrigida e defendida por Bruno Vieira Fernandes e aprovada pela Banca Examinadora.

Campinas, 19 de dezembro de 2003.

Prof. Dr. Nelson Luis Saldanha da Fonseca

(Orientador)

Prof. Dr. Otto Carlos Muniz Bandeira Duarte

(Co-orientador)

Trabalho Final apresentado ao Instituto de Computação, UNICAMP, como requisito parcial para a obtenção do título de Mestre em Computação na área de Engenharia de Computação.

TERMO DE APROVAÇÃO

Tese defendida e aprovada em 19 de dezembro de 2003, pela Banca Examinadora composta pelos Professores Doutores:

Profº. Drº. Omar Carvalho Branquinho
PUC-CAMPINAS

Profº. Drº. Célio Cardoso Guimarães
IC - UNICAMP

Profº. Drº. Nelson Luis Saldanha da Fonseca
IC - UNICAMP

Resumo

As redes móveis sem infraestrutura, conhecidas como redes *ad hoc*, vêm crescendo notoriamente, devido principalmente a simplicidade de implementação, o baixo custo e a diversidade de aplicações que tais redes proporcionam em áreas como a militar, corporativa ou residencial.

Entretanto, vários são os fatores que influenciam no desenvolvimento e no desempenho das aplicações para redes *ad hoc*. Um dos fatores consiste no roteamento dos pacotes na rede. Com isto, protocolos de roteamento para redes *ad hoc* vêm sendo estudados, visando adaptar-se a restrições da rede como o consumo de energia dos dispositivos móveis e a largura de banda, além de reduzir o número de mensagens, a quantidade de processamento realizado e de dados transmitidos, mesmo quando houver mudanças de topologia na rede.

Neste trabalho, descreve-se os protocolos de roteamento para redes ad hoc conhecidos como DSDV (*Destination Sequenced Distance Vector*), WRP (*Wireless Routing Protocol*), CSGR (*Clusterhead Switch Gateway Routing*), AODV (*Ad Hoc On-Demand Distance Vetor*) e DSR (*Dynamic Source Routing*), comparando suas principais características.

Abstract

The use of ad hoc networks has increased in the past few years due to its low cost. Such networks allows a variety of services in the military, in the corporate as well as in the residential areas. However, the wide spread of ad hoc networks faces several challenges yet to be overcome. One of the factors is the design of efficient routing algorithms. This work describes protocols for ad hoc networks, such as DSDV (*Destination Sequenced Distance Vector*), WRP (*Wireless Routing Protocol*), CSGR (*Clusterhead Switch Gateway Routing*), AODV (*Ad Hoc On-Demand Distance Vector*) and DSR (*Dynamic Source Routing*) and compares their main characteristics.

Dedicatória

Dedico este trabalho a minha família, em especial a Sabrina, minha filha.

Agradecimentos

Agradeço a Deus, inicialmente.

Aos meus pais, Luiz e Sonia, pelo apoio que sempre me deram, em todos os momentos de minha vida.

À minha filha, Sabrina.

Às minhas irmãs, Regina e Raquel.

Aos meus avôs e avós: Augusto, Felizarda, Nacib, Nazir e Manoel.

Aos Professores Nelson Luiz Saldanha da Fonseca e Otto Carlos Muniz Bandeira Duarte, pela dedicação na orientação deste trabalho.

Aos colegas do Instituto de Computação.

Conteúdo

Índice de Figuras

Índice de Tabelas

Capítulo 1

Introdução

O crescimento da comunicação sem fio tem aumentado notavelmente nos últimos anos, principalmente devido a facilidade de instalação quando comparado com as redes com fio e a mobilidade, permitindo maior flexibilidade e praticidade. As aplicações para as redes sem fio abrangem desde comunicações a curtas distâncias e pouca mobilidade, como encontros em salas de reunião, a comunicações com maiores distâncias e grande mobilidade, como em operações de resgate ou militares. Muitas destas aplicações seriam inconvenientes ou mesmo inviáveis de serem efetuadas em redes com fio. Genericamente, existem dois tipos de abordagem para permitir que unidades sem fio móveis se comuniquem:

a) Infraestruturada: baseadas no conceito de um sistema celular, nos quais os dispositivos móveis se comunicam com pontos de acesso, como estações base, conectados a uma rede fixa infraestruturada. Exemplos típicos deste tipo de rede incluem o *GSM (Global System for Mobile Communication)*, UMTS (*Universal Mobile Telecomunications System*) e o WLAN (*Wireless Local Area Network*); e
b) Sem infraestrutura: são conhecidas como redes móveis ad hoc ou MANET (*Mobile Ad Hoc Network*), e consiste em uma coleção de dispositivos móveis sem fio (nós) que podem dinamicamente formar uma rede para a troca de informações, sem a necessidade do uso de uma rede fixa infraestruturada. As redes ad hoc dividem-se em: comunicação direta, nos quais os nós da rede só se comunicam com aqueles que se encontram em seu raio de cobertura e de múltiplos saltos, cujas estações funcionam como roteadores, permitindo a comunicação entre nós da rede cuja distância ultrapassa o raio de cobertura.

As redes móveis ad hoc e WLAN vêm crescendo notoriamente, devido principalmente a simplicidade de implementação, o baixo custo e a diversidade de aplicações que tais redes proporcionam. Conforme [1], o total de equipamentos de redes sem fio entregues no mercado atingiu a marca de 19,5 milhões em 2002, representando um aumento de 120% em relação a 2001. Especialmente nas redes WLANs, o padrão IEEE 802.11 se destaca notavelmente pois, além das características listadas acima, somam-se ainda a aplicação do padrão em vários cenários como salas de aula, videoconferências e escritórios, com possibilidade de operar das duas formas, infraestruturada e não infraestruturada ou ad hoc. Além disto, diferentes tipos de aplicações podem ser desenvolvidas utilizando-se as redes ad hoc. Algumas das mais importantes são:

- Aplicações no trabalho: possibilita que um usuário seja detectado pela rede ao se aproximar com seu dispositivo móvel, permitindo a sincronização do seu equipamento com a rede e possibilitando, por exemplo, a transferência de arquivos, leitura de e-mail ou mesmo a agenda do dia.
- Aplicações residenciais: vários equipamentos em uma residência podem fazer parte de uma rede ad hoc, como equipamentos de áudio de vídeo, geladeiras, sistemas de alarme, etc. Os dispositivos ad hoc para cada usuário poderão ter diferentes níveis de acesso e se comunicar com os dispositivos ad hoc de uma residência para destrancar portas, acender lâmpadas, ligar unidades de áudio e vídeo, bem como desativar alarmes de segurança [2].
- Aplicações em automóveis: um motorista com o seu carro em um outro Estado pode receber mensagens de e-mail através de um sistema sem fio instalado em seu automóvel. Com estações base distribuídas ao longo da rodovia e com conexão à Internet o usuário pode acessá-las a qualquer momento para obter informações de restaurantes, postos de gasolina ou centros de compra que se encontram ao longo da rodovia. Além disto, um carro com um dispositivo móvel pode se comunicar com outro carro dentro de sua área de cobertura, e assim por diante, formando uma rede ad hoc.
- Aplicações em campos de batalha: os dispositivos sem fio podem ser instalados em veículos, tanques, caminhões ou mesmo portado por soldados, o que cria uma rede

móvel ad hoc. Através da comunicação por múltiplos saltos, os soldados podem se comunicar remotamente através do roteamento de pacotes, de um rádio para outro [2].

Outro cenário em um campo de batalha é o gerenciamento de sensores sem fio. Os sensores cabeados podem ser facilmente detectados, possuem pouca praticidade e escalabilidade. Os sensores sem fio podem ser instalados com maior facilidade, visando obter informações sobre o local de batalha com rapidez, o que agiliza e facilita a tomada de decisões para o ataque pelo centro de comando da tropa.

• Aplicações móveis colaborativas: o trabalho colaborativo suportado pelo computador (*Computer-Supported Collaborative Work – CSCW*) tem sido aplicado em redes cabeadas com estações equipadas com dispositivos multimídia suportando áudio e vídeo. É uma aplicação importante para aumentar a produtividade e o fluxo de trabalho. Os usuários móveis podem detectar a presença de seus colegas de trabalho e estabelecer uma rede ad hoc com *multicast*, permitindo múltiplos grupos de discussão ou o desenvolvimento de trabalho cooperativo. Devido a heterogeneidade dos tipo de dispositivos móveis que os usuários podem utilizar, as aplicações móveis CSCW devem ser capazes de se adaptar e prover interface gráfica apropriada aos usuários [2].

No desenvolvimento das aplicações para redes ad hoc, devem ser consideradas diversas características e limitações da rede como a mobilidade dos nós, altas taxas de erro, reduzida banda passante e de fornecimento de energia dos dispositivos móveis. Com isto, vários são os fatores que influenciam no desenvolvimento e no desempenho das aplicações para redes ad hoc, e alguns deles são listados a seguir:

• Acesso ao meio: como o mesmo meio é compartilhado por múltiplos nós, o acesso ao canal deve ser realizado de forma adequada, através da presença de um protocolo da camada MAC, que deve buscar o acesso ao canal e ao mesmo tempo evitar possíveis colisões com os nós vizinhos. A presença de terminais escondidos e de mobilidade deve ser considerada quando estiver sendo desenvolvido um protocolo MAC para redes móveis ad hoc [2].

• Roteamento: a presença de mobilidade em uma rede implica que conexões são formadas e desfeitas de forma não deterministica. Nas redes móveis, os nós podem se

mover mais livremente, resultando em uma mudança dinâmica da topologia. Os protocolos de roteamento baseados em vetor de distância e baseados no estado do enlace são incapazes de lidar com as mudanças freqüentes de conexões nas redes móveis ad hoc, resultando em uma convergência deficiente de rotas e baixa vazão (*throughput*).

• *Multicast*: esta técnica endereça pacotes para um grupo de nós. Com isto, as aplicações enviam somente uma cópia de cada pacote, endereçado a um grupo, ao invés de endereçar e enviar um mesmo pacote para cada nó (*unicast*), economizando largura de banda e aumentando a eficiência da rede [3]. Portanto, o roteamento *multicast* em redes ad hoc deve ser considerado como uma ferramenta básica em aplicações como conferência [32], em distribuição compartilhada de uma base de dados, processamento paralelo ou grupos de bate-papo.

• Energia: muitos protocolos de rede existentes não consideram o consumo de energia como um problema, já que é assumida a presença de dispositivos estáticos. Entretanto, a maioria dos dispositivos móveis opera com baterias, e o tempo de uso de uma bateria Li-ion é baixa (duas a três horas). Tal limitação nas horas de operação de um dispositivo implica na necessidade de conservação de energia que é, portanto, necessária para redes móveis ad hoc [2].

• Desempenho do protocolo TCP (Transmission Control Protocol): o TCP é um protocolo orientado a conexão e para transmissão fim a fim, que implementa controle de fluxo e de congestionamento em uma rede. Logo, existe uma fase de estabelecimento da conexão anterior a transmissão dos dados. A conexão é removida quando a transmissão de dados estiver completa.

Para concluir se ocorreu congestionamento na rede, o TCP mede o tempo que um pacote leva para ir e retornar de um computador a outro, chamado de RTT (*Round-Trip-Time*) e a perda de pacote. Porém, o TCP não é capaz de distinguir a presença de mobilidade e de congestionamento na rede. Mobilidade pelos nós em uma conexão pode resultar em perda de pacote e um RTT longo. Portanto, algumas mudanças são necessárias para assegurar que o protocolo de transporte apresente um desempenho apropriado sem afetar a vazão (*throughput*) de comunicação fim a fim [2].

• Segurança e privacidade: nas redes ad hoc, ao contrário das redes infraestruturadas, a ausência de dispositivos que centralizem e coordenem a comunicação

aumenta a complexidade na implementação de dispositivos de segurança. Os mecanismos utilizados em redes infraestruturadas não são convenientes para utilização em redes ad hoc, devido às hipóteses geralmente adotadas como a disponibilidade de servidores de autenticação. Nas redes ad hoc, normalmente são os próprios nós da rede que estabelecem uma relação de segurança entre si.

Como a comunicação utilizando-se uma rede ad hoc apresenta determinadas limitações como altas taxas de erros, fornecimento restrito de energia dos dispositivos móveis e pequena largura de banda, é necessário a utilização de protocolos de roteamento eficazes que reduzam o número de mensagens, a quantidade de processamento realizado, de dados transmitidos e que sejam capazes de restaurar a comunicação entre o nó de origem e o nó fonte, através de outros nós (nós intermediários), mesmo quando houver mudanças de topologia na rede. Esses problemas estão sendo pesquisados e diversos protocolos de roteamento e formas de busca e manutenção de rotas tem sido propostos e aprimorados nos últimos anos.

O objetivo do presente trabalho é o de apresentar alguns dos principais protocolos de roteamento para redes ad hoc, bem como comparar as principais características de cada um deles. Além disto, será apresentado o padrão IEEE 802.11, bem como as principais aplicações para as redes móveis ad hoc.

O restante deste trabalho está organizado da seguinte forma: o capítulo 2 descreve os padrões IEEE 802.11a, IEEE 802.11b e IEEE 802.11g, ressaltando os conceitos, suas camadas física e de controle, e a comparação entre as principais características destes padrões. O capítulo 3 descreve alguns dos protocolos de roteamento mais utilizados pela comunidade científica e apresenta a comparação entre eles para cada uma de suas características. O capítulo 4 apresenta as conclusões sobre o trabalho assim como sugestões para pesquisas.

Capítulo 2

O Padrão IEEE 802.11

Dentre as redes sem fio, a aplicação das WLAN (*Wireless Local Area Network*) cresceu muito nos últimos anos. Por isso, o IEEE *(Institute of Electrical and Electronic Engineers*) constituiu alguns grupos de padronização cujo objetivo, dentre outros, é o de definir um nível físico para redes locais sem fio, onde as transmissões são realizadas nas freqüências de rádio ou infravermelho, e um protocolo de controle de acesso ao meio da camada MAC (*Medium Access Control*). O projeto, conhecido como IEEE 802.11, ganhou notoriedade pela facilidade de instalação, baixo custo, bem como pela diversidade de aplicações. Conforme será visto a seguir, alguns suplementos à especificação básica foram elaborados, como o 802.11b, 802.11a e 802.11g, que adicionam maiores capacidades ao nível físico, permitindo taxas de transmissão mais altas.

Existem dois tipos de rede definidos no padrão IEEE 802.11 [4]: Ad Hoc e Infraestrutura. Nas redes ad hoc com IEEE 802.11, ou também chamadas de *IBSS (Independent Basic Service Set*), não existe um ponto central e nenhuma infraestrutura de rede. Cada nó móvel pode se comunicar com qualquer outro nó móvel da rede, sem passar por um ponto de acesso centralizado. Nas redes com infraestrutura, existem pontos de acesso centrais com os quais os nós móveis se comunicam.

Uma WLAN 802.11 é baseada na arquitetura de células, similar a um sistema celular [5], onde cada célula é chamada de BSA (*Basic Service Area*). Um conjunto de terminais comunicando-se dentro de uma BSA é chamado de BSS (*Basic Service Set*). Para permitir a construção de redes cobrindo áreas maiores do que uma célula, múltiplas BSA's são interligadas através de um sistema de distribuição via pontos de acesso (*AP – Access Point*). Os AP's são estações responsáveis pela captura das transmissões realizadas pelas estações de sua BSA, destinadas a estações localizadas em outras BSA's, retransmitindo-as, usando o sistema de distribuição. Os BSA's interligados por um sistema de distribuição através de AP's definem uma ESA (*Extended Service Area*).

O conjunto de estações formado pela união dos vários BSS's e conectados por um sistema de distribuição define um ESS (*Extended Service Set*), que constitui uma rede sem fio com infraestrutura, conforme ilustrado na Figura 2.1.

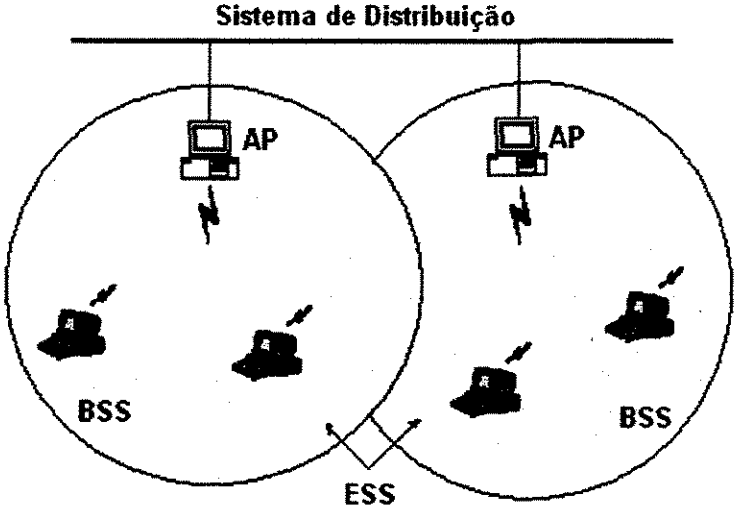

Figura 2.1 - Rede sem fio com infraestrutura.

2.1. A Camada Física do Padrão IEEE 802.11

Na camada física do padrão IEEE 802.11, original de 1997 [4], são definidas as seguintes tecnologias de transmissão: espalhamento de espectro por seqüência direta *(Direct Sequence Spread Spectrum - DSSS)*, espalhamento de espectro por salto em freqüência (*Frequency-Hopping Spread Spectrum – FHSS)* ou infravermelho. Os outros suplementos acrescentam novas taxas, utilizando o DSSS e OFDM, que serão descritos a seguir.

2.1.1. Espalhamento de Espectro por Seqüência Direta (DSSS)

O DSSS (*Direct Sequence Spread Spectrum*) é um método de espalhamento de espectro que no padrão IEEE 802.11 utiliza a banda ISM (*Industrial, Scientific and Medical*) de 2,4 GHz [4]. Nesta técnica, para taxas de transmissão de 1 e 2 Mbps, cada bit transmitido é modulado com uma seqüência de 11 bits, chamada de código barker (+1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1). Este processo espalha a potência do sinal de RF sobre

uma larga banda de freqüência. Além disto, a inserção dos dados redundantes (código barker) no sinal original possibilita sua recuperação em caso de distorção, tornando-o menos susceptível a interferências [6]. A Figura 2.2 ilustra o método DSSS aplicado a um sinal.

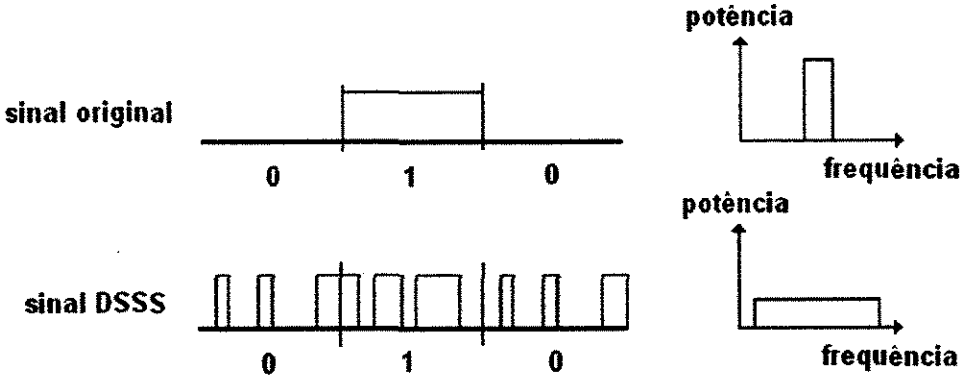

Figura 2.2 - Forma do sinal aplicando-se o processo DSSS.

No padrão IEEE 802.11, para transmissões a 1 Mbps é utilizada a modulação binária por chaveamento de *fase (Binary Phase Shift Keying - BPSK)*. Para transmissões de 2 Mbps, é utilizada a modulação quaternária por chaveamento de *fase (Quadrature Phase Shift Keying - QPSK)*, que permite a codificação de 2 bits de informação ocupando o mesmo espectro do BPSK, dobrando a taxa de transmissão.

2.1.2. Espalhamento de Espectro por Salto de Freqüência (FHSS)

O FHSS (*Frequency-Hopping Spread Spectrum*) [4] é uma técnica de espalhamento que divide a banda passante total em vários canais de pequena banda e faz com que o transmissor e o receptor permaneçam em um desses canais por um determinado período e depois saltem para outro canal. Permite-se com isto que várias redes coexistam em uma mesma área. O custo dos rádios é baixo e utiliza-se baixa potência para transmissão. Nos EUA e em quase toda a Europa, a camada física do padrão IEEE 802.11 usa 79 canais, espaçados de 1 MHz. Para o acesso básico de 1 Mbps, é utilizada a modulação gaussiana por chaveamento de freqüência (*Gaussian Frequence Shift Keying – GFSK*) de dois níveis. Neste acesso, o dado passa por um filtro gaussiano em banda base e é modulado em

freqüência, onde o 1 lógico é codificado usando uma freqüência $F_c + f$ e o 0 lógico usa uma freqüência $F_c - f$. Para a taxa de acesso opcional de 2 Mbps, utiliza-se um GFSK de quatro níveis, onde dois bits são codificados por vez usando quatro freqüências.

2.1.3. Infravermelho

O infravermelho foi projetado para áreas internas, recebendo dados por transmissões predominantemente em linha de visada ou refletidas e com comprimentos de onda de 850 a 950 nm. Operam com transmissões cujo alcance varia de 10 a 20 m, dependendo da sensibilidade do receptor.

2.2. Multiplexação por Divisão Ortogonal de Freqüência (OFDM)

A multiplexação por divisão ortogonal de freqüência (*OFDM – Orthogonal Frequency Division Multiplexing*) [7,8] é uma técnica de transmissão por múltiplas portadoras, reconhecido como um excelente método para comunicação bidirecional de dados sem fio e em alta velocidade.

A modulação OFDM processa um sinal em múltiplos pequenos conjuntos de sinais e modula cada um em diferentes subportadoras, transmitindo-os simultaneamente e em freqüências diferentes. A tecnologia alcança alta largura de banda, utilizando-se uma quantidade em paralelo de subportadoras espaçadas ortogonalmente e próximas, sem haver sobreposição de sinais e com o mínimo de interferência.

Com altas taxas de transmissão, é importante que haja um mecanismo contra a perda de dados [7]. Este mecanismo, chamado de FEC (*Forward Error Correction*), consiste no envio de uma segunda cópia ao longo da informação primária. Se parte da informação primária for perdida, é possível que o receptor recupere a informação, eliminando a necessidade de se retransmitir todo o sinal.

Cada portadora é modulada e são adicionadas antes da transmissão. No receptor, as portadoras moduladas devem ser separadas antes da demodulação. O método tradicional de separação de bandas é a utilização de filtros que utilizam a multiplexação por divisão de freqüência (*FDM – Frequency Division Multiplexing*) [9].

A Figura 2.3 mostra o espectro de um sinal OFDM com três subportadoras. O lóbulo principal de cada uma recai sobre os valores de potência nulo das demais. Portanto diz-se que as subportadoras são ortogonais. Mesmo quando as subportadoras estão muito próximas, elas não interferem umas com as outras.

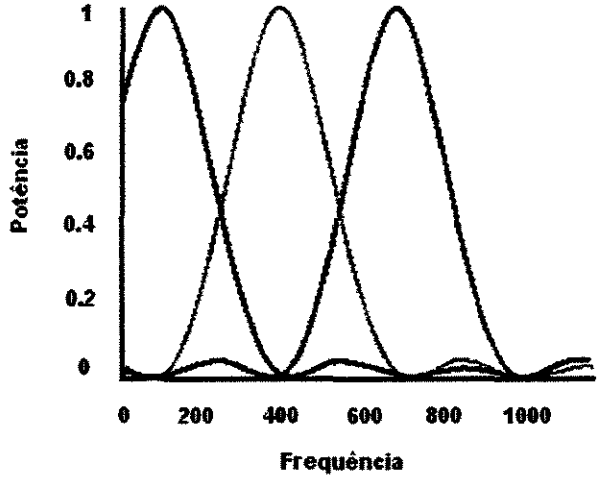

Figura 2.3 - Espectro de um sinal OFDM com três subportadoras.

A ortogonalidade dos subcanais OFDM permite que eles estejam sobrepostos, aumentando assim a eficiência do espectro, ou seja, enquanto forem ortogonais, não haverá interferência entre canais no sistema OFDM.

Uma das vantagens do OFDM é a capacidade de minimizar os efeitos de atraso por vários caminhos [10]. Quando um sinal deixa a antena transmissora, ele sofre um espalhamento temporal. Se o sinal refletir em alguma superfície, ele pode degradar ou cancelar o sinal original. Ainda, se o atraso for muito longo, o sinal com atraso pode espalhar-se nas transmissões seguintes. Porém, como a taxa de dados em cada subportadora é muito baixa, o período de um símbolo é muito longo, minimizando-se assim a interferência de uma transmissão nas seguintes.

Além disto, em cada pulso OFDM, existe um tempo de guarda (*guard interval*) que contém informações redundantes, podendo ser descartado no receptor sem afetar a correta decodificação do símbolo [16]. Este período é selecionado de forma a ser maior do que os atrasos encontrados, evitando-se assim interferências por múltiplos caminhos no sinal original.

Um problema encontrado no sistema OFDM diz respeito a distorção de fase, ruído e sensibilidade quando ocorre instabilidade de freqüência, causado quando o oscilador controlado por tensão (*VCO – Voltage-Controlled Oscilator*) do receptor não está exatamente na mesma freqüência do VCO do transmissor.

2.3. A Camada MAC do Padrão IEEE 802.11

A camada MAC é um conjunto de protocolos responsáveis em manter a ordem no uso do meio compartilhado. Ela é a mesma para os padrões IEEE 802.11a, IEEE 802.11b e IEEE 802.11g. Fornece dois tipos de serviços: assíncrono, que está sempre disponível e o síncrono, que é opcional. O assíncrono é fornecido por uma Função de Coordenação Distribuída (DCF), que implementa o protocolo CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*). O serviço síncrono, opcional, é fornecido pela Função de Coordenação Pontual (PCF), e basicamente implementa um método de acesso denominado *pooling*, que atua como coordenador, consultando de tempos em tempos os terminais e oferecendo a oportunidade de transmissão.

2.3.1. Função de Coordenação Distribuída (DCF)

O DCF é dividido em dois tipos [4]: o DCF básico, baseado em CSMA/CA e o outro que envolve o esquema RTS/*CTS (Request-To-Send/Clear-To-Send*). O método de acesso CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*), embora muito utilizado nas redes IEEE 802.3, não é adequado para as redes 802.11 pois a detecção de colisões é muito difícil, já que todas as estações ouvem as outras e seriam necessários rádios *full-duplex*, de custo elevado, usando a técnica FDD e não TDD.

De acordo com o DCF básico, a estação para transmitir deve verificar se o meio está livre e encontra-se neste estado por um tempo maior do que um espaço distribuído entre quadros (*Distributed InterFrame Space – DIFS*). Se o canal não estiver livre, a transmissão é adiada e a estação calcula um intervalo de tempo aleatório, chamado de *backoff*, uniformemente distribuído entre zero e um máximo (Janela de Disputa - CW). O intervalo de *backoff* determinará o tempo que a estação irá esperar até que tenha permissão para

transmitir seu pacote, que será decrementado em um valor chamado de slot toda vez que o meio estiver livre por mais de DIFS segundos. Após o intervalo de *backoff*, a estação envia o seu pacote.

Após a utilização do método de verificação cíclica (CRC) para a detecção de erros e caso o pacote esteja correto, utiliza-se um reconhecimento positivo, informando à estação de origem que o quadro transmitido foi recebido com sucesso. A transmissão de um reconhecimento (ACK) pela estação receptora é iniciada depois de um intervalo de tempo pequeno entre quadros, chamado de SIFS (*Short InterFrame Space*) que é, por definição, menor do que o DIFS. Depois da transmissão de um quadro, com ou sem sucesso, se a estação ainda quiser enviar informações, ela deverá executar um novo processo de *backoff*, evitando-se assim que uma estação capture o meio. Se o reconhecimento não for recebido pela origem após um determinado tempo, assume-se que o quadro transmitido foi perdido, e inicia-se um novo processo de *backoff*.

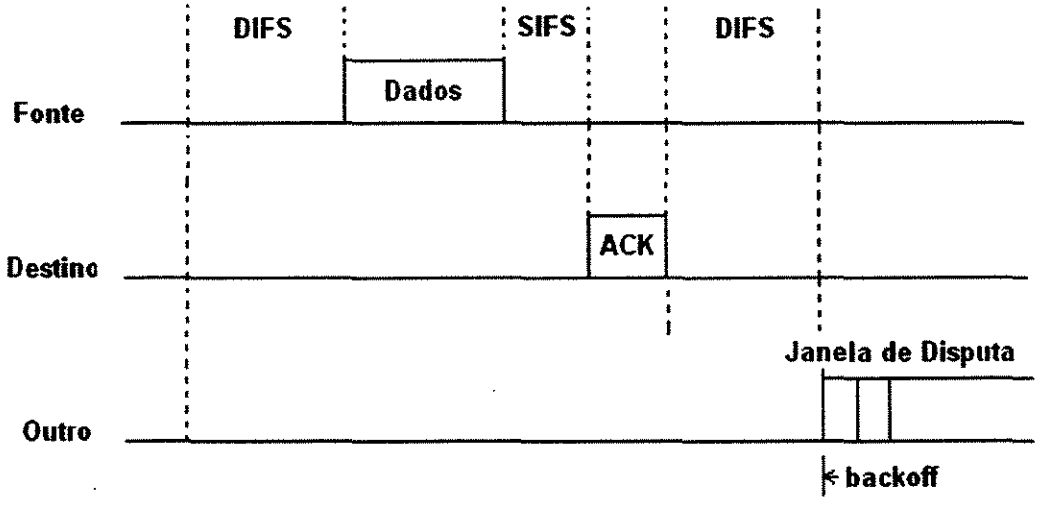

Figura 2.4. Esquema básico de acesso no DCF.

Em sistemas de rádio baseados em verificação do meio, quando uma estação está apta a receber quadros de duas ou mais estações, mas estes terminais não recebem sinais um do outro, aparece um fenômeno conhecido como problema do terminal escondido, ilustrado na Figura 2.5, que resulta em uma probabilidade de colisão. Para a solução do problema, utiliza-se o esquema RTS/*CTS (Request To Send / Clear To Send)*, em adição ao esquema básico.

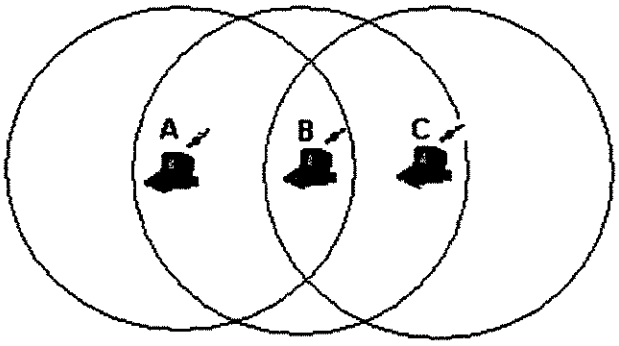

Figura 2.5 - Problema do Terminal Escondido.

No esquema RTS/CTS, ilustrado na Figura 2.6, uma estação para reservar o canal envia um RTS antes de cada transmissão. Se o destino estiver pronto para receber, ele responderá com um CTS e o canal estará reservado durante o envio dos pacotes. Quando a origem receber o CTS, ela começará a transmitir seus quadros através do canal reservado por ela durante todo o processo. As estações que ouvirem o RTS, o CTS, ou o quadro de dados, utilizam a informação de duração da transmissão destes quadros para atualizar o seu vetor de alocação de rede (*Network Allocation Vector – NAV*), utilizado para detecção virtual da portadora (Figura 2.6). Com o NAV, as estações não envolvidas na transmissão evitam fazer uso do meio no período de tempo reservado. Logo, qualquer terminal escondido poderá adiar sua transmissão, evitando-se assim colisões. As estações só tentarão novas transmissões quando seus vetores de alocação da rede indicarem não haver mais transmissões pendentes.

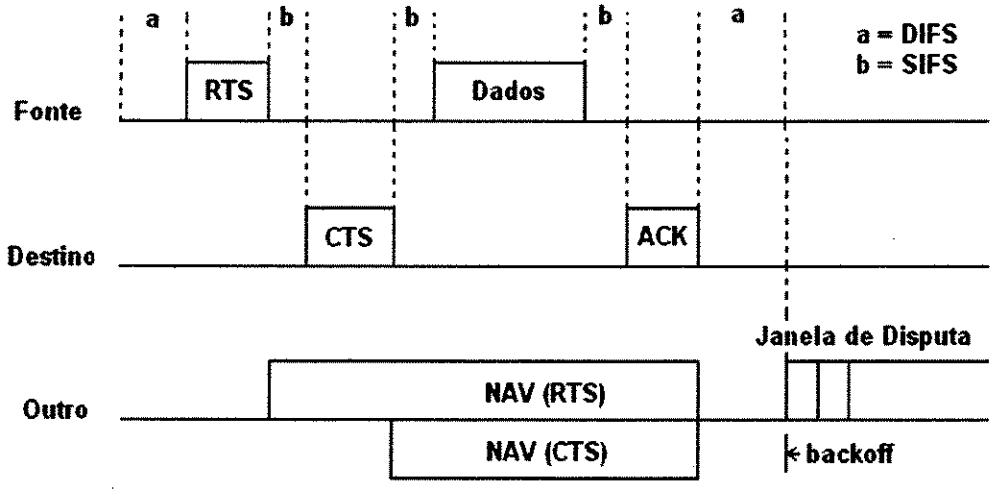

Figura 2.6 - Esquema RTS/CTS.

2.3.2. Função de Coordenação Pontual (PCF)

O PCF é um outro tipo de acesso da camada MAC do 802.11 que, ao contrário do DCF, não é obrigatório sua implementação. É um mecanismo centralizado que requer a presença de uma estação base funcionando como um coordenador de ponto (CP). Através da consulta a cada estação, o coordenador de ponto controla o acesso ao meio, proporcionando a transmissão sem disputa.

Se o PCF for utilizado, ele irá coexistir com o DCF e o tempo será dividido em superquadros, conforme a Figura 2.7. Cada superquadro consiste em um período de disputa para o DCF e um período livre de disputa (*Contention Free Period – CFP*) onde o PCF é utilizado.

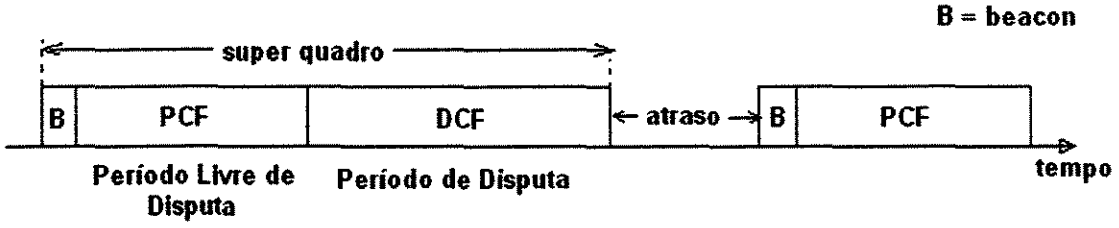

Figura 2.7 - Modos DCF e PCF operando juntos.

O período livre de disputa inicia-se com um sinal de marcação, chamado de *beacon*, enviado pela estação base. O coordenador de ponto mantém uma lista com todas as estações móveis que solicitaram ser eleitas para transmitir dados. Durante o período livre de disputa, o CP envia quadros para as estações informando quando elas estarão livres para acessar o meio. Para assegurar que nenhuma estação DCF será capaz de interromper o modo PCF, o IFS entre os pacotes de dados do CP é menor do que o DIFS. Este IFS é chamado de PIFS (*PCF Interframe Space*). As estações que não transmitirem por alguns ciclos serão retiradas da lista de consulta e serão consultadas novamente no início do próximo período livre de disputa.

2.4. O Padrão IEEE 802.11a

O padrão 802.11a [11] foi desenvolvido para operar na banda de 5 *GHz (U-NII – Unlicensed National Information Infrastructure)*, suportando taxa de dados de até 54 Mbps

[11]. Foram alocados 300 MHz do espectro na banda de 5 GHz, sendo que 200 MHz na faixa de freqüência de 5,15 a 5,35 GHz, e outros 100 MHz na faixa de 5,725 a 5,825 GHz [12]. Os primeiros 100 MHz estão restritos a máxima potência de saída de 50 mW e quatro canais. O segundo bloco de 100 MHz a 250 mW e com 4 canais e o último bloco, a 1 W e 4 canais.

Com relação à camada física, o padrão IEEE 802.11a utiliza a tecnologia chamada de OFDM, citada no item 2.2. A vantagem desta tecnologia sobre a *spread spectrum* consiste na maior disponibilidade de canais e na maior taxa de transmissão de dados. No padrão IEEE 802.11a, foram definidos doze canais de 20 MHz de largura, cada canal subdividido em 52 portadoras de 300 KHz de largura. A OFDM utiliza 48 destas portadoras para dados, sendo que as outras quatro portadoras para correção de erro (Figura 2.8).

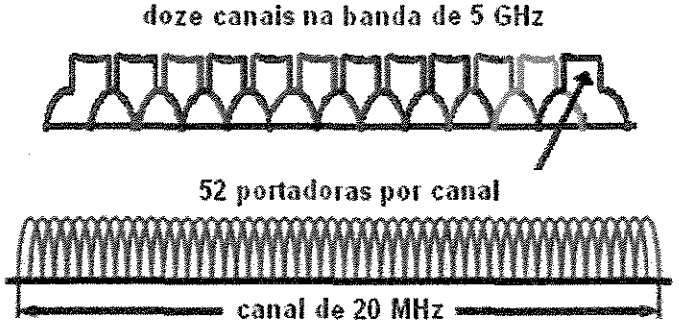

Figura 2.8 - Divisão de canais na tecnologia OFDM.

Com relação à taxa de dados, utilizando-se a modulação BPSK (*Binary Phase Shift Keying*), codifica-se 125 Kbps por portadora, obtendo-se 6 Mbps de velocidade. Utilizando-se QPSK (*Quadrature Phase Shift Keying*), dobra-se a taxa de transmissão de dados para 250 Kbps por portadora, obtendo-se 12 Mbps de velocidade. Com a modulação 16-QAM (*16-level quadrature amplitude modulation*), codifica-se 4 bits por hertz, alcançando-se uma taxa de 24 Mbps. Por último, com a modulação 64-QAM (*64-level quadrature amplitude modulation*), obtém-se taxas de até 54 Mbps. De acordo com [12], quanto maior o número de bits por ciclos (Hz) codificados, mantendo-se a potência de saída constante, mais susceptível ficará o sinal a interferências.

2.4.1. Especificação Física dos Sinais

A camada física do padrão IEEE 802.11a [11] é dividida em duas partes, chamadas de protocolo de convergência de nível físico *(PLCP - Physical Layer Convergence Protocol)* e PMD *(Physical Medium Dependent)*. A subcamada PMD define as características e os métodos para o envio e recepção de dados entre duas ou mais estações, que no caso do padrão IEEE 802.11a é a utilização da banda de 5 GHz com a técnica OFDM. Já a subcamada PLCP define métodos para mapear o meio físico no formato de quadros *(frames)*, adequados para o envio e o recebimento de dados e o gerenciamento de informações entre duas ou mais estações, utilizando-se a subcamada PMD. Também permite que a camada MAC opere com a mínima dependência da subcamada PMD. É subdividido em PLCP *Preamble* e PLCP *Header*, conforme ilustrado na Figura 2.9.

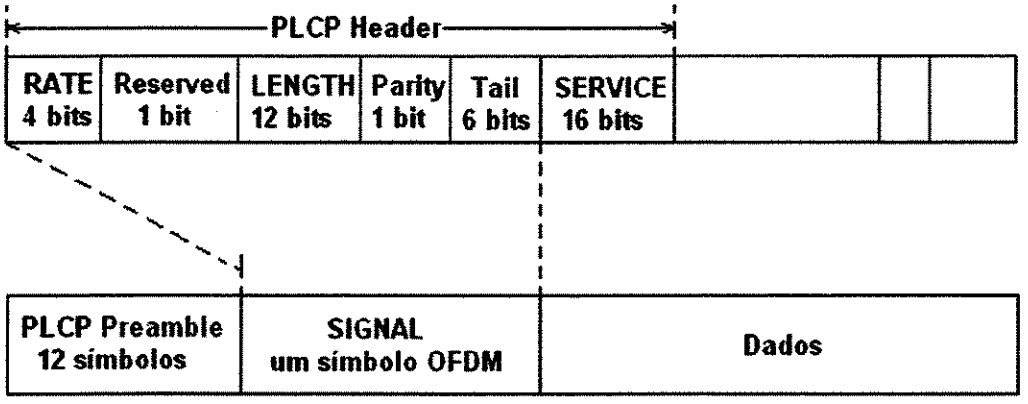

Figura 2.9 - A subcamada PLCP do padrão IEEE 802.11a.

A subcamada PLCP *Preamble* é utilizada para sincronização. Já a subcamada PLCP *Header* é dividida nas seguintes partes:

a – RATE: quatro bits que possuem informações sobre o tipo de modulação utilizado;

b – Reserved: um bit reservado para usos futuros;

c – LENGTH: 12 bits que indicam o número de octetos que a camada MAC está solicitando à camada física para transmitir;

d – Parity: um bit (17) de paridade;

e – Tail: seis bits (18 a 23), todos setados em zero; e

f – SERVICE: 16 bits, denotados de 0 a 15. O bit 0 será transmitido primeiro. Os bits de 0 a 6, que serão transmitidos inicialmente, são setados em zero e são utilizados para sincronização com o receptor. Os nove bits restantes estão reservados para uso futuro.

2.5. O Padrão IEEE 802.11b

O padrão IEEE 802.11b [13,14] utiliza a tecnologia DSSS, conforme citado no item 2.1.1, na banda ISM (*Industrial, Scientific and Medical*) de 2,4 GHz. Para cada taxa de transmissão, é utilizada determinada técnica de modulação. Para transmissões de 1 Mbps, o código barker de 11 bits é utilizado, com a modulação binária por chaveamento de fase (*BPSK*). Para transmissões de 2 Mbps, é utilizado o código barker com a modulação quaternária por chaveamento de fase (*QPSK*), que permite a codificação de 2 bits de informação com a mesma faixa que o BPSK ocupa para codificar 1 bit.

Para taxas de transmissão de 5,5 e 11 Mbps, foi criado um padrão chamado de CCK (*Complementary Code Keying*) [15]. O código CCK é modulado com a tecnologia QPSK. Ao invés de se utilizar o código barker, ele utiliza um símbolo, com tamanho de 8 bits ou 8 chips (chip – padrão de bit redundante), a uma taxa de 11 Mchips/s, de um conjunto de 64 símbolos, e o modula utilizando-se os bits de informação. Para 5,5 Mbps cada símbolo, a uma taxa de 11 Mchips/s, representa quatro bits de informação, sendo que dois bits de informação são utilizados para selecionar um dos símbolos (de um conjunto de quatro símbolos) e os outros dois bits de informação são utilizados para a modulação QPSK. Para transmissões de 11 Mbps, cada símbolo, a uma taxa de 11 Mchips/s, representa oito bits de informação, sendo que seis bits de informação determinam um dos 64 símbolos e os outros dois bits de informação são utilizados para a modulação QPSK, isto é, rotacionam o símbolo de 8 chips.

2.5.1. Especificação Física dos Sinais

A camada física do padrão IEEE 802.11b [13] é dividida em duas partes, chamadas de PLCP (*Physical Layer Convergence Protocol*) e PMD (*Physical Medium Dependent*). A subcamada PMD define as características e os métodos de transmissão e recepção de dados através de um meio sem fio, conforme descrito no item 2.5. O PLCP é dividido em PLCP *Preamble* e PLCP *Header*. O PLCP *Preamble* consiste de 144 bits (conforme Figura 2.10), usados para determinar o ganho do dispositivo. É subdividido em 128 bits para sincronização e 16 bits para o padrão 1111001110100000. Este conjunto de 16 bits, chamado de SFD (*Start Frame Delimiter*) é utilizado para marcar o começo de cada *frame*.

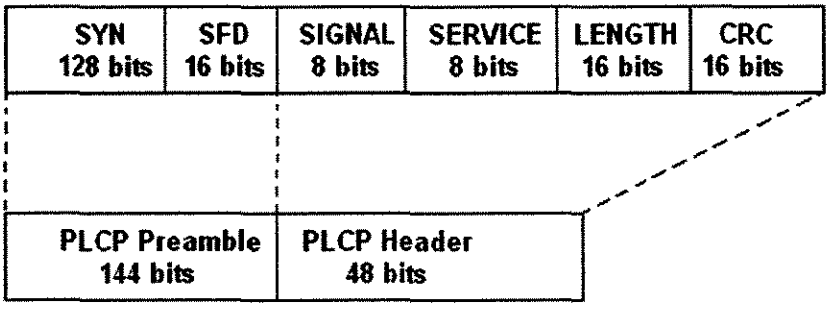

Figura 2.10 - A Subcamada PLCP do padrão IEEE 802.11b.

Na subcamada PLCP *header*, temos a seguinte seqüência de campos:

a) SIGNAL (8 bits): indica a taxa de transmissão (modulação) que será usada para transmissão (h0A 1Mbps DBPSK, h14 2Mbps DQPSK, h37 5,5 Mbps e h6E 11 Mbps);

b) SERVICE (8 bits): reservado para uso futuro;

c) LENGTH (16 bits): indica o número de bytes na unidade de dados de protocolo da camada MAC (*MPDU – MAC Layer Protocol Data Unit*); e

d) CRC – *Cyclic Redudancy Check* (16 bits): utilizado para detecção de erros e correção do PLCP *Header*.

2.6. O Padrão IEEE 802.11g

Em março de 2000, o grupo de trabalho IEEE 802.11, com o intuito de estender o padrão IEEE 802.11b para atingir taxas de transmissão maiores do que 20 Mbps, criou o padrão IEEE 802.11g, que utiliza o mesmo espectro de 2,4 GHz do padrão IEEE 802.11b e a mesma estrutura de pacotes, tecnologia de modulação e altas taxas de dados que o padrão IEEE 802.11a.

Um dos desafios para o desenvolvimento de equipamentos WLAN consiste nas distorções do sinal devido aos múltiplos caminhos. Um sinal refletido pode se combinar com o sinal original construtivamente ou destrutivamente. Em ambientes internos, a energia que chega no receptor através de atrasos de caminho podem atingir símbolos subsequentes, ou seja, a energia transmitida em um período de símbolo pode distorcer vários símbolos subsequentes. Portanto, o atraso por múltiplos caminhos pode causar uma interferência entre símbolos (*Inter-Symbol Interference – ISI*). Além disso, a quantidade de símbolos distorcidos varia com o período de um único símbolo.

Em 11 Mbps, o padrão IEEE 802.11b utiliza o CCK *(Complementary Code Keying)*, onde oito símbolos com a modulação QPSK representam oito bits de informação. A taxa do QPSK é de 11 milhões de símbolos por segundo o que fornece um período para cada símbolo de aproximadamente 91 nano segundos. Alguns caminhos secundários possuem atrasos de 400 a 500 nano segundos [16]. Nesta situação, a interferência entre símbolos (ISI) afeta de cinco a seis símbolos subsequentes. Para compensar os efeitos provocados por múltiplos caminhos nesta situação, são utilizados canais de equalização baseados no domínio do tempo [16], que tornam-se mais complexos a medida que a taxa de transmissão aumenta, já que mais símbolos subsequentes serão afetados.

Ao contrário de sistemas com portadora simples, o OFDM distribui os dados ao longo de várias subportadoras. No padrão IEEE 802.11a e IEEE 802.11g, são utilizadas 52 subportadoras, 48 delas para a transmissão de dados [16]. Desta forma, a taxa de transmissão de dados em cada portadora é muito menor do que a utilizada em sistemas com uma única portadora, obtendo-se períodos de símbolos mais longos. Nos padrões IEEE 802.11a e g, a duração de um símbolo para uma taxa de transmissão de 11 Mbps é de 4 μs,

44 vezes maior do que símbolos utilizando o CCK do 802.11b [16]. O intervalo de guarda neste caso é de 800 ns.

Uma vez que o período de guarda é eliminado, o pulso restante, de comprimento 3200 ns, estará livre de interferência entre símbolos, já que o intervalo de guarda é maior do que qualquer atraso por múltiplos caminhos. Logo, a complexidade dos canais de equalização de um processador com OFDM será menor do que com o CCK, já que a interferência entre símbolos no OFDM é menor para uma mesma taxa de transmissão. Este é o motivo pelo qual os sistemas OFDM são mais usados em aplicações WLAN para altas taxas de transmissão.

A versão final do padrão 802.11g foi aprovada pelo IEEE em julho de 2003. Foi estabelecido que será mandatário manter a compatibilidade com os rádios que utilizam o padrão IEEE 802.11b (2,4 GHz), bem como utilizar a técnica de modulação por múltiplas portadoras OFDM, visando o aumento da taxa de dados em até 54 Mbps. Foi estabelecido ainda que o padrão inclua o CCK (*CCK – Complementary Code Keying*) e o PBCC (*Packet Binary Convolutional Code*) como elementos opcionais [17].

2.6.1. Estrutura de Pacotes

Cada pacote de dados do padrão IEEE 802.11g transmitido consiste de duas partes principais (Figura 2.11) e suas partes podem ser transmitidas conforme os itens a, b, c e d do item 2.6.1.2.

Figura 2.11 – Estrutura do pacote de dados do padrão IEEE 802.11g.

2.6.1.1. Preamble/Header

Possui como função alertar aos rádios que compartilham um dado canal que a transmissão de dados está começando. O *preamble* é uma seqüência conhecida de 0's e 1's cuja função é a de disponibilizar tempo aos rádios para se prepararem no recebimento dos

dados. Quando o *preamble* estiver completo, o receptor deverá estar pronto para receber dados. O *header* segue imediatamente ao *preamble* e carrega importantes informações do pacote, uma delas é o comprimento do *payload*, cuja importância é a de informar aos receptores que "ouvem" o *preamble/header* sobre o comprimento da transmissão que segue. Os outros rádios não iniciarão a transmissão durante este período, evitando-se colisão na rede.

2.6.1.2. Payload

Pode variar significativamente em comprimento (64 a 1500 bytes), dependendo da taxa de dados e do número de bytes sendo transmitido. Os formatos para o *preamble/header* e *payload* podem ser os seguintes: CCK-CCK, OFDM-OFDM, CCK-OFDM e CCK-PBCC [17].

a) CCK - CCK

Ambos *preamble/header* e *payload* são transmitidos utilizando-se o CCK (Figura 2.12), utilizada no padrão IEEE 802.11b, que consiste de uma única portadora.

Figura 2.12 - Estrutura de um pacote utilizando-se CCK-CCK.

b) OFDM – OFDM

A tecnologia OFDM é a utilizada no padrão IEEE 802.11a. É uma ótima opção para altas taxas de dados (54 Mbps). Além disto, outra característica da tecnologia é o pequeno comprimento do *preamble*, desejável já que resulta em menor sobrecarga na rede. A OFDM é utilizada tanto no *preamble/header* quanto no *payload* (Figura 2.13).

Figura 2.13 - Estrutura de um pacote utilizando-se OFDM-OFDM.

c) CCK – OFDM

Conforme a Figura 2.14, o sistema é híbrido, utiliza o CCK para transmitir o *preamble/header* e o OFDM para transmitir o *payload*. O motivo em se utilizar o sistema híbrido é que quando o sistema estiver operando na presença de dispositivos IEEE 802.11b, o CCK *header* é transmitido para alertar a todos os dispositivos com o padrão IEEE 802.11b que a transmissão está para começar e informá-los sobre a duração da transmissão. O *payload* pode então ser transmitido com uma taxa de transmissão maior utilizando-se OFDM. Embora os dispositivos com o padrão IEEE 802.11b não sejam capazes de receber o *payload* com OFDM, qualquer colisão será prevenida pelo fato de que estes dispositivos podem coexistir com os dispositivos IEEE 802.11g, utilizando-se o CCK-OFDM. O uso do CCK *preamble* resulta em maior sobrecarga do que nos dispositivos utilizando o OFDM *preamble*.

Figura 2.14 – Estrutura de um pacote utilizando-se CCK – OFDM.

d) CCK - PBCC

Sistema híbrido com uma única portadora, permite taxa de transmissão máxima de 33 Mbps e emprega uma constelação mais complexa de sinais (8 – PSK) . Conforme a Figura 2.15, observa-se que no *preamble/header* é utilizado o CCK e no *payload* o PBCC.

Figura 2.15 – Estrutura de um pacote utilizando-se CCK – PBCC.

2.6.1.3. Listen-Before-Talk

Sob condições normais, todos os rádios de um determinado canal compartilham acesso por um mecanismo "*listen-before-talk*" (ouça antes de falar), cujo termo técnico é o CSMA/CA (*Carrier Sense Multiple Access / Colision Avoidance*). Logo, cada rádio do canal que desejar transmitir deverá esperar até que nenhuma transmissão esteja ocorrendo.

Rádios com o padrão IEEE 802.11g são capazes de receber tanto transmissões CCK quanto o OFDM. Porém, rádios com o CCK (dispositivos IEEE 802.11b) apenas recebem transmissões CCK, não "ouvindo" transmissões OFDM. A situação de dois rádios em um mesmo canal utilizando o primeiro apenas o CCK e o segundo apenas o OFDM é análoga ao problema do terminal escondido (descrito no item 2.3.1). Logo, a estrutura de um pacote utilizando-se o CCK-OFDM, para estações com o padrão IEEE 802.11g, soluciona o problema quando estações com o padrão IEEE 802.11b estiverem no mesmo alcance.

2.6.1.4. O mecanismo RTS/CTS

Nem sempre as estações e o ponto de acesso, compartilhando um mesmo canal, ouvem uns aos outros. Existem situações onde todas as estações podem ouvir ou serem ouvidas pelo ponto de acesso, porém não podem ouvir umas as outras, por causa da distância entre elas. Com isto, o mecanismo *listen-before-talk* não será eficiente, já que uma estação poderá detectar o canal livre para o ponto de acesso, enquanto outra estação estiver transmitindo para o mesmo ponto de acesso (problema do terminal escondido).

Logo, é utilizado outro mecanismo, chamado de RTS/CTS (*Request-To-Send / Clear-To-Send*), no qual cada nó envia uma mensagem RTS e recebe uma mensagem CTS antes que a transmissão ocorra (Figura 2.16).

Figura 2.16 – Pacote com o mecanismo RTS / CTS.

2.7. Segurança

O padrão IEEE 802.11 contém diversas formas de segurança [18], tais como o identificador de serviço (*SSID - Service Set Identifier*), WEP (*Wired Equivalent Privacy*) ou autenticação com chave compartilhada (*Shared Key Authentication*), que serão descritos abaixo.

2.7.1. Service Set Identifier (SSID)

O SSID [18] é um nome de rede que identifica uma área coberta por um ou mais AP's. Uma forma de operação é o AP periodicamente enviar seu SSID através de um sinal de marcação (*beacon*). A estações que desejarem se conectar com o referido AP recebem esta identificação e se associam. Outra forma de operação consiste nos AP's não transmitirem seus SSID's. As estações sem fio que desejarem se associar deverão possuir o SSID do AP requerido.

2.7.2. Wired Equivalent Privacy (WEP)

O modo WEP [18] é baseado no algoritmo de criptografia desenvolvido pela RSA Data Systems chamado de RC4. O processo de criptografia está ilustrado na Figura 2.17.

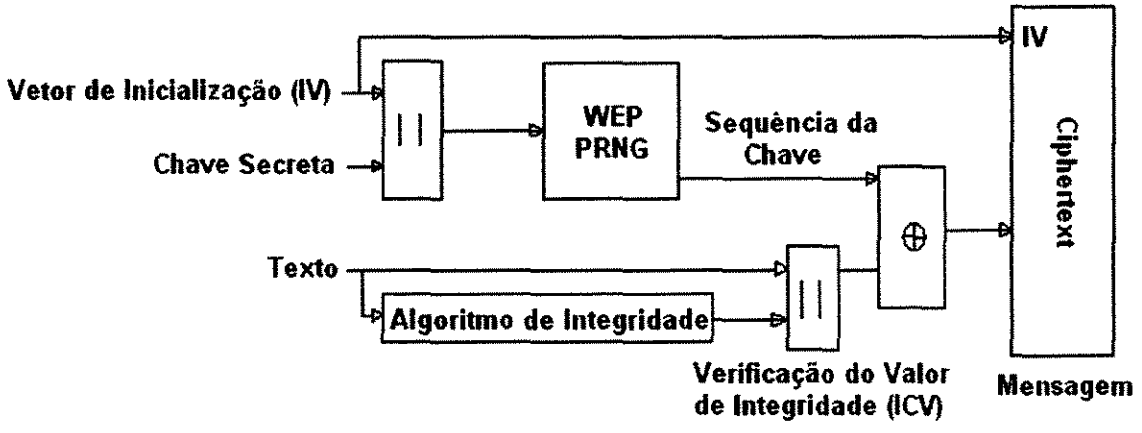

Figura 2.17 - Criptografia WEP.

O algoritmo opera da seguinte forma: assume-se que o transmissor e o receptor possuem a chave secreta. Na estação transmissora, a chave secreta de 40 bits é concatenada com o vetor de inicialização " IV " de 24 bits, resultando em uma chave de 64 bits de tamanho como entrada do WEP PRNG. Este resultado passa por um gerador de números pseudo aleatórios que gera um vetor baseado na chave de 64 bits. A seqüência resultante é usada para criptografar os dados através de um operador XOR, gerando uma seqüência chamada de *cyphertext* que será transmitida, concatenada com o vetor " IV ".

2.7.3. Autenticação Shared Key

Esta autenticação [18] implementa WEP e considera que ambas as estações que farão parte do processo compartilham a mesma chave (*Shared Key*). A estação que irá ser autenticada recebe um pacote do AP, criptografa utilizando a chave compartilhada e envia para o AP. Se depois de descriptografado pelo AP os pacotes forem iguais, a autenticação em um sentido está pronta. Para o outro sentido, processo inverso deverá ser executado. Uma das vulnerabilidades desta autenticação é a captura da forma criptografada de um pacote, fornecendo dados para corromper a criptografia WEP (*Wired Equivalent Privacy*).

2.8. Comparação entre os padrões IEEE 802.11a, IEEE 802.11b e IEEE 802.11g

Na definição de uma rede sem fio para um determinado ambiente e situação, devem ser analisadas diversas características para a escolha do melhor padrão, tais como velocidade de transmissão, vazão (*throughput)*, alcance, capacidade de canais e interferência com outros sistemas. A vazão (*throughput*) é definida como o número de pacotes de dados recebidos no destino com sucesso. A seguir serão comparados os padrões IEEE 802.11a, IEEE 802.11b e IEEE 802.11g para cada uma das características.

De acordo com [10] e a Figura 2.18, temos uma comparação entre os padrões IEEE 802.11a e IEEE 802.11b, com relação à taxa de transmissão, conforme o dispositivo se afasta do ponto de acesso (AP). Observa-se que, em qualquer distância do AP, o padrão IEEE 802.11a possui maior taxa de transmissão do que o padrão IEEE 802.11b. Porém,

para os padrões IEEE 802.11a e IEEE 802.11g, que possuem altas taxas de transmissão (54 Mbps), como um sinal na freqüência de 2,4 GHz possui maior facilidade de penetração em estruturas de concreto do que um sinal na freqüência de 5 GHz, temos que o sinal do padrão IEEE 802.11a se degrada com maior facilidade do que no padrão IEEE 802.11g. Logo, o alcance de dispositivos IEEE 802.11g é maior do que os padrões IEEE 802.11a e IEEE 802.11b.

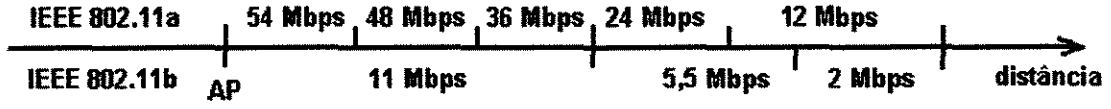

Figura 2.18 - Comparação entre os padrões IEEE 802.11a e IEEE 802.11b com relação a distância/taxa de transmissão.

Ambos os padrões IEEE 802.11a e IEEE 802.11g definem taxas de transmissão máximas de 54 Mbps [11,17]. Já o padrão IEEE 802.11b possui taxa de transmissão máxima de 11 Mbps [13]. Porém estas taxas são consideradas como velocidades "brutas" de transmissão em um sentido. Para cada padrão, uma taxa de transmissão de dados é alcançada com um determinado tipo de modulação, conforme indicado na Tabela 2.1 [19].

Tabela 2.1 – Taxa de transmissão de dados para padrões IEEE 802.11.

Taxa	**802.11b (2,4 GHz)**		**802.11g (2,4 GHz)**		**802.11a (5 GHz)**	
(Mbps)	**Mandatório**	**Opcional**	**Mandatório**	**Opcional**	**Mandatório**	**Opcional**
1	Barker		Barker			
2	Barker		Barker			
5,5	CCK		CCK	PBCC		
6			OFDM	CCK-OFDM	OFDM	
9				* *		OFDM
11	CCK		CCK	PBCC		
12			OFDM	CCK-OFDM	OFDM	
18				* *		OFDM
22				PBCC		
24			OFDM	CCK-OFDM	OFDM	
33				PBCC		
36				* *		OFDM
48				* *		OFDM
54				* *		OFDM

(* *) - OFDM, CCK - OFDM

A taxa de transmissão agregada é a combinação das taxa de transmissão de dados de cada dispositivo na rede que transmitem de uma vez [20]. Por exemplo, uma rede IEEE 802.11a (banda de freqüência de 5 GHz) suporta doze canais simultaneamente (definido para a América do Norte). Cada canal transmite a uma taxa máxima de 54 Mbps. Logo, a taxa de transmissão agregada da rede é de 12 x 54 Mbps, ou 648 Mbps. Para o caso de uma rede 802.11b, temos três canais simultâneos, cada canal a uma taxa máxima de 11 Mbps, logo a taxa de transmissão agregada é de 3 x 11 Mbps ou 33 Mbps. Para redes 802.11g, temos três canais simultâneos, cada um com taxa máxima de 54 Mbps. Logo, a taxa de transmissão agregada é de 3 x 54 Mbps, ou 162 Mbps.

Quando dois dispositivos de freqüências distintas (por exemplo o padrão IEEE 802.11a e IEEE 802.11b) operam em uma mesma rede, não há interferência de um dispositivo com o outro, logo temos a soma da taxa de transmissão agregada (para o exemplo, teríamos 648 + 33 = 681 Mbps). O mesmo não ocorre quando dois dispositivos com freqüências iguais são utilizados em um mesmo ambiente. Quando dois clientes em um mesmo ambiente utilizam os padrões IEEE 802.11g (cliente 1) e IEEE 802.11b (cliente 2), e tendo em vista que o padrão IEEE 802.11g necessita operar em um modo mais lento para tornar-se compatível com o padrão IEEE 802.11b, observa-se uma redução substancial no desempenho da rede, conforme pode ser observado na Figura 2.19 [20].

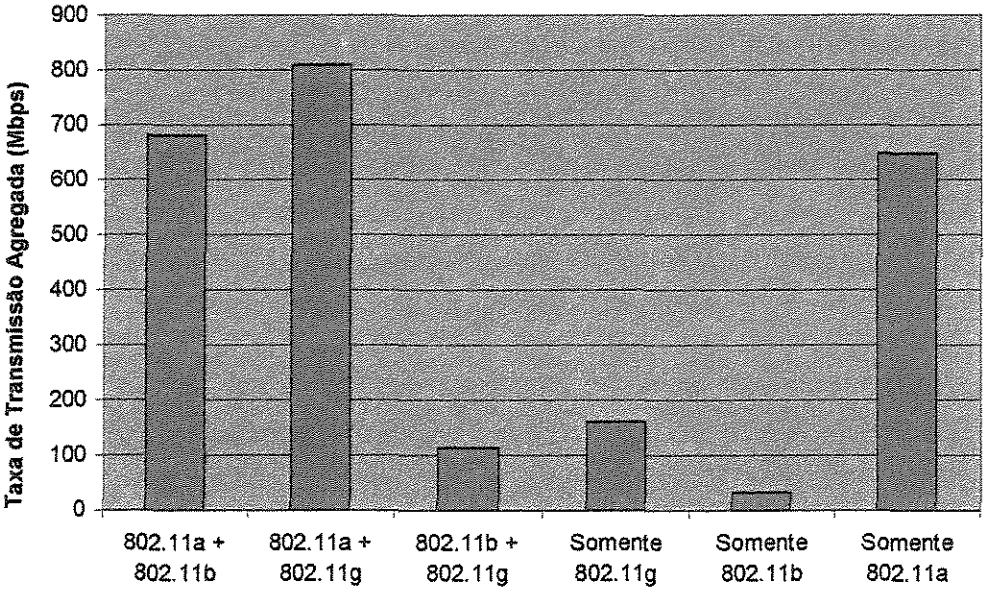

Figura 2.19 - Taxa de transmissão agregada para vários padrões IEEE 802.11.

A vazão (throughput) é definida como o número de pacote de dados recebidos no destino com sucesso. Verifica-se que em uma rede apenas com o padrão IEEE 802.11a, o potencial de vazão (*throughput*) é maior do que nos padrões IEEE 802.11b e IEEE 802.11g devido, sobretudo, a quantidade de canais e a taxa máxima de transmissão de dados por canal (54 Mbps). Porém, conforme citado anteriormente, devido as perdas do sinal serem maiores em dispositivos com freqüências de 5 GHz do que naqueles com freqüências de 2,4 GHz, quando atravessando superfícies de concreto (paredes), temos que a vazão para o padrão IEEE 802.11g é maior do que para o padrão IEEE 802.11a tanto para longas distâncias quanto com obstáculos. Em situações onde os dispositivos estejam muito próximos e sem obstáculos, as taxas de transmissão podem ser iguais.

A Tabela 2.2 mostra a vazão (*throughput*) alcançada em determinados cenários, analisados em [21]. Em todas as situações, uma série de pacotes de 1500 bytes de tamanho estão sendo transmitidos do AP para dois clientes, alternadamente, com as taxas de transmissão para cada cliente indicadas no campo descrição. A vazão total da Tabela 2.2 consiste na quantidade de pacotes recebidos sem erro em a e b durante um intervalo de tempo, que inclui também o tempo para o envio de um ACK do cliente para o AP e do intervalo de disputa. No cenário a, um pacote leva 1323 μs para ir do AP para cada cliente. O tempo do ACK mais o período de disputa[1] é de 350 μs. Logo, temos que após a transferência de dois pacotes de 1.500 bytes, a vazão é de: [2 x (8 x 1.500)] / [2 x (1.323 + 350) 10^{-6}] = 7,2 Mbps, que corresponde a vazão total, já que foi considerado que não há erros na transferência de pacotes, e que os períodos do ACK e de disputa são constantes. No cenário b, a taxa de transmissão para o cliente 1 é de 1 Mbps e para o cliente 2 é de 11 Mbps. Com isto, o tempo para transmitir um pacote do AP para o cliente 1 é de 12.794 μs, e para o cliente 2, de 1.323 μs. Da mesma forma que o cenário a, temos que a vazão total é de: [2 x (8 x 1.500)] / [(12.794 + 350) x 10^{-6} + (1.323 + 350) x 10^{-6}] = 1,6 Mbps. A queda da vazão entre os cenários a e b foi de 77%. De forma análoga, porém com valores de tempo de transmissão de pacote, de período de ACK e de disputa diferentes, observou-se uma queda de 70% do cenário c para o cenário d, devido a utilização de um cliente com taxa de transmissão menor.

[1] período de disputa: intervalo de backoff, conforme item 2.3.1.

Em um ambiente onde são utilizados os padrões IEEE 802.11b e IEEE 802.11g, como no cenário f, é necessária a utilização do mecanismo RTS/CTS, para que o padrão IEEE 802.11b (CCK) saiba quando o dispositivo com o padrão IEEE 802.11g (OFDM) irá transmitir. Os pacotes do padrão 802.11g são precedidos pelo pacote CTS, transmitido utilizando-se a modulação CCK. O pacote CTS transporta a quantidade de tempo para o aparecimento do pacote OFDM e ACK. Um dispositivo quando recebe esta informação permanece ocioso pelo período de tempo determinado, evitando-se assim colisões com a troca de pacotes. Este efeito, contudo, torna os dispositivos da rede mais lentos. A vazão total nesta situação, obtida em [21] foi de 11,2 Mbps, representando uma queda de 64% com relação ao cenário e da Tabela 2.2 (utilizando-se apenas o padrão IEEE 802.11g). A queda resultante é significativa, porém é menos severa com relação a redes utilizando os padrões IEEE 802.11a ou IEEE 802.11b.

Tabela 2.2 – Vazão (*throughput*) total em diversas configurações de rede sem fio.

Cenário	**Descrição**	**Vazão total**
a	Dois cliente operando a 11 Mbps Padrão IEEE 802.11b para ambos	7,2 Mbps
b	Cliente 1 (1 Mbps) e Cliente 2 (11 Mbps) IEEE 802.11b e IEEE 802.11b	1,6 Mbps
c	Dois clientes operando a 54 Mbps Padrão IEEE 802.11a para ambos	30 Mbps
d	Cliente 1 (6 Mbps) e Cliente 2 (54 Mbps) IEEE 802.11a e IEEE 802.11a	9,2 Mbps
e	Dois clientes operando a 54 Mbps Padrão IEEE 802.11g para ambos	30 Mbps
f	Cliente 1 (11 Mbps) e Cliente 2 (54 Mbps) IEEE 802.11b e IEEE 802.11g	11,2 Mbps

No padrão IEEE 802.11b e IEEE 802.11g, equipamentos com a tecnologia *bluetooth* bem como equipamentos eletrônicos como telefones sem fio ou fornos de microondas podem interferir no sistema, pois trabalham com freqüências próxima a dos padrões (2,4 GHz), o que não acontece com o padrão IEEE 802.11a (5 GHz). Além disto, os padrões IEEE 802.11a e IEEE 802.11g são mais imunes a efeitos provocados por reflexão do sinal (multi caminhos) do que no padrão IEEE 802.11b, devido à utilização da modulação OFDM.

Capítulo 3

Protocolos de Roteamento em Redes Ad Hoc

Nas redes ad hoc, os nós funcionam como roteadores, recebendo e processando pacotes. Como a função do roteamento é de encaminhar um pacote de um nó fonte para um nó destino, torna-se necessário que os roteadores escolham uma rota adequada com base nas informações que possuem da rede.

Para o correto funcionamento do roteamento, os nós trocam informações entre si, de tal forma que conheçam as rotas disponíveis para cada destino. Como a topologia das redes ad hoc é dinâmica, os protocolos de roteamento tradicionais, como o *Routing Information Protocol – RIP* (baseado em Vetor de Distância) [22] e o *Open Shortest Path First – OSPF* (baseado em Estado do Enlace) [23] apresentam problemas para convergir nestas redes. No caso das redes cabeadas, que apresentam topologias estáticas, tais protocolos são mais adequados.

Além disso, a existência de enlaces assimétricos[2] faz com que a recepção de um sinal não forneça informações sobre a qualidade da conexão no sentido inverso, dificultando o roteamento em transmissões sem fio. Com isto, as informações de roteamento em um sentido podem não ser úteis no sentido reverso. Outro ponto a ser observado consiste no gasto com energia, já que os dispositivos das redes ad hoc funcionam com baterias, que possuem um tempo curto de operação. A redundância nas redes ad hoc não pode ser controlada, já que a topologia é dinâmica e é um fator determinante, diferentemente das redes cabeadas que possuem uma pequena e controlada redundância.

Logo, quando são projetados algoritmos para redes ad hoc, três fatores devem ser considerados [24]:

a) inexistência de uma entidade central;

b) capacidade de rápidas mudanças topológicas; e

c) ocorrência de todas as comunicações através de rádio freqüência.

---

[2] enlaces assimétricos: não possuem necessariamente as mesmas características em ambas as direções.

A falta de um ponto central, que coordene a rede como um todo, requer algoritmos distribuídos mais sofisticados para enfrentar o problema de roteamento. As mudanças topológicas podem deixar rapidamente obsoletas as informações de localização. Além disto, outro fator limitante a ser observado consiste no gasto com energia, que deve ser considerado em cada fase do projeto de algoritmos de roteamento para redes ad hoc.

De acordo com [25], as principais características para um algoritmo de roteamento são:

a) simplicidade: o algoritmo deve oferecer os serviços com a mínima quantidade de processamento;
b) robustez: o algoritmo deve funcionar corretamente por anos sem que ocorram falhas no sistema e deve sempre chegar a uma resposta aceitável;
c) escalabilidade: mesmo com o aumento do número de nós da rede, o algoritmo deve prever e continuar funcionando adequadamente;
d) convergência para a rota ótima: como as rotas podem mudar rapidamente, o algoritmo deve escolher a rota ótima de forma rápida;
e) aceitação de parâmetros de QoS (*Quality of Service*): para determinados tipos de tráfego, é imprescindível o suporte a parâmetros de QoS como perda de pacotes e atraso máximo;
f) adaptabilidade: o algoritmo deve ser capaz de trabalhar com mudanças freqüentes na topologia;
g) independência da tecnologia de rede: o algoritmo deve funcionar com a maior variedade de computadores e meios físicos; e
h) equidade ("*fairness*"): todos os nós móveis devem ser capazes de acessar os recursos providos pela rede.

Além das características citadas acima, o grupo de trabalho MANET (*Mobile Ad Hoc Networks*), que trata dos problemas relativo às redes ad hoc, definiu que as principais qualidades para protocolos de roteamento em redes ad hoc são [26]:

a) operar de forma distribuída;
b) ausência de *loops*: com relação a pacotes que trafegam na rede por períodos arbitrários de tempo, o algoritmo deve ser robusto, evitando-se que o desempenho da rede se degrade como um todo;
c) operações baseadas em demanda de tráfego: o método deve ser capaz de se adaptar a diferentes condições de tráfego e, se realizado de forma eficiente, tem-se melhor utilização dos recursos de rede e da energia da bateria;
d) segurança: se as camadas de rede e de enlace não garantirem segurança, os protocolos de roteamento MANET estarão vulneráveis a muitas formas de ataque. Portanto, é necessário que haja mecanismos para inibir modificações nas operações dos protocolos;
e) adaptação a inatividade: o protocolo deve ser capaz de adaptar-se, sem muitas conseqüências, a períodos de inatividade dos nós móveis, sejam estes períodos avisados com antecedência ou não; e
f) suporte a conexões unidirecionais: tipicamente os algoritmos de roteamento para redes ad hoc assumem conexões bidirecionais, sendo que muitos algoritmos não funcionam sobre conexões unidirecionais. Entretanto, o suporte a conexões unidirecionais é válido em situações onde um par de conexões unidirecionais (em direções opostas) forma a única conexão bidirecional entre dois grupos de redes ad hoc.

Desde o advento das redes DARPA nos anos 70, vários protocolos de roteamento foram desenvolvidos para redes ad hoc. Tais protocolos devem lidar com determinadas limitações da rede, tais como consumo de potência, pequena largura de banda e altas taxas de erros, além de mudanças freqüentes na sua topologia.

Duas classes são definidas para os protocolos de rede ad hoc: pró-ativos e sob-demanda (reativos) [27,2]. Para cada uma destas classes, vários protocolos foram desenvolvidos e alguns deles serão descritos a seguir.

3.1. Protocolos pró-ativos

Os protocolos pró-ativos procuram avaliar continuamente as rotas de modo que, quando se necessitar encaminhar um pacote, a rota já seja conhecida e possa ser utilizada imediatamente (de maneira similar aos protocolos de roteamento para redes fixas). Neste caso, os nós mantêm uma ou mais tabelas com informações referentes à rede e respondem a mudanças de topologia propagando atualizações, de modo a manter a consistência do roteamento. Estas atualizações são feitas periodicamente, o que faz com que haja sempre um número constante de transmissões em andamento.

Serão estudados os protocolos DSDV (*Destination Sequenced Distance Vector*), WRP (*Wireless Routing Protocol*) e CSGR (*Cluster Switch Gateway Routing*), descrevendo seus principais mecanismos.

3.1.1. Destination Sequenced Distance Vector (DSDV)

O algoritmo de roteamento por distância de vetor, ou de Bellman-Ford [28], foi utilizado na ARPANET, precursora da atual Internet. Possui maior eficiência computacional e maior simplicidade em relação aos algoritmos por estado de conexão (*link state*), porém apresenta a formação de *loops*, principalmente em situações onde ocorrem mudanças freqüentes de topologia na rede [29]. Daí, foi desenvolvido o protocolo DSDV [2,29], com base no algoritmo de Bellman-Ford e com melhorias para evitar a formação de *loops*.

No protocolo DSDV, cada nó na rede móvel mantém uma tabela de roteamento que possui todos os possíveis destinos dentro da rede, o número de saltos para cada destino e um número seqüencial para cada destino. O sistema de números seqüenciais é utilizado para distinguir novas rotas de velhas rotas, evitando-se assim a formação de *loops*. As atualizações da tabela de roteamento são realizadas de cada nó aos seus vizinhos (nós que se encontram dentro do alcance do sinal transmitido). Quando uma estação recebe novas informações, elas são comparadas com as disponíveis na tabela de roteamento. Qualquer rota com um número seqüencial mais recente é utilizada e as rotas com números seqüenciais mais antigos são descartadas. Se duas rotas (de um dado nó para um mesmo

destino) possuírem os mesmos números seqüenciais, então aquela que possuir o menor número de saltos é escolhida.

A atualização das informações de roteamento são acionadas pelo nó de duas formas: a primeira, pelo tempo, ocorre quando não há mudanças de topologia e o tempo expira. É necessário para informar a cada nó sobre sua existência na rede, através da transmissão de mensagens *hello*. A segunda forma, pelo evento, ocorre quando há mudanças de topologia na rede.

Para evitar que o tráfego na rede aumente, provocado pelas atualizações das informações de roteamento, o protocolo DSDV utiliza dois tipos de pacotes de atualização de rotas: o primeiro pacote, chamado de incremental (*incremental dump*), carrega somente as informações de roteamento modificadas desde o último pacote completo, não sendo necessário carregar toda a tabela de roteamento, evitando desperdício de banda. É adequado para redes relativamente estáveis. O segundo pacote, chamado de completo (*full dump*), carrega todas as informações de roteamento disponíveis. É adequado para redes com mudanças freqüentes de topologia, onde enviar vários pacotes incrementais para substituir algumas métricas de uma rota ocasionaria em uma carga de roteamento[3] maior do que com uma única substituição na tabela com o pacote completo.

As falhas de conexão podem ocorrer quando as estações se movem de um lugar para o outro. Uma falha de conexão é representada pela métrica ∞ e pode ser detectada pelo protocolo da camada de enlace ou pode ser deduzida se nenhuma transmissão tiver sido recebida por um vizinho. Quando ocorre uma falha de conexão para o próximo salto, qualquer rota que utilize esta conexão é imediatamente marcada com ∞ e uma atualização de rota é requerida. Um nó, ao receber um pacote com a métrica ∞, deve verificar, em sua tabela, se possui um número de seqüência com uma métrica finita para aquele destino. Se possuir, o nó dispara uma atualização de rota para disseminar as informações sobre o destino [29].

[3] carga de roteamento: número total de pacotes de roteamento transmitidos durante uma simulação. Pacotes enviados por múltiplos saltos, cada salto é contabilizado como uma transmissão.

3.1.2. Wireless Routing Protocol (WRP)

O WRP [30] é um protocolo de roteamento pró-ativo cujos nós de roteamento informam o predecessor e a distância a cada destino da rede sem fio. Predecessor é definido como o último nó antes do destino, contido em uma rota da fonte para o destino. Cada nó verifica a consistência das informações relativas ao predecessor, reportado por todos os seus vizinhos, eliminando-se situações de *loops* e provendo convergência de rotas mais rápidas. Vizinho de um nó é definido como aquele que possui conexão com o nó, ou seja, quando o nó e seu vizinho trocam diretamente mensagens de atualização com sucesso.

O WRP mantém quatro tabelas:

a) Tabela de distância (*distance table*): a tabela de distância de um nó i é uma matriz contendo, para cada destino j e para cada vizinho de i (k), a distância até j (D_{jk}^{i}) e o predecessor (p_{jk}^{i}) informado por k;
b) Tabela de Roteamento (*routing table*): a tabela de roteamento de um nó i é um vetor com uma entrada para cada destino j, especificando um identificador para o destino, a distância para o destino (D_j^i), o predecessor do menor caminho escolhido em direção a j (p_j^i), o sucessor do menor caminho escolhido para j (s_j^i) e um marcador (*tag*) utilizado para atualizar a tabela de roteamento;
c) Tabela de custo de conexão (*link-cost table*): lista para cada nó i o custo para transmitir uma informação através de cada vizinho k e o número de períodos de atualização que ocorreram desde que o nó i recebeu uma mensagem de erro de k. Quando ocorre uma falha de conexão, o custo para esta conexão é considerado como infinito (∞); e
d) Tabela de mensagens para transmissão *(message retransmission list table - MRL)*: permite que um nó i saiba quais atualizações de uma mensagem de atualização devem ser retransmitidas e quais vizinhos devem reconhecer tais transmissões. Cada entrada contém um número seqüencial de uma mensagem de atualização, um contador de retransmissão que é decrementado toda vez

que o nó *i* enviar uma nova mensagem de atualização, um marcador (*flag*) que especifica se o nó *k* enviou um ACK para a mensagem de atualização e uma lista de atualizações enviadas na mensagem de atualização.

Para assegurar que as informações de roteamento sejam precisas, os nós enviam mensagens de atualização periodicamente aos seus vizinhos. Logo, um nó pode decidir em atualizar sua tabela de roteamento após receber uma mensagem de atualização de um vizinho ou detectar uma mudança na conexão com o vizinho. Ao receber uma mensagem de atualização livre de erros, o nó destino envia um reconhecimento positivo (ACK) indicando que a conexão está adequada e que processou a mensagem de atualização. As mensagens de atualização contêm um identificador do nó que enviou a mensagem, um número seqüencial designado pelo nó emissor da mensagem, uma lista de atualizações (destino, distância ao destino, o predecessor do nó destino) e uma lista de resposta com os nós que devem enviar um ACK para a mensagem de atualização. A lista de resposta evita a situação de um vizinho enviar múltiplos ACK's para uma mesma mensagem de atualização, simplesmente porque algum outro vizinho não reconheceu a mensagem. Logo, além deste protocolo requerer que cada nó mantenha um grande volume de informações armazenadas, o tráfego na rede sem fio é maior devido às trocas de informações de roteamento.

Em adição aos ACK's, a conectividade pode ser averiguada com o recebimento de uma mensagem de um vizinho, que não necessita ser uma mensagem de atualização. Logo, mesmo se os nós não estiverem emitindo pacotes, eles sabem da existência de seus vizinhos através de mensagens de reconhecimento *(hello messages)*, transmitidas periodicamente. Quando um nó recebe uma mensagem *hello* de um novo nó, as informações do novo nó são adicionadas à tabela de roteamento de quem recebeu a mensagem. Se um nó não receber nenhum tipo de mensagem de seu vizinho por um período específico de tempo (três ou quatro vezes o intervalo de transmissão das mensagens *hello*), o nó deve assumir que a conectividade com seu vizinho foi perdida.

A Figura 3.1 ilustra o funcionamento de uma rede com o protocolo WRP. Assume-se que todos os nós e conexões possuem os mesmos atrasos de propagação. Os custos de conexão estão indicados na figura. O nó A é o fonte, D o destino e os nós B e C são

vizinhos do nó A. As setas nas conexões indicam a direção das mensagens de atualização e os valores entre parênteses são a distância e o predecessor ao destino D. Cada atualização é reconhecida pelo recebimento de uma mensagem ACK do vizinho. Quando a conexão (D,C) falhar, os nós D e C enviarão mensagens de atualização para seus nós vizinhos. Quando A recebe a mensagem de atualização de C, ele atualiza sua tabela de distância através de C e procura um caminho alternativo para D através de outros nós vizinhos. Se nenhum pacote estiver sendo transmitido ou nenhuma mensagem de atualização estiver ocorrendo, mensagens *hello* serão transmitidas, visando a conectividade da rede.

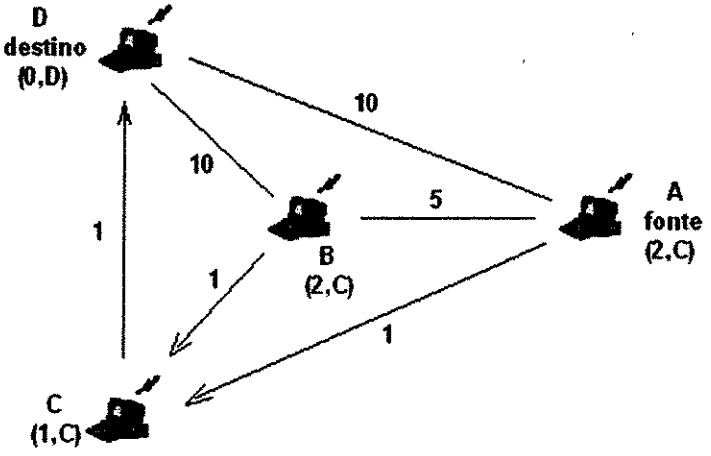

Figura 3.1 - Exemplo de operação com o WRP.

3.1.3. Cluster Switch Gateway Routing (CSGR)

No protocolo CSGR [2, 31], a rede é particionada em grupos (*cluster*), e cada grupo é controlado por um *cluster head*, introduzindo a idéia de hierarquia. O agrupamento (*clustering*) possibilita o estabelecimento de uma estrutura para o acesso aos canais, roteamento e alocação de largura de banda.

Os nós podem ser de três tipos: o primeiro tipo, *cluster head*, roteia as informações entre os nós de um *cluster* e o nó ponte (*gateway*); o segundo tipo, nó ponte (*gateway*), é o nó de ligação entre dois *clusters*; o terceiro tipo é considerado como nó geral, já que não possui as características dos nós cluster head e ponte, conforme ilustrado na Figura 3.2.

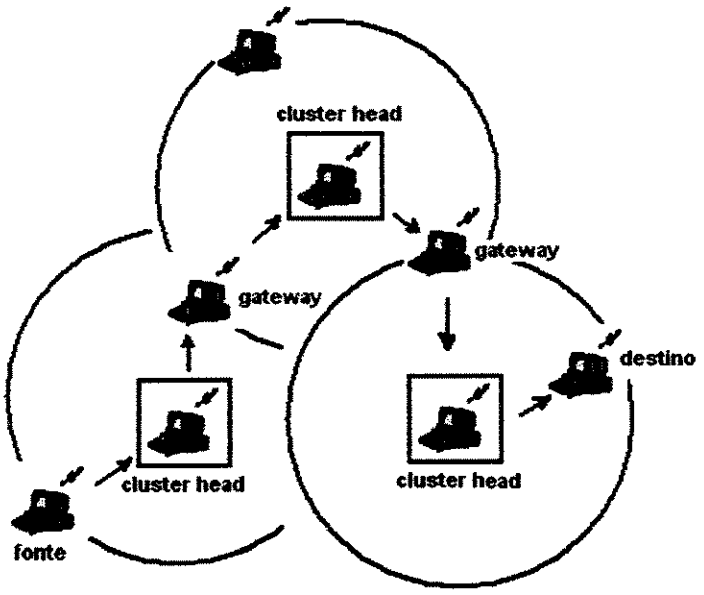

Figura 3.2 - Representação dos tipos de nós em uma rede com protocolo CSGR.

Um pacote enviado por um nó (fonte) é primeiro roteado para seu *cluster head.* Após, o pacote é roteado através do caminho *cluster head - gateway – cluster head* até chegar ao nó destino. Cada nó deve manter uma tabela, denominada *cluster member table*, onde são guardados os cluster head para cada nó da rede. A tabela é transmitida periodicamente pela rede utilizando o protocolo DSDV. Além disto, cada nó deve manter uma tabela de roteamento, usada para determinar o próximo salto para alcançar o destino [2]. Ao receber o pacote, o nó consultará sua tabela *cluster member table* para determinar o *cluster head* ao longo da rota mais próximo para o destino. O nó então verifica em sua tabela de roteamento o próximo salto para alcançar o *cluster head.*

Mudanças freqüentes no *cluster head* afetam o desempenho da rede, já que os nós despendem muito tempo convergindo para um *cluster head* ao invés de enviar os dados para o destino desejado. Para evitar que novos *cluster head* sejam selecionados com freqüência, um algoritmo de mínima mudança de grupo (*Least Cluster Change – LCC*) é introduzido. Com este algoritmo, o *cluster head* muda somente se dois deles estiverem muito próximos, ou quando um nó mover-se para fora do alcance de todos os *cluster heads.*

3.2. Protocolos sob-demanda ou reativos

Esta classe de protocolos de roteamento cria as rotas somente quando o nó fonte necessitar, iniciando um processo de descoberta da rota dentro da rede. Este processo é completado se a rota for descoberta ou se todas as possíveis rotas alternativas forem examinadas. Uma vez que a rota é descoberta e estabelecida, utiliza-se um procedimento de manutenção de rota para que a mesma continue ativa. Como a necessidade de transmissão de um pacote de dados é o evento que dispara a descoberta das rotas, estes protocolos não trocam mensagens a intervalos regulares, o que economiza banda passante e energia. O volume de tráfego de controle de roteamento varia de acordo com a utilização da rede. Porém, estes protocolos apresentam uma maior latência no encaminhamento das mensagens, uma vez que a transmissão de dados só pode ser efetuada após a construção de uma rota para o destino.

Serão estudados os protocolos AODV (*Ad Hoc On-Demand Distance Vector Routing*) e DSR (*Dynamic Source Routing*), descrevendo seus principais mecanismos.

3.2.1. Ad Hoc On-Demand Distance Vector Routing (AODV)

Com o objetivo de eliminar a necessidade de transmissões periódicas, foi desenvolvido o protocolo AODV [2,32], que cria rotas sob demanda ao invés de manter uma lista atualizada de rotas para todos os nós, como no protocolo DSDV (item 3.1.1), o que minimiza o número de transmissões requeridas. Ele utiliza tabelas de roteamento em cada nó intermediário, cada uma com uma entrada por destino. O projeto do algoritmo não considera o meio físico no qual os nós se encontram. O único requisito para o meio físico é que cada nó detecte a transmissão de cada um de seus vizinhos (vizinho de um nó é aquele que recebe com sucesso o sinal transmitido do nó), e que cada vizinho detecte a transmissão do nó.

Os objetivos primários do algoritmo são:

a) transmitir os pacotes de descoberta de rotas somente quando necessário;

b) distinguir o gerenciamento de conectividade local (detecção da vizinhança) e manutenção da topologia; e

c) disseminar informações sobre mudanças de conectividade local para os nós vizinhos que necessitarem.

O AODV usa conexões simétricas entre os nós vizinhos e um mecanismo de descoberta de rota como utilizado no protocolo DSR (*Dynamic Source Routing*) [33], com algumas modificações. Ao invés do roteamento na fonte, o AODV estabelece tabelas de rotas dinâmicas em cada nó intermediário. Esta diferença é vantajosa já que a largura de banda para transportar um pacote de dados é menor. Para manter as informações de roteamento mais recentes entre os nós, é utilizado o conceito de número seqüencial, como no DSDV [29]. Cada nó mantém um contador de número seqüencial crescente, usado para substituir as rotas antigas armazenadas. A combinação destas técnicas resulta em um algoritmo que utiliza eficientemente a largura de banda, responde às mudanças de topologia e assegura um roteamento livre de *loops*. O protocolo utiliza dois mecanismos, descoberta da rota e manutenção da rota, que serão descritos a seguir.

3.2.1.1. Descoberta da Rota

Mecanismo através do qual o nó fonte obtém uma rota para o nó destino, diretamente se o destino estiver dentro de seu alcance ou através de nós intermediários, visando a transmissão de pacotes. O nó fonte inicia a descoberta da rota transmitindo um pacote de solicitação de rota (*Route Request Packet - RREQ*) para seus vizinhos. O RREQ contém os seguintes campos:

- endereço da fonte;
- número seqüencial da fonte;
- *broadcast_id*;
- endereço do destino;
- número seqüencial do destino; e
- contador de saltos (*hop_cnt*).

O par < endereço da fonte, *broadcast_id* > identifica unicamente um RREQ. O *broadcast_id* é incrementado toda vez que o nó fonte emitir um novo RREQ. O número seqüencial da fonte é usado para manter as informações mais recentes da rota reversa para a fonte. O número seqüencial do destino especifica o quão recente a rota para o destino deve estar antes de ser aceita pela fonte. Se um nó ao receber o RREQ for o destino, enviará um pacote de resposta de rota (*Route Reply Packet – RREP*) para a fonte. Se um nó intermediário receber um RREQ e posteriormente receber outros RREQ's com o mesmo *broadcast_id* e endereço da fonte, então ele descartará os últimos RREQ's e não os transmitirá. Se um nó não satisfaz o RREQ ao recebê-lo, ele incrementa o hoc_cnt, transmite o pacote a seus vizinhos e guarda as seguintes informações do RREQ:

- endereço do destino;
- endereço da fonte;
- *broadcast_id*;
- tempo limite para a rota reversa; e
- número seqüencial do nó fonte.

Conforme o RREQ é transmitido da fonte para os demais nós, ele automaticamente forma a rota reversa para a fonte, conforme ilustrado na Figura 3.3 (setas em azul), gravando em cada nó o endereço do nó vizinho que enviou o RREQ. A rota reversa é mantida por tempo suficiente para que o RREQ atravesse a rede e produza uma resposta para o nó fonte.

Um RREQ eventualmente encontra um nó intermediário que possui uma rota até o destino. O nó inicialmente verifica se o RREQ foi recebido sobre uma conexão bidirecional. Se for, ele verifica se a rota é a mais atual, comparando o número seqüencial de destino do RREQ com o número seqüencial de destino existente no nó. Se o número seqüencial de destino do RREQ for maior do que o do nó intermediário, então a rota até o destino contida no nó intermediário não será usada. O nó apenas transmite o RREQ a seus vizinhos. Se o número seqüencial de destino do RREQ for menor ou igual ao do nó intermediário, então o nó transmite um RREP ao vizinho que enviou o RREQ. O RREP contém as seguintes informações:

- endereço da fonte;
- endereço do destino;
- número seqüencial de destino;
- contador de saltos (*hop_cnt*); e
- tempo de duração da rota (*lifetime*).

Quando o RREQ alcança um nó que possui uma rota válida até o destino, a rota reversa já está estabelecida. Enquanto o RREP é transmitido para a fonte, cada nó intermediário da rota atualiza as informações do tempo de duração da rota e grava o último número seqüencial para o destino. Os nós que não pertencerem a rota determinada pelo RREP, após 3 s, terão suas rotas reversas apagadas [32].

O nó que recebe o primeiro RREP o propaga em direção a fonte. Se outros RREP's forem recebidos para uma mesma fonte, então somente aqueles que possuírem números seqüenciais de destino maiores ou iguais com a menor contagem de saltos serão atualizados pelo nó fonte, assegurando informações de roteamento mais rápidas e atualizadas.

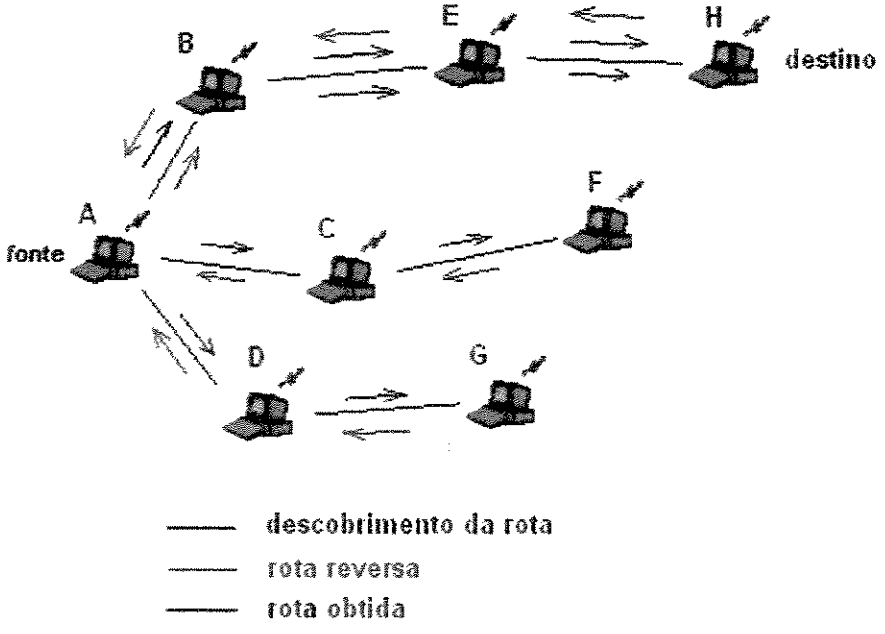

Figura 3.3 - Descoberta da rota e resposta no protocolo AODV.

3.2.1.2. Manutenção da Rota

Cada nó móvel mantém uma tabela para as rotas ativas para cada destino com as seguintes informações:

- destino;
- próximo salto;
- número de saltos (métrica);
- número seqüencial para o destino;
- vizinhos ativos para a rota; e
- tempo de duração para a rota (*timeout*).

Toda vez que uma tabela de rota é usada para transmitir dados da fonte para o destino, o tempo de duração da rota (*timeout*) é reinicializado. Caso uma nova rota seja oferecida para o nó, ela será utilizada se o seu número seqüencial de destino for maior ou igual (com menor número de saltos) ao existente no nó.

Um nó ao detectar uma falha de conexão, propaga uma mensagem de notificação de falha de conexão, que consiste em transmitir aos seus vizinhos um RREP com número seqüencial de destino maior do que o existente na rota e com o valor do número de saltos (*hop_cnt*) igual a ∞. Ao receber a notificação, caso os nós fonte continuem necessitando de uma rota ao destino, inicializarão o processo de descoberta da rota transmitindo um RREQ com um número seqüencial de destino maior do que os anteriores.

Um aspecto adicional do protocolo consiste na transmissão periódica de mensagens de reconhecimento denominadas mensagens *hello*, de um nó para os seus vizinhos, visando assegurar a conectividade local de um nó, bem como detectar falhas de conexão. As mensagens *hello* contêm um identificador e um número seqüencial do nó emissor. O gerenciamento da conectividade local com mensagens *hello's* pode também ser usado para assegurar que somente nós com conectividade bidirecional sejam considerados como vizinhos.

3.2.2. Dynamic Source Routing (DSR)

O roteamento da fonte é uma técnica na qual o nó fonte do pacote determina e constrói a seqüência completa de nós para encaminhar o pacote. O nó fonte lista a rota no cabeçalho do pacote, identificando cada endereço dos nós para transmitir o pacote até o nó destino. O DSR [2,33] é um protocolo de roteamento na fonte, que não utiliza mensagens de reconhecimento como as utilizadas no AODV (mensagens *hello*), o que reduz a largura de banda necessária e o consumo de energia das baterias dos dispositivos sem fio.

Para enviar um pacote de dados para um nó destino, o nó fonte constrói uma rota no cabeçalho do pacote. O nó fonte então transmite o pacote de dados para o primeiro nó identificado na rota. Quando o nó recebe o pacote, se ele não for o destino, ele simplesmente transmite o pacote para o próximo salto (nó) identificado no cabeçalho do pacote. Cada nó fonte da rede mantém em sua memória (*route cache*) as rotas que foram descobertas, dado que estas podem ser utilizadas por um outro nó até o mesmo destino. Caso não possua, será utilizado o mecanismo de descoberta da rota.

Enquanto o nó fonte estiver utilizando uma determinada rota, um monitoramento deve ser feito para garantir sua correta operação. Por exemplo, se o nó fonte, destino, ou qualquer nó intermediário mover-se para fora do alcance da transmissão de seus nós anterior ou posterior, a rota não mais poderá ser utilizada até o destino. Este monitoramento é chamado de manutenção da rota. Quando este mecanismo detectar algum problema com a rota, um novo caminho deverá ser utilizado até o destino. A seguir, os mecanismos de descoberta e manutenção da rota são descritos.

3.2.2.1. Descoberta da Rota

Mecanismo através do qual um nó S obtém uma rota para D, diretamente se o destino estiver dentro de seu alcance, ou através de nós intermediários, visando a transmissão de pacotes. O nó inicia a descoberta da rota transmitindo um pacote de solicitação de rota (*Route Request Packet - RREQ*) que será recebido por aqueles nós que estiverem dentro de seu alcance de transmissão. No exemplo da Figura 3.4, suponha que o nó A deseja transmitir um pacote para o nó E. Para o iniciar o processo de descobrimento

de rota, o nó A transmite um pacote de solicitação de rota, por difusão, para todos os nós que estiverem dentro de seu alcance de transmissão. Cada pacote de solicitação de rota contém o nó de origem e o nó de destino, um identificador único determinado pela origem (*request id*) e uma lista de endereços, iniciada pelo nó de origem, de cada no intermediário por onde ele tenha passado até então. Para que se detecte requisições de rotas duplicadas, cada nó da rede mantém uma lista com o endereço da fonte e *request_id* das RREQ's recebidas.

Quando qualquer outro nó (por exemplo, B ou C) receber o pacote de solicitação de rota, processará a resposta de acordo com os seguintes passos:

a) O nó intermediário confere se é o destino. Se for, responde para o nó fonte do processo (RREP), com uma cópia da rota acumulada no pacote de solicitação de rota. O nó A armazena esta informação em seu *route cache*;

b) Se não for o destino (E), o nó verifica se este pacote já foi recebido ou se o seu endereço já está listado na requisição de rota. Se qualquer uma das alternativas for verdadeira, o pacote é descartado;

c) Senão, o nó procura em sua memória uma rota para E. Caso exista, ele envia uma resposta de rota (RREP) para o nó origem contendo o caminho completo até o destino;

d) Caso contrário, ele adiciona seu próprio endereço e transmite o pacote por difusão.

O pacote segue o mesmo processo até alcançar o destino ou até que todas as tentativas sejam realizadas. O processo de descartar um pacote quando o endereço do nó intermediário já estiver listado na rota elimina a possibilidade do pacote se propagar em *loop*.

Quando o nó destino receber o pacote de solicitação de rota, ele deverá transmitir um pacote de resposta de rota (*Route Reply Packet - RREP*) para o nó de origem. Se o destino possuir uma rota em seu *route cache* para o nó fonte, o pacote de resposta será transmitido utilizando-se tal rota. Se ele não possuir o pacote de resposta de rota (RREP), seguirá a rota reversa do pacote de solicitação de rota (RREQ). Isto requer enlaces bidirecionais que, embora evitem a sobrecarga de um novo descobrimento de rota, não funcionam em determinados meios ou protocolos da camada MAC. Além disto, o destino responderá à fonte a todos os RREQ's que forem recebidos com mesmo *request_id* e

endereço da fonte. Logo, a fonte assegura rotas alternativas para o destino, caso a rota primária (a mais curta) falhe.

Algumas otimizações foram disponibilizadas para o protocolo DSR. A primeira delas consiste em um nó poder adicionar entradas em sua *route cache* sempre que receber uma nova rota. Por exemplo, com os nós da Figura 3.4, se um pacote for transmitido de A para F com um único salto (sem passar por B), A usará esta nova rota para F, diminuindo o caminho para o nó E (destino). A segunda otimização consiste em evitar que vários RREP's sejam transmitidos à fonte com rotas maiores do que outras. O nó calcula um período de atraso, dependente do número de saltos da rota, que irá atrasar a transmissão do pacote de resposta. Se durante este intervalo qualquer outro pacote de solicitação de rota com o mesmo *request_id* e endereço da fonte for recebido com uma rota menor, a resposta para o pacote de solicitação de rota anterior será descartada e uma resposta para o novo pacote de solicitação de rota será transmitida. Na terceira otimização, se um nó estiver contido em uma rota e transmitir um pacote como nó intermediário, ele poderá verificar toda a rota no pacote e adicionar em seu *route cache* as informações de roteamento para vários destinos.

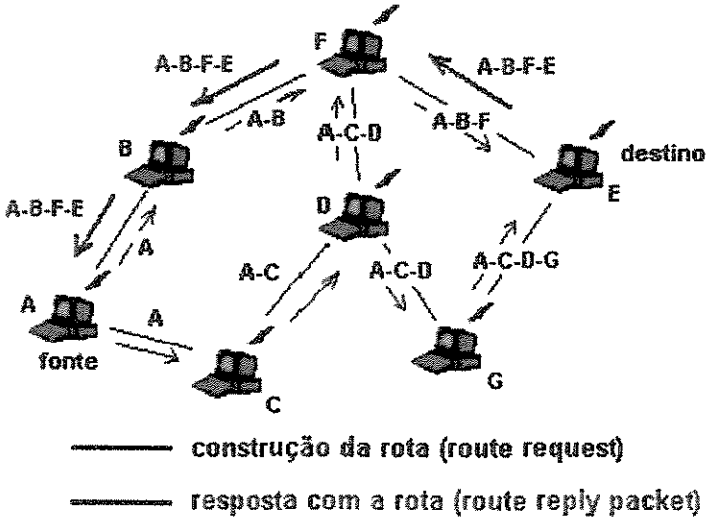

Figura 3.4 - Criação da rota do nó fonte ao nó destino, no protocolo DSR.

3.2.2.2. Manutenção da Rota

Neste algoritmo, não existem pacotes de atualização periódicos e sim um procedimento que monitora a operação da rota e informa à fonte sobre qualquer erro de roteamento. Se a camada de enlace (*data link)* encontrar algum problema de transmissão e não puder recuperá-lo (por exemplo, quando exceder o número máximo de pacotes que um nó atende), o nó envia um pacote de erro de rota (*route error packet*) para o emissor do pacote. O pacote de erro de rota contém o endereço do nó que detectou o erro e do nó que receberia o pacote. Para o retorno do pacote de erro de rota até a fonte, o nó deverá possuir em seu *route cache* uma rota para o nó fonte, que originou o pacote. Se o nó não possuir tal rota em seu *route cache*, o pacote de erro deve seguir a rota reversa do pacote de solicitação de rota. A última opção é a de salvar o pacote de erro de rota no nó, iniciar a descoberta da rota até o nó fonte e, após receber a resposta da rota, enviar o pacote de erro com a rota descoberta. Quando o pacote de erro de rota for recebido pelo nó fonte, o salto com erro é removido do *route cache* do nó e de todas as rotas que contiverem tal salto.

Em complemento às mensagens de erro de rota, são utilizados reconhecimentos do tipo passivo, com a finalidade de verificar a correta operação das conexões da rota. O reconhecimento passivo funciona da seguinte forma: depois de enviar um pacote para o próximo nó da rota, o nó emissor do pacote deve ser capaz de "ouvir" o próximo nó transmitir o pacote para seu nó subsequente e contido na rota. Da Figura 3.4, o nó B deve ser capaz de "ouvir" a transmissão de F para E. Se o reconhecimento passivo não for recebido por um determinado período de tempo, o nó B irá pressupor que o enlace de F para E se rompeu. O nó B deverá remover este enlace de sua memória (*cache*) e deverá retornar uma mensagem de erro de rota para a fonte (A). Se o nó A possuir outra rota até E em seu *route cache*, o pacote de dados será transmitido; senão, um novo descobrimento de rota deverá ser iniciado.

3.3. Comparação entre os protocolos de roteamento ad hoc

Nesta seção são comparadas as duas classes de protocolos de roteamento ad hoc: pró-ativa e sob-demanda. Além disto, são comparados, em cada classe, os protocolos de roteamento descritos neste trabalho: DSDV, WRP e CSGR para a classe pró-ativa e AODV e DSR para a classe sob-demanda.

3.3.1. Comparação entre as classes pró-ativa e sob-demanda

Conforme citado anteriormente, os protocolos pró-ativos mantém rotas constantemente atualizadas e disponíveis para todos os destinos, mesmo que elas não sejam necessárias. É utilizado um mecanismo de atualização das tabelas de roteamento, que envolve a constante propagação das informações de roteamento. Esta característica, embora útil para o tráfego de datagramas (por exemplo, a transmissão de voz pela rede), aumenta substancialmente o consumo de energia e a *carga* de roteamento (*overhead*) na rede. Nos protocolos da classe sob-demanda, uma rota será descoberta quando um nó for transmitir um pacote de dados. Com isto, o nó deverá esperar até que a rota seja descoberta, o que aumenta o tempo de espera para a transmissão dos dados, porém diminui o consumo de energia, já que não será necessário transmitir freqüentemente as informações de roteamento, como nos protocolos pró-ativos.

Outra consideração consiste no uso dos esquemas de endereçamento plano ou hierárquico. No endereçamento plano, os endereços não têm relação alguma com o lugar onde estão os nós dentro da rede. Já no endereçamento hierárquico, o endereço de um nó é constituído de acordo com os endereços correspondentes aos vários níveis hierárquicos de que ele faz parte. Todos os protocolos constantes neste trabalho, exceto o CSGR, utilizam o esquema de endereçamento plano, pois é menos complexo e mais fácil de usar, quando comparado com o esquema de endereçamento hierárquico. Porém, conforme citado em [34], existem dúvidas quanto a sua escalabilidade. A Tabela 3.1 lista as diferenças básicas entre as duas classes de protocolos.

Tabela 3.1 - Diferenças entre as classes de protocolos pró-ativo e sob-demanda.

Parâmetros	Protocolos sob-demanda	Protocolos pró-ativos
Informações de roteamento	Disponível quando necessário	Sempre disponível
Filosofia de roteamento	Plana	Plana, exceto pelo CSGR
Atualização periódica das rotas	Não requer	Requer

3.3.2. Comparação entre os protocolos de roteamento pró-ativos

O protocolo DSDV é basicamente uma modificação do algoritmo de roteamento de Bellman-Ford [28], com modificações na garantia de não haver *loops* e com um protocolo de atualização das rotas. O DSDV seleciona uma rota baseado no número seqüencial mais recente ou, caso os números seqüenciais das duas rotas sejam iguais, naquela que contiver o menor número de saltos. São utilizados dois tipos de mensagens de atualização, uma menor do que a outra. A menor é utilizada em atualizações incrementais para que não seja necessária a transmissão de toda a tabela de roteamento quando houver alguma mudança de topologia na rede.

No protocolo CSGR, o roteamento ocorre através de nós *cluster heads* e *gateways*. É utilizada uma tabela de *cluster head* e uma tabela de roteamento. O tamanho da tabela de roteamento do CSGR é menor, pois somente um salto é gravado para todos os nós de um *cluster* (até o *cluster head* local). Portanto, o tamanho do pacote de atualização da tabela de roteamento é menor, tornando-o mais eficiente para redes maiores. Uma das desvantagens consiste na dificuldade em se manter a estrutura de um *cluster*, em ambientes onde os nós se movimentam freqüentemente.

No WRP, cada nó possui quatro tabelas de roteamento, o que aumenta substancialmente a necessidade de memória dos dispositivos móveis. O protocolo utiliza mensagens de reconhecimento (*hello messages*) quando não há transmissão de pacotes para um determinado nó, o que consome uma grande quantidade de largura de banda. Para evitar o problema de criação de *loops* temporários, cada nó é forçado a realizar verificações nas informações do predecessor, que são reportadas por todos os seus vizinhos.

Algumas características qualitativas são utilizadas para comparar os três protocolos listados acima. A primeira delas consiste na utilização de mensagens *hello*, necessárias para informar à rede, após um determinado período de tempo, sobre a existência de um nó quando não ocorrem mudanças de topologia, assegurando com isto a conectividade da rede. O DSDV e o WRP utilizam e transmitem mensagens *hello* periodicamente, enquanto o CSGR não as utiliza. As desvantagens deste tipo de mensagem consistem em uma maior carga de roteamento na rede e consumo de energia nos dispositivos móveis, mesmo quando não ocorrem mudanças de topologia na rede.

Os três protocolos possuem mecanismos que os tornam livre de *loops*. Nos protocolos DSDV e CSGR, o número seqüencial introduzido em cada pacote de atualização é utilizado para distinguir novas rotas das velhas rotas, evitando-se assim a formação de *loops*. No protocolo WRP, além do número seqüencial em cada pacote de atualização, cada nó verifica a consistência das informações relativas aos predecessores, reportados pelos seus vizinhos, evitando-se assim a formação de *loops*.

Nos três protocolos, os pacotes de atualização das informações de roteamento são transmitidos de cada nó para seus vizinhos, viabilizando a atualização dos nós que não se encontram no alcance de transmissão dos nós emissores dos pacotes. No CSGR, além dos vizinhos pertencentes ao *cluster* do nó emissor, os pacotes são transmitidos para seu *cluster head*. As atualizações permitem que as tabelas possuam as informações de roteamento mais recentes, mesmo quando ocorrem mudanças de topologia na rede, porém aumenta a carga de roteamento, de forma mais acentuada quando o número de nós na rede aumentar. No caso do protocolo DSDV, pode ocorrer periodicamente ou quando houver mudança de topologia na rede. No CSGR, a atualização das transmissões ocorre apenas periodicamente. Já no protocolo WRP, a atualização pode ocorrer periodicamente ou quando se detectar uma mudança de conexão com o vizinho. Para esta característica e com um número maior de nós na rede, o protocolo CSGR apresenta melhor desempenho em relação aos protocolos DSDV e WRP, já que as transmissões ocorrem apenas periodicamente, diminuindo a carga de roteamento na rede [27].

Os protocolos DSDV e WRP utilizam o endereçamento plano, enquanto o CSGR utiliza o endereçamento hierárquico. O endereçamento plano, comparado ao hierárquico, possui maior facilidade de uso e menor complexidade, porém existem dúvidas quanto a sua escalabilidade [34], ou seja, quando aumenta o número de nós na rede. Além disso, transmissões freqüentes da tabela de roteamento, conforme o número de nós aumenta, degrada a vazão do acesso aos canais e aumenta a carga de roteamento. Neste caso, o esquema de endereçamento hierárquico foi criado, visando a melhoria de desempenho da rede para um número maior de nós.

O número de tabelas de roteamento influencia na necessidade de memória dos dispositivos móveis. Nos protocolos DSDV e CSGR, o número de tabelas é igual a um e dois, respectivamente. Já no WRP, o número de tabelas é igual a quatro, aumentando com isto a quantidade de memória em cada dispositivo móvel.

Os protocolos DSDV e WRP não possuem nós críticos. No CSGR, o *cluster head* é considerado como nó critico pois, quando um nó movimenta-se para fora do alcance de seu *cluster head*, um novo *cluster head* deverá ser selecionado, diminuindo a performance na rede. Com relação a métrica de roteamento, todos os três protocolos citados utilizam o menor caminho, ou seja, o menor número de saltos.

A vazão (*throughput*) é definida como o número de pacotes de dados recebidos com sucesso no destino. Este valor está diretamente relacionado com a carga de roteamento da rede. Para uma quantidade pequena de nós na rede, os protocolos DSDV e WRP possuem maior vazão do que o CSGR, devido a inexistência de nós críticos no DSDV e WRP. Quando a quantidade de nós na rede aumenta, a vazão do DSDV e do WRP é menor do que a do CSGR, já que o DSDV e o WRP, além de transmitir os pacotes de atualização de rotas periodicamente, os transmitem quando ocorrem mudanças de topologia na rede ou quando se detecta mudanças de conexão com os vizinhos. A Tabela 3.2 [35] lista e compara as características citadas acima, para os protocolos DSDV, CSGR e WRP.

Tabela 3.2 - Comparação entre os protocolos pró-ativos.

Parâmetros		**DSDV**	**CSGR**	**WRP**
Utiliza mensagens *hello*?		Sim	Não	Sim
Livre de *loops*?		Sim	Sim	Sim
Atualizações transmitidas para		Vizinhos	Vizinhos e *cluster head*	Vizinhos
Freqüência na atualização das transmissões		Periódica e quando necessário	Periódica	Periódica e quando necessário
Número de tabelas necessárias		Uma	Duas	Quatro
Filosofia de roteamento		Plano	Hierárquico	Plano
Nós críticos?		Não	Sim (*cluster head*)	Não
Métrica de roteamento		Menor caminho	Menor caminho	Menor caminho
Carga de Roteamento	Poucas fontes de tráfego	Baixo	Maior do que o DSDV e WRP	Baixo
	Muitas fontes de tráfego	Maior do que o CSGR	Baixo	Maior do que o CSGR
Vazão (*throughput*)	Poucas fontes de tráfego	Maior do que o CSGR	Baixa	Maior do que o CSGR
	Muitas fontes de tráfego	Baixa	Maior do que o DSDV e WRP	Baixa

3.3.3. Comparação entre os protocolos de roteamento sob-demanda

Uma comparação entre os protocolos AODV e DSR é fornecida na Tabela 3.3. Algumas das características citadas no item 3.3.2 (protocolos pró-ativos) serão utilizadas para comparar os protocolos sob-demanda. Nos dois protocolos, são utilizados procedimentos para a descoberta e manutenção das rotas. O protocolo DSR emprega um procedimento para descoberta da rota com algumas diferenças em relação ao AODV. Uma delas consiste no tamanho do pacote de descobrimento de rota, que no caso do DSR é maior do que no AODV, já que carrega o endereço de todos os nós da rota, enquanto que, no AODV, os nós intermediários não estão contidos no pacote, apenas informações como o endereço da fonte e do destino. Da mesma forma, a resposta de rota no DSR é maior do que no AODV já que contém o endereço de cada nó ao longo da rota. No AODV, a resposta da rota carrega apenas informações como o endereço da fonte e do destino. Com isto, cada nó fonte no protocolo DSR necessita de maior capacidade de armazenamento do que no AODV, pois guarda todos os nós intermediários de uma rota para um destino.

O AODV transmite periodicamente mensagens *hello* de um nó para seus vizinhos, visando assegurar a conectividade local de um nó, bem como detectar falhas de conexão. O DSR não utiliza nenhum tipo de anunciador de roteamento periódico, nem mensagens *hello*, porém utiliza procedimentos que monitoram a operação da rota, além de reconhecimentos do tipo passivo, conforme citado no item 3.2.2.2. A ausência de anunciadores de roteamento periódicos ou de mensagens *hello* no protocolo DSR reduz o consumo de energia dos dispositivos e de largura de banda, principalmente quando não ocorrem mudanças de topologia na rede.

Os dois protocolos possuem mecanismos que os tornam livres de *loops*. No AODV, o mecanismo consiste no uso de números seqüenciais. No caso do DSR, o mecanismo consiste em descartar um determinado pacote de solicitação de rota quando o endereço do nó que está recebendo o pacote já estiver listado na requisição de rota ou quando um pacote de solicitação de rota com mesmo endereço da fonte e *request_id* já foi recebido. O DSR não contém nenhum mecanismo para expirar velhas rotas ou preferir rotas mais novas quando houver várias opções. As rotas antigas, embora habitualmente removidas por pacotes de erro de rotas, podem atingir outros nós, devido a mobilidade dos mesmos na rede. Otimizações no protocolo DSR selecionam pacotes de solicitação de rota com o menor número de saltos. O AODV, por outro lado, possui um mecanismo, baseado em números seqüenciais, que escolhe as rotas mais recentes, ou seja, com números seqüenciais maiores. Caso dois pacotes de solicitação de rota sejam recebidos com números seqüenciais iguais, então aquele com menor número de saltos será utilizado. Ainda, as entradas que não forem utilizadas, depois de um certo tempo, serão removidas da tabela de roteamento.

A filosofia de roteamento nos dois protocolos é a plana, e não existem nós críticos nos dois protocolos. A métrica de roteamento utilizada no DSR é a do menor caminho (menor número de saltos). No AODV, a métrica é a do número seqüencial mais recente (maior número seqüencial) ou, caso o nó receba um pacote de solicitação de rota com número seqüencial igual ao da rota utilizada, utilizará a métrica do menor caminho (menor número de saltos), assegurando com isto informações de roteamento mais rápidas e atualizadas do que no DSR.

O protocolo AODV utiliza apenas conexões bidirecionais para transmitir os pacotes de resposta de rota. No DSR, se o nó destino possuir uma rota até a fonte, ela será utilizada

para enviar o RREP. Caso não possua, a rota reversa será utilizada, necessitando com isto de enlaces bidirecionais. Neste caso, o DSR é superior, já que utiliza inicialmente enlaces unidirecionais. Os enlaces bidirecionais evitam a sobrecarga de um novo descobrimento de rota, porém não funcionam em determinados meios ou protocolos da camada MAC.

O *multicast* [32] é uma técnica que endereça um pacote de dados para um grupo de nós, ao invés de um único nó. Requer menor largura de banda do que em transmissões *unicast* (para uma mesma mensagem) sendo, portanto, adequado para aplicações multimídia. Extensões do AODV possuem suporte para *multicast*, adequando-se ao roteamento de tráfego multimídia. Nenhum dos algoritmos discutidos neste trabalho incorpora comunicação *multicast*.

Devido ao roteamento na fonte, o DSR possui acesso a uma quantidade significativamente maior de informações de roteamento do que o AODV. No DSR, durante um ciclo de solicitação e resposta de rota, o nó fonte e os nós intermediários podem obter acesso as rotas de todos os nós contidos no trajeto e armazená-las em seus *route caches*. Ainda, como o destino responde à fonte a todos os RREQ's recebidos com mesmo *request_id* e endereço da fonte, a fonte possuirá várias rotas alternativas para um mesmo destino, o que será útil caso a rota primária (a mais curta) falhe. Da mesma forma, quando um nó intermediário receber um pacote de dados para transmiti-lo, é possível obter acesso a toda rota que o pacote seguirá. Tendo acesso a rotas alternativas evita que novos procedimentos de descoberta de rotas sejam realizados no DSR. No AODV, o roteamento não é realizado na fonte e, ao receber os pacotes de solicitação de rota, cada nó intermediário obtém acesso apenas ao salto anterior, não obtendo acesso a toda rota. Com isto, a necessidade de realizar novas descobertas de rotas no AODV é maior do que no DSR, o que poderá aumentar a carga de roteamento em redes com o protocolo AODV.

Perkins *et al* [36] comparou os protocolos AODV e DSR utilizando-se quatro métricas: razão de entrega de pacotes (*packet delivery fraction*), que é a razão entre os pacotes de dados entregues no destino com aqueles gerados por fontes CBR (*continuous bit-rate*); atraso fim-a-fim médio (*average end-to-end delay*), que inclui todos os possíveis atrasos causados durante a descoberta de rota nas interfaces (fila FIFO) e em retransmissões na camada MAC; carga de roteamento normalizada *(normalized routing load)*, que é a razão entre o número de pacotes de roteamento transmitidos pelo número de pacotes de

dados entregues no destino e a vazão, que é o número de pacotes de dados recebidos no destino com sucesso. Cada salto de transmissão de um pacote de roteamento foi contabilizado como uma transmissão. As primeiras duas métricas são importantes para avaliar o tráfego na rede. Já a carga de roteamento normalizada e a vazão avaliam a eficiência do protocolo de roteamento.

Para a simulação, Perkins *et al* [36] usou o ns-2 [37], que é um simulador para protocolos de rede. Esse simulador encontra-se em desenvolvimento dentro do projeto *Virtual InterNet Testbed* (VINT), uma colaboração entre o *Lawrence Berkeley National Laboratory* (LBNL), a Universidade da Califórnia em Berkeley, o laboratório Xerox PARC e o *Information Sciences Institute* (ISI) da Universidade da Califórnia do Sul (USC). O ns-2 usa as linguagens C++ e Otcl (*Object Tool Command Language*) sendo que, para permitir melhor desempenho, seu núcleo é implementado em C++. As simulações executadas são configuradas através de *scripts* Otcl que descrevem a topologia, o cenário de mobilidade, os protocolos e as aplicações a serem simuladas.

O ns-2 disponibiliza módulos para simular as camadas física e de enlace do padrão IEEE 802.11. No caso do trabalho de Perkins *et al*, foi utilizado um modelo de rádio similar ao Lucent's WaveLAN [38] e com suporte para as camadas física e MAC. Para a camada MAC, foi utilizado a função de coordenação distribuída (DCF) do padrão IEEE 802.11 para redes LAN sem fio, além de pacotes de controle RTS e CTS para transmissões de dados *unicast*[4] aos nós vizinhos, com o intuito de reduzir o problema dos terminais escondidos. Ambos os protocolos possuem um *buffer* para 64 pacotes de dados que esperam por uma rota, por exemplo, pacotes que esperam por uma resposta de rota. Pacotes são descartados se permanecerem no *buffer* por mais de trinta segundos. Os pacotes de roteamento e de dados, enviados pela camada de roteamento, são dispostos em uma fila FIFO (*First In, First Out*) de tamanho máximo igual a 64, para que a camada MAC os transmita. Para a entrada nesta fila, os pacotes de roteamento possuem prioridade sobre os pacotes de dados.

Foram utilizadas fontes de tráfego CBR (*Continuous Bit-Rate*) e pacotes de dados de 512 bytes de tamanho. O modelo de mobilidade utilizado foi o de *waypoint* aleatório, disponibilizado no pacote do ns-2, em um espaço de tamanho 1500 m x 300 m para 50 nós e 2200 m x 600 m para 100 nós. Os nós fonte e destino foram espalhados aleatoriamente

[4] unicast: técnica que endereça um pacote para um único dispositivo (nó).

pela rede e cada nó partiu de um local aleatório para um destino aleatório com uma velocidade escolhida aleatoriamente entre 0 e 20 m/s. Uma vez alcançado o destino, outro nó destino será escolhido depois de um tempo, chamado tempo de pausa (*pause time)*, que afeta a velocidade relativa dos nós móveis. Quanto menor o tempo de pausa, maior a mobilidade dos nós. Quanto maior o tempo de pausa, menor a mobilidade dos nós. Perkins *et al* utilizou 900 segundos de simulação para 50 nós (exceto para a razão de entrega de pacotes, que foram utilizados 500 segundos), e realizou 4 simulações com 10, 20 e 30 fontes de tráfego a uma taxa de 4 pacotes por segundo e 40 fontes de tráfego a uma taxa de 5 pacotes por segundo. Para 100 nós, foram utilizados 500 segundos de simulação e realizadas 3 simulações com 10 e 20 fontes de tráfego a uma taxa de 4 pacotes por segundo e 40 fontes de tráfego a uma taxa de 2 pacotes por segundo.

A primeira métrica avaliada em foi a da razão de entrega de pacotes. Os resultados obtidos de Perkins *et al* [36] mostraram que, para 50 nós e com 10 e 20 fontes de tráfego, a razão de entrega de pacotes do DSR é praticamente similar ao AODV. Para 30 e 40 fontes de tráfego, o DSR possui menor razão de entrega de pacotes do que o AODV. Com 100 nós e 10 fontes de tráfego, o DSR possui maior razão de entrega de pacotes do que o AODV. Com 20 e 40 fontes de tráfego, o DSR possui menor razão de entrega de pacotes do que o AODV. O motivo do DSR possuir maior razão de entrega de pacotes do que o AODV, quando existem poucas fontes de tráfego e baixa carga oferecida (4 pacotes/s), é devido aos nós, em seus *route caches*, possuírem várias rotas disponíveis para um mesmo destino, minimizando a necessidade de pacotes de descoberta de rotas, ou seja, a utilização das múltiplas rotas existentes em cada *route cache* no DSR torna-se mais eficiente do que os vários mecanismos de descoberta de rota realizados no AODV. Porém, quando o número de fontes de tráfego aumenta, a razão de entrega de pacotes no DSR é menor do que no AODV, pois o uso de rotas antigas das *route cache*, que são pouco eficientes e aumentam o tempo de roteamento e entrega de um pacote de dados no destino, ao invés de rotas mais recentes, provoca atrasos nos pacotes em espera na fila FIFO com a consequente perda de alguns pacotes de dados localizados no *buffer* devido ao tempo de permanência.

Com relação ao atraso fim a fim médio, os resultados obtidos do trabalho de Perkins *et al* [36] mostraram que, para 50 nós e 10 ou 20 fontes de tráfego, o DSR possui menor atraso fim a fim do que o AODV. Para 30 ou 40 fontes de tráfego, o DSR possui maior

atraso fim a fim do que o AODV. Para 100 nós, o DSR possui menor atraso fim a fim para 10 fontes de tráfego e maior atraso fim a fim para 20 e 40 fontes de tráfego. A explicação para os resultados é a seguinte: no AODV, com poucas fontes de tráfego, o atraso ocorre principalmente na fila FIFO, devido a maior necessidade de requisições de rotas (RREQ). Já a disponibilidade de múltiplas rotas no DSR diminui a espera dos pacotes de dados na fila FIFO e faz com que o atraso fim a fim seja menor do que no AODV, com poucas fontes de tráfego. Para uma quantidade maior de fontes de tráfego, a utilização de rotas mais antigas no DSR faz com que o atraso na fila FIFO aumente . Já no AODV, como o nó destino responde ao primeiro RREQ, ou seja, a rota menos congestionada, o atraso fim a fim é menor do que no DSR.

Para a carga de roteamento normalizada, os resultados de Perkins *et al* [36] mostraram que, com poucas ou muitas fontes de tráfego, a carga de roteamento no AODV é sempre maior do que no DSR. O motivo é devido a soma no número de pacotes RREQ e RREP no AODV ser maior do que no DSR, principalmente por causa do maior número de pacotes de descoberta de rotas (RREQ) no AODV. Além disto, o uso periódico de mensagens *hello* favorece o aumento do número de pacotes de roteamento no AODV. O DSR não faz uso de anunciadores de roteamento periódicos, o que reduz o consumo de energia [33].

Perkins *et al* também simulou o efeito da vazão (*throughput*) no DSR e AODV quando se varia a carga na rede. Foi utilizada a mobilidade máxima (tempo de pausa igual a zero), 100 nós e número de fontes de tráfego iguais a 10 e 40. A vazão foi representada pelo autor como a soma das vazões recebidas em cada destino. O resultado obtido da simulação de Perkins *et al* mostra que o DSR possui menor vazão do que o AODV em situações com maior carga oferecida e com poucas ou muitas fontes de tráfego. Este resultado é devido ao DSR utilizar com freqüência rotas mais antigas das *route caches*.

Logo, com os resultados de Perkins *et al* [36], observa-se que o DSR é mais adequado para redes com poucas fontes de tráfego e menor carga e o AODV para redes com muitas fontes de trafego e maior carga. A Tabela 3.3 lista todas as características e parâmetros utilizados para comparar os protocolos AODV e DSR.

Tabela 3.3 - Comparação entre os protocolos sob-demanda.

Parâmetros		**AODV**	**DSR**
Utiliza mensagens *hello*?		Sim	Não
Livre de *loops*?		Sim	Sim
Filosofia de roteamento		Plano	Plano
Nós críticos		Não	Não
Métrica de roteamento		Mais recente ou menor caminho	Menor caminho
Necessita de conexões simétricas?		Sim	Não
Capacidade de *Multicast*?		Sim	Não
Possibilidade de múltiplas rotas?		Não	Sim
Rotas mantidas em		Tabela de rotas (nós intermediários)	*Route cache* (nós fonte)
Razão de entrega de pacotes	Poucas fontes de tráfego	Baixa	Alta
	Muitas fontes de tráfego	Alta	Baixa
Atraso fim a fim	Poucas fontes de tráfego	Alta	Baixa
	Muitas fontes de tráfego	Baixa	Alta
Carga de roteamento normalizada	Poucas fontes de tráfego	Alta	Baixa
	Muitas fontes de tráfego	Alta	Baixa
Vazão (*throughput*)	Poucas fontes de tráfego e carga alta	Alta	Baixa
	Muitas fontes de tráfego e carga alta	Alta	Baixa

Capítulo 4

Conclusões e Trabalhos Futuros

Com o crescente desenvolvimento, nos últimos anos, dos dispositivos móveis sem fio, as redes ad hoc vem recebendo especial atenção pelos pesquisadores. Tais redes não possuem qualquer tipo de infraestrutura que forneça suporte à mobilidade, o que provoca um aumento na complexidade de seus nós, tornando mais difícil o roteamento dos dados pela rede e consequentemente a transmissão de tráfego em tempo real. Uma variedade de protocolos de roteamento foram propostos para as redes sem fio ad hoc, visando solucionar ou minimizar os problemas citados acima, bem como aumentar a performance da rede.

Este trabalho descreveu e comparou cinco protocolos distribuídos nas duas classes de protocolos de roteamento das redes ad hoc: pró-ativa e sob-demanda. Os protocolos pró-ativos mantém rotas constantemente atualizadas e disponíveis para todos os destinos, mesmo que não sejam necessárias, enquanto que nos protocolos sob-demanda, uma rota é descoberta somente quando um nó desejar, o que conserva largura de banda e energia nos dispositivos móveis.

Com relação aos protocolos pró-ativos, o DSDV mantém apenas uma tabela de roteamento, enquanto o CSGR mantém duas. O WRP possui quatro tabelas de roteamento, o que aumenta a necessidade de memória nos dispositivos móveis. Nos protocolos DSDV e WRP, os pacotes de atualização de rotas em um nó são transmitidos para seus vizinhos e podem ser transmitidos periodicamente, quando houver mudança de topologia na rede ou se forem detectadas mudanças de conexão com os seus vizinhos. No CSGR, os pacotes de atualização são transmitidos apenas periodicamente, reduzindo a carga de roteamento na rede em relação ao DSR e WRP, quando o número de nós na rede é grande. A transmissão no CSGR ocorre do nó emissor aos seus vizinhos dentro do *cluster* e para seu *cluster head.* A inexistência de mensagens *hello* no CSGR também faz com que a carga de roteamento seja menor do que no DSDV e WRP, para uma quantidade grande de nós.

O DSDV e o WRP utilizam o endereçamento plano, pois são menos complexos e fáceis de usar. No CSGR, é utilizado o endereçamento hierárquico, visando a melhoria do desempenho da rede em relação ao endereçamento plano, para um número grande de nós. Quando o número de nós na rede é pequeno, a carga de roteamento no CSGR é maior, pois quando um nó movimenta-se para fora do alcance de seu *cluster*, um novo *cluster head* (nó crítico) deverá ser selecionado.

Os protocolos sob-demanda descritos neste trabalho foram o AODV e o DSR. O DSR utiliza o roteamento na fonte, *route caches*, não depende de nenhuma atividade periódica, utiliza mecanismos para evitar *loops* e mantém múltiplas rotas por destino. O AODV, por outro lado, utiliza tabelas de roteamento em cada nó intermediário, uma rota por destino, números seqüenciais, mecanismos para evitar loops e para determinar rotas mais recentes. Em [36], foram utilizados parâmetros como a razão de entrega de pacotes (*packet delivery fraction*), atraso fim a fim médio (*average end-to-end delay)*, carga de roteamento normalizada e a vazão (*throughput*) para comparar quantitativamente os protocolos DSR e AODV. Dos resultados obtidos em Perkins *et al* [36], observou-se que o DSR possui maior razão de entrega de pacotes, menor atraso fim a fim e menor carga de roteamento normalizada do que o AODV, para uma quantidade pequena de nós. Para uma quantidade maior de nós, o DSR possui menor razão de entrega de pacotes, maior atraso fim a fim e menor carga de roteamento normalizada do que o AODV. Para uma rede com cargas maiores, a vazão no AODV é sempre maior do que no DSR, para uma rede com muitas ou poucas fontes de tráfego. Logo, concluiu-se que o DSR possui melhor performance para uma rede com poucas fontes de tráfego nós e menor carga na rede e o AODV possui melhor desempenho para uma rede com uma quantidade maior de fontes de tráfego e maior carga na rede. A diferença é acentuada quando a mobilidade dos nós é maior (menor tempo de pausa). Portanto, fatores como a mobilidade e topologia de rede dinâmica devem ser considerados no desenvolvimento de protocolos de roteamento para redes ad hoc.

Como sugestão para trabalhos futuros, recomenda-se:

a) um estudo comparativo envolvendo outros protocolos de roteamento sob demanda como por exemplo o *TORA (Temporally Ordered Routing Algorithm)*, ABR (*Associativity-Based Routing*) ou SSR (*Signal Stability Routing*);
b) desenvolvimento e avaliação de mecanismos no DSR para eliminar rotas mais antigas, visando o aumento de seu desempenho quando o número de fontes de tráfego na rede for grande.
c) criação de um protocolo sob-demanda que reuna as propriedades e o desempenho do DSR quando o número de fontes de tráfego e carga na rede for pequeno e do AODV quando o número de fontes de tráfego e carga na rede aumentar. Este tipo de protocolo seria adequado em redes com relativa freqüência na variação do número de fontes de trafego, como no caso de veículos com dispositivos móveis em uma estrada, onde variações no trânsito podem ocorrer com freqüência.
d) Avaliar os protocolos pró-ativos para transmissões em tempo real (voz e vídeo) e compará-los com os protocolos sob-demanda, já que manter todas as informações de roteamento disponíveis é mais adequado para transmissões em tempo real, porém o consumo maior de energia e de largura de banda nos protocolos pró-ativos podem influenciar no desempenho das transmissões.

Glossário

16-QAM: *16-Level Quadrature Amplitude Modulation.* Técnica de modulação de 16 níveis, com mudança de amplitude e fase do sinal. Utilizado no padrão IEEE 802.11a.

64-QAM: *64-Level Quadrature Amplitude Modulation.* Técnica de modulação de 64 níveis, com mudança de amplitude e fase do sinal. Utilizado no padrão IEEE 802.11a.

ABR: *Associativity Based Routing.* Protocolo de roteamento para redes ad hoc da classe sob-demanda.

ACK: *Acknowledge.* Sinal de reconhecimento de *status* usado em comunicação de dados.

AODV: *Ad Hoc On-Demand Distance Vector Routing.* Protocolo de roteamento para redes ad hoc da classe sob-demanda.

AP: *Acess Point.* Ponto de Acesso. Estação responsável pela captura das transmissões realizadas pelas estações de sua BSA, destinadas a estações localizadas em outras BSA's.

BPSK: *Binary Phase Shift Keying.* Tipo de modulação onde é utilizado o deslocamento de fase de 0° ou 180° para cada bit.

BSA: *Basic Service Area.* Célula de uma rede LAN 802.11.

CBR: *Continuous Bit-Rate.* Tráfego contínuo com taxa constante.

CCK: *Complementary Code Keying.* Código que utiliza símbolos de 8 bits.

CFP: *Contention Free Period.* Período Livre de Disputa da camada MAC do padrão IEEE 802.11.

Cluster Head: tipo de nó do protocolo CSGR, que roteia as informações entre os nós de um cluster (grupo).

CP: Coordenador de Ponto, utilizado na Função de Coordenação Pontual (PCF).

CSGR: *Cluster Switch Gateway Routing.* Protocolo de roteamento para redes ad hoc da classe pró-ativa.

CSMA/CA: *Carrier Sense Multiple Access with Collision Avoidance.* Método de acesso utilizado para evitar colisões.

CSMA/CD: *Carrier Sense Multiple Access with Collision Detection.* Método de acesso com detecção de colisão.

CW: *Contention Window.* Janela de Disputa, utilizado na Função de Coordenação Distribuída (DCF) da camada MAC do padrão IEEE 802.11.

DARPA: *Defense Advanced Research Projects Agency.* Organização central de pesquisa e desenvolvimento do Departamento de Defesa dos Estados Unidos.

DCF: *Distributed Coordination Function.* Função de Coordenação Distribuída da camada MAC do padrão IEEE 802.11.

DIFS: *Distributed InterFrame Space.* Espaço distribuído entre quadros no DCF. Período que indica se o meio está livre ou não para a transmissão de dados.

DSDV: *Destination Sequenced Distance Vector.* Protocolo de roteamento para redes ad hoc da classe pró-ativa.

DSR: *Dynamic Source Routing.* Protocolo de roteamento para redes ad hoc da classe sob-demanda.

DSSS: *Direct Sequence Spread Spectrum.* Técnica de espalhamento de espectro por seqüência direta utilizada no padrão IEEE 802.11.

ESA: *Extended Service Area.* Conjunto de BSA's interligados por um sistema de distribuição através de pontos de acesso.

ESS: *Extended Service Set.* Conjunto de estações formado pela união dos vários BSS's e conectados por um sistema de distribuição.

FEC: *Forward Error Correction.* Mecanismo contra a perda de dados.

FDM: *Frequency Division Multiplexing.* Multiplexação por divisão de freqüência.

FHSS: *Frequency-Hopping Spread Spectrum.* Técnica de espalhamento de espectro por salto de freqüência, utilizado no padrão IEEE 802.11.

FIFO: *First In, First Out.* Primeiro que entra na fila é o primeiro que sai da fila.

Gateway: tipo de nó, do protocolo CSGR, que é a ligação entre dois clusters (grupos).

GFSK: *Gaussian Frequence Shift Keying.* Método de modulação de freqüência que utiliza filtro Gaussiano.

GSM: *Global System for Mobile Communications.* Sistema móvel de segunda geração.

IBSS: *Independent Basic Service Set.* Rede ad hoc com o padrão IEEE 802.11.

IEEE: *Institute of Electrical and Electronic Engineers.* Instituto responsável pelo padrão IEEE 802.11.

ISI: *Inter-Symbol Interference.* Interferência entre símbolos.

ISM: *Industrial, Scientific and Medical.*

ISO: *International Standards for Organization.* Organização que cria padrões internacionais para diversas áreas.

LCC: *Least Cluster Change.* Algoritmo de mínima mudança de cluster head do protocolo CSGR.

MAC: *Medium Access Control.* Controle de acesso ao meio.

MANET: *Mobile Ad Hoc Network.* Grupo relativo às redes ad hoc.

Mensagens Hello: Mensagens de reconhecimento do tipo ativo.

MRL: *Message Retransmission List Table.* Tabela de mensagens para transmissão do protocolo WRP.

Multicast: Técnica que endereça pacotes para um grupo de nós.

NAV: *Network Allocation Vector.* Vetor de alocação de rede, utilizado para detecção virtual de uma portadora no padrão IEEE 802.11.

NS2: *Network Simulator.* Simulador para pesquisa em redes.

OFDM: *Orthogonal Frequency Division Multiplexing.* Multiplexação por divisão ortogonal de freqüência. Técnica de transmissão por múltiplas portadoras, utilizada nos padrões IEEE 802.11a e IEEE 802.11g.

OSPF: *Open Shortest Path First.* Protocolo de roteamento baseado em estado de enlace.

PBCC: *Packet Binary Convolutional Code.* Código utilizado no padrão IEEE 802.11g, para atingir taxa máxima de transmissão de 33 Mbps.

PCF: *Point Coordination Function.* Função de coordenação pontual. Tipo de acesso da camada MAC do padrão IEEE 802.11.

PIFS: *PCF InterFrame Space.* Espaço entre os pacotes de dados do coordenador de ponto, na Função de Coordenação Pontual do padrão IEEE 802.11.

PLCP: *Physical Layer Convergence Protocol.* Parte da camada física do padrão IEEE 802.11, que define métodos para mapear o meio físico no formato de quadros.

PMD: *Physical Medium Dependent.* Parte da camada física do padrão IEEE 802.11, que define as características e os métodos para o envio e recepção de dados entre duas ou mais estações.

QoS: *Quality of Service.* Qualidade de Serviço.

QPSK: *Quadrature Phase Shift Keying.* Tipo de modulação onde são utilizados quatro deslocamentos de fase (0°, 90°, 180° ou 270°).

RIP: *Routing Information Protocol.* Protocolo de roteamento baseado em vetor de distância.

RREP: *Route Reply Packet.* Pacote de resposta de rota dos protocolos AODV e DSR.

RREQ: *Route Request Packet.* Pacote de solicitação de rota dos protocolos AODV e DSR.

RRER: *Route Error Packet.* Pacote de erro de rota do protocolo DSR.

RTS/CTS: *Request To Send / Clear To Send.* Mecanismo no qual uma estação, para reservar o canal, envia um pacote RTS à estação receptora, que responderá com um pacote CTS se o meio estiver livre. Visa eliminar o problema do terminal escondido, que pode ocorrer em redes com o padrão IEEE 802.11.

SIFS: *Short InterFrame Space.* Pequeno espaço entre o pacote de dados e o ACK. Utilizado no DCF do padrão IEEE 802.11.

SSID: *Service Set Identifier.* Nome de rede que identifica uma área coberta por um ou mais pontos de acesso.

SSR: *Signal Stability Routing.* Protocolo de roteamento para redes ad hoc da classe sob-demanda.

TORA: *Temporally Ordered Routing Algorithm.* Protocolo de roteamento para redes ad hoc da classe sob-demanda.

UMTS: *Universal Mobile Telecomunications System.* Sistema móvel de terceira geração.

U-NII: *Unlicensed National Information Infrastructure.*

VCO: *Voltage-Controlled Oscilator.* Oscilador controlado por tensão.

WEP: *Wired Equivalent Privacy*. Padrão de criptografia utilizado em redes LAN.

WLAN: *Wireless Local Area Network*. Rede sem fio local.

WRP: *Wireless Routing Protocol*. Protocolo de roteamento para redes ad hoc da classe pró-ativa.

Referências Bibliográficas

[1] CESAR, R. Novo Padrão Movimenta o Mercado. ComputerWorld, São Paulo, ano 9, n. 390, p. 18-18, jul. 2003.

[2] TOH, C. –K. Ad Hoc Mobile Wireless Networks: Protocols and Systems. Upper Saddle River: Prentice Hall PTR, 2002, 302p. ISBN 0-13-007817-4.

[3] OBRACZKA, K., TSUDIK, G. Multicast Routing Issues in Ad Hoc Networks. USC Information Science Institute, Marina del Rey, Out. 1998. Disponível em: <http://www.ics.uci.edu/~atm/adhoc/paper-collection/obraczka-multicast-issues.pdf>. Acesso em: 12 mar. 2003.

[4] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Computer Society, Los Alamitos, 1999. Disponível em: <http:// standards.ieee.org / getieee802 / download / 802.11-1999.pdf>. Acesso em: 17 dez. 2002.

[5] BRENNER, P. A Technical Tutorial on the IEEE 802.11 Protocol. Breezecom Wireless Communications, Jul. 1996. Disponível em: <http:// www.sss-mag.com / pdf / 802_11tut.pdf>. Acesso em: 12 mar. 2003.

[6] MAXIM INTEGRATED PRODUCS. An Introduction to Spread-Spectrum Communications. Sunnyvale, Fev. 2003. Disponível em: <http:// www.maxim-ic.com / tarticle / view_article.cfm / article_id / 1890>. Acesso em: 12 mar. 2003.

[7] INTEL INC. 802.11a Scalable 5 GHz Wireless Lan. Santa Clara, 2001. Disponível em: <http:// www.intel.com / network / connectivity / resources / doc_library / white_papers / NP2040_11.01.pdf>. Acesso em: 12 mar. 2003.

[8] VAUGHAN-NICHOLS, S. J. OFDM: Back to the Wireless Future. Revista Computer, v. 35, n. 12, p. 19-21, dez. 2002.

[9] WI-LAN INC. Wide-band Orthogonal Frequency Multiplexing (WOFDM). Calgary, Set. 2000. Disponível em: <http:// www.wi-lan.com / library / whitepaper_wofdm_technical.pdf>. Acesso em: 12 mar. 2003.

[10] PROXIM CORPORATION. 802.11a: A Very-High-Speed, Highly Scalable Wireless LAN Standard. Sunnyvale, 2002. Disponível em: <http:// www.proxim.com / learn / library / whitepapers / 80211a.pdf>. Acesso em 12 mar. 2003.

[11] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High-speed Physical Layer in the 5 GHz Band. IEEE Computer Society, Los Alamitos, 1999. Disponível em: <http:// standards.ieee.org / getieee802 / download / 802.11a-1999.pdf>. Acesso em: 17 dez. 2002.

[12] CONNOVER, J. 802.11a: Making Space for Speed. Network Computing, Skokie, Jan. 2001. Disponível em: <http:// www.networkcomputing.com / 1201 / 1201ws1.html>. Acesso em 12 mar. 2003.

[13] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band. IEEE Computer Society, Los Alamitos, 1999. Disponível em: <http:// standards.ieee.org / getieee802 / download / 802.11b-1999.pdf>. Acesso em: 17 dez. 2002.

[14] SARINNAPAKORN, K. IEEE 802.11b "High Rate" Wireless Local Area Network. Fairleigh Dickinson University, Teaneck, Mar. 2001. Disponível em: <http:// alpha.fdu.edu / ~kanaksri / IEEE80211b.html>. Acesso em: 12 mar. 2003.

[15] ANDREN, C. E WEBSTER, M. CCK Modulation Delivers 11 Mbps for High Rate IEEE 802.11 Extension. Intersil Corporation, Milpitas, 1998. Disponível em: <http:// www.intersil.com / prism / papers / CCK_Mod_Delivers_11Mbps.htm>. Acesso em: 17 dez. 2002.

[16] ZYREN, J., ENDERS, E., EDMONDSON, T. IEEE 802.11g Offers Higher Data Rates and Longer Range. Intersil Corporation, Milpitas, Dez. 2002. Disponível em: <http:// www.intersil.com / data / wp / WP0555.pdf>. Acesso em: 12 mar. 2003.

[17] ZYREN, J. IEEE 802.11g Explained. Intersil Corporation, Milpitas, Dez. 2001. Disponível em: <http:// www.intersil.com / design / prism / WP_IEEE802gExpla_12_06.pdf>. Acesso em: 12 mar. 2003.

[18] KING, J. S. An IEEE 802.11 Wireless LAN Security White Paper. US Department of Energy, Livermore, Out. 2001. Disponível em: <http:// www.llnl.gov / asci / discom / ucrl-id-147478.pdf>. Acesso em: 12 mar. 2003.

[19] CARNEY, W. IEEE 802.11g New Draft Standard Clarifies Future of Wireless LAN. Texas Instruments, Dallas, Jan. 2002. Disponível em: <http:// focus.ti.com / pdfs / vf / bband / 802_11g_whitepaper.pdf>. Acesso em: 12 mar. 2003.

[20] INTEL INC. 54 Mbps IEEE 802.11 Wireless LAN at 2.4 GHz. Deploying standards-based Wireless LAN solutions. Santa Clara, Nov. 2002. Disponível em: <http:// www.networld.pl / whitepapers / pdf/802_11g.pdf>. Acesso em: 12 mar. 2003.

[21] WENTINK, M., GODFREY, T., ZYREN, J. Overcoming IEEE 802.11g's Interoperability Hurdles. Communication System Design Magazine, v. 9, n. 5, p. 19-23, maio 2003.

[22] MALKIN, G. RFC 2453 RIP Version 2. Internet FAQS Archives, 1998, Disponível em: < http:// www.faqs.org/rfcs/rfc2453.html>. Acesso em: 12 mar. 2003.

[23] MOY, J. RFC 2328 OSPF Version 2. Internet FAQS Archives, 1998, Disponível em: <http:// www.faqs.org/rfcs/rfc2328.html>. Acesso em: 12 mar. 2003.

[24] HAAS, Z. J., HAAS, S. T. On Some Challenges and Design Choices in Ad Hoc Communications. In: IEEE MILCOM, 1998, Belford. *Proceedings...* New York: IEEE Communications Society, 1998.

[25] TANENBAUM, A. S. Computer Networks. 3.ed. Upper Saddle River: Prentice Hall, 1996, 813p. ISBN 0-13-349945-6.

[26] CORSON, S., MACKER, J. Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations. RFC 2501. Jan. 1999. Disponível em: <http:// www.faqs.org / rfc2501.html>. Acesso em 12 mar. 2003.

[27] MOGHIM, N., HENDESSI, F., MOVEHHEDIMA, N., GULLIVER, T. A. Comparing Ad-Hoc Wireless Network Routing Protocols and Proposing and Extension to AODV. University of Victoria, Victoria. Disponível em <http:// www.ece.uvic.ca / ~agullive / Aodv.doc>. Acesso em 15 dez. 2002.

[28] FORD JR, L. R., FULKERSON, D. R. Flows in Network. Princeton: Princeton University Press, 1962, 198p.

[29] BHAGWAT, C. P. P. Highly Dynamic Destination-Sequenced Distance Vector Routing (DSDV) for Mobile Computers. In: ACM SIGCOMM 94, 1994, Londres. *Proceedings...* New York: ACM Press, set. 1994, v.1, p. 234-244.

[30] MURTHY, S., GARCIA-LUNA-ACEVES, J.J. A Routing Protocol for Packet Radio Networks. In: ACM First International Conference on Mobile Computing & Networking (MOBICOM'95), 1995, Berkeley. *Proceedings...* New York: ACM Press, nov. 1995, v. 1, p. 86-95.

[31] CHIANG, C. –C., WU, H. –K., LIU, W., GERLA, M. Routing in Clustered Multihop Mobile Wireless Networks with Fading Channel. University of California, Los Angeles. Disponível em: <http://www.cs.ucla.edu / NRL / wireless / PAPER / Chiang_sicon97.ps.gz>. Acesso em 12 mar. 2003.

[32] PERKINS, C., ROYER, E. Ad Hoc On-Demand Distance Vector Routing. In: 2nd IEEE Workshop on Mobile Computing Systems and Applications, 1999, New Orleans. Proceedings... Los Alamitos: IEEE Computer Society, fev. 1999.

[33] JOHNSON, D. B., MALTZ, D. A. Dynamic Source Routing in Ad Hoc Wireless Networks. New York: Kluwer Academic Publishers, 1996, Cap. 5, p. 153-181.

[34] BAKER et al, Flat vs. Hierarchical Network Control Architecture, ARO/DARPA Workshop on Mobile Ad-Hoc Networking. University of Maryland, Maryland, Mar. 1997. Disponível em: <http://www.isr.umd.edu / Courses / Workshops / MANET / program.html>. Acesso em 12 mar. 2003.

[35] ROYER, E. M., TOH, C. –K. A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks. IEEE Personal Communications Magazine, New York, v. 6, n. 2, p. 46-55, abr. 1999.

[36] PERKINS, C. E., DAS, S. R., ROYER, E. M. Performance Comparison of Two On-demand Routing Protocols for Ad Hoc Networks. IEEE Personal Communications Magazine, New York, v. 8, n. 1, p. 16-29, fev. 2001.

[37] FALL, K., VARADHAN, K. ns notes and documentation. University of Southern California, Marina del Rey, 1999. Disponível em: <http://www.isi.edu/nsnam/ns/ns-documentation.html>. Acesso em 12 mar. 2003.

[38] TUCH, B. Development of WaveLAN, an ISM band wireless LAN. AT&T Technical Journal, v. 72, n. 4, p. 27-33, Jul./Ago. 1993.