

UNIVERSIDADE FEDERAL FLUMINENSE
CENTRO TECNOLÓGICO - ESCOLA DE ENGENHARIA
MESTRADO EM ENGENHARIA DE TELECOMUNICAÇÕES

ANNA VERÔNICA FERNANDES RIBEIRO

USO DE REDES MESH COMO SOLUÇÃO PARA O CANAL DE RETORNO DA
TV DIGITAL INTERATIVA

RIO DE JANEIRO
2007

ANNA VERÔNICA FERNANDES RIBEIRO

USO DE REDES MESH COMO SOLUÇÃO PARA O CANAL DE RETORNO DA
TV DIGITAL INTERATIVA

Dissertação apresentada ao Curso de Pós-Graduação “Stricto Sensu” em Engenharia de Telecomunicações da Universidade Federal Fluminense, como requisito parcial para obtenção do Grau de Mestre. Linha de Pesquisa: Sistemas de Telecomunicações.

Orientador: Profa. Dra. DÉBORA CHRISTINA MUCHALUAT SAADE
Co-orientador: Prof. Dr. CÉLIO VINÍCIUS NEVES DE ALBUQUERQUE

Rio de Janeiro
2007

Ficha Catalográfica elaborada pela Biblioteca da Escola de Engenharia e Instituto de Computação da UFF

R484 Ribeiro, Anna Verônica Fernandes.

Uso de redes mesh como solução para o canal de retorno da TV digital interativa / Anna Verônica Fernandes Ribeiro. – Niterói, RJ : [s.n.], 2007.

128 f.

Orientadora: Débora Christina Muchaluat Saade.

Dissertação (Mestrado em Engenharia de Telecomunicações) - Universidade Federal Fluminense, 2007.

1. Televisão digital. 2. Rede Mesh. 3. Inclusão digital. 4. Comunicações digitais. I. Título.

CDD 621.388

USO DE REDES MESH COMO SOLUÇÃO PARA O CANAL DE RETORNO DA
TV DIGITAL INTERATIVA

ANNA VERÔNICA FERNANDES RIBEIRO

Dissertação de mestrado submetida ao Programa de Mestrado em Engenharia de Telecomunicações da Universidade Federal Fluminense, como requisito parcial para obtenção do título de Mestre. Linha de Pesquisa: Sistemas de Telecomunicações.

Aprovada em Outubro de 2007:

Profa. Dra. Débora Christina Muchaluat Saade
Universidade Federal Fluminense
(Orientadora)

Prof. Dr. Célio Vinícius Neves de Albuquerque
Universidade Federal Fluminense
(Co-orientador)

Profa. Dra. Maria Luiza D'Almeida Sanchez
Universidade Federal Fluminense

Prof. Dr. Alexandre de Oliveira Dal Forno
Universidade Estadual do Rio de Janeiro

Niterói, 9 de outubro de 2007

SUMÁRIO

1. INTRODUÇÃO	1
1.1. MOTIVAÇÃO	5
1.2. OBJETIVOS	13
1.3. ESTRUTURA DA DISSERTAÇÃO	15
2. REDES SEM FIO LOCAIS E METROPOLITANAS.....	16
2.1. TECNOLOGIAS DE ACESSO AO MEIO	16
2.1.1. WiMAX.....	16
2.1.2. WI-FI	19
2.2. COMUNICAÇÃO SEM FIO ATRAVÉS DE MÚLTIPLOS SALTOS.....	22
2.2.1. REDES AD-HOC	22
2.2.2. REDES MESH	24
2.3. APLICABILIDADE – REDES CONVERGENTES	26
2.3.1. VoIP.....	26
2.3.2. IPTV	27
3. PROJETOS RELACIONADOS A REDES MESH.....	30
3.1. CIDADES DIGITAIS.....	30
3.1.1. TIRADENTES DIGITAL (MG)	30
3.1.2. PIRAÍ DIGITAL (RJ).....	32
3.1.3. SUD MENUCCI DIGITAL (SP)	33
3.1.4. TAIPEI (Taiwan).....	34
3.1.5. FILADÉLFIA (EUA)	35
3.2. PROJETOS DE PEQUISA SOBRE REDES MESH	37
3.2.1. REMESH.....	37
3.2.2. ROOFNET.....	38
3.2.3. VMESH.....	38
3.2.4. PROJETO LAPTOP A U\$100,00 (OLPC)	39
4. PROTOCOLOS DE ROTEAMENTO AD-HOC	42
4.1. PROTOCOLOS PRÓ-ATIVOS.....	43
4.1.1. DSDV (<i>Destination-Sequenced Distance Vector</i>).....	44
4.1.2. OLSR (<i>Optimized Link State Routing</i>)	44
4.1.3. WRP (<i>Wireless Routing Protocol</i>)	49
4.1.4. CGSR (<i>Cluster Gateway Switch Routing</i>).....	50
4.1.5. FSR (<i>Fisheye State Routing</i>)	51
4.2. PROTOCOLOS REATIVOS.....	54
4.2.1. DSR (<i>Dynamic Source Routing</i>).....	54
4.2.2. AODV (<i>Ad Hoc On-Demand Distance Vector</i>)	58
4.2.3. TORA (<i>Temporally Ordered Routing Algorithm</i>).....	62
4.2.4. ABR (<i>Associativity Based Routing</i>)	66
4.2.5. SSA (<i>Signal Stability-Based Adaptive Routing Protocol</i>).....	67
4.3. PROTOCOLOS HÍBRIDOS	69
4.3.1. ZRP (<i>Zone Routing Protocol</i>).....	69
4.4. TRABALHOS RELACIONADOS SOBRE COMPARAÇÃO DE PROTOCOLOS DE ROTEAMENTO AD-HOC	71
5. PROPOSTA E AVALIAÇÃO DE SOLUÇÃO PARA CANAL DE RETORNO.....	78
5.1. PROPOSTA PARA COMPARAÇÃO DE PROTOCOLOS DE ROTEAMENTO AD-HOC.....	78
5.2. CENÁRIOS CONSIDERADOS.....	79
5.3. SIMULAÇÕES REALIZADAS	85
5.4. RESULTADOS OBTIDOS	88
5.4.1. Perda	88
5.4.2. Vazão.....	92
5.4.3. Atraso	95
5.4.4. <i>Overhead</i>	104
6. CONCLUSÕES.....	106

6.1. CONTRIBUIÇÕES	108
6.2. TRABALHOS FUTUROS	108
REFERÊNCIAS BIBLIOGRÁFICAS	110

LISTA DE FIGURAS

Figura 1: Comparação da taxa de acesso à Internet em relação a urbanização.	2
Figura 2: Mapa da exclusão digital no Brasil.	2
Figura 3: Teledensidade - Concentração de acessos fixos instalados no território nacional. .	6
Figura 4: Evolução da teledensidade no Brasil.	7
Figura 5: Evolução dos acessos fixos instalados em território nacional.....	7
Figura 6: Densidade populacional brasileira e potencial de consumo per capita brasileiro. .	10
Figura 7: Penetração da Banda Larga.....	11
Figura 8: Acessos banda larga no território nacional.	12
Figura 9: Topologia de rede mesh.....	13
Figura 10: Padrões IEEE 802 para redes sem fio.	17
Figura 11: Taxa das variedades do padrão IEEE 802.11	20
Figura 12: Comparação entre as variedades do Padrão IEEE 802.11.....	21
Figura 13: Redes ad-hoc. A) Comunicação em um salto. B) Comunicação em vários saltos.	22
Figura 14: Redes mesh.	24
Figura 15: Redes mesh – WiMAX e Wi-Fi.	25
Figura 16: Padrões de uma rede VoIP.	26
Figura 17: Elementos de uma rede IPTV.	27
Figura 18: Modelos de set-top box (STB).....	28
Figura 19: Rede mesh na cidade de Tiradentes, MG	32
Figura 20: Topologia do Projeto Piraí Digital no Rio de Janeiro.	33
Figura 21: Topologia do Projeto Sud Menucci Digital no estado de São Paulo.	34
Figura 22: Arquitetura da rede mesh da Nortel Networks implantada em Taipei.	35
Figura 23: Área abrangida pelo Projeto cidade digital da Filadélfia.	36
Figura 24: Arquitetura da solução da empresa Tropos Networks, usada na Filadélfia.	37
Figura 25: Topologia simplificada do Projeto VMesh.	39
Figura 26: Laptop de U\$100,00, modelo 2B1, desenvolvido para propiciar a inclusão digital.	40
Figura 27: Adesão mundial ao projeto OLPC.	41
Figura 28: Principal classificação dos protocolos de roteamento ad-hoc.....	43
Figura 29: Multipoint Relays.	45
Figura 30: Formato básico do pacote no OLSR.	46
Figura 31: Formato do pacote <i>Hello</i> no OLSR.	46
Figura 32: Formato do pacote TC no OLSR.....	47
Figura 33: Trajeto dos pacotes – protocolo CGSR.....	51
Figura 34: Formato do pacote de estado do enlace para o protocolo FSR.....	53
Figura 35: Formato do pacote route request do protocolo DSR.....	57
Figura 36: Formato do pacote route reply do protocolo DSR.....	57
Figura 37: Formato do pacote route error do protocolo DSR.....	57
Figura 38: Formato do pacote de confirmação (ACK) do protocolo DSR - opcional.....	58
Figura 39: Formato do pacote de RREQ do protocolo AODV.....	59
Figura 40: Formato do pacote de RREP do protocolo AODV.....	59
Figura 41: Formato do pacote de RERR do protocolo AODV.....	61
Figura 42: Formato do pacote de query (QRY) do protocolo TORA.....	63
Figura 43: Formato do pacote de update (UPD) do protocolo TORA.....	63
Figura 44: Manutenção e eliminação de rota no protocolo TORA.....	64
Figura 45: Formato do pacote de clear (CLR) do protocolo TORA.....	64
Figura 46: Formato do pacote optimization (OPT) do protocolo TORA.....	65
Figura 47: Formato do pacote route query/reply do protocolo IERP (inter-zona - reativo)..	70
Figura 48: Tabela comparativa utilizada pela referência [Sesay et al, 2004] para definição do protocolo de roteamento mais indicado para o cenário proposto.	71

Figura 49: Tabela comparativa utilizada pela referência [Pereira e Pedroza, 2004] para definição do protocolo de roteamento mais indicado para o cenário proposto.....	72
Figura 50: Tabela comparativa utilizada pela referência [Campista et al, 2006] para definição dos cenários propostos para simulação.....	73
Figura 51: Tabela comparativa utilizada pela referência [Broch, 1998] para 20 fontes CBR, identificando a quantidade de pacotes entregues ao destino que utilizaram a rota de melhor caminho ou precisaram de mais saltos do que a rota de melhor caminho.....	75
Figura 52: Ranking elaborado a partir dos resultados encontrados conforme referência [Peiyan e Layuan, 2006].	77
Figura 53: Vista aérea atual da Comunidade da Maré.	80
Figura 54: Topologia de rede mesh utilizada - backbone.....	83
Figura 55: Gráfico referente a perda do protocolo AODV.	88
Figura 56: Gráfico referente a perda do protocolo DSDV.....	89
Figura 57: Gráfico referente a perda do protocolo DSR.	89
Figura 58: Gráfico referente a Perda do protocolo OLSR.	89
Figura 59: Gráfico comparativo referente a Perda CBR de todos os protocolos avaliados: AODV, DSR, DSDV e OLSR.	90
Figura 60: Gráfico comparativo referente a Perda TCP de todos os protocolos avaliados: AODV, DSR, DSDV e OLSR.	91
Figura 61: Gráfico referente a vazão do protocolo AODV.	92
Figura 62: Gráfico referente a vazão do protocolo DSDV.	92
Figura 63: Gráfico referente a vazão do protocolo DSR.....	93
Figura 64: Gráfico referente a vazão do protocolo OLSR.	93
Figura 65: Gráfico referente a vazão agregada	94
Figura 66: Gráfico consolidado referente ao atraso dos protocolos: AODV, DSDV, DSR e OLSR.	95
Figura 67: Gráfico referente ao overhead dos protocolos AODV, DSR, OLSR e DSDV....	104

LISTA DE TABELAS

Tabela 1: Padrões 802.16 com suas características técnicas	17
Tabela 2: Padrões 802.11 com suas características técnicas	19
Tabela 3: Variedades do padrão 802.11 (Wi-Fi)	20
Tabela 4: Características dos protocolos de roteamento: DSDV, DSR, AODV e OLSR.....	78
Tabela 5: População em Municípios do Estado do Rio de Janeiro.....	81
Tabela 6: População nas principais comunidades carentes do Município do Rio de Janeiro.	81
Tabela 7: Quadro comparativo do percentual de perda, maior e menor atraso identificados em cada protocolo de roteamento.	96
Tabela 8: Pacotes TOP 10 em atraso para os piores casos (atrasos superiores a 3 segundos)	97
Tabela 9: Atribuição de notas para os protocolos de acordo com os parâmetros mensurados.	107

RESUMO

Esta dissertação propõe o uso de redes mesh como solução para a implementação do canal de interatividade para o Sistema Brasileiro de TV Digital em áreas do país onde não existe infra-estrutura de cabeamento instalada, como por exemplo, nas comunidades urbanas carentes das grandes cidades brasileiras. A dissertação analisa características do cenário considerado, e também discute e compara alguns protocolos de roteamento para redes ad-hoc através de simulações realizadas com o software *Network Simulator 2* (NS-2).

Palavras-chaves. TV Digital Interativa, Canal de Retorno, Redes Mesh, Protocolo de Roteamento Ad-Hoc, Inclusão Digital.

ABSTRACT

This dissertation proposes the use of wireless ad hoc networks as a solution for the interactivity channel of the Brazilian Digital TV System in geographical areas where no cabling infrastructure exists, e.g. underprivileged communities in big Brazilian cities. It analyzes the background information of this scenario as well as explores and compares some routing protocols for ad hoc networks through simulations with the Network Simulator software (NS-2).

Keywords. Digital TV, Interactivity Channel, Routing Protocols for Ad Hoc Networks, Digital Inclusion.

1. INTRODUÇÃO

Atualmente, com o desenvolvimento das tecnologias de comunicação de dados, o desenvolvimento da Internet, o desenvolvimento de interfaces mais amigáveis aos usuários comuns de computadores e, por conseguinte, a crescente facilidade em se encontrar informações sobre praticamente qualquer assunto na *web*, nos deparamos com uma sociedade baseada no acesso às informações.

Nesta sociedade, a lacuna entre a camada da população que tem acesso às informações e a camada que não possui tal acesso torna-se cada vez maior à medida que o conhecimento fica restrito e condicionado a existência de uma renda suficiente para se dispor de equipamentos que permitam o acesso à Internet. Assim, as melhores oportunidades de crescimento profissional e até mesmo pessoal e cultural também ficam restritas. Este fenômeno é chamado de exclusão digital [Becker e Montez, 2004]. Com o intuito de diminuir esta diferença e proporcionar a inclusão digital (e conseqüentemente social), o governo brasileiro tem investido esforços para tentar facilitar o acesso das classes mais baixas a computadores pessoais com acesso à Internet.

A Figura 1 mostra a comparação da taxa de acesso à Internet com relação à urbanização, identificando toda a região rural como um potencial foco de investimento em inclusão digital. A Figura 1 possui como fonte CPS (Centro de Políticas Sociais) / FGV (Fundação Getúlio Vargas) [CPS/FGV, 2007] [CPS/FGV b, 2007] a partir dos dados Sistema Nacional de Avaliação da Educação Básica (SAEB) / Ministério da Educação (MEC).

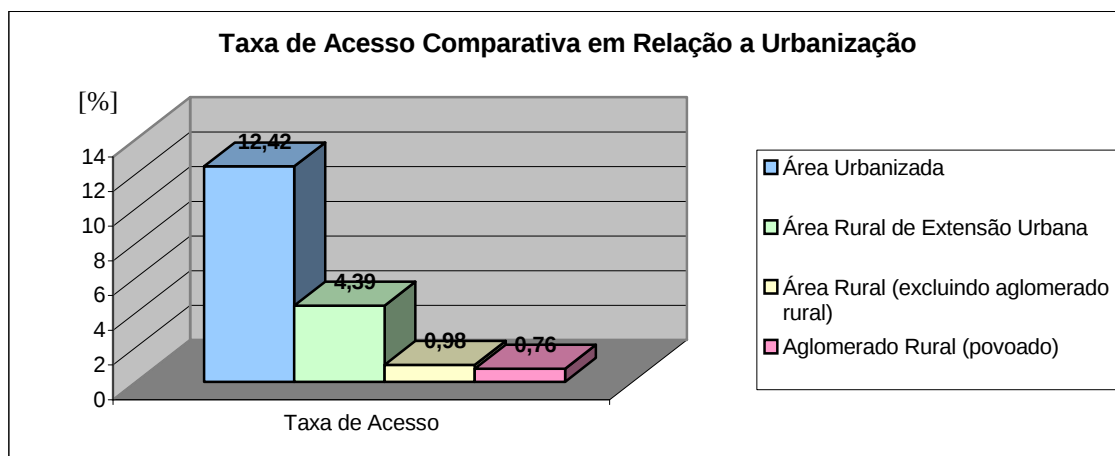


Figura 1: Comparação da taxa de acesso à Internet em relação a urbanização.

Fonte: CPS/FGV a partir dos dados SAEB/MEC [CPS/FGV, 2007] [CPS/FGV b, 2007].

A Figura 2 mostra o mapa de exclusão digital no Brasil, o qual indica alguns estados com quase a totalidade de seus territórios de excluídos digitais.

MAPA DA EXCLUSÃO DIGITAL

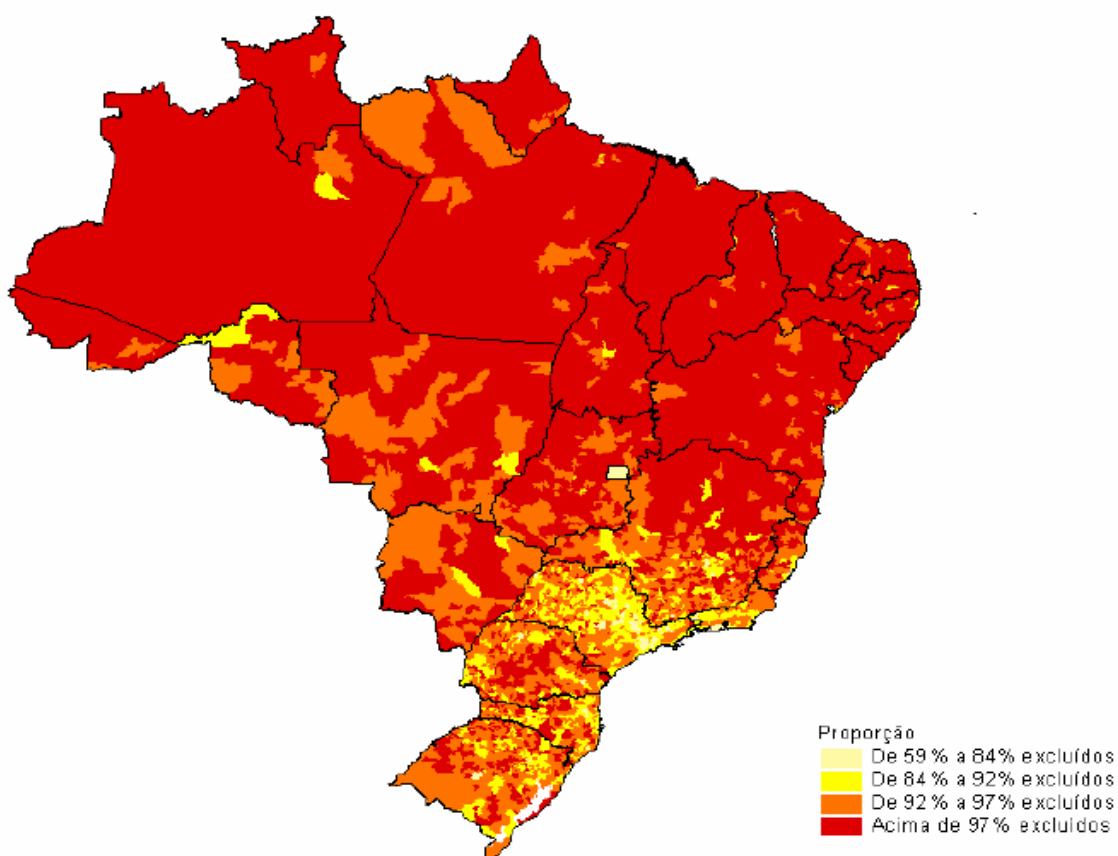


Figura 2: Mapa da exclusão digital no Brasil.

Fonte: CPS/FGV a partir dos dados SAEB/MEC [CPS/FGV, 2007] [CPS/FGV b, 2007]

Em outro âmbito, ocorreu nos últimos anos uma grande discussão sobre a tecnologia que deveria ser adotada para a implementação do novo Sistema Brasileiro de Televisão Digital. Dentre os padrões testados encontravam-se: o europeu (DVB – *Digital Video Broadcast*), o japonês (ISDB – *Integrated Services Digital Broadcasting*) e o americano (ATSC – *Advanced Television Systems Committee*) [Becker e Montez, 2004]. No dia 29 de junho de 2006, foi definido que o Sistema Brasileiro de TV Digital Terrestre (SBTVD-T) será baseado no sistema japonês (ISDB), mas incluirá inovações desenvolvidas pelos pesquisadores e centros científicos brasileiros em conjunto com os japoneses através de um Fórum Internacional. Estas inovações estarão focadas no suporte a interatividade, principal desvantagem do padrão japonês. No prazo de sete anos, o novo sistema deverá estar funcionando em todo o país.

Assim, o país já identificou que a inclusão digital é uma necessidade da grande maioria da população, e esse assunto está sendo colocado pelo governo como prioridade para definição da plataforma e dos serviços a serem oferecidos com o novo sistema.

A televisão aberta atinge hoje a grande maioria dos lares brasileiros e, através da televisão digital aberta e gratuita, almeja-se levar a todas as classes da população o acesso à informação hoje não disponível para quem não possui um computador conectado à Internet. Entretanto, para oferecer o acesso à informação através de aplicações interativas, como a *web*, por exemplo, é necessária a presença de um canal de interatividade que permitirá a transmissão de dados no sentido contrário ao do canal de difusão, ou seja, do usuário para a emissora de TV.

Para o recebimento do sinal digital, os usuários precisariam trocar os aparelhos de televisão analógicos. Com o intuito de amenizar este investimento inicial, pode-se utilizar um set-top box capaz de converter o sinal digital para o aparelho de TV tradicional, que tem um custo bem inferior ao de uma televisão digital. O set-top box é o equipamento que fica efetivamente conectado ao canal de retorno.

A interatividade será habilitada pelo canal de retorno e possibilitará aplicações como compras online, escolhas antecipadas de programação de TV, permissão ou proibição de canais ou até mesmo possibilidade de o assinante prover conteúdo de

vídeo. Entretanto, a banda disponível no canal de retorno é um fator que limita o nível de interatividade que estará disponível ao usuário final.

Para prover o canal de retorno deve-se optar por algum meio (cabo metálico, fibra, rádio, satélite dentre outros), por alguma tecnologia (protocolo a ser utilizado, equipamentos associados à tecnologia) e também se deve definir a largura de banda mínima necessária, assim como outros parâmetros limitantes do canal de comunicação (atraso máximo, perda máxima, entre outros).

A escolha por estes parâmetros em detrimento de outros varia de acordo com o grau de interatividade a ser proporcionado e o cenário em que o ambiente está inserido. Por exemplo, em uma comunidade urbana carente a densidade populacional é alta, enquanto que em uma zona rural afastada, nos deparamos com o oposto. Assim, esta avaliação torna-se fundamental para a escolha do meio, da tecnologia e dos outros parâmetros limitantes mencionados.

A capilaridade da rede e o valor a ser pago pelo serviço de acesso também devem ser considerados, uma vez que é intenção do governo brasileiro incentivar o uso desta tecnologia por todas as camadas da população.

Este trabalho investiga o uso de redes sem fio de múltiplos saltos, como alternativa de baixo custo, para implementação do canal de interatividade da TV digital em certas áreas do país. Propõe-se uma comparação de desempenho entre os principais protocolos de roteamento ad-hoc usados em redes sem fio, para viabilização da utilização do canal de retorno da TV digital interativa para inclusão digital.

Para a determinação do protocolo de roteamento mais adequado ao cenário proposto, são avaliadas métricas de vazão, atraso, perda e overhead para cada um dos protocolos considerados. O fator predominante para a escolha de um protocolo de roteamento ad-hoc é o tipo de aplicação a ser utilizada no cenário proposto. Para a implementação do canal de retorno da TV digital interativa compartilhando banda com aplicações na Internet, uma importante, senão a principal característica, é a vazão conseguida, seguida pelo atraso e percentual de perda, com o overhead sendo uma questão para otimização da rede.

1.1. MOTIVAÇÃO

Uma das opções viáveis é a utilização de linhas telefônicas como solução para o canal de retorno, porém conforme a Figura 3, o Brasil ainda tem muitas áreas com uma teledensidade (total de linhas instaladas por 100 habitantes) muito pequena, o que inviabilizaria determinadas regiões de possuírem o canal de retorno e um provável acesso à Internet. A Figura 4 mostra a evolução da teledensidade no Brasil [Revista Teletime, 2006].

Outra possibilidade seria o provimento deste acesso através da telefonia móvel, a qual já chega a 100 milhões de terminais habilitados¹ em território nacional (somando-se as bandas A, B, D e E). Porém os altos preços praticados pelas operadoras de telecomunicações inviabilizam a adoção deste meio para a solução do canal de retorno, uma vez que a intenção é permitir acesso para todas as classes sociais.

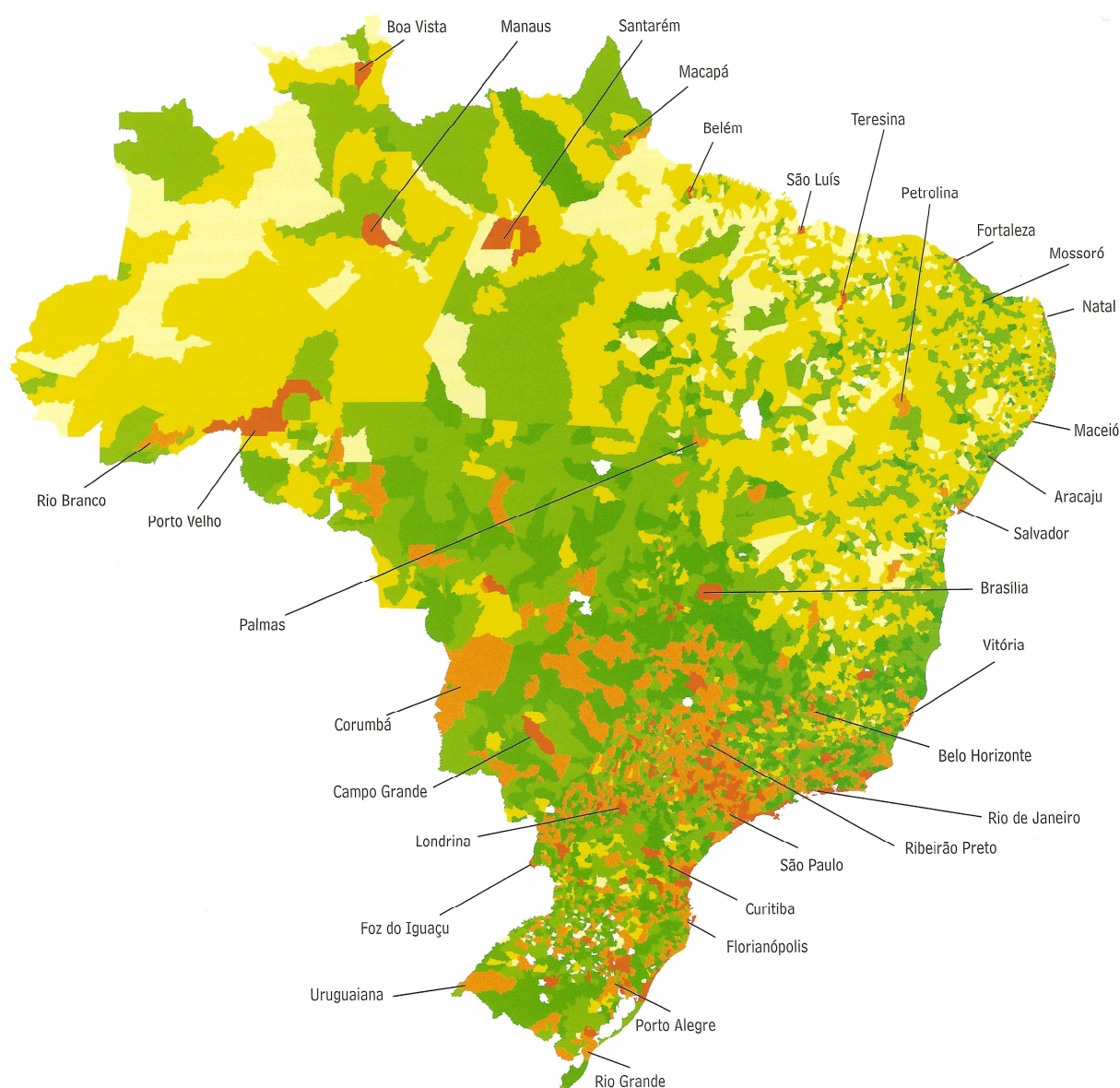
¹ Referência: ano de 2006 conforme dado da Revista Teletime - Atlas Brasileiro de Telecomunicações, Número 6, 2006 [Revista Teletime, 2006].



Telefonia fixa

Teledensidade

Concentração de acessos fixos instalados no território nacional



LINHAS INSTALADAS POR 100 HABITANTES

0 a 3 (434)	7 a 13 (1.523)	Acima de 33 (171)
3 a 25 (1.848)	10 a 20 (1.068)	
5 a 7 (753)	20 a 33 (690)	

Obs.: As áreas plotadas representam o território total dos municípios representados, e não apenas o perímetro urbano. Os números entre parênteses representam o total de municípios cobertos por faixa.

Fonte: Anatel e Brasil em Foco 2005. Base: acessos instalados em setembro/2005.

Figura 3: Teledensidade - Concentração de acessos fixos instalados no território nacional.

Fonte: Atlas Brasileiro de Telecomunicações 2006 – Revista TELETIME



Figura 4: Evolução da teledensidade no Brasil.

Fonte: Atlas Brasileiro de Telecomunicações 2006 – Revista TELETIME

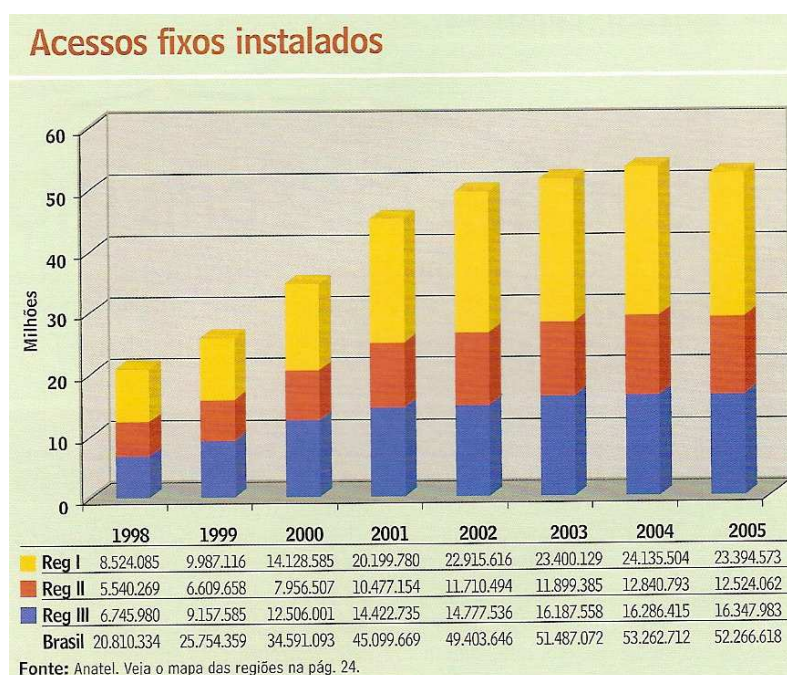


Figura 5: Evolução dos acessos fixos instalados em território nacional.

Fonte: Atlas Brasileiro de Telecomunicações 2006 – Revista TELETIME

A Figura 5 mostra a evolução da quantidade absoluta de acessos telefônicos fixos desde 1998 (ano da privatização do Sistema Telebrás de Telecomunicações) até 2005. O crescimento inicial foi motivado pelo PGMU - Plano Geral de Metas de Universalização outorgado pela ANATEL (Agência Nacional de Telecomunicações), no qual as *incumbents*² deveriam cumprir uma série de imposições para manterem

² *Incumbents*: Empresas oriundas das empresas do sistema Telebrás: Telemar, Brasil Telecom e Telefônica.

seus direitos de concessão. Uma das obrigações a cumprir seria a instalação de acessos telefônicos em lugares que possuíssem no mínimo 100 habitantes³, tais metas deveriam ser atendidas até o início do ano de 2005. Nos anos seguintes a 2002, o crescimento manteve-se muito tímido, tendo até um decréscimo do ano de 2004 para 2005. Evidencia-se um desinteresse por parte das operadoras de telecomunicações em investir em novos acessos telefônicos, o que pode ser explicado pela Figura 6, a qual identifica o poder de consumo brasileiro, assim como a densidade populacional brasileira. Uma empresa privada, em geral, visa o lucro e investir em certas regiões do Brasil é garantia de não obter o buscado retorno dos investimentos, pois existem muitas regiões que não possuem nenhuma condição de manter os altos custos de uma linha telefônica, muito menos das tarifas das ligações.

Para tentar minimizar esta dificuldade, a ANATEL outorgou também a criação do FUST - Fundo de Universalização dos Serviços de Telecomunicações - conforme Lei Número 9.998, de 17 de agosto de 2000. O FUST teve por finalidade proporcionar recursos destinados a cobrir a parcela de custo exclusivamente atribuível ao cumprimento das obrigações de universalização de serviços de telecomunicações, que não possa ser recuperada com a exploração eficiente do serviço.

A criação do FUST teve como principais objetivos:

- Atendimento a localidades com menos de cem habitantes;
- Complementação de metas estabelecidas no Plano Geral de Metas de Universalização para atendimento a comunidades de baixo poder aquisitivo;
- Implantação de acessos individuais para prestação do serviço telefônico, em condições favorecidas, a estabelecimentos de ensino, bibliotecas e instituições de saúde;
- Implantação de acessos para utilização de serviços de redes digitais de informação destinadas ao acesso público, inclusive da Internet, em condições favorecidas, a instituições de saúde, estabelecimentos de ensino e bibliotecas, incluindo os equipamentos terminais para operação pelos usuários;

³ O PGMU garante o direito da população a um telefone público (TUP) em localidades com no mínimo 100 habitantes e garante a obrigatoriedade de instalação caso ocorra a solicitação de telefone residencial em localidades com no mínimo 300 habitantes.

- Redução das contas de serviços de telecomunicações de estabelecimentos de ensino e bibliotecas referentes à utilização de serviços de redes digitais de informação destinadas ao acesso do público, inclusive da Internet, de forma a beneficiar em percentuais maiores os estabelecimentos freqüentados por população carente, de acordo com a regulamentação do Poder Executivo;
- Instalação de redes de alta velocidade, destinadas ao intercâmbio de sinais e à implantação de serviços de teleconferência entre estabelecimentos de ensino e bibliotecas;
- Atendimento a áreas remotas e de fronteira de interesse estratégico;
- Implantação de acessos individuais para órgãos de segurança pública;
- Implantação de serviços de telecomunicações em unidades do serviço público, civis ou militares, situadas em pontos remotos do território nacional;
- Fornecimento de acessos individuais e equipamentos de interface a instituições de assistência a deficientes;
- Fornecimento de acessos individuais e equipamentos de interface a deficientes carentes;
- Implantação da telefonia rural.

Mesmo com todas as iniciativas e projetos para permitir e incentivar o acesso à Internet à camada da população mais pobre, o resultado é muito aquém ao esperado. O telefone fixo pré-pago, por exemplo, oferecido atualmente pelas operadoras, é uma tentativa de baratear os custos, porém ainda existe uma grande parcela da população que ainda assim não consegue arcar com tais custos.

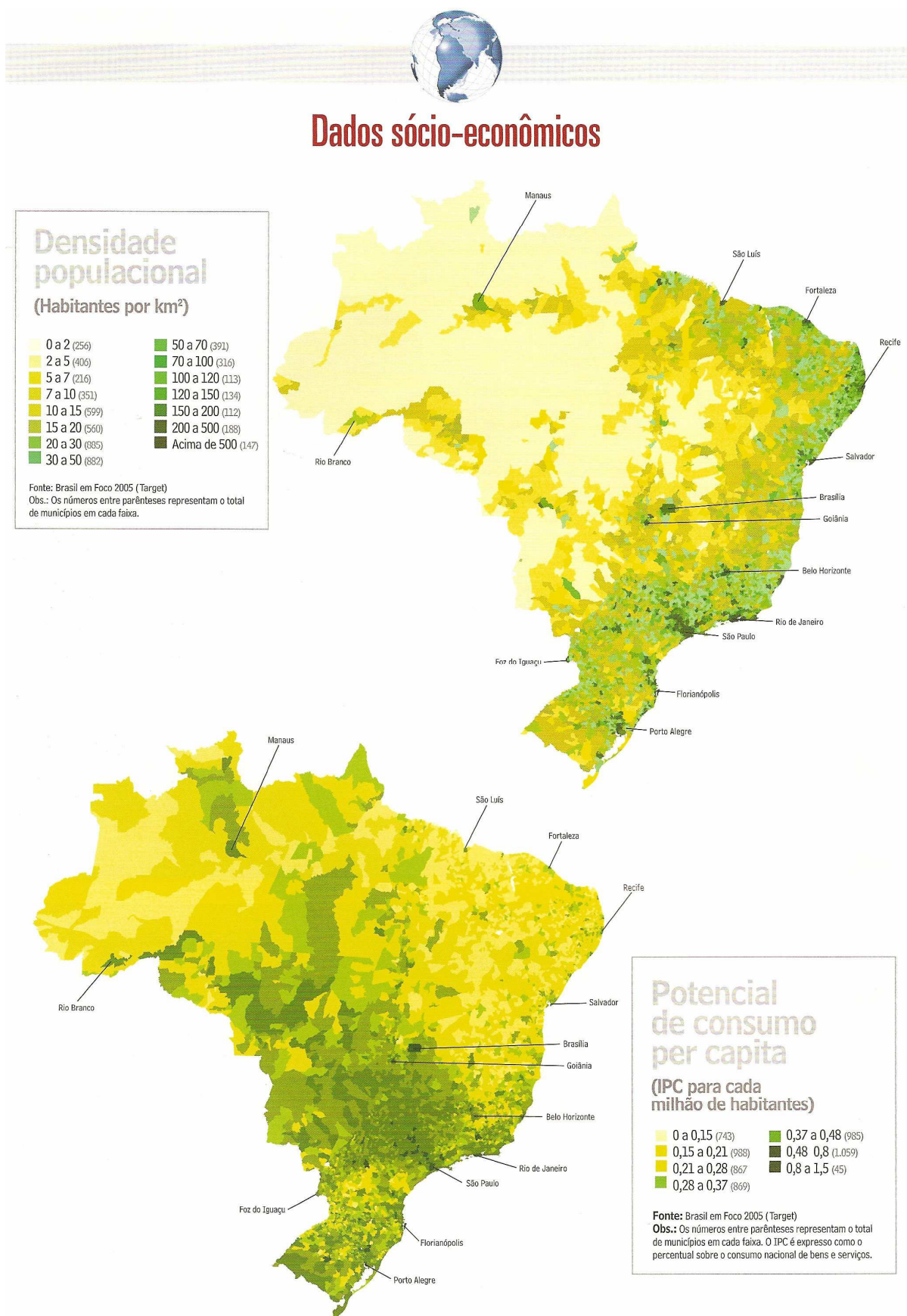


Figura 6: Densidade populacional brasileira e potencial de consumo per capita brasileiro.

Fonte: Atlas Brasileiro de Telecomunicações 2006 – Revista TELETIME

Tecnologias de acesso como ADSL e *cable modem* precisam necessariamente de infra-estrutura cabeada chegando ao local do assinante. A Figura 7 mostra a penetração dos acessos banda larga no Brasil comparado a outros países. Na Figura 8 é explicitada a distribuição das tecnologias de acessos banda larga em território nacional.

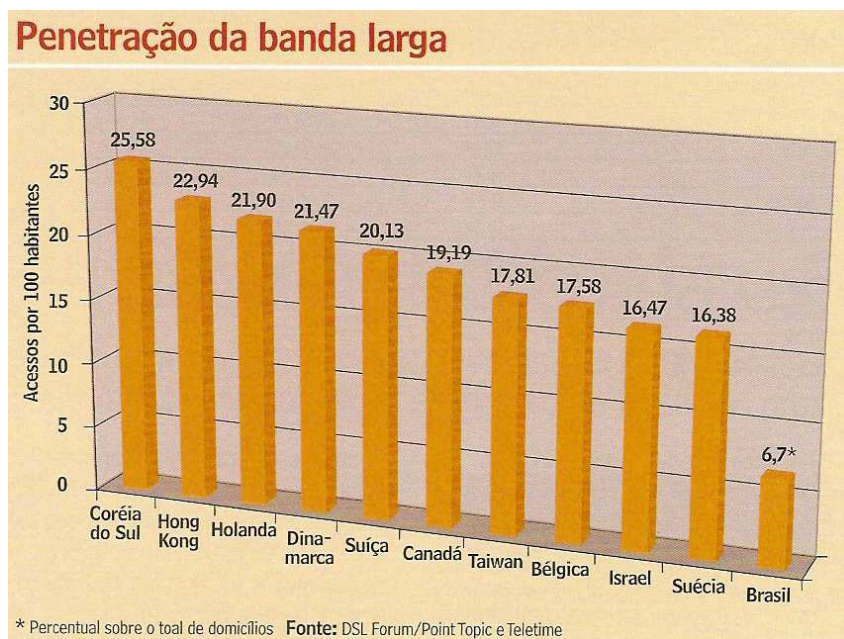


Figura 7: Penetração da Banda Larga.

Fonte: Atlas Brasileiro de Telecomunicações 2006 – Revista TELETIME

Serviço residencial e SoHo

Distribuição das tecnologias de banda larga por município



Figura 8: Acessos banda larga no território nacional.

Fonte: Atlas Brasileiro de Telecomunicações 2006 – Revista TELETIME

Considerando o cenário apresentado, vivenciado pela maioria da população brasileira, são necessárias formas alternativas de baixo custo para possibilitar o

acesso à Internet, principalmente para a população mais carente. As redes sem fio podem ser uma alternativa para popularizar o acesso à Internet em comunidades com baixo poder aquisitivo, através do canal de interatividade disponibilizado pela TV digital aberta e gratuita.

É com esta motivação que a presente dissertação aborda alternativas de baixo custo usando comunicação sem fio, através de redes em malha, para popularização do acesso à Internet.

1.2. OBJETIVOS

As redes mesh (redes em malha) são construídas através de nós fixos e móveis interconectados via enlaces sem fio, formando uma rede ad-hoc de múltiplos saltos.

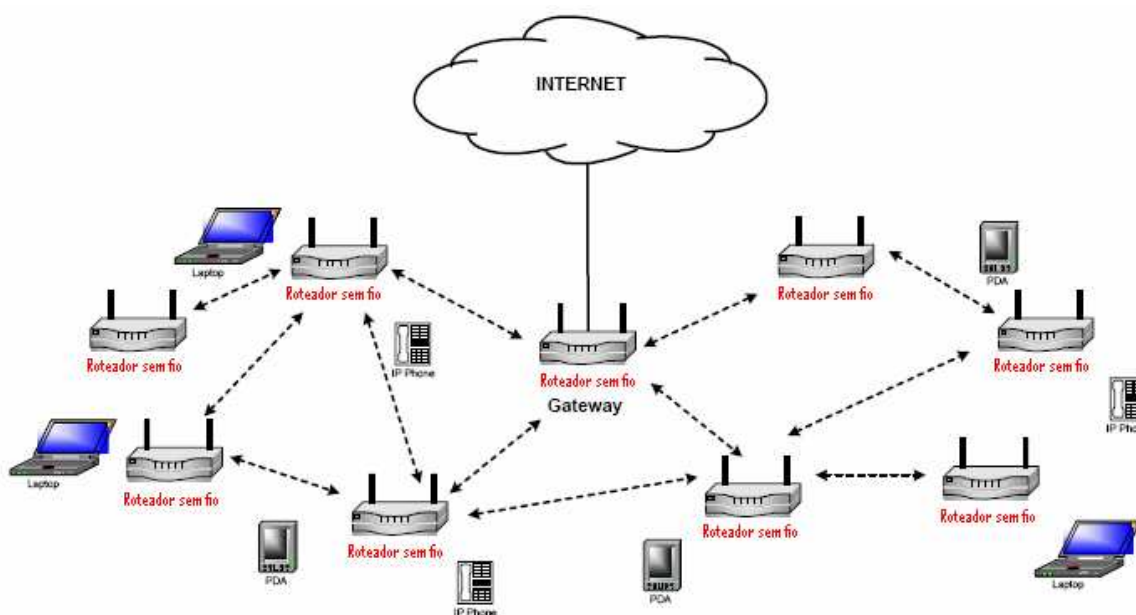


Figura 9: Topologia de rede mesh.

A Figura 9 apresenta um exemplo de topologia de redes mesh, onde os roteadores sem fio comunicam-se com a Internet através de um roteador *gateway*.

Esta dissertação investiga o uso de redes mesh para popularizar o acesso à Internet em comunidades carentes brasileiras e como possível solução para o canal de interatividade do novo Sistema Brasileiro de Televisão Digital em regiões do país

onde não existe infra-estrutura de cabeamento instalada, como por exemplo, nas comunidades urbanas carentes das grandes cidades brasileiras. Considerando o uso de redes mesh, as quais utilizam protocolos de roteamento de redes ad-hoc [Manoj e Murthy, 2004] para realizar a transmissão em múltiplos saltos, faz-se necessária a escolha do protocolo de roteamento do núcleo da rede. Existem várias possibilidades de escolha de protocolos de roteamento propostos na literatura [Manoj e Murthy, 2004] [Cordeiro e Agrawal, 2002]. Como intuito de orientar esta escolha, esta dissertação:

- apresenta um *survey* sobre os principais protocolos existentes;
- avalia o desempenho de alguns protocolos através de simulações usando o software *Network Simulator 2* (NS-2) [NS2, 2005], considerando o uso da rede por diferentes aplicações (dados, voz e vídeo). Para a comparação de desempenho entre os protocolos de roteamento considerados, são avaliadas métricas de vazão, atraso, perda e overhead para cada um dos protocolos considerados.

Assim sendo, esta dissertação tem como objetivo principal avaliar uma forma alternativa para permitir o acesso à Internet para a população de baixa renda. Este enfoque é fundamental, dentre outras motivações, por iniciar ou aprofundar a discussão sobre a inclusão digital, desta forma a proposta não só é válida por tentar identificar uma maneira de solucionar a falta de acesso à Internet das comunidades carentes, mas também por motivar a discussão sobre assunto, incentivando o estudo, e assim o surgimento de novas propostas.

Dentre as contribuições desta dissertação, pode-se destacar:

- Estudo sobre os principais protocolos de roteamento para redes ad-hoc;
- Modelagem de um cenário que representa comunidades carentes, usando a comunidade urbana carente da cidade do Rio de Janeiro, chamada Maré, como referência. O cenário modelado considera o uso da rede de acesso por diferentes aplicações que geram tráfego de dados tradicionais, voz e vídeo, considerando diferentes níveis de interatividade em um sistema de TV digital levando em consideração que o acesso à Internet poderia ser viabilizado inicialmente para centros comunitários, hospitais e postos de saúde;

- Avaliação do desempenho de protocolos de roteamento ad-hoc, considerando vazão, perda de pacotes, retardo e overhead de controle;
- Avaliação do desempenho de aplicações multimídia, de voz e vídeo, co-existindo com aplicações de dados.

1.3. ESTRUTURA DA DISSERTAÇÃO

Esta dissertação está organizada como segue. No Capítulo 2, é apresentada uma visão geral sobre os principais padrões para redes sem fio locais e metropolitanas utilizados para construção de redes mesh, comentando o seu uso para serviços que envolvem comunicação de dados, voz e vídeo. No Capítulo 3, são comentados os principais projetos comerciais e acadêmicos que utilizam o conceito de redes mesh sem fio para acesso à Internet de baixo custo e promoção da inclusão digital. No Capítulo 4, são discutidos os principais protocolos de roteamento para redes ad-hoc citados na literatura, apontando alguns trabalhos relacionados a comparação de desempenho de diversos protocolos através de simulações. No Capítulo 5, é detalhada a proposta de solução para canal de retorno, assim como os cenários pesquisados, as métricas usadas para a avaliação dos protocolos de roteamento com o uso do software NS-2, as simulações realizadas e os resultados obtidos. No Capítulo 6, são apresentadas as conclusões, salientando as principais contribuições da dissertação e os trabalhos futuros.

2. REDES SEM FIO LOCAIS E METROPOLITANAS

Existem algumas possibilidades, dentre as tecnologias disponíveis atualmente, para se prover a comunicação de dados, permitindo o acesso à Internet. Assim, é necessário entender o funcionamento e as especificidades de cada uma para que ocorra uma escolha embasada. O Comitê 802 do IEEE (*Institute of Electrical and Electronics Engineers*) é o grupo que lidera a padronização de redes locais (LANs) e metropolitanas (MANs) em âmbito mundial. As próximas seções comentam os principais padrões para redes sem fio locais e metropolitanas que podem ser utilizados para a construção de redes mesh, salientando o seu uso para serviços que envolvem comunicação de voz e vídeo.

2.1. TECNOLOGIAS DE ACESSO AO MEIO

2.1.1. WiMAX

WiMAX (*Worldwide Interoperability for Microwave Access*) [WiMAX, 2006] [WiMAX Fórum, 2006] [IEEE b, 2006] é uma tecnologia que permite que dispositivos estabeleçam comunicação sem fio provendo conexões de banda larga com alta vazão sob distâncias em uma área metropolitana. É uma tecnologia padronizada pelo IEEE 802.16 e também é conhecida como *broadband wireless access* (BBWA).

A Figura 10 identifica o padrão IEEE 802.16 dentre os tipos de redes sem fio possíveis: PAN (*Personal Area Network*), LAN (*Local Area Network*), MAN (*Metropolitan Area Network*) e WAN (*Wide Area Network*).

Padrões para Redes sem Fio

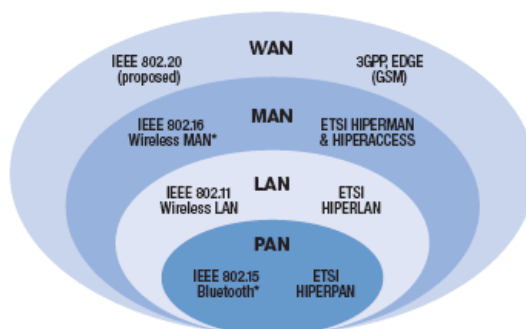


Figura 10: Padrões IEEE 802 para redes sem fio.

Fonte: Referência [IEEE b, 2006].

O padrão IEEE 802.16, como a maioria dos outros padrões, sofreu melhorias conforme sua evolução. Primeiramente, o padrão IEEE 802.16 foi estabelecido em dezembro de 2001 e situava as faixas de frequências entre 10 GHz e 66 GHz, com linha de visada. Já a versão posterior, IEEE 802.16a, concluída em janeiro de 2003, situava as faixas de frequências entre 2 GHz e 11 GHz, sem linha de visada e já considerando alguns aspectos de interoperabilidade. A Tabela 1 especifica alguns padrões do WiMAX com seus aspectos principais de acordo com a evolução ocorrida nestas especificações. Existe uma grande distinção feita em relação aos padrões: IEEE 802.16-2004 (também conhecido como revisão D ou 802.16d, inclui versões anteriores: 802.16-2001, 802.16c de 2002 e 802.16a de 2003) e IEEE 802.16e-2005, o primeiro é chamado de fixo e o segundo de móvel ou *nomadic* (nômade).

Tabela 1: Padrões 802.16 com suas características técnicas

Padrão	Data	Detalhes		
IEEE 802.16	Dezembro de 2001	10-66 GHz	Linha de visada	Até 34 Mbps (canalização de 28 MHz)
IEEE 802.16c	Dezembro de 2002	Interoperabilidade.		
IEEE 802.16a	Janeiro de 2003	2-11 GHz	Sem linha de visada	Até 75Mbps (canalização de 20 MHz)
IEEE 802.16d	1o Trimestre de 2004	Modificações no 802.16a e interoperabilidade.		
IEEE 802.16e	4o Trimestre de 2004	Mobilidade - nômades		

Com o objetivo de promover o uso do WiMAX e estabelecer as padronizações IEEE 802.16 para garantir a compatibilidade e interoperabilidade dos dispositivos que utilizam o WiMAX, foi criado o WiMAX fórum [WiMAX Fórum, 2006]. O WiMAX fórum é uma organização sem fins lucrativos formada por diversas empresas líderes de mercado, fabricantes de equipamentos e de componentes.

Um importante aspecto do padrão IEEE 802.16 é que este define uma camada MAC (*Media Access Control*) que suporta múltiplas especificações de camada física (PHY), permitindo adaptar vários tipos de exigências de usuários finais.

O WiMAX é baseado em OFDMA (*Orthogonal Frequency Division Multiple Access*) com três modos de operação de modulação: SOFDMA (*single carrier*), OFDM 256 (modo mais utilizado) ou OFDMA 2048.

O WiMAX permite elevadas taxas de vazão com longo alcance, além de ser tolerante às reflexões de sinais. Conforme [WiMAX Fórum, 2006], tanto o 802.16-2004 quanto o 802.16e apresentam desempenho similar. A vazão máxima por setor em ambas versões do WiMAX aproxima-se de 15Mbps por canal de 5MHz ou 35Mbps por canal de 10MHz, com alcance de poucos quilômetros (9Km), dependendo das condições de propagação. Este padrão habilita também uma modulação dinâmica adaptativa, na qual a estação base pode negociar a vazão conforme o alcance. Assim, se existe dificuldade em se estabelecer um enlace robusto entre a estação base e uma estação distante utilizando o esquema de modulação de maior ordem, como 64 QAM (*Quadrature Amplitude Modulation*), a modulação é reduzida para 16 QAM ou QPSK (*Quadrature Phase Shift Keying*), reduzindo a vazão, porém aumentando o alcance do sinal.

2.1.2. WI-FI

Uma *Wireless LAN* (WLAN) é uma rede local sem fio padronizada pelo IEEE 802.11. É conhecida também pelo nome de Wi-Fi [IEEE b, 2006], abreviatura de “*wireless fidelity*” (fidelidade sem fios) e marca registrada pertencente à *Wireless Ethernet Compatibility Alliance* (WECA).

O padrão inicial 802.11 de 1999 foi aperfeiçoado, sendo definidas algumas alternativas, listadas na Tabela 2 e na Tabela 3.

Tabela 2: Padrões 802.11 com suas características técnicas

Padrões	Freqüências	Técnica de Modulação	Taxa de Dados
802.11b	2400-2483,5 MHz	DSSS	até 11 Mbit/s
802.11g		DSSS, OFDM	até 54 Mbit/s
802.11a	5150-5350 MHz 5725-5850 MHz 5470-5725 MHz	OFDM	até 54 Mbit/s

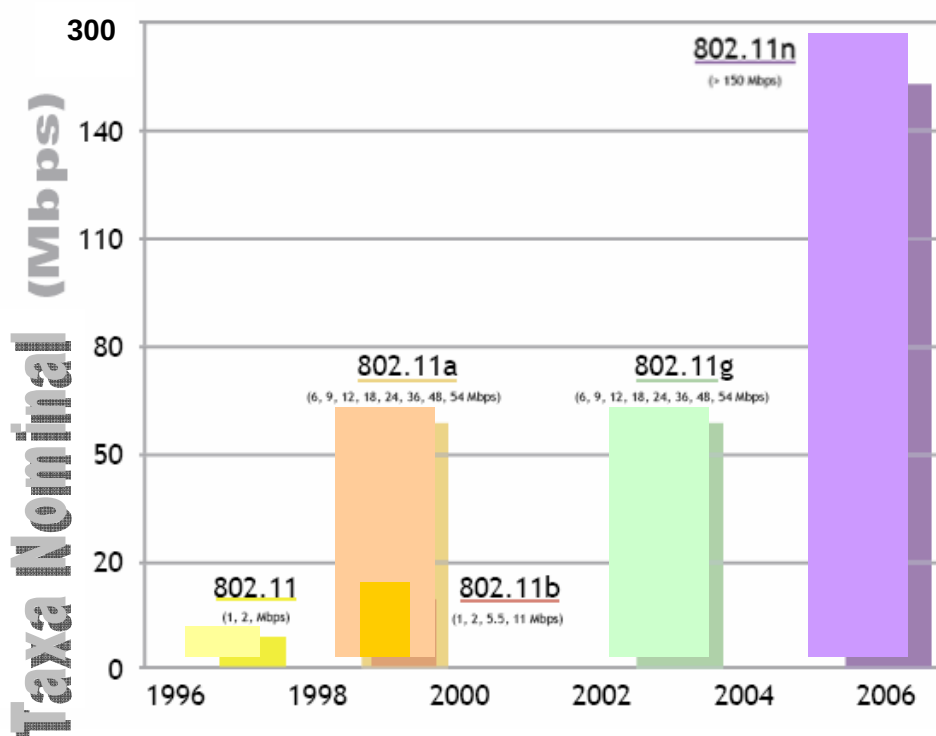
As técnicas de modulação mais comuns nas variantes do padrão 802.11 são:

- DSSS (*Direct Sequence Spread Spectrum*) é o espalhamento espectral por seqüência direta. Distribui o sinal baseado em uma gama extensiva da faixas de freqüência e reorganiza os pacotes no receptor.
- OFDM (*Orthogonal Frequency Division Multiplexing*) ou Multiplexação Ortogonal por Divisão de Freqüência é uma técnica de modulação mais eficiente que o DSSS.
- FHSS (*Frequency Hopping Spread Spectrum*) salta de canal para canal de acordo com uma seqüência de saltos pseudo-randômica que, uniformemente, distribui o sinal ao longo de toda a banda. Também é utilizada no padrão IEEE 802.15 – também conhecido como Bluetooth.

As redes Wi-Fi (802.11b/g) utilizam freqüências que não precisam de autorização para utilização. As condições de uso destas freqüências no Brasil estão estabelecidas pelo Regulamento sobre Equipamentos de Radiocomunicação de Radiação Restrita (seções IX e X), reeditado pela resolução 365 de 10/05/04 da ANATEL.

Tabela 3: Variedades do padrão 802.11 (Wi-Fi)

802.11	Padrão original WLAN. Suporta de 1 a 2Mbps.
802.11a	Padrão de alta velocidade WLAN para banda de 5GHz. Suporta 54Mbps.
802.11b	Padrão WLAN para banda de 2,4GHz. Suporta 11Mbps.
802.11c	Protocolo usado para bridges.
802.11d	Roaming International – automaticamente configura dispositivos para encontrar regulação local de RF.
802.11e	Endereça os requisitos de qualidade de serviço para todas as interfaces de rádio IEEE WLAN.
802.11f	Define o ponto de acesso de comunicação para facilitar a distribuição de múltiplos fornecedores de redes WLAN.
802.11g	Estabelece uma técnica adicional de modulação para banda de 2,4GHz. Suporta velocidade de até 54Mbps.
802.11h	Define o gerenciamento de espectro da banda de 5GHz. Seleção dinâmica de frequências.
802.11i	Provê maior segurança, através de autenticação e políticas de segurança. A criptografia é usada, substituindo-se o protocolo WEP (<i>Wired Equivalent Privacy</i>) pelos protocolos TKIP (<i>Temporal Key Integrity Protocol</i>) e AES (<i>Advanced Encryption Standard</i>).
802.11n	Provê melhor vazão com taxas de até 300Mbps.
802.11s	Especifica uma extensão do padrão IEEE 802.11 para solucionar problemas de interoperabilidade, segurança e outros relacionados a redes mesh

**Figura 11:** Taxa das variedades do padrão IEEE 802.11 .

Fonte: Fontes: Artigos conforme referência [Tropos, 2006] .

Extensões do padrão 802.11	
Extensões Mesh	802.11s
Extensões QoS	802.11e
Extensões de Segurança	802.11i
Rádio & Regulatório	802.11d, 802.11h
Altas taxas de dados	802.11b, 802.11a, 802.11g, 802.11n

Figura 12: Comparação entre as variedades do Padrão IEEE 802.11.

Fonte: Conforme referência [IEEE b, 2006].

Existe ainda um padrão em desenvolvimento que visa a construção de redes mesh, o IEEE 802.11s (*ESS Mesh Networking*) [IEEE, 2006], o qual especifica uma extensão do padrão IEEE 802.11 para solucionar problemas de interoperabilidade, segurança e outros relacionados a redes mesh.

Na Figura 11 são identificadas as taxas para as extensões do padrão IEEE 802.11 e na Figura 12, é explicitada, resumidamente, a função de cada padrão (em vermelho estão apresentadas as extensões ainda não aprovadas. Em resumo, os padrões 802.11n e 802.11s ainda aguardam aprovação).

2.2. COMUNICAÇÃO SEM FIO ATRAVÉS DE MÚLTIPLOS SALTOS

2.2.1. REDES AD-HOC

Também conhecidas como MANETs (*mobile ad-hoc networks*) [Macker e Corson, 1999], redes ad-hoc são redes sem fio, onde os dispositivos móveis são capazes de trocar informações entre si sem a necessidade de um ponto de acesso. Os dispositivos podem servir como roteadores sem fio, exercendo as duas funções ao mesmo tempo: terminal onde as aplicações rodam e roteador dos pacotes de rede. Desta forma, esses dispositivos móveis também podem ser chamados de nós de rede. Este tipo de rede é utilizado principalmente em situações em que não se justifica o custo da instalação de rede física ou em locais de difícil acesso, ou ainda em caso de desastres naturais (como terremotos, furacões, tsunamis entre outros) ou guerra.

Em uma rede ad-hoc, a comunicação entre dois dispositivos móveis pode ocorrer de forma direta, ou seja, quando um dispositivo está no raio de alcance do outro e vice-versa. Ou de forma indireta, na qual são necessários vários saltos (*hops*) para que ocorra troca de informações, e então os dispositivos funcionam exatamente como roteadores.

A Figura 13 identifica uma comunicação direta e uma indireta e seus vários saltos, também chamada de *multi-hop*.

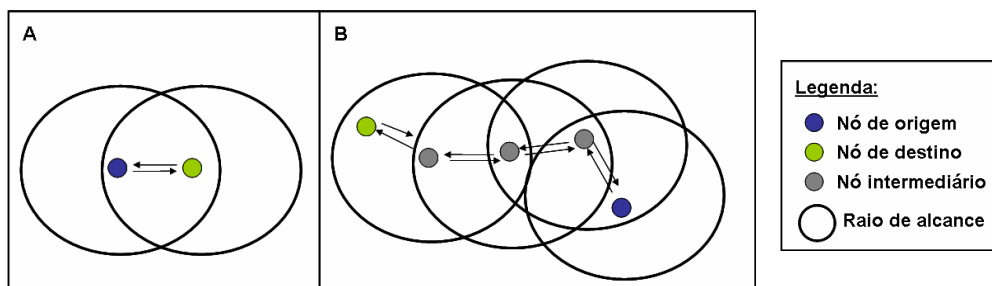


Figura 13: Redes ad-hoc. A) Comunicação em um salto. B) Comunicação em vários saltos.

Fonte: RFC conforme referência [Macker e Corson, 1999].

Quando a comunicação ocorre de forma indireta, faz-se necessário um protocolo de roteamento, da mesma maneira que acontece em uma rede cabeada.

Porém os protocolos de roteamento de uma rede ad-hoc devem ser preparados para alguns aspectos ausentes nas redes cabeadas, como principalmente a mudança de topologia da rede. Estes aspectos foram fundamentais, pois orientaram uma série de estudos para adaptação de alguns protocolos às características de cada rede. Assim, protocolos de roteamento de redes cabeadas serviram e ainda servem como base para os protocolos de redes ad-hoc.

Existem alguns fatores determinantes em redes ad-hoc, que são:

- Bateria: em geral, a bateria dos nós de uma rede ad-hoc tem tempo de autonomia limitada, desta forma, quanto mais troca de informações ocorre entre os nós, mais rápido acaba a bateria dos mesmos;
- Mobilidade: os nós podem se mover, alterando a topologia da rede, dependendo do tipo de rede, essa mobilidade pode ocorrer com uma velocidade alta, exigindo uma rápida adaptação do roteamento da rede;
- Banda limitada: é limitada de acordo com a tecnologia de acesso ao meio, desta forma, existe um compartilhamento da banda entre os nós existentes na rede;
- Conectividade (rede isolada): devido à mobilidade, pode ocorrer um isolamento de parte da rede, impedindo a comunicação entre parte dos nós.

Como vantagens de uma MANET, pode-se citar: a facilidade de instalação (sem necessidade de infra-estrutura previamente instalada); possibilidade de mobilidade; custo mais baixo que em redes infra-estruturadas (em uma grande parte dos cenários), entre outras. Como desvantagens, são identificadas: a banda passante limitada; roteamento mais complexo devido às constantes mudanças de topologia; taxa de erro alta no enlace (em geral constata-se 1 bit errado a cada 10^5 ou 10^6 bits trafegados, enquanto em uma fibra ótica, por exemplo, verifica-se uma taxa de um bit errado a cada 10^{12} a 10^{15} bits trafegados) e segurança física inexistente (tendo apenas a parte lógica – software – como responsável pela segurança das informações).

As redes ad-hoc começaram a ser estudadas há 30 anos atrás, aproximadamente, porém sempre com intuito de aplicá-las para fins militares ou em casos de catástrofes. Apenas recentemente, vislumbrou-se a possibilidade de

aplicação doméstica e/ou comercial. Nesta mesma tendência, houve abertura para o estudo de redes com conceitos que em parte baseavam-se nas redes ad-hoc, como por exemplo, as redes mesh, comentadas na próxima seção.

2.2.2. REDES MESH

As redes mesh são construídas combinando nós fixos e móveis interconectados via enlaces sem fio, formando uma rede ad-hoc de múltiplos saltos.

Diferente das redes ad-hoc, as redes mesh possuem uma hierarquia entre seus componentes formando sua arquitetura. A Figura 14 identifica a arquitetura de uma rede mesh com alguns tipos de componentes: usuários móveis, estando na camada mais baixa, em seguida são mostrados os roteadores sem fio e então os *gateways* que se conectam ao *backbone* da Internet através de rede cabeada.

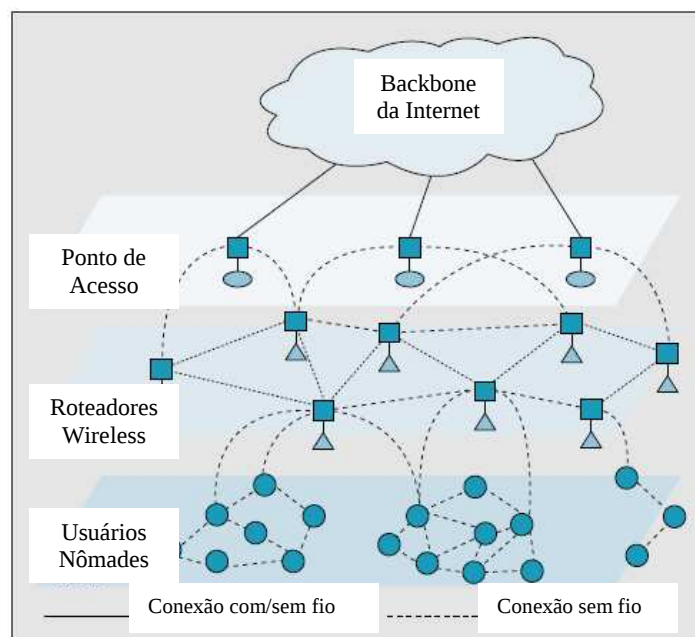


Figura 14: Redes mesh.

Fonte: Artigo conforme referência [Gregori et al, 2005].

Conforme [Gregori et al, 2005] podemos classificar as redes mesh em dois tipos: *off-the-shelf* e soluções proprietárias. O tipo *off-the-shelf* são redes comunitárias utilizando principalmente o padrão IEEE 802.11 provendo acesso a um grupo de usuários, os quais compartilham a mesma conexão à Internet. As redes mesh tornaram-se também uma possibilidade comercial, assim algumas empresas

desenvolveram soluções proprietárias para aproveitar a oportunidade para disponibilizar produtos no mercado, com aplicação *indoor* e *outdoor*.

As redes mesh possuem algumas vantagens, dentre as quais pode-se citar:

- Redução do custo de instalação: devido à infra-estrutura ser necessária somente em poucos pontos de conexão para o *backbone* cabeado;
- Confiabilidade: à medida que o *backbone* sem fio permite inúmeras conexões entre os nós, desde que os mesmos estejam dentro do raio de alcance, aumenta a redundância de enlaces, ocorrendo menos probabilidade de indisponibilidade do serviço;
- Auto-configuração: não é necessária nenhuma configuração prévia dos enlaces quando um novo nó é adicionado à rede. Automaticamente, o nó detecta seus nós vizinhos e através dos protocolos de roteamento encontra as rotas desejadas.

Uma possibilidade para compor uma rede mesh é utilizar mais de um padrão de acesso ao meio, como na Figura 15, que mostra uma rede composta por Wi-Fi (IEEE 802.11) e WiMAX (IEEE 802.16) integrando a mesma rede mesh. Desta forma, pode-se aproveitar as vantagens de cada padrão; as grandes distâncias disponibilizadas pelo WiMAX com o uso popularizado do padrão Wi-Fi.

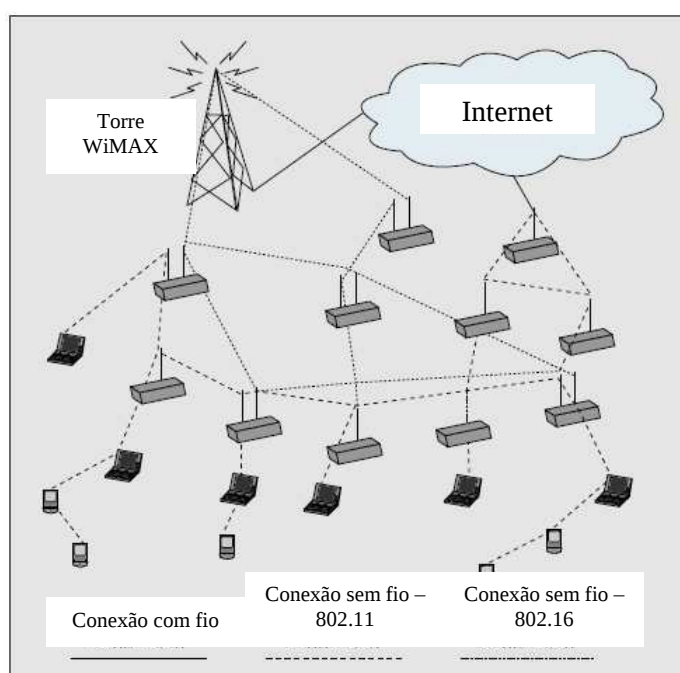


Figura 15: Redes mesh – WiMAX e Wi-Fi.

Fonte: Artigo conforme referência [Gregori et al, 2005].

2.3. APLICABILIDADE – REDES CONVERGENTES

2.3.1. VoIP

VoIP (*Voice over IP* – Voz sobre IP) [Hersent et al, 2002] é a denominação dada a um serviço que permite o tráfego de voz sobre uma rede IP, com soluções que permitem a qualidade do serviço e a interligação do mundo IP com a PSTN (*Public Switched Telephone Network*).

A Figura 16 identifica, resumidamente, alguns padrões possíveis para se prover o serviço VoIP. Cada padrão utiliza uma arquitetura diferente, com elementos que possuem as funções de: troca de sinalização com a rede PSTN, autenticar os usuários, registrar as chamadas, encapsular e desencapsular os sinais de voz em IP. Para todas estas funções são definidos alguns protocolos, os quais também variam de acordo com o padrão utilizado. Maiores informações sobre os padrões para serviços VoIP podem ser encontrados em [Hersent et al, 2002].

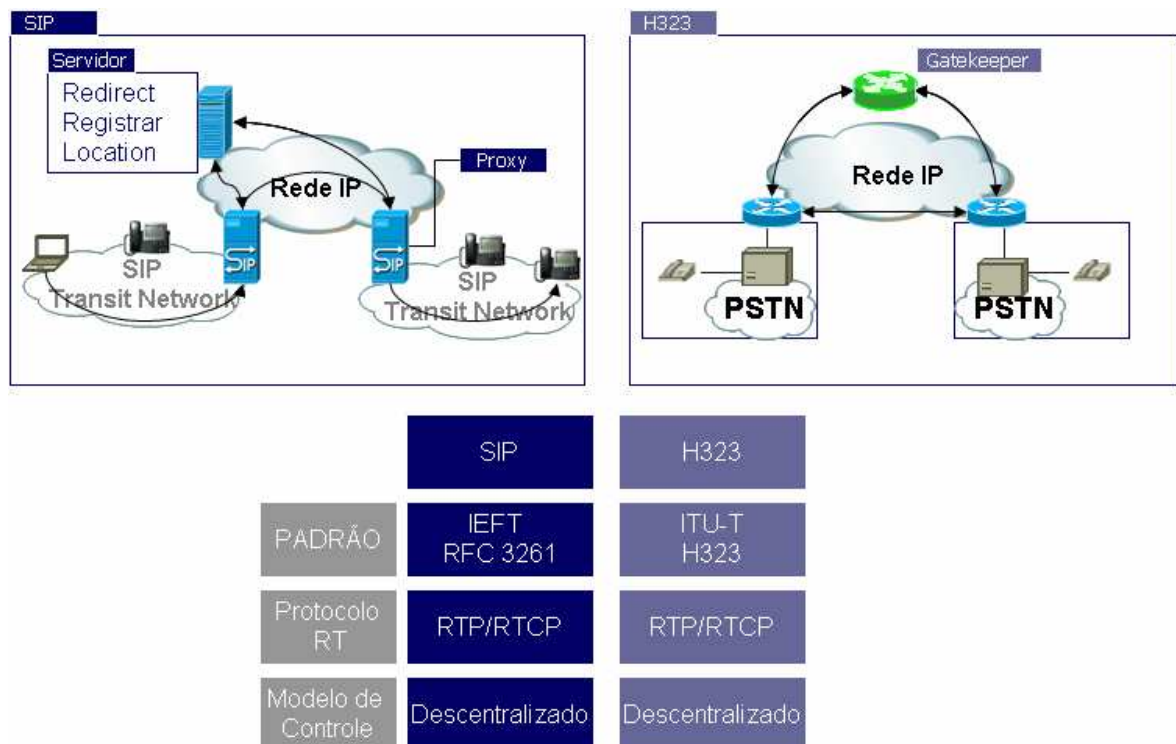


Figura 16: Padrões de uma rede VoIP.

Fonte: Livro conforme referência [Hersent et al, 2002].

2.3.2. IPTV

IPTV (TV sobre rede IP) [IPTV, 2006] [IPTV b, 2006] é a denominação dada a um serviço que permite que o tráfego de televisão digital (transmissão em tempo real de vídeo entre outras possibilidades) sobre uma rede IP.

Alguns fatores são responsáveis pela viabilização do tráfego dos sinais da televisão digital por uma rede IP: a evolução das plataformas que permitem a oferta de serviços de transmissão de conteúdo em vídeo sob demanda (*streaming on demand*), utilizando uma infra-estrutura IP convergente, o aumento de banda oferecido pelo acesso banda larga, o desenvolvimento de algoritmos de compressão mais eficientes e de esquemas de proteção de conteúdo, também conhecidos por DRM (*Digital Rights Management*).

Um sistema IPTV é composto de quatro elementos, conforme ilustrado na Figura 17. Uma importante vantagem do IPTV sobre os tradicionais sistemas de televisão é a possibilidade da comunicação bidirecional. Esses elementos combinados formam a arquitetura conhecida como SDV (*switched digital video*). SDV refere-se a uma arquitetura de rede de sistema de distribuição de televisão na qual apenas os canais selecionados são distribuídos individualmente para os assinantes.

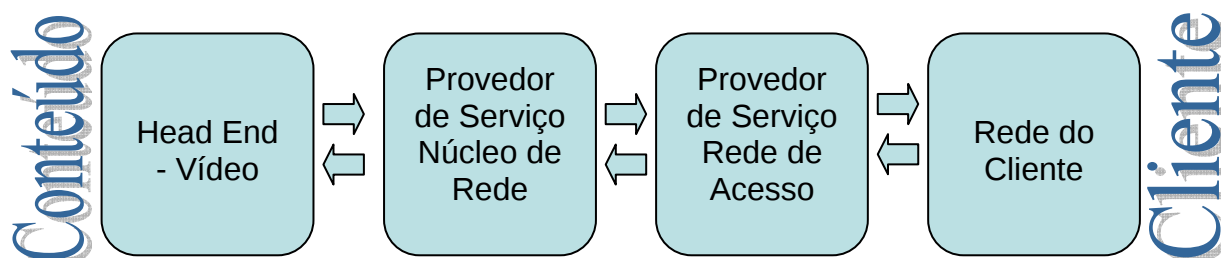


Figura 17: Elementos de uma rede IPTV.

Fonte: Artigo conforme referência [IPTV b, 2006].

Como nos sistemas de televisão a cabo ou satélite, em uma rede IPTV também é necessário um *head-end*, no qual o conteúdo é capturado e formatado para distribuição, no caso, sobre uma rede IP. Um *head-end* trata cada canal individualmente, codificando-os em um formato digital de vídeo, como o MPEG-2. Os provedores de serviço estão começando a utilizar o padrão MPEG-4, que possui algumas vantagens como necessitar menor taxa para codificar os sinais de televisão.

Após a codificação, cada canal é encapsulado em IP e enviado através da rede. Estes canais são tipicamente fluxos IP *multicast*, entretanto, alguns fornecedores desta tecnologia também utilizam fluxos IP *unicast*. Transmissão em *multicast* IP possui muitas vantagens, pois permite que os provedores de serviços propaguem um fluxo IP para diversos assinantes, no caso de múltiplos usuários desejarem assistir ao mesmo canal, ao mesmo tempo.

Quem é o responsável pelo transporte dos fluxos de vídeo para os assinantes são os provedores de serviço, os quais possuem uma rede IP. Esta rede IP é composta de um *backbone* (núcleo de rede) e de equipamentos de borda de rede, os quais se conectam a rede de acesso aos assinantes.

A rede de acesso, também chamada de última milha (*last mile*), é a rede responsável por conectar os assinantes ao núcleo da rede IP e, por conseguinte ao *head-end*. Existem algumas tecnologias disponíveis para habilitar esta rede a prover este acesso banda larga, como: tecnologias sobre fibra óptica como PON (*passive optical networking*), tecnologias DSL (assimétrica: ADSL, ou de alta velocidade: VDSL).

O quarto elemento é o *home network*, o qual distribui o serviço IPTV na casa do assinante, e tem como principal componente o *set-top box* (STB). O STB permite decodificação dos sinais de vídeo. A Figura 18 mostra alguns modelos de STB disponíveis no mercado.



Figura 18: Modelos de set-top box (STB).

Fonte: Artigo conforme referência [IPTV b, 2006].

Diversas operadoras no mundo, sobretudo na Europa e na Ásia, já oferecem comercialmente serviços de IPTV como, por exemplo, a France Telecom (França), Free (França), Fastweb (Itália), Telefônica (Espanha), Chunghwa Telecom (Taiwan) e PCCW (Hong Kong). Nos Estados Unidos, as operadoras AT&T (fusão da SBC com AT&T) e BellSouth (em processo de aquisição pela AT&T) já possuem produtos customizados e estão em fase de implementação do serviço. No Brasil, a Telemar está em fase de teste de algumas soluções de fornecedores para determinar a

melhor tecnicamente, formulação dos produtos que serão ofertados e definição dos melhores processos de instalação e reparo. As empresas Telefônica e Brasil Telecom também começaram a estudar o conceito e a realizar testes.

A possibilidade de uso do canal de retorno da TV digital interativa por aplicações multimídia como VoIP e IPTV precisa ser considerada na escolha da tecnologia a ser utilizada na implementação do canal de retorno. Essas aplicações estão cada vez mais populares entre os usuários da Internet e seu uso é fundamental para permitir um nível de interatividade mais atrativo aos futuros usuários da TV digital brasileira.

Este trabalho propõe o uso de redes mesh sem fio como tecnologia de acesso para inclusão digital, considerando a convivência de aplicações tradicionais, como a *web* e aplicações multimídia, como VoIP e IPTV. São avaliados desempenhos de diferentes protocolos de roteamento ad-hoc com uso de modelos de geração de tráfego que consideram aplicações que enviam dados, voz e vídeo, simulando um determinado nível de interatividade para o usuário da rede sem fio, como será visto no Capítulo 5.

3. PROJETOS RELACIONADOS A REDES MESH

Neste capítulo serão abordados diversos trabalhos relacionados, que consideram o uso de redes mesh sem fio para possibilitar inclusão digital à população de baixa renda e para prover acesso à Internet a custo baixo.

3.1. CIDADES DIGITAIS

Também conhecidas como *city cloud*, *digital city* ou *wireless city*, as cidades digitais são cidades ou municípios onde são desenvolvidos projetos para prover acesso sem fio à Internet para toda a comunidade, sem depender de serviços oferecidos por operadoras de telecomunicações. Cidades digitais estão se tornando, cada vez mais, uma realidade em todo o mundo. Apenas nos EUA são mais de 100 cidades desenvolvendo projetos de cidade digital.

A tecnologia mais utilizada na construção de cidades digitais é a de redes mesh usando enlaces IEEE 802.11 para redes locais sem fio (Wi-Fi), ou mesmo IEEE 802.16 (WiMAX). Algumas destas iniciativas são explicitadas a seguir.

3.1.1. TIRADENTES DIGITAL (MG)

O Projeto Tiradentes Digital [Tiradentes Digital, 2006] foi colocado em prática na cidade de Tiradentes em Minas Gerais, distante 210 quilômetros da capital Belo Horizonte, em 24 de março de 2006. Este projeto consiste em disponibilizar acessos à Internet em banda larga gratuitamente a escolas, postos de saúde, centros de turismo e órgãos públicos, com o objetivo de



promover a inclusão social. A parceria entre governo e empresas privadas permitiu o desenvolvimento deste projeto com a compra de computadores e investimento em capacitação em informática para a população. Este acesso é viabilizado através de uma rede mesh sem fio usando o padrão IEEE 802.11.

A Cisco Networks (empresa privada muito conhecida por suas soluções para redes IP) participa da iniciativa de inclusão digital tendo como grande parceira a Telemar, operadora de telecomunicações que disponibilizou gratuitamente um enlace dedicado de 2 Mbps para acesso à Internet.

Tiradentes é uma cidade serrana, tombada pelo Patrimônio Histórico Nacional com terreno ondulado, no qual estão instalados chafarizes, casarões, sobrados, museus e outros tesouros históricos, constituindo uma combinação que representava um grande desafio para implementação de uma rede mesh.

Em uma avaliação mais apurada, detectou-se que a implementação da tecnologia seria melhor em locais altos, resultando em uma rede capaz de cobrir grandes distâncias e oferecer acesso de qualidade nos terrenos acidentados. Assim, foram instalados rádios da série Aironet 1500 Lightweight Mesh AP (equipamento CISCO) nos seguintes pontos: igreja São Francisco/Rodoviária (ponto de acesso), igreja Matriz (ponto de acesso), escola Basílio da Gama (ponto de acesso) e o ponto central foi localizado na Prefeitura Municipal (roteador e gerência).

Os equipamentos utilizados no teste foram:

- (4) Rádios Aironet 1510 Series Mesh Access Point;
- (2) Rádios Aironet 1131;
- (1) Router 2801 – CCME (Router de conexão a Internet, gateway de conexão a rede de telefonia analógica da prefeitura e Call Controller da Rede de telefonia IP);
- (1) Software de gerência da Rede Mesh CISCO WCS;
- (1) Controller da Rede Wireless CISCO 2006;
- (2) Telefones IP modelo 7940G;
- (5) Telefones IP wireless modelo 7920;
- (1) Switch modelo 2912;
- (2) Switch modelo CE500;
- (30) Placas Wireless USB da Linksys – para as estações de trabalho;
- (5) Câmeras Wireless da Linksys.

A solução CISCO de redes mesh sem fio é parte da arquitetura CISCO de redes *wireless* unificadas. A solução é baseada na série CISCO Aironet 1500, tendo

os pontos de acesso mesh externos (802.11a/b/g – modelo 1510 – e 802.11b/g – modelo 1505), e usa o protocolo CISCO *Adaptive Wireless Path Protocol* (AWPP), com patente em processo de registro, para comunicação entre os roteadores.

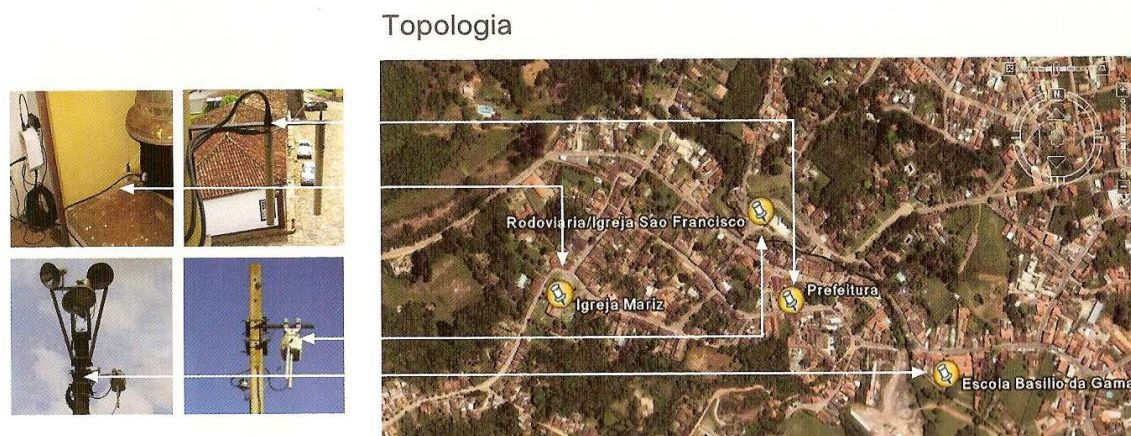


Figura 19: Rede mesh na cidade de Tiradentes, MG.

Fonte: Folheto explicativo da CISCO sobre o projeto.

A Figura 19 identifica a topologia com a solução CISCO de rede mesh implantada na cidade de Tiradentes - MG.

3.1.2. PIRAÍ DIGITAL (RJ)

Outro projeto também em desenvolvimento é o Pirai Digital [Pirai Digital, 2006] [Pirai Digital b, 2006] na cidade de Pirai no estado Rio de Janeiro, distante 80 quilômetros da capital deste estado, com 23.600 habitantes. Este projeto se dispõe a prover acesso à Internet em banda larga através de uma rede sem fio, optando por soluções de software livre. O Pirai Digital recebeu, em 13 de junho de 2006, em Nova York o prêmio *Top Seven Intelligent Communities*, ficando entre as sete cidades mais inteligentes do mundo no ano de 2005. É um projeto em parceria de organizações privadas e públicas. A topologia da rede foi elaborada para garantir uma cobertura de 95% do território urbano de Pirai.

A rede é chamada de SHSW (sistema híbrido com suporte *wireless*) e através desta rede sem fio é provida uma rede pública para comunicação de dados e transmissão de voz. A Figura 20 identifica a topologia de rede utilizada.

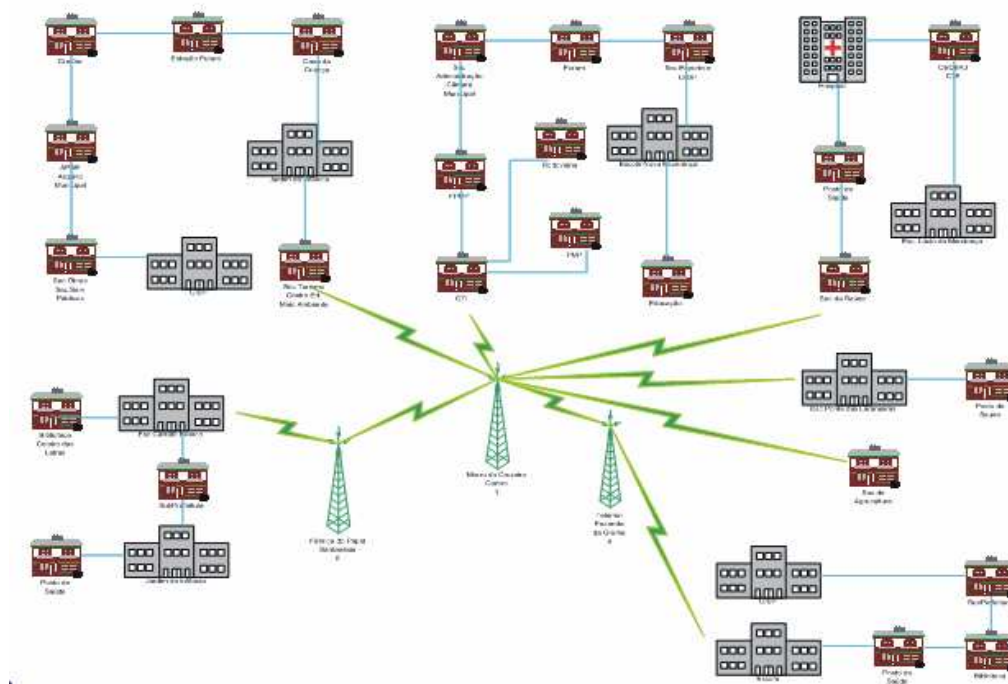


Figura 20: Topologia do Projeto Pirai Digital no Rio de Janeiro.

Fonte: Site Oficial do Projeto Pirai Digital.

3.1.3. SUD MENUCCI DIGITAL (SP)

O projeto Sud Menucci Digital [Sud Mennucci Digital, 2006] está sendo desenvolvido na cidade de Sud Menucci no estado de São Paulo, com 7.500 habitantes e duas mil moradias, das quais mais de 180 estão conectadas à Internet gratuitamente. Este projeto se dispõe a prover acesso à Internet em banda larga através de uma rede sem fio, com pontos de acesso distribuídos pela cidade. O próximo passo é prover a comunicação através da tecnologia de voz sobre IP (VoIP). Nesta cidade, em 2002, quando se deu o início do projeto, existiam apenas 20 computadores conectados à Internet via acesso discado. Esta foi uma das cidades pioneiras no Brasil em inclusão digital através de rede sem fio.

A rede consiste da tecnologia Wi-Fi, com dois transmissores centrais operando na faixa de 2,4GHz (IEEE 802.11b/g), com alcance de 15 Km, habilitando acesso em qualquer lugar da cidade.



Figura 21: Topologia do Projeto Sud Menucci Digital no estado de São Paulo.

Fonte: Site Oficial do Projeto Sud Menucci Digital.

3.1.4. TAIPEI (Taiwan)

A cidade de Taipei, capital da ilha de Taiwan, está desenvolvendo um projeto de uma rede mesh, a qual provê acesso sem fio para uma grande parte da população através da tecnologia Wi-Fi (IEEE 802.11b). Quando completo, é esperado que possua 10.000 pontos de acesso instalados cobrindo 90% dos 272 Km² com uma população de 2,65 milhões de habitantes.

A solução da rede mesh é da empresa canadense Nortel Networks, a arquitetura da rede é mostrada na Figura 22.

Existem duas empresas que comercializam tal rede *wireless* para a população: a Q-ware Systems (<http://www.wifly.com.tw/wifly3/en/>) e Chunghwa Telecom Co (<http://www.cht.com.tw/CHTFinale/Web/>), os valores da assinatura da rede são próximos a 12 dólares mensais.

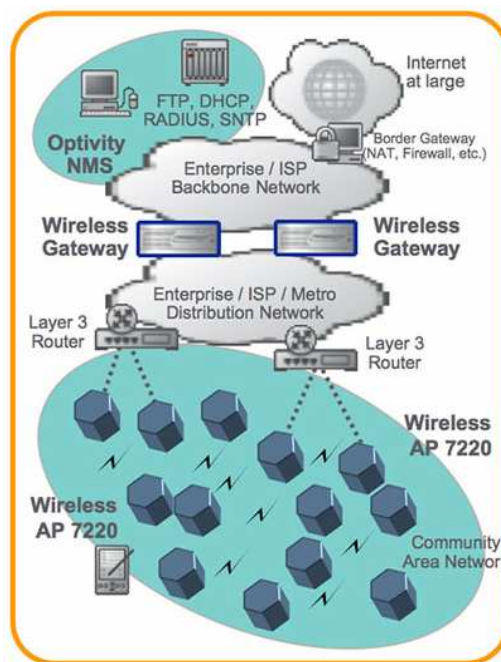


Figura 22: Arquitetura da rede mesh da Nortel Networks implantada em Taipei.

Fonte: Site conforme referência [Taipei Digital, 2006].

3.1.5. FILADÉLFIA (EUA)

A prefeitura da cidade da Filadélfia (EUA) investiu no desenvolvimento de um projeto, *Wireless Filadélfia – cidade digital* [Filadélfia Digital, 2006] [Filadélfia Digital b, 2006], para prover acesso à Internet através de uma rede mesh de baixo custo. É uma iniciativa sem fins lucrativos, que almeja viabilizar o uso do acesso banda larga para a população de mais baixa renda. A rede é baseada no padrão IEEE 802.11b/g e é composta de roteadores sem fio espalhados pela cidade. A Figura 23 mostra a área coberta pelos roteadores. A solução da rede foi idealizada pela empresa Tropos Networks. A Figura 24 identifica a arquitetura de uma rede da Tropos, incluindo os dispositivos para gerência da mesma.

Esta cidade digital ficou famosa pela disputa com uma das maiores operadoras de telecomunicações dos EUA, a Verizon, a qual tenta juridicamente bloquear o projeto, pois identificou uma grande possibilidade de perda de receita. A maior argumentação da empresa é que não se trata de uma competição justa, à medida que os municípios são isentos de impostos e podem utilizar recursos públicos para financiar os projetos.

Esta cidade digital disponibilizará acesso sem custo em alguns lugares públicos como: Love Park, the Historic Square Mile, Penn's Landing, Cobbs Creek Environmental Center, Hunting Park, Wissahickon Environmental Center, Pennypack Environmental Center, FDR Park e Penn Treaty Park. Para ter acesso em casa, o assinante pagará entre 9 dólares e 22 dólares, valores mais baixos do que os praticados no local por operadoras de telecomunicações.

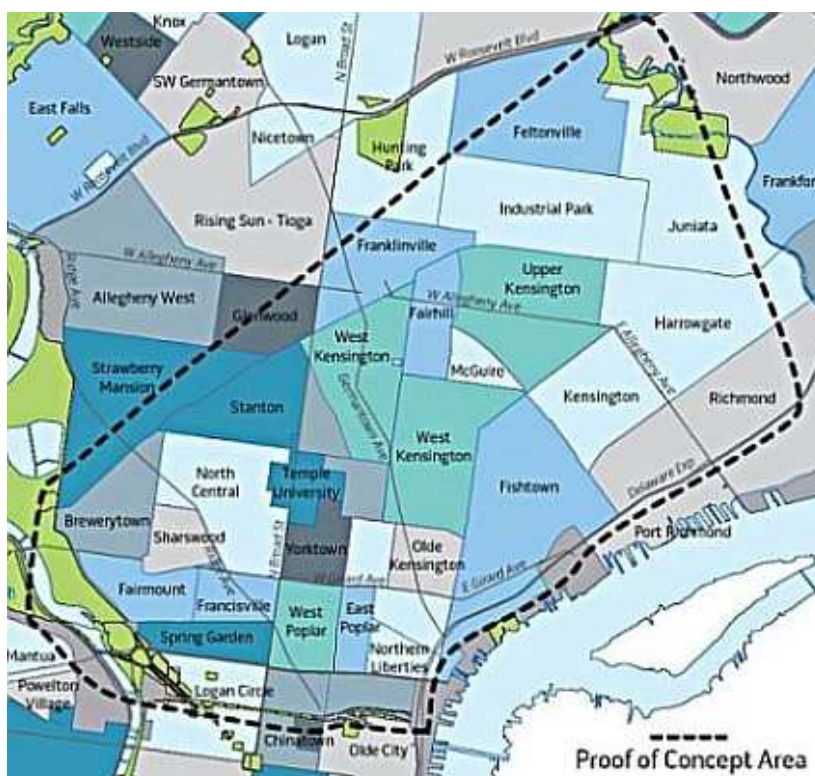


Figura 23: Área abrangida pelo Projeto cidade digital da Filadélfia.

Fonte: Site conforme referências [Filadélfia Digital, 2006] [Filadélfia Digital b, 2006].

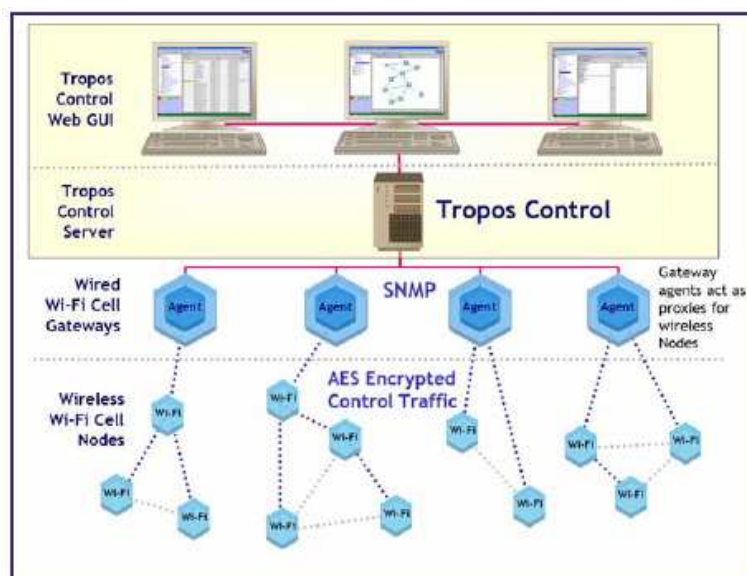


Figura 24: Arquitetura da solução da empresa Tropos Networks, usada na Filadélfia.

Fonte: Site conforme referência [Tropos, 2006].

3.2. PROJETOS DE PESQUISA SOBRE REDES MESH

3.2.1. REMESH

O projeto ReMesh [Remesh, 2006] está sendo desenvolvido por uma equipe de pesquisadores da Universidade Federal Fluminense (UFF) e apoiado pelo GT Rede Mesh da RNP (Rede Nacional de Ensino e Pesquisa) e destina-se a realizar um teste piloto de uma rede mesh para permitir o acesso banda larga para universitários da UFF que residam próximo ao campus. Para isso, foram implementados protótipos de roteadores sem fio, mecanismos de autenticação de usuários, endereçamento estático e dinâmico, dentre outras necessidades, para efetivar o experimento.

Como um dos objetivos do projeto, almeja-se otimizar o desempenho da rede e encontrar soluções para obter garantia da qualidade do serviço nas comunicações através de múltiplos saltos. Além do aspecto tecnológico e científico, este também é um projeto que visa à inclusão digital através de redes mesh.

Nos testes elaborados dentro do escopo do projeto ReMesh são utilizados roteadores wireless da Linksys – WRT54G e WRT54GS, com o sistema operacional OpenWRT [OpenWRT, 2005] e ainda o software de simulação NS-2 [NS2, 2005]. Os testes realizados basearam-se em protocolos que garantem QoS, como INSIGNIA [Lee et al, 2000] e ASAP[Xue et al, 2003].

3.2.2. ROOFNET

O Projeto Roofnet [Bicket et al, 2004] foi elaborado por uma equipe de pesquisadores do Instituto de Tecnologia de Massachusetts (MIT - *Massachusetts Institute of Technology*) com o objetivo de estudar o comportamento de redes sem fio de grande escala. Para isso, foi montada uma rede *wireless* com 50 nós (próximos à universidade em questão). O acesso é realizado por um hardware específico fornecido pelos pesquisadores, incluindo PC com sistema operacional Linux e placa de rede sem fio padrão 802.11b. O protocolo de roteamento utilizado é o SRCR [Aguayo et al, 2004], que é baseado no protocolo DSR, que será explorado no próximo capítulo.

3.2.3. VMESH

O projeto VMesh [Tsarmpopoulos et al, 2005] foi elaborado por uma equipe de pesquisadores da Universidade de Thessaly, Grécia, com o objetivo de implantar uma rede mesh de baixo custo na cidade de Volos (Grécia) para prover acesso à Internet aos estudantes da universidade, funcionários e professores, a partir de suas residências. A rede é composta por 9 roteadores wireless, conforme topologia simplificada mostrada na Figura 25, instalados no topo de prédios para permitir melhor conectividade. O protocolo de roteamento escolhido foi o OLSR, implementado nos roteadores wireless através de uma modificação no sistema OpenWRT [OpenWRT, 2005]. O modelo dos roteadores é o Linksys WRT54G e WRT54GS.

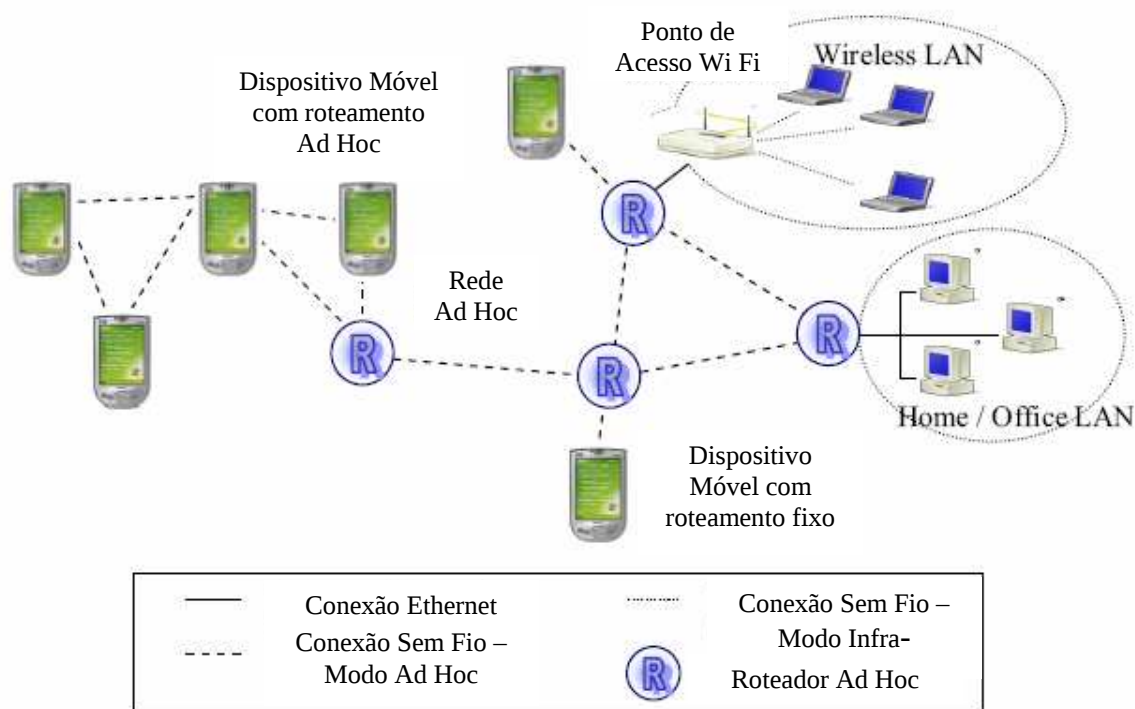


Figura 25: Topologia simplificada do Projeto VMesh.

Fonte: Artigo conforme referência [Tsarmpopoulos et al, 2005].

3.2.4. PROJETO LAPTOP A U\$100,00 (OLPC)

O projeto OLPC (*One Laptop per Child*) [OLPC, 2006] foi proposto por Nicholas Negroponte, responsável pelo Media Lab do Instituto de Tecnologia de Massachusetts (MIT - *Massachusetts Institute of Technology*) e está sendo desenvolvido de acordo com algumas parceiras, incluindo o Brasil, o qual participa do projeto através da ajuda de profissionais do LSI (Laboratório de Sistemas Integráveis) da Escola Politécnica da Universidade de São Paulo (USP); e do Centro de Pesquisas Renato Archer (CenPRA), de Campinas.

Este projeto propõe o fornecimento de um laptop por criança, a um custo de US\$ 100,00 cada, incentivando a inclusão digital em países em desenvolvimento. A máquina proposta e em desenvolvimento utiliza-se de software livre e não possui disco rígido, inclui processador de 500MHz, memória de 128MB, quatro portas USB e memória flash de 512MB. A proposta para a viabilização do acesso à Internet é ligar esses laptops em uma rede mesh, onde cada uma das máquinas possa atuar em modo ad-hoc.

Uma equipe de pesquisadores de várias universidades brasileiras, coordenados pela Universidade Federal Fluminense, foi contratada para testar a solução de rede mesh do projeto OLPC, ou ainda UCA (sigla em português: Um Computador por Aluno).

O Brasil tem atuado em três vertentes do projeto: sistema operacional, display do aparelho - que é um dos itens que mais encarecem a produção, e na cadeia de fornecimento, o que inclui planejamento de recursos que podem ser produzidos internamente e o que terá que ser importado. Para aderir ao programa, o país interessado deve adquirir no mínimo 1 milhão de máquinas, o que representaria um investimento mínimo de 100 milhões de dólares.

Além dos institutos e universidades brasileiros, existem outras parcerias para ajudar no desenvolvimento deste projeto, como: Programa de Desenvolvimento das Nações Unidas (UNDP), RedHat (empresa fabricante de algumas das distribuições disponíveis para o sistema operacional Linux), Advanced Micro Devices (AMD – empresa fabricante de processadores), Brightstar, Google, News Corp. e Nortel Networks entre outras empresas e institutos.

Uma ilustração do modelo a ser distribuído é mostrada na Figura 26. O término deste projeto está previsto para final de 2007, conforme informação do site oficial [OLPC, 2006].



Figura 26: Laptop de U\$100,00, modelo 2B1, desenvolvido para propiciar a inclusão digital.

Fonte: Site conforme referência [OLPC, 2006].

A adesão dos países ao Projeto OLPC é mostrada Figura 27. Os países em verde já estão inseridos no projeto inicial; os países em laranja já expressaram interesse em participar através do Ministério da Educação ou de algum outro órgão competente; os países em amarelo estão iniciando a prestar suporte a este projeto. Os países integrantes do projeto desde seu início são Brasil, Argentina, China, Índia, Egito, Nigéria e Tailândia.

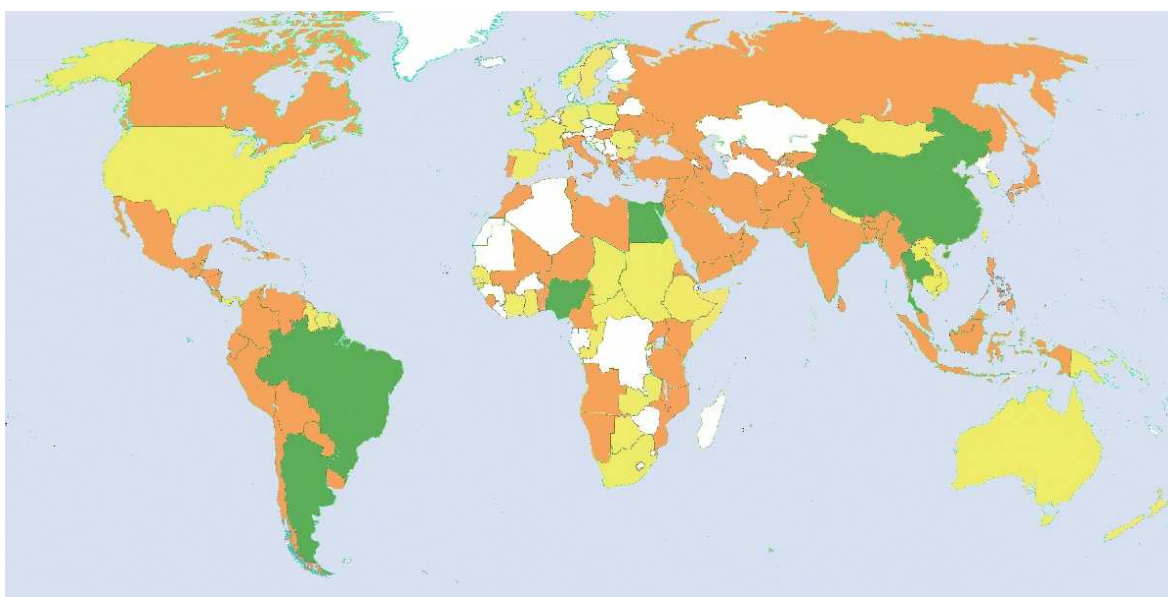


Figura 27: Adesão mundial ao projeto OLPC.

Fonte: Site conforme referência [OLPC, 2006].

4. PROTOCOLOS DE ROTEAMENTO AD-HOC

Para se implementar uma rede mesh com múltiplos saltos, é necessário escolher um protocolo de roteamento sem fio e os protocolos de roteamento ad-hoc já existentes podem ser utilizados para prover tal funcionalidade. O protocolo de roteamento estabelece a rota pela qual os pacotes, originados em um determinado nó, trafegarão pela rede até que cheguem ao nó destino, inclusive podendo passar por nós intermediários.

Existem vários protocolos de roteamento para redes ad-hoc propostos na literatura, os quais podem ser classificados de acordo com algumas características principais. Uma das classificações mais utilizadas [Manoj e Murthy, 2004] [Cordeiro e Agrawal, 2002] é em reativo (*on-demand*); pró-ativo (*table driven*) e híbrido. Esta classificação se dá pelas características dos protocolos em relação ao descobrimento e armazenamento das rotas. Desta forma, os protocolos do tipo pró-ativo mantêm uma tabela atualizada em todos os nós para todas as rotas possíveis; em contrapartida, os protocolos do tipo reativo apenas descobrirão a rota, para um determinado destino, quando houver a necessidade e por fim, os protocolos do tipo híbrido agregam características do tipo reativo e do tipo pró-ativo, geralmente definindo áreas onde se usa um tipo e outras áreas onde se usa o outro tipo.

Como exemplo de protocolos do tipo pró-ativo, pode-se citar os protocolos: DSDV (*Destination-Sequenced Distance Vector*) [Perkins e Bhagwat, 1994], WRP (*Wireless Routing Protocol*) [Murthy e Garcia, 1996], OLSR (*Optimized Link State Routing*) [Clausen e Jacquet, 2003], FSR (*Fisheye State Routing*) [Iwata et al, 1999] [Gerla et al, 2001], CGSR (*Cluster Gateway Switch Routing*) [Manoj e Murthy, 2004]. Já do tipo reativo encontramos os seguintes protocolos disponíveis: DSR (*Dynamic*

Source Routing) [Johnson e Maltz, 1996] [Johnson et al, 2002], AODV (*Ad Hoc On-Demand Distance Vector*) [Perkins e Royer, 1999] [Perkins e Royer, 2003] , TORA (*Temporally Ordered Routing Algorithm*) [Corson e Park, 2001], ABR (*Associativity Based Routing*) [Toh, 2002] , SSA (*Signal Stability-Based Adaptive Routing Protocol*) [Dube, 1997] . Do tipo híbrido, pode-se citar ZRP (*Zone Routing Protocol*) [Haas, 2001] [Haas et al, 2001 b] [Haas et al, 2001], entre outros. A Figura 28 reúne alguns dos protocolos de roteamento mais conhecidos na literatura, sendo detalhados em seguida. Alguns dos protocolos citados são padronizados [IETF, 2005] e já são utilizados amplamente no mercado.

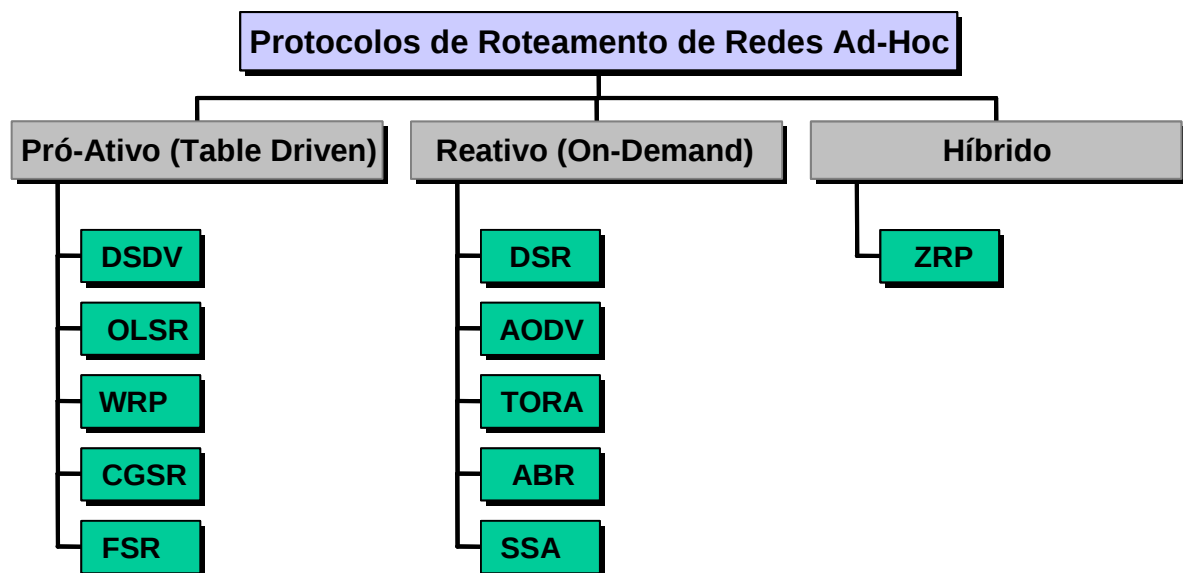


Figura 28: Principal classificação dos protocolos de roteamento ad-hoc.

Fonte: Livro conforme referência 0.

4.1. PROTOCOLOS PRÓ-ATIVOS

Os protocolos pró-ativos mantêm as tabelas atualizadas em todos os nós contendo todas as rotas existentes. Por isso, o tempo de descoberta de rota no momento da demanda de comunicação entre os nós tende a zero, isto devido ao fato das rotas já serem conhecidas, assim o tempo curto para a descoberta de rota é uma das vantagens dos protocolos do tipo pró-ativo. Em contrapartida, esta mesma característica possui suas inconveniências, como alto consumo de energia e alta utilização da banda com pacotes de controle se comparado a protocolos reativos.

4.1.1. DSDV (*Destination-Sequenced Distance Vector*)

O DSDV [Perkins e Bhagwat, 1994] é um protocolo pró-ativo baseado na técnica de vetor de distância (*distance vector*), que utiliza número de saltos para calcular as melhores rotas. Cada entrada na tabela de rotas possui um número de seqüência, para identificação da rota mais atual, ou seja, a rota com número de seqüência mais recente será considerada a atual. Quando existem duas rotas para o mesmo destino com o mesmo número de seqüência, é escolhida a de menor distância até o destino, ou seja, com o menor número de saltos.

Além do número de seqüência, são armazenadas as seguintes informações na tabela: endereço de destino e número de saltos necessários para se alcançar o nó destino.

Estas tabelas são atualizadas periodicamente por toda a rede para manter as rotas válidas. A cada mudança ocorrida na rede, pacotes são enviados com o intuito de manter os nós sempre atualizados sobre as mudanças topológicas da rede.

Existem dois tipos de pacotes para esta atualização:

- *Full dump*: Onde são trafegados várias NPDUs (*network protocol data unit*).
- *Small increment*: Apenas uma NPDU trafega na rede. São atualizadas apenas as mudanças desde o último *full dump*.

4.1.2. OLSR (*Optimized Link State Routing*)

O OLSR [Clausen e Jacquet, 2003] [Jacquet et al, 2005] é baseado na técnica de estado de enlace (*link state*) [Kurose e Ross, 2004], porém realiza algumas otimizações para diminuir a quantidade de pacotes de controle que trafegam na rede. O OLSR tem todos os seus pacotes de controle enviados sobre UDP (*User Datagram Protocol*), utilizando a porta de número 698.

Neste protocolo são definidos *multipoint relays* (MPRs), que são nós selecionados que possuem funções de roteamento mais completas na rede. Os

MPRs são os únicos nós a solicitarem o início do broadcast na rede e também são os únicos a retransmitirem pacotes broadcast usados nos processos de *flooding*.

O objetivo de definir alguns MPRs é diminuir a quantidade de pacotes de controle na rede, pois se evita que os pacotes de controle trafeguem pelos outros nós. Com um objetivo similar, os pacotes de controle são transmitidos com informações parciais de estado de enlace, tendo assim seus tamanhos diminuídos. Desta forma, a quantidade total de bytes de controle trafegando através da rede pode ser significativamente reduzida, comparado a este mesmo protocolo caso não utilizasse este mecanismo de MPR.

Cada nó elege um ou mais vizinhos como MPR, como ilustrado na Figura 29. Então, cada nó MPR mantém informações de estado de enlace com os nós que o elegeram MPR – através de pacotes *hello*, cujo formato está ilustrado na Figura 31 e possuem seu TTL igual a 1, ou seja, não são reencaminhados. Todos os nós que não são MPRs recebem e processam as mensagens de broadcast recebidas, porém não as retransmitem. Na Figura 30, é mostrado o formato básico do pacote OLSR.

Um nó escolhe seu(s) MPR(s) entre seus vizinhos distantes de um salto, de forma que todos os vizinhos distantes de dois saltos sejam cobertos pelos MPRs. Assim um nó N possui como diretriz escolher o menor número de MPRs, que necessariamente estão distantes de um salto de N, para isso precisa escolher os MPRs que se comunicam com o maior número de nós distantes de dois saltos de N.

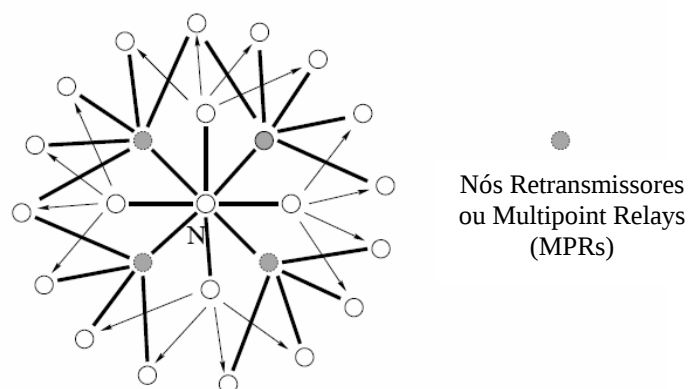


Figura 29: Multipoint Relays.

Fonte: Artigo conforme referência [Jacquet et al, 2005].

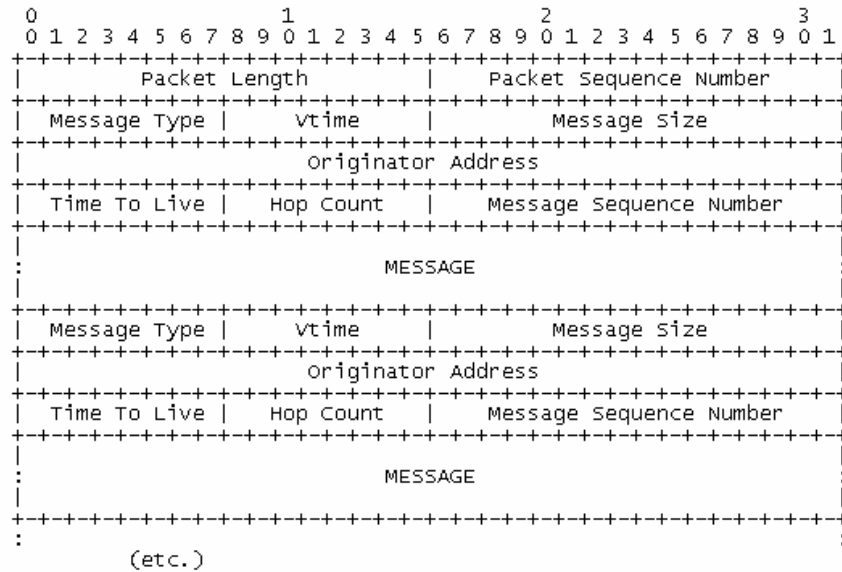


Figura 30: Formato básico do pacote no OLSR.

Fonte: RFC 3626.

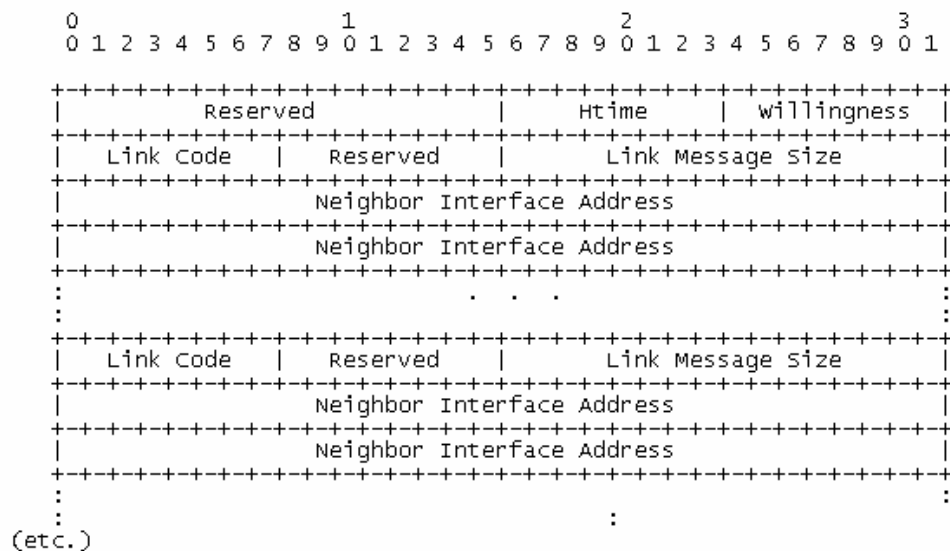


Figura 31: Formato do pacote *Hello* no OLSR.

Fonte: RFC 3626.

São definidos dois tipos de pacotes de controle: pacote *Hello*, conforme já explicado, e pacotes TC (*Topology Control Messages*). Estes últimos, cujo formato está mostrado na Figura 32, são disseminados pelos nós MPR, contendo informações suficientes para que cada nó construa suas tabelas de roteamento.

Nas implementações existentes do OLSR são utilizadas duas métricas, número de saltos (HOP), onde a menor distância entre dois nós é a única levada em conta para determinação da rota, e a métrica ETX (*Expected Transmission Count*), que utiliza a taxa de perda de pacotes para determinar o melhor caminho. Porém nenhuma dessas métricas leva em conta o tempo de transmissão entre dois nós, cuja solução é a proposta da métrica ETT (*Estimated Transmission Time*). Nos trabalhos [Schiller, 2007] e [Esposito et al, 2007], foi desenvolvido um *plugin* para implementar a métrica ETT no protocolo OLSR, sendo realizados diversos testes para avaliar seu desempenho. A grande vantagem dessa escolha é de não haver necessidade de modificar o código, privilegiando desta forma a portabilidade. Em [Schiller, 2007], a implementação demonstrou um pior desempenho se comparado ao ETX e assim, foi proposta como trabalho futuro uma alternativa para a implementação do ETT não apenas por um *plugin*, mas sim pela modificação do próprio protocolo OLSR. É importante destacar, que a métrica foi testada em um ambiente de testes real construído com roteadores Linksys e microcomputadores. Na referência [Esposito et al, 2007], a métrica ETT foi comparada com as métricas número de saltos (HOP) e ETX, em relação à taxa de perda de pacotes e à estabilidade das rotas. Os testes experimentais envolveram uma rede em malha implantada no Centro de Tecnologia da UFRJ composta por computadores pessoais e roteadores. Os resultados de [Esposito et al, 2007] mostraram que a métrica ETT obteve um melhor desempenho na média que o número de saltos e o ETX. O desempenho das métricas cientes da qualidade é melhor, caso haja mais de uma rota com qualidade e número de saltos diferentes entre origem e destino. Em particular, o ETT é vantajoso caso haja mais de uma rota até o destino com probabilidade de perda equivalente, porém com taxas de transmissão diferentes. Em relação à estabilidade das rotas, o número de trocas de rotas executadas com a métrica ETT ficou entre a quantidade das métricas HOP e ETX. Desta forma, com a métrica ETT o protocolo OLSR se adaptou melhor às variações de qualidade dos enlaces, sem gerar oscilações de rotas desnecessárias, obtendo o melhor desempenho em termos de entrega de pacotes.

4.1.3. WRP (*Wireless Routing Protocol*)

O WRP [Murthy e Garcia, 1996] é um protocolo que mantém as tabelas de roteamento completas em todos os nós da rede. Cada nó possui e mantém atualizadas quatro tabelas:

- Distância;
- Roteamento;
- Custo do enlace;
- Lista de retransmissão de mensagem (MRL).

Cada entrada da tabela MRL possui os seguintes parâmetros:

- Número de seqüência;
- Contador de retransmissões;
- *Flag* de confirmações requeridas, sendo uma entrada por vizinho;
- Lista de atualizações enviadas através das mensagens de atualização.

Os nós comunicam-se notificando mudanças do estado dos enlaces através das mensagens de atualização. Este tipo de mensagem é enviado somente para os nós vizinhos e contém uma lista de atualizações (o endereço do nó destino, a distância até o nó destino, e o nó predecessor do destino), assim como uma lista de respostas indicando os nós que deveriam enviar um pacote de confirmação (ACK) para as mensagens de atualização.

Um nó reconhece a existência dos nós vizinhos através do recebimento de pacotes de confirmação e de outras mensagens. Portanto, caso um nó não necessite enviar mensagens por um longo tempo, o mesmo deve enviar mensagens *hello* em intervalos regulares de tempo, garantindo assim o reconhecimento deste(s) enlace(s) para outros nós vizinhos. Caso um nó não receba mais nenhuma mensagem de outro determinado nó, o mesmo passa a considerar este nó como inalcançável.

Um novo nó é reconhecido por seus vizinhos através de mensagens *hello* que são enviados pelo nó “entrante” na rede. Assim, o nó que detectou o novo nó adiciona o endereço do novo nó na tabela de roteamento e envia uma cópia desta mesma tabela para o novo nó.

4.1.4. CGSR (*Cluster Gateway Switch Routing*)

No protocolo CGSR [Manoj e Murthy, 2004], a rede é organizada em *clusters*, identificando um nó que possuirá a responsabilidade de coordenar o cluster e todos os seus membros, chamado de *cluster-head*, que é único por *cluster*. Este *cluster-head* é selecionado dinamicamente através de um algoritmo chamado *least cluster change* (LCC). No CGSR, todo tráfego deve necessariamente passar pelo *cluster-head*. Todos os membros do cluster devem conseguir se comunicar diretamente com o *cluster-head* com apenas um salto. A comunicação entre dois clusters ocorre por nós chamados de *gateway*. Cada cluster pode possuir um ou alguns *gateways* para possibilitar a comunicação entre clusters. Os *gateways* são membros de mais de um cluster, podendo estabelecer comunicação com mais de um *cluster-head*.

Um nó deixa de ser *cluster-head* quando entra na área de outro *cluster-head*. Assim os dois nós irão “competir” para ser o *cluster-head*. O nó com menor ID ou com maior conectividade “ganha” a disputa e passa a ser o coordenador daquele determinado cluster.

Cada cluster compartilha a banda internamente. Então, dividindo-se a rede em clusters, diferentes *cluster-heads* podem operar diferentes códigos de espalhamento de nível físico, melhorando o reuso do canal.

O algoritmo usado é uma extensão do DSDV [Perkins e Bhagwat, 1994]. Cada nó membro do cluster mantém uma tabela de roteamento contendo o *cluster-head* destino para cada nó da rede. Além da tabela de membros do cluster, cada nó mantém uma tabela de roteamento que guarda uma lista dos próximos nós para alcançar cada cluster destino.

Quando um nó possui pacotes a serem transmitidos a um nó destino, o mesmo espera por sua vez para comunicar-se com o *cluster-head*, que obtém do nó origem, o *cluster-head* destino e o próximo nó, contidos na tabela de membros do *cluster* e na tabela de roteamento, respectivamente. E assim, os pacotes vão sendo encaminhados pelos *gateways* e *cluster-heads* intermediários até chegar ao *cluster-head* destino e em seguida chegar ao nó destino. A Figura 33 demonstra esse trajeto dos pacotes.

As tabelas mantidas pelos nós que usam o protocolo CGSR são:

- *Cluster member table* - tabela de membros do *cluster* (onde se encontra o *cluster-head* destino);

- *Routing table* - tabela de roteamento (onde se encontra o próximo nó).

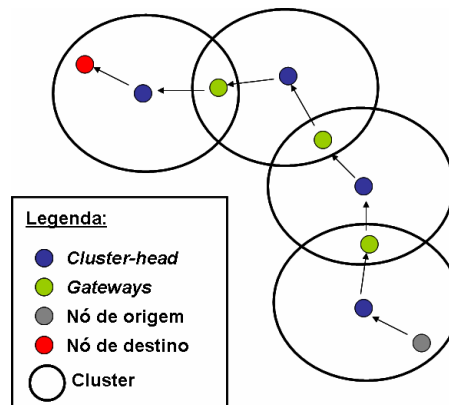


Figura 33: Trajeto dos pacotes – protocolo CGSR.

Fonte: Livro conforme referência 0.

Dentre as desvantagens desse protocolo, pode-se identificar sua característica de incrementar o tamanho do caminho e instabilidade em sistemas com alta mobilidade quando a taxa de mudanças de *cluster-heads* é alta. O consumo de bateria no *cluster-head* é consideravelmente mais alto do que os outros nós, o que pode acarretar na “perda” de tais nós e conseqüentemente em uma nova escolha de *cluster-head* e na quebra de algumas rotas.

4.1.5. FSR (*Fisheye State Routing*)

O FSR [Iwata et al, 1999] [Gerla et al, 2001] é um protocolo pró-ativo e utiliza a técnica de olho de peixe (*fisheye*) para reduzir o overhead causado pelos pacotes de controle. O princípio básico desta técnica é a propriedade de visão do peixe, na qual se pode capturar com mais acurácia as informações mais próximas ao ponto focal, enquanto as imagens mais distantes aparecem fora de foco.

Assim, o FSR tenta determinar com mais exatidão a topologia local e, em contrapartida, guarda informações menos exatas sobre os nós mais distantes. O detalhamento das informações da rede diminui com o aumento da distância do ponto focal.

O FSR mantém a topologia da rede de cada nó, mas não inunda toda a rede com estas informações. Ao invés da inundação, um nó troca informações da

topologia com os nós vizinhos. Existe uma seqüência numérica para identificar a topologia mais recente.

O FSR define o escopo do roteamento, que significa o conjunto de nós alcançáveis por uma determinada quantidade de saltos. A frequência de atualização muda conforme o escopo (grau de foco), modificando significativamente o overhead. Assim, quanto mais perto estiverem os nós, maior a frequência de troca de informações sobre eles.

O FSR, como os outros protocolos pró-ativos baseados em estado de enlace, mantém um mapa da topologia para cada nó da rede. A principal diferença deste protocolo é o modo pelo qual as informações de roteamento são difundidas, pois o protocolo FSR utiliza a técnica *fisheye* com o objetivo de diminuir o overhead de controle que trafega na rede.

Cada nó da rede mantém atualizadas três tabelas:

- Lista de vizinhos;
- Tabela da topologia;
- Tabela de roteamento.

a) Lista de vizinhos

Quando um nó recebe uma mensagem de estado do enlace, o mesmo grava e atualiza o endereço do nó que a enviou na lista de vizinhos. Se durante um período de tempo (*Neighbor_Timeout_Interval*) este nó não receber mais nenhuma mensagem de atualização do vizinho, este vizinho será descartado da lista. Nesta lista, constam as seguintes informações:

- ID (identificador) do nó vizinho;
- Último instante de tempo em que o nó recebeu a mensagem de atualização do nó vizinho.

b) Tabela da topologia

Esta tabela contém as informações sobre a topologia da rede obtidas através das mensagens de estado do enlace. Cada destino possui uma entrada na tabela. Cada entrada da tabela possui três partes: informações do destino, informações sobre o estado do enlace e variáveis para seleção das entradas. É baseada nesta tabela, que a tabela de roteamento é calculada.

c) Tabela de roteamento

Esta tabela provê a informação de próximo salto para o encaminhamento para outros destinos da rede. As entradas são atualizadas de acordo com as mudanças ocorridas na tabela da topologia. Desta forma, esta tabela possui os seguintes campos:

- Endereço de destino;
- Endereço do próximo salto;
- Distância.

d) Mensagens de estado do enlace

Periodicamente, os nós enviam em broadcast uma porção efetiva da tabela de topologia para seus vizinhos. Ouvindo tais mensagens, cada nó constrói e atualiza suas tabelas. O formato da mensagem de estado do enlace é mostrado na Figura 34.

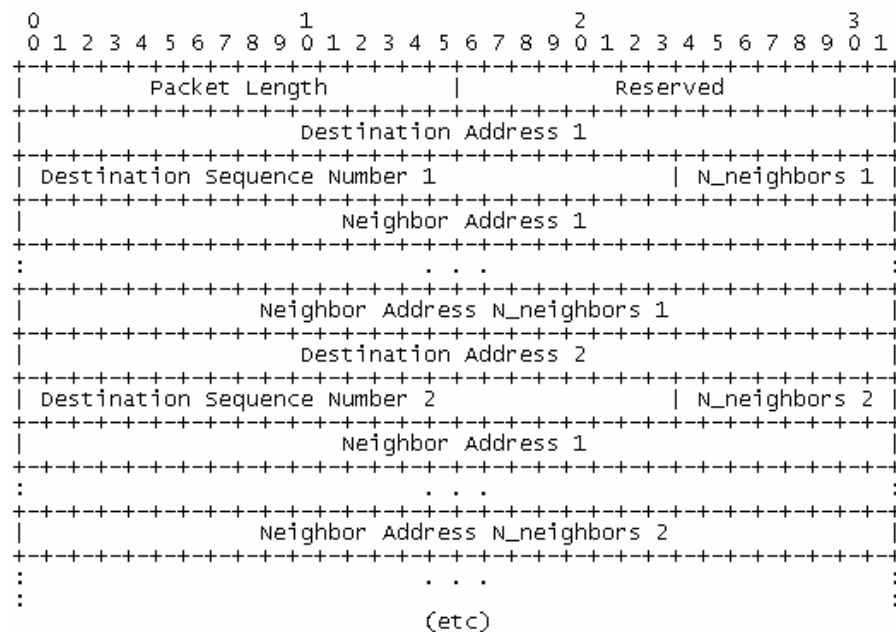


Figura 34: Formato do pacote de estado do enlace para o protocolo FSR.

Fonte: INTERNET-DRAFT, Fisheye State Routing Protocol (FSR) for Ad Hoc Networks. [Gerla et al, 2001]

Este protocolo tende a reduzir significativamente o consumo de banda, sendo mais apropriado para redes amplas (grande quantidade de nós) e com alta mobilidade dos nós. A escolha do número de saltos associados com o escopo do

nível (grau do foco) tem influência no desempenho da rede. Como desvantagem é identificada a perda de desempenho em redes menores.

4.2. PROTOCOLOS REATIVOS

Nos protocolos de roteamento reativos, os nós só procuram um determinado caminho quando existe a necessidade de comunicação com um destino específico. Uma das vantagens deste tipo de protocolo é uma redução considerável de pacotes de controle que trafegam através da rede, pois não há necessidade de tráfego de pacotes de controle para atualização de rotas e exclusão de rotas válidas. Como desvantagem significativa, pode-se identificar o tempo longo de descoberta de rota para o nó destino. Este atraso é um fator a ser considerado, principalmente quando ocorre um cenário de muitas mudanças de rota durante a comunicação entre os nós.

4.2.1. DSR (*Dynamic Source Routing*)

O DSR [Johnson e Maltz, 1996] [Johnson et al, 2002] é um protocolo do tipo roteamento na origem (*source routing*) e como tal, lida com rotas completas que são aprendidas através da etapa de descobrimento de rotas iniciada pelo dispositivo de origem, caso o mesmo não conheça a rota para um determinado destino. Como é um protocolo reativo, o DSR apenas inicia o mecanismo de descobrimento de rotas quando existe a necessidade de comunicação com um destino e a rota não é conhecida, não sendo necessários pacotes periódicos de atualização de rota.

Assim, é possível identificar duas etapas principais deste protocolo:

- Descobrimento de rotas;
- Manutenção de rotas (através de confirmação de entrega).

O mecanismo de manutenção de rotas, utilizado enquanto há comunicação entre dois dispositivos, é necessário para identificação de rotas que se tornaram inválidas. Quando rotas inválidas são identificadas, uma rota alternativa já conhecida é escolhida ou o mecanismo de descobrimento de rotas é iniciado novamente.

Existe uma tabela de rotas aprendidas recentemente, denominada *cache* de rotas, onde cada rota possui um tempo de validade dependente da mobilidade do ambiente. Os nós, de origem e intermediários, armazenam em seus *caches* tanto as

rotas aprendidas através do mecanismo de descobrimento de rotas, quanto àquelas identificadas através de pacotes que são encaminhados tendo a rota completa em seus cabeçalhos.

a) Mecanismo de descobrimento de rotas

Como já citado anteriormente, este mecanismo é iniciado quando surge a demanda de envio de tráfego para um destino desconhecido pela origem. Assim um pacote de *route request* é enviado em broadcast para todos os nós da rede até que algum nó intermediário conheça a rota para o destino ou até que o *route request* chegue ao nó destino.

O pacote *route request* contém um campo onde é armazenada a seqüência de nós pelos quais o pacote passa, durante a descoberta da rota, até alcançar o destino. Este campo é identificado como registro de rota.

Desta forma, são encontrados no pacote de *route request* alguns campos como:

- Identificador de requisição, usado para diferenciar cada pedido de rota;
- Nó de origem;
- Nó de destino;
- Registro de rota.

Ao receber um *route request*, primeiramente, o nó verifica se as informações nó de origem e identificador de requisição já foram processadas recentemente, para evitar que a mesma solicitação seja processada mais de uma vez. Isso é possível, pois cada nó possui uma lista de requisições que foram processadas pelo mesmo recentemente. Em seguida, o nó verifica se ele mesmo se encontra no registro de rotas, pois se isso ocorrer significa que se o nó encaminhar esta requisição estará gerando um *loop* (ou seja, o caminho passaria duas vezes pelo mesmo nó). Dando continuidade ao processo, o nó verifica se ele mesmo é o destino:

- Sendo o destino, o mesmo procura em seu *cache* se existe uma rota válida para origem. Existindo, responde com um *route reply*, o qual possui o registro completo de nós pelo qual o *route request* passou até chegar ao destino. Caso o nó não tenha a rota para o nó origem

registrada, pode enviar o *route reply* para o sentido inverso da rota já descoberta.

- Não sendo o destino, o nó inclui seu endereço no registro de rota e encaminha o pacote *route request* em difusão (broadcast).

b) Mecanismo de manutenção de rotas

Para a identificação da validade da rota, ocorre uma monitoração da rota por parte dos nós que a integram. Ao ser estabelecida uma comunicação entre dois nós, existe a necessidade de confirmação de recebimento do pacote de informação, ou seja, ao encaminhar um pacote, o nó aguarda uma confirmação de recebimento do nó seguinte na ordem do registro de rota. Assim, utiliza-se este mecanismo para identificar quebras de rotas, uma vez que não existem pacotes de atualização neste protocolo.

Este reconhecimento pode ser feito em modo promíscuo, ou seja, verificando o reenvio do pacote, pelo nó que o recebeu, para o próximo nó do registro da rota, quando é chamado de reconhecimento passivo. Desta forma, pode-se evitar um pacote de ACK, por exemplo.

Cada nó estima o RTT (*round trip time*) para os outros nós os quais este tentou transmitir pacotes, assim, estima o *timeout* (tempo para expirar) para cada retransmissão de pacote.

Caso esta confirmação não seja enviada, após uma determinada quantidade máxima de retransmissões que pode ser estipulada, o nó que a estava aguardando, envia para o nó origem um pacote de erro de rota, detectando falha na rota. O pacote erro de rota identifica o nó que detectou a falha e o nó que tentou ser alcançado. Desta forma, o nó origem atualiza seu *cache* e apaga todas as rotas que possuam este enlace, agora inválido.

Tendo outra rota válida para o destino em seu *cache*, o nó origem envia suas informações por esta rota. Caso não tenha, reinicia o processo de descobrimento de rota.

Os formatos de pacote *route request*, *route reply*, *route error* e ACK são ilustrados respectivamente na Figura 35, Figura 36, Figura 37, Figura 38.

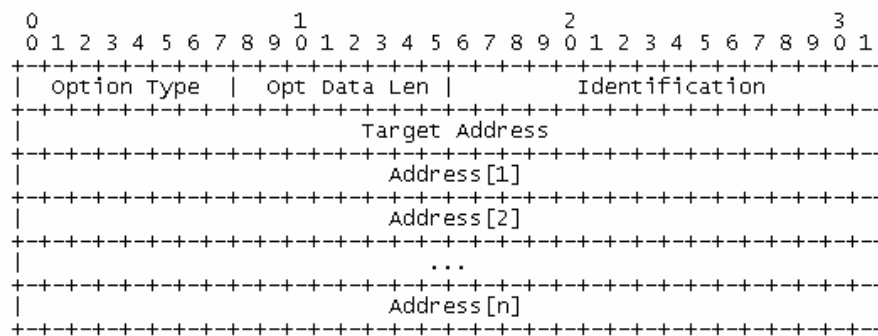


Figura 35: Formato do pacote route request do protocolo DSR.

Fonte: INTERNET-DRAFT, The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR). [Johnson e Maltz, 1996]

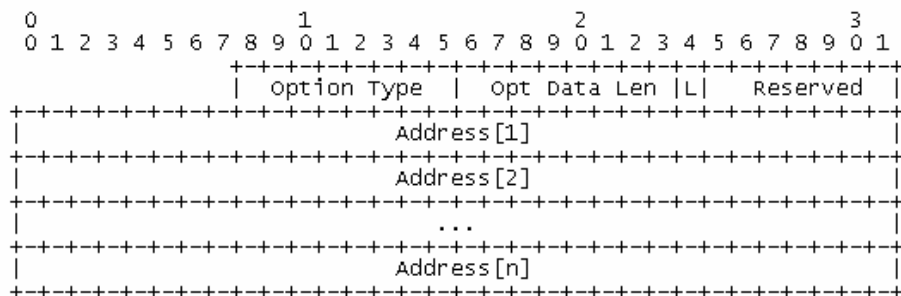


Figura 36: Formato do pacote route reply do protocolo DSR.

Fonte: INTERNET-DRAFT, The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR). [Johnson e Maltz, 1996]

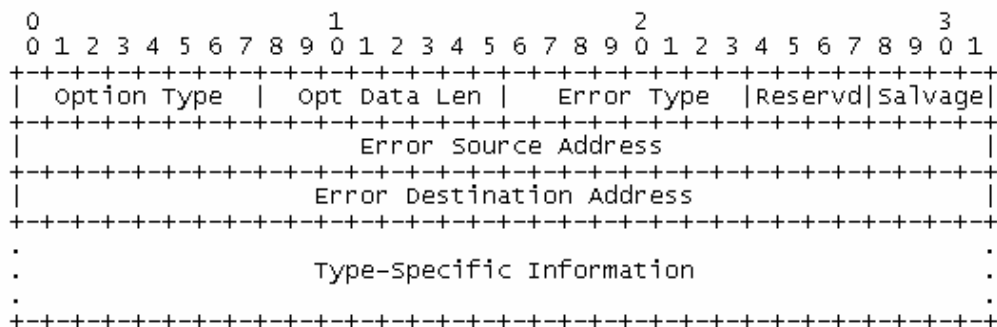


Figura 37: Formato do pacote route error do protocolo DSR.

Fonte: INTERNET-DRAFT, The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR). [Johnson e Maltz, 1996]

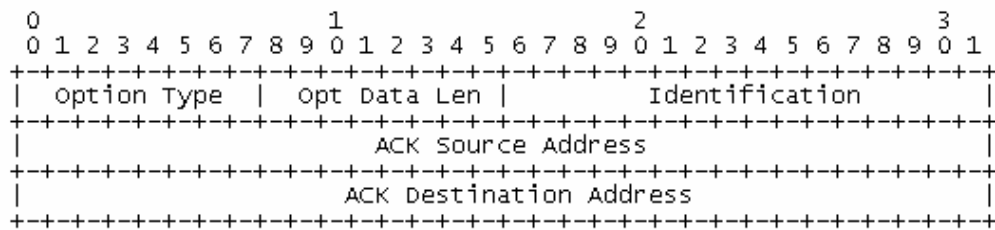


Figura 38: Formato do pacote de confirmação (ACK) do protocolo DSR - opcional.

Fonte: INTERNET-DRAFT, The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR). [Johnson e Maltz, 1996]

Uma das vantagens do DSR é a existência do *cache* utilizado por cada nó, identificando rotas válidas. Porém estes mesmos *caches* tendem a ficar demasiadamente grandes em caso de redes com muitos nós, gerando ineficiência no processamento das rotas.

Como desvantagem, identifica-se a tendência de crescimento de pacotes *route request* e *route reply*, tanto em quantidade como em tamanho dos pacotes, caso a rede seja densa e com grande quantidade de nós.

Além das desvantagens comentadas, ainda pode-se citar a questão do *overhead* (banda despendida para controle). Como todo o protocolo de roteamento na origem, a quantidade de bytes de *overhead* é geralmente mais alta comparando-se com outros tipos de protocolos, devido a todos os pacotes carregarem em seus cabeçalhos todas as informações referentes à rota para a comunicação.

4.2.2. AODV (*Ad Hoc On-Demand Distance Vector*)

O AODV [Perkins e Royer, 1999] [Perkins e Royer, 2003] é um protocolo considerado reativo, mas utiliza-se de algumas facilidades dos protocolos considerados pró-ativos. É um protocolo baseado no algoritmo de vetor de distância [Kurose e Ross, 2004], porém com algumas modificações para um funcionamento eficiente em redes sem fio. Tenta eliminar a necessidade de um *broadcast* global das informações de roteamento, evitando o alto consumo de banda por pacotes de controle.

O AODV possui algumas características que possibilitam uma rápida adaptação a modificações de topologia.

a) Pacotes de Controle

Existem três tipos principais de pacotes de controle neste protocolo: *route request* (RREQ), *route reply* (RREP) e *route error* (RERR). Os formatos de pacote são exibidos na Figura 39, Figura 40 e Figura 41.

O pacote RREQ é enviado quando algum nó necessita transmitir informações para algum nó destino e não possui, em sua tabela de roteamento, nenhuma entrada para este destino. Cada RREQ possui um ID (identificação chamada de RREQ ID), que junto com o endereço IP de origem, serve para diferenciar uma mensagem RREQ específica de outras mensagens RREQs. O RREQ ID é incrementado pela origem a cada RREQ.

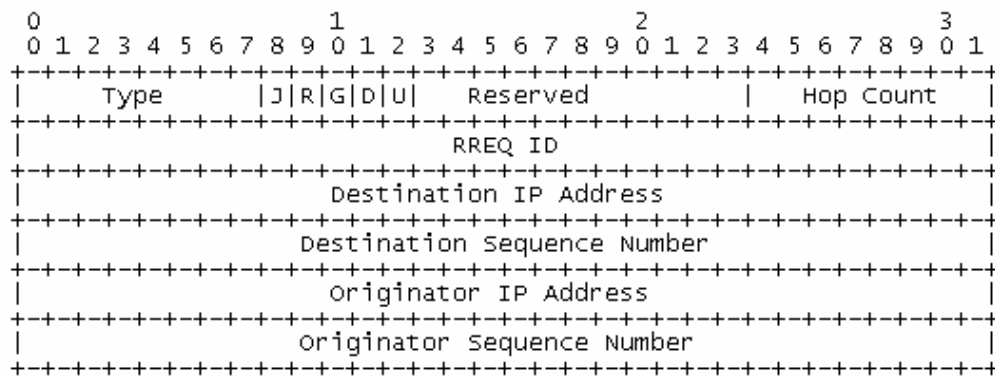


Figura 39: Formato do pacote de RREQ do protocolo AODV.

Fonte: RFC 3561.

O pacote RREP é usado para responder a requisição feita pelo pacote RREQ, ou seja, até que o pacote RREQ chegue ao nó destino ou a um nó que conheça uma rota atual e válida para o destino. Assim, o RREP é encaminhado para o nó de origem da requisição.

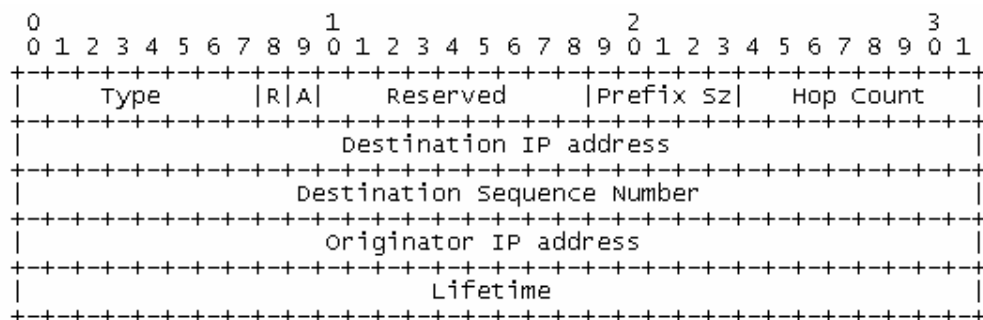


Figura 40: Formato do pacote de RREP do protocolo AODV.

Fonte: RFC 3561.

b) Tabela de roteamento

Cada nó possui uma tabela com todas as rotas já usadas em um determinado momento. Nestas tabelas são armazenadas as seguintes informações:

- Endereço de destino;
- Número de seqüência do destino;
- *Flag* de validade do número de seqüência do destino;
- Estado da rota (válida, inválida, reparável e sendo reparada);
- Interface de rede;
- Saltos (quantidade de saltos para chegar ao nó destino);
- Próximo salto;
- Lista de precursores (nós que utilizam a rota);
- Tempo de vida da rota.

c) Princípios do funcionamento do protocolo

Conforme já adiantado, quando um nó possui a necessidade de enviar informações para outro nó da rede e não identifica uma rota válida em sua tabela de roteamento para tal nó destino, o nó origem envia um pacote de requisição de rota, chamado RREQ, em *broadcast*.

Os nós intermediários verificam se são o destino ou se os mesmos conhecem uma rota para o destino. No caso do nó ser o destino ou de possuir em sua tabela de roteamento o caminho para o nó destino, o mesmo envia um RREP para o nó de origem da requisição, pelo mesmo caminho no sentido oposto, mantendo o número de seqüência do pacote RREQ. Caso não seja o destino e não conheça o caminho para o destino, o nó intermediário encaminha a solicitação adiante aos seus nós vizinhos.

Cada nó conhece apenas o próximo salto para chegar ao destino e a quantidade de saltos até o destino, não identificando a rota completa como no caso do protocolo DSR.

Cada nó possui seu número de seqüência, o qual é incrementado a cada mensagem RREQ, RREP ou RERR. Este número de seqüência serve para identificar a rota mais recente. Um nó sabe que o número maior é mais recente, portanto, não propaga uma rota com um número menor do que uma rota que este já

tenha propagado. Além disso, permite identificar se uma requisição de descobrimento de rota chegou duplicada. Em caso afirmativo, pode desconsiderar o último pacote de broadcast e evitar processamento e encaminhamento desnecessário do pacote em questão.

Para a identificação rápida de quebra de enlace, mensagens *hello* são enviadas periodicamente de cada nó para seus vizinhos. Se ocorrer de um nó não receber mais mensagens *hello* de um vizinho, o mesmo assume que aquele enlace não está mais ativo e dissemina a informação que este enlace está indisponível para os nós que dependiam dele para estabelecer determinadas rotas. Este aviso é realizado pelo pacote RREP com valor de saltos extremamente alto, assim o mesmo é propagado através da rede até a origem, a qual opta se utiliza o mecanismo de requisição de rotas para reconhecer outro caminho ou se apenas interrompe a comunicação com o nó destino. Além disso, as rotas mais antigas são eliminadas após algum tempo sem uso.

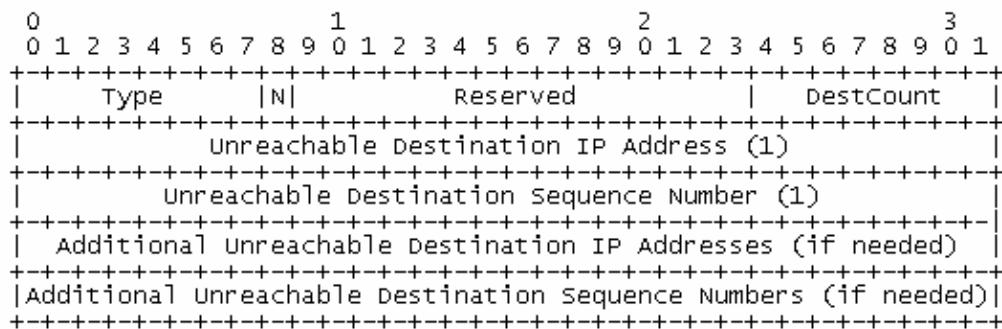


Figura 41: Formato do pacote de RERR do protocolo AODV.

Fonte: RFC 3561.

O AODV apresenta apenas uma rota para cada destino, sendo este um problema em caso de perda da rota, pois é necessário reiniciar o mecanismo de requisição de rota.

4.2.3. TORA (*Temporally Ordered Routing Algorithm*)

O protocolo TORA [Corson e Park, 2001] procura diminuir o tráfego de controle, mesmo que para isso a rota encontrada não seja a ótima. Para minimizar a quantidade de pacotes de controle, as mudanças topológicas são divulgadas apenas para os vizinhos mais próximos, assim, cada nó possui informações referentes somente aos seus vizinhos. Este protocolo pode estabelecer múltiplos caminhos para um mesmo destino.

O TORA trabalha em conjunto com o protocolo IMEP (*Internet MANET Encapsulation protocol*), que possui as seguintes atribuições:

- Monitorar e manter o estado das conexões;
- Controlar a entrega dos pacotes;
- Resolver os endereços de rede;
- Autenticar e prover segurança.

O TORA possui alguns mecanismos diferentes para o estabelecimento das comunicações entre os nós da rede:

- Criação de rotas;
- Manutenção de rotas;
- Eliminação de rotas;
- Otimização de rotas.

a) Criação de rotas

A criação de rotas ocorre através da construção de um grafo acíclico dirigido até o destino (DAG – *directed acyclic graph*). Cada nó está a uma certa “altura” (quantidade de saltos) do destino. Resumindo, DAG é o conjunto de rotas, orientadas de um nó origem para um nó destino.

Quando um nó deseja estabelecer comunicação com um determinado nó destino e não conhece previamente a rota, o mesmo dispara na rede um pacote chamado *query* (QRY) (cujo formato é exibido na Figura 42), o qual será respondido pelo nó destino ou por algum nó intermediário que conheça o caminho até o nó destino. Esta resposta ocorre através de um pacote denominado *update* (UPD), cujo

formato é ilustrado na Figura 43, o qual possuirá a “altura” do nó em relação ao destino. À medida que o pacote UPD é propagado na rede, os nós que recebem tal pacote ajustam sua “altura” a um valor incrementado em relação a seu vizinho, que lhe enviou o pacote.

Quando o pacote QRY é encaminhado, os nós ajustam um *flag* de rota requisitada para *on* e descartam qualquer pacote QRY subsequente recebido para o mesmo destino.

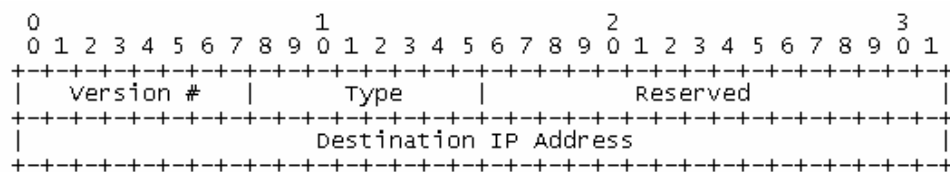


Figura 42: Formato do pacote de query (QRY) do protocolo TORA.

Fonte: INTERNET-DRAFT, Temporally-Ordered Routing Algorithm (TORA). [Corson e Park, 2001]

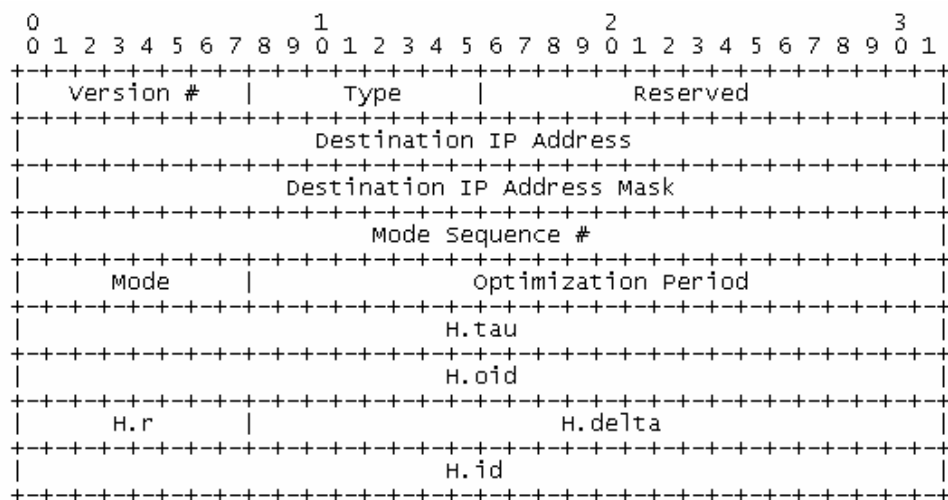


Figura 43: Formato do pacote de update (UPD) do protocolo TORA.

Fonte: INTERNET-DRAFT, Temporally-Ordered Routing Algorithm (TORA). [Corson e Park, 2001]

b) Manutenção e eliminação de rotas

Quando um nó descobre que uma rota para um determinado nó passou a ser inválida, o mesmo ajusta sua “altura” para um valor mais alto do que de seus vizinhos e origina um pacote *update*, e o encaminha em um sentido reverso, no sentido contrário ao DAG. Este processo está explícito na Figura 44, onde o nó 1 é a origem, e já foi estabelecida rota para comunicação com o nó 7. A rota que está sendo usada é através dos nós intermediários 4 e 5. Porém houve uma quebra de

cujo formato é demonstrado pela Figura 46. Este pacote é processado e encaminhado pelos nós da rede. O pacote OPT identifica o nó destino, o modo de operação para o nó destino e a “altura” do nó que está enviando o pacote OPT. Este pacote também contém uma seqüência numérica usada para identificá-lo e garantir que cada nó intermediário processe e encaminhe o pacote OPT de um determinado destino somente uma vez. Quando o pacote OPT é encaminhado, os nós mudam seu modo de operação, readaptando suas “alturas” e enviando o pacote OPT para seus vizinhos que identificam o destino e a nova “altura” do nó que enviou o pacote UPD.

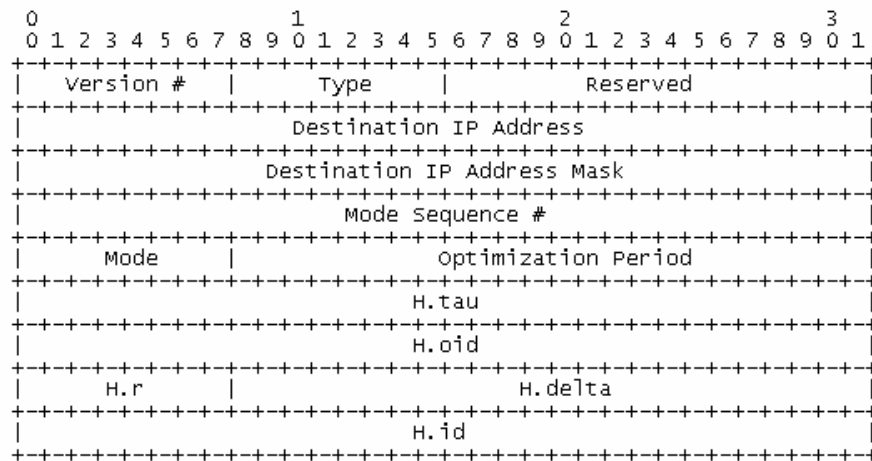


Figura 46: Formato do pacote optimization (OPT) do protocolo TORA.

Fonte: INTERNET-DRAFT, Temporally-Ordered Routing Algorithm (TORA). [Corson e Park, 2001]

Uma vantagem do TORA é armazenar múltiplos caminhos para um mesmo par de nós, pois caso ocorra uma queda de enlace e a rota torne-se inválida, rapidamente outra rota válida passa a ser utilizada. Em contrapartida, quando ocorre uma quebra de rota e escolhe-se outra rota já armazenada, em geral, a nova rota escolhida pode não ser a melhor rota. Isto pode causar, dependendo da topologia da rede, prejuízo de desempenho de várias formas, tais como aumento da perda de pacotes, aumento do atraso, grande quantidade de saltos até o destino, entre outros parâmetros, que podem estar significativamente abaixo do padrão aceitável para determinadas aplicações.

4.2.4. ABR (*Associativity Based Routing*)

O protocolo ABR [Toh, 2002] estabelece as rotas de acordo com o grau de estabilidade de associação - *degree of association stability*. Esta é a métrica usada para o cálculo da rota a ser escolhida para a comunicação entre dois nós distintos.

Todos os nós enviam periodicamente *beacons* para seus vizinhos. A cada *beacon* recebido, é incrementado o contador do grau de associação do nó que gerou o sinal. Quanto mais alto o valor do contador de *beacons* recebidos, maior é o grau de estabilidade de associação, pois significa que o enlace é mais estável. Quando esses contadores estão com valores baixos, o grau de associação é baixo, uma vez que poucos *beacons* foram registrados entre os nós em questão.

O ABR possui três mecanismos:

- Descobrimiento de rotas;
- Reconstrução de rotas;
- Eliminação de rotas.

Sendo um protocolo reativo, o processo de descobrimiento de rotas é iniciado quando existe a necessidade de estabelecimento de comunicação entre dois nós e o nó origem não possui em seu *cache* a rota para alcançar o nó destino. O nó origem envia um pacote de requisição, *route request*, inundando a rede para o descobrimiento da rota. À medida que os nós intermediários recebem este pacote, os mesmos adicionam no pacote seu endereço e seu valor do grau de associação e encaminham o pacote. O nó intermediário seguinte, que recebe o pacote *route request*, retira do pacote o valor do grau de associação antigo, inserindo o seu e o valor de associação da rota percorrida pelo pacote. Quando o primeiro *route request* chega ao nó destino, o nó aguarda um período ($T_{\text{RouteSelectTime}}$) para chegarem mais alguns *route requests*, que atravessaram a rede por outras rotas. Assim, o nó destino escolherá o caminho de acordo com a rota que possuir a maior estabilidade dos enlaces. Em caso do grau de associação ser igual em dois caminhos, o que possuir menor número de saltos será o escolhido. No caso de mais de um caminho possuir o mesmo grau de associação e o mesmo número de saltos, um caminho é escolhido aleatoriamente.

Uma das vantagens encontradas no ABR é a utilização de rotas estáveis, as quais, dependendo da rede, possuem menor probabilidade de quebra de rota, reduzindo assim a quantidade de pacotes de controle utilizados para a reconstrução de rotas perdidas. Em contrapartida, o protocolo pode por muitas vezes escolher caminhos mais longos, por utilizar o critério de estabilidade entre os nós vizinhos e não levar em consideração a quantidade de saltos do nó origem até o nó destino.

4.2.5. SSA (*Signal Stability-Based Adaptive Routing Protocol*)

O SSA [Dube, 1997] é um protocolo reativo, que baseia sua escolha da rota na estabilidade do sinal (medida pela força do sinal). Assim, *beacons* são enviados entre os nós vizinhos e através destes a potência do sinal é mensurada, possibilitando a classificação do enlace em estável e instável.

O SSA é composto por dois outros protocolos:

- Protocolo de encaminhamento (FP);
- Protocolo de roteamento dinâmico (DRP).

O DRP de um determinado nó interage com o DRP dos outros nós, mantendo a tabela de roteamento. O FP é responsável pelo encaminhamento propriamente dito, encaminhando um pacote para um destino através do próximo salto, determinado na tabela de roteamento.

Cada nó mantém uma tabela que contém um contador de *beacon* e a potência do sinal de cada enlace para o nó vizinho. Existe uma tabela em cada nó da rede, chamada de tabela de estabilidade do sinal (SST), a qual possui a listagem da medição da potência do sinal de cada nó vizinho. Desta forma, quando um nó recebe um *route request*, o mesmo utiliza a SST para encaminhá-lo priorizando o caminho mais estável (com maior potência de sinal).

Caso ocorra uma falha na tentativa de envio do *route request* através dos enlaces estáveis, o protocolo inunda a rede sem considerar a estabilidade dos enlaces. Porém, um nó apenas processa um *route request* se o tiver recebido de um enlace estável, diferente da maioria dos outros protocolos de roteamento de redes ad-hoc. Assim, um *route request* recebido de um enlace instável é descartado sem ser processado. O destino seleciona o primeiro *route request* recebido através de um

enlace estável e então envia um *route reply*, notificando o caminho escolhido para o nó origem.

Ao contrário do ABR, o SSA restringe o encaminhamento do pacote *route request* para os nós intermediários, se o pacote foi recebido através de um enlace fraco. Quando um *route request* é enviado pelo nó origem, primeiramente é processado por todos os nós vizinhos. Em seguida, cada nó vizinho verifica se o pacote chegou através de um enlace estável. Caso tenha utilizado um enlace fraco, o pacote não é retransmitido para os próximos nós.

O nó origem, depois de receber um pacote de notificação de quebra de rota, envia novamente o *route request* em broadcast pela rede para encontrar outro caminho estável para o nó destino. Entradas antigas apenas são removidas da tabela de roteamento caso pacotes de dados, que usam a informação da rota antiga, falharem ao tentar alcançar o próximo nó. Se nenhum caminho estável está disponível quando um enlace apresenta falha, então uma nova rota é estabelecida considerando enlaces instáveis também. Isto ocorre quando múltiplos *route requests* falham ao tentar obter um caminho para o nó destino usando somente enlaces estáveis.

A principal vantagem do protocolo SSA está quando a rede é pouco dinâmica, assim escolhem-se caminhos estáveis, os quais possuem menor probabilidade de perda de pacotes devido a enlaces não estáveis. Em contrapartida, o protocolo pode por muitas vezes escolher caminhos mais longos, por utilizar o critério de estabilidade devido à potência do sinal entre os nós vizinhos e não levar em consideração a quantidade de saltos do nó origem até o nó destino. Outra desvantagem é quando se utiliza este protocolo em uma rede muito dinâmica, sendo necessários muitos pacotes de controle para se achar um caminho após uma falha. Isso ocorre principalmente porque este protocolo, inicialmente, não aceita o uso de caminhos pouco estáveis nos primeiros pacotes de *route request*, sendo necessário mais de um *broadcast* para se encontrar uma rota que em determinado momento não possui caminhos estáveis disponíveis.

4.3. PROTOCOLOS HÍBRIDOS

4.3.1. ZRP (*Zone Routing Protocol*)

O ZRP [Haas, 2001] é um protocolo híbrido, ou seja, utiliza-se de dois diferentes protocolos de roteamento, IERP [Haas et al, 2001 b] e IARP [Haas et al, 2001], e define zonas de roteamento. Dentro de tais zonas, o protocolo usado é do tipo pró-ativo e chamado IARP (*intra-zone routing protocol*). Entre as zonas de roteamento, o protocolo usado é reativo e é chamado de IERP (*inter-zone routing protocol*).

O raio da zona de roteamento é determinado pelo número de saltos a partir de um determinado nó central (ex. $r=3$, três saltos delimitam o raio da zona). Assim, cada nó possui sua zona de roteamento, com um tamanho comum de raio definido para toda rede.

Caso nó de destino e nó de origem, que desejam trocar informações, estejam na mesma zona de roteamento, geralmente nenhum mecanismo de descoberta de rota será iniciado, pois os mesmos já possuem em suas tabelas de roteamento a rota para estabelecer a comunicação.

Caso o nó destino não esteja na mesma zona de roteamento do nó origem, o nó origem gera um pacote de *route query* (também chamado de *route request*), que é identificado pelo ID (identificador) do nó origem e pelo número de requisição. Este pacote é enviado para todos os nós de borda da zona de roteamento, em *unicast*, evitando uma inundação de pacotes de controle dentro da zona de roteamento. A seqüência de IDs de todos os nós é gravada no pacote *route query*, determinando a rota (cada nó que encaminha este pacote insere seu endereço no pacote). Se o destino não estiver naquela zona, os nós de borda vão reenviar o pacote de *route query* para os nós periféricos da zona (nós de borda) e assim sucessivamente até encontrar o nó destino. Se o destino está naquela zona de roteamento, um *route reply* é enviado de volta para a origem, através da rota reversa que foi acumulada. Um nó descartará qualquer outro pacote de *route query*, quando já foi anteriormente encontrada a rota. Um *route reply* pode encontrar inúmeras rotas para um destino, porém este protocolo utiliza apenas uma rota para cada destino, assim, a qualidade

4.4. TRABALHOS RELACIONADOS SOBRE COMPARAÇÃO DE PROTOCOLOS DE ROTEAMENTO AD-HOC

A referência [Sesay et al, 2004] comparou protocolos de roteamento ad-hoc (AODV, DSR, TORA e DSDV) em um cenário com mobilidade dos nós. Para tal estudo foi utilizado o software para simulações NS-2 [NS2, 2005]. O cenário teve como variação de parâmetro, a velocidade máxima dos nós (1,5 m/s e 30 m/s) e a quantidade de nós (30 e 60 nós). Foram comparadas 4 situações distintas com a combinação destas variações de parâmetros.

As métricas usadas para esta avaliação foram: vazão, overhead, tempo de aquisição de rota, entre outras. Para cada caso, foi atribuída uma nota para cada protocolo (1 é a melhor nota e 4 é a pior), conforme a Figura 48. O resultado identificou o protocolo AODV como o melhor para o cenário proposto por apresentar os melhores resultados: maior quantidade de notas 1 e menor somatório de notas, conforme seguem: 29 (DSDV), 16 (AODV), 21 (DSR) e 27 (TORA).

Table 1: Numerical comparison of the four routing protocols

Metrics	DSDV	AODV	DSR	TORA
Scalability	4	2	3	1
Delay	1	3	2	4
Routing overload	4	2	1	3
Packet drop	4	1	2	3
Route acquisition time	1	2	4	3
Throughput	3	1	2	4
Adaptability to dynamic environment	4	2	3	1
Bandwidth conservation	4	1	3	2
Energy conservation	4	2	1	3

Figura 48: Tabela comparativa utilizada pela referência [Sesay et al, 2004] para definição do protocolo de roteamento mais indicado para o cenário proposto.

Fonte: Artigo conforme referência [Sesay et al, 2004].

Em [Oliveira, 2006], foram comparados protocolos de roteamento ad-hoc com protocolos de sensores sem fio, sendo que estes últimos, em geral, demonstraram

melhor desempenho se comparado aos protocolos de roteamento ad-hoc. As métricas utilizadas foram: vazão, percentual de perdas, percentual de perdas por congestionamento, percentual de perdas por colisões e atraso, tanto em transmissões ponto-a-ponto, quanto em ponto-multiponto.

As referências [Pereira, 2004] e [Pereira e Pedroza, 2004] focam em redes ad-hoc para aplicações militares. Com o objetivo de analisar o melhor protocolo de roteamento ad-hoc para este tipo de cenário, três protocolos de roteamento foram simulados: AODV, DSR e DSDV no NS-2 [NS2, 2005]. Nesse trabalho, a mobilidade teve grande influência, incluindo características de movimentação específicas para retratar uma situação real de uma operação militar em um campo de batalha. As métricas utilizadas foram:

- Taxa média de entrega de pacotes - razão entre o número de pacotes entregues para o destino e o número de pacotes gerados pela aplicação na fonte;
- Atraso médio de pacotes de dados - inclui todos os possíveis atrasos causados pela latência da descoberta de rotas, propagação, atrasos devido a retransmissões do nível MAC e tempos de transferência;
- Número de pacotes de roteamento - foi medido o número de pacotes de roteamento;
- Número de pacotes entregues - foi medido o número de pacotes de dados entregues para o destino.

MÉTRICAS	DSDV	AODV	DSR
Taxa Média de Entrega	86,05%	96,35%	96,60%
Atraso Médio (seg)	0,0308	0,0379	0,0567
Pacotes de Roteamento	2595	3207	1811
Pacotes Entregues	30566	34223	34355

Figura 49: Tabela comparativa utilizada pela referência [Pereira e Pedroza, 2004] para definição do protocolo de roteamento mais indicado para o cenário proposto.

Fonte: Artigo conforme referência [Pereira e Pedroza, 2004].

A Figura 49 identifica o resultado obtido das simulações realizadas em [Pereira e Pedroza, 2004]. Considerando taxa média de entrega de pacotes, o DSDV teve o pior desempenho, o que tem grande associação ao descarte por “quebra de enlace” que foi responsável por 44% dos descartes, sendo o principal ofensor. O DSDV descartou 50% dos pacotes na fila de roteamento, pois sua implementação restringe a 5 pacotes aguardando na fila de roteamento por rota para um

determinado destino. O DSDV e o AODV apresentaram o melhor desempenho em relação à métrica de atraso, já que o DSR, como tem múltiplas rotas para o mesmo destino, pode enviar pacotes por rotas antigas armazenadas no seu *cache*, que não são mais válidas.

O AODV gerou mais pacotes de roteamento do que o DSR, embora os dois operem por demanda. Embora o DSDV exija trocas periódicas de tabelas de roteamento, com a finalidade de manter suas tabelas atualizadas, esse protocolo gerou número de pacotes de roteamento inferior ao AODV, já que não utiliza pacotes de requisição de rotas, que são específicos dos protocolos que operam por demanda.

Assim, o DSR, que opera sob demanda e tem característica de múltiplas rotas, foi considerado o protocolo que apresentou o melhor desempenho nas diversas simulações realizadas, apesar de apresentar um atraso suavemente maior. Esta escolha foi baseada nas características do cenário proposto, em que os nós dentro de um grupo estão próximos uns dos outros. Neste caso, as rotas são facilmente restabelecidas em caso de quebra de enlace, já que, em geral, qualquer nó dentro de um grupo pode servir para encaminhar pacotes.

As referências [Campista et al, 2006] e [Cerveira e Costa, 2006] abordam a questão da capacidade do canal de interatividade ad-hoc para a TV digital e para tal simulam os protocolos de roteamento AODV e OLSR. As simulações foram realizadas no NS-2, considerando cinco cenários diferentes: Rocinha, Ramos, Copacabana, Parque Anchieta e Paty do Alferes, conforme Figura 50.

	Rocinha	Ramos	Copacabana	Parque Anchieta	Paty do Alferes
Área total (km ²)	1,4	2,8	4,1	3,9	319
Área residencial (km ²)	1,4	1,5	2,5	2,2	-
Número de domicílios	17000	11819	61000	7778	6813
Densidade (dom./km ²)	12142	8117	24797	3487	21
Beta (β)	3,9	3,9	3,9	3,9	3,0
Disposição dos nós	grade	grade	grade 3D	grade	aleatória

Figura 50: Tabela comparativa utilizada pela referência [Campista et al, 2006] para definição dos cenários propostos para simulação.

Fonte: Artigo conforme referência [Campista et al, 2006]

Utilizou-se o modelo de propagação de perda de percurso, que possui um parâmetro β definido de acordo com o ambiente de propagação de cada cenário. O objetivo deste artigo foi analisar o canal de interatividade ad-hoc sem fio IEEE 802.11, de acordo com os cenários geográficos brasileiros. A capacidade do canal

de retorno foi avaliada através de simulações que tiveram como objetivos determinar a influência do número de saltos na vazão da rede e o ponto de saturação da rede.

Para redes densas, o protocolo OLSR mostrou uma melhor vazão se comparado ao AODV. Em contrapartida, em redes esparsas, o protocolo AODV mostrou-se mais adequado do que o OLSR.

Em [Broch, 1998], os protocolos de roteamento ad-hoc AODV, DSDV, DSR e TORA foram simulados no software NS-2. O modelo de tráfego utilizado é baseado em fluxos CBR com algumas opções variadas em cada simulação: 1, 4 e 8 pacotes por segundo; 10, 20 e 30 fontes CBR e tamanhos de pacote de 64 e 1024 bytes. Os nós são mantidos em movimento com variação de 1 a 20 m/s (com uma média de 10 m/s). As métricas utilizadas foram:

- Taxa de entrega de pacotes: é a taxa entre o número de pacotes originados pelas fontes CBR no nível de aplicação e o número de pacotes recebidos pelo nó destino;
- Overhead de roteamento: é o número total de pacotes de roteamento transmitidos durante a simulação;
- Caminho ótimo: é a diferença entre o número de saltos que um pacote leva para chegar ao seu destino e o comprimento do menor caminho que fisicamente existiria através da rede quando o pacote foi originado.

Na métrica taxa de entrega de pacotes, o DSR e o AODV apresentaram resultado independente da carga de tráfego, com taxa de entrega de pacotes variando entre 95% e 100% em todos os casos. O DSDV falha para convergir com pequenos valores de *pause time* (pequenos valores de *pause time* significam alta velocidade de mobilidade e maiores valores de *pause time* significam menores velocidades de mobilidade) - menores que 300 segundos e maiores valores de mobilidade, assim, o mesmo apresentou resultado pobre com descarte de 70% dos pacotes. Porém com *pause times* maiores que 300 segundos, a entrega de pacotes aumentou para 92%. O TORA apresentou bons resultados com 10 e 20 fontes CBR, com taxa de entrega de pacotes entre 90% e 95%. Com 30 fontes, entretanto, a taxa média de entrega de pacotes cai para 40%, e variações extremas entre as taxas de entrega de pacotes de 8% a 91%.

Na métrica overhead de roteamento, o DSR e o AODV, protocolos sob demanda, tiveram formato de curva similar, entretanto, os valores absolutos foram bem diferentes com o AODV precisando de 5 vezes mais pacotes de overhead do

que o DSR. O overhead do TORA é o resultado do mecanismo de descobrimento de vizinhos do IMEP, que necessita que cada nó envie pelo menos um pacote *Hello* por período de um segundo (*beacon period*), assim, basta multiplicar o tempo de simulação pela quantidade de nós para saber qual a quantidade mínima de pacotes de overhead a simulação de deve apresentar. O DSDV apresentou um overhead constante, independente da carga de tráfego e da velocidade da mobilidade.

Na métrica caminho ótimo, tanto o DSDV quanto o DSR utilizaram rotas muito próximas das ótimas. Já o TORA e o AODV apresentaram um caminho maior com 4 ou mais saltos em relação ao caminho ótimo. É válido destacar que o TORA não foi implementado para otimizar o caminho. A Figura 51 mostra um dos gráficos disponibilizados na referência [Broch, 1998].

O gráfico da Figura 51 representa quantos pacotes foram entregues utilizando-se a melhor rota (eixo x sendo igual a 0) em cada protocolo avaliado, ou seja, a quantidade y de pacotes foi entregue ao destino com uma rota distante zero saltos da rota ótima.

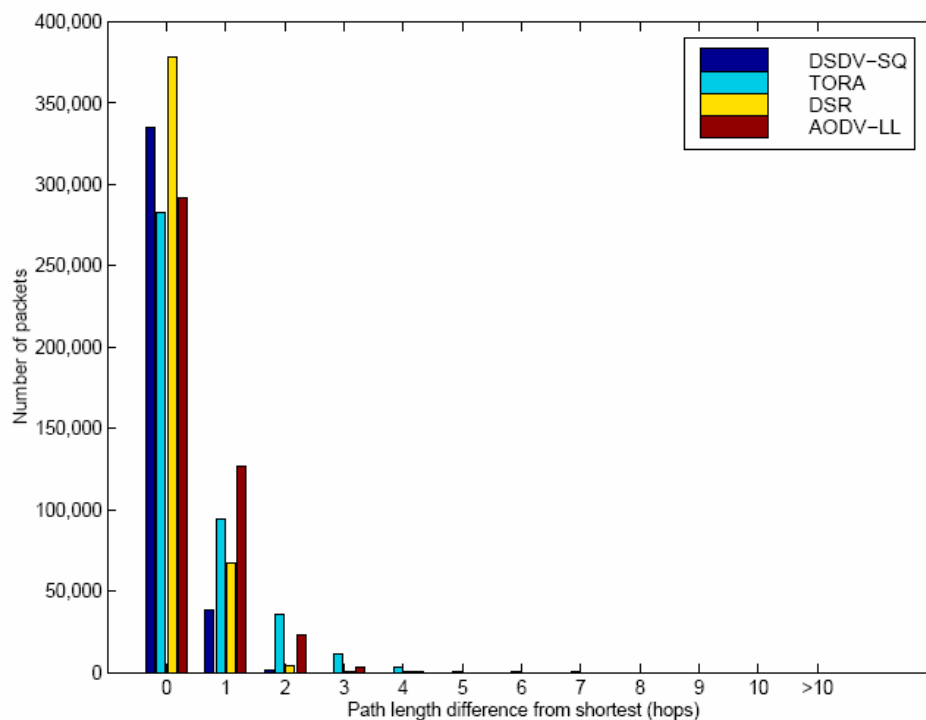


Figura 51: Tabela comparativa utilizada pela referência [Broch, 1998] para 20 fontes CBR, identificando a quantidade de pacotes entregues ao destino que utilizaram a rota de melhor caminho ou precisaram de mais saltos do que a rota de melhor caminho.

Fonte: Artigo conforme referência [Broch, 1998].

Em [Silva e Oliveira, 2005], os protocolos de roteamento ad-hoc unicast AODV, DSR, LAR1, Bellman Ford e WRP foram simulados nos softwares GloMoSim e BonnMotion. O objetivo desse trabalho foi avaliar os protocolos já citados em diferentes modelos de mobilidade. Foram alocados 40 nós com mobilidade habilitada em um *grid* de 200 X 200 metros e o tempo de simulação foi de 600 segundos. O modelo de tráfego utilizado foi baseado em fluxos CBR executados a partir de 3 segundos da simulação iniciada e com taxa de 4Kbps por nó. A velocidade era variada de 5 a 10 m/s. As métricas utilizadas foram:

- Razão entre o número de pacotes de controle (overhead) sobre o número de pacotes recebidos;
- Vazão;
- Número de saltos;
- Mudança do estado do enlace.

Dentre os protocolos avaliados, o WRP e o AODV apresentaram pior desempenho com as maiores taxas de pacotes de controle, independente do modelo de mobilidade utilizado.

Para a métrica de vazão, os protocolos pró-ativos apresentaram melhor desempenho, com o DSR apresentando a pior vazão dentre os protocolos avaliados. As curvas não variaram muito quando se muda o modelo de mobilidade utilizado.

No caso da métrica de número de saltos, o AODV novamente apresentou o pior desempenho, independente do modelo de mobilidade.

Em [Peiyan e Layuan, 2006] foram simulados os protocolos de roteamento AODV, TORA, DSDV e DSR no NS-2. O cenário abordado variou a quantidade de nós (10, 20, 40, 50 e 100 nós) espalhados randomicamente em uma área de 1000m X 1000m, com taxa nominal de 2Mbps. Os nós se mantiveram em velocidade entre 0m/s e 40m/s e *pause time* igual a 0s, que significa que os nós estiveram sempre em movimento durante todo o tempo de simulação. O tempo de simulação foi de 300 segundos e as métricas utilizadas para a análise dos protocolos foram: atraso médio fim-a-fim, *jitter*, vazão, taxa de perda de pacotes e o overhead. Foi utilizado um gerador de tráfego CBR, o qual originou 6, 12, 24, 30 ou 60 pares de fluxos UDP pela rede. Os pacotes CBR foram gerados com tamanho de 512 bytes e a cada 1 segundo um pacote era enviado.

Os resultados encontrados foram analisados e a partir disso foi elaborado um ranking dos protocolos mostrados na Figura 52, onde “4” significa o pior desempenho e “1” o melhor, para os cenários avaliados.

Protocols Metrics	A O D V	DSR	TORA	D S D V
Delay	2	4	3	1
Jitter	1	4	3	2
Loss ratio	1	3	4	2
Throughput	1	3	4	2
Routing load	3	2	1	4
Scalability	3	2	1	4
Connectivity	1	2	4	3
Supporting Multicast	Y E S	N O	N O *	N O

Figura 52: Ranking elaborado a partir dos resultados encontrados conforme referência [Peiyan e Layuan, 2006].

Fonte: Artigo conforme referência [Peiyan e Layuan, 2006].

A grande maioria dos trabalhos relacionados pesquisados insere a variável mobilidade nas simulações realizadas inviabilizando uma real comparação dos resultados encontrados, além das próprias diferenças entre os cenários abordados. A referência [Campista et al, 2006] não inclui mobilidade no cenário analisado. Assim, a referência [Campista et al, 2006] é a mais indicada a auxiliar as interpretações dos resultados gerados nesta dissertação.

Entretanto o maior objetivo das simulações geradas pelo artigo citado foi avaliar o impacto do número de saltos sobre a vazão de um único nó. Assim, os resultados aqui apresentados são relevantes, pois suas análises podem complementar trabalhos já elaborados que não contemplam determinados aspectos (como falta de mobilidade, comparação entre fluxos CBR e TCP, comparação do comportamento da rede resultado de múltiplos fluxos de tráfego gerados simultaneamente), conforme parâmetros escolhidos (banda, topologia, modelo de energia), dos protocolos de roteamento abordados (DSDV, DSR, AODV e OLSR).

5. PROPOSTA E AVALIAÇÃO DE SOLUÇÃO PARA CANAL DE RETORNO

5.1. PROPOSTA PARA COMPARAÇÃO DE PROTOCOLOS DE ROTEAMENTO AD-HOC

As redes ad-hoc podem ser utilizadas para prover o meio do canal de retorno da TV digital, desta forma, faz-se necessário avaliar os protocolos de roteamento ad-hoc disponíveis para então determinar o protocolo que melhor se adapta ao cenário estipulado.

Neste trabalho avaliamos quatro protocolos de roteamento ad-hoc: DSDV, OLSR, DSR e AODV. O motivo dessa escolha deve-se ao fato de que estes quatro protocolos são os mais comumente utilizados e os protocolos mais citados na literatura. As diferenças básicas entre estes quatro protocolos são explanadas na Tabela 4.

Tabela 4: Características dos protocolos de roteamento: DSDV, DSR, AODV e OLSR.

Protocolo de Roteamento	Aquisição de Rota	Flooding para Descobrimto de Rota	Atraso para Descobrimto de Rota	Falhas em Rotas
DSDV	Pró-ativo, mantém tabela de todas as rotas possíveis	Não	Não	As rotas são atualizadas constantemente através de toda a rede
DSR	Sob demanda, apenas quando necessário	Sim, agressivo. Usa o cache para armazenar informações de rotas e reduzir overhead	Sim	Um pacote de Route Error é propagado para a fonte apagando o caminho inválido
AODV	Sob demanda, apenas quando necessário	Sim, conservativo. Usa o cache para armazenar informações de rotas e reduzir overhead	Sim	Um pacote Route Error é enviado em broadcast para apagar o caminho inválido
OLSR	Pró-ativo	Não	Não	O estado de enlace é verificado pelos pacotes Hello

5.2. CENÁRIOS CONSIDERADOS

Visando a inclusão digital da população de baixa renda, alguns cenários importantes precisam ser considerados, dentre estes, pode-se citar comunidades urbanas carentes, meios rurais e aldeias indígenas. Neste trabalho, o cenário escolhido foi uma comunidade urbana carente da cidade do Rio de Janeiro, chamada Maré.

Localizada junto à Baía de Guanabara, à Av. Brasil e às principais vias de acesso à cidade, a Maré ocupa uma presença significativa no estado do Rio de Janeiro. A Maré possui em sua maior parte relevo plano.

Foi, durante muito tempo, dominada por palafitas – habitações precárias suspensas sobre a lama e a água – em visível contraste com as modernas arquiteturas do Aeroporto Internacional e da Cidade Universitária da UFRJ (Universidade Federal do Rio de Janeiro). Este fato contribuiu para uma visão generalizada da região como um espaço miserável, violento e sem condições dignas de vida.

Quanto aos itens básicos de infra-estrutura, como luz, água e esgoto, a Maré conquistou importantes avanços nos últimos 20 anos. Mas o mesmo não ocorreu no campo econômico e cultural. Como exemplo, até o início dos anos 90 só 0,6% da população local tinha diploma de graduação, enquanto o número de analfabetos beirava os 20%. Já quando o assunto é geração de renda, mais de 2/3 dos trabalhadores da Maré afirmam que ganham menos de dois salários mínimos por mês.

Suas 16 comunidades estão distribuídas em pouco mais de 800 mil m² e formam o chamado Complexo da Maré. Esta comunidade carente tem, segundo o Censo 2000, 132 mil habitantes, divididos em sub-regiões. Possui 16 escolas, sendo uma de ensino médio. A Figura 53 exibe uma vista aérea da região.

O IBGE define favela, como o fez ainda no último censo, como: “Aglomerado subnormal (favelas e similares) é um conjunto constituído de no mínimo 51 unidades habitacionais, ocupando ou tendo ocupado até período recente, terreno de propriedade alheia (pública ou particular) dispostas, em geral, de forma desordenada e densa, bem como carentes, em sua maioria, de serviços públicos essenciais.” Apesar do Complexo da Maré ser caracterizado como uma favela, este termo é

evitado para minimizar a questão da discriminação com os moradores da comunidade geralmente denominados “favelados”.



Figura 53: Vista aérea atual da Comunidade da Maré.

Fonte: Censo Maré 2000.

O bairro Maré tem a maior concentração de população de baixa renda do município do Rio de Janeiro e do Brasil. O conjunto de 16 comunidades totaliza, segundo o Censo Maré – 2.000 [Ceasm, 2000], uma população de 132.176 pessoas, abrigada em 38.273 domicílios⁴. Tomadas no interior de uma mesma unidade territorial, as comunidades que compõem o bairro da Maré possuem, na sua dimensão populacional absoluta, uma expressão significativa em relação ao conjunto da população da região metropolitana e do próprio estado do Rio de Janeiro.

A população do bairro da Maré representa 2,26% da população do município do Rio de Janeiro e apenas 0.97 % dos habitantes do estado do Rio de Janeiro. Contudo, demarcando uma outra escala geográfica para a análise, a exemplo da

⁴ A Maré é constituída por 16 comunidades. O Censo Maré, a fim de melhor descrever a heterogeneidade local, considerou a comunidade de Mandacaru, localizada no território de Marcílio Dias, como uma comunidade específica, devido às suas condições peculiares.

escala municipal, observa-se um destaque indiscutível dessa população no território fluminense.

Tabela 5: População em Municípios do Estado do Rio de Janeiro.

Municípios	População	Municípios	População
Rio de Janeiro	5.851.944	Itaboraí	187.127
Nova Iguaçu	915.366	Nova Friburgo	173.321
São Gonçalo	889.828	Barra Mansa	170.593
Duque de Caxias	770.865	Nilópolis	153.572
Niterói	458.465	Teresópolis	138.019
São João de Meriti	449.229	Macaé	131.550
Belford Roxo	433.120	Cabo Frio	126.894
Campos de Goytacases	406.511	Queimados	121.688
Petrópolis	286.348	Angra dos Reis	119.180
Volta Redonda	242.046	Resende	104.482
Magé	205.699	Barra do Piraí	88.475

Fonte: Censo IBGE 2000 [Ceasm, 2000].

A Tabela 5 apresenta os 22 municípios mais populosos da malha municipal do estado do Rio de Janeiro, hoje composta por 91 unidades administrativas. Um olhar superficial verifica que o bairro da Maré possui um número de habitantes superior aos identificados para Macaé, Cabo Frio, Queimados, Angra dos Reis, Resende e Barra do Piraí. E, numa classificação por ordem de grandeza, se o bairro da Maré recebesse o status de município, ocuparia a 17^a posição em termos populacionais nesse estado.

A Tabela 6 identifica as principais comunidades carentes do Município do Rio de Janeiro.

Tabela 6: População nas principais comunidades carentes do Município do Rio de Janeiro.

Localidade	1991	1996	2000
Rocinha	42.892	45.585	56.313
Alemão	51.591	54.795	65.637
Jacarezinho	37.393	34.919	36.428
Maré	62.458	68.817	113.817 / 132.176*

Fonte: Censo IBGE – 2000; *Censo CEASM-2000

O recorte definido pelo IBGE ignorou a condição formal de bairro da Maré, estabelecida desde o final da década de 80, sendo as comunidades locais reconhecidas como unidades territoriais específicas. Tal opção metodológica, além de descaracterizar o bairro do ponto de vista sócio-geográfico, gerou um registro

limitado da população residente na Maré para os anos de 1991 e 1996. Caso fosse mantido no Censo de 2000 do Instituto o mesmo recorte territorial, considerando-se apenas as nove comunidades supracitadas, seria identificada uma população residente de apenas 77.292 pessoas, de acordo com as informações colhidas pelo Censo CEASM – 2000. Isto significaria a exclusão de 54.884 moradores na contagem da população local.

O Centro de Estudos e Ações Solidárias da Maré – CEASM – é uma associação civil, sem fins lucrativos, criada em 15 de agosto de 1997. Os projetos desenvolvidos pelo CEASM visam superar as condições de pobreza e exclusão existentes na Maré, apontado como o terceiro bairro de pior IDH (Índice de Desenvolvimento Humano) da cidade.

A materialização de um censo profundo e abrangente na Maré, Censo Maré 2000, foi obra de diversos parceiros. A iniciativa começou com o CEASM que buscava viabilizar o empreendimento desde 1998. O Banco Nacional de Desenvolvimento Econômico e Social – BNDES e a Prefeitura do Rio também consideraram que uma iniciativa como essa poderia, além de fornecer informações inéditas sobre as comunidades populares, servir de referência para a produção de diagnósticos mais precisos a respeito dos investimentos que se propõem a realizar.

O cenário proposto neste trabalho considera que o acesso à Internet à população da Maré é viabilizado, inicialmente, para algumas escolas, centros comunitários, hospitais e postos de saúde. Por isso, nas simulações realizadas, a topologia possui 20 nós que representam tais centros comunitários e escolas.

Algumas considerações a respeito do cenário de rede foram adotadas. Uma delas é a ausência de movimentação dos nós, já que a infra-estrutura de redes mesh é instalada em pontos fixos na comunidade. Outra característica é o uso de um acesso principal à comunidade, onde se considera a presença de um nó que faz a interligação da rede mesh com a rede cabeada tradicional.

Na Figura 54 é mostrada a topologia do *backbone* sem fio utilizada nas simulações, onde cada nó é representado por um número. O posicionamento de cada nó na topologia foi gerado de forma aleatória, porém uma vez definidas as posições de cada nó, não mais foram alteradas em todas as simulações e para todos os protocolos.

Os nós da topologia representam roteadores sem fio, disponibilizados em lugares variados, com a intenção de cobrir todos os centros comunitários, escolas,

hospitais e postos de saúde da comunidade. O alcance considerado para cada nó é de 250m.

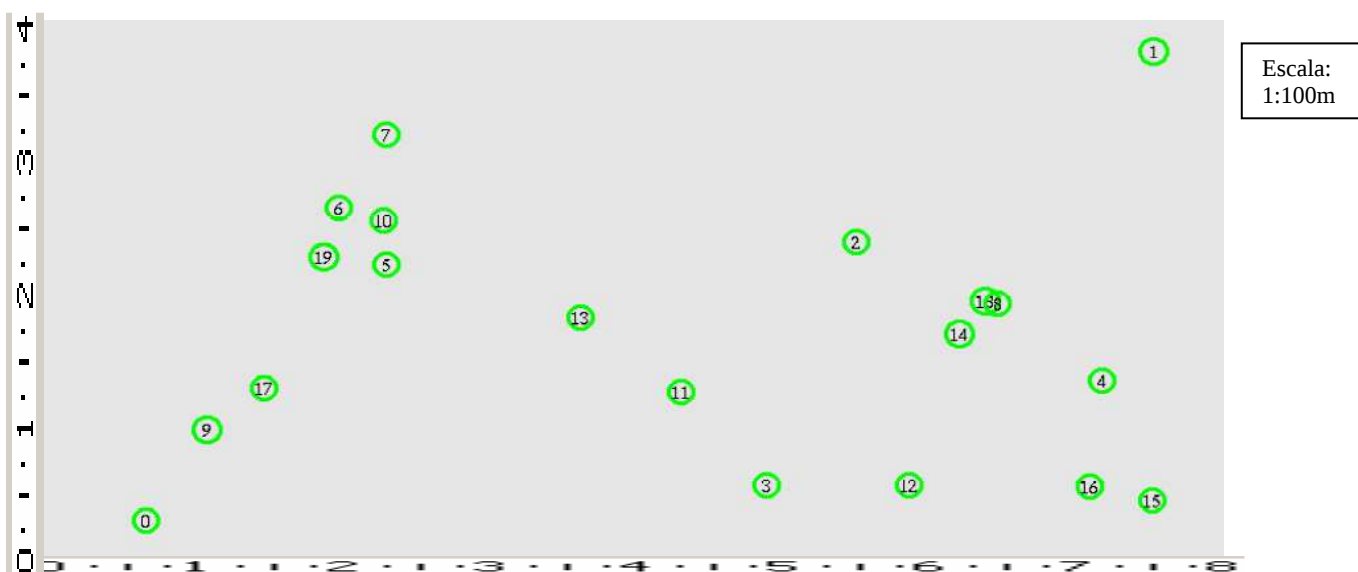


Figura 54: Topologia de rede mesh utilizada - backbone.

Fonte: Simulação realizada no NS-2, capturada do software gráfico.

Outra questão importante para a definição do canal de retorno em um sistema de TV digital é o grau de interatividade. Conforme [Becker e Montez, 2004], existem sete níveis de interatividade, porém revisamos tais níveis de interatividade específicos para o foco em televisão digital:

Nível 0: Estágio em que a televisão expõe imagens e dispõe de alguns canais. A ação do espectador resume-se a ligar e desligar o aparelho, regular o volume, brilho ou contraste e trocar de um canal para outro (com ou sem controle remoto).

Nível 1: A facilidade de gravação de programas é inserida de alguma forma à televisão, através de periféricos ou acoplada ao próprio aparelho de televisão.

Nível 2: Algum grau de interatividade de características digitais, o telespectador pode então interferir no conteúdo a partir de telefones, por fax ou por correio eletrônico.

Nível 3: Estágio da chamada televisão interativa em que se pode participar do conteúdo em tempo real, escolhendo ângulos de câmeras, diferentes encaminhamentos das informações etc. Apesar disso, o telespectador ainda não possui controle total sobre a programação. O mesmo apenas reage a impulsos e caminhos pré-definidos pelo transmissor. Ainda não sendo considerado, portanto, uma televisão interativa e sim reativa.

Nível 4: A possibilidade de interatividade é maior com gravação dos conteúdos por programa e não por tempo definido; congelar a tela e reiniciar a partir de um programa sendo executado ao vivo; acesso à Internet via set-top box, porém com páginas desenvolvidas em linguagem específica para acesso via televisão. Para este nível de interatividade é necessário um canal de retorno ligando o telespectador à emissora, chamado de canal de interação, porém sem grandes necessidades de largura de banda. Um acesso equivalente ao de uma linha discada (33,6 Kbps) é suficiente.

Nível 5: O telespectador pode ter uma presença mais efetiva no conteúdo, saindo da restrição de apenas escolher as opções definidas pelo transmissor. Passa a existir a opção de participar da programação enviando vídeo de baixa qualidade, que pode ser originado por intermédio de uma *webcam* ou filmadora analógica. Para isso, torna-se necessário um canal de retorno com largura de banda maior, como por exemplo, um acesso banda larga de 128 Kbps.

Nível 6: A largura de banda do canal de retorno aumenta mais, oferecendo a possibilidade de envio de vídeo de alta qualidade, semelhante ao transmitido pela emissora. Desta forma, a interatividade chega a um nível muito superior a simples reatividade, como caracterizado no nível 3.

Nível 7: Neste nível, a interatividade plena é atingida. O telespectador passa a se confundir com o transmissor, podendo gerar conteúdo. Esse nível é semelhante ao que acontece na Internet hoje, onde qualquer usuário pode publicar um site, bastando ter as ferramentas pertinentes. O telespectador pode produzir programas e enviá-los à emissora, rompendo o monopólio da produção e veiculação das tradicionais redes de televisão, que conhecemos hoje.

Este trabalho considera que um canal de retorno para prover pelo menos o nível 5 de interatividade é adequado, pois permite o acesso banda larga, facilitando a inclusão digital dos telespectadores.

Para avaliar a qualidade do acesso através do canal de retorno implementado com o uso de redes mesh, alguns pontos mais críticos devem ser levados em consideração, como segue:

1. Banda: a banda é compartilhada em uma rede local sem fio, por isso deve-se garantir uma vazão mínima, para que a banda estreita não interfira na reprodução dos dados da aplicação e principalmente que o efeito de banda limitada não seja sentido pelo “consumidor”;

2. Atraso: deve-se garantir que o atraso máximo não prejudique a transmissão. No caso de redes mesh, mensurar o atraso máximo inserido pela necessidade de descoberta das rotas do algoritmo de roteamento é um requisito;
3. Taxa de perdas: médias contínuas permitem alguma perda de pacotes, entretanto, mesmo considerando o envio de fluxos de voz e vídeo no nível de interatividade 5, uma taxa de perda muito alta prejudica a transmissão;
4. Overhead do protocolo de roteamento ad-hoc: como a banda é limitada em redes sem fio, minimizar a porcentagem de banda gasta com transmissão de pacotes de controle dos protocolos de roteamento também é um requisito desejável.

Em contrapartida, outros aspectos, importantes para outros cenários que utilizam redes ad-hoc sem fio, não precisam ser considerados no cenário em questão, como:

1. Energia: os roteadores são ligados diretamente na rede de energia elétrica.
2. Mobilidade: os roteadores são instalados em posições fixas, portanto não há mobilidade dos dispositivos.

5.3. SIMULAÇÕES REALIZADAS

As simulações foram realizadas com 20 nós conforme apresentado na Figura 54, onde cada nó é representado por um número e participa do roteamento da rede. Os 20 nós foram aleatoriamente distribuídos pelo *grid* uma vez, após isso, esta distribuição foi mantida em todas as simulações realizadas.

O nó receptor de todos os fluxos foi definido como sendo o nó 1, simulando este nó como a porta (*gateway*) para redes externas, como a Internet. O modelo de tráfego escolhido simula fluxos TCP e CBR (*Constant Bit-Rate*). Os fluxos TCP representam, por exemplo, uma simulação de transferência de dados na *web* e os fluxos CBR representam uma simulação de transmissão de voz ou vídeo. Desta forma, objetivou-se reproduzir aplicações reais comuns utilizadas simultaneamente

nos dias de hoje. Em todas as simulações foram mantidos 4 fluxos TCP e variadas as quantidades de fluxos CBR. Desta forma, a estes 4 fluxos TCP foram somados os seguintes fluxos CBR: nenhum fluxo CBR, 1 fluxo CBR, 2 fluxos CBR, 5 fluxos CBR, 10 fluxos CBR, 20 fluxos CBR e 40 fluxos CBR; totalizando assim 7 simulações para cada protocolo. Desta maneira, pode-se determinar parâmetros de rede com fluxos sendo incrementados até que uma saturação de banda seja conseguida.

Cada fluxo TCP utilizou-se de pacotes de tamanho 1500 bytes, tentando representar um tamanho de pacote geralmente utilizado na Internet. Cada fluxo CBR (UDP) utilizou-se de pacotes de tamanho 160 bytes, com intervalo de 20 milissegundos com uma taxa de 64Kbps. Esta taxa é a utilizada para transmissões de voz com CODEC's baseados na forma do sinal, como o padrão de telefonia G.711, simulando a maior taxa (pior caso) usada para aplicações de voz sobre IP (VoIP). Um fluxo CBR de 64 Kbps também pode representar transmissão de vídeo, por exemplo, com a utilização de CODEC's H.261 ou H.263. Os enlaces sem fio operam à taxa nominal de 2Mbps conforme o padrão IEEE 802.11.

As fontes de tráfego foram alteradas a cada simulação, conforme se segue.

1. Determinação dos nós fonte (de origem) de tráfegos de forma arbitrária

a) Nenhum Fluxo CBR e 4 Fluxos TCP

Os nós que foram determinados a originar os fluxos TCP: 0, 7, 3 e 15.

Nenhum fluxo CBR foi originado.

b) 1 Fluxo CBR e 4 Fluxos TCP

Os nós que foram determinados a originar os fluxos TCP: 0, 7, 3 e 15.

O nó que foi determinado a originar o fluxo CBR: 0.

c) 2 Fluxos CBR e 4 Fluxos TCP

Os nós que foram determinados a originar os fluxos TCP: 0, 7, 3 e 15.

Os nós que foram determinados a originar os fluxos CBR: 0 e 19.

d) 5 Fluxos CBR e 4 Fluxos TCP

Os nós que foram determinados a originar os fluxos TCP: 0, 7, 3 e 15.

Os nós que foram determinados a originar os fluxos CBR: 0, 19, 18, 17 e 16.

e) 10 Fluxos CBR e 4 Fluxos TCP

Os nós que foram determinados a originar os fluxos TCP: 0, 7, 3 e 15.

Os nós que foram determinados a originar os fluxos CBR: 0, 19, 18, 17,16, 15, 14, 13, 12 e 11.

f) 20 Fluxos CBR e 4 Fluxos TCP

Os nós que foram determinados a originar os fluxos TCP: 0, 7, 3 e 15.

Os nós que foram determinados a originar os fluxos CBR: 0 (dois fluxos sendo originados), 19, 18, 17,16, 15, 14, 13, 12,11, 10, 9, 8, 7, 6, 5, 4, 3 e 2.

g) 40 Fluxos CBR e 4 Fluxos TCP

Os nós que foram determinados a originar os fluxos TCP: 0, 7, 3 e 15.

Os nós que foram determinados a originar os fluxos CBR: 0 (três fluxos sendo originados), 19 (três fluxos sendo originados), 18 (dois fluxos sendo originados), 17 (dois fluxos sendo originados), 16 (dois fluxos sendo originados), 15 (dois fluxos sendo originados), 14 (dois fluxos sendo originados), 13 (dois fluxos sendo originados), 12 (dois fluxos sendo originados), 11 (dois fluxos sendo originados), 10 (dois fluxos sendo originados), 9 (dois fluxos sendo originados), 8 (dois fluxos sendo originados), 7 (dois fluxos sendo originados), 6 (dois fluxos sendo originados), 5 (dois fluxos sendo originados), 4 (dois fluxos sendo originados), 3 (dois fluxos sendo originados) e 2 (dois fluxos sendo originados).

2. Determinação do nó destino de tráfegos

Como dito anteriormente, o nó 1 foi estabelecido como o *gateway* entre a rede mesh e a rede cabeada, sendo o destino de todos os fluxos originados.

O tempo de cada simulação, realizada para cada protocolo de roteamento, foi de 300 segundos, porém os primeiros 60 segundos foram descartados com o objetivo de minimizar os erros por questão de convergência ou de demoras para o início do envio dos pacotes como acontece com a implementação de alguns protocolos. O tamanho do *grid* utilizado foi de 800 X 400 metros, totalizando 320000 metros quadrados, sendo mais que suficiente para cobrir toda a extensão do cenário proposto.

Para cada simulação as seguintes métricas foram calculadas: percentual de perda de pacotes, vazão média, atraso médio e overhead de controle do protocolo de roteamento.

5.4. RESULTADOS OBTIDOS

5.4.1. Perda

Esta métrica foi calculada com base nos pacotes que saíram de seus nós fonte (os nós fontes foram alterados conforme o acréscimo de fluxos CBR em cada simulação) e chegaram ao nó receptor 1. Desta forma, é calculado o percentual de perda de pacotes conforme a fórmula:

$$\% \text{ perda} = \frac{Q_p}{Q_e} * 100\% \quad [\%]$$

Onde:

Q_p é a quantidade de pacotes perdidos

Q_e é a quantidade total de pacotes enviados

Para o cálculo da perda foram considerados apenas os pacotes do nível de aplicação do trace do NS-2.

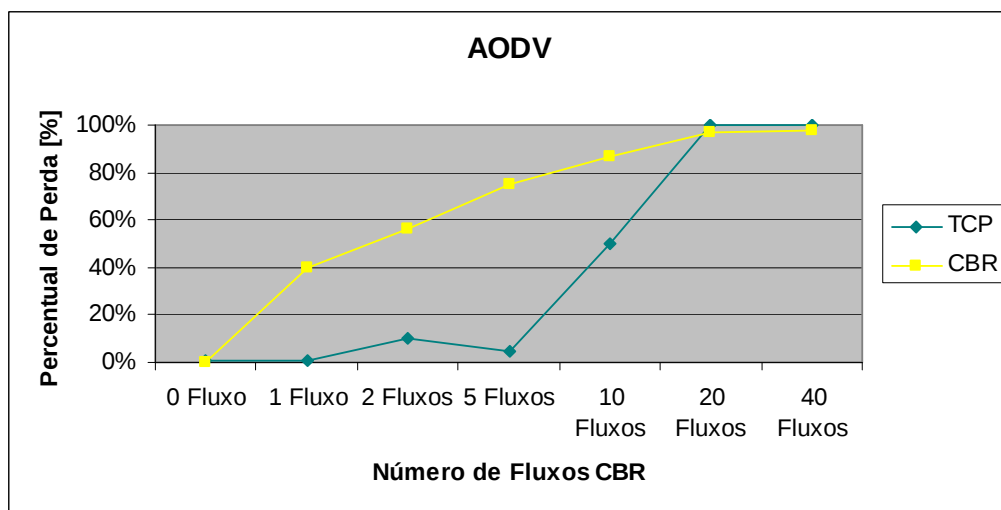


Figura 55: Gráfico referente a perda do protocolo AODV.

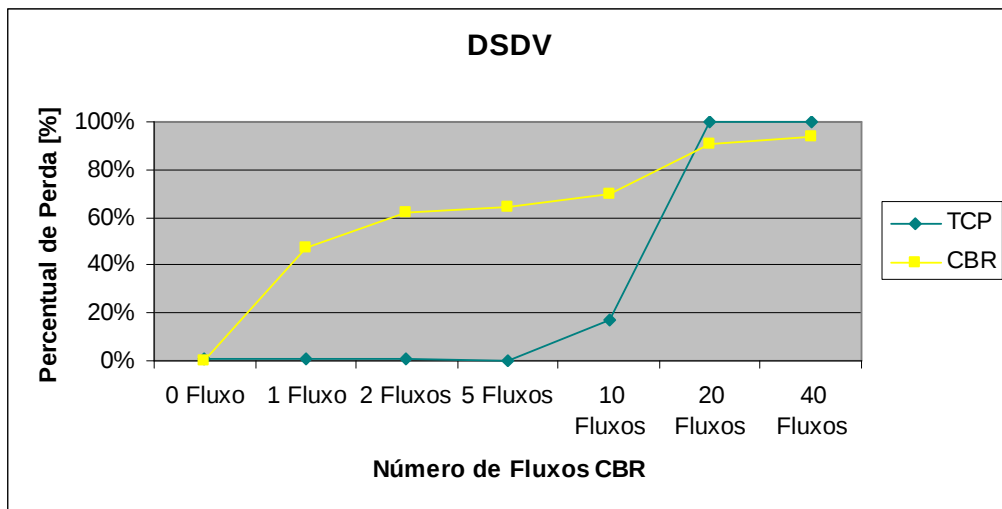


Figura 56: Gráfico referente a perda do protocolo DSDV.

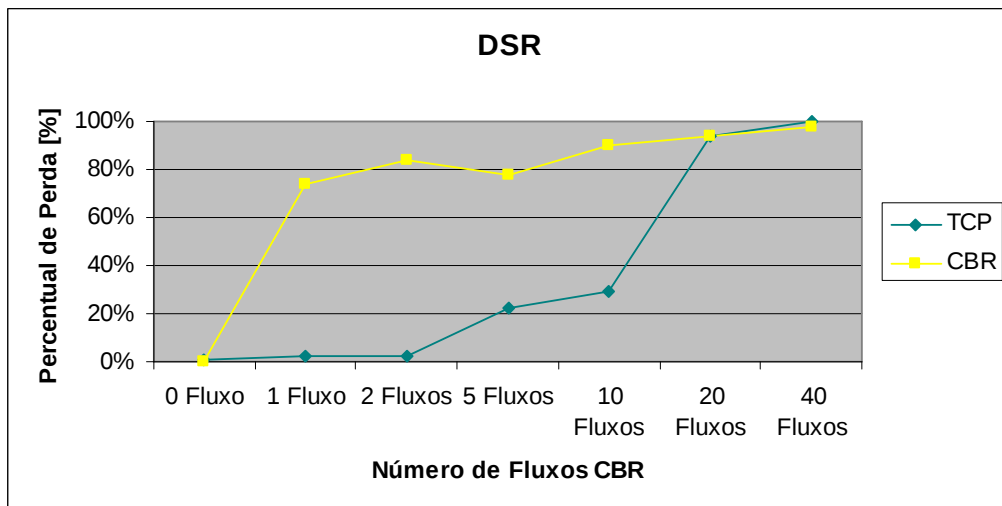


Figura 57: Gráfico referente a perda do protocolo DSR.

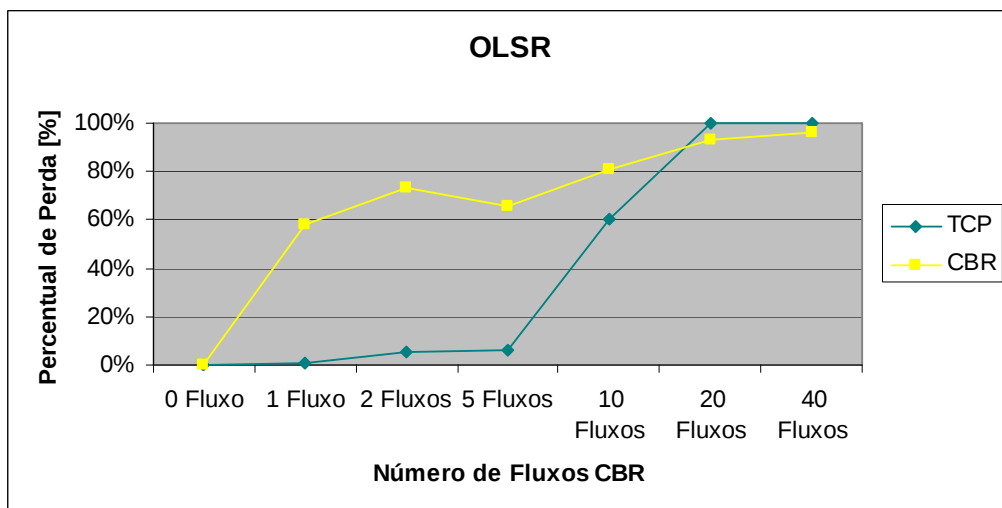


Figura 58: Gráfico referente a Perda do protocolo OLSR.

As Figuras 55, 56, 57 e 58 apresentam os resultados das simulações realizadas em relação à métrica perda de pacotes, dos protocolos AODV, DSDV, DSR e OLSR, respectivamente.

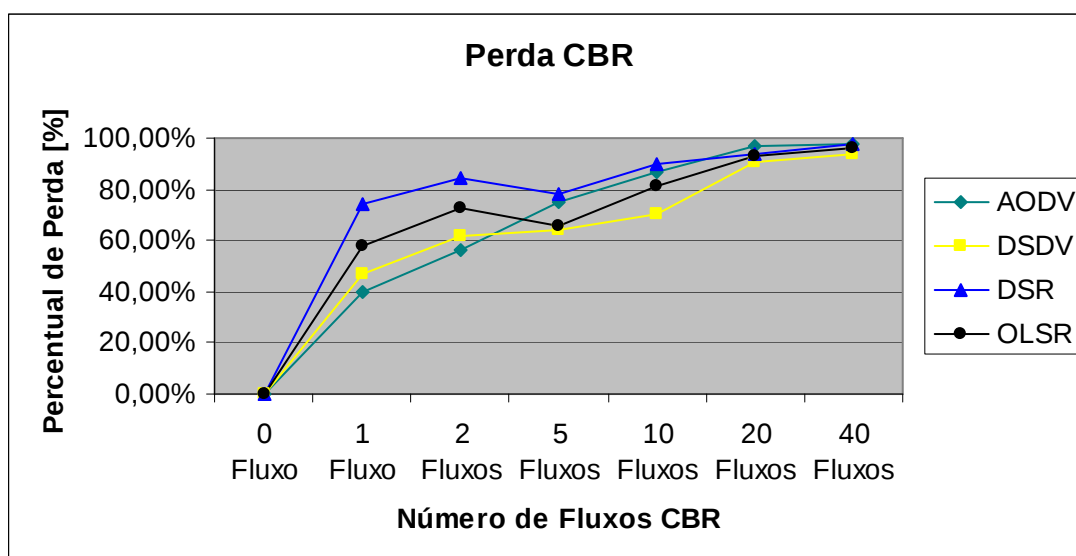


Figura 59: Gráfico comparativo referente a Perda CBR de todos os protocolos avaliados: AODV, DSR, DSDV e OLSR.

A Figura 59 apresenta os resultados das simulações realizadas em relação à métrica perda de pacotes dos fluxos CBR, dos protocolos AODV, DSDV, DSR e OLSR, de forma consolidada para facilitar as análises. O protocolo DSDV apresentou melhor desempenho neste item de avaliação. O motivo principal é devido à falta de quebra de enlaces, pois muitas rotas conseguiram ser mantidas ao longo de toda simulação. Se o cenário tivesse maior grau de mobilidade ou ainda com alguns nós alterando seu estado de ativo para inativo, o resultado esperado seria bem pior ao apresentado. Vale ressaltar que nos cenários apresentados a rede chegou a seu limite em relação a sua capacidade de tratar a quantidade de fluxos que foram gerados, ou seja, com 4 fluxos TCP acrescidos de 40 fluxos CBR a rede chegou à saturação, o que explica o grande percentual de perda apresentado.

A partir de 20 fluxos fica evidente a saturação da rede. A principal razão para esta saturação é o fato da existência de apenas um nó *gateway* para a Internet. Desta forma, uma solução para este problema seria a inserção de mais alguns nós *gateway*, localizados estrategicamente e dividindo carga do tráfego.

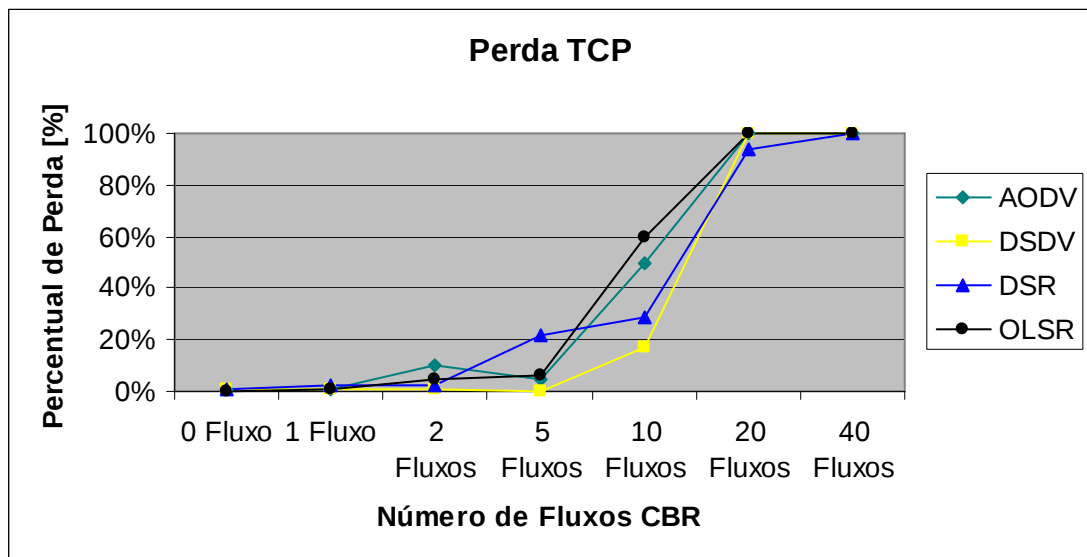


Figura 60: Gráfico comparativo referente a Perda TCP de todos os protocolos avaliados: AODV, DSR, DSDV e OLSR.

A Figura 60 apresenta os resultados das simulações realizadas em relação à métrica perda de pacotes dos fluxos TCP, dos protocolos AODV, DSDV, DSR e OLSR, de forma consolidada para facilitar as análises. O protocolo DSDV apresentou melhor desempenho novamente, onde até com 5 fluxos CBR a perda se aproximou a zero e em 10 fluxos se manteve bem abaixo do resultado dos outros protocolos com perda inferior a 20%.

5.4.2. Vazão

Esta métrica foi calculada a partir da média da vazão dos pacotes recebidos pelos nós de destino, conforme a fórmula:

$$Vazão = \frac{Q_r * T * 8}{T_s * 1000 * 1000} \text{ [Mbps]}$$

Onde:

Q_r é a quantidade de pacotes recebidos pelo nó destino

T é o tamanho dos pacotes em bytes

T_s é o tempo de simulação

Para o cálculo da vazão foram considerados apenas os pacotes do nível de aplicação do trace do NS-2.

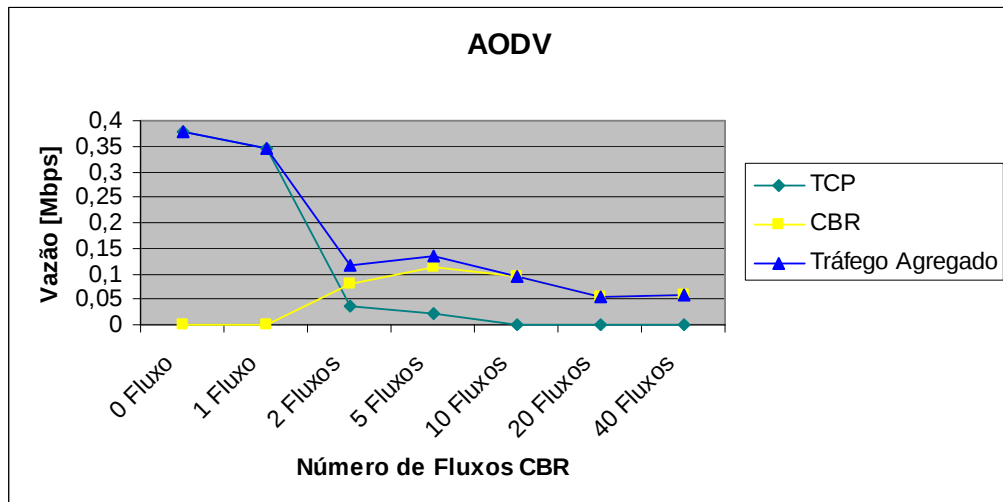


Figura 61: Gráfico referente a vazão do protocolo AODV.

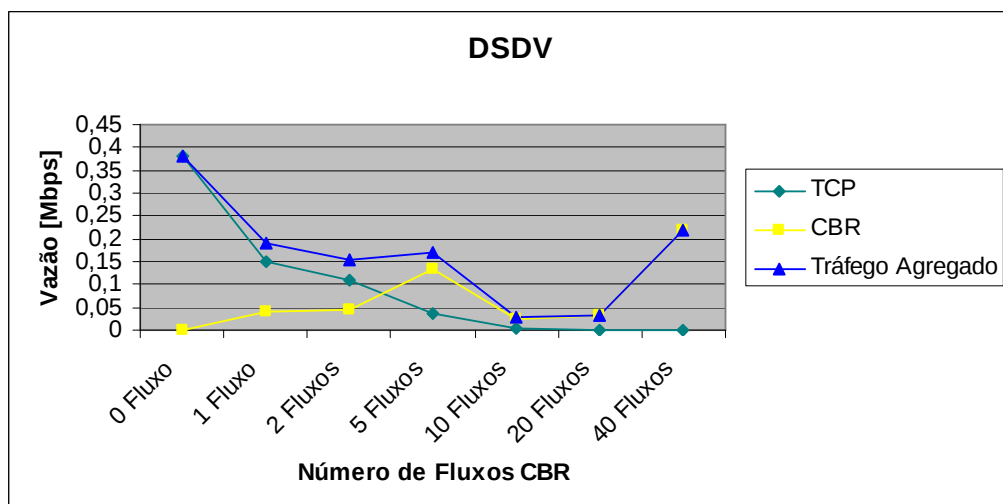


Figura 62: Gráfico referente a vazão do protocolo DSDV.

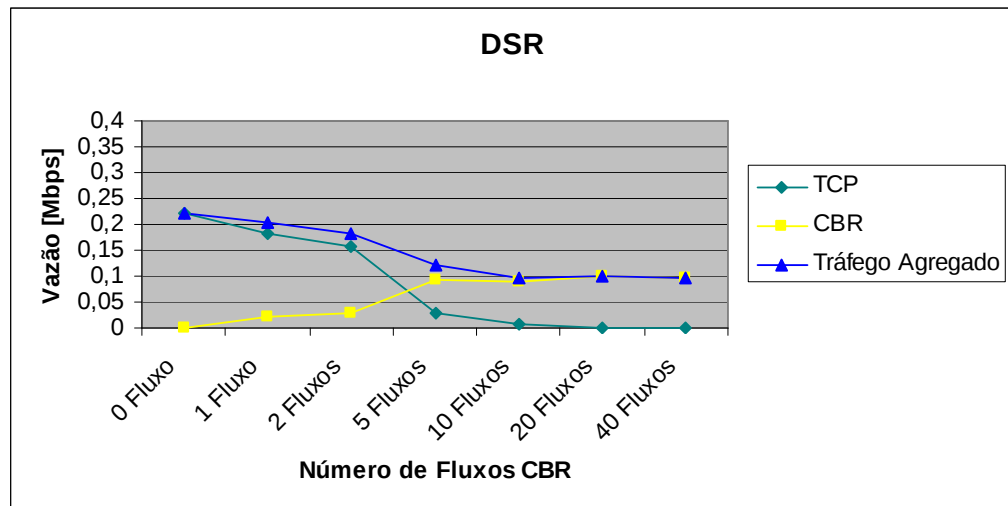


Figura 63: Gráfico referente a vazão do protocolo DSR.

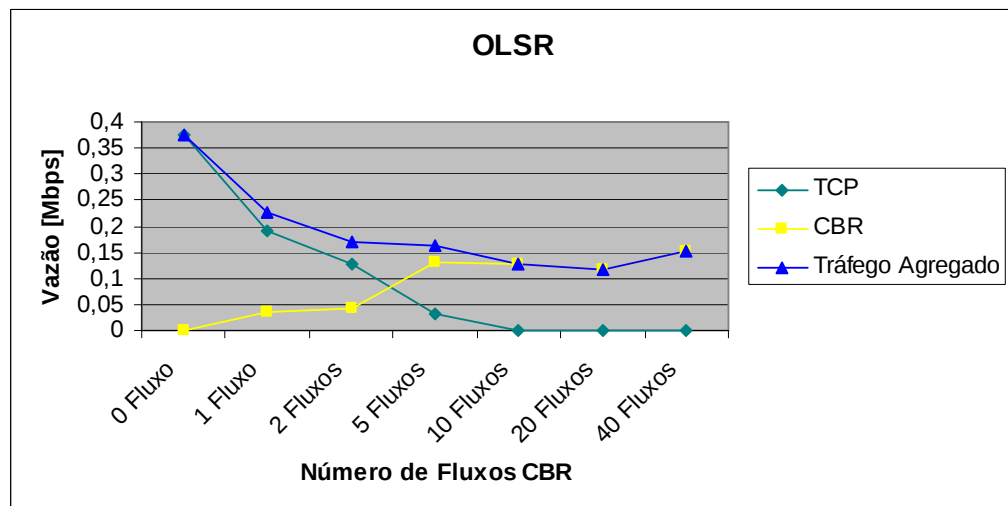


Figura 64: Gráfico referente a vazão do protocolo OLSR.

As Figuras 61, 62, 63 e 64 apresentam os resultados das simulações realizadas em relação à métrica vazão, dos protocolos AODV, DSDV, DSR e OLSR, respectivamente.

Os valores resultado da vazão estão em conformidade com [Villela, 2004], no qual a vazão máxima não chega ao valor máximo nominal da taxa devido a problemas de interferência, terminal escondido ou exposto, questões comuns em casos de canal compartilhado em redes em fio.

Devido ao fato do TCP ter mecanismo de controle de congestionamento, sempre que o volume de carga dos tráfegos CBR é aumentado, existe um ponto de saturação em que a vazão do tráfego TCP tende a zero. Desta forma, caso no cenário proposto seja importante a coexistência de ambos os tipos de tráfego,

recomenda-se utilizar algum mecanismo que garanta banda para os fluxos TCP, como os mecanismos de escalonamento utilizados quando se oferece qualidade de serviço.

Todos os protocolos tiveram o momento de saturação do tráfego TCP próximo a 10 fluxos CBR, porém os protocolos DSDV, DSR e OLSR tiveram o momento de em que a vazão do tráfego CBR ultrapassou o tráfego TCP próximo a 5 fluxos CBR, em contrapartida, no protocolo AODV este momento se deu próximo a 2 fluxos CBR.

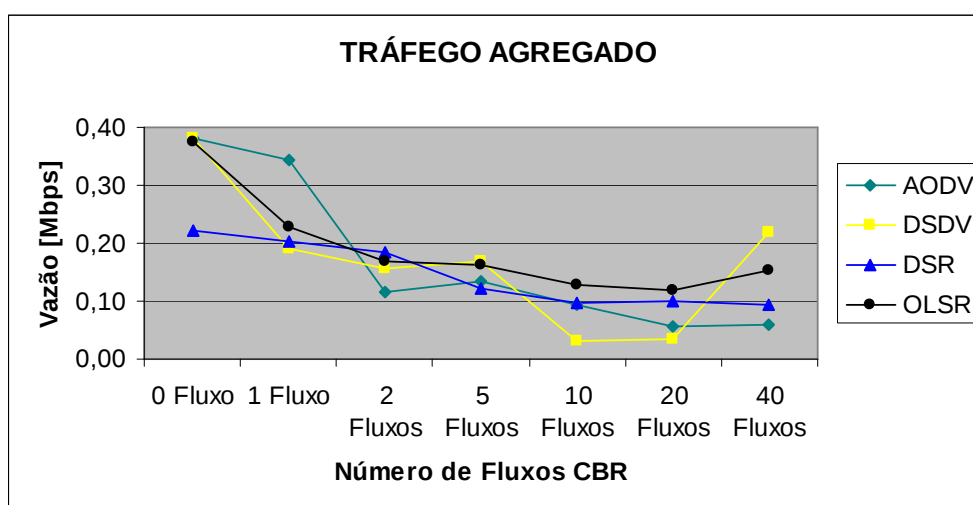


Figura 65: Gráfico referente a vazão agregada .

A Figura 65 mostra a comparação do desempenho dos protocolos em relação ao tráfego agregado. Todos os protocolos tiveram um desempenho muito similar, porém, o protocolo que demonstrou resultado ligeiramente melhor foi o OLSR, sempre se mantendo com o melhor ou o segundo melhor desempenho com qualquer das variações de fluxos CBR. Além disso, não é possível determinar um ranking dos outros protocolos com relação à vazão agregada, pois seus resultados foram muito próximos e a cada mudança da quantidade dos fluxos CBR, ocorreu muita variação da ordem de desempenho entre os protocolos DSR, AODV e DSDV.

5.4.3. Atraso

Esta métrica foi calculada a partir do atraso médio de todos os pacotes enviados e trafegados através da rede, conforme a fórmula:

$$\text{Atraso} = Tr - Ts \text{ [segundos]}$$

Onde:

Tr é o tempo em que o pacote foi recebido

Ts é o tempo em que o pacote foi enviado

Para o cálculo do atraso foram considerados apenas os pacotes do nível de aplicação do trace do NS-2.

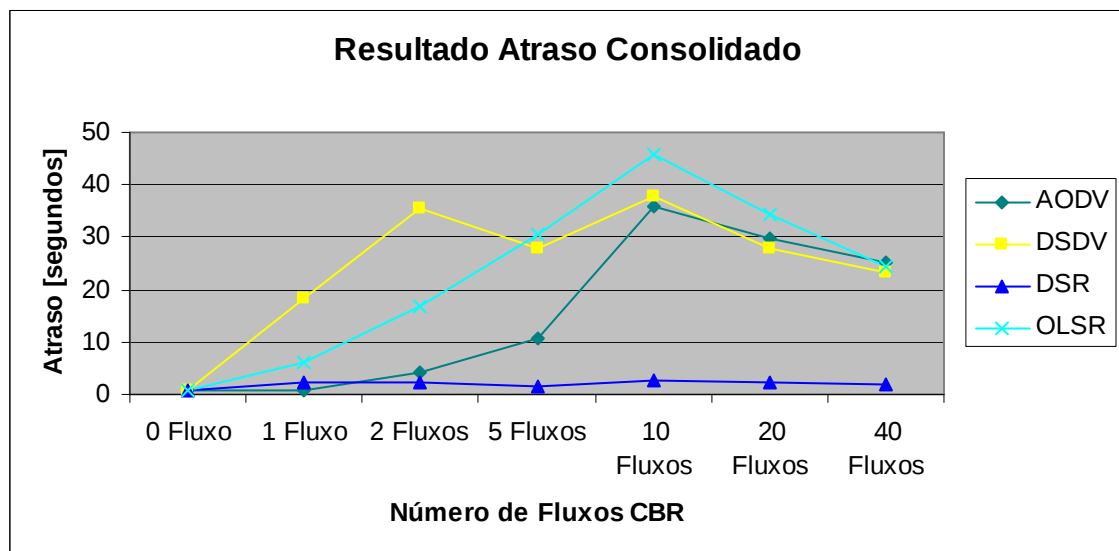


Figura 66: Gráfico consolidado referente ao atraso dos protocolos: AODV, DSDV, DSR e OLSR.

A Figura 66 apresenta os resultados das simulações realizadas em relação à métrica atraso, comparando os protocolos AODV, DSDV, DSR e OLSR.

O protocolo que apresentou melhor desempenho foi o DSR, o qual se manteve como atraso quase constante independentemente da quantidade de fluxos inseridos. Os protocolos AODV, DSDV e OLSR tiveram um desempenho bem similar, o qual se mostrou saturado após 10 fluxos CBR. Assim, verifica-se que são protocolos em que se deve manter o tamanho da rede bem controlado para se evitar uma quantidade significativa de fluxos trafegando através da rede.

Tabela 7: Quadro comparativo do percentual de perda, maior e menor atraso identificados em cada protocolo de roteamento.

Protocolo / Fluxos CBR	Perda (%)	Maior Atraso (s)	Menor Atraso (s)
olsr / 40 fluxos CBR	95,937	191,367	5,447
olsr / 20 fluxos CBR	93,708	216,859	6,611
olsr / 10 fluxos CBR	86,351	158,091	8,437
olsr / 5 fluxos CBR	71,883	149,062	0,044
olsr / 2 fluxos CBR	71,799	61,127	0,012
olsr / 1 fluxo CBR	48,907	30,253	0,028
olsr / 0 fluxo CBR	0,358	1,431	0,030
aodv / 40 fluxos CBR	98,433	164,632	9,318
aodv / 20 fluxos CBR	97,066	168,022	0,060
aodv / 10 fluxos CBR	90,056	162,736	0,020
aodv / 5 fluxos CBR	75,493	36,832	0,007
aodv / 2 fluxos CBR	56,878	14,496	0,028
aodv / 1 fluxo CBR	70,021	2,699	0,028
aodv / 0 fluxo CBR	0,787	17,258	0,036
dsr / 40 fluxos CBR	97,149	76,497	0,059
dsr / 20 fluxos CBR	93,948	44,318	0,003
dsr / 10 fluxos CBR	89,290	22,918	0,014
dsr / 5 fluxos CBR	77,338	16,521	0,006
dsr / 2 fluxos CBR	76,353	50,378	0,028
dsr / 1 fluxo CBR	60,416	19,489	0,028
dsr / 0 fluxo CBR	0,779	10,722	0,028
dsdv / 40 fluxos CBR	94,215	121,036	4,912
dsdv / 20 fluxos CBR	95,277	79,908	8,005
dsdv / 10 fluxos CBR	92,455	83,210	3,578
dsdv / 5 fluxos CBR	70,802	146,526	0,982
dsdv / 2 fluxos CBR	70,514	85,960	0,028
dsdv / 1 fluxo CBR	47,612	85,596	0,028
dsdv / 0 fluxo CBR	0,421	0,972	0,028

A Tabela 7 apresenta os resultados das simulações realizadas em relação ao atraso (independente da aplicação UDP / TCP), além dos resultados de maior e menor tempo de atraso, dos protocolos OLSR, DSR, DSDV e AODV em cada cenário de quantidade fluxos CBR diferentes (0, 1, 2, 5, 10, 20 e 40 fluxos CBR), porém todos com 4 fluxos TCP. Esta tabela evidencia que a partir de que momento (quantidade de fluxos CBR originados no cenário) os protocolos em questão apresentaram um ou mais pacotes com dificuldade para chegar em seu destino, ou seja, mostra o pior e o melhor desempenho dos pacotes trafegados na rede.

Para uma melhor análise dos altos valores de atraso encontrados, foram estratificados os pacotes chamados de TOP 10, ou seja, os 10 pacotes que demoraram mais tempo trafegando na rede, evidenciados na Tabela 8. Esta tabela

permitiu entender que existem momentos em que a rede tem dificuldade de superar um congestionamento o que causa um atraso grande, o qual eleva a média do atraso para padrões não aceitáveis. Porém estes momentos são curtos, durando poucos segundos, e afetando o desempenho dos protocolos quando se tentou obter uma saturação da rede por meio de uma quantidade mais alta de fluxos CBR.

Tabela 8: Pacotes TOP 10 em atraso para os piores casos (atrasos superiores a 3 segundos).

dsdv / 40 fluxos CBR			
ID do pacote	Tempo de Envio	Tempo de Recebimento	Atraso
147504	63,943	184,979	121,036
147339	63,880	184,861	120,981
147299	63,865	184,811	120,946
145332	63,118	183,979	120,861
146899	63,712	184,567	120,855
148979	64,505	185,337	120,832
149019	64,520	185,340	120,820
144891	62,950	183,763	120,813
148899	64,474	185,283	120,809
145492	63,179	183,982	120,803
dsdv / 20 fluxos CBR			
ID do pacote	Tempo de Envio	Tempo de Recebimento	Atraso
75387	62,586	142,494	79,908
75429	62,616	142,519	79,903
77191	63,957	143,841	79,884
77211	63,972	143,844	79,872
83452	68,727	148,555	79,828
75125	62,388	142,215	79,827
77151	63,927	143,746	79,820
75267	62,494	142,292	79,798
83412	68,696	148,484	79,788
75347	62,555	142,339	79,784
dsdv / 10 fluxos CBR			
ID do pacote	Tempo de Envio	Tempo de Recebimento	Atraso
40403	65,227	148,437	83,210
40423	65,257	148,461	83,204
40443	65,288	148,480	83,193
40323	65,105	148,213	83,108
40313	65,090	148,196	83,107
40333	65,120	148,216	83,096
40343	65,135	148,222	83,087
40353	65,150	148,225	83,075
40393	65,211	148,272	83,061
40383	65,196	148,254	83,058
dsdv / 5 fluxos CBR			
ID do pacote	Tempo de Envio	Tempo de Recebimento	Atraso
49134	147,502	294,028	146,526
50357	151,129	296,796	145,667

48344	145,170	288,399	143,229
47864	143,754	286,519	142,765
48154	144,622	287,335	142,713
48223	144,821	286,808	141,987
48518	145,674	287,627	141,953
46667	140,219	280,957	140,738
52925	158,793	294,832	136,039
52914	158,763	294,144	135,381
dsdv / 2 fluxos CBR			
ID do pacote	Tempo de Envio	Tempo de Recebimento	Atraso
29335	188,265	274,225	85,960
29321	188,158	273,539	85,381
29315	188,112	273,473	85,361
29313	188,097	273,455	85,357
29311	188,082	273,436	85,354
29317	188,128	273,480	85,352
29319	188,143	273,489	85,346
29309	188,067	273,405	85,338
30424	196,051	280,897	84,846
30418	196,006	280,024	84,018
dsdv / 1 fluxo CBR			
ID do pacote	Tempo de Envio	Tempo de Recebimento	Atraso
17459	189,118	274,714	85,596
17718	192,135	277,428	85,293
17659	191,434	276,715	85,281
17658	191,419	276,685	85,266
17706	191,968	277,173	85,206
17708	191,983	277,176	85,193
17715	192,090	277,254	85,165
17705	191,952	277,115	85,163
17657	191,404	276,535	85,131
17704	191,937	277,061	85,124
dsdv / 0 fluxo CBR			
ID do pacote	Tempo de Envio	Tempo de Recebimento	Atraso
10107	171,464	172,437	0,972
10106	171,462	172,422	0,960
10103	171,443	172,390	0,947
10075	171,016	171,960	0,945
8637	148,205	149,146	0,941
15182	252,272	253,203	0,932
4492	82,587	83,517	0,931
16776	277,581	278,508	0,926
14817	246,450	247,371	0,921
4513	82,951	83,859	0,908
olsr / 40 fluxos CBR			
ID do pacote	Tempo de Envio	Tempo de Recebimento	Atraso
159133	68,075	259,443	191,367
157683	67,527	257,721	190,194
147499	63,671	248,241	184,570
145323	62,849	238,601	175,753
307372	124,203	299,205	175,002
145291	62,835	236,700	173,865

145282	62,833	236,495	173,662
145201	62,803	236,283	173,480
145161	62,788	236,264	173,477
144685	62,607	235,992	173,386
olsr / 20 fluxos CBR			
ID do pacote	Tempo de Envio	Tempo de Recebimento	Atraso
80213	65,626	282,484	216,859
79791	65,306	275,119	209,814
79668	65,214	273,289	208,075
107996	86,499	283,984	197,485
116864	93,158	284,409	191,251
115774	92,334	272,671	180,336
121628	96,744	274,113	177,370
149161	117,448	287,649	170,201
157721	123,883	293,445	169,562
149059	117,371	286,740	169,368
olsr / 10 fluxos CBR			
ID do pacote	Tempo de Envio	Tempo de Recebimento	Atraso
70086	108,172	266,264	158,091
81651	125,280	281,321	156,041
81734	125,402	281,373	155,971
81814	125,524	281,414	155,891
81281	124,731	280,474	155,743
82158	126,042	281,568	155,526
69542	107,350	262,381	155,031
71349	110,037	264,955	154,918
71193	109,809	264,724	154,916
71339	110,022	264,745	154,723
olsr / 5 fluxos CBR			
ID do pacote	Tempo de Envio	Tempo de Recebimento	Atraso
51194	148,431	297,494	149,062
51126	148,249	292,143	143,895
51077	148,111	291,994	143,882
51033	147,990	291,820	143,831
51027	147,974	291,712	143,738
50968	147,807	291,482	143,676
50863	147,503	291,162	143,659
51022	147,959	291,604	143,645
50927	147,686	291,281	143,596
26212	77,408	217,335	139,927
olsr / 2 fluxos CBR			
ID do pacote	Tempo de Envio	Tempo de Recebimento	Atraso
16470	98,924	160,050	61,127
16472	98,939	160,056	61,117
16474	98,954	160,060	61,105
16476	98,970	160,069	61,099
16468	98,909	159,965	61,057
16466	98,893	159,867	60,974
16464	98,878	159,837	60,959
16462	98,863	159,809	60,946
16460	98,848	159,754	60,906
16458	98,832	159,693	60,860

olsr / 1 fluxos CBR			
ID do pacote	Tempo de Envio	Tempo de Recebimento	Atraso
22091	199,008	229,260	30,253
22090	198,992	229,237	30,244
22093	199,023	229,266	30,243
22052	198,703	228,889	30,186
22054	198,718	228,895	30,177
22080	198,931	229,092	30,161
22079	198,916	229,071	30,155
22049	198,688	228,837	30,149
22082	198,947	229,095	30,149
22059	198,779	228,925	30,146
olsr / 0 fluxo CBR			
ID do pacote	Tempo de Envio	Tempo de Recebimento	Atraso
16218	214,823	216,253	1,431
16239	215,124	216,519	1,395
16240	215,154	216,535	1,381
16217	214,806	216,139	1,332
16155	214,190	215,498	1,307
16232	215,012	216,319	1,306
16163	214,275	215,576	1,301
16153	214,178	215,477	1,299
16171	214,332	215,626	1,293
16237	215,075	216,368	1,293
aadv / 40 fluxos CBR			
ID do pacote	Tempo de Envio	Tempo de Recebimento	Atraso
305041	124,037	288,669	164,632
320148	129,793	288,462	158,669
303601	123,489	281,220	157,731
231624	96,070	247,166	151,097
264216	108,487	259,366	150,880
286656	117,035	266,106	149,071
282576	115,481	264,323	148,842
361458	145,530	273,889	128,358
384259	154,216	281,104	126,888
431259	172,121	298,836	126,715
aadv / 20 fluxos CBR			
ID do pacote	Tempo de Envio	Tempo de Recebimento	Atraso
107901	87,510	255,531	168,022
107881	87,494	255,467	167,973
105841	85,940	251,466	165,526
87301	71,814	233,813	161,999
75241	62,626	221,060	158,435
75141	62,550	220,644	158,095
124005	99,776	257,708	157,932
75061	62,489	219,316	156,827
74741	62,245	217,630	155,385
72801	60,767	215,574	154,807
aadv / 10 fluxos CBR			
ID do pacote	Tempo de Envio	Tempo de Recebimento	Atraso
83084	130,443	293,179	162,736

51761	82,725	238,541	155,816
51391	82,161	237,600	155,439
51571	82,435	237,799	155,364
51561	82,420	237,704	155,284
48450	77,681	232,553	154,872
48320	77,483	231,766	154,283
48240	77,361	231,274	153,913
39243	63,667	217,380	153,713
49730	79,631	233,031	153,399
aodv / 5 fluxos CBR			
ID do pacote	Tempo de Envio	Tempo de Recebimento	Atraso
65851	200,191	237,024	36,832
65846	200,176	236,990	36,813
65836	200,146	236,854	36,708
65841	200,161	236,867	36,706
65831	200,130	236,312	36,181
65826	200,115	236,270	36,154
65821	200,100	236,247	36,147
65816	200,085	236,136	36,052
65811	200,070	236,043	35,974
65796	200,024	235,987	35,964
aodv / 2 fluxos CBR			
ID do pacote	Tempo de Envio	Tempo de Recebimento	Atraso
18305	134,134	148,630	14,496
18381	134,713	149,208	14,495
18307	134,150	148,643	14,493
18383	134,729	149,220	14,492
18309	134,165	148,655	14,490
18301	134,104	148,588	14,485
18389	134,774	149,256	14,482
18299	134,089	148,570	14,481
18297	134,073	148,554	14,481
18385	134,744	149,223	14,479
aodv / 1 fluxo CBR			
ID do pacote	Tempo de Envio	Tempo de Recebimento	Atraso
27291	229,712	232,412	2,699
15953	134,459	137,058	2,599
27874	234,634	237,212	2,578
15952	134,444	136,511	2,067
15951	134,429	136,459	2,030
18655	157,173	159,173	2,000
15688	132,298	134,222	1,925
16040	135,018	136,896	1,878
16032	134,941	136,783	1,842
16038	135,002	136,799	1,798
aodv / 0 fluxo CBR			
ID do pacote	Tempo de Envio	Tempo de Recebimento	Atraso
10735	183,476	200,734	17,258
11592	197,435	200,585	3,150
9891	169,743	172,094	2,351
13601	230,675	232,809	2,134
13816	234,242	236,125	1,883

13792	233,917	235,799	1,882
13790	233,842	235,720	1,878
13794	233,954	235,829	1,875
13815	234,240	236,045	1,805
13801	234,057	235,845	1,788
dsr / 40 fluxos CBR			
ID do pacote	Tempo de Envio	Tempo de Recebimento	Atraso
393807	154,588	231,085	76,497
525188	203,871	248,186	44,314
525348	203,932	248,192	44,259
524862	203,750	247,948	44,198
543259	210,654	252,864	42,209
547548	212,283	253,763	41,481
548079	212,483	253,827	41,345
550645	213,458	254,085	40,627
183594	75,117	114,855	39,738
278568	110,999	147,549	36,550
dsr / 20 fluxos CBR			
ID do pacote	Tempo de Envio	Tempo de Recebimento	Atraso
193789	147,664	191,981	44,318
322059	244,508	285,785	41,278
321579	244,142	284,615	40,474
182780	139,471	179,668	40,196
326113	247,555	286,000	38,445
80388	62,900	99,861	36,961
111933	86,626	123,569	36,944
253814	192,951	228,835	35,884
334098	253,553	287,115	33,561
193926	147,765	180,619	32,854
dsr / 10 fluxos CBR			
ID do pacote	Tempo de Envio	Tempo de Recebimento	Atraso
192545	273,079	295,997	22,918
50554	70,580	92,697	22,117
50542	70,565	92,536	21,971
133255	188,702	209,076	20,374
49490	69,087	88,705	19,618
50283	70,184	89,788	19,604
189121	268,111	287,656	19,544
190410	269,940	289,462	19,522
52479	73,414	92,825	19,411
58301	81,445	100,816	19,371
dsr / 5 fluxos CBR			
ID do pacote	Tempo de Envio	Tempo de Recebimento	Atraso
92988	229,647	246,167	16,521
93254	230,165	246,190	16,025
93737	231,525	245,930	14,406
94206	232,637	245,826	13,189
29412	66,619	79,538	12,919
41853	97,537	109,675	12,138
41847	97,522	109,659	12,137
41846	97,521	109,631	12,110
92774	229,007	241,022	12,016

92769	228,991	240,950	11,958
dsr / 2 fluxos CBR			
ID do pacote	Tempo de Envio	Tempo de Recebimento	Atraso
25044	67,070	117,449	50,378
68666	180,626	195,228	14,603
100423	280,943	295,458	14,515
70008	185,811	199,428	13,616
70010	185,827	199,431	13,604
82375	221,327	234,683	13,356
100869	282,451	295,591	13,140
29554	83,686	96,733	13,048
29485	83,503	96,209	12,706
101051	283,137	295,578	12,441
dsr / 1 fluxo CBR			
ID do pacote	Tempo de Envio	Tempo de Recebimento	Atraso
33535	109,667	129,156	19,489
33545	109,728	129,012	19,284
33543	109,712	128,636	18,924
33540	109,697	128,603	18,906
30764	98,924	117,609	18,685
33538	109,682	128,320	18,639
34357	114,375	132,966	18,591
30888	99,244	117,586	18,343
52816	179,244	197,582	18,338
31033	99,579	117,716	18,137
dsr / 0 fluxo CBR			
ID do pacote	Tempo de Envio	Tempo de Recebimento	Atraso
43018	105,977	116,699	10,722
43016	105,977	116,207	10,230
43711	108,339	116,918	8,579
109953	221,862	226,807	4,945
110035	222,005	226,773	4,768
110143	222,227	226,846	4,619
107775	213,661	218,010	4,349
107786	213,751	218,096	4,345
54712	125,270	129,532	4,262
103364	201,752	205,970	4,218

Um fator importante para se analisar o motivo pelo qual os pacotes com alto atraso continuaram a trafegar pela rede, mesmo dezenas de segundos depois de serem enviados, foi o tamanho da fila do buffer dos roteadores escolhida ("set val(ifqlen) 1000 ;# max packet in ifq")⁵. Pois os pacotes poderiam ser descartados anteriormente, caso este parâmetro fosse menor, porém esta análise não poderia ser realizada, pois não ficaria tão explícito que os protocolos não possuem um mecanismo eficaz para controlar o atraso.

⁵ Linha extraída dos arquivos TCL elaborados para as simulações dos protocolos AODV, DSR, DSDV e OLSR.

Apesar das Tabelas 7 e 8 mostrarem o maior atraso sendo de 76s para um determinado pacote, a média do atraso do protocolo DSR mostrou-se baixa, isto porque a maioria dos pacotes trafegados na rede apresentou atraso pequeno.

5.4.4. Overhead

Esta métrica foi calculada a partir dos pacotes de controle que trafegaram pela rede, conforme a fórmula:

$$\%Overhead = \frac{\sum Bce}{\sum Bte} * 100\% \quad [\%]$$

Onde:

Bce é o número de bytes dos pacotes de controle enviados e

Bte é o número de bytes de todos os pacotes enviados.

É importante destacar que somente foram considerados os pacotes do nível de rede do *trace* do NS-2.

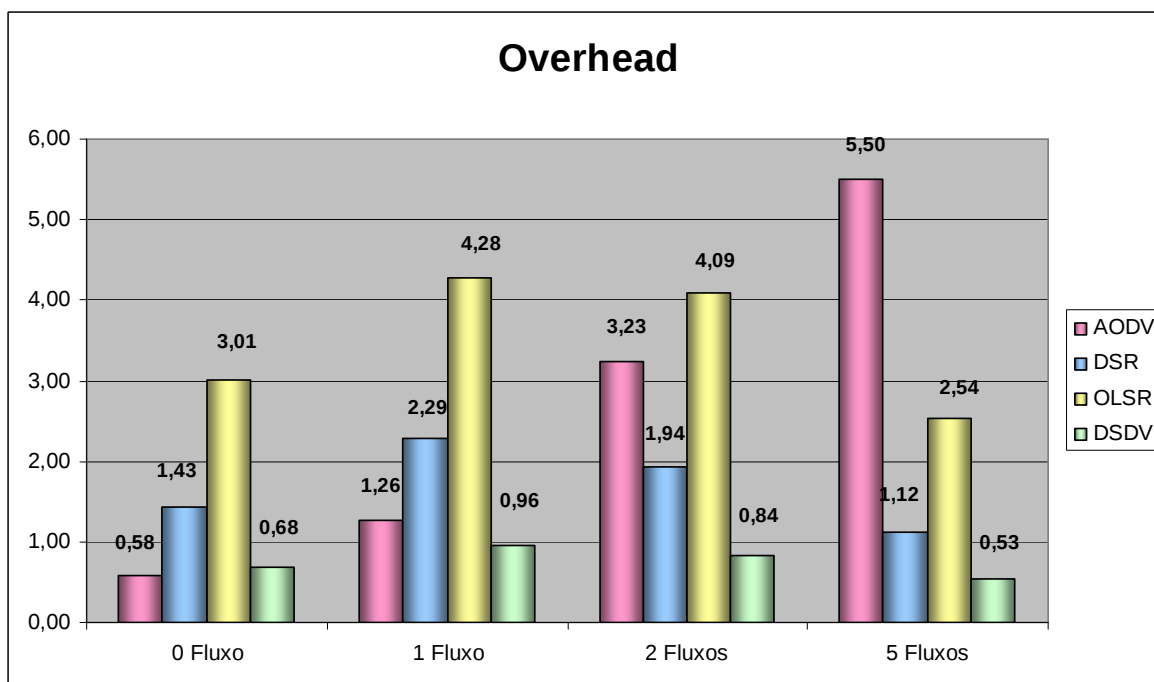


Figura 67: Gráfico referente ao overhead dos protocolos AODV, DSR, OLSR e DSDV.

A Figura 67 apresenta os resultados das simulações realizadas em relação à métrica overhead, dos protocolos AODV, DSDV, DSR e OLSR de forma consolidada. Para se analisar o resultado, optou-se por visualizar apenas os resultados com até 5 fluxos CBR, pois a partir de 10 fluxos, todos os protocolos tiveram o tráfego saturado, desta forma, a análise a partir de 10 fluxos CBR fica inconclusiva.

O bom desempenho do DSR é principalmente associado à utilização agressiva de *cache* e pelo fato de não ocorrerem quebras de rota devido aos nós serem estáticos.

O bom desempenho do DSDV pode ser atribuído ao fato que a frequência para envio dos pacotes de controle está baixa, próxima a 15 segundos, o que pode ser benéfico caso não existam muitas quebras de enlace. Entretanto isto pode causar um grande problema existindo quebras de rotas, pois o protocolo demoraria a descobrir rotas inválidas, causando aumento da taxa de perda de pacotes e atraso.

O AODV apresentou pior desempenho com uma taxa crescente de overhead conforme o aumento de fluxos CBR.

O OLSR apresentou resultado quase constante com o aumento de fluxos CBR. Os pacotes de Hello são enviados em períodos de 2 segundos, enquanto os pacotes TC têm período de envio de 5 segundos nas simulações realizadas. Desta forma, explica-se o motivo deste protocolo ter apresentado um desempenho muito inferior ao DSDV, pois este último apresenta frequência de 15 segundos para os pacotes de atualização. Para uma comparação mais justa, seria necessário, antes de tudo, especificar o tempo ideal para todos estes pacotes periódicos de controle através de simulações específicas.

Os baixos percentuais de overhead (máximo de 5,5% para o AODV) apresentados nestas simulações se devem ao fato de que ocorreram poucas quebras de enlace, resultando em menos inundação na rede de pacotes de controle. As poucas quebras de enlace foram devido à falta de mobilidade dos nós, além da ausência do modelo de energia, o qual faria com que os nós “desligassem” à medida que a energia do nó cessasse.

6. CONCLUSÕES

De acordo com os resultados das simulações, pode-se constatar que os protocolos de roteamento tiveram desempenho muito similar, porém apresentando destaques em cada métrica, conforme segue.

O protocolo DSDV apresentou melhor desempenho na métrica perda, enquanto que na comparação de desempenho da métrica vazão média, o protocolo que demonstrou melhor resultado foi o OLSR, sempre se mantendo com o melhor ou o segundo melhor desempenho com qualquer das variações de fluxos CBR. Em relação ao atraso, o protocolo que apresentou destaque foi DSR, o qual manteve desempenho similar em todos os cenários, mesmo com a inserção da quantidade máxima de fluxos CBR originados pelos nós. O protocolo DSDV obteve ótimo desempenho em relação à taxa de overhead. O AODV apresentou pior desempenho em relação ao overhead. O OLSR apresentou resultado quase constante com o aumento de fluxos CBR.

Um fator predominante para a escolha do melhor protocolo de roteamento ad-hoc, é o tipo de aplicação a ser utilizada no cenário proposto. Para a implementação do canal de retorno da TV digital interativa compartilhando banda com aplicações Internet, uma importante, senão a principal característica é a vazão conseguida, seguida pelo atraso e percentual de perda, com o overhead sendo uma questão para otimização da rede.

Para uma escolha de acordo com os critérios salientados, foram estipuladas notas para cada métrica de cada protocolo. Estas notas foram padronizadas conforme fator predominante para a aplicação a ser utilizada no cenário proposto. A Tabela 9 explicita as notas de acordo com o desempenho de cada protocolo em cada métrica avaliada.

Tabela 9: Atribuição de notas para os quatro protocolos de acordo com as métricas avaliadas.

Notas para estabelecimento do melhor protocolo	Protocolo com melhor desempenho	Protocolos com desempenho intermediário		Protocolo com pior desempenho
Vazão	50	25	25	10
Atraso	40	20	20	10
Perda	30	15	15	5
Overhead	20	10	10	5

Notas para estabelecimento do melhor protocolo	Protocolo com melhor desempenho	Protocolos com desempenho intermediário		Protocolo com pior desempenho
Vazão	OLSR	DSDV	DSR	AODV
Atraso	DSR	AODV	OLSR	DSDV
Perda	DSDV	OLSR	AODV	DSR
Overhead	DSDV	DSR	OLSR	AODV

Protocolo	Nota TOTAL
OLSR	95
DSDV	85
DSR	80
AODV	50

Analisando os resultados exibidos na Tabela 9, o protocolo mais indicado para o cenário em questão foi o OLSR. Mesmo apresentando o melhor desempenho, são sugeridas algumas alterações em parâmetros deste protocolo de forma a proporcionar menor overhead e controlar o atraso dos pacotes que apresentam altos valores (na ordem de dezenas de segundos).

Para as melhorias citadas, propõe-se ajustar o tamanho de fila do buffer dos roteadores para que o mecanismo de descarte de pacotes funcione mais adequadamente. Para tal, é necessário realizar simulações específicas com o cenário que se quer adotar, para então se determinar o melhor valor para este parâmetro.

Além disso, propõe-se também diminuir a quantidade de pacotes de controle da rede, utilizando para isso uma frequência menor para o envio dos pacotes de controle. Uma vez que a rede simulada nesta dissertação não possuía mobilidade, diminuindo assim a quantidade de quebras de enlaces, é menos fundamental a troca de pacotes de atualização / controle sendo enviados a todo instante.

6.1. CONTRIBUIÇÕES

Dentre as principais contribuições desta dissertação estão:

- a proposta e avaliação de uma forma alternativa para permitir o acesso à Internet para a população de baixa renda, focando a inclusão digital;
- a realização de um estudo sobre os principais protocolos de roteamento para redes ad-hoc;
- a modelagem de um cenário que representa comunidades carentes, usando a comunidade urbana carente da cidade do Rio de Janeiro, chamada Maré, como referência;
- a comparação do desempenho de protocolos de roteamento ad-hoc, considerando medidas de vazão, perda de pacotes, atraso e overhead, considerando o uso de aplicações multimídia, de voz e vídeo, co-existindo com aplicações de dados.

6.2. TRABALHOS FUTUROS

Como trabalhos futuros, pode ser implementado um protocolo novo e específico para o cenário abordado, desta forma, o mesmo poderia ser otimizado de acordo com as necessidades encontradas, assim como expurgada qualquer informação extra que trafega pela rede e que efetivamente não representa nenhum ganho nestas condições apresentadas.

Simular outros protocolos também pode ser uma alternativa de trabalho futuro, para tal, seria necessário primeiramente implementar o protocolo no NS-2, caso seja utilizado este simulador. Neste trabalho, os protocolos simulados foram AODV, DSR, DSDV e OLSR, porém vários outros foram citados.

Outra proposta interessante é implementar em campo, no cenário escolhido, roteadores sem fio com o protocolo escolhido e avaliar o comportamento real da rede, pois algumas características, como interferências, podem alterar sensivelmente o desempenho de redes sem fio. Estes resultados poderiam ser comparados a resultados de vários softwares simuladores existentes atualmente como: NS-2 (*Network Simulator 2*) [NS2, 2005], GloMoSim (*Global Mobile Information Systems Simulation Library*) [Zeng et al, 1998] , MaRS (*Maryland Routing Simulator*) [Alaettinoglu, 1994] , MobiCS2 (*Mobile Computing Simulator 2*) [Endler et al, 2001]. Assim, a precisão dos resultados poderia ser comparada de forma a se determinar o melhor simulador de redes mesh / ad-hoc para cenários parecidos com o determinado.

REFERÊNCIAS BIBLIOGRÁFICAS

[Clausen e Jacquet, 2003] CLAUSEN, Thomas; JACQUET, Philippe. "Optimized Link State Routing Protocol (OLSR)", RFC 3626. Outubro de 2003.

[Aguayo et al, 2004] AGUAYO, Daniel; BICKET, John; BISWAS, Sanjit; JUDD, G.; MORRIS, Robert. "A Measurement Study of a Rooftop 802.11b Mesh Network", Proceedings of ACM SIGCOMM Conference (SIGCOMM 2004), Setembro de 2004.

[Alaettinoglu, 1994] ALAETTINOGLU, C; et al. "Design and Implamentation of MaRS: A Routing Testbed". Journal of Interworking Research and Experience, 5, no 1. 1994.

[Becker e Montez, 2004] BECKER, Valdecir; MONTEZ, Carlos. "TV Digital Interativa: Conceitos, desafios e perspectivas para o Brasil", Livro. Florianópolis, 2004.

[Bicket et al, 2004] BICKET, John; AGUAYO, Daniel; BISWAS, Sanjit; MORRIS, Robert. "Architecture and Evaluation of an Unplanned 802.11b Mesh Network", In ACM SIGCOMM 2004, Agosto de 2004.

[Broch, 1998] BROCH, Josh; MALTZ, David A.; JOHNSON, David B.; HU Y.C.; Jetcheva, J. "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols". Proceedings of the Fourth Annual International Conference on Mobile Computing and Networking (MobiCom'98), ACM, Dallas, TX. Outubro de 1998.

[Campista et al, 2006] CAMPISTA, M. E. M., MORAES, I. M., ESPOSITO, P. M., AMODEI Jr., A., CUNHA, D. O., COSTA, L. H. M. K., e DUARTE, O. C. M. B. "Capacidade do Canal de Interatividade Ad Hoc para a TV Digital". XXIV Simpósio Brasileiro de Redes de Computadores - SBRC'2006, pp. 1065-1068, Curitiba, PR. Maio de 2006.

[Ceasm, 2000] <http://www.ceasm.org.br/> . Site sobre Censo Maré 2000.

[Cerveira e Costa, 2006] CERVEIRA, C. R. e COSTA, L. H. M. K. "A Time-Based Admission Control Mechanism for IEEE 802.11 Ad Hoc Networks". 8th IFIP IEEE International Conference on Mobile and Wireless Communication Networks - MWCN'2006, pp. 217-228. Santiago, Chile. Agosto de 2006.

[Clausen e Jacquet, 2003] CLAUSEN, Thomas; JACQUET, Philippe. "Optimized Link State Routing Protocol (OLSR)", RFC 3626. Outubro de 2003.

[Cordeiro e Agrawal, 2002] CORDEIRO, Carlos de M.; AGRAWAL, Dharma P. "Mobile Ad Hoc Networking", SBRC – 20o. Simpósio Brasileiro de Redes de Computadores. Minicursos. Búzios - RJ, Maio de 2002.

[Corson e Park, 2001] CORSON, S.; PARK, V. "Temporally-Ordered Routing Algorithm (TORA) Version 1", INTERNET-DRAFT. IETF MANET Working Group. Julho de 2001.

[CPS/FGV b, 2007]

http://www2.fgv.br/ibre/cps/mapa_exclusao/apresentacao/SUM%C1RIO.pdf .

Artigo disponibilizado pelo CPS / FGV a respeito de dados sobre Exclusão Digital. Janeiro de 2007.

[CPS/FGV, 2007] <http://www.fgv.br/ibre/cps/> . Site do CPS (Centro de Políticas Sociais) organizado pela FGV (Fundação Getúlio Vargas) a respeito de dados sobre Exclusão Digital. Janeiro de 2007.

[Das et al, 1998] DAS, Samir R., CASTAÑEDA, Robert; YAN, Jiangtao; SENGUPTA, Rimli. "Comparative Performance Evaluation of Routing Protocols for Mobile, Ad hoc Networks". Proc. of IEEE the Seventh

International Conference on Computer Communications and Networks (IC3N '98), Outubro de 1998.

[Dube, 1997] DUBE, R.; et al. "Signal Stability Based Adaptive Routing for Ad Hoc Mobile Networks", Proceedings of IEEE Personal Communications. Fevereiro de 1997.

[Endler et al, 2001] ENDLER, Markus; et al. "MobiCS: An Environment for prototyping and simulating distributed protocols for mobile networks". IEEE Int. Conference on Mobile and Wireless Communications Networks. Recife, 2001.

[Esposito et al, 2007] ESPOSITO, P. M., SCHILLER, F. O. B., CAMPISTA, M. E. M., MORAES, I. M., RUBINSTEIN, M. G., COSTA, L. H. M. K., DUARTE, O. C. M. B. "Implementação da Métrica de Roteamento Tempo Esperado de Transmissão em Redes em Malha Sem Fio". XII Workshop de Gerência e Operação de Redes e Serviços - WGRS'2007, pp. 25-36. Belém, PA. Maio de 2007.

[Filadélfia Digital b, 2006] <http://www.wirelessphiladelphia.org/index.html> . Site sobre a cidade digital da Filadélfia. Outubro de 2006.

[Filadélfia Digital, 2006] http://www.wirelessphiladelphia.org/news/wp_news1.html . Site sobre a cidade digital da Filadélfia. Outubro de 2006.

[Gerla et al, 2001] GERLA, Mario; HONG, Guangyu; PEI, Guangyu. "Fisheye State Routing Protocol (FSR)", INTERNET-DRAFT. IETF MANET Working Group. Dezembro de 2001.

[Gregori et al, 2005] R. Bruno, M. Conti, and E. Gregori, "Mesh Networks: Commodity Multihop Ad Hoc Networks", IEEE Communications Magazine, vol. 43, no. 3, pp. 123—131. Março de 2005.

[Haas et al, 2001 b] HAAS, Zygmunt J.; PEARLMAN, Marc R.; SAMAR, Prince. "The Interzone Routing Protocol (IERP) for Ad Hoc Networks", INTERNET-DRAFT. IETF MANET Working Group. Junho de 2001.

[Haas et al, 2001] HAAS, Zygmunt J.; PEARLMAN, Marc R.; SAMAR, Prince. "The Intrazone Routing Protocol (IARP) for Ad Hoc Networks", INTERNET-DRAFT. IETF MANET Working Group. Junho de 2001.

[Haas, 2001] HAAS, Zygmunt J. "The Performance of Query Control Schemes for the Zone Routing Protocol (ZRP)", IEEE/ACM Transactions of Networking, VOL 9, No. 4. Agosto de 2001.

[Hersent et al, 2002] HERSENT, Oliver; GUIDE, David; PETIT, Jean-Pierre. "Telefonia IP – Comunicação multimídia baseada em pacotes", Editora PEARSON Addison Wesley. São Paulo, 2002.

[IEEE b, 2006] <http://www.ieee.org>. Site oficial do IEEE. Outubro de 2006.

[IEEE, 2006] http://grouper.ieee.org/groups/802/11/Reports/tgs_update.htm . Site sobre IEEE 802.11s (Redes Mesh). Setembro de 2006.

[IETF, 2005] <http://www.ietf.org> Site do grupo IETF - Internet Engineering Task Force. Maio de 2005.

[IPTV b, 2006] <http://www.broadbandservicesforum.org/> . Site sobre IPTV. Outubro de 2006.

[IPTV, 2006] <http://www.itu.int/ITU-T/IPTV/> . Site sobre IPTV. Outubro de 2006.

[Iwata et al, 1999] IWATA, Atsushi; et al. "Scalable Routing Strategies for Ad Hoc Wireless Networks", IEEE Journal on Selected Areas in Communications, vol. 17, no. 8. Agosto de 1999.

[Jacquet et al, 2005] JACQUET, P., MÜHLETHALER, T., et al. "Optimized Link State Routing Protocol of Ad Hoc Networks", Proceedings of INMIC'01. Paquistão, Dezembro de 2005.

[Jhansson et al, 1999] JHANSSON, Per; LARSSON, Tony; HEDMAN, Nicklas; MIELCZAREK, Bartosz; DEGERMARK, Mikael. "Scenario-based performance analysis of routing protocols for mobile ad-hoc networks". International Conference on Mobile Computing and Networking. Proceedings of the 5th

annual ACM/IEEE international conference on Mobile computing and networking, Estados Unidos, NY. 1999.

[Johnson e Maltz, 1996] JOHNSON, D. ; MALTZ, D. “Dynamic Source Routing (DSR) in Ad Hoc Wireless Networks”, Mobile Computing, Kulwer Academic. 1996.

[Johnson et al, 2002] JOHNSON, David B.; MALTZ, David A.; HU, Yih-Chun. “The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks for Ipv4 (DSR)”, RFC 4728. IETF MANET Working Group. Fevereiro de 2002.

[Kurose e Ross, 2004] KUROSE, James F.; ROSS, Keith W. “Redes de Computadores e a Internet - Uma Nova Abordagem”, Editora PEARSON Addison Wesley. São Paulo, 2004.

[Lee et al, 2000] LEE, S-J; AHN, J-S; ZHANG, X; CAMPBELL, A.T. “INSIGNIA: An IP based Quality of Service Framework for Mobile Ad Hoc Networks” Academic Press. Flórida, EUA, 2000.

[Macker e Corson, 1999] Macker, J. Corson, S. “Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations”, RFC 2501. Janeiro de 1999.

[Manoj e Murthy, 2004] MANOJ, B. S.; MURTHY, C. Siva. “Ad Hoc Wireless Networks: Architectures and Protocols”, Editora Prentice Hall. New Jersey - USA, 2004.

[Murthy e Garcia, 1996] MURTHY, Shree; GARCIA-LUNA-ACEVES, J.J. “An efficient routing protocol for wireless networks”, ACM Mobile Networks and Applications Journal. Outubro de 1996.

[NS2, 2005] <http://www.isi.edu/nsnam/ns/> . Site do NS-2. Maio de 2005.

[Oliveira, 2006] OLIVEIRA, Etienne. “Avaliação de Protocolos para Redes de Sensores e Redes Ad Hoc aplicados à TV Digital Interativa e Cidades Digitais” Dissertação de Mestrado, Departamento de Ciência da Computação, UFF. Niterói, RJ, 2006.

[OLPC, 2006] <http://laptop.org/> . Site sobre o projeto OLPC, laptop a U\$100,00. Outubro de 2006

[OpenWRT, 2005] <http://openwrt.org> . Site sobre o projeto Open WRT, 2005.

[Peiyan e Layuan, 2006] PEIYAN, Yuan; LAYUAN, Li. "Performance evaluation and simulations of routing protocols in ad hoc networks". ACM International Conference Proceeding Series; Vol. 196. Proceedings of the 2006 workshop on Broadband wireless access for ubiquitous networking, Itália. 2006.

[Pereira e Pedroza, 2004] PEREIRA, Ivana C.M.; PEDROZA, A.C.P. "Redes Móveis Ad Hoc Aplicadas em Cenários Militares", IV Congresso Brasileiro de Computação - CBComp'2004, Itajaí, SC, Brasil, Outubro de 2004.

[Pereira, 2004] PEREIRA, Ivana Cardial de Miranda. Orientador: Aloysio de Castro Pinto Pedroza "Análise de Roteamento em Redes Móveis Ad Hoc em Cenários de Operações Militares". Tese de mestrado. COPPE/PEE/UFRJ – Rio de Janeiro, Junho de 2004.

[Perkins e Bhagwat, 1994] PERKINS, Charles E.; BHAGWAT, Pravin. "Highly Dynamic Destination-Sequenced Distance Vector Routing (DSDV) for mobile computers", Computer Comm. Review. Outubro de 1994.

[Perkins e Royer, 1999] PERKINS, Charles E.; ROYER, E.M. "Ad Hoc On-Demand Distance Vector Routing (AODV)", Proceedings of IEEE Workshop on Mobile Computing Systems and Applications 1999, pp. 90-100. Fevereiro de 1999.

[Perkins e Royer, 2003] PERKINS, Charles E.; ROYER, E.M.; DAS, S. "Ad hoc On-Demand Distance Vector (AODV) Routing", RFC 3561. IETF MANET Working Group. Julho de 2003.

[Pirai Digital b, 2006] <http://www.piraidigital.com.br/> . Site oficial sobre o projeto Pirai Digital. Junho de 2006.

[Pirai Digital, 2006] <http://www.pirai.rj.gov.br/paginamenu.php?id=11> . Site sobre Pirai Digital. Junho de 2006.

[Remesh, 2006] <http://mesh.ic.uff.br> . Site sobre iniciativa de Redes Mesh na UFF: Projeto ReMesh. Setembro de 2006.

[Revista Teletime, 2006] Revista Teletime - Atlas Brasileiro de Telecomunicações, Número 6, 2006.

[Schiller, 2007] SCHILLER, Felipe Ortigão Sampaio Buarque. Orientador: Luís Henrique Maciel Kosmowski Costa. "Estudo, Implementação e Análise de Métricas Baseadas na Qualidade do Enlace para o Protocolo OLSR" Projeto final de graduação. DEL/POLI/UFRJ – Rio de Janeiro, Janeiro de 2007.

[Sesay et al, 2004] SESAY, Samba; YANG, Zongkai; QI, Biao; HE, Jianhua. "Simulation Comparison of Four Wireless Ad Hoc Routing Protocols", Huazhong University of Science and Technology, Wuhan. Information Technology Journal 3, 2004.

[Silva e Oliveira, 2005] SILVA, Alan P.T.; OLIVEIRA, Gustavo A.; Orientador: Paulo Roberto de Lira Gondim. "Comparação de Protocolos de Roteamento sob diferentes modelos de mobilidade em redes ad hoc". Projeto de Final de curso de graduação, Brasília, DF, Brasil. Janeiro de 2005.

[Sud Mennucci Digital, 2006]
<http://www.sudmennucci.sp.gov.br/wifi/index.php> . Site oficial sobre o projeto Sud Menucci Digital. Junho de 2006.

[Taipei Digital, 2006]
http://www.nortel.com/corporate/news/newsreleases/2005b/06_02_05_qware.html . Site da empresa Nortel Networks sobre Taipei Digital. Outubro de 2006.

[Tiradentes Digital, 2006]
<http://www.idbrasil.gov.br/Members/carla.cg@terra.com.br/tiradentes> . Site sobre Tiradentes Digital. Junho de 2006.

[Toh, 2002] TOH, C. K. "Evaluating the Communication Performance of an Ad Hoc Wireless Network", IEEE Transactions on Wireless Communications, VOL I, No. 3. Julho de 2002.

[Tropos, 2006] <http://www.tropos.com/technology/whitepapers.html> . Site da empresa Tropos, na qual diversos artigos são disponibilizados. Outubro de 2006.

[Tsarmopoulos et al, 2005] TSARMPOPOULOS, N., KALAVROS, I., LALIS, S. "A Low-Cost and Simple-to-Deploy Peer-to-Peer Wireless Network base don Open Source Linux Routers", Proceedings of the 1st International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities (TRIDENTCOM'05), 2005.

[Villela, 2004] VILLELA, Bernardo A. M., "Análise da Vazão Máxima em Redes Ad Hoc", Dissertação de mestrado. COPPE – UFRJ – Msc. Julho de 2004.

[WiMAX Fórum, 2006] <http://www.wimaxforum.org/home> . Site oficial sobre WiMAX Forum. Outubro de 2006.

[WiMAX, 2006] http://www.intel.com/netcomms/technologies/wimax/wimax_docs.htm . Site da Intel que reúne documentos sobre a tecnologia WiMAX. Outubro de 2006.

[Xue et al, 2003] XUE, J; STUEDI, P; ALONSO, G. "ASAP: An Adaptative QoS Protocol for Mobile Ad Hoc Networks", 14th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, China. Setembro de 2003.

[Zeng et al, 1998] ZENG, Xiang; et al. "GloMoSim: A Library for Parallel Simulation of Large-scale Wireless Network". Proceedings of PADS'1998. Los Angeles, EUA, 1998.