UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE INFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM COMPUTAÇÃO

LUIS ANTÔNIO SCHNEIDERS

Uma Proposta de Otimização no Processo de Integração Entre Redes Infra-Estruturadas e MANET´s

Dissertação apresentada como requisito parcial para a obtenção do grau de Mestre em Ciência da Computação

Prof. Dr. Juergen Rochol
Orientador

Porto Alegre, junho de 2006.

CIP – CATALOGAÇÃO NA PUBLICAÇÃO

Schneiders, Luis Antônio

Uma Proposta de Otimização no Processo de Entre Redes Infra-Estruturadas (IP) e MANET´s (AODV) / Luis Antônio Schneiders – Porto Alegre: Programa de Pós-Graduação em Computação, 2006.

83 f.:il.

Dissertação (mestrado) – Universidade Federal do Rio Grande do Sul. Programa de Pós-Graduação em Computação. Porto Alegre, BR – RS, 2006. Orientador: Juergen Rochol.

1.Redes de Computadores. 2.Redes Móveis Ad Hoc 3.Protocolos de Roteamento. I. Rochol, Juergen Orientador. II. Título.

A Deus por orientar meus pensamentos, a minha esposa pela paciência, amor e confiança, a meus pais, minha família e amigos, pela compreensão e tolerância a mim concedidos, elementos fundamentais para a realização do presente trabalho.

AGRADECIMENTOS

A minha esposa pelo companheirismo, doação, paciência, amor e confiança em mim depositados.

A toda minha família, e em especial aos meus pais, pelo apoio, pela doação e por acreditarem no meu potencial.

Aos meus irmãos pela alegria e compreensão nos momentos mais difíceis.

Ao meu tio Paulo pela sua ajuda desprendida e imprecindível em momentos decisivos na minha formação acadêmica.

A minha amiga e sogra Carmenzita que por muitas vezes com palavras e orações fortaleu a minha determinação e a minha fé.

Ao professor Juergen, pela singular paciência, por sua compreensão e o apoio na luta pelo objetivo final em todos os momentos.

Ao meu amigo Oscar, por ter sido uma mão amiga em momentos difíceis.

E a todos que de uma forma ou outra contribuíram para a realização deste trabalho.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SÍMBOLOS E SIGLAS

ω	Pacotes esperando na fila
μ	Eventos atendidos por unidade de tempo
λ	Taxa de chegada de pacotes
t	Tempo de espera na fila
q	Total de eventos no sistema
s	Tempo de transmissão de um pacote
n	Número médio de bits por pacote
p	Fator de utilização (processador)
C	Capacidade do *link* de saída

ABR	Associativity-Based Routing
AC	Access Categories
AES	Advanced Encryption Standard
AIFS	Arbitration Interface Space
ANATEL	Agência Nacional de Telecomunicação
AODV	Ad Hoc On-Demand Distance Vector Routing
AP	Access Point
BAR	Block-Acknowledgement Request
BPSK	BiPhase Shift Keying
BSS	Basic Service Set
CBR	Constant bit rate
CCA	Clear Channel Assessment Signal
CCC	Central de Comutação e Controle
CCK	Complementary Code Keying
CDMA	Code Division Multiple Access
CFP	Contention Free Period
CP	Contention Period

CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear to Send
CW	Contention Window
DARPA	Defense Advanced Research Projects Agency
DBPSK	Differential Binary Phase Shift Keying
DCF	Função de Coordenação Distribuída
DFWMAC	Distribution Foundation Wireless Medium Access Control
DIFS	Distributed InterFrame Space
DQPSK	Differential Quadrature Phase Shift Keying
DS	Distribution System
DSDV	Destination-Sequenced Distance-Vector
DSP	Digital Signal Processing
DSR	Dynamic Source Routing Protocol
DSSS	Direct Sequence Spread Sprectum
EDCF	Enhanced DCF
ERP	Enhanced Rate PLCP
ESS	Extended Service Set
FEC	Forward Error Correction
FHSS	Frequence Hopping Spread Sprectum
GPS	Global Positioning System
GSM	Global System for Mobile Communications
GSR	Global State Routing
HC	Hybrid Coordinator
HCF	Hibrid Coordination Function
HDLC	High Data *Link* Control
HT SG	High Throughput Study Group
IAPP	Inter-Access Point Protocol
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Enginereering Task Force
IFS	InterFrame Space
IP	Internet Protocol
IR	Infra-Red
ISM	Industrial, Scientific and Medical
ISO	International Standards Organization
LAR	Location-Aided Routing

LLC	*Link* Layer Control
LMR	Lightweight Mobile Routing protocol
LPDU	LLC Protocol Data Unit
MAC	Medium Access Control
MACA	Medium Access with Collision Avoidance
MACAW	MACA for Wireless
MANET	Mobile Ad Hoc Networks
MAODV	AODV Multicasting
MH	Mobile Host
MIB	Management Information Base
MIC	Message Integrity Check
MIMO	Multiple-Input Multiple-Output
MONARCH	Mobile Network Architecture
MPDU	MAC PDU
MSDU	MAC Service Data Units
MTU	Maximum Transfer Unit
NAV	Network Allocation Vector
NS	Network Simulator
OFDM	Orthogonal Frequency Division Multiplexing
OLSR	Optimized *Link* State Routing Protocol
ODMRP	On-Demand Multicast Routing Protocol
PBCC	Packet Binary Convolutional Code
PCF	Função de Coordenação Pontual
PCN	Personal Communication Network
PCS	Personal Communication Systems
PDA	Personal Digital Assistants
PDU	Protocol Data Unit
PHY	Physical Layer Specifications
PIFS	Point Coordination InterFrame Space
PLCP	Physical Level Convergence Protocol
PMD	Physical Medium Dependent
PPDU	PHY PDU
PRNET	Rede de Pacotes via Rádio
QoS	Qualidade de Serviço
QPSK	Quadrature Phase Shift Keying

RADIUS	Remote Authentication Dial-In User Service
RF	Rádio Freqüência
RFC	Request For Comment
RM-OSI	Interconnection of the International Standardization Organization
RREP	Route Reply
RREQ	Route Request
RTS	Request to Send
SAP	Service Access Point
SIFS	Short InterFrame Space
STA	Estação (Station)
TC	Traffic Classes
TCP/IP	Tranfer Control Protocol/Internet Protocol
TG	Task Group
TORA	Temporally – Ordered Routing Algorithm
TPC	Transmission Power Control
TTL	Time To Live
TXOP	Transmit Opportunity
TKPI	Temporal Key Protocol Integrity
TORA	Temporally-Ordered Routing Algorithm
UHF	Ultra Hight Frequency
UMTS	Universal Mobile Telecommunications System
WEP	Wired Equivalent Privacy
WI-FI	Wireless Fidelity
WIMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WPA	Wi-Fi Protected Access
WRP	Wireless Routing Protocol
WWAN	Wireless Wireless Area Network
ZRP	Zone Routing Protocol
QAM	Quadrature Amplitude Modulation
3G	Terceira Geração de Telefonia Celular

RESUMO

Uma **Rede Móvel *Ad Hoc*** (MANET) consiste em uma coleção de terminais que possuem uma interface de transmissão e recepção sem fio (*wireless*) e que se movimentam em uma determinada área de abrangência. Geralmente esses terminais fazem uso de freqüências de rádio nas comunicações e configuram uma rede não infra-estruturada. As MANETs, também conhecidas como independentes, não necessitam de qualquer infra-estrutura pré-existente para prover comunicação entre os nós, contudo, são utilizadas, principalmente quando integradas à Internet. Essa integração, apesar de possível, normalmente necessita de um *gateway* que encaminhe os pacotes entre as **redes de computadores**, respeitando as suas características individuais. Problemas, assim como atrasos e perdas de pacotes, podem ser provocados pelas diferenças intríncias aos protocolos de roteamento.

Embora o Internet Engineering Task Force (IETF) proponha diversos protocolos de roteamento para as MANETs, o presente trabalho investiga o **protocolo de roteamento** *Ad hoc On-Demand Distance Vector* (AODV), por ser considerado um dos protocolos mais implementados e estudados pelo grupo de trabalho do IETF. O nodo *gateway*, embora já esteja implementado no **protocolo de roteamento** AODV (HAMIDIAN, 2003), deve ser capaz de interagir com as funções de roteamento da Internet, trocando tráfego com a mesma, de modo transparente e eficiente. O protocolo AODV, por ser reativo, pode demorar até 0,05 segundos para estabelecer uma rota entre um nodo origem e um nodo destino. Nos padrões atuais esse tempo pode ser considerado exageradamente alto, gerando gargalos entre sub-redes, descarte de pacotes e baixa eficiência.

O presente trabalho apresenta uma proposta de customização do protocolo de roteamento AODV com atuação restrita ao nodo gateway. Esta customização consiste na adição de uma métrica de **confiabilidade** no processo de descoberta e utilização de rotas visando a redução no número de pacotes descartados e um ganho de eficiência no fluxo de dados entre as sub-redes envolvidas.

Palavras Chave: Redes Móveis Ad Hoc, redes de computadores, protocolos de roteamento e confiabilidade.

A Optimization Proposal on Integration Process Between Infraestructured Networks and MANETs

ABSTRACT

A **Mobile Ad Hoc Network** (MANET) consists of a collection of mobile hosts, moving in certain range area, that has a wireless interface for transmission and receiving data. Usually these terminals make use of radio frequencies in communications and configure a non infrastructured network. The MANETs, also known as independent, require no pre-existing infrastructure to provide communication between network mobile nodes, however, are used, preferably when integrated with the Internet. This integration, although possible, usually need a gateway that forwards packets between both **computer networks**, keeping their individual characteristics. Problems such as delays and packet losses can be caused by differences inherent in the routing protocols.

Although the Internet Engineering Task Force (IETF) proposes several routing protocols for MANETs, this paper investigates the Ad hoc On-Demand Distance Vector (AODV) **routing protocol**, viewed as one of more implemented and studied protocol by the IETF work group. The gateway node, which is already implemented in the AODV routing protocol (Hamidian, 2003), should be able to interact, transparently and efficiently, with the Internet routing functions exchanging traffic between them. The AODV protocol, being reactive, can take up to 0.05 seconds to establish a route between a source node and a destination node. By today's standards this time may be considered excessively high, creating bottlenecks between subnets, packet drop and low efficiency.

This paper proposes an AODV routing protocol customization restricted to the gateway node activities. This customization consists of adding **reliability** metric in the route discovery process and its consequent use in order to reduce the number of dropped packets and get increased efficiency in the data flow between the subnets involved.

Keywords: Mobile Ad Hoc Network, computer networks, routing protocol and reliability.

1 INTRODUÇÃO

A indústria da comunicação móvel vem se desenvolvendo em ritmo extraordinário nos últimos 10 anos. Não apenas na telefonia móvel, mas em tecnologias com suporte à mobilidade como um todo. O avanço tecnológico dos circuitos digitais e de rádio-freqüência (RF), dos circuitos integrados mais modernos, da miniaturização dos dispositivos e das interfaces mais inteligentes vem tornando os equipamentos móveis (celulares, PDAs etc.) menores, mais confiáveis e mais baratos. Técnicas modernas de comunicação digital vêm fomentando o desenvolvimento em larga escala de redes de comunicação sem fios. Essa tendência deve continuar a crescer durante os próximos anos. Tomando como base a Lei de Cooper, formulada por Martin Cooper, é possível afirmar que o número de transmissões que conseguimos enviar pelo ar, dobra a cada 30 meses. Ainda segundo Cooper, a capacidade humana de enviar dados e voz pelo ar já aumentou 1 trilhão de vezes e deve continuar aumentando por, pelo menos, mais 60 anos, apenas com as tecnologias já conhecidas.

Com o expressivo crescimento de uso dos Sistemas Celulares assim como dos Serviços de Comunicação Pessoal (PCS) associados a eles, através do mundo, cada vez mais se percebe a necessidade de se fazer frente à competitividade e de se manter sintonizado com os cenários futuros. As tecnologias da Internet móvel, os impactos da mobilidade nos processos e novos serviços devem ser considerados em tais cenários. Nos últimos anos duas tecnologias, a internet e as comunicações com suporte a mobilidade, vêm se posicionando como um novo paradigma: a Internet Móvel (ANDERSON, 1999). A Internet Móvel combina a inegável convergência para a Internet com a mobilidade proporcionada por sistemas com suporte à mobilidade.

A infra-estrutura empregada nas tecnologias de comunicações com suporte à mobilidade está em constante evolução objetivando dar suporte necessário às aplicações de usuários baseadas no protocolo IP (ANDERSON, 1999). Maior capacidade, com mais largura de banda no enlace de rádio, está sendo suportada às redes móveis, contudo ainda insuficientes em alguns casos (STALLINGS, 2004). No entanto, os protocolos da Internet (TCP/IP Transmission Control Protocol / Internet Protocol) são complexos e, por exigirem muito recurso de banda e memória, não são apropriados para a maioria dos sistemas de comunicações móveis (CORDEIRO, 2002).

Na atualidade, a telefonia celular é a tecnologia de comunicação sem fio com maior abrangência geográfica (ANDERSON, 1999). Essa tecnologia é baseada em comutação de circuitos, tanto para o serviço de voz quanto para dados ou multimídia. Com o advento dos sistemas de comunicação celular de 3ª geração, o processo de comutação passa a ser totalmente por datagramas. Desse modo é possível que cada dispositivo móvel, compatível com esse sistema, opere de forma idêntica a um computador conectado à Internet. Por outro lado, as WLANs (Wireless Local Área Networks) estão se difundindo em larga escala e ocupando áreas que eram dominadas, até então, por redes cabeadas.

De acordo com a Agência Nacional de Telecomunicações (ANATEL), a expansão do mercado de telefonia móvel no Brasil aponta para uma constatação irrefutável: não se conhecia no país qualquer evolução tecnológica tão expressiva quanto ao de celulares. Em 1999 havia cerca de 15 milhões de celulares, saltando para 23,2 milhões ainda em dezembro de 2000. Esse aumento representou um aumento real de 54,7%. O crescimento continua a surpreender nos dias de hoje, assim como as previsões para os próximos anos. A Figura 1.1 mostra a projeção da quantidade de acessos no sistema móvel no período de 2002 a 2009.

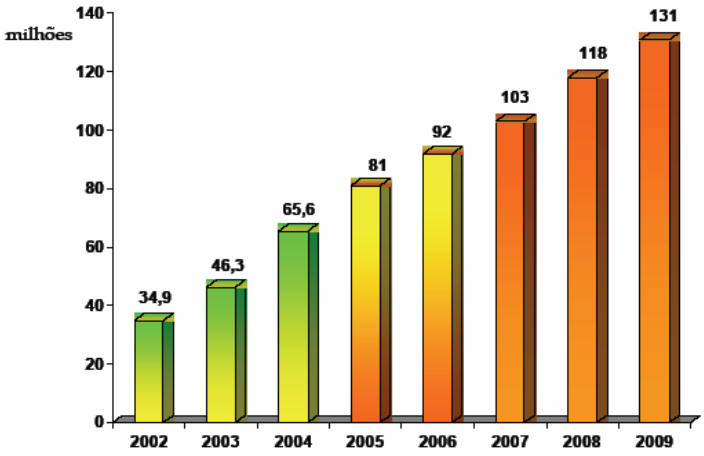


Figura 1.1: Número de acessos em Serviço Móvel Pessoal

Num cenário de convergência, redes como a Internet, WLANs (IEEE, 2001), MANET´s (CORDEIRO, 2002), WIMAX (IEEE 802.16), Telefonia Celular (ANDERSON, 1999) e outras devem permitir uma integração total e transparente.

Com esta interligação será possível, por exemplo, alargar a cobertura das redes celulares fazendo com que um terminal móvel sem fios numa zona escura possa comunicar com uma antena do operador através de outros terminais.

Num outro cenário, poderemos ter um conjunto de sensores ou redes locais sem fios (WLANs) que, colocados numa casa, no escritório de uma pessoa, ou num comboio, conseguem comunicar-se entre si e ter acesso à Internet através de um nó que, por ser mais complexo, fará a interligação a um operador público de telecomunicações. A interligação de MANETs com redes estruturadas torna-se, assim como outros, um tema importante de investigação. A investigação realizada neste trabalho se dá, essencialmente, com base no padrão IEEE 802.11 no processo de comunicação entre os nós de uma MANET e a Internet, através de um *gateway* que implemente o protocolo de roteamentoAODV.

1.1 Posicionamento

No que se refere à mobilidade, as MANETs vêm apresentando importância e notoriedade crescentes, principalmente, quando conectadas à Internet. As MANETs, embora sejam relacionadas, com certa freqüência, à possibilidade de experimentar problemas na comunicação, seja por interferências, quebra do link, mudança na topologia ou diferenças entre protocolos de comunicação. Com base nessa premissa, sabe-se que os protocolos de roteamento das MANETs precisam constantemente lidar com informações imprecisas sobre o estado da topologia da rede e também que, na maioria dos casos, faz uso de protocolos de roteamento incompatíveis com os

protocolos da Internet. Tais características afetam significativamente as comunicações entre MANETs e a Internet.

O roteamento deve, entre outras coisas, garantir que os pacotes sejam encaminhados através dos diferentes nós das redes da melhor forma possível. Na Internet existem equipamentos específicos, os roteadores, que implementam as funções de roteamento para encaminhar pacotes entre *hosts* de origem e de destino. Já nas MANETs, todos os *hosts* devem incorporar também as funções de roteamento.

A Internet e as MANETs utilizam protocolos de roteamento distintos. Embora o *Internet Engineering Task Force* (IETF, 2000) proponha diversos protocolos de roteamento para as MANETs, o protocolo de roteamento *Ad hoc On-Demand Distance Vector* (AODV) (PERKINS, 2003), por ser compatível com o protocolo IP e também por já existirem trabalhos relacionados é o protocolo foco deste estudo. As principais funções dos protocolos de roteamento tradicionais da Internet, são considerados porém não detalhados no presente trabalho.

A implementação de ispositivos de convergência (*gateway*) que encaminhem pacotes entre duas redes ou sub-redes é fundamental, desde que respeitadas as caraterísticas intríncicas de cada protocolo, quando se busca uma integração entre as mesmas.

No protocolo de roteamento AODV, o tempo gasto no processo de descoberta de uma rota, pode chegar, em alguns casos, a 50 milissegundos. Esse tempo também pode ser considerado o pior caso para o protocolo em questão (HAMIDIAN, 2003). Se diversos fluxos de dados chegarem ao nodo *gateway* oriundos da Internet e destinados a uma MANET, o tempo de descoberta das rotas poderá gerar ainda mais descarte de pacotes e/ou atrasos nas entregas dos mesmos. Esse problema é signifivativo quando consideradas as diferenças de performance da Internet em relação às MANETs.

O trabalho em questão visa a propor modificações no protocolo de roteamento AODV (HAMIDIAN, 2003), incorporando regras de confiabilidade (TOH, 2002) no processo de obtenção de rotas, de forma a reduzir o tempo gasto na obtenção destas pelo nodo *gateway*. As modificações aqui propostas atuam apenas no nodo *gateway*. Os demais nodos da MANET continuam utilizando o protocolo de roteamento AODV, proposto por Hamidian.

1.2 Motivação

É esperado que, em um conceito mais amplo, os usuários com grande necessidade de mobilidade, ou usuários nômades, possam permanecer conectados a variados recursos da Internet mesmo quando estes se movimentarem entre diferentes sistemas de comunicação. A terceira geração de telefonia móvel já possibilita, em parte, tal mobilidade, contudo, desde que permaneçam na área de cobertura da operadora. Além da possibilidade de grande mobilidade, também é esperado que seja possível prover algum ganho de qualidade de serviços (QoS – Quality of Service) à mesma.

Os usuários que geram tráfego integrado (voz+dados+vído+...) vêm ganhando terreno em relação à quantidade de carga gerada pelos usuários de voz. Esse tipo de usuário distingue-se dos usuários tradicionais.

Já é possível identificar estudos investigativos, assim como de implementação de mudanças nos protocolos originais, que exploram o processo de integração entre redes infra-estruturadas e MANETs. O presente trabalho toma como base os trabalhos já

realizados por (HAMIDIAN, 2003) e (TOH, 2002). Também estão sendo realizadas pesquisas sobre Link Layer Feedback (AMORIN, 2002) e sobre o uso de métricas de associatividade entre os nodos (TOH, 2002), que demonstram a viabilidade de se alcançar níveis de QoS satisfatórios, a partir da modificação de alguns parâmetros no protocolo da subcamada MAC. Pesquisas como a apresentada por Roche (2002) mostram que é possível prover serviços de QoS através de métricas da previsão de deslocamentos, *feasible routes* e largura de banda. Contudo, estudos que investiguem o impacto da aplicação de características de confiabilidade e estabilidade a serem aplicadas no processo de descoberta de rotas em redes móveis Ad Hoc ainda são raros e constituem uma área a ser mais amplamente explorada.

1.3 Objetivo do Trabalho

Neste trabalho, é apresentada uma extensão ao protocolo de roteamento *Ad hoc On-Demand Distance Vector* (AODV) originalmente proposto por PERKINS (1998), otimizado por HAMIDIAN (2003) com objetivo de otimizar o processo de descoberta de rotas por nodos *gateways* a partir do uso de uma métrica de confiabilidade.

É objetivo do presente trabalho, reduzir a ocorrência de descarte de pacotes no nodo *gateway* e, consequentemente aumentar a eficiência no fluxo de dados quando este receber fluxos de pacotes oriundos da Internet e destinados a *hosts* em uma MANET.

Para atingir esse objetivo, serão introduzidas modificações no protocolo AODV e analisados os resultados de diferentes cenários de simulação, procurando encontrar as vantagens da aplicação de características de confiabilidade ao processo de descoberta de rotas em redes móveis *Ad Hoc*.

1.4 Organização do Trabalho

Este trabalho está dividido em cinco capítulos. O primeiro é a introdução e os subseqüentes estão organizados conforme apresentados abaixo.

Capítulo 2 – Redes Locais *Wireless* (WLANs). Neste capítulo será apresentado um estudo sobre as principais características das redes locais sem fios, tendo como objetivo, estabelecer as referências necessárias das funções das camadas física e de enlace aos *links* utilizados no processo de descoberta de rotas das MANETs.

Capítulo 3 – Os Protocolos de Roteamento das Redes Móveis *Ad Hoc*. Este capítulo apresenta uma revisão bibliográfica sobre as MANETs, apresentando os principais conceitos, a arquitetura básica e os componentes dessas redes, mantendo o foco nas funções de roteamento e nos mecanismos de QoS.

Capítulo 4 – Proposta de Otimização do Processo de Integração de uma Rede Móvel *Ad Hoc* com a Internet. Neste capítulo é definido um ambiente de trabalho e simulação, bem como são apresentadas as modificações realizadas no protocolo, assim como uma análise comparativa entre o desempenho do protocolo AODV original em relação às modificações propostas.

Capítulo 5 – Conclusão e Trabalhos Futuros. Apresenta as principais conclusões tomando como base os resultados obtidos a partir do processo de simulação e também descreve alguns caminhos que poderão ser seguidos para trabalhos futuros.

2 COMUNICAÇÃO SEM FIOS (*WIRELESS*)

O principal objetivo dos sistemas de transmissão sem fios ou sistemas *wireless*, ou redes *wireless*, como são conhecidos, é permitir a troca de informações entre dispositivos, sem a necessidade de uma infraestrutura de cabos de condução. Na atualidade, qualquer tipo de informação pode ser enviada para todos os cantos do mundo sem a utilização de cabos.

Redes *wireless*, WLANs (*Wireless Local Área Network*), WMANs (*Wireless Metropolitan Área Network*) e WWANs (*Wireless Metropolitan Área Network*), normalmente são utilizadas de modo complementar às redes cabeadas existentes, estendendo as suas aplicações, mesmo quando projetadas para funcionarem de forma independete. A compatibilidade das redes *wireless* com o padrão Ethernet, mesmo sem a necessidade de conversão de protocolo, é um exemplo desta integração. Como não necessitam de uma complexa infraestrutura de cabos de condução, as redes *wireless* estão se definindo como uma ótima opção, pela sua mobilidade e flexibilidade frente às novas aplicações que surgem. Por outro lado, a interconexão através de cabos pode custar caro quando envolve hosts geograficamente separados (RAPPAPORT, 1996).

No contexto da mobilidade a tecnologia celular vem se destacando gradualmente no contexto das transmissões sem fios, já sendo totalmente digital na atualidade. Redes digitais, por serem mais eficientes do que redes analógicas, suportam maior *throghput* e com maior segurança do que os sistemas analógicos. A tecnologia digital permite ainda a utilização de serviços com valor agregado, como garantia de entrega, priorização, entre outros. (AMORIN, 2002).

O impacto da comunicação sem fios tem sido e continuará sendo muito intenso. A oferta de novos dispositivos e aplicativos que incorporam diversas tecnologias, estão cada vez mais presentes no nosso dia-a-dia. Também os padrões envolvidos, responsáveis pela interação destes dispositivos, estão rapidamente convergindo para um padrão único global, que suportará uma grande variedade de serviços (AMODEI, 2003).

As redes *wireless* são focadas no nível de enlace, considerando os subníveis MAC e LLC, com maior atenção no subnível MAC. Consideram ainda, a contribuição das informações geradas neste nível ao nível de rede e, conseqüentemente, à função de roteamento. Esta seção aborda essencialmente as WLANS, tomando como base o padrão IEEE 802.11.

2.1 O Padrão IEEE 802.11

As primeiras redes locais sem fios, fazendo uso de rádio-freqüência, implementaram ou transmissão por espalhamento espectral (*spread spectrum*) ou transmissão infravermelha difusa. A primeira, basicamente está associada ao uso das faixas de freqüência ISM (*Industrial, Scientific and Medical*) (Tabela 2.1), distribuídas

em três faixas independentes, de 902 a 928 MHz; de 2,40 a 2,4835 GHz e de 5,725 a 5,85 GHz. Estas faixas de freqüência possuem baixa interoperabilidade, uma vez que cada rede necessita de *hardware* específico para operar em cada faixa. Desse modo os fabricantes passaram a desenvolver suas redes e seus dispositivos com base em seus próprios critérios.

Em 1991, o IEEE autoriza a formação do Grupo de Trabalho 802.11, agrupado na família IEEE 802, com o objetivo de definir um conjunto de especificações para a conectividade sem fios, em uma área de abrangência local (ROCHOL, 2004). Esse grupo passou a definir as regras de funcionamento para uma WLAN.

Na atualidade, segundo o IEEE, exitste um grande conjunto de documentos de padronização de redes *wireless*, dos quais se destacam:

2.1.1 IEEE Std. 802.11 (IEEE, 1999)

Documento extenso, composto por mais de 400 páginas, que apresenta, de forma inédita até então, um padrão para WLANs, que especifica os aspectos das subcamadas MAC e PHY do modelo de referência RM-OSI. Apresenta dois mecanismos de acesso, um com polling (sem contenção) e outro assíncrono CSMA/CA (com contenção). No início especificava as taxas de transmissão de 1 e 2 Mbit/s com base nas técnicas de DSSS (Direct Sequence Spread Spectrum) e FHSS (Frequency Hopping Spreed Spectrum). O padrão 802.11 foi especificado para operar na faixa de freqüência de 2,4 GHz, dentro da faixa ISM. Esse documento também apresenta os aspectos da transmissão por radiação infravermelha, porém encontra-se fora do escopo do presente trabalho. Publicado em 1997 o 802.11 já passou por diversas revisões, as quais geraram publicações de documentos posteriores (extensões) que serão apresentados a seguir.

No restante desse documento os padrões das redes *wireless* publicados pela IEEE poderão ser apresentadas, tanto na sua forma extensa (IEEE 802.11x) quanto na sua forma abreviada (802.11x), pois em ambas as apresentações a referência é feita ao mesmo padrão.

2.1.2 IEEE 802.11b (IEEE2, 1999)

Em julho de 1999, o IEEE publicou o padrão IEEE 802.11b, a primeira extensão do IEEE 802.11. O padrão 802.11b passaria a operar a uma taxa de transmissão de até 11 Mbps. Essa extensão passou a utilizar a modulação HR/DSSS, operando, assim como o 802.11, na faixa de freqüência 2,4 GHz. Para o aumento na taxa de transmissão, mesmo utilizando a mesma banda e mesma taxa de chips, passou a utilizar o CCK (*Complementary Code Keying*), um novo esquema de modulação.

Este padrão é projetado para transmitir dados a taxas de 11 e 5,5 Mbps na modulação HR/DSSS e 2 e 1 Mbps na modulação DSSS (DHIR, 2004).

2.1.3 IEEE 802.11a (IEEE1, 1999)

O padrão 802.11a é uma extensão que apresenta uma nova especificação de nível físico, especificando o uso da faixa de freqüência de 5 GHz. Este padrão especifica também, uma nova técnica de transmissão, o OFDM (*Orthogonal Frequency Division Multiplexing*). O OFDM permite que o 802.11a opere em taxas de 6, 9, 12, 18, 24, 36, 48 e 54 Mbit/s. Essa técnica permite a utilização de até 54 subportadoras. Estas, por sua vez, utilizam diversas técnicas de modulação, assim como BPSK, QPSK, 16QAM ou 64QAM (ROCHOL, 2004). Esse padrão especifica a faixa de freqüência compreendida

dos 5,725 aos 5,85 GHz tornando-se incompatível com dispositivos que trabalham na banda de 2,40 a 2,4835 GHz (CUNHA, 2004).

Essa extensão apresenta melhorias, assim como um aumento na taxa de transmissão, maior disponibilidade de canais por área geográfica, conseqüentemente um menor nível de interferência, já que há mais canais a serem disputados pelas redes. Por outro lado, contudo, trouxe alguns problemas, principalmente quanto a padronização da faixa de freqüência e das técnicas de transmissão, tornando esse padrão incopatível com o 802.11b (AMODEI, 2003). Outro fator que contribuiu para o baixo uso do padrão 802.11a foi o surgimento do padrão 802.11g, que opera na faixa de freqüência de 2,4 GHz, compatível com o padrão 802.11b, a uma taxa de transmissão de 54 Mbps.

2.1.4 IEEE 802.11g (IEEE3, 2003)

O padrão IEEE 802.11g é uma evolução do padrão IEEE 802.11b, contudo operando na mesma faixa de freqüência de 2,4 GHz e mantendo a compatibilidade com os padrões que já operavam nesta faixa de freqüência. O padrão 802.11g também pode ser visto como uma fusão dos padrões 802.11a e 802.11b. Este novo padrão faz uso das melhores características dos padrões 802.11a e 802.11b. A modulação OFDM do 802.11a e a faixa de freqüência do 802.11b, a ISM de 2,4 GHz (AMODEI, 2003).

Este padrão também utiliza o OFDM e acresenta um novo esquema de transmissão, o PBCC (Packet Binary Convolutional Code) passando a ser conhecido como ERP-PBCC e ERP-OFDM, onde ERP é a abreviatura para Enhanced Rate PLCP (*Physical Level Convergence Protocol*). Esse novo esquema permite taxas de transmissão de 22, 33 Mbit/s e 54 Mbit/s. As taxas de 1, 2, 5,5 e 11 Mbps, também suportadas no 802.11g, funcionam de modo idêntico ao 802.11b (ROCHOL, 2004).

A tabela 2.1 apresenta um resumo das publicações IEEE apresentadas acima.

Tabela 2.1: Faixas de freqüência ISM utilizadas em Redes *Wireless* IEEE 802.11

Padrão	Publicação	Freqüências (GHz)	Modulação	Taxa (bps)
802.11	1997	2,400 – 2,483	DSSS, FHSS	1 e 2 Mbps
802.11a	1999	5,150 – 5,350 5,470 – 5,725 5,725 – 5,850	OFDM	54 Mbps
802.11b	1999	2,400 – 2,483	DSSS, HR-DSSS	11 Mbps
802.11g	2003	2,400 – 2483	DSSS, HR-DSSS, OFDM	54 Mbps

Fonte: (ROCHOL, 2004)

2.2 Grupos de tarefas (Task Groups)

Nos últimos anos, além das normas já apresentadas, existem outras que, no intuito de desenvolver as redes sem fios, ou estão sendo desenvolvidas ou já estão desenvolvidas por outros Grupos de Tarefa (*Task Groups*) da IEEE 802.11. Algumas destas normas são apresentadas a seguir:

2.2.1 IEEE 802.11c

O padrão 802.11c já foi publicado e é utilizado pelos fabricantes de dispositivos para redes *wireless* no processo de desenvolvimento de seus APs. Este padrão fornece as especificações necessárias e suficientes, de modo a assegurar a operação em modo

bridge entre dois APs. Esse padrão especifica propriedades de operação da subcamada MAC, onde é estabelecida a operação em modo *bridge* (CUNHA, 2004).

2.2.2 IEEE 802.11d

O padrão 802.11d, publicado em 2001 e desenvolvido para as áreas que estão fora dos cinco domínios regulatórios estabelecidos (EUA, Canadá, Europa, Japão e Austrália). O padrão definiu requisitos para a sub-camada PHY do nível físico que atendam ao processo regulatório de outros países. É essencial para a operação na banda de 5 GHz, por motivo de não conformidade no uso das faixas de freqüência dessa banda nos países fora dos domínios regulatórios. Assim como no padrão 802.11c, o padrão 802.11d aplica-se basicamente para os fabricantes que desenvolvem produtos para os padrões 802.11.

2.2.3 IEEE 802.11e

Atento às necessidades de QoS e de padronização em redes 802.11, o IEEE criou o 802.11e para especificar uma extensão que introduzisse métodos de provisão de QoS a partir da subcamada MAC. Essa extensão é identificada como MAC *Enhancements for Quality of Service* (STALLINGS, 2004).

O IEEE 802.11e especifica a troca das funções de coordenação DCF e PCF pela DCF avançada (EDCF – *Enhanced DCF*) e pela Coordenação Híbrida (HCF - *Hibrid Coordination Function*) respectivamente.

Um AP compatível com o 802.11e deve suportar tanto o EDCF quanto HCF. A diferença existente entre os diferentes APs com suporte ao 802.11e está na configuração de QoS para diferentes TCs (*Trafic Classes*), já que Muitos dos atuais APs permitem apenas uma simples configurações no controle de banda.

2.2.4 IEEE 802.11f

O IEEE 802.11f (2003) introduz novos esquemas de interoperabilidade entre APs (*Access Points*) e sistemas de distribuição (DS – Distribution Sistems) entre equipamentos de diferentes fornecedores. Essa interoperabilidade pode ser definida como um *roaming* entre APs. Processo similar a um *roaming* entre células em sistemas de telefonia celular.

Segundo Rochol (2004), o trabalho deste grupo consiste na criação de um protocolo de interoperabilidade entre pontos de acesso (IAPP - *Inter-Access Point Protocol*).

2.2.5 IEEE 802.11h

Essa norma introduz funcionalidades que são imprescindíveis em redes *wireless* de alto desempenho, assim como a seleção DFS (*Dynamic Frequency Selection*) e o TPC (*Transmission Power Control*).

Com a sobreposição de freqüências, decorrente do uso crescente de sistemas wireless, significa que podem existir interferências entre dispositivos ou redes sem fios. O padrão 802.11h poderá fazer ajustes de freqüência ou potência, se auto-ajustando no intuito de eliminar ou diminuir tal interferência (ROCHOL, 2004).

2.2.6 IEEE 802.11i

O grupo de trabalho IEEE 802.11i foi criado em 2001 com o objetivo de propor melhoria às funções de segurança e criar mecanismos de autenticação na subcamada MAC do protocolo 802.11. Apresentado e aprovado em 2004, torna-se o padrão oficial para segurança em redes *wireless*.

O 802.11i incorpora o WPA (Wi-Fi Protected Access), o qual faz uso do protocolo de criptografia TKPI (Temporal Key Protocol Integrity). O WPA – TKIP é de fácil configuração, podendo ainda utilizar o protocolo RADIUS (baseado no IEEE 802.1x) para autenticação de usuários (GRIFFITH, 2004).

Mais recentemente, o AES (*Advanced Encryption Standart*) foi adicionado ao padrão. Esse protocolo é utilizado para criptografia e para verificação de integridade, permitindo que o padrão 802.11i utilize chaves criptográficas de até 128 bits (PEREZ, 2004).

2.2.7 IEEE 802.11n

Segundo (SHOEMAKE, 2004), em julho de 2003 o *High Throughput Study Group* (HT SG) do IEEE obteve autorização para a formação do grupo de trabalho (*Task Group* – TG) IEEE 802.11n, sendo oficialmente implantado em setembro do mesmo ano.

Uma das maiores exigências desse novo padrão é a de manter compatibilidade e interoperabilidade com os padrões a, b e g. Essa interoperabilidade, alcançada a partir de mudanças realizadas na camada física (*fisic layer*) e na sub-camada MAC (Medium Access Control), garantirá uma transição suave sem causar qualquer impacto sobre o desempenho dos outros padrões (GRIMM, 2004). O modelo IEEE 802.11n especifica algumas alterações nas propriedades do 802.11 de modo que seja possível aumentar a taxa de transferência em redes deste padrão, até então restrita a 54 Mbps, um dos maiores desafios deste tipo de rede (WILSON, 2004).

2.3 A arquitetura do padrão IEEE 802.11

O BSS, formado por um conjunto determinado de STAs (*Stations*), controladas por um AP, define a arquitetura básica de uma rede *wireless*. O AP (*Access Point*) controla as STAs que estão em sua área de cobertura e pode assumir os papéis de uma STA ou de um equipamento específico de AP. Quando encontramos diversos BSSs (*Basic Service Set*) distintos e interconectados através de seus APs, que por suavez implementam o DS (*Distribution System*), passamos a ter uma arquitetrua de ESS (Extended Service Set), como pode ser observado na Figura 2.1. Uma estação, enquanto permanecer na área de cobertura de uma ESS, pode migrar dinamicamente entre BSSs, sem perder a sua conexão. Este processo é conhecido como *roaming*. Cada estação passa a ter a sua área de cobertura estendida à toda a área de cobertura do ESS, isto é, a soma de todas as áreas dos BSSs (ROCHOL, 2004).

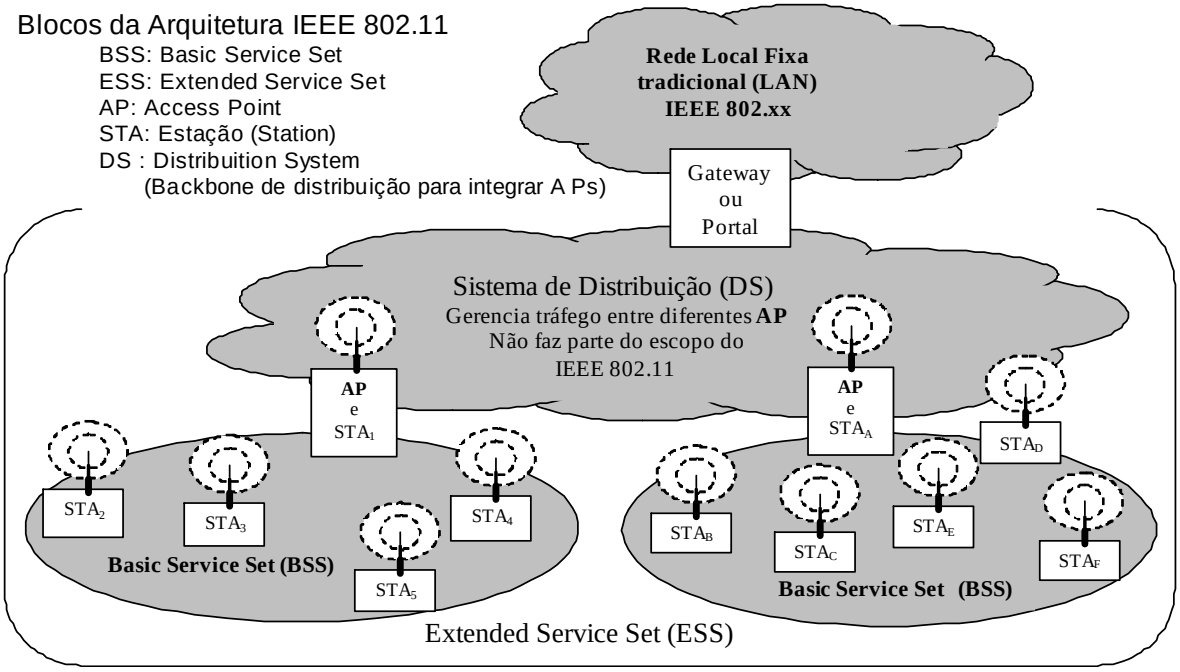


Figura 2.1: Arquitetura Funcional do IEEE 802.11

O sistema de distribuição (DS) pode ser constituído por uma outra rede *wireless*, um backbone, ou uma rede fixa. O sistema de distribuição, por sua vez, pode ter uma interconexão com qualquer rede local fixa tipo IEEE 802.xx a partir de um *gateway* ou portal, (Figura 2.1).

2.4 Os serviços do padrão IEEE 802.11

O padrão IEEE 802.11 definiu nove serviços a serem oferecidos por redes *wireless* para que possa oferecer uma funcionalidade equivalente a das redes locais cabeadas. Na tabela 2.2 são apresentadas duas formas de classificação desses serviços: (1) interação entre estações com envolvimento do Sistema de Distribuição, e (2) interação direta entre estações (RAPPAPORT, 1996).

Tabela 2.2: Serviços disponibilizados por uma rede *wireless* IEEE 802.11

Provedor do Serviço	Serviços	Função
Sistema de Distribuição (DS)	Associação	Repasse de MSDU
	Dissociação	
	Reassociação	
	Distribuição	
	Integração	
Estação (STA)	Entrega do MSDU	Repasse de MSDU
	Privacidade	Acesso à rede local *Wireless* e segurança
	Autenticação	
	Desautenticação	

Fonte: (ROCHOL, 2004)

É importante ressaltar que o principal suporte oferecido por estes serviços é o repasse de MSDUs (MAC Service Data Units). Também os aspectos de segurança (autenticação e privacidade), são fundamentais para qualquer rede *wireless*.

Na Figura 2.2 é apresentada a localização dos diferentes serviços implementados em redes *wireless*, considerando o contexto de um ESS. A estação, antes de começar a transmitir dados, precisa se conectar, fazendo uma associação ao AP. Quando esta estação migra para outra área de cobertura, isto é, outro BSS, deve executar o serviço de reassociação no novo AP. Ao concluir a sessão, a estação faz uma desassociação (ROCHOL, 2004).

- *Privacidade/Autenticação/Desautenticação*

É grande a vulnerabilidade em qualquer sistema de transmissão em Rádio Frequência (RF). Procurando diminuir esta vulnerabilidade na transmissão em RF, as redes *wireless*, antes de se iniciar a troca de dados entre duas STAs, força que estas se identifiquem mutuamente (*Autentication*). Uma vez identificados os parceiros, dá-se início à troca de informações. A troca de informações ocorre de forma sigilosa (criptografada), desde que utilizados os serviços apropriados.

- *Distribuição*

É um serviço que oferece troca de MSDUs entre estações de diferentes BSSs de um mesmo ESS.

- *Integração*

É um serviço que oferece troca de MSDUs entre uma rede WLAN e uma LAN. Entre uma rede 802.11 e uma rede IEEE 802.3, por exemplo.

- *Entrega do MSDU*

Serviço responsável por suportar a troca dos MSDUs entre as estações de uma rede sem fio (*wireless).*

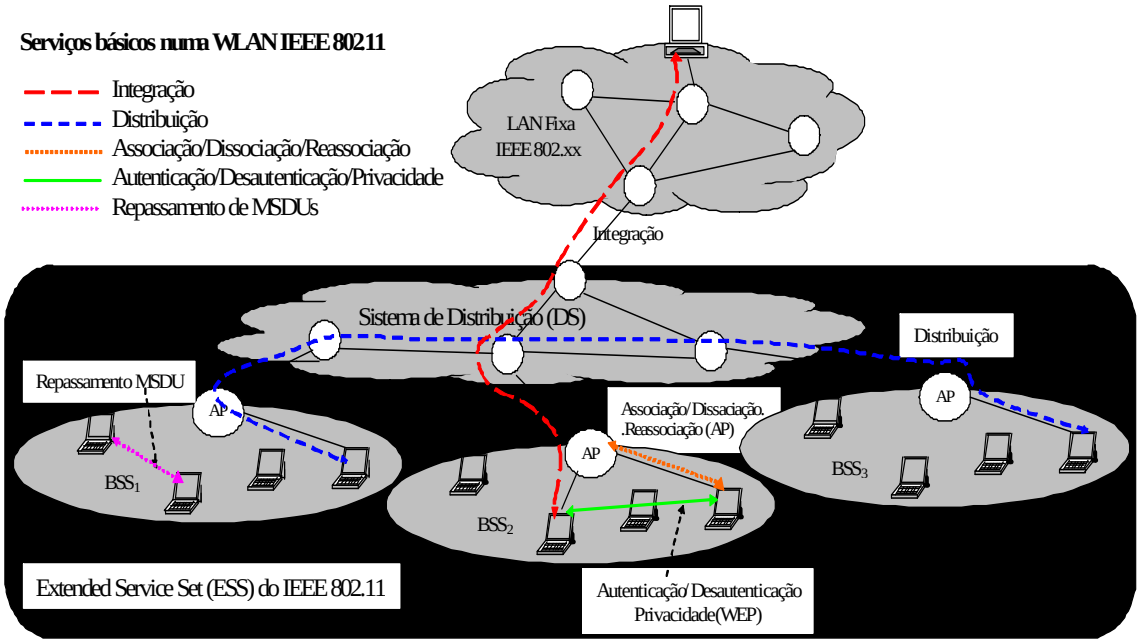


Figura 2.2: Localização dos Serviços em ambiente *wireless*

2.5 O Modelo de Referência de Protocolos do IEEE 802.11

O escopo do padrão IEEE 802.11 resume-se às camadas física e de enlace do modelo de referência OSI (RM-OSI). A camada física é composta pelas subcamadas

PMD e PLCP enquanto a cadada de enlace é composta pelas subcamadas LLC e MAC. A seguir são detalhadas as subcamadas da camada física:

(1) *subcamada física inferior* ou PMD (*Physical Medium Dependent*): oferece quatro diferentes técnicas de transmissão que consistem nos aspectos de modulação e codificação do sinal. Cada um dos padrões do 802.11 usa uma ou mais das quatro técnicas de transmissão: Raios infravermelhos difusos (IRDA), rádio-frequência por espectro de espalhamento com saltos de freqüência (FHSS - Frequency Hopping Spread Spectrum) e rádio-frequência por espectro de espalhamento em seqüência direta DSSS – Direct Sequence Spread Spectrum) e rádio-freqüência por ortogonalidade (OFDM – Ortogonal Frequency Division Multiplexing), esta última a mais atual (ROCHOL, 2004). Novas técnicas poderão surgir a medida que as redes *wireless* evoluem.

(2) *subcamada física superior* ou PLCP (*Physical Layer Convergence Procedure*): implementa os pontos de acesso aos serviços de convergência comuns aos quatro métodos de transmissão física. Sua principal função é de gerência, registrando as estatísticas da camada física para a MIB (Management Information Base) (ROCHOL, 2004).

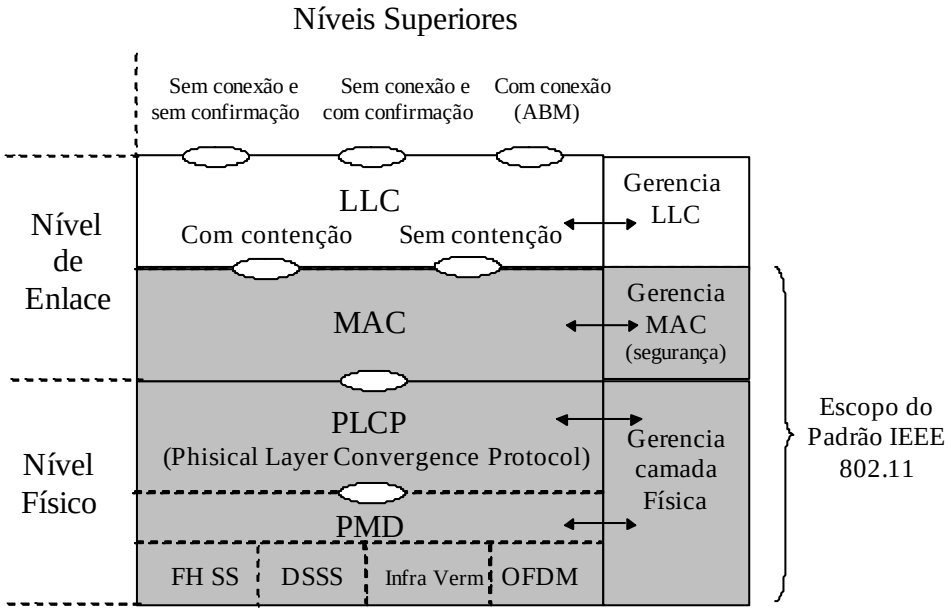


Figura 2.3: Arquitetura do Modelo IEEE 802.11

A camada física também incorpora uma função CCA (*Clear Channel Assessment*), que informa para a subcamada MAC quando um sinal foi detectado.

A camada de enlace é composta por duas subcamadas: LLC (*Logical Link Control*), responsável pela interação com as camadas superiores e MAC (*Medium Access Control*), responsável pela interação com a camada física. A subcamada de LLC assegura a interoperabilidade entre todas as tecnologias de LAN, sejam estas com ou sem fios, consequentemente fora do escopo do padrão IEEE 802.11. A subcamada LLC, por outro lado, fornece três tipos distintos de serviços (Figura 2.3) para as camadas superiores:

(1) Serviço sem conexão e sem confirmação. É um serviço simples e do tipo datagrama. Não implementa mecanismos de controle de erro ou de controle de fluxo para as LPDUs (LLC Protocol Data Units).

(2) Serviço com conexão e confirmação. Responsável por estabelecer uma conexão lógica entre duas STAs e também por implementar controles de erro e de fluxo.

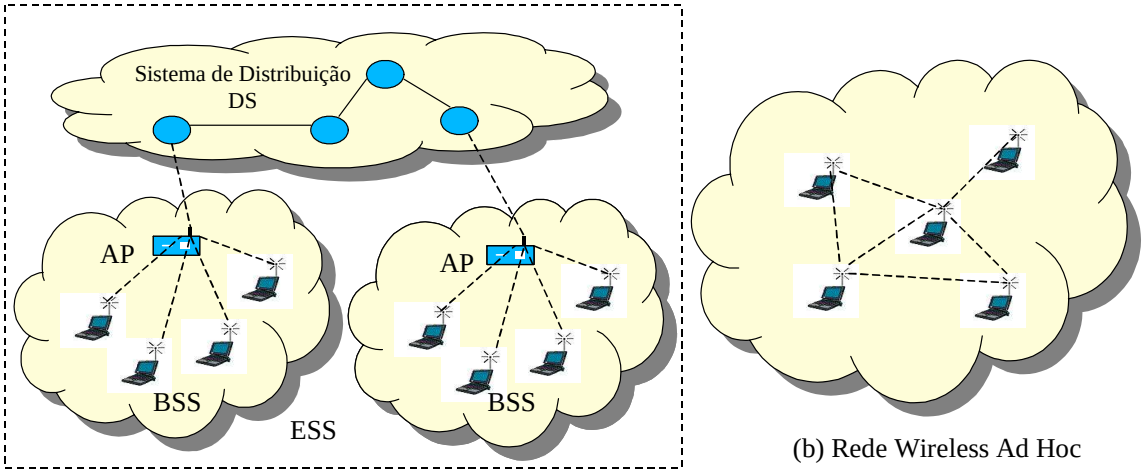
(3) Serviço sem conexão com confirmação. É um serviço onde as LPDUs (LLC *Protocol Data Units*) são repassadas entre dois usuários sem haver uma conexão lógica entre eles, porém exigindo confirmação pelo usuário remoto.

O subnível MAC do IEEE 802.11 fornece dois tipos de mecanismos distintos de acesso ao meio; (1) um por contenção e o outro (2) sem contenção, demonstrados na figura 2.3.

(1) Segundo Stallings (2004), o serviço de acesso sem contenção é oferecido pela função PCF (*Point Coordination Function*). Esse tipo de acesso se destina aos serviços com características síncronas e de baixa latência. O PCF é implementado através de uma dinâmica do tipo poll/select presente no AP e na STA. Em razão das suas características, o PCF é oferecido somente em redes *wireless* infra-estruturadas, pois necessita obrigatoriamente um AP definido (Figura 2.4a).

(2) O serviço de acesso com contenção, oferecido pela função DCF é obrigatoriamente implementado em cada STA e também em cada AP. Este serviço é oferecido tanto em redes infraestruturadas (WLANs) como em redes não infreaestruturadas (MANETs). Já para as MANETs, esse é o único método de acesso disponível (Figura 2.4b).

Considerando os dois mecanismos apresntados acima, é possível implementar dois tipos de redes *wireless*: redes infraestruturadas, que podem oferecer acesso, tanto com contenção quanto sem contenção e as MANETs que oferecem somente o acesso com contenção. A seguir são apresentados alguns detalhes destas duas abordagens de redes *wireless*.



(a) Rede Wireless Infra-Estruturada

(b) Rede Wireless Ad Hoc

Figura 2.4 : Rede *Wireless*: (a) Estruturada e (b) *Ad Hoc*

As Redes Infra-Estruturadas (Figura 2.4a) caracterizam-se por possuírem STAs e APs. Cada AP é responsável pela conexão das STAs que estão dentro da área de abrangência do BSS com a rede cabeada. O AP executa tarefas de coordenação que são fundamentais ao acesso das STAs: aceita ou rejeita a entrada de uma nova STA à rede, recebe e manipula dados estatísticos objetivando o gerenciamento de cada canal e gerencia a migração entre BSSs distintos (*roaming*). O serviço de autenticação e de roaming das STAs entre APs de BSSs distinas é realizada pela entidade de Gerência da

subcamada MAC. Cada STA pode se associar a apenas um ponto de acesso por vez. Quando migra entre BSSs, deve se desassociar do AP antigo e reassociar no AP novo (ROCHOL, 2004).

As MANETs, Figura 2.4b, caracterizam-se por não necessitarem de qualquer infra-estrutura, seja de cabos de comutação ou de WLANs, são formadas por STAs móveis que estabelecem comunicação ponto-a-ponto de múltiplos saltos entre si. Essas redes apresentam topologia dinâmica, não necessitam de um ponto central de coordenação e podem alcançar pontos distintos realizando múltiplos saltos, salto-a-salto (hop-by-hop multi hop). As STAs de uma MANET colaboram entre si para encaminhar e reenviar os pacotes de outros nós que estão fora de alcance do nó de destino, permitindo alcançar a qualquer nó da rede, mesmo não possuindo link direto ao mesmo (STALLINGS, 2004).

Na seção 2.6, serão detalhadas algumas funções da camada física e da camada MAC do padrão IEEE 802.11.

2.6 Camada Física em redes IEEE802.11

A transmissão sem fios possui propriedades únicas, diferenciando-a dos outros meios. Os sistemas de rádio-freqüência apresentam alguns atributos inerentes a este meio (ROCHOL, 2004):

- o intervalo da faixa de frequência para a comunicação é limitado;
- a detecção da portadora de ondas eletromagnéticas apresenta baixa confiabilidade e não pode ser realizada durante a transmissão a um custo de produto razoável já que o sistema opera em half-duplex;
- alta taxa de erros de bits transmitidos quando comparadas a redes locais cabeadas;
- rápida atenuação do sinal decorrente de obstáculos e condições climáticas.
- é de domínio público;

Outra conseqüência do fato do meio ser de domínio público reside na inabilidade em controlar e gerenciar o acesso ao canal, ficando sujeito a interferências de toda ordem, podendo ainda tais interferência serem provocadas intencionalmente para sabotagem eletrônica, visto que um ruído ocupa a banda para transmissão, paralisando completamente a operação da rede (RAPPAPORT, 1996).

O padrão IEEE 802.11 é implementado a partir do uso das faixas de freqüência ISM. As faixas ISM são de livre utilização e são utilizadas por diversas tecnologias que, por sua vez, devem fazer uso de mecanismos que evitem as interferências indesejadas além de cumprir as especificações de potência do sinal e emissão espectral (SANTANA, 2004).

2.7 Controle de Acesso ao Meio Físico (MAC – IEEE 802.11)

A subcamada MAC é responsável pela interface de acesso ao meio pelas estações de uma rede *wireless*. O principal problema a ser resolvido nessas redes é a alocação de um canal de RF para cada um das STAs que o disputam. Esta alocação deve fazer uso de métodos determinísticos, controlados por APs, visto que a as colisões, quando ocorrem, diminuem drasticamente o desempenho das redes wireless (STALLINGS, 2004).

A subcamada MAC, específica para *wireless*, deve ser apresentada à subcamada LLC e camadas superiores de forma idêntica as demais redes 802.x funcionando de modo transparente com protocolos de níveis superiores já existentes. O subnível MAC das redes *wireless* deverá gerenciar os recursos físicos, evitando atrasos na propagação e, consequentemente, a perda de desempenho (TANENBAUM, 1996). Para tornar isso possível, o padrão IEEE 802.11 descreve:

- Funções, serviços e aspectos referentes à mobilidade, necessários para os dispositivos nas redes 802.11 (Tabela 2.2);
- Serviços com garantias de segurança e privacidade;
- Procedimentos de suporte à comunicação assíncrona e de entrega dos dados em fatias de tempo (*slot times*).

O IEEE define o DFWMAC (*Distributed Foundation Wireless Medium Access Control*) como o protocolo a ser implementado para a subcamada MAC das redes *wireless*. O DFWMAC apresenta um método de acesso distribuído básico, que é obrigatório e também um método centralizado, este opcional (vide seção 2.5). Esses dois métodos, segundo a especificação do padrão, podem coexistir. O DFWMAC também é responsável pelo tratamento de problemas como *roaming* e estações escondidas (*hidden node*) (STALLINGS, 2004).

A figura 2.5, a seguir, apresentada a arquitetura de protocolos do IEEE 802.11, com seus diferentes blocos funcionais e hierarquizações.

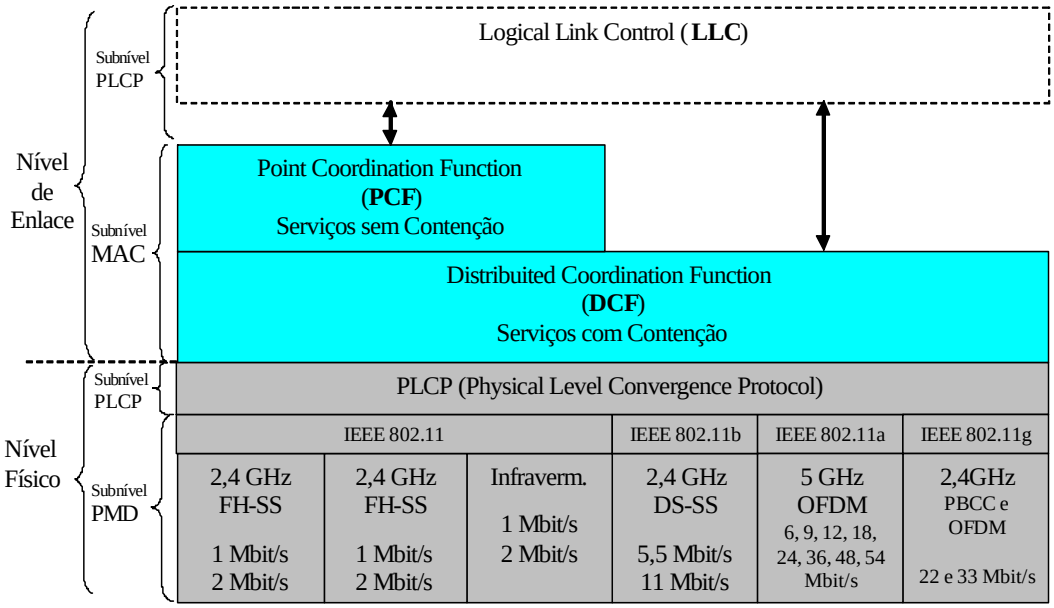


Figura 2.5: Os níveis físico e MAC do IEEE 802.11

Na subcamada MAC são implementados dois métodos de acesso ao meio. O método de acesso distribuído (DCF) e o método centralizado (PCF). Nessa estrutura o método centralizado depende do método distribuído para operar, enquanto que o método distribuído pode operar de modo independente (vide figura 2.5). Ambos os métodos são necessários para uma estação possa saber se tem permissão para transmitir. (STALLINGS, 2004). A Figura 2.6, a seguir, apresenta a hierarquização da subcamada MAC.

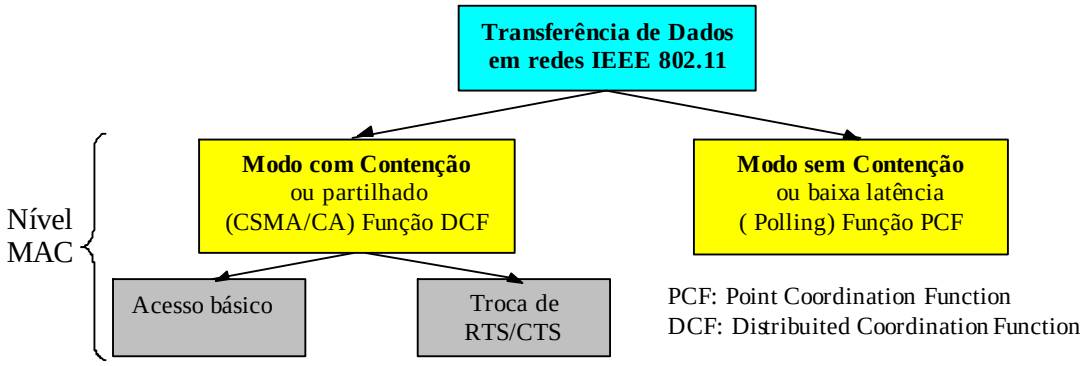


Figura 2.6: Transferência de dados do nível MAC no IEEE 802.11

O DCF responsável pela execução do algoritmo do CSMA/CA, consequentemente do procedimento de *backoff*, fundamental para as WLANs e está a cargo da transmissão assíncrona e distribuída de dados. A sua implementação é obrigatória e aplica-se a qualquer rede sem fio. O DCF também é a base para a contrução do PCF (*Point Coordination Function*). O PCF, por sua vez, é responsável por organizar os serviços sensíveis à latência. A figura 2.5 apresenta o esquema de implementação das funções PCF e DCF na subcamada MAC. A figura 2.6, por sua vez, demonstra a hierarquização destas funções.

No PCF, o AP envia mensagem às STAs para saber se estas possuem dados a serem transmitidos. Se uma STA possuir dados a serem transmitidos, os transmite durante o período de execução do PCF apenas quando esta for selecionada. A implementação do PCF não é obrigatória, permitindo assim que, em uma mesma rede, coexistam estações operando no modo PCF e outras não.

Segundo (STALLINGS, 2004), o AP deve possuir acesso de modo privilegiado durante o período de PCF, evitando que alguma estação comum passe a controlar o canal, pois isso poderia comprometer a transmissão de dados dos serviços sensíveis à latência. O AP é responsável por organizar a comunicação neste período, definindo sua duração e convidando as estações a transmitirem uma de cada vez. Esse acesso privilegiado é obtido, pois o AP possuir um tempo menor de escuta em relação ao tempo de escuta que as STAs usam para monitorar o canal e saberem se ele está livre.

2.7.1 Associação a Pontos de Acesso e *Roaming*

Uma rede wireless infra-estruturada necessita obrigatoriamente de um AP, formando uma BSS. Ess rede normalmente é utilizada para estender uma rede cabeada, permitindo que as STAs interajam com serviços de outras redes. Uma STA deve se associar a um AP para que consiga fazer uso destes serviços e desassociar-se ao abandonar a rede. Em uma ESS, o serviço de reassociação é que permite o migração de STAs entre diferentes BSSs (SANTANA, 2004).

Uma estação, antes do envio de informações, deve primeiramente solicitar um serviço de associação ao ponto de acesso. A associação mapeia a estação no sistema de distribuição através do ponto de acesso. Cada estação pode associar-se a um único ponto de acesso em um determinado tempo, porém todos os pontos de acesso podem ter múltiplas estações associadas. (SANTANA, 2004). O serviço de reassociação deve ser executado quanto uma STA migra entre BSSs de uma mesma ESS. Esse serviço é conhecido como *roaming* e exige que a STA registre-se automaticamente no novo AP

de modo que este possa informar ao AP da BSS de origem sobre a sua nova posição (ROCHOL, 2004). O AP da BSS de origem fica sabendo da nova posição da STA, reenviando a informação a ela destinada, para o endereço da nova BSS, como se a STA estivesse em sua própria BSS.

2.8 IEEE 802.11 em relação às Redes Móveis *Ad Hoc*

As redes móveis *Ad Hoc* são um tipo especial de redes sem fios. Essas redes são definidas no nível de rede do modelo RM-OSI, visto que cada estação móvel é vista como um nó da rede com capacidade de estabelecer rotas entre origem e destino. Este tipo de rede faz uso de sistemas de comunicação sem fios, que por sua vez são implementados nas camadas inferiores do modelo RM-OSI. Neste trabalho, em específico, a rede móvel *Ad Hoc* é implementada sobre uma rede sem fio, segundo o padrão IEEE 802.11. Outro padrão de rede *wireless* poderia ter sido utilizado, porém optou-se pelo padrão IEEE 802.11 para simplificar o processo de simulação utilizado para a apresentação dos resultados.

Ao contrário da maioria das atuais redes *wireless*, as MANETs não requerem uma infraestrutura prévia, pois os nós *de* uma MANET colaboram entre si no processo de comunicação fim-a-fim, encaminhando e reenviando os pacotes de outros nós.

Para o trabalho aqui apresentado, é considerado que o subnível LLC do nível de enlace, através do serviço sem conexão e sem confirmação, é responsável por receber as comunicações dos níveis superiores. É considerado também que será utilizado o protocolo UDP do nível de transporte. O serviço sem contenção é muito simples do tipo datagrama e será essencial para o processo de implementação e simulação do presente trabalho.

Já o subnível LLC se comunica com o subnível MAC através do serviço de acesso com contenção. Serviço que é oferecido pela função de DCF (*Distributed Coordination Function*) do subnível MAC. Em redes do tipo *Ad Hoc* esse é o único método de acesso disponível.

A Figura 2.9, apresenta o caminho a ser seguido pelo fluxo de datagramas em cada um dos nós da rede *Ad Hoc* provenientes do nível de rede. Esse fluxo será respeitado durante os processos de implementação e simulação.

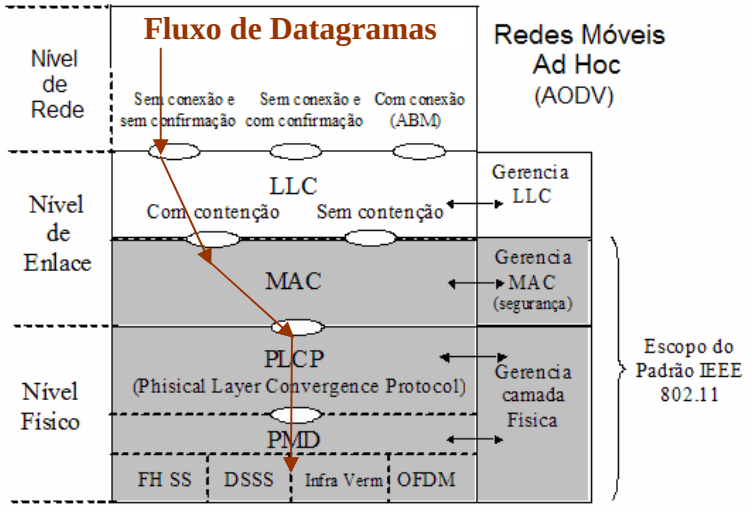


Figura 2.9: Fluxo da comunicação entre camadas 1, 2 e 3

3 ROTEAMENTO EM REDES MÓVEIS *AD HOC*

O IETF, órgão responsável pela padronização das tecnologias relacionadas à Internet, estabeleceu um grupo de trabalho com os objetivos de analisar os problemas relacionados às redes não infraestruturadas e de propor um ou mais algoritmos de roteamento para as Redes Móveis *Ad Hoc* (MANET). A RFC 2501 apresentada por (CORSON e MACKER, 1999) e publicada em janeiro de 1999, salienta a topologia dinâmica, a operação para economia de energia, a largura de banda restrita e a segurança física limitada como as principais características dessas redes. Essa RFC especifica ainda as principais funções e estratégias de roteamento para redes móveis *Ad Hoc*.

As Redes *Ad Hoc*, referidas pelo IETF4 como MANET, (*Mobile Ad hoc NETwork*) utilizam as comunicações sem fios não infratestruturadas como meio de transmissão, primando pela mobilidade do terminal. A premissa da mobilidade permite alterações dinâmicas da topologia da rede e, consequentemente, conexões e desconexão em grande quantidade. A figura 3.1 apresenta a variação da topologia de uma rede *Ad Hoc*.

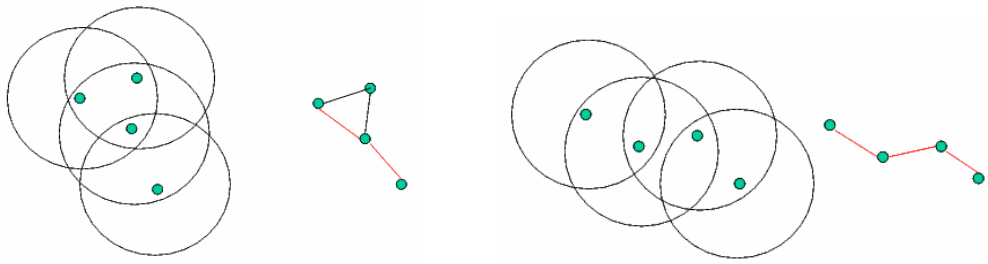


Figura. 3.1: Mudança de Topologia em redes *Ad Hoc*

A topologia dinâmica permite a livre movimentação de todos os terminais sem que, para tanto, necessite de alguma infra-estrutura de comunicação, cabeada ou não cabeada. Um pacote de informações, ao ser enviado a um nó de destino que esteja fora da área de abrangência direta (um salto), deverá passar por outros nós (múltiplos saltos), chamados nós intermediários, até alcançar o seu destino, considerando que um terminal móvel só consegue transmitir informações para os seus vizinhos (salto-a-salto). AMANET está relacionada à transmissão eficiente de pacotes de dados de uma estação móvel (*mobile station*) para o outra, percorrendo todos os nós intermediários entre a origem e destino, através de funções de roteamento apropriadas (AMORIM, 2002).

A função de roteamento em MANETs, diferentemente das redes infraestruturadas, onde há equipamentos específicos para esta tarefa, é executada em cada nó participante da rede. Por outro lado, o roteamento em MANETs deve ser realizado de forma autônoma, deve ser eficiente, justo e seguro, assim como ocorre nas redes infraestruturadas. Consequentemente, a função de roteamento das MANETs, deve

permitir o uso de rotas dinâmicas entre os nós de origem e destin, permitindo ainda o uso ou a possibilidade de uso de várias rotas distintas (TOH, 2002).

Esse tipo de rede poderá vir a ser independente ou interligada a outras, a partir da implementação de um *gateway*. Esse *gateway* deve compreender as funções de roteamento de todas as redes às quais possui conexão, passando a ter função fundamental no processo de interligação, visto que, na maioria dos casos são incompatíveis (CORDEIRO, 2002).

Por terem um controle descentralizado, as Redes *Ad Hoc* normalmente apresentam maior robustez, rapidez na instalação, mobilidade, conectividade e tolerância a quebras de links em relação às redes centralizadas. Por outro lado, a banda passante reduzida, o alto índice de erros no enlace sem fio, o fato do nó de origem não conhecer a localização física do nó de destino e a topologia dinâmica são as características negativas desse tipo de Rede (TOH, 2002).

3.1 Protocolos de Roteamento em Redes *Ad Hoc*

A partir do surgimento da Internet, o uso de meios para a interconexão de redes de modo a possibilitar a troca de dados entre elas, passou a ser requisito básico de operação. Com o crescimento e o aperfeiçoamento dessas redes, requisitos de qualidade e mobilidade passaram a ganhar notoriedade. A adaptação das rotas e o encaminhamento dos pacotes de dados com confiabilidade, passam a se estabelecer como uma regra geral. Segundo (TANENBAUM, 1996), a principal função dos protocolos de roteamento é receber pacotes, fazer com que sejam encaminhados a partir do host de origem, passando por vários nós intermediários, chegar à estação de destino. O caminho, formado por nós ou roteadores, como são conhecidos estabelecem a rota (caminho entre as redes) por onde os pacotes de dados devem trafegar.

Na atualidade contamos com uma variedade muito grande de algoritmos de roteamento, (TANENBAUM, 1996). Os algoritmos de roteamento normalmente implementam uma tabela de roteamento em cada nó (roteador, *gateway*, *mobile host*), a qual armazena informações sobre as possíveis rotas aos destinos conhecidos (topologia da rede). Quando uma estação necessita transmitir pacotes para um destino em uma rede qualquer, estes são enviados para o roteador de borda da sua rede que procura rotas conhecidas para o destino informado, a partir da sua tabela de roteamento. O roteador de borda deve então, informar a rota e repassar o pacote para o próximo nó da rota até alcançar algum nó que conheça o host de destino. Esse processo não é válido para redes que realizam a descoberta da rota reativa com base no nodo origem. Cada protocolo especifica as suas características, determinando maior ou menor adequação de cada rede em particular (COMMER, 1991). Os diversos protocolos de roteamento implementam algoritmos específicos para satisfazerem uma necessidade ou um conjunto de necessidades. Os algoritmos dos protocolos de roteamento, embora possam ser classificados de diversas maneiras distintas, utilizam mecanismos de vetor de distância ou de estado do enlace.

Alguns erros podem surgir no processo de descoberta e uso de rotas, os quais podem provocar problemas na propagação de rotas e na atualização das informações da tabela de roteamento. A principal causa para isso está na mistura de protocolos utilizados, nas mudanças muito freqüentes de topologia ou interpretação incorreta das informações contidas nos pacotes, como por exemplo, as métricas. Essas métricas podem não ser utilizadas em um protocolo, mas requeridas em outro.

Os algoritmos de roteamento podem ser diferenciados a partir de várias características (CISCO, 1995). O objetivo particular do projetista do algoritmo determina a operação do protocolo de roteamento resultante, assim como as suas principais características. Os seguintes tipos de algoritmos são possíveis: estático, dinâmico, rota única, múltiplas rotas, plano, hierárquico, intradomínios, inter-domínios e estado do enlace, vetor de distância. Em qualquer caso, os algoritmos de roteamento implementam métricas que afetam o cálculo das melhores rotas. Os mais sofisticados, porém, podem apoiar a sua escolha em várias métricas combinadas, resultando, contudo em um valor único. As métricas mais utilizadas são o comprimento da rota, o atraso na propagação, a largura de banda, a confiabilidade, a carga, o custo da comunicação e o MTU (*Maximum Transfer Unit*). A atividade essencial de um roteador podem ser definida como a escolha da melhor rota, a ser definida a partir de métricas pré-determinadas em cada protocolo.

O endereço IP é a base do roteamento em uma rede IP e, por ser parte da informação contida no cabeçalho, é enviado em cada pacote. Quando o pacote chega ao roteador, o mesmo abre o cabeçalho do pacote, verifica o endereço IP de destino e faz o encaminhamento do pacote para outro roteador na vizinhança. Por outro lado, o endereço IP não é utilizado pela maioria dos protocolos de roteamento das MANETs.

Uma rede móvel *Ad Hoc*, basicamente pode implementar um protocolo de roteamento orientado a tabelas (proativo) ou iniciar o processo de descoberta sob demanda. No segundo caso a rota somente passa a ser conhecida após o início de uma transmissão pelo nó de origem (reativo).

Cada protocolo de roteamento em MANETs poderá vir a fazer uso de diferentes métricas e diferentes estratégias para conseguir determinar a melhor rota. Com base nas métricas e estratégias, os algoritmos conseguem definir a melhor rota para cada destino. Os protocolos de roteamento diferenciam-se entre si a partir da forma que realizam as funções de roteamento, principalmente quanto ao método de escolha pela melhor rota. Vários protocolos foram desenvolvidos para as MANETs. Esses protocolos, além de lidarem com as funções básicas de roteamento, devem lidar ainda com as limitações intrínsecas, assim como banda reduzida, quebra de links, mudanças na topologia, e altas taxas de erros.

A comunicação entre dois nós pode ser interrompida decorrente do desligamento de dispositivos, da degradação do nível de sinal recebido e da interferência eletromagnética, cada vez mais presente nas comunicações sem fios. Para esses casos, o processo de roteamento, deve implementar mecanismos capazes de reestabelecer nova rota. Também deve existir um mecanismo de gerenciamento de rotas com o objetivo estabelecer e manter uma rota ativa e válida até o fim da comunicação.

Os sistemas das Redes Móveis *Ad Hoc* são mais complexos do que os sistemas de Redes cabeadas (CORSON e MACKER, 1999) por possuírem características como:

- topologia dinâmica: os nós são se moverem arbitrariamente, permitindo mudanças constantes na topologia da rede;
- tamanho de banda: normalmente os enlaces das redes sem fio possuem capacidade menor que os enlaces das redes fixas;
- qualidade do sinal: em redes sem fio o sinal se deteriora na medida que enfrenta obstáculos ou os dispositivos se movimentam para fora da área de cobertura ou a intensidade das interferências aumenta;

- segurança física: as redes wireless, em geral, são mais sucetíveis a escuta, invasão e ataques em razão do meio utilizado para as transmissões. Os dispositivos de defesa, por outro lado, aumentam o *overhead* nas transmissões;
- consumo de energia: A maioria dos nós em uma MANET fazem uso de energia fornecida por baterias, ou seja, a conservação dessas baterias é fundamental para o correto funcionamento do sistema.

Características das camadas, física e de enlace, inerentes ao meio da comunicação sem fio como a vazão reduzida, o retardo elevado, a interferência, gerenciamento distribuído (os nós são autônomos) e a comunicação por interface aérea, dificultam o processo de obtenção de rota de um nó móvel em uma MANET, assim como a própria transmissão de dados (AMORIN, 2002). O que difere uma MANET de outras redes sem fios é que esta se estabelece no nível três do modelo RM-OSI. Camada esta responsável pelas atividades de roteamento de pacotes de um nó de origem para um ou mais nós de destino. No caso específico deste tipo de redes, cada nó móvel (*mobile station*) é também um nó (roteador da rede) e que deve implementar os protocolos de roteamento desta (CORDEIRO, 2002).

3.2 Organização dos Protocolos de Roteamento em uma MANET

Segundo (TANEMBAUN, 1996), os algoritmos de roteamento para redes infraestruturadas são divididos em duas classes principais: algoritmos não-adaptativos (estáticos) e algoritmos adaptativos (dinâmicos). Em ambos os casos são algoritmos pró-ativos, isto é, as rotas são estabelecidas de modo pró-ativos, antes do início efetivo da transmissão de dados.

Já em Redes Móveis *Ad Hoc*, em razão da mobilidade dos nós e topologia dinâmica, existe apenas a classe de algoritmos dinâmicos. Estes algoritmos, contudo, passam a assumir características pró-ativas, reativas ou híbridas, baseados nos algoritmos, Estado de Enlace (*Link State*) e Vetor de Distância (*Distance Vector*) (CORDEIRO, 2002). Na Figura 3.2, apresentada abaixo, são apresentados alguns algoritmos de roteamento que respresentam estas características.

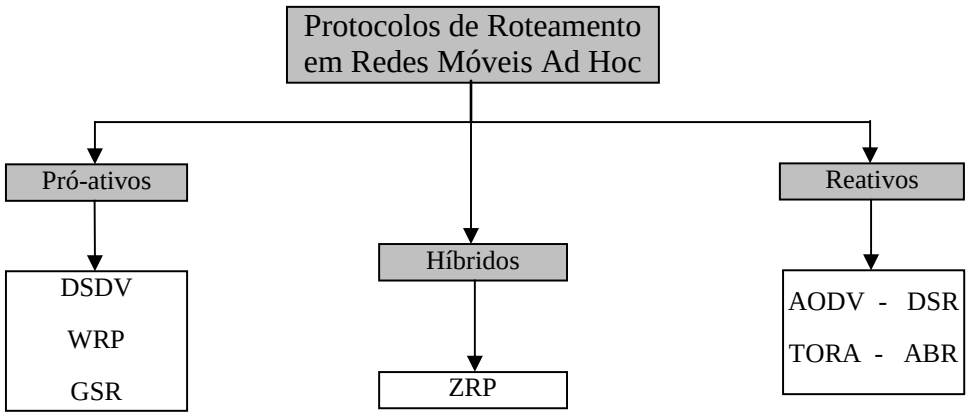


Figura 3.2: Organização dos Protocolos de Roteamento *Ad Hoc*

Throughput, atraso fim-a-fim dos pacotes de dados, capacidade de gerenciar e escolher a melhor rota, número de pacotes de controle para o funcionamento do protocolo *versus* porcentagem de pacotes entregues e tempo gasto na obtenção de uma

rota (principalmente em protocolos reativos), são propriedades que devem ser consideradas em uma análise quantitativa nos protocolo de roteamento para MANETs.

Por outro lado, o grupo IETF introduziu algumas propriedades qualitativas, tais como as apresentadas em Amorim (2002) a seguir:

- operação distribuída: propriedade que permite a operação autônoma e independente dos nós, evitando a centralização dos processos;
- operação baseada na demanda: o algoritmo adaptável às condições de tráfego, eliminando ou reduzindo o tráfego desnecessário, conseqüentemente aumentanto a eficiência energética assim como o uso da banda;
- operação pró-ativa: nos casos onde o consumo de energia e a largura de banda permitirem, é desejável que se utilize operações pró-ativas ao invés de reativas em função da latência adicionada pela operação baseada na descoberta de rota sob demanda;
- protocolos livres de loops: limitar o tempo que o pacote fica trafegando na rede. Pode-se utilizar uma variável do tipo TTL (*time to live*), assim como no TCP/IP ou um número de seqüência, que pode apresentar melhores resultados;
- segurança: mecanismos que inibam modificações não previstas nas operações dos protocolos devem ser implementados, visto que as MANETs são vulneráveis a diversas formas de ataque;
- operação nos períodos de "sonolência" do nó: os nós devem poder encaminhar pacotes de outros mesmo quando estes não estejam transmitindo e/ou recebendo dados, ou seja, durante um período de inatividade;
- suporte a enlaces unidirecionais: mesmo que muitos algoritmos sejam incapazes de funcionar corretamente sobre enlaces unidirecionais, estes podem ocorrer em redes *Ad Hoc*.

Ainda segundo Amorim (2002), além das propriedades qualitativas e quantitativas, é possível classificar as Redes *Ad Hoc* de outras maneiras, dependendo de suas características físicas e lógicas. No presente trabalho será apresentada uma característica com relação à filosofia de roteamento, uma com relação à construção das rotas e uma quanto ao tipo de relação entre o emissor e o receptor.

1) a filosofia de roteamento pode ser:

a. plano: nestas redes todos os nós são iguais, isto é, e implementam as mesmas funcionalidades e características do algoritmo.

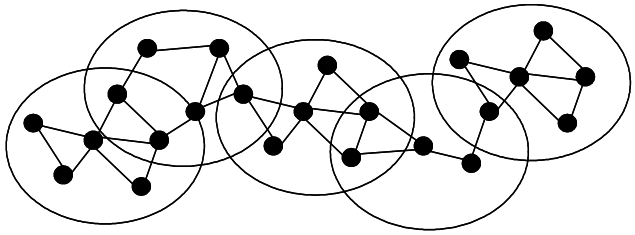


Figura. 3.3: Roteamento Plano

b. hierárquico: nestas redes, segundo Amorim (2002), os roteadores são divididos em zonas. Assim, cada roteador conhece todos os detalhes de roteamento para atuar corretamente dentro de sua própria zona, porém pouco ou nada conhece da topologia de outras zonas, justamente por estarem em zonas de níveis diferentes. Nesse roteamento existem ao menos dois níveis, podendo variar, dependendo da sua implementação. No nível mais baixo (primeiro nível), é onde os nós próximos geograficamente criam redes ponto-a-ponto. Neste nível ao menos um nó é utilizado como gateway para o nível acima. Os nós gateway, situados na borda de cada zona, normalmente incorporam maior poder de transmissão e recepção. A Figura 3.4 ilustra um roteamento hierárquico. O nível mais alto (segundo nível) pode atuar de modo semelhante a um Sistema de Distribuição (DS) de uma WLAN. Pode simplesmente aumentar a área geográfica de cobertura ou atuar como um backbone entre as zonas de nível 1.

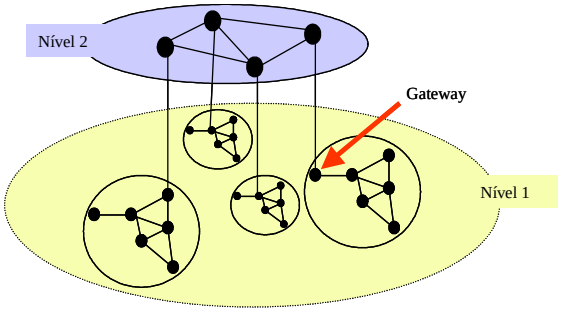


Figura 3.4: Roteamento Hierárquico

2) No processo de Obtenção e Manutenção e Remoção das Rotas os algoritmos podem ser (a) reativos ou sob demanda, (b) pró-ativos ou baseados em tabelas e (c) híbridos:

a. nos protocolos reativos ou sob demanda, um nó cria a rota para um determinado destino, somente quando necessita enviar dados a ele e ainda não possui tal rota. Atrasos decorrentes da obtenção da rota, antes de iniciar a transmissão de dados, são esperados, contudo estes protocolos possibilitam significativa economia de banda e de energia elétrica (CORDEIRO, 2002);

b. nos protocolos que são baseados em tabela, conhecidos como pró-ativos, todos os nós atualizam a sua tabela de roteamento de forma periódica e as mantém armazenadas localmente, para que estejam disponíveis e para uso imediato quando solicitadas pelo nó, reduzindo assim, o atraso inicial (CORDEIRO, 2002);

c. os protocolos híbridos permitem que os nós implementem ambas as construções ou que uma parte dos nós faça atualização periódica e a outra trabalhe de forma reativa. Esta estratégia busca implementar, em um único protocolo de roteamento, as vantagens dos algoritmos reativos e pró-ativos (CAMARA e LOUREIRO, 2004).

3) Quanto ao tipo de relação entre o emissor e o receptor os algoritmos de roteamento, segundo Cordeiro (2002), podem ser:

a. *unicast*, quando um único host emissor envia mensagens para um único *host* receptor;

b. *multicast*, como uma técnica usada para enviar cópias de um mesmo pacote a um subconjunto de todos os possíveis destinatários.

3.2.1 Protocolos de Roteamento Sob Demanda ou Reativos

Nessa categoria de protocolos, os nós não conhecem rotas a algum detino até que uma tentativa de comunicação seja iniciada, isto é, o nó de origem não conhece rotas para alcançar qualquer nó de destino. Essa é uma característica desejável para dispositivos móveis que possuem um *throughput* baixo e/ou pouca capacidade de memória e processamento. Assim, quando um terminal móvel requer uma rota, este dá inicio a um processo que é denominado obtenção de rotas. Esse processo é iniciado pela origem, ou seja, o emissor e termina com a obtenção da rota para o destino, quando o nó destino é encontrado, quando um nó intermediário conhece uma rota para o destino ou quando todas as rotas possíveis foram testadas e o destino não foi alcançado. Quando uma nova rota é estabelecida, outro procdimento é iniciado. Esse procedimento é conhecido como manutenção de rotas e deve manter as rotas ativas até que um link seja quebrado, invalidando a rota ou até que a comunicação esteja concluída. Não há troca de mensagens relacionadas ao roteamento enquanto não houver um nó querendo iniciar uma transmissão. Essa característica gera uma redução no tráfego da rede e no consumo de bateria. Por outro lado esses algoritmos provocam um atraso inicial, decorrente do descobrimento da rota (CORDEIRO, 2002). A seguir serão descritos alguns dos principais protocolos de roteamento reativos.

3.2.1.1 Dynamic Source Routing (DSR)

O DSR, apresentado em (JOHNSON, D.B.; MALTZ, D.A., 1996) é tido como o exemplo mais puro de algoritmo de roteamento pela origem (*Source Routing*). Nesse tipo de roteamento o nó de origem determina qual a rota que pela qual o pacote deve seguir pela rede. Cada nó mantém as rotas que aprendeu em *cache* com o objetivo de otimizar o processo de descoberta das rotas. Quando um nó é consultado quanto a uma determinada rota e esta estiver armazenada em *cache*, o nó de origem passa a utilizá-la imediatamente reduzindo o tempo de atraso decorrente do processo de descoberta de rota. O DSR considera que o diâmetro (distância entro os nós mais distantes) da rede seja pequeno e que a velocidade dos nós seja moderada de modo a reduzir o número de descoberta de novas rotas e, consequentemente, pouca manutenção das já existentes. O nó de origem armazena em *cache*, o registro da rota (*route record*), com uma lista de todos os nós intermediários de uma rota. Esse registro é adicionado ao cabeçalho de todas as mensagens que são enviadas (apenas) para o primeiro nó indicado na lista, este para o segundo e assim até que o nó destino seja alcaçado.

O funcionamento do protocolo consiste basicamente de duas fases principais: (a) descoberta da rota e (b) manutenção da rota (TOH, 2002).

a. na fase de descoberta da rota, o nó de origem consulta primeiramente aos seus vizinhos consultando as rotas que os mesmos possuem armazenadas em *cache*. Se uma rota ao destino solicitado existir, a origem passa a utilizá-la, concluindo a fase de descoberta. Caso contrário é aplicado o protocolo de descobrimento de rotas para encontrar uma rota válida para o destino. O processo de descoberta sempre é inicializado a partir do envio de pacotes do tipo *route request* em *broadcast* pela rede. A mensagem *route request* contém o endereço do nó destino e um número de identificação único. Cada nó que receber a mensagem verifica se conhece uma rota ao destino. Caso não conheça, insere o seu próprio endereço no registro da rota da mensagem *route*

request e o encaminha pelos seus links de saída. Uma mensagem *route reply* destinada ao nó de origem é gerada se algum nó intermediário conhecer a rota solicitada ou se o nó de destino foi alcançado, quando alcançado. O pacote *route reply* contém o *route record* necessário para o nodo de origem iniciar a transmissão de dados. Se duas requisições de rotas chegarem ao mesmo tempo ao nó de destino, a rota a ser escolhida será aquela que for composta pelo menor número de nós intermediários ou por aquela que apresentar o menor custo.

b. A fase de manutanção é iniciada quando da ocorrência de erros. Sempre que ocorrer um erro em qualquer rota, um pacote do tipo *route error* é enviado. Quando algum nó receber a mensagem de erro, primeiramente verifica se possui algum registro para a rota contida na mensagem e a exclui da memória. A mensagem de erro é enviada sempre que for identificado um link quebrado ou o destino se tornar inalcaçável.

O DSR apresenta desvantagens como a utilização de inundação (*flooding*) no processo de descoberta de rotaso que gera problemas de escalabilidade típicos desse mecanismo e a aplicação de enlaces unidirecionais. No modelo de enlaces unidirecionais, as interfaces trabalham em modo promíscuo, permitindo que todas as informações sejam acessadas a partir de um nó qualquer, estando ou não direcionadas a ele. Isso ocorre uma vez que o nó precisa obter todas as informações possíveis sobre as rotas e não recebe mensagens do tipo *route reply* com informações da rota (*route record*) e que a proximidade dos nós não garante que um enlace esteja ativo. O modo promíscuo permite que qualquer pessoa tenha acesso aos dados que são encaminhados de e para o nó.

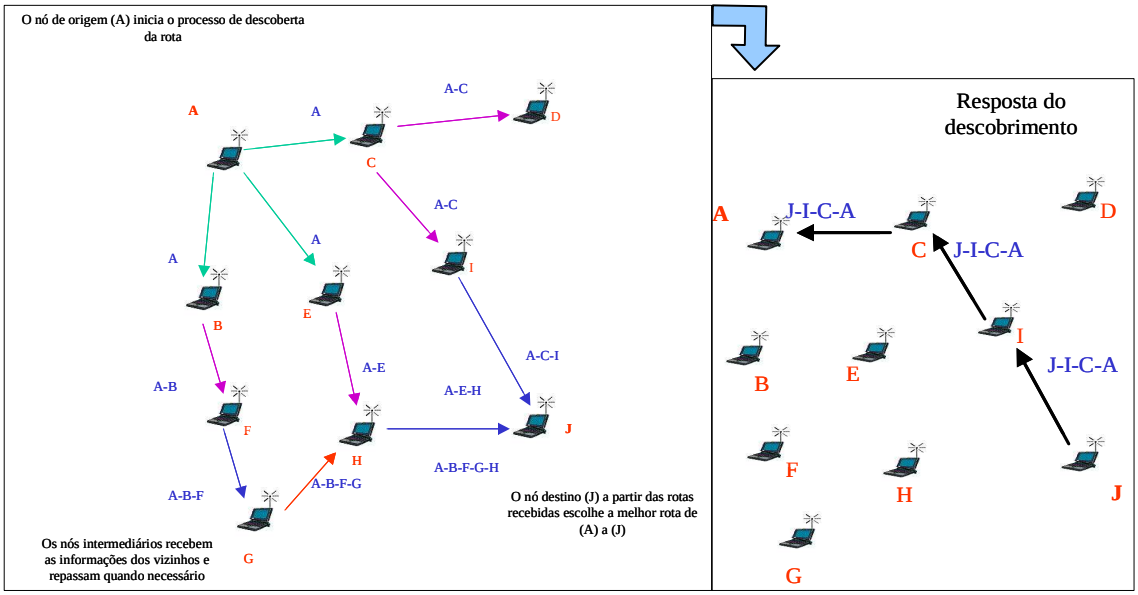


Figura 3.5: Requisição a resposta ao pedido de obtenção de rota. A é o nó de origem enquanto o nó de destino é o J

A principal vantagem do protocolo DSR é a utilização do algoritmo do tipo reativo, o qual permite economia de banda e de consumo de energia elétrica já que não necessita atualizar as informações dos nós continuamente e também por realizar descoberta de rotas sob demanda.

3.2.1.2 Ad Hoc On-Demand Distance Vector Routing (AODV)

O protocolo AODV descrito em (PERKINS e ROYER, 1998) é semelhante ao DSR, é reativo, permite multicasting e foi baseado no destinatário - Sequenced Distance-Vector Sua diferença básica está em não suportar enlaces unidirecionais. No AODV são criados enlaces reversos. Estabelece as rotas a partir da origem até o destino, tomando por base o ID de pacotes *broadcast* do tipo RREQ. Com base nesse ID o nó de destino sabe a seqüência de nós que os pacotes do tipo RREP irão seguir, em rota reversa, até o nó de origem. Esse método também é útil para que não ocorram rotas com loops (CORDEIRO, 2002).

O AODV minimiza o número de *broadcasts* através da criação puramente sob demanda das rotas. O AODV não armazena informações nem troca tabelas de roteamento entro os nós da rede, nem mesmo nos momentos de repouso. Segundo TOH (2002) este protocolo suporta apenas *links* simétricos com duas fases diferentes:

- Descobrimento e Manutenção de Rota;
- Encaminhamento de dados.

Quando um nó origem deseja enviar uma mensagem ele inicia um processo de descobrimento de rota para alcançar o nodo de destino correspondente. O nó origem envia um pacote RREQ por *broadcast* para todos os vizinhos, que por sua vez encaminham para os seus vizinhos, repetindo o processo até encontrar o destino ou um nodo que possua uma rota atualizada recentemente para o destino. AODV utiliza números de seqüência do destino para se precaver contra a ocorrência de *loops* nos nós contidos na rota e também para garantir que possuam a informação de rota mais recente. Cada nó mantém o seu próprio número de seqüência assim como um ID de *broadcast*. A cada novo RREQ o nó deve incrementar o ID de *broadcast*, que, juntamente com o endereço IP do nodo, identifica de forma única cada um dos RREQs que circulam na rede. Junto ao número de seqüência e o ID de *broadcast* do nodo, o RREQ inclui o número de seqüência mais recente que possui do destino. Pacotes RREQs respondidos por nodos intermediários somente são válidos se possuírem uma rota ao destino e o número de maior ou igual ao contido no RREQ recebido (CORDEIRO, 2002).

Durante o processo de descoberta de rotas, ocorre o encaminhamento do RREQ. Nesse processo, todos os nós intermediários armazenam em sua tabela de roteamento os endereços dos vizinhos dos quais recebem a primeira cópia do pacote RREQ em *broadcast*. Esse armazenamento dá condição de se estabelecer um caminho reverso. Se cópias em duplicata do mesmo RREQ são recebidas, são simplesmente descartadas. Uma vez que o RREQ atingiu seu destino, ou um nodo intermediário que possua uma rota atualizada recentemente para o destino, este nodo responde por *unicast* um pacote "route replay" (RREP) pelo caminho reverso. Os nodos ao longo desse caminho atualizam as rotas de encaminhamento em suas tabelas de roteamento que apontam para o nodo de onde vem o RREP. Essa atualização indica a rota de encaminhamento ativa. A cada atualização de rota, está associado um temporizador de rota que causa a deleção desta se a mesma não for utilizada durante um tempo de vida específico. O AODV foi projetado para suportar apenas *links* simétricos. Condição fundamental, já que o RREP é enviado obrigatoriamente pelo caminho estabelecido pelo RREQ (CORDEIRO, 2002).

No processo de manutenção das rotas, o nó de origem deve executar um novo processo de descoberta de rota sempre que a topologia da rede sofrer alguma alteração. Se um nodo se mover, mudando a sua posição na topologia da rede, este deve notificar

aos seus vizinhos que estão na direção do nó de origem, atravéz da propagação de mensagens RREP com métrica infinita, notificando a quebra do *link* e, consequentemente da rota. Esse processo é repetido até que o nodo origem seja notificado. A partir desta notificação o nodo de origem passa a executar um novo processo de descoberta de rota. Isso se a rota ainda for necessária (TOH, 2002).

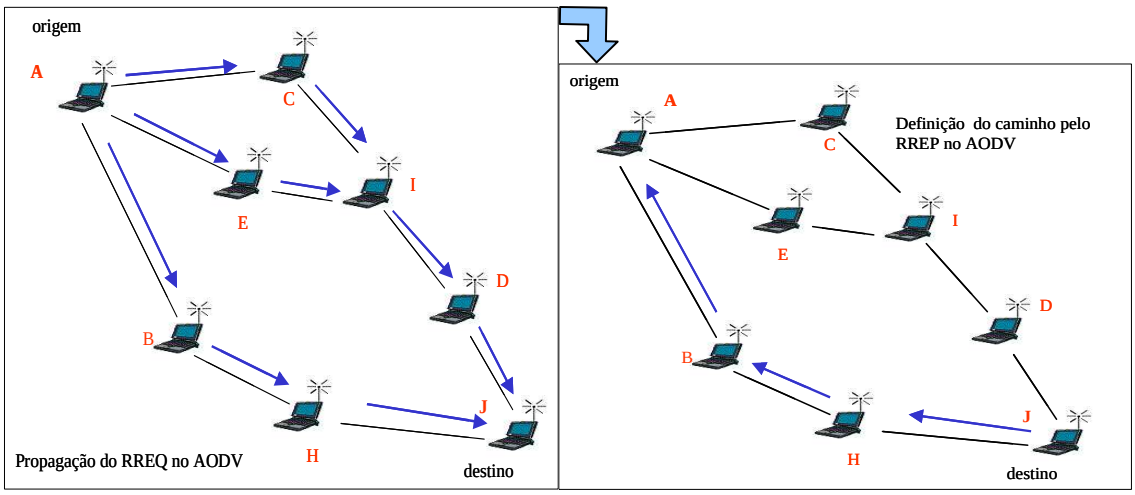


Figura 3.6: Exemplo de requisição de rotas e de uma resposta à esta requisição no AODV

3.2.1.3 Temporally – Ordered Routing Algorithm (Tora)

O TORA (TOH, 2002) é um algoritmo de roteamento distribuído, adaptativo e livre de loops. Assim como o AODV, este algoritmo também é baseado no conceito de *link* reverso. Suporta redes com grande mobilidade e, mesmo assim, sofre pouco impacto decorrente das mudanças topológicas da rede. O TORA tolera a escolha de rotas que não sejam as melhores rota e a possibilidade de existência de várias rotas da origem até o destino. A estratégia da concepção do TORA está centrada no alcance restrito das mensagens de controle a um grupo reduzido de nós. Normalmente aos seus vizinhos mais próximos (*one-hope nodes*), de onde ocorreu a mudança na topologia. Para isso, os nodos precisam manter informações de roteamento atualizadas sobre o estado dos nodos vizinhos, mesmo enquanto não houver solicitação de rotas. O protocolo organiza as suas rotas a partir de três funções básicas: criação, manutenção e deleção.

Durante as fases de criação e manutenção das rotas, os nodos utilizam uma métrica de altura (quantidade de saltos) que possibilita a criação de um grafo acíclico apontando para o destino, a partir do nodo de origem. Esse grafo é composto por todos os enlaces intermediários que interligam a origem ao destino. Sempre que um nó solicitar uma rota, ele envia um pacote de requisição informando o endereço de destino. Este pacote é propagado pela rede até que alcance o nó de destino ou a algum nó que conheça essa rota. O nó alcançado envia uma resposta à origem informando a sua altura, em número de saltos, em relação ao destino. Cada nó indicado pelo grafo irá ajustar a sua altura (a quantidade de saltos do nó em questão até o destino) a um valor maior que o do vizinho de quem recebeu a resposta. Depois de concluídas as estapas, um grafo com valores decrecentes direcionam a rota partindo do nó de origem até o nó de destino (TOH, 2002).

Um nó, ao detectar que uma rota já não é mais válida, deve iniciar o processo de manutenção de rota. Esse processo consiste em ajustar a sua altura em relação aos seus vizinhos de modo a garantir que seja a maior em relação a eles. No momento em que

este nó receber a resposta, o nó terá o valor correto de sua altura. A fase de manutenção é idêntica a fase de obtenção de rota.

Quando um nó detecta uma fragmentação na rede deve imediatamente dar início ao processo de deleção de rotas, removendo assim as rotas que já não são mais válidas.

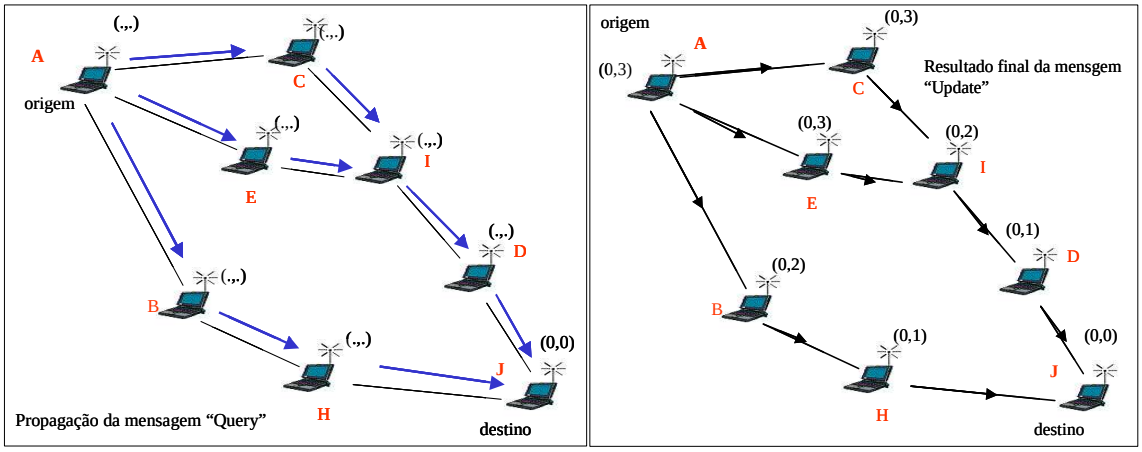


Figura 3.7: TORA nas etapas inicial e final de manutenção de rotas

O TORA, embora robusto e eficiente, apresenta um dos piores resultados de desempenho entre os algoritmos pertencentes a esta classe, em redes com mais de trinta nós (CORDEIRO, 2002). O resultado apresentado indica sérios problemas de implementação uma vez que se mostrou incapaz de gerenciar o seu próprio tráfego.

3.2.1.4 Associativity - Based Routing (ABR)

O protocolo ABR também faz uso do método de roteamento pela origem. Este protocolo somente mantém rotas aos nós de destinos enquando os nós de origem as estiverem utilizando. Para que um nó encontre uma rota válida ao destino desejado deve iniciar o processo de descoberta e esperar que o destino lhe aponte os nodos intermediários para alcançá-lo. O nó de origem inunda a rede com um pacote "*query*", enquanto o nodo destino, quando identificado, responde com uma mensagem "*query-replay*". A melhor rota é selecionada pelo destino, que deve considerar métricas de associatividade em suas escolhas. Estas métricas procuram informar a melhor rota encontrada no caminho mais curto, considerando para tal, a estabilidade dos links intermediários e também no menor número de saltos entre os nós origem e destino.

O Segundo Toh (2002), o protocolo de roteamento ABR não requer freqüentes atualizações de rotas. Por outro lado, define que o protocolo considere o grau de associatividade como métrica básica no processo de definição das rotas. A métrica de associatividade é calculada a partir da geração de mensagens de controle (*beacons*) a serem transmitidos de tempos em tempos na rede. O grau de associatividade é mantido em cada nó e, cada vez que este ouvir um *beacon*, incrementa o contador de associatividade referente ao nó que gerou o sinal. As rotas com o maior valor no grau de associatividade indicam uma maior estabilidade. Assim, quando um nó pouco se move, tende a manter a topologia inalterada, implicando em um aumento na estabilidade. Cada nó, a partir da sua tabela de associatividade/estabilidade, classifica os *links* dos seus vizinhos como estáveis ou instáveis. Com este mecanismo o protocolo pode encontrar rotas com tempo de vida maior. O ABR, na definição do grau de associatividade, se baseia em dados como atraso, potência do sinal, duração da bateria,

tráfego, período de atividade e características temporais e espaciais, coletados a partir dos *beacons* e outros pacotes..

Segundo Toh (2002), o ABR pode ser organizado em três fases: descobrimento da rota, reconstrução ou reparo da rota e deleção de rotas. Quando uma rota é requisitada e se não existir informação da mesma na memória *cache*, a fase de descobrimento de rotas é iniciada. Nessa faze, o nó faz requisitante inicia uma difusão da requisição para os nós vizinhos. Cada vizinho, ao receber essa requisição, verifica se ele é o nó de destino. Se não for, o seu endereço é incluído no pacote, juntamente com o valor de sua associatividade com os vizinhos. O pacote é então novamente enviado aos vizinhos até que o nó de destino seja localizado. Cada mensagem é enviada apenas uma única vez. O nó sucessor deve substituir as informações de associatividade do nó anterior, com as suas, assim como informar o caminho percorrido. O destino, poderá então, escolher a melhor rota, apenas considerando a associatividade de cada nó. Na figura 3.8 três rotas são possíveis: 1ª) 1-5-10-14-15, 2ª) 1-5-4-12-15 e 3ª) 1-2-4-8-13-15. Neste caso, a terceira rota é escolhida em função da porcentagem de *links* estáveis.

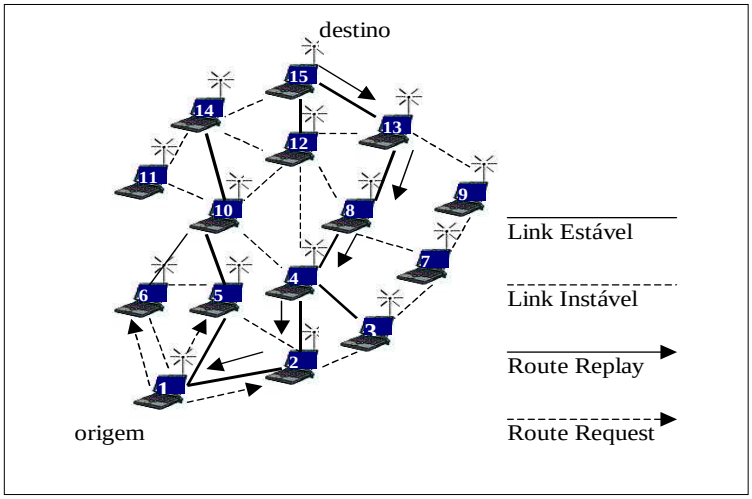


Figura 3.8: Descobrimento de Rota no ABR

Se o mesmo grau de associatividade for informado por duas rotas distintas, será escolhida a que possuir o menor número de nós. O nó de destino, ao escolher uma rota, envia uma mensagem de resposta por este caminho em direção ao nó de origem. Os nós pertencentes ao caminho escolhido marcam esta rota como válida.

No caso de um *link* romper, a fase de reconstrução das rotas será dada por um descobrimento de rotas parcial ou por um novo processo de descobrimento de rota, caso não consiga estabelecer uma rota válida a partir do link quebrado. No caso de um rompimento do *link*, o nodo envia um pacote *RouterRepair* em *broadcast*, chamado *Local Query* com um tempo limitado TTL. O *link* rompido é ignorado localmente sem inundar a rede com uma nova mensagem query em *broadcast*. No caso do nó de origem se movimentar provocando uma alterção na topologia, um novo processo de descoberta de rotas é iniciado, e uma mensagem é enviada aos nós da rota indicando que devem apagar a rota antiga. Quando acontece uma movimentação do nó de destino, o nó imediatamente anterior verifica se existe uma rota utilizando outro nó e, se existir, o nó destino responde ao solicitante a nova rota utilizando o melhor caminho. Se não for possível encontrar o nó de destino, o processo de descoberta é reiniciado a partir do nó imediatamente anterior. Se o processo voltar em rota reversa até o nó de origem, é iniciado um novo processo de descoberta de rota. Com base na figura 3.8, se o *link* 8-

13-15 romper o nodo 8 inicia um "*Local Query*" por difusão e determinará a nova rota como sendo 8-12-15.

A fase de deleção de rota é realizada a partir do momento em que uma rota já não é mais necessária. Uma mensagem de deleção de rota "*RouteDelete*" é enviada por *broadcast* para todos os nós intermediários de modo que esses possam atualizar suas tabelas retirando a rota indicada mesmo se estes se moverem durante a execução do processo.

O ABR, segundo Toh (2002), implementa conceitos como:

- associatividade e recuperação de rotas;
- implementa parâmetros de QoS.

Muito embora o ABR permita o uso de parâmetrosde de QoS, como atraso, qualidade do link e largura de banda na seleção de rota, esse protocolo apresenta as mesmas limitaçõe dos demais algoritmos sob demanda.

3.2.1.5 Location-Aided Routing (Lar)

O protocolo LAR faz uso da localização geográfica dos nós através do sistema GPS (*Global Positioning System*), como estratégia para fundamental no processo de descoberta de uma rota. Com o uso do GPS, a área para pesquisa de uma nova rota é reduzida a uma pequena zona geográfica, pois toma como base a localização geográfica do próprio nó de destino. Com uma área menor de circulação dos pacotes de obtenção de rota, o tráfego de sinalização diminui.

Esse protocolo, por outro lado, define dois conceitos: (a) "*Expected Zone*" e (b) "*Request Zone*". O protocolo LAR assume que o emissor possui conhecimentos avançados sobre a localização e velocidade do destino. Baseado na localização e velocidade, a "*Expected Zone*" pode ser definida. A "*Request Zone*" compreende a zona onde se encontra o emissor e a "Expected Zone". Usando o processo de inundação (*flooding*) na rede, o protocolo envia um pacote de requisição da localização de um nó. O destino, ao receber o pacote com a requisição, retorna, através dos nós intermediários, um pacote contendo as informações necessárias para que uma rota entre o nó de origem e de destino seja estabelecida (TOH, 2002).

Existem duas variações para LAR (AMORIN, 2002), o LAR1 e o LAR2. O LAR1, implementa uma zona de requisição (*Expected Zone*), que pode conter o destino. Cada nó, ao receber uma requisição de rota, verifica se está dentro da "*Request Zone*". Se estiver, envia este pacote para os seus vizinhos e, caso contrário, ignora os pacotes. A Figura 3.9 demonstra a "*Request Zone*" em uma rede LAR1. A zona de requisição é representada por um retângulo. O nó de origem "A" envia um pacote de requisição de rota para os vizinhos B e D. Os dois nós recebem uma cópia do mesmo pacote, porém o nó B o descarta por não fazer parte da zona de requisição. O nó D, por fazer parte da "*Request Zone*", encaminha a mensagem para os seus vizinhos, já que D não é o nó destino. Para esse caso, o pacote de descoberta de rota continua percorrendo a rede até que chegue ao seu destino ou um pacote de erro seja retornado.

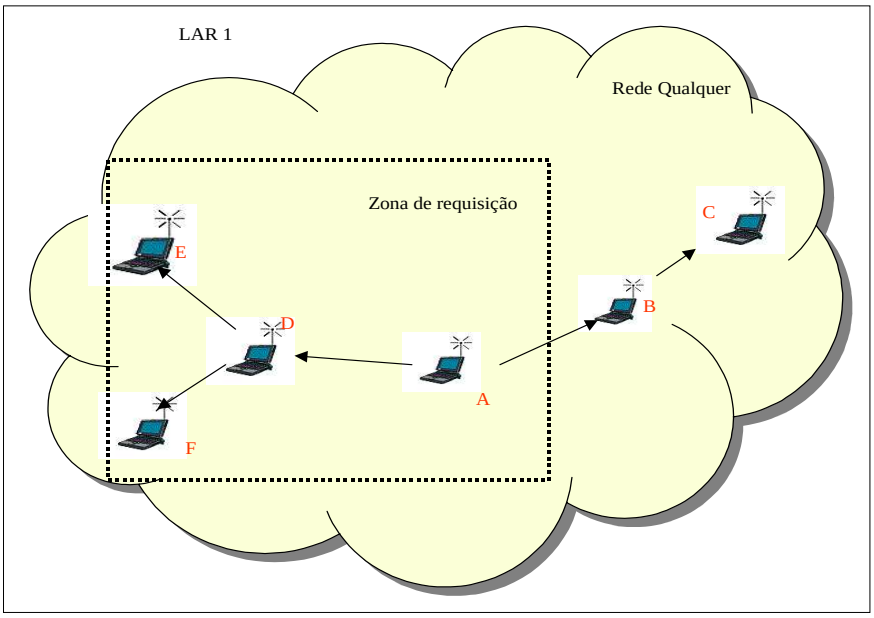


Figura 3.9: LAR esquema 1

Na variação LAR2 é considerado que o pacote de descoberta de rota conheça previamente as coordenadas do na de destino, bem como uma estimativa da distância que este pode estar dessa coordenada. As duas informações são usadas pelos nós intermediários para identificar a zona onde o nó de destino pode ser encontrado. Cada nó, com base nas informações do pacote de descoberta recebido, verifica se está geograficamente mais próximo do destino do que o nó anterior, ou seja, o nó que o enviou (AMORIM, 2002). Se estiver mais próximo, reenvia o pacote em *broadcast* para seus vizinhos e, caso contrário, descarta o pacote (vide Figura 3.10).

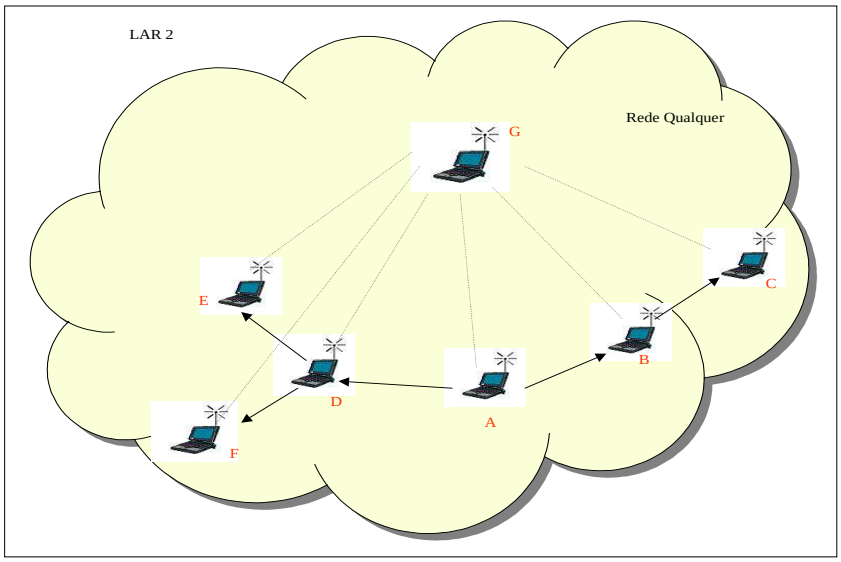


Figura 3.10: LAR esquema 2

3.2.1.6 Light Wight Móbile Routing (LMR)

Este protocolo estabelece uma rota para o nó de destino com base em um grafo acíclico relacionando os nós intermediários entre os nós origem e destino. O LMR é embasado no protocolo de link reverso, suporta múltipls rotas ao mesmo destino,

possuir baixo *overhead*, possui bom funcionamento em redes com mobilidade moderada e não necessita iniciar um novo processo de descoberta de rota até que todas as rotas conhecidas falharem.

Cada nó pertencente a esta rede conhece e mantém informações sobre os seus vizinhos diretos. Quando um pacote de requisição de rota é recebido o nó verifica se ele é o destino ou se conhece uma rota válida até ele. Caso este não seja o nó destino e também não conhece uma rota para o mesmo, o pacote de requisição é repassado para os vizinhos do nó em questão até que o destino seja alcançado. Quando o destino é alcançado ou, uma mensagem de retorno (*RouteReplay*) é enviada no caminho reverso.

O processo de manutenção de rota, por sua vez, somente é executado quando o nó de origem não possuir mais nenhuma rota válida para o destino. Quando isso ocorrer, o nó em torno dos *links* quebrados evia uma mensagem de erro (*RouteError*) aos seus vizinhos. Os vizinhos são informados que não existem mais rotas válidas ao nó de destino e um novo processo de descoberta de rota é iniciado.

O principal problema deste protocolo é a tendência de tempo ilimitado para se recuperar de fracionamentos da rede, mostrando, assim como o TORA que é incapaz de gerenciar o seu próprio tráfego.

3.2.2 Protocolos de Roteamento *Unicast* Pró-Ativos

Protocolos de roteamento pró-ativos em MANETs, são similares aos encontrados em redes infraestruturadas. Protocolos deste tipo procuram manter consistentes as informações topológicas da rede, mesmo em períodos de inatividade. As atualizações são realizadas em períodos de tempo pré-definidos pelo protocolo ou quando um nó percebe alguma mudança na topologia, permitindo a consistência das rotas válidas na rede em cada nó. As informações da toplogia, ou seja, as rotas aos destinos válidos da rede são armazenadas nas tabelas de roteamento presentes em cada nó da rede e trocadas entre os si constantemente. Consequentemente os protocolos pró-ativos requerem mais recursos de memória e banda. Protocolos pró-ativos diferem quanto número de tabelas de roteamento necessárias para a armazengem das informações assim como pelos métodos de propagação destas informações (ROYER, 1999). O método de roteamento pró-ativo apresenta sua maior vantagem no processo de disponibilização de rotas, sendo que estas estarão disponíveis a qualquer momento para uso imediato. O tempo gasto no processo de descoberta de uma rota é muito pequeno, já que este foi previamente executado. Embora existam diversos protocolos pró-ativos, o presente trabalho apresenta os que melhor representam essa estratégia.

3.2.2.1 Wireless Routing Protocol (Wrp)

O protocolo WRP (CORDEIRO, 2002) é um protocolo pró-ativo orientado a tabelas com o objetivando manter informações de roteamento ao longo de toda a rede. O WRP exige que o fluxo de informações seja livre de loops, para tanto, apresenta uma importante exceção em relação à classe de olgoritmos a que pertence. Este protocolo evita o problema de contagem ao infinito, fazendo com que cada nodo execute checagens consistentes das informações dos seus predecessores repassadas por seus vizinhos. Desse modo, além de evitar situações de loop, possibilita rápida convergência de rotas decorretes da falhas em links.

No WRP os nodos são informados sobre a existência dos seus vizinhos pelo recebimento de “ACK´s” e outras mensagens. Se um nodo não está enviando mensagens ou dados, ele deve enviar uma mensagem do tipo “*hello*” para garantir

conectividade, já que a falta de mensagens do nodo indica a falha do *link*, podendo causar um falso alarme. Quando um nodo recebe uma mensagem do tipo "*hello*" de um nodo novo, este novo nodo deve ser adicionado à tabela de roteamento do nodo móvel e este deve enviar uma cópia das informações contidas em sua tabela de roteamento ao nodo novo (TOH, 2002). O *link* é considerado quebrado quando um nó não receber qualquer tipo de mensagem por um longo período de tempo.

Cada nó da rede deve implementar e manter quatro tabelas: tabela de distância, tabela de custo do *link,* tabela da Lista de Retransmissão de Mensagens (MRL) e a tabela de roteamento. Cada entrada da MRL é composta pelo número de seqüência da atualização da mensagem, um contador de retransmissão, um vetor de flags com uma entrada para cada vizinho conhecido e uma lista de atualizações enviadas. Os registros MRL com atualizações em uma mensagem de atualização precisam ser retransmitidos e os vizinhos necessitam confirmar a retransmissão.

Para garantir a fidelidade das informações de roteamento, os nós, periodicamente enviam mensagens de atualização, informando aos demais sobre mudanças no *link*. As mensagens de atualização são trocadas somente entre nodos vizinhos, assim como uma lista informando quais nós devem confirmar o recebimento da atualização (ACK). Após processar as alterações dos vizinhos ou detectar uma mudança em um *link,* os nodos móveis enviam mensagens de atualização para seus vizinho, menos para o vizinho de onde veio a mensagem. Quando um *link* entre dois nodos é perdido, estes devem enviar mensagens de atualização aos seus vizinhos. Estes vizinhos alteram as suas entradas na tabela de distâncias que por sua vez apresenta possíveis rotas alternativas, passando por outros nodos. Todas as rotas novas são enviadas de volta para os nodos origem, de forma a possibilitar as alterações apropriadas (TOH, 2002).

3.2.2.2 Destination-Sequenced Distance-Vector (DSDV)

O DSDV é um protocolo livre de *loops* implementado a partir do uso de tabelas, com base no algoritmo de roteamento distribuído Bellman Ford. Cada nó que implementa o protocolo DSDV, mantém uma tabela de roteamento contendo rotas para todos os destinos possíveis e tamém o número de saltos (neste caso, o número de rádios) para cada um. Próximo salto, métrica (normalmente a quantidade de saltos) e o número de seqüência (estabelecido pelo nó de destino) são os atributos considerados nas rotas para cada destino. Nesse tipo de protocolos as informações de roteamento estão sempre disponíveis para leitura, sem querer saber se algum nó necessita da rota ou não (TOH, 2002).

O número de seqüência é utilizado em cada tabela de roteamento para ordenar as informações de roteamento com o objetivo de evitar *loops*. Outra função do número de seqüência é servir como critério na seleção de uma rota. Será utilizada preferencialmente aquela rota que possuir um número de seqüência mais alto, permitindo que os hosts distingam aquelas rotas com maior estabilidade. Para os casos de conflito do número de seqüência a métrica passa a atuar como critério de desempate. Assim, a sequência que tiver a melhor métrica é utilizada e a outra poderá ser descartada ou armazenada como rota secundária, dependendo do seu estado (CORDEIRO, 2002).

Atualizações constantes são utilizadas para manter a consistência das tabelas de roteamento. Essas atualizações podem ser periódicas ou disparadas. Atualizações disparadas são usadas adicionalmente e de modo assíncrono, com o objetivo atualizar mudanças na topologia da rede o mais rápido possível. As atualizações periódicas são feitas em períodos pré-determinados pelo protocolo, buscando manter os valores das rotas sempre atualizados. Nas mensagens de atualização estão incluídos todos os

destinos que podem ser alcançados pelo nó, assim como o número de saltos até ele. Ao receber uma mensagem de atualização de rota, cada nó compara as informações contidas em sua própria tabela com as informações recebidas do nó vizinho. Rotas novas são imediatamente propagadas para os vizinhos enquanto que as rotas com números de seqüência mais antigos são simplesmente descartadas.

Quando um destino torna-se inalcançável ou um enlace se rompe, imeditamente todas as rotas afetadas são marcadas e anunciadas com um número de seqüência maior ou com uma métrica infinita. Esse evento faz com que o nó encaminhe uma mensagem de atualização, pois considera ser uma informação importante para a rede. Rotas com métrica infinita deverão rapidamente ser trocadas por outras e esta informação imediatamente propagada na rede (TOH, 2002).

Assim como no WRP, uma das maiores vantagens do DSDV é a implementação de rotas livres de *loop*. Como desvantagem, pode-se relacionar a excessiva sobrecarga na comunicação, provocada por inúmeras mensagens de atualizações de rotas disparadas e periódicas. Além disso, a sincronização centrada no destino implica no problema de latência, enquanto o número de seqüência impede o roteamento com múltiplos caminhos (CORDEIRO, 2002).

3.2.2.3 Global State Routing (GSR)

O GSR propõe um algoritmo de roteamento baseado no Estado de Enlace (*Link State*) que faz uso de mecanismos sofisticados e eficientes no controle do *throughput* assim como cálculos precisos de rotas, buscando a diminução do tamanho das tabelas de roteamento e implementando a capacidade de manipular parâmetros de QoS (CORDEIRO, 2002).

Neste protocolo, quando é detectada uma alteração na topologia existente, seja por destino inalcançável, quebra de link ou por qualquer outro problema que possa ocorrer, o nó deve preservar essa informação em uma tabela de topologia, juntamente com outras informações recebidas de seus vizinhos. Todas as informações coletadas são preparadas e disseminadas em períodos pré-determinados para os vizinhos de um salto de distância, evitando assim a disseminação das informações de roteamento por inundação. Cada nó implementa também outras tabelas assim como lista de vizinhos, próximo nó e distâncias. Todos os nós são inicializados com as tabelas vazias e, após inicializá-las, passa a “ouvir” o meio para “apredener” quem são os seus vizinhos e obter as informações necessárias (AMORIN, 2002). No intuito de reduzir o tamanho das mensagens de atualização utilizadas no GSR, duas técnicas são apresentadas: (a) Atualização Mais Recente (*Fresh Update*) e (b) Olho de Peixe (*Fisheye*).

a. Atualização Mais Recente: Essa técnica assume que o vizinho pode conter informações mais recentes do que o nó em questão. Com base nessa premissa cadanó limita-se a enviar apenas informações de mudanças, pois podem ser consideradas úteis. Nada é enviado se o nó não conseguir identificar tais informaçãoes. Segundo (AMORIN, 2002), para a impelementação desta técnica é imperativo que cada nó mantenha um Vetor de Números de Seqüência (VNS). Esse vetor, além de armazenar todos os destinos que estão na tabela de roteamento, indica a idade de cada informação já enviada. O nó de destino compara o seu VNS com os valores recebidos e, no caso da entrada ser mais antiga, a mensagem de atualização é descartada;
b. Olho de Peixe: técnica que recebeu este nome devido à semelhança que existe entre a representação desta topologia, (vide Figura 3.11) e o olho de um peixe.

Nesta técnica um grande volume de informações é trocado com os nós mais próximos (vizinhos de um salto), repassando todas as informações que o nó conhece. O volume de infomações trocadas entre os nós diminui em proporção inversa ao número de saltos, ou seja, quanto mais distante (em saltos) menor a quantidade de informações trocadas.

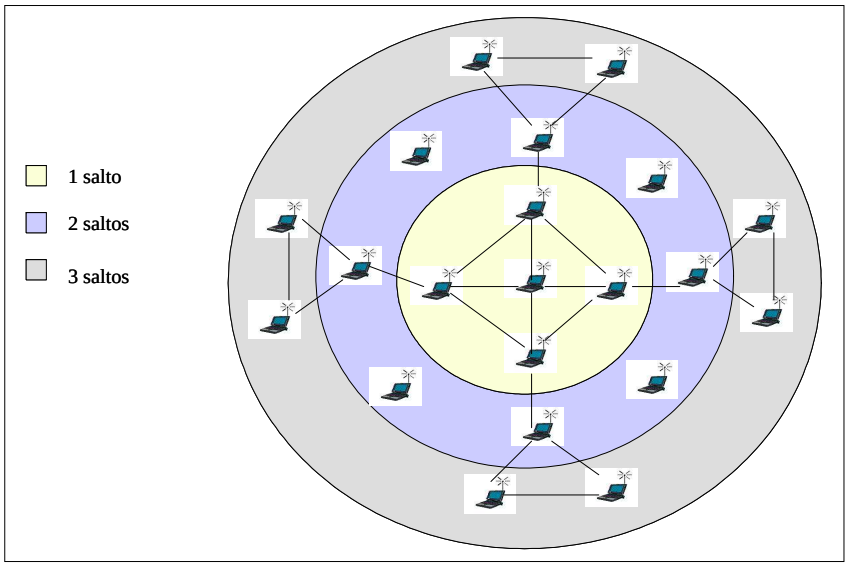


Figura 3.11 Técnica Olho de Peixe

Conforme ilustrado na figura 3.11, a quantidade de informações trocadas vai diminuindo à medida que os nós vão se afastando do nó mais ao centro do círculo central. O afastamento é contado em saltos e a cada salto a mais que as informações devem percorrer, é diminuído o volume e o tamanho dos pacotes. Este é um processo que promove a redução no consumo de energia e na largura de banda (AMORIN, 2002).

3.2.2.4 Cluster Switch Gateway Routing (CSGR)

O CSGR é um protocolo de roteamento baseado em tabelas e mantém os nodos móveis organizados em *clusters.* Em cada *cluster* existe a figura de um nodo cabeça o qual introduz uma forma de hierarquia (TOH, 2002). Um nodo cabeça pode gerenciar um grupo de nodos contidos no *cluster*, controlando os canais de acesso, as funções de roteamento e a alocação de banda. O nodo cabeça realiza as funções de controle e coordenação de todos os nodos presentes no *cluster*. O nodo cabeça é definido a partir de um algoritmo distribuído de eleição. Quando o nodo cabeça deixar de exisitr, se mover para fora da área de cobertura da rede ou se move por outros *clusters*, um novo processode eleição deve ser realizado com o objetivo de definir um novo nodo cabeça. Isso pode ser problemático se o nodo cabeça migrar entre *cluster*s com grande freqüência, uma vez que o processo consome banda e processamento.

O CSGR usa o esquema de roteamento do DSDV, entretanto introduz o recurso de roteamento hierárquico a partir da implimentação de um nodo cabeça, que, além de outras coisas, é o *gateway* do prórprio *cluster*. Todo a tráfego entre *clusters* é controlado pelo nodo cabeça. Desse modo, para que consiga comunicar, cada nó deve fazer parte de um *cluster* e conhecer o seu nodo cabeça (TOH, 2002).

A tabela dos membros do *cluster* é encaminhada a todos os membros do *cluster* em modo *broadcast* quando ocorrer qualquer mudança na tabela. Este encaminhamento é realizado com base no protocolo DSDV. Os nodos, ao receberem a mensagem de alteração, atualizam a sua tabela de roteamento. Cada nodo deve ainda, manter uma

tabela de rota utilizada para determinar o próximo salto para alcançar o destino (TOH, 2002).

Quando um nodo recebe um pacote o mesmo realiza uma consulta em sua tabela de roteamento para, a partir desta, determinar o nodo cabeça mais próximo que pode alcançar o destino.

3.2.3 Protocolos Híbridos

Os protocolos considerados híbridos são aqueles que procuram fornecer funções reativas e pró-ativas à mesma rede, podendo trabalhar de maneira complementar uma a outra. O funcionamento mais comum para este grupo de protocolos é aquele onde cada terminal define uma área de serviço, denominada zona considerando a sua potência de transmissão. Todo o nó, enquanto se mantém em sua zona, trabalha de modo pró-ativo, trocando as tabelas de roteamento com os seus vizinhos. Deste modo, todos os nós de uma determinada zona, possuem uma visão completa da topologia de sua área de abrangência. Quando as informações da rota requerida não são encontradas nas tabelas de roteamento contidas nos nós de uma zona, um processo de descoberta de rota em modo reativo é iniciado a partir do nó de origem. No modo reativo os nodos de borda das zonas são consultados, expandindo a consulta em um salto, até que o destino seja encontrado ou até que uma mensagem de erro seja encaminhada para o nó origem. Os protocolos híbridos, diferentemente dos demais protocolos, atuam de forma pró-ativa na área denominada intra-zona e de forma reativa restante da rede. Por serem protocolos ainda pouco explorados, o presente trabalho limita-se a apresentar aquele que é considerado o mais estudado desta categoria.

3.2.3.1 Zone Routing Protocol (Zrp)

No ZRP a zona é definida a partir de cada nó considerando aqueles nós que estão a uma distância mínima, medida em saltos, do nó em questão. Esta área de abrangência é considerada a intra-zona e normalmente é um número pré-definido de saltos, que é denominado como raio da zona. Quando o destino estiver dentro da zona do nó que iniciou a transmissão de dados, o pacote é imediatamente enviado com base na sua tabela de roteamento previamente estabelecidao. Quando o destino não estiver na intra-zona, o nó de origem consulta os nós da borda desta zona, solicitando uma rota para o destino. Uma mensagem de resposta afirmativa informando pelo nodo de borda caso este alcance o destino em sua intra-zona ou no caso de conhecer uma rota para ele. Caso nenhum nó de borda de uma determinada zona conhece uma rota ao destino solicitado, a mensagem passa a ser enviada para os nós da borda desta zona. Esse procedimento é repetido até que uma confirmação chegue ou até que uma mensagem de erro seja enviada ao nó de origem. O erro normalmente ocorre quando o número de saltos for excedido (CORDEIRO, 2002).

O ZRP, por ser protocolo híbrido, pode utilizar o melhor das abordagens reativas e pró-ativas. Enquanto na intra-zona, a descoberta de rota é extremamente rápida, diminuindo o atraso no início da transmissão de dados, pois as rotas já são previamente estabelecidas pela abordagem pró-ativa. Por outro lado, para alcançar os nós fora da sua zona, o algoritmo faz uso das vantagens da abordagem reativa, a qual possibilita economia significativa no consumo de energia e de banda reduzindo o tráfego do próprio protocolo.

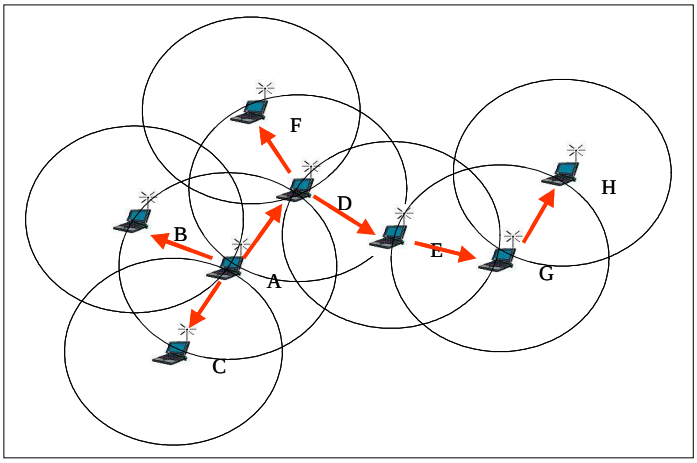


Figura 3.12: Exemplo de requisição de rota do nó A para o nó H

Conforme demonstrado na Figura 3.12 o nó A, por não possuir uma rota para H (H está fora da sua intra-zona), envia pacotes de requisições de rota para os nós da borda da sua zona, isto é, para os nós B, C e D. Estes, procuram em suas tabelas pelo destino. Como não encontram, a requisição é encaminhada aos nós da borda da sua zona. O process é reproduzido até que a requisição chegue ao nó destino, neste caso o nó G. Este, como possui uma rota para H, envia a requisição para o nó H, que estabelece a rota entre os nós origem e destino.

3.2.4 Protocolos de Roteamento *Multicast*

O multicast consiste em enviar pacotes de um transmissor para múltiplos destinos identificados por um único endereço, o endereço de grupo. Assim como nas redes cabeadas, *multicast* em MANETs também é uma tarefa complicada, porém ainda mais difícil, visto que, além dos problemas inerentes ao *multicast*, a topologia pode alterar freqüentemente. Portanto, os protocolos multicast devem considerar as alterações de topologia, inerente às MANETs, bem como as suas implicações. O *multicast*, pode ser visto como uma importante ferramenta na solução dos problemas de largura de banda das MANETs, por permitir significativa redução no envio em duplicidade de pacotes na rede. Segue abaixo, uma breve explicação dos protocolos MAODV e ODMRP, representantes da classe dos protocolos de roteamento *multicast*.

3.2.4.1 AODV Multicasting (MAODV)

O algoritmo de roteamento MAODV faz uso de mensagens similares às utilizadas em operações *unicast* do algoritmo AODV. Os nodos se inscrevem nos grupos multicast sob demanda criando, neste processo, a árvore *multicast*. A árvore consiste nos membros e nos nós do grupo conectados aos membros do grupo. Isso permite um nodo receptor se juntar a um grupo, mesmo se estiver a mais de um hop distante de um membro do grupo *multicast*. A operação do *unicast* do protocolo beneficia-se também da informação que é recolhida quando descobre rotas para o tráfego multicast, reduzindo o tráfego de sinalização da rede (CORDEIRO, 2002).

3.2.4.2 On-Demanda Multicast Routing Protocol (ODMRP)

O algoritmo ODMRP é um protocolo embasado na topologia *mesh*, a qual fornece objetiva fornecer uma conectividade mais rica entre os membros do grupo *multicast*. Com base em uma topologia mesh e possibilitando múltiplas rotas ao destino, os pacotes *multicast* podem alcançar os destinos, mesmo na ocorrência de movimentos do nó e de mudanças da topologia. Além disso, os inconvenientes de árvores do *multicast*

em redes *wireless* móveis (conexões intermitentes, reconfiguração freqüente da árvore, concentração de tráfego, etc.) são evitados. Para disponibilizar uma topologia *mesh* para cada grupo *multicast*, o protocolo ODMRP usa o conceito de encaminhamento em grupo. O encaminhamento de grupo é formado a partir de um conjunto de nós responsáveis pelo encaminhamento de dados *multicast* através de rotas mais curtas entre um par de membros. O ODMRP também aplica técnicas de roteamento sob demanda para evitar sobrecarga do canal e incrementar escalabilidade. Nenhuma mensagem de controle adicional é necessária para sair de um grupo (CORDEIRO, 2002).

3.3 COMPARAÇÕES dos protocolos DE ROTEAMENTO *AD HOC*

Nos dias de hoje, a importância dos sistemas de comunicação sem fio, bem como a necessidade de integração desses sistemas com os sistemas cabeados fica cada vez mais evidente. Também se percebe uma tendência para sistemas com suporte à mobilidade, uma vez que, cada vez mais, surge a necessidade das aplicações e dados acompanharem os usuários por onde estiverem. Também é importante salientar que um novo tipo de usuário está cada vez mais presente, o usuário nômade. Estes usuários, além de necessitarem das informações no local onde estiverem, seguidamente precisarão de aplicações que os acompanhem e que permaneçam em funcionamento, mesmo quando estes mudarem de rede ou de ponto de inserção à rede. A partir destes pontos, podemos também perceber que ainda existem vários problemas a serem resolvidos para alcançar o estado da arte da comunicação sem fio para aplicações com suporte à mobilidade. A interligação de MANETs com redes infraestruturadas é um exemplo.

A partir da revisão dos protocolos de roteamento para Redes Móveis *Ad Hoc*, apresentada anteriormente nesse trabalho, pôde-se analisar as vantagens e desvantagens dos seus principais protocolos de roteamento. Cada protocolo de roteamento discutido no presente documento, possui características específicas que podem se tornar vantajosas ou não dependendo do ambiente a ser utilizado. Percebe-se também, uma grande preocupação em permitir ou implementar uma convergência transparente para os sistemas de comunicação cabeados. Percebe-se também que a integração de alguns ou de todos os modelos apresentados é desejada, uma vez que o usuário final se torna cada vez mais exigente e móvel.

A função de encaminhar pacotes entre as redes também é conhecida como função de roteamento ou comutação de pacotes. Em redes de computadores, esta função é crítica para a comunicação entre redes interconectadas, pois é fundamental que se considere os requisitos de confiabilidade, os quais exigem a possibilidade de rotas alternativas. Requisitos como QoS e segurança também são desejados. A função de roteamento também deve decidir a saída pela qual um pacote entrante deve ser transmitido (a melhor rota). O processo de seleção da melhor rota para o encaminhamento de pacotes, normalmente está apoiado em informações voláteis e dinâmicas. Esta característica pode gerar problemas de atraso, sobrecarga da rede e de escolha de uma rota errada, gerando instabilidades (HARTMANN, 1997).

Em função do limitado espectro eletromagnético, cada sistema de comunicação sem fio procura otimizar o seu acesso ao meio físico, visando prover maior vazão de dados. Para tanto buscam implementar protocolos cada vez mais eficientes e com melhor aproveitamento de canais de comunicação. Nas MANETs tais problemas são potencializados, uma vez que se trata de uma rede não infraestruturada onde os nós trabalham de modo independente e autônomo, porém com objetivos comuns. Em alguns sistemas, assim como na telefonia móvel de terceira geração, no WIMAX (IEEE-

802.16) e nas WLANs (IEEE 802.11), conseqüentemente, começam a surgir serviços e soluções cada vez mais concorrentes ou complementares. As WLANs normalmente são utilizadas para prover o suporte de comunicação para as MANETs. Por outro lado, tanto as WLANs quanto as MANETs implementam, cada uma, diversos padrões. Surgem esforços direcionados para a redução no número de padrões, objetivando que, independente da necessidade, o usuário se conecta, realiza as suas tarefas, sem saber da tecnologia que foi empregadas. Também percebe-se que vários padrões podem interagir, porém desde que estejam fortemente integrados.

É possível visualizar um futuro em que a convergência de meios e tecnologias permitirá um cenário de grande mobilidade, a Internet Móvel. Na atualidade, existem duas correntes básicas de convergência. Uma afirmando que as pessoas terão à disposição uma rede pessoal, onde todos os seus aparelhos estarão se comunicando uns com os outros através de sistemas como o Bluetooth, o Wi-Fi (WLANs), o celular ou o WIMAX. Outra afirmando que as pessoas usarão apenas um dispositivo e que este atuará de forma diferente, de acordo com a situação. O *smartphone* (um telefone celular com funcionalidades avançadas) é, na atualidade, um bom exemplo desta tendência.

A Internet móvel e as tecnologias sem fio podem criar uma ruptura no cenário de negócios e na relação dos usuários com os seus sistemas. A grande dificuldade é que mercados futuros e que ainda não existem não podem ser analisados e muito menos previstos com exatidão. É prudente considerar que os sistemas adaptados aos cenários convergentes serão fundamentais para a sociedade do futuro, seja no lazer ou mesmo na maneira de realizar negócios. O presente trabalho procura apresentar uma proposta de integração otimizada entre uma redes *Ad Hoc* e uma rede infraestruturada IP. Para tanto buscou-se identificar as características básicas de diversos porotocolos utilizados em MANETs e apontar aquele que apresentar as melhores características.

Na tabela 3.1, são apresentadas algumas das características básicas para a função de roteamento em redes *Ad Hoc* (MANETs). Tais propriedades também poderão se tornar determinantes quando tratamos da integração com outras redes. Outras propriedades podem ser observadas, contudo estão fora do escopo deste documento. As MANETs quando integradas às redes infraestruturadas podem apresentar um cenário válido para as redes convergentes.

Além das informações comparativas apresentadas na tabela 3.1, outros elementos são motivadores ao uso do protocolo AODV no presente trabalho. Estes elementos são apresentados a seguir:

- É o protocolo de roteamento *Ad Hoc* mais amplamente discutido na atualidade e com o maior número de implementações;
- Já existe uma implementação de um gateway em ns-2, o que contribui em muito ao presente trabalho;
- É, dentre os demais, o protocolo que melhor representa a classe dos protocolos reativos (roteamento pela origem);
- Interage com o protocolo IP;
- Ainda não apresenta suporte a QoS.

Tabela 3.1: Comparação de propriedades básicas de roteamento para MANETs

Propriedade	**Pró-Ativos**			**Reativos**					**Híbrido**
	DSDV	*WRP*	*GSR*	*TORA*	*ABR*	*DSR*	*AODV*	*LAR*	*ZRP*
Inundação	Não	Não	Não	Sim	Sim	Sim	Sim	Sim	Se necessário
Inundação controlada	Não	Não	Não	Sim	Sim	Sim	Sim	Não	Sim
Inundação para descoberta de rota	Não	Não	Não	Sim (só um no início)	Sim	Sim (usa cache)	Sim (usa cache)	Sim (usa informação de localização)	Somente fora do escopo da zona
Roteamento pela Origem	Não	Não	Não	Sim	Sim	Sim	Sim	Sim	Sim
Atraso para descoberta da rota	Não	Não	Não	Sim (na construção do DAG)	Sim	Sim	Sim	Sim	Somente se o destino está fora da zona do nó origem
Múltiplas rotas	Não	Não	Não	Sim	Não	Não, mas estabelece uma nova rapidamente	Não, mas pesquisas recentes indicam viabilidade	Não	Não
Uso de GPS	Não	Não	Não	Não	Não	Não	Não	Sim	Não
Suporta QoS	Não	Não	Sim	Não	Sim	Não	Não	Não	Não
Métrica de Roteamento	Número de seqüência mais novo e menor caminho	Menor Caminho	Estado do Enlace	Menor Caminho	Estado de Enlace (Associatividade) e Menor Caminho	Menor Caminho	Número de seqüência mais novo, menor caminho e *beacon* periódico	Menor distância ou zona de requisição	Depende do Algoritmo Utilizado
Seqüenciação de Mensagem	Sim	Não	Não	Sim	Não	Não	Sim	Não	Não
Aquisição da Rota	Calculado	Calculado	Calculado	Sob Demanda	*Beacon* / Estabilidade	Sob Demanda	Sob Demanda	Sob Demanda	Calculado e Sob Demanda
Protocolo livre de loops	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Não	Sim

Fica então definido, a partir da análise das principais características dos protocolos de roteamento das MANETs, o protocolo AODV, por apresentar características favoráveis aos objetivos do presente trabalho, como aquele a ser utilizado no processo de integração de uma MANET com uma rede infra-estruturada IP. O restante desta seção aborda os elementos de integração entre o protocolo AODV e uma rede infra-estruturada IP, tomando como base a RFC 3561.

3.4 O uso do protocolo AODV com outras redes

Em algumas configurações, uma rede AODV pode fornecer conectividade entre os domínios de roteamento externos que não usam AODV. Nestas configurações os pontos do contato às outras redes devem poder agir como roteadores de sub-redes para qualquer rede relevante dentro dos domínios externos do roteamento. Assim, a rede *Ad Hoc* pode manter a conectividade aos domínios de roteamento externos. Dessa forma, as redes de roteamento externas também podem usar a rede *Ad Hoc* definida pelo AODV como uma "*transit network*" (HAMIDIAN, 2003).

A fim de fornecer esta característica, um ponto do contato a uma rede externa deve agir como roteador de sub-rede para cada sub-rede externa de interesse, de forma que o roteador da rede infra-estruturada possa alcançar um nó pertencente à uma MANET. Isso também inclui a necessidade de manter um número de seqüência do destino para essa sub-rede externa (WAKIKAWA, 2001).

3.4.1 A Pilha de protocolos nos modelos OSI, TCP/IP e *Ad Hoc*

Na Figura 3.13 é apresentada a pilha de protocolos do envolvidos em uma MANET, que consiste em cinco camadas: camada física, camada de enlace, camada de rede, camada de transporte e camada de aplicação. Essa pilha de protocolos é similar à pilha de protocolos apresentada no modelo TCP/IP. Pode-se observar que as camadas de seção, apresentação e aplicação do modelo OSI são agrupadas em uma única seção, a camada de aplicação. Já o modelo TCP/IP é similar ao modelo *Ad Hoc*, diferenciando basicamente na camada de redes, uma vez que todos os nodos da rede *Ad Hoc* implementam protocolos de roteamento específicos. Na camada física e na camada de enlace, os nodos móveis implementam, de forma idêntica, os mesmos protocolos projetados para redes *wireless* infraestruturadas.

Na pilha de protocolos de uma MANET, o padrão IEEE 802.11 é definido como o padrão a ser utilizado nas camadas um (Físico) e dois (Enlace). Existem diversas variações do padrão IEEE 802.11, este trabalho, contudo, está focado essencialmente em roteamento *Ad Hoc*, que é manipulado pela camada três, a camada de rede. Essa camada é dividida em duas partes: Rede e Roteamento *Ad Hoc*. O protocolo utilizado na camada de Rede é o Internet Protocol (IP) e o protocolo de roteamento, específico da MANET, é o *Ad Hoc On-Demand Distance Vector* (AODV).

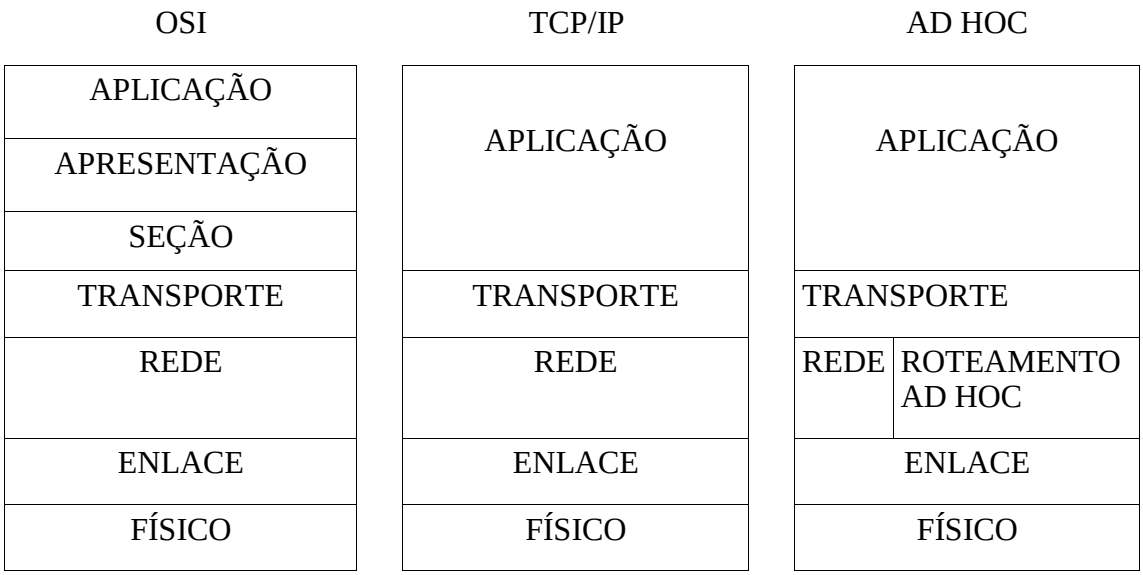


Figura 3.13: A Pilha de Protocolos dos modelos OSI, TCP/IP e AD

Uma das razões de se utilizar o protocolo AODV no presente trabalho, é o fato deste protocolo ser um dos mais desenvolvidos e implementados em pesquisas relacionadas. Outra razão existência de extensões das mensagens de descoberta de rotas para a descoberta dos nodos gateways (HAMIDIAN, 2003). Por outro lado, também é importante considerar que o AODV utiliza o protocolo IP e que é um dos protocolos reativos ou por-demanda com o menor atraso para descoberta de rotas.

Na camada de transporte será utilizado o protocolo UDP em detrimento ao TCP, pois o TCP geraria um *overhead* ainda maior e, conseqüentemente, o desempenho do AODV iria reduzir sensivelmente, podendo também vir a interferir nos resultados esperados, uma vez que a perda de pacotes pode ser um fenômeno bastante presente em função das mudanças na topologia e dos erros de transmissão (HAMIDIAN, 2003).

3.4.2 O protocolo AODV entre redes

Quando um nodo móvel está enviando pacotes para uma rede infra-estruturada, ele precisa primeiramente identificar e enviar os pacotes, tanto de roteamento quanto de dados, para um nodo *gateway* (HAMIDIAN, 2003). Da mesma forma, quando um nodo de uma rede infra-estruturada deseja enviar pacotes para uma MANET, é necessário que os pacotes sejam alcancem o roteador da sub-rede, ou seja, o nodo gateway da MANET.

A pilha de protocolos presente no processo de comunicação entre um *host* origem localizado em uma rede infra-estruturada e um nodo destino localizado em uma MANET é apresentado na Figura 3.14. O gateway utilizado como um elemento de ligação age como uma bridge entre MANETs e a Internet. Entretanto, é necessário implementar a pilha de protocolos MANET e IP. Embora a Figura 3.14 apresente todas as camadas para o *gateway*, não é necessário implementar a todas. A pilha de protocolos do gateway está ao centro da Figura 3.14, e tem como implementação obrigatória as camadas um (físico), dois (enlace) e três (rede). O nodo *gateway*, portanto, deve implementar os protocolos de rede, tanto de uma rede AODV, como de uma rede infra-estruturada (Internet), respeitando as particularidades de cada uma.

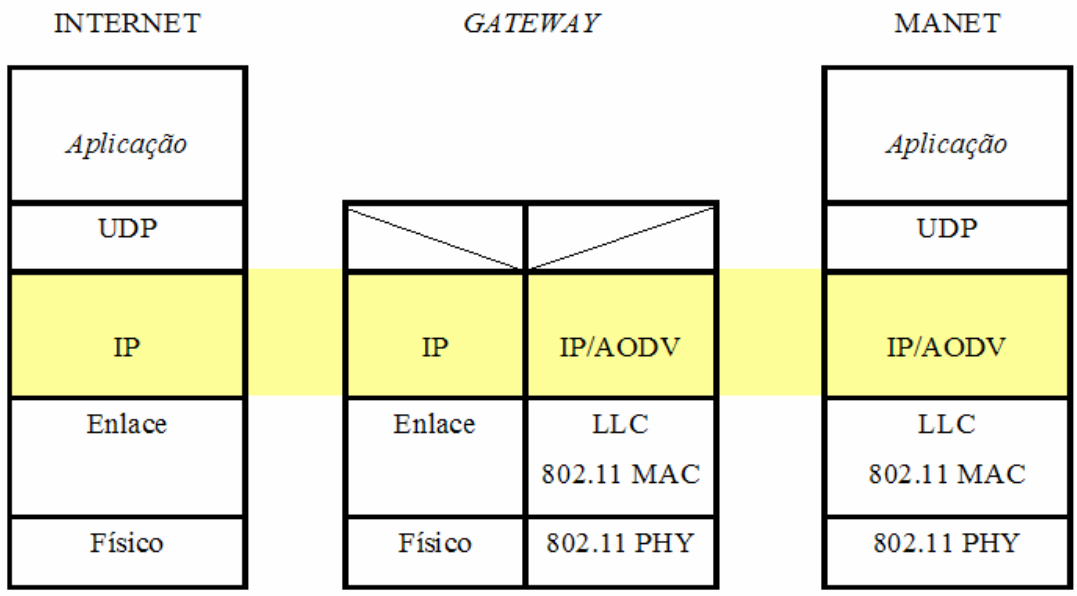


Figura 3.14: Pilha de protocolos envolvida na integração da comunicação MANET e a Internet

A pilha de protocolos da MANET está posicionada mais a direita na Figura 3.14 e a pilha de procolos dos nodos em redes fixas IP está mais a esquerda da mesma figura. O gateway deve ser capaz de compreender estas duas arquiteturas, os seus protocolos e permitir o encaminhamento de pacotes entre elas. Pretende-se, neste trabalho, com base na pilha de protocolos apresentada na figura 3.14, otimizar o fluxo de dados quando este tiver uma origem em uma rede infra-estruturada e um destino em uma MANET.

3.4.3 O Roteamento e Sub-Redes

Tanto a entrega de pacotes de dados quanto o processo de descoberta das rotas afetam o desempenho e o tempo de atraso nos protocolos de roteamento. Os protocolos de roteamento pela origem possuem caracteristicamente um atraso maior no processo de obtenção de rota, pois a rota somente é estabelecida a partir do nodo de origem quando este desejar transmitir dados a algun nodo de destino. Nesse sentido, segundo (HAMIDIAN, 2003), o protocolo de roteamento AODV possui o menor atraso fim-a-fim, não mais de 0,05 segundos. Por outro lado o AODV possui uma das maiores cargas de roteamento e, conseqüentemente, um dos maiores overheads entre os protocolos reativos.

O protocolo de roteamento AODV foi projetado para ser usado em nodos móveis mantendo compatibilidade com os endereços IP de uma rede infraestruturada. Estes nodos não exigem que estejam diretamente relacionados entre si, para criar uma rede *Ad Hoc*. Entretanto, em alguns casos, uma coleção de nodos móveis pode se comunicar com todos os outros através de um relacionamento fixo e compartilhar um prefixo de sub-rede comum, agrupando uma área onde uma rede *Ad Hoc* foi formada (HAMIDIAN, 2003). Essa coleção é identificada como “sub-rede”. É possível, para este caso, que um único nó dentro desta sub-rede anuncie alcançabilidade a todos os nós contidos nela, respondendo via mensagem do tipo RREP a todas mensagens do tipo RREQ recebidas que possuam o prefixo de roteamento da sub-rede. Este nó é identificado como “roteador da sub-rede”. Para que este nó possa executar o protocolo AODV em toda a extensão da sub-rede, deverá manter um número de seqüência do destino para toda a sub-rede. Em uma mensagem de RREP emitida pelo roteador da

sub-rede, o campo do tamanho do prefixo da mensagem de RREP deve ser ajustado ao comprimento do prefixo da sub-rede. Outros nós que compartilham o prefixo da sub-rede não devem emitir mensagens de RREP, e devem encaminhar mensagens de RREQ ao roteador da sub-rede (HAMIDIAN, 2003).

O processamento de RREPs que fornecem rotas às sub-redes (i.e. Possuem tamanho de prefixo diferente de zero) é o mesmo que para as mensagens RREPs de nodos específicos. Cada nó que recebe o RREP com informação do tamanho do prefixo deve criar ou atualizar o registro da tabela de roteamento para a sub-rede, incluindo o número de seqüência fornecido pelo roteador da sub-rede, e incluir a informação apropriada do antecessor. Assim o nó poderá usar esta informação evitando a emissão de novos RREQs para outros nodos da mesma sub-rede no futuro (WAKIKAWA, 2001).

4 PROPOSTA DE OTIMIZAÇÃO DO PROCESSO DE INTEGRAÇÃO DE UMA REDE MÓVEL AD HOC COM A INTERNET

Nesta seção é apresentada uma proposta de otimização no protocolo de roteamento AODV (HAMIDIAN, 2003), visando a incorporar regras de confiabilidade (TOH, 2002) no processo de obtenção de rotas. Espera-se, com essas modificações, reduzir o tempo de obtenção das rotas pelo nodo *gateway*. Também são apresentados os resultados de diferentes cenários de simulação, que demonstram as vantagens desta proposta.

4.1 A integração de uma MANET com uma rede infra-estruturada

De um lado, encontramos uma Rede Móvel *Ad Hoc* que consiste em uma coleção de terminais que possuem transmissores e receptores e se movimentam arbitrariamente em uma determinada área geográfica. Esses terminais geralmente utilizam sistemas *wireless* nas comunicações, configurando uma rede wireless não infraestruturada. As MANETs também conhecidas como redes independentes, não dependem de qualquer infra-estrutura pré-existente para prover comunicação entre os nós da sua rede, conseqüentemente, exigindo que todos os nós incorporem as funções de roteamento (IETF, 2000).

Do outro lado, encontramos as redes infra-estruturadas, compostas por terminais transmissores e receptores, que, apesar de poderem alterar o seu ponto de inserção em uma rede, tendem a manter uma topologia bem mais estável do que as redes móveis *Ad Hoc*. Outra característica importante das redes infra-estruturadas é que os terminais não necessitam implementar funções de roteamento, pois estas redes incorporam dispositivos específicos para isso.

Com características tão distintas, pode-se rapidamente concluir que tais redes são de difícil integração. Esse processo de integração pode se tornar ainda mais difícil se for levada em conta a diferença de performace entre elas. É justamente por essas razões que nas pesquisas recentes é empregado um elemento com funções diferenciadas para estabelecer a integração entre estas redes. Esse elemento é chamado nodo *gateway*.

Uma MANET, assim como qualquer outra rede, pode funcionar perfeitamente de forma independente. Ocorre, porém, que uma rede independente se torna extremamente limitada. A integração é necessária a partir do momento em que se pretende, por exemplo, estabelecer uma conexão com a Internet, interligar pontos avançados, suportar usuários nômades etc.

4.1.1 O processo de integração

O processo de integração apresentado neste trabalho é estabelecido no nível de rede do modelo RM-OSI, considerando as métricas de atraso (*delay*) e vazão (*throughput*). A integração de uma MANET fazendo uso do protocolo *Ad hoc On-Demand Distance Vector* -AODV, com a Internet é o foco deste trabalho.

Outros trabalhos também já foram realizados sobre o protocolo de roteamento AODV, entre os quais está o de Hamidian (2003) que apresenta um processo de integração de uma MANET com outras redes, a partir da implementação de um nodo *gateway*. Essa implementação foi realizada no simulador de redes NS-2. O cenário apresentado por Hamidian, contudo, define a implementação de um nodo *gateway* com o objetivo de possibilitar que uma rede móvel *Ad Hoc* que esteja implementando o protocolo de roteamento AODV possa se comunicar com outras redes, sejam MANETs ou infra-estruturadas. O processo de integração proposto por Hamidian está embasado na RFC-3561 e no trabalho de Belding-Royer (2001).

Como um dos objetivos do presente trabalho é diminuir os impactos negativos provenientes da integração dessas redes tão distintas, dois trabalhos relacionados, os quais também abordam o processo de otimização na integração das redes definidas no ambiente de investigação (vide Figura 4.1), são utilizados como referência.

O primeiro, realizado por Hamidian (2003), apresenta uma modificação à implementação original do protocolo AODV segundo Perkins (1998). Hamidian (2003) propõe funcionalidades de descoberta do nodo *gateway* pelos demais nodos da rede. O autor modifica os pacotes RREQ e RREP, adicionando pacotes RREQ-I e RREP-i, através da adição de um campo adicional nos cabeçalhos dos respectivos pacotes. O código implementado por Hamidian é o ponto de partida para o presente trabalho.

O segundo, realizado por Toh (2002), apresenta o protocolo de roteamento ABR para redes *Ad Hoc*, que age segundo a associabilidade das rotas e o menor caminho entre as mesmas. Esse processo proporciona atualizações menos freqüentes e, conseqüentemente, um *overhead* menor. O ABR apresenta uma importante métrica conhecida como grau de associabilidade. Essa métrica baseia-se no conceito de que "quanto menos dinâmica for a topologia, maior o grau de associabilidade" (TOH, 2002), considerando o atraso na propagação dos datagramas nos *links*, a potência e qualidade do sinal, duração da bateria, carga do *link*, período de funcionamento/presença do *link* e características temporais e espaciais. (Esse protocolo está patenteado, contudo, o autor disponibiliza o algoritmo do protocolo para estudos). Com base na métrica de associabilidade (TOH, 2002), é proposta, neste trabalho, a implementação de uma nova métrica de confiabilidade para o protocolo de roteamento AODV, agindo no nodo *gateway* implementado em Hamidian (2003).

Partindo dos estudos de Hamidian (2003) e Toh (2002), este trabalho propõe modificações no protocolo AODV, que irão atuar nos nodos *gateways* de uma MANET, procurando estabelecer regras para uma nova métrica de confiabilidade com base na estabilidade das rotas já estabelecidas e ainda disponíveis na memória *cache*. As técnicas de Hamidian e Toh, quando integradas, se complementam e podem ser utilizadas no processo de otimização do processo de integração de uma rede infra-estruturada com uma rede móvel *Ad Hoc*. Portanto, espera-se otimizar o fluxo diminuindo o descarte e o atraso dos pacotes, no nodo *gateway*, através da diminuição no tempo de descoberta de rotas pelas MANETs que fazem uso do protocolo de roteamento AODV.

4.2 Ambiente utilizado para a investigação da proposta

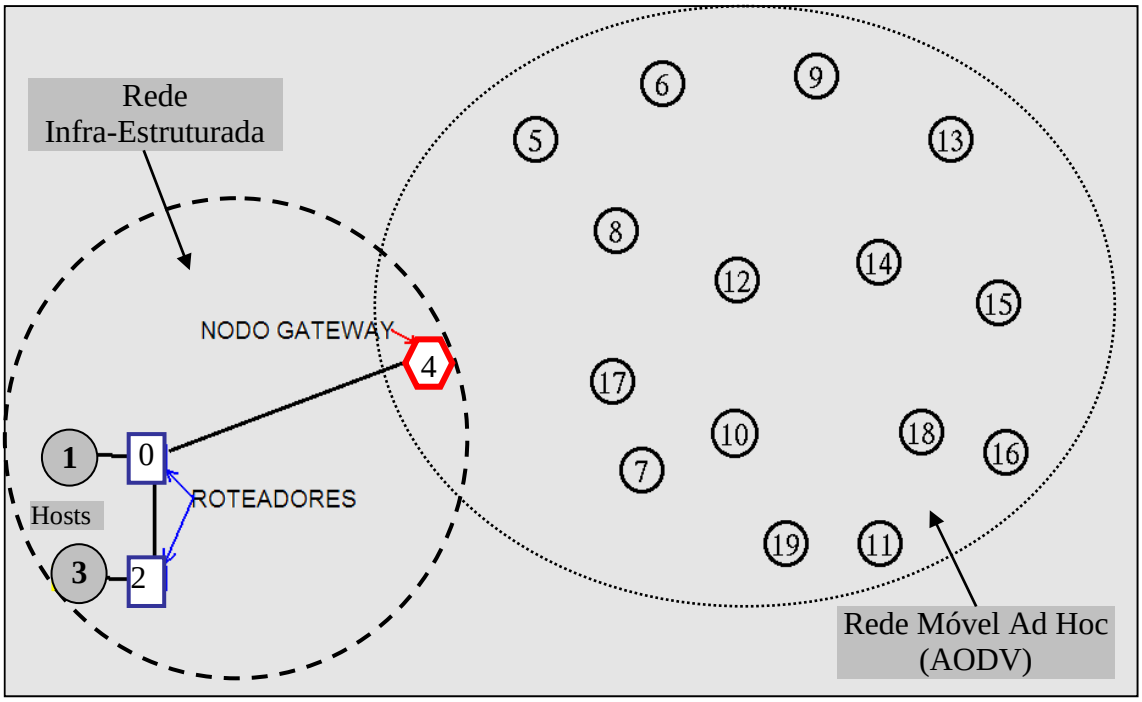


Figura 4.1: Cenário de investigação

O ambiente deste trabalho é composto por três elementos distintos e interligados: uma rede infra-estruturada, uma rede móvel *Ad Hoc* que implementa o protocolo de roteamento AODV (deste ponto em diante, referenciada apenas como Rede AODV), um nodo gateway, que implementa o protocolo de roteamento AODV e, por estar conectado a uma rede infra-estruturada, o protocolo IP. O ambiente apresentado na Figura 4.1 é criado no simulador de redes ns-2, a partir do qual são realizadas as modificações propostas e a execução dos testes para conseqüente avaliação dos resultados.

4.2.1 O nodo gateway como elemento de ligação

O nodo *gateway* é um nodo integrante da rede móvel *Ad Hoc*, implementa o protocolo de roteamento AODV e deve possuir uma interface para esta rede. O nodo *gateway* também é conectado à rede infra-estruturada e, conseqüentemente, deve ser capaz de interagir com esta a partir de uma interface apropriada. As duas interfaces são distintas e atuam de acordo com a rede onde estão conectadas.

O tempo gasto no processo de descoberta de uma rota pelo protocolo AODV em uma MANET pode, em algumas situações, chegar a 50 milissegundos (HAMIDIAN, 2003). Se considerarmos diversos fluxos de dados chegando ao nodo *gateway* oriundos da Internet e destinados a uma MANET com taxas de transferência elevadas, poderá ocorrer descarte de pacotes e/ou atrasos nas entregas dos mesmos. Esse problema pode ser agravado ainda mais se consideradas as diferenças de desempenho impostas às redes que integram esse ambiente.

O nodo *gateway* deve, além de proporcionar uma interface entre as redes móveis *Ad Hoc* e as redes infra-estruturadas, procurar:

- estabelecer uma rota inicial a partir de um *link* infraestruturado estável, no momento que se torne necessário convergir para uma rede Ad Hoc, ao nodo de

destino, procurando oferecer alguma garantia quanto à manutenção e estabilidade desta rota no contexto fim-a-fim;

- amenizar os efeitos provocados pelas diferenças das taxas de vazão, visto que, em uma rede infra-estruturada, normalmente, as taxas de vazão são superiores àquelas encontradas em MANETs;
- evitar o descarte de pacotes quando o fluxo de pacotes atinge o *gateway* da rede *Ad Hoc*;
- reduzir o atraso no processo de entrega dos pacotes.

4.2.2 A rede infra-estruturada

Conforme apresentado na Figura 4.1, a rede infra-estruturada é composta por dois *hosts* e dois roteadores. O nodo *gateway* é constituído de duas interfaces de rede: uma conectada à rede infra-estruturada (Internet), e outra sem fios, que implementa o padrão IEEE 802.11b (IEEE, 2001), conectada à MANET. Todos os pacotes oriundos da rede infra-estruturada, ao chegarem ao *gateway*, devem ser verificados quanto aos seus destinos. Se o destino estiver na rede AODV, então o *gateway* deve procurar identificar se existem rotas em *cache* para o nodo destino. Se uma rota for encontrada, o *gateway* a utiliza imediatamente, dispensando o processo de descoberta de rota do protocolo AODV. Se não for encontrada uma rota, o *gateway* deve iniciar o processo de descoberta de rota original.

4.2.3 A rede móvel *Ad Hoc* para o ambiente de investigação

No ambiente em questão, é assumido que a rede AODV utiliza o padrão IEEE 802.11. É esperado, contudo, que o desempenho dessa rede não interfira diretamente nos resultados, pois o que se pretende observar é o desempenho dos protocolos de roteamento quando interligados com outras redes. Mais precisamente, espera-se observar o atraso e o descarte de pacotes gerados a partir do processo de interligação do protocolo de roteamento AODV com outros protocolos de roteamento da rede infra-estruturada, no nodo *gateway*.

De modo a focar a investigação aqui proposta, serão considerados apenas o atraso e a quantidade de pacores descartados no processo de descoberta de uma rota no protocolo de roteamento AODV, pelo nodo gateway.

4.2.4 Fluxo de datagramas utilizado no ambiente de investigação

Para o ambiente em questão, é considerado apenas o fluxo de datagramas gerados pelos terminais que estão conectados à rede infra-estruturada (*hosts* de origem) e que possuam como destino, terminais conectados a uma rede AODV. Qualquer outro fluxo, exceto o fluxo gerado pelo próprio algoritmo de roteamento, não será considerado de forma a não comprometer a análise dos resultados.

No presente trabalho, dois terminais fixos conectados à Internet (rede infra-estruturada), se comunicam com 5 nodos móveis através do nodo *gateway*. Os dois terminais fixos, ou terminais de origem, geram um tráfego CBR com taxas de entrada variando entre 84, 100, 125, 167 e 250 datagramas/s.

O protocolo de transporte a ser utilizado no presente trabalho é o UDP e o tamanho dos datagramas varia entre 64, 128, 256, 512, 1024 e 2048 bytes.

As taxas de transmissão geradas por cada fluxo são determinadadas segundo a fórmula ((datagramas/s) x (tamanho do datagrama) x (8 bits/s)), a qual resulta em uma taxa de bits/s para cada fluxo.

4.2.5 A movimentação dos nodos para o ambiente de investigação

Os nodos móveis movimentam-se segundo o modelo "random waypoint" (JOHNSON, 1996). Cada nodo inicia parado por um determinado período de tempo após o início da simulação. Logo após a pausa, os nodos movem-se randomicamente até um ponto de chegada sobre a área topográfica definida em 500m x 800m, a uma velocidade não superior a 10 metros por segundo. Os nodos, após chegarem ao ponto de destino, param novamente por um período de tempo, selecionam um novo destino e se movimentam até ele, seguindo sempre o mesmo padrão. Esse padrão de movimentação ocorre durante todo o período de simulação.

O nodo *gateway*, apresentado no ambiente de simulação (vide Figura 4.1), muito embora também implemente o protocolo AODV, não se movimenta e possui uma inserção cabeada à rede infra-estruturada.

4.3 As modificações propostas ao protocolo AODV

A identificação do nodo *gateway* pelos nodos que implementam o protocolo de roteamento AODV é fundamental (HAMIDIAN, 2003). Nas modificações propostas neste trabalho, o nodo *gateway* é responsável pela implementação e manutenção de uma tabela de confiabilidade, a qual é armazenada unicamente no próprio nodo *gateway*. Nenhum outro nodo da MANET deve implementar essa tabela. O processo de otimização proposto é aplicável apenas ao nodo *gateway*. Todos os demais nodos executarão o protocolo de roteamento AODV, proposto por Hamidian (2003).

O nodo *gateway* monitora as mensagens *Route Request* (RREQ), *Route Response* (RREP) e *Route Error* (RERR) do protocolo AODV original e também as mensagens RREQ-I e RREP-I propostas no trabalho de Hamidian (2003). Todas essas mensagens são do protocolo AODV e são geradas sempre que algum nodo inicia um processo de descoberta de rota ou responde a uma requisição de rota. O *gateway*, ao identificar uma mensagem do tipo RREQ ou RREQ-I, procura identificar esta rota na tabela de confiabilidade. Se o gateway não encontrar uma entrada, executa o protocolo AODV original para encontrar a rota e a adiciona à tabela de confiabilidade, atribuindo-lhe um valor de confiabilidade inicial igual a 10 (Ex.: Grau_Confiabilidade = 10). Se essa rota já existir em sua tabela de confiabilidade, o valor de confiabilidade é incrementado (Ex.: Grau_Confiabilidade = Grau_Confiabilidade + 10). O *gateway*, ao identificar uma mensagem do tipo RERR, identifica o nodo destino da mensagem e, se uma entrada para este destino for encontrada na sua tabela de confiabilidade, essa é excluída imediatamente. O *gateway* ainda deve implementar um tempo de vida para cada rota inserida em sua tabela de confiabilidade. Se alguma rota exceder o tempo de vida sem receber qualquer tipo de mensagem, deve ser excluída imediatamente. O tempo de vida de uma rota na tabela de confiabilidade é de quatro vezes o tempo de vida de uma rota convencional, segundo as definições do protocolo original. Se o tempo de vida for excedido, a rota é excluída como se tivesse ocorrido um erro, pois não é possível saber se o nodo foi desligado, se está fora do alcance ou se simplesmente não foi solicitado para compor alguma rota.

A Tabela 4.1 apresenta parte das informações que devem estar contidas na tabela de roteamento do *gateway* e manipuladas pelo protocolo AODV. Os dados contidos nesta tabela tomam como base a Figura 4.1.

Tabela 4.1: Exemplo da tabela de roteamento contida no nodo *gateway*

Destino	**Nro IP**	**Rota**	**Grau_Confiabilidade**
I	200.248.113.35	A – B - J	80
I	200.248.113.35	A - B - H	70
E	200.248.113.26	A - B	80
E	200.248.113.26	A - C	80
F	200.248.113.28	A - C - D	60
...	...	...	...

Através do mecanismo “grau de confiabilidade”, com o passar do tempo, será possível conhecer as rotas que podem oferecer um maior grau de confiabilidade e estabilidade. A vazão também pode ser melhorada, uma vez que, ao utilizar uma rota estável e disponível, são reduzidos os tempos e os recursos da rede gastos no processo de descoberta das rotas.

A partir do uso dessa tabela de confiabilidade, pretende-se otimizar o fluxo de informações no processo de integração entre MANETs e a Internet. O processo de otimização proposto pra este trabalho é focado no processo de obtenção de rotas da rede AODV, através de modificações no processo de descoberta de rotas no nodo gateway.

O nodo gateway, ao receber um pacote de dados de uma rede infra-estruturada com destino a uma nodo da rede AODV, examina, em sua tabela de confiabilidade do lado *Ad Hoc*, aquela rota que apresentar o maior grau de confiabilidade. Se uma rota for encontrada, a mesma é utilizada imediatamente. Se não for, o processo original de descoberta de rota é iniciado. Essa tabela de confiabilidade é mantida dinamicamente e deve ter referência a todos os elementos ativos da MANET, permitindo, assim, conhecer a sua topologia.

Com essa otimização, espera-se também qualificar algumas características pertinentes ao QoS do nível de rede, assim como a latência e a vazão. Quando existirem rotas com graus de confiabilidade semelhantes, o nodo *gateway* deverá poder escolher aquela rota que oferecer a maior taxa de transmissão[1] (Valores obtidos a partir da sub-camada MAC).

4.4 Modificações realizadas no código do simulador ns-2

A modificação proposta sugere o emprego de regras de confiabilidade (TOH, 2002) no processo de obtenção de rotas em uma MANET que implementa o protocolo de roteamento AODV. Para tanto, diversas alterações no código do simulador de redes ns-2, referentes ao uso desse protocolo são propostas (HAMIDIAN, 2003).

[1] Este processo será explorado em trabalhos futuros.

Para realizar as alterações propostas, assim como para efetuar as simulações desejadas, utilizou-se o simulador de redes ns-2. Os pseudo-códigos apresentados neste trabalho são extraídos de programas modificados pelo autor que implementam o protocolo de roteamento AODV no referido simulador.

As alterações propostas consistem em implementar e manter um coeficiente de confiabilidade a ser associado a cada uma das diferentes rotas alcançadas a partir do nodo *gateway*. Essas rotas passam a ser armazenadas pelo nodo *gateway* em uma tabela adicional, que passa a ser denominada tabela de confiabilidade. Cada *gateway* deve possuir e manter atualizada a sua tabela de confiabilidade.

A tabela de confiabilidade é criada tomando-se como base a tabela de rotas mantida na memória *cache* de cada nodo de uma MANET. Esta tabela de rotas é criada pelo protocolo AODV, enquanto é construída uma rota para um destino qualquer. Um campo numérico, que representa o coeficiente de confiabilidade, é adicionado e a nova estrutura passa a ser replicada em uma nova tabela, identificada como tabela de confiabilidade.

O código adicionado permanece indefinidamente monitorando os eventos realizados pelo protocolo. Eventos como identificação de uma nova rota pelo nodo *gateway*, detecção de erros, exclusão de uma rota por estrapolar *timeout* ou quebra de link e reencaminhamento de pacotes são monitorados e disparam os processos de manutenção da tabela e do coeficiente de confiabilidade apresentadas a seguir.

4.4.1 Processo de Carga da Tabela de Confiabilidade

Toda vez que um nodo *gateway* identificar uma rota válida ou for solicitado a encontrar uma nova rota, o mesmo deve chamar o procedimento de carga da tabela de confiabilidade (transfere_routing_table()). Esta carga é feita a partir da tabela de roteamento original mantida na *cache*, copiando as informações da rota e inicializando o grau de confiabilidade em 10.

Se a rota para o destino em questão não for encontrada na tabela de confiabilidade, essa rota é adicionada imediatamente, inicializando o seu grau de confiabilidade. Caso a rota já exista, o procedimento de alteração do grau de confiabilidade é executado para incrementá-lo (rt_update_conf(nsaddr_t id, int val)).

A Figura 4.2 apresenta o código adicionado ao protocolo para a realização da carga da tabela de confiabilidade.

```
void
AODV::transfere_routing_table() {
  aodv_rt_entry *my_rt;            aodv_rt_entry *gw_rt;
  aodv_rt_entry *gw2_rt;           int i=1;
  my_rt = rtable.head();           gw_rt = rtable_gw.head();
  if (rtable_gw.rt_lookup(my_rt->rt_dst) == 0 ){          // Rota inexistente...
    for(my_rt; my_rt; my_rt = my_rt->rt_link.le_next) {   // Adiciona à tabela
      gw2_rt = rtable_gw.rt_add(my_rt->rt_dst);
      gw2_rt->rt_nexthop = my_rt->rt_nexthop;
      gw2_rt->rt_hops = my_rt->rt_hops;
      gw2_rt->rt_seqno = my_rt->rt_seqno+100;
      gw2_rt->rt_expire = my_rt->rt_expire*4;
      gw2_rt->rt_flags = my_rt->rt_flags;
      gw2_rt-> rt_lev_conf=10; }  }
  else  {                                    //Incrementa grau da rota já existente
        rt_update_conf(gw_rt->rt_dst, 10)}   }
```

Figura 4.2: Carga da tabela de confiabilidade

O tempo de vida (TTL) de uma rota convencional, segundo o protocolo original, é de 5s. Nas modificações propostas, esse valor é multiplicado por 4, passando então para

20s. Este tempo é considerado razoável, visto que os nodos movimentam-se a uma velocidade máxima de 10m/s.

Como o protocolo de roteamento AODV utiliza um número de seqüência no intuito de evitar *loops*, soma-se 100 ao número de seqüência no nodo *gateway*, a fim de evitar números duplicados, *loops* e, conseqüentemente, a perda de rotas.

4.4.2 Processo de Alteração do Grau de Confiabilidade

Para o caso de a rota já existir, o processo de carga da tabela de confiabilidade (transfere_routing_table()) chama o procedimento de alteração do grau de confiabilidade de uma rota (rt_update_conf(nsaddr_t id, int val)), passando os parâmetros "endereço do destino" e "valor a ser incrementado" para atualizar o grau de confiabilidade. O grau de confiabilidade não pode ultrapassar o número 1000, o maior valor possível.

A Figura 4.3 apresenta o código adicionado ao protocolo para a realização da alteração do grau de confiabilidade.

```
void
AODV::rt_update_conf(nsaddr_t id, int val) {
if (rt_lookup(id) != 0){                    //confirma a existência da rota
  aodv_rt_entry *rt = rt_lookup(id);
   if(rt->rt_lev_conf < 1000){                      //1000 é o grau máximo
     rt->rt_lev_conf = rt->rt_lev_conf + (val);    //o grau de confiabilidade
    }                                               // é incrementado
  }
}
```

Figura 4.3: Alteração do valor do grau de confiabilidade

O valor máximo de confiabilidade a ser obtido por uma rota qualquer é 1000, o mínimo é 0 e o incremental é 10. Em qualquer operação de alteração do grau de confiabilidade ou de exclusão de uma rota da tabela de confiabilidade, nenhuma mensagem é enviada, ocorrendo ambas de forma silenciosa.

4.4.3 Processo de Remoção de uma Rota da Tabela de Confiabilidade

No caso de mensagens RERR ocorrerem e de a rota associada à mensagem existir na tabela de confiabilidade, a rota é descartada silenciosamente. Esse descarte também acontece se o tempo expirar por falta de comunicação ou se o protocolo gerar um pacote de erro (RERR), seja por motivo de o destino estar fora de alcance, seja por decorrência da sua movimentação.

Nos dois casos apresentados, o procedimento de exclusão da rota é chamado pelo nodo *gateway* (delete_gw_routing_table(nsaddr_t rt_id)) ou por qualquer outro nodo da MANET.

A Figura 4.4 apresenta o código adicionado ao protocolo para a realização da exclusão de uma rota da tabela de confiabilidade.

```
void
AODV::delete_gw_routing_table(nsaddr_t rt_id){
  aodv_rt_entry *gw_rt;
  gw_rt = rtable_gw.head();
  if (rtable_gw.rt_lookup(rt_id) != 0 ){
    for(gw_rt; gw_rt; gw_rt = gw_rt->rt_link.le_next) {
      rtable_gw.rt_delete(gw_rt->rt_dst);
    } } }
```

Figura 4.4: Remoção de rotas da tabela de confiabilidade

4.4.4 Processo de Uso da Rota Mais Confiável

Toda vez que algum nodo *gateway* for reencaminhar algum pacote de dados a um destino de uma MANET, deve, primeiramente, verificar se existe alguma entrada para esse destino na tabela de confiabilidade. Se existir, usa a rota com o maior grau de confiabilidade encontrado na tabela de confiabilidade. Caso não exista, realiza o procedimento padrão do protocolo.

A Figura 4.5 apresenta o código adicionado ao protocolo para a localização o uso da rota mais confiável pelo nodo *gateway*.

```
rt_gw = rtable_gw.rt_lookup(ih->daddr());
  if (rt_gw != 0 ) {      // Se a rota existir, utilizá-la
    assert(rt_gw->rt_hops != INFINITY2);
    forward(find_send_entry(rt_gw), p, NO_DELAY);
  }
else
      // A partir deste ponto é executado
      //  o procedimento original de descoberta de rota
```

Figura 4.5: Uso da rota mais confiável

4.5 Obtenção dos dados para análise

Dois conjuntos de dados são gerados para análise. Para obter o primeiro conjunto de dados, toma-se como base a implementação de um nodo *gateway* em uma rede móvel *Ad Hoc*, que utiliza o protocolo de roteamento AODV (HAMIDIAN, 2003). Com base na implementação de Hamidian, é executado o simulador de redes, o ns-2, e, conseqüentemente, gerados os arquivos "*trace*", para posterior análise.

Para obter o segundo conjunto de dados, é alterado o código fonte utilizado na simulação anterior. Essas alterações são apresentadas nas seções 4.3 e 4.4 e executadas no simulador de redes, o ns-2, tomando como base o ambiente apresentado na seção 4.2, e, posteriormente, gerados os arquivos "*trace*", para análise.

Toda a implementação ocorre no ambiente de simulação ns-2, instalado no sistema operacional Linux, distribuição Slackware, versão 10.0. O código utilizado pelo simulador de redes é aberto e permite que sejam realizadas as alterações e programações necessárias. Para alcançar os objetivos discriminados na seção 4.2 deste capítulo, são realizadas as etapas abaixo discriminadas:

- Instalação do ambiente ns-2, versão 2.14. Essa versão específica é necessária tendo em vista a versão do compilador C++ instalada no sistema operacional Linux (Slackware 10.0) e também por ser compatível com a versão do código desenvolvido por Hamidian (2003), uma implementação do protocolo AODV, com um nodo *gateway* no ns-2, que é o ponto de partida da implementação proposta por este estudo;
- Obtenção dos dados e valores gerados pelo simulador, segundo o modelo proposto por Hamidian e com base nas configurações de fluxo propostas na seção 4.3.1;
- Alteração do código proposto por Hamidian (2003), no simulador ns-2, tomando como base o algoritmo apresentado na seção 4.4 deste capítulo;
- Configuração do ambiente proposto na seção 4.3, a partir da criação de um arquivo ".tcl" específico;

- Elaboração do código “tcl” para a geração dos fluxos de datagramas, suas características e agentes participantes, segundo o ambiente proposto;
- Elaboração do código “tcl” para a definição da mobilidade dos nodos, com as alterações do *lay-out* em tempo de execução com a finalidade de gerar informações próximas de um modelo real, segundo o ambiente proposto;
- Realização das modificações necessárias nos programas “*table.cc*” e “*aodv.cc*”, com a finalidade de obter arquivos “*trace*” com os valores necessários para a geração dos gráficos pretendidos;
- Aplicação de filtros de busca utilizando o programa “*awk”* com o objetivo de obter valores quantitativos de cada tipo de pacote gerado na simulação e arquivos menores para uma análise mais detalhada;
- Aplicação do “Dplot” (DETSCH, 2003) – uma ferramenta plotadora de gráficos que utiliza a ferramenta “*gnu-plot*” do Linux, porém otimizada, sobre os arquivos “*trace*” obtidos. Os gráficos serão gerados para os dados e valores obtidos antes das alterações realizadas no protocolo AODV e após a realização das mesmas;
- Comparação dos gráficos obtidos a partir da execução do “Dplot”, conforme item anterior;
- Apresentação das conclusões.

Para a obtenção dos dados e valores é, portanto, empregada a metodologia de simulação sobre um ambiente estável e confiável, o ns-2.

4.6 Análise dos resultados

A análise dos resultados é feita segundo a Teoria de Filas. Para tanto, é feita uma breve apresentação de um modelo genérico referente a essa teoria e da sua aplicabilidade ao trabalho em questão. O modelo genérico de um sistema de fila é apresentado na Figura 4.6.

Com base no modelo genérico de um sistema de fila, pode-se considerar as fórmulas a seguir:

$\mu = \frac{1}{s}$ → O número médio de eventos atendidos por unidade de tempo. Segundo o modelo apresentado na Figura 4.6, o número de eventos atendidos é influenciado pelo tempo de transmissão de um pacote. O roteamento pode influenciar nesse tempo, caso os pacotes que forem chegando no sistema tiverem que esperar mais ou esperar menos até que uma rota válida seja encontrada.

$\rho = \lambda s = \frac{\lambda}{\mu}$ → O fator de carga ou fator de utilização do sistema.
No AODV em uma MANET, o tempo de descoberta de uma rota pode chegar a 0,05s, necessitando ainda somar o tempo de inserção de pacote na interface de saída.

$t_m = \frac{1}{\lambda}$ → O tempo médio entre as chegadas dos eventos:
Caso o tempo médio de chegada dos eventos for significativamente maior do que o número médio de eventos atendidos, o *buffer* é utilizado para armazenar os pacotes em ula lista de espera até que sejam atendidos.

Pode-se, então, concluir que, se a taxa de chegada "λ" for significativamente superior à capacidade do *link* de saída "C", o *buffer* de entrada é utilizado para armazenar os pacotes que não conseguem ser reencaminhados imediatamente. Se esta situação se mantiver assim por um período de tempo significativo, irá ocorrer o descarte de pacotes, já que o *buffer* é limitado.

A diferença entre a taxa de pacotes que chegam ao sistema e os pacotes atendidos, ainda pode ser acentuada pelo atraso médio que um pacote sofre ao passar pelo roteador. Esse atraso é gerado tanto pelo tempo gasto no processo de descoberta de uma rota, provocado pelo protocolo de roteamento, como pelo tempo total gasto no sistema de fila.

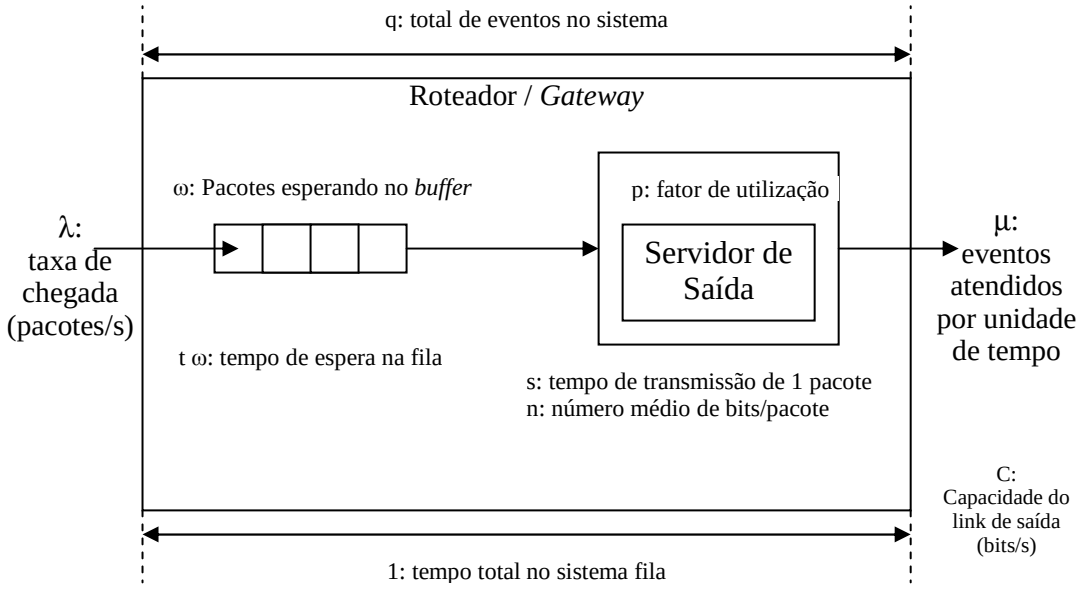


Figura 4.6: Modelo genérico de um sistema de fila

4.6.1 O Descarte de Pacotes

Segundo Hamidian (2003), o protocolo de roteamento AODV possui o menor atraso fim-a-fim, não mais de 50 milissegundos. Por conveniência, esse tempo é assumido como sendo o tempo gasto para o pior caso necessário para a descoberta de uma rota no protocolo AODV. Se este dado for aplicado a uma situação específica, onde o *gateway* recebe um fluxo de pacotes da rede infra-estruturada e precisa enviá-los para um nodo destino localizado na rede AODV, com base na teoria de filas, podemos concluir que: durante o tempo gasto com a descoberta de rota (0,05s), "μ" é igual a zero e "λ" será obrigatoriamente maior que zero, pois já foi iniciado um fluxo de pacotes na entrada. Dependendo do valor de "λ", o "ω" poderá vir a ser maior que a capacidade da fila, provocando atrasos no encaminhamento de pacotes, uma vez que estes permanecem algum tempo armazenados no *buffer* de espera (fila). Se esse processo permance ocorrendo por um período de tempo significativo, o *buffer* enche e novos pacotes não conseguem entrar no sistema. Ocorre então o descarte de pacotes. Também pode-se entender que, mesmo não assumindo o pior caso, "ω" será maior que zero, fazendo com que o atraso médio sofrido por um pacote ao passar pelo roteador seja aumentado.

Com base nos dados contidos na figura 4.2, é possível assumir que:

- Se “μ” for menor que “λ”, o “ω” aumenta;
- Com o aumento de “ω” o “t ω”, também aumenta, provocando atrasos;
- Se “μ” for muito maior que “λ”, o “ω” pode ser maior que a capacidade da fila, provocando descarte de pacotes;
- É fundamental equilibrar o “μ” em relação ao “λ” ao grau máximo possível, pois, neste estudo de caso estamos falando em enlaces sem fios, onde, normalmente, a vazão é menor, a taxa de erros é maior e ainda podemos ter um *overhead* maior em função do Cabeçalho MAC do padrão IEEE 802.11.

4.7 Apresentação dos Resultados

Espera-se apresentar mecanismos que diminuem o atraso na obtenção de rotas em uma rede *Ad Hoc* que utiliza o protocolo de roteamento AODV e uma solução que possa prover um ganho significativo na performance de comunicação entre redes infra-estrutudadas e redes MANETs, a partir da utilização de um nodo *gateway* entre estas redes, bem como validar o grau de confiabilidade no processo de obtenção de rotas pelo nodo *gateway*.

Para tanto, serão explorados os dados gerados em dois processos de simulação. O primeiro processo, identificado como Cenário “A”, é executado com base no protocolo AODV original, enquanto o segundo, identificado como Cenário “B”, é executado com base nas modificações no protocolo sugeridas neste trabalho. Em ambos os casos será utilizado o ambiente definido na Figura 4.1. Por fim, os dados gerados nos dois cenários de simulação são comparados a fim de analisar e quantificar os resultados obtidos em cada processo. Com base nesses resultados, são tabuladas as diferenças encontradas.

Toda a seção 4.7 é embasada no arquivo *w_w_1gw.td*, implementado no simulador de redes ns-2, o qual define o ambiente apresentado na seção 4.2, o tráfego utilizado e o padrão de movimentação. O tráfego utilizado nos processos de simulação é gerado a partir de dois *hosts* que se encontram na Internet, gerando 5 fluxos de dados, tendo como destino 5 nodos móveis da rede móvel *Ad Hoc*. O padrão de mobilidade é estabelecido segundo o modelo “random waypoint” (JOHNSON, 1996).

Os fluxos de dados invariavelmente devem passar pelo nodo *gateway* para que possam alcançar os destinos estabelecidos na rede móvel *Ad Hoc*.

Para cada um dos dois cenários de investigação propostos neste trabalho, trinta processos de simulação foram executados, variando a taxa de entrada entre 84, 100, 125, 167 e 250 pacotes/s e o tamanho dos pacotes entre 64, 128, 256, 512, 1024 e 2048 bytes.

Todos os demais parâmetros necessários para a realização das simulações estão relacionados na Tabela 4.2 e na seção 4.2 e são comuns a todos os processos de simulação realizados.

Tabela 4.2: Parâmetros gerais para a simulação

Parâmetro	**Valor**
Limite de alcance	250m
Tempo de simulação	900s
Tamanho da topologia	800m x 500m
Número de nodos móveis	15
Número de *gateways*	1
Fluxos de dados	5
Tráfego	CBR
Taxa de pacotes	Variável
Tamanho dos pacotes	Variável
Tempo de parada	5s
Velocidade máxima dos nodos	10 m/s

4.7.1 Cenário "A"

O processo de simulação proposto no cenário "A" foi executado com base nas configurações do protocolo de roteamento AODV (HAMIDIAN, 2003). Como resultado desse processo de simulação, foram obtidos os dados apresentados na Tabela 4.3.

Neste cenário o nodo *gateway* tende a estar constantemente sobrecarregado por ser o elo de ligação entre duas redes com características distintas. Somando-se a isso há a tendência de as redes infra-estruturadas possuírem uma performance superior e o problema do tempo de espera para se obter rotas da rede móvel *Ad Hoc*. Como resultado dessa sobrecarga, ocorre um grande número de descarte de pacotes no nodo *gateway*, porém com um comportamento progressivo de descarte de pacotes em função da taxa de bits transferidos. Quanto menor o intervalo de inserção e maior o tamanho do pacote, maior a taxa de bits transferidos.

Tabela 4.3: Resumo do descarte de pacotes gerado no cenário "A"

Descarte de Pacotes por Intervalo de Inserção e Tamanho dos Pacotes

		64 Bytes		128 Bytes		256 Bytes		512 Bytes		1024 Bytes		2048 Bytes	
Interv de Inser	Tot de Pcts	%	Pcts	%	Pcts	%	Pcts	%	Pcts	%	Pcts	%	Pcts
20 ms	45000	7,09%	3190	9,01%	4056	13,28%	5975	20,43%	9194	29,50%	13274	62,90%	28303
30 ms	30000	0,41%	124	2,40%	720	7,91%	2373	12,61%	3783	32,61%	9782	58,83%	17650
40 ms	22500	0,11%	25	0,12%	28	3,70%	832	9,33%	2100	20,24%	4554	47,70%	10733
50 ms	18000	0,02%	4	0,08%	15	0,93%	168	6,21%	1118	33,82%	6088	53,67%	9661
60 ms	15000	0,01%	1	0,01%	1	1,03%	154	0,96%	144	32,74%	4911	66,46%	9969

Com base na Tabela 4.3, é gerado um gráfivo que representa a taxa de descarte de pacotes, tomando-se como base, o tamanho dos pacotes e também o intervalo de inserção. Na Figura 4.7, cada linha do gráfico representa um dos intervalos de inserção apresentados na primeira coluna da tabela 4.3.

Neste cenário percebe-se que o pior caso é gerado com pacotes de 2048 bytes e com um intervalo de inserção de 60ms.

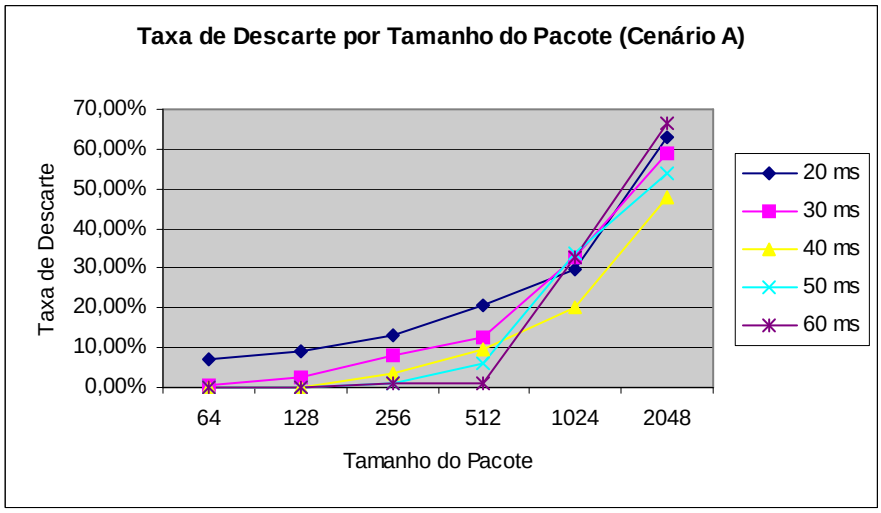


Figura 4.7: Descarte por tamanho e intervalo de inserção dos pacotes - Cenário “A”

4.7.2 Cenário “B”

Após realizadas as modificações no código fonte do protocolo AODV, apresentadas na seção 4.4 deste documento, o processo de simulação foi novamente executado. Como resultado desse processo de simulação foram obtidos os dados apresentados na Tabela 4.4.

O número de pacotes descartados diminuiu significativamente, como é possível verificar na Tabela 4.4. Na média geral, houve melhorias, contudo, em alguns casos, os resultados do cenário “B” foram menos favoráveis do que os resultados obtidos no cenário “A”.

Tabela 4.4: Resumo do descarte de pacotes após alterar o protocolo

Descarte de Pacotes por Intervalo de Inserção e Tamanho dos Pacotes

		64 Bytes		128 Bytes		256 Bytes		512 Bytes		1024 Bytes		2048 Bytes	
Interv de Inser	Tot de Pcts	%	Pcts	%	Pcts	%	Pcts	%	Pcts	%	Pcts	%	Pcts
20 ms	45000	5,77%	2596	10,60%	4769	9,20%	4139	12,64%	5687	32,31%	14541	69,24%	31157
30 ms	30000	1,73%	520	1,41%	422	8,25%	2474	16,05%	4815	22,54%	6762	43,54%	13062
40 ms	22500	0,08%	19	0,09%	20	3,75%	844	6,39%	1438	38,16%	8586	48,88%	10998
50 ms	18000	0,02%	4	0,01%	2	0,16%	29	4,33%	780	27,84%	5012	59,53%	10715
60 ms	15000	0,00%	0	0,00%	0	0,03%	5	1,33%	199	15,53%	2330	58,49%	8773

Com base na Tabela 4.4, é gerado um gráfivo que representa a taxa de descarte de pacotes, tomando-se como base, o tamanho dos pacotes e também o intervalo de inserção. Na Figura 4.8, cada linha do gráfico representa um dos intervalos de inserção apresentados na primeira coluna da tabela 4.4.

Neste cenário percebe-se que o pior caso é gerado com pacotes de 2048 bytes e com um intervalo de inserção de 20ms.

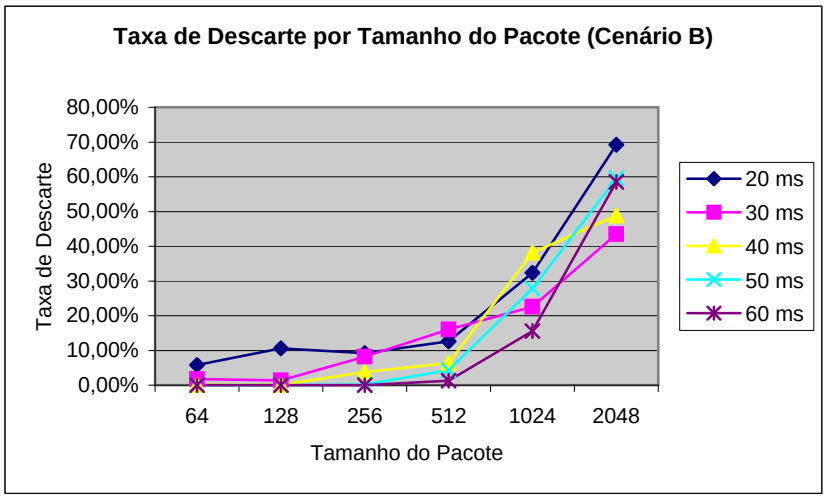


Figura 4.8: Descarte por tamanho e intervalo de inserção dos pacotes - Cenário “B”

4.7.3 Análise Comparativa de Descarte Entre os Cenários “A” e “B”

Com base nos dados coletados nos processos de simulação, é apresentado, a seguir, um conjunto de gráficos que demonstra a quantidade de pacotes descartados no nodo *gateway*, variando o intervalo de inserção entre os pacotes. Cada um dos gráficos apresentados refere-se a um tamanho específico de pacotes.

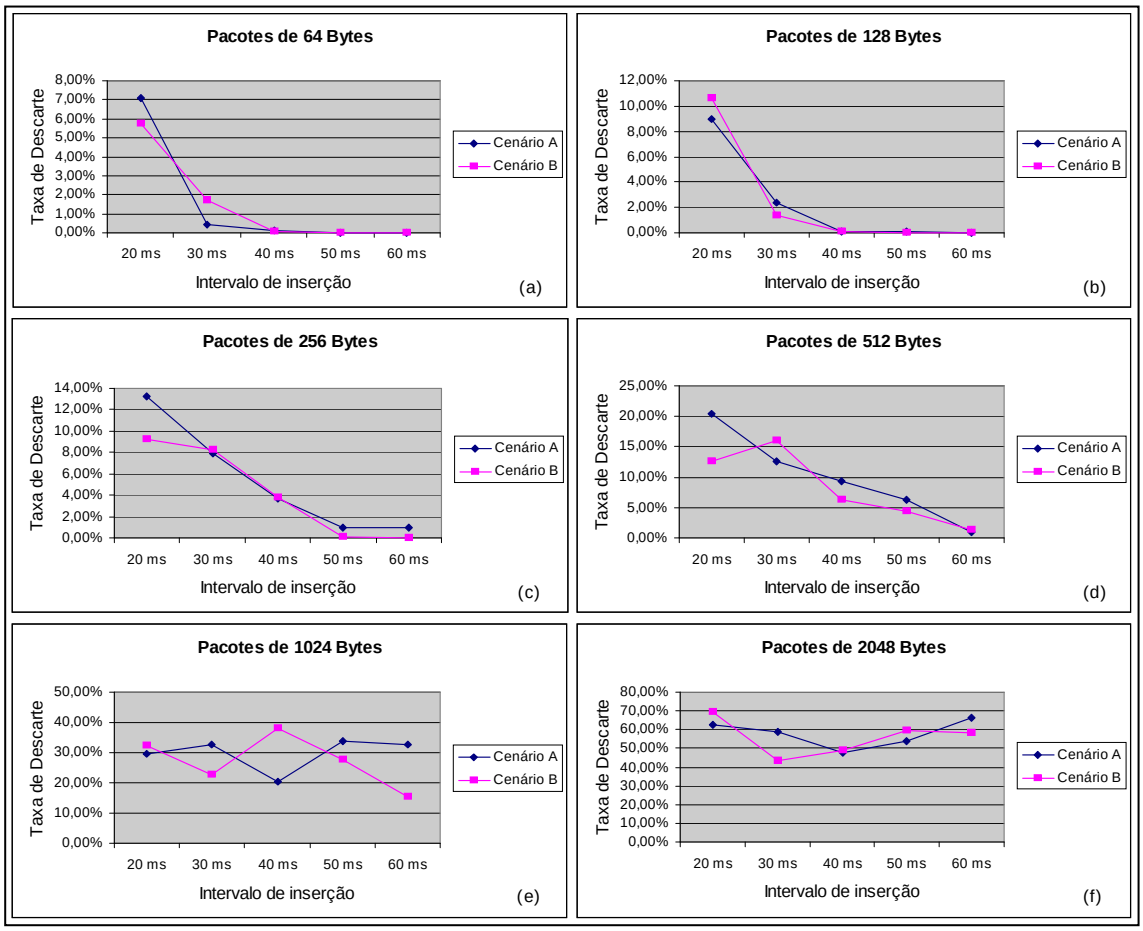


Figura 4.9: Número de pacotes descartados no nodo *gateway* por intervalo de inserção

Nas figuras 4.9 a 4.12 é demonstrado o resultado comparativo com base nos dados gerados a partir dos processos de simulação dos cenários “A” e “B”. Constata-se que não existe um padrão comportamental que justifique o aumento ou a diminuição do número de pacotes descartados. Observa-se, contudo, que, na maioria das situações, o protocolo modificado produz um descarte menor de pacotes no nodo *gateway*. Entretanto,o maior benefício do protocolo modificado é percebido quando utilizados pacotes de 512 bytes, conforme apresentado na Tabela 4.5, a seguir.

Para o trabalho em questão foi analisada a quantidade de pacotes descartados. O o tamanho dos pacotes variando entre 64, 128, 256, 512, 1024 e 2048 bytes. A Figura 4.9 apresenta o conjunto de gráficos gerados a partir dos dados obtidos.

Tabela 4.5: Diferenças no descarte entre os cenários “A” e “B”

		Tamanho dos pacotes em Bytes						
Intervalo de inserção		**64**	**128**	**256**	**512**	**1024**	**2048**	Tot. pacotes descart. p/ intervalo
0,02 s	Quantidade de pacotes descartados por intervalo e tam. do pacote.	594	-713	1836	3507	-1267	-2854	1103
0,03 s		-396	298	-101	-1032	3020	4588	6377
0,04 s		6	8	-12	662	-4032	-265	-3633
0,05 s		0	13	139	338	1076	-1054	512
0,06 s		1	1	149	-55	2581	1196	3873
Tot. pacotes descart. por tam. pacote	→	269	-265	2267	3932	2402	3659	**8232**

Percebe-se que o nodo *gateway* tende a estar constantemente sobrecarregado. Isso ocorre por ser o elo de ligação entre duas redes com características distintas: uma infra-estruturada e uma MANET. O descarte de pacotes, por outro lado, tende a tornar-se mais significativo quando a taxa de inserção de pacotes é aumentada.

Neste trabalho procurou-se enfocar o problema do tempo de espera para a obtenção de rotas do protocolo AODV de uma MANET. Para tanto a taxa de inserção de pacotes foi mantida em padrões nos quais as duas redes pudessem disponibilizar banda suficiente de forma a suportar o tráfego gerado.

Com os dados obtidos a partir dos processos de simulação gerados para os cenários “A” e “B”, foi comparado também, o descarte de pacotes gerados pelo nodo gateway com o descarte gerado nos demais nodos da MANET. O resultado obtido a partir dessa comparação é apresentado na Figura 4.10.

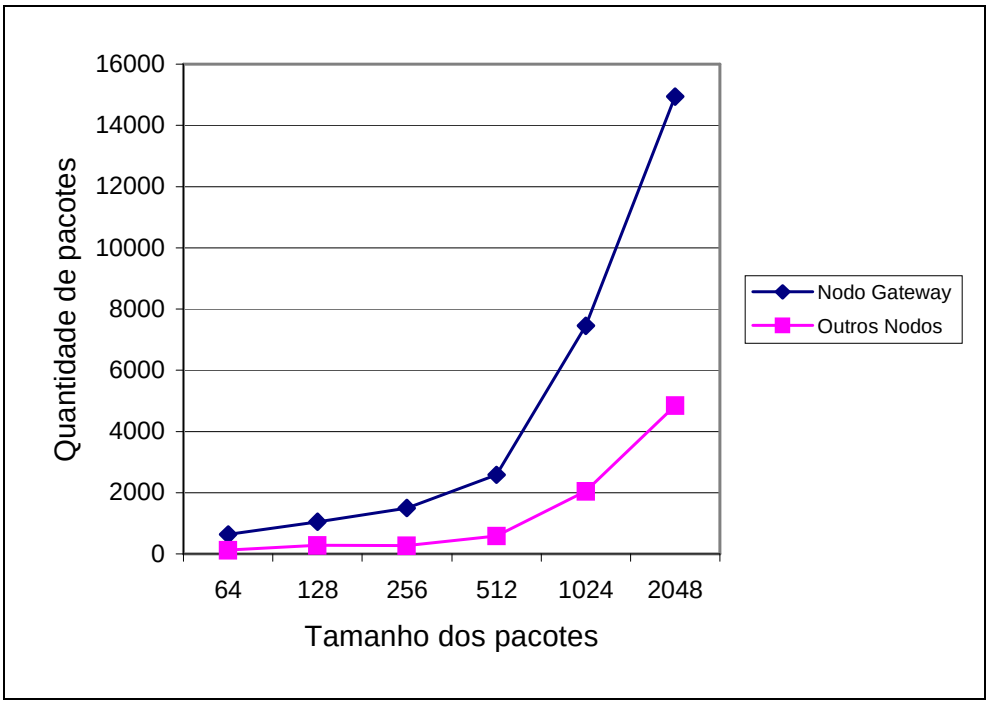


Figura 4.10: Comparação do descarte médio de pacotes no nodo *gateway* com o descarte médio de pacotes nos demais nodos

Pode-se observar que o descarte de pacotes no nodo *gateway* é muito superior ao dos demais nodos da MANET, representando 71% do descarte total ocorrido durante o processo de simulação.

Essa situação deve-se basicamente ao fato de o nodo *gateway* concentrar todas as entradas de fluxos de pacotes. Se os pacotes passaram pelo nodo *gateway*, têm grandes possibilidades de passar por todos os demais nodos, uma vez que todos possuem as mesmas características da comunicação sem fios e de mobilidade.

O descarte de pacotes nos nodos não-*gateways* pode, então, ser atribuído a características intrínsecas à comunicação sem fios, assim como a interferências eletromagnéticas, a atenuação do sinal e a desconexões dos dispositivos.

Em análise mais detalhada, a quantidade de pacotes do tipo *Route Error* (RERR) e o *overhead* de pacotes de roteamento gerados pelos processos de identificação de rotas do protocolo AODV foi comparada entre os dados obtidos nos cenários “A” e “B”.

Na Figura 4.11 é apresentada uma análise comparativa de pacotes tipo “RERR” gerados a partir do cenário “A” (protocolo original) e do cenário “B” (protocolo modificado).

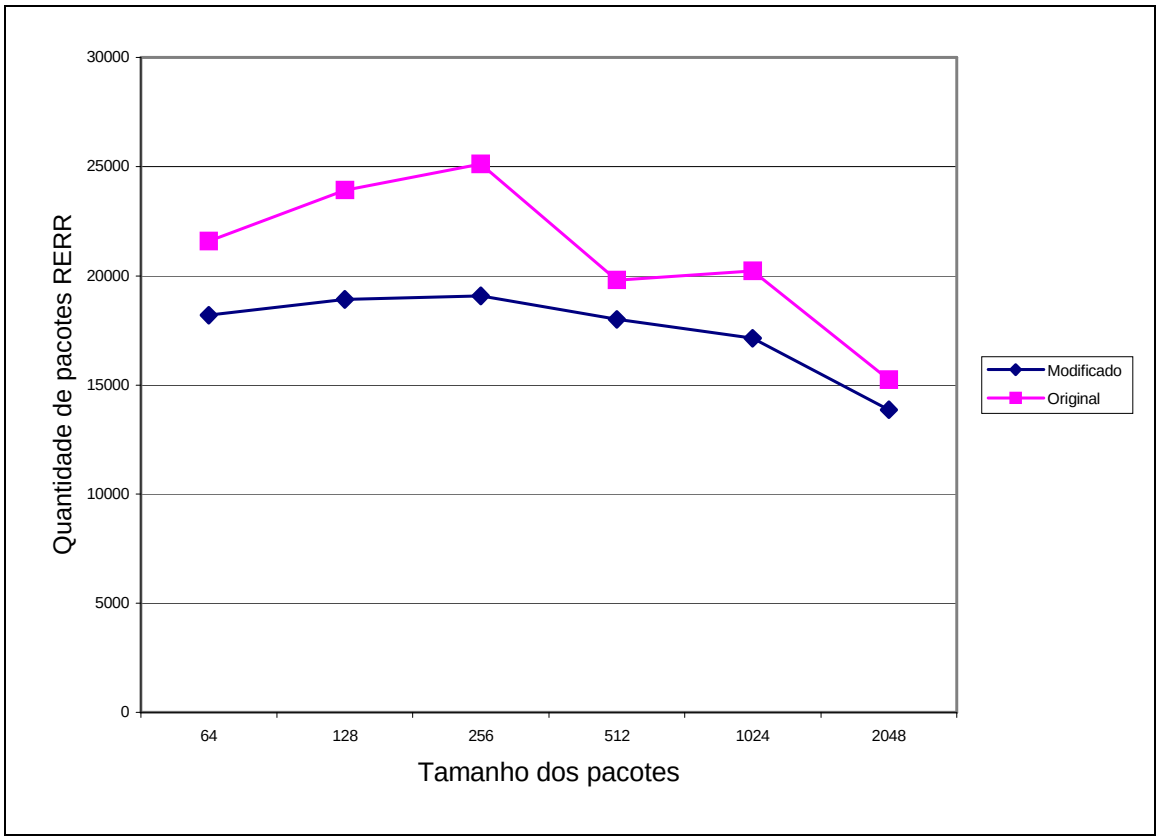


Figura 4.11: Análise comparativa do número de pacotes RERR gerado pelo protocolo

Os valores apresentados nas Figuras 4.11 e 4.12 correspondem à média das 5 taxas de tráfego de pacotes propostas para este trabalho.

Com base na Figura 4.11, pode-se perceber uma redução de pacotes do tipo "RERR". Isso demonstra que ocorreram menos quebras de rotas e, conseqüentemente, provocando uma diminuição no número mensagens para a descoberta de rotas, diminuindo o *overhead* gerado pelo protocolo de roteamento.

Na Figura 4.12 é apresentada uma análise comparativa da média de pacotes de mensagem (*overhead)* do protocolo gerada para cada um dos cenários propostos.

Pode-se perceber que o protocolo proposto neste trabalho (cenário "B") gera um *overhead* menor do que o protocolo original (cenário "A"). O nodo *gateway* realiza um número menor de processos de descobertas de rotas em razão de poder utilizar rotas que estão à sua disposição para uso imediato em sua tabela de confiabilidade. Como conseqüência da diminuição no número de processos de descoberta de rotas, menos tráfego de roteamento é gerado, sobrando mais banda para o tráfego de dados.

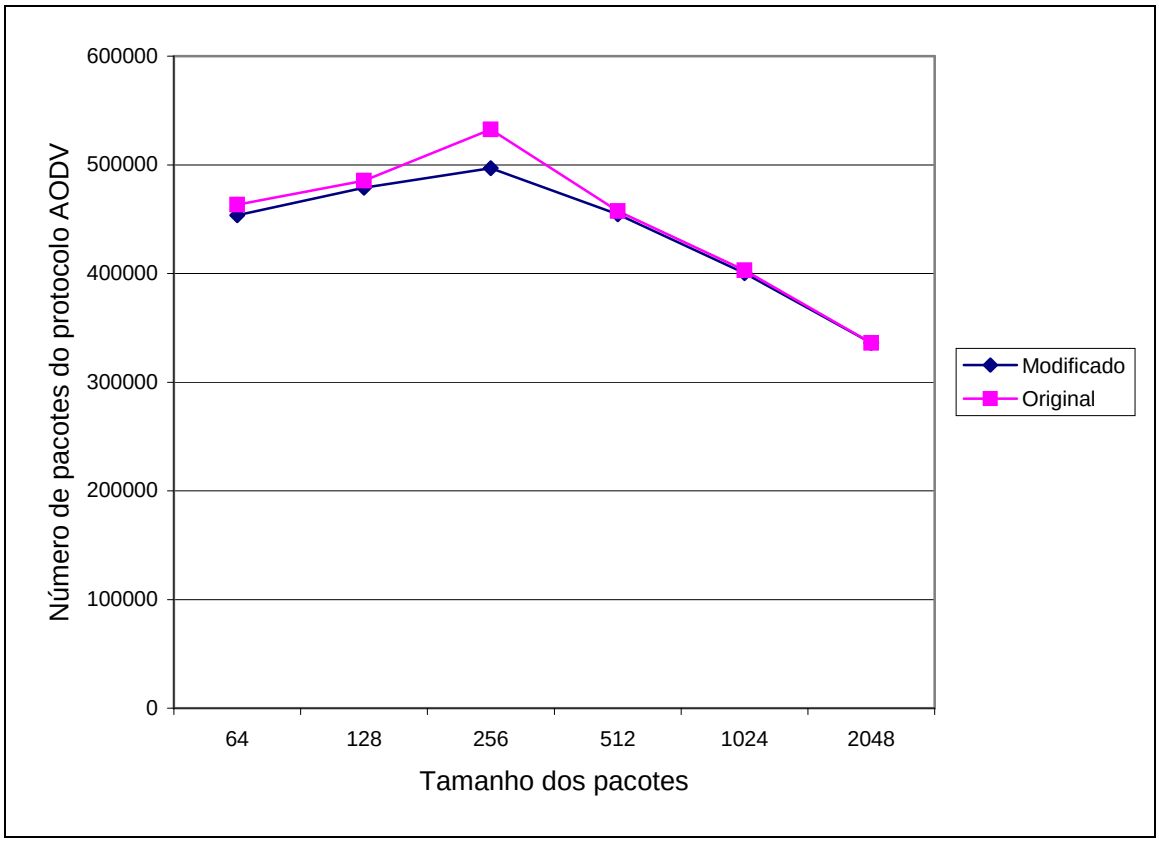


Figura 4.12: Análise comparativa do número de pacotes de sinalização do protocolo

5 CONCLUSÕES E TRABALHOS FUTUROS

5.1 Conclusões

Com o presente trabalho objetivou-se apresentar uma extensão ao protocolo de roteamento *Ad hoc On-Demand Distance Vector* (AODV) proposto por PERKINS (1998), otimizado por HAMIDIAN (2003) buscando otimizar o processo de descoberta de rotas por nodos *gateways* ao encaminhar pacotes oriundos da Internet para um nodo destino em uma MANET. Para tanto foi definido um ambiente de simulação específico, apresentado na Figura 4.1.

Essa otimização foi embasada na adição e uso de regras de confiabilidade no processo de descoberta de rotas pelo nodo *gateway* em uma rede *Ad Hoc* que implemente o protocolo de roteamento AODV. Com essa otimização era esperado reduzir o tempo gasto no processo de descoberta de uma rota pelo nodo *gateway* e também reduzir o descarte de pacotes a partir do uso de regras de confiabilidade.

Observou-se que, na maioria das vezes, o número de pacotes descartados pelo nodo *gateway* diminuiu significativamente. Também foi possível observar que as modificações realizadas no protocolo AODV, agindo especificamente no nodo *gateway*, tornam o processo de integração entre a Internet e uma MANET mais estável e com melhor desempenho do que o protocolo original. Além disso, a utilização de regras de confiabilidade no processo de obtenção de rotas a partir do nodo *gateway* influencia no desempenho do protocolo de roteamento AODV já que reduz o *overhead* de mensagens geradas pelo próprio protocolo.

Inicialmente foram tabulados e analisados apenas os resultados gerados a partir das mesmas configurações dos parâmetros de simulação propostas por Hamidian (2003). Pacotes com tamanho de 512 Bytes e intervalo de inserção de 40ms. Nessa análise obteve-se uma redução de 33% no número total de pacotes descartados e uma redução de 32% no número de pacotes descartados pelo nodo *gateway*. Nesse caso, tomando como base a Figura 4.6 e os resultados apresentados na Figura 4.9(d), pode-se observar que ao conseguir um equilíbrio entre o número de eventos atendidos "μ" em relação à taxa de chegada "λ", o descarte de pacotes é reduzido e o desempenho da rede é melhorado.

Por outro lado, a variação do número de bits por pacote "n" e também do intervalo de inserção dos pacotes, provocou um número maior de descarte de datagramas do que o esperado em algumas situações. Esse fenômeno requer uma análise mais detalhada, a ser realizada em trabalhos futuros. A redução no descarte de pacotes no nodo *gateway*, embora significativa para várias situações, mostrou-se instável e deverá ser melhor investigada.

A otimização proposta, de modo geral, proporcionou uma redução de 8%, em média, no número de pacotes do tipo "RERR" gerados pelo protocolo AODV e também proporcionou uma redução de 6%, em média, no total de pacotes destinados a obtenção

e manutenção de rotas, diminuindo o *overhead* e aumentando a sua carga útil. Esses dados podem ser observados nas Figuras 4.9, 4.10, 4.11 e 4.12 deste trabalho.

A redução de pacotes do tipo “RERR”, demonstra ainda que ocorreram menos quebras de rotas. Conseqüentemente ocorre um número menor de processos de descoberta de rotas pelo nodo gateway, a partir do uso de rotas que estão à sua disposição para uso imediato em sua tabela de confiabilidade.

Embora não se tenha conseguido medir, acredita-se que as alterações propostas nessa dissertação aumentam o consumo de recursos computacionais, assim como memória e processamento pelo nodo gateway. Alcançou-se um ganho operacional com um aumento do custo computacional. Como, na atualidade os dispositivos de comunicação e de processamento, estão cada vez mais eficientes e poderosos, acredita-se que o custo computacional não será significativo o suficiente para inviabilizar este processo.

Novas tecnologias e padrões na comunicação sem fios contribuirão para o aumento da performance das redes móveis, estejam elas isoladas ou integradas. Somado a isso, estudos sobre técnicas de otimização dos protocolos de roteamento, assim como a diferenciação de serviços, poderão tornar os protocolos de roteamento em MANETs mais completos e eficientes.

Também pode-se concluir que a taxa de pacotes fornecidas pelas fontes CBR foi pequena em comparação à cpacidade da rede infra-estruturada. Mesmo assim pôde-se perceber descarte de pacotes na interface de fila, tanto no nodo *gateway* como em outros nodos da rede móvel *Ad Hoc*. Conseqüentemente, aumentar a carga na rede ou aumentar o padrão de mobilidade, isto é, aumentar a velocidade dos nós que era, no máximo de 10 m/s (36 km/h), poderia criar um ambiente inviável.

5.2 Trabalhos Futuros

Os resultados obtidos representam apenas a análise realizada no nodo gateway e com o fluxo de pacotes originados em uma rede infra-estruturada, tendo como destino, nodos localizados na rede móvel *Ad Hoc*. Esses resultados, contudo, podem ser estendidos de modo que seja possível avaliar a relação entre todos agentes que compõem o *Mobilenode*. Assim as regras de estabilidade e confiabilidade poderiam maximizar o desempenho do protocolo como um todo.

O trabalho em questão utiliza apenas regras de estabilidade/confiabilidade de uma rota. Criar mecanismos de desempate para as situações onde duas rotas possuem o mesmo grau de confiabilidade poderia tornar os resultados mais estáveis e mais atrativos. Uma possibilidade seria criar um mecanismo que levasse em conta a combinação do estado dos *links* que geram a rota como um todo. A melhor somatória dos estados dos *links* poderiam gerar o desempate.

Somado a isso, técnicas de diferenciação de serviços podem ser testadas, utilizando outras métricas, tais como: vazão e sobrecarga de roteamento. Finalmente, as técnicas podem ser introduzidas em protocolos que já utilizam outro método para aumentar a velocidade de reação às mudanças topológicas como por exemplo, os protocolos de roteamento propostos em (CAMARA, 2004) e (TOH, 2002). Isso poderia potencializar os dois métodos e, dessa forma, melhorar ainda mais o desempenho do protocolo.

Pretende-se de imediato, realizar o mesmo processo de simulação, porém utilizando o protocolo TCP na camada de transporte e também utilizando fluxos de dados inconstantes e que permitam rajadas. Como trabalho de continuação, pretende-se

implementar o protocolo AODV com as alterações propostas nesse trabalho, em um ambiente linux utilizando os padrões IEEE 802.11b, IEEE 802.11g e IEEE 802.11a comparando os resultados com os resultados obtidos no ambiente de simulação ns-2, apresentados neste trabalho.

REFERÊNCIAS

AMODEI JR, A. **Esquema de Modulação do IEEE 802.11**. Disponível em: http://www.gta.ufrj.br/seminarios/semin2003_1/aurelio/, Acesso em: 19 de nov. 2004.

AMORIM, G. F. **Análise de Desempenho de Protocolos de Roteamento com Diferenciação de Serviços em Redes de Comunicação Ad Hoc**. 2002. Dissertação (Mestrado) - Ministério da Defesa – Exército Brasileiro, Secretaria de Ciência e Tecnologia, Instituto Militar de Engenharia, Rio de Janeiro.

ANATEL. Disponível em: <http://www.anatel.gov.br >. Acesso em: 2004.

ANDERSSON C.; SVENSSON P. Mobile internet An Industry-Wide Paradigm Shift? **Ericsson Review**, [S.l.], n.4, 1999.

BELDING-ROYER E.M.; SUN Y.; PERKINS C. **Global Connectivity for IPv4 Mobile Ad Hoc Networks**. [S.l.]: IETF Internet Draft, 2001.

CAMARA, D.; LOUREIRO, A. A. F.; ALMEIDA R. B. **GPSAL – Um algoritmo de Roteamento para Redes Móveis Ad Hoc**. Disponível em <http://www.eurecom.fr/~camara/dissertacao/node76.html>. Acesso em: 2 jun. 2004.

CHENG, T.-W. **Efficient Routing Quality of Service Support for Ad Hoc Wireless Networks**. 1998. Tese (Doutorado) - Universidade da California, Los Angeles.

CISCO SYSTEMS, INC.. **Routing Basics**. [S.l.], 1995.

COMER, D. E. **Internetworking With TCP/IP**: Principles, Protocols, and Architecture. Englewood Cliffs, NJ: Prentice-Hall, 1991.

CORDEIRO, C. de M.; et al. **Mobile Ad hoc Networking**, In: SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES, SBRC, 20., 2002 Búzios. **Minicursos**: hvro texto. Búzios: II/UFRJ, 2002.

CORSON, S.; MACKER, J. **Mobile Ad hoc networks (manet)**: Routing protocol performance issues and evaluation considerations: IETF RFC 2501. [S.l.]: IETF, 1999.

CUNHA, D. de O. **Conservação de Energia em Redes Ad Hoc.** 2004. Dissertação (Mestrado em Ciências em Engenharia Elétrica) - COPPE/UFRJ, Rio de Janeiro. Disponível em: <http://www.gta.ufrj.br/ftp/gta/TechReports/Cunha04/Cunha04.pdf>. Acesso em: 18 de nov. 2004.

DETSCH, A. **Dplot**. Disponível em <http://200.132.73.114/~detsch/>. Acesso em: 10 jan. 2005.

DHIR, A. FPGAs e WLANs. **RTI Redes, Telecom e Instalações**, [S.l.], n. 62, 2004.

GRIFFITH, E. 802.11i **Security Specification Finalized.** Disponível em: <http://www.internetnews.com/wireless/print.php/3373441>. Acesso em: 23 nov. 2004.

GRIMM, C. B. **IEEE 802.11n.** Disponível em: <http://www.wi-fi.org/OpenSection/pdf/802.11n_Q_A.pdf>. Acesso em: 19 de nov. 2004.

HAMIDIAN, A. A. **Study of Internet Connectivity for Mobile Ad Hoc Networks in NS 2.** Department of Communication Systems, Lund Institute of Technology, Lund University. 2003.

HARTMANN, L. **Gerência de Roteamento em Redes Interconectadas**. 1997. Dissertação (Mestrado em Ciência da Computação) - CPGCC - UFRGS, Porto Alegre. Disponível em: < http://penta2.ufrgs.br/Lisiane/>. Acesso em: 15 de mar. 2003

IEEE STANDARDS DEPARTMENT: IEEE STD. 802.11G (2003); Part 11: **Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications,** Amendment 4: Further Higher Date Rate Extension in the 2.4 GHz Band. Estados Unidos, 2003, 67p.

IEEE1, **Wireless LAN medium access control (MAC) and physical layer (PHY) specifications: High-speed physical layer in the 5 GHz band**. IEEE Standard 802.11a, 1999. Disponível em: <http://grouper.ieee.org/groups/802/11/> Acesso em: 2001.

IEEE2, **Wireless LAN medium access control (MAC) and physical layer (PHY) specifications: Higher-speed physical layer extension in the 2.4 GHz band**. IEEE Standard 802.11b, 1999. Disponível em: <http://grouper.ieee.org/groups/802/11/>. Acesso em: 2001.

IETF, Internet Engineering Task Force. Disponível em: <http://www.ietf.org>. Acesso em: 2000.

JOHNSON, D.B.; MALTZ, D.A. **Dynamic Source Routing in Ad HocWireless Networks**, In: IMIELINSKI, T.; KORTH, H. **Mobile Computing**. [S.l.: s.n.], 1996 p.153-181.

KO, Y.; VAIDYA, N. H. **Location Aided Routing (LAR) in mobile ad hoc networks**. In INTERNATIONAL CONFERENCE ON MÓBILE COMPUTING AND NETWORKING, 4.,1998. **Proceedings…** [S.l.: s.n.], 1998.

PERES, A.; WEBER, R. F. **Considerações sobre segurança em Redes Sem Fio.** In: SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES, SBRC, 21., 2003. **Anais Vol.I** Natal: UFRN/DIMAp, 2003, p.53-60.

PERKINS, C. E.; ROYER, E. M. **Ad hoc on demand distance vector (AODV) routing**. [S.l.], 1998.

PERKINS, C. E.; BHAGWAT, P. **Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers**. In: ACM SIGCOMM CONFERENCE, 1994, London. **Communications architectures, protocols and applications**: proceedings. [S.l.: s.n.], 1994.

RAPPAPORT, THEODORE, S. **Wireless Communications – Principles and Practices**. New Jersey: Ed. Prentice Hall PTR, 1996. 617p.

ROCHE A. et al. **Quality of Service for Ad Hoc Wireless Network**. In: SCCC XII International Conference of the Chilean Computer Science Society, 2002, Chile. Proceedings… [S.l.], 2002.

ROCHOL, J. **Redes Locais Wireless**: Texto Didático. 2004, Universidade Federal do Rio Grande do Sul – Instituto de Informática.

SANTANA, A. A. et al. **Novos Paradigmas de Projeto e Soluções de Segurança e Desempenho em Redes Sem Fio.** In: SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES, SBRC, 22, 2004, Gramado. **Minicursos**: hvro texto. Gramado: II/UFRGS,2004.

SHOEMAKE, M. B.; **Status of Project IEEE 802.11n.** Disponível em: <http://grouper.ieee.org/groups/802/11/Reports/tgn_update.htm>. Acesso em: 19 de nov. 2004.

STALLINGS, W. **Wireless Communications and Networks.** New Jersey: Prentice–Hall, 2004. 584p.

TANEMBAUN, A. S. **Computer Networks**. 3rd ed. New Jersey: Prentice Hall PTR, 1996. 813p.

TOH, C.-K. **Ad Hoc Mobile Wireless Networks:** Protocols and Systems, Upper Saddle River, New Jersey: Prentice Hall, 2002. 302p.

WAKIKAWA R. et al. **Global Connectivity for IPv6 Mobile Ad Hoc Networks**, [S.l.]: IETF, 2001.

WILSON, J. M. **Surge a próxima geração de LAN sem fio com o 802.11n.** Disponível em: <http://www.intel.com/portugues/update/contents/wi08041.htm>. Acesso em: nov. 2004.