



COPPE/UFRJ

UM NOVO PROTOCOLO DE ROTEAMENTO PARA REDES EM MALHA
SEM FIO

Miguel Elias Mitre Campista

Tese de Doutorado apresentada ao Programa de Pós-graduação em Engenharia Elétrica, COPPE, da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Doutor em Engenharia Elétrica.

Orientadores: Luís Henrique Maciel
Kosmalski Costa
Otto Carlos Muniz Bandeira
Duarte

Rio de Janeiro
Dezembro de 2008

UM NOVO PROTOCOLO DE ROTEAMENTO PARA REDES EM MALHA
SEM FIO

Miguel Elias Mitre Campista

TESE SUBMETIDA AO CORPO DOCENTE DO INSTITUTO ALBERTO LUIZ
COIMBRA DE PÓS-GRADUAÇÃO E PESQUISA DE ENGENHARIA (COPPE)
DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO COMO PARTE DOS
REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE DOUTOR
EM CIÊNCIAS EM ENGENHARIA ELÉTRICA.

Aprovada por:

Prof. Luís Henrique Maciel Kosmalski Costa, Dr.

Prof. Otto Carlos Muniz Bandeira Duarte, Dr.Ing.

Prof. Aloysio de Castro Pinto Pedroza, Dr.

Prof. Célio Vinicius Neves de Albuquerque, Ph.D.

Prof. Marcelo Gonçalves Rubinstein, D.Sc.

Prof. Nelson Luis Saldanha da Fonseca, Ph.D.

RIO DE JANEIRO, RJ – BRASIL

DEZEMBRO DE 2008

Campista, Miguel Elias Mitre

Um Novo Protocolo de Roteamento para Redes em Malha Sem Fio/Miguel Elias Mitre Campista. – Rio de Janeiro: UFRJ/COPPE, 2008.

XIII, 94 p.: il.; 29, 7cm.

Orientadores: Luís Henrique Maciel Kosmalski Costa

Otto Carlos Muniz Bandeira Duarte

Tese (doutorado) – UFRJ/COPPE/Programa de Engenharia Elétrica, 2008.

Referências Bibliográficas: p. 83 – 94.

1. Redes Sem Fio. 2. Redes em Malha Sem Fio.
3. Roteamento. 4. Justiça. I. Costa, Luís Henrique Maciel Kosmalski *et al.*. II. Universidade Federal do Rio de Janeiro, COPPE, Programa de Engenharia Elétrica. III. Título.

*Aos meus pais,
Francisco e Deise,
à minha irmã, Raquel e
à minha futura esposa, Renata.*

Agradecimentos

Gostaria de agradecer a todos que me ajudaram nessa jornada de anos. Como são muitos anos e, conseqüentemente, muitos nomes, peço perdão se ao longo desses agradecimentos eu não lembrar todos que cruzaram o meu caminho e de certa forma contribuíram com a minha formação. Para que eu chegasse até o ponto que me encontro, contando desde a graduação, lá se vão onze anos de dedicação aos estudos, os quais por muitas vezes coloquei em dúvida se valeriam à pena. Agora, ao final dessa jornada, já sinto saudades e percebo que todo o esforço e os anos de bolsa de estudos valem à pena quando se faz o que realmente se gosta.

Em primeiro lugar, gostaria de agradecer a Deus pela oportunidade e pelos dons recebidos. Gostaria de agradecer à minha família, em especial aos meus pais e à minha irmã, por todo o amor, sacrifício, educação e apoio incondicional ao longo de toda minha vida. Eles são a base de tudo que sou e um espelho para o meu futuro. Sem eles, nada disso teria sido possível. Além dos meus familiares, nos últimos anos, uma pessoa muito especial entrou na minha vida, a minha futura esposa Renata. Gostaria de agradecer a ela pela compreensão, pelo amor recíproco e ainda por ter me proporcionado novos familiares. Sua presença é uma motivação a mais para o prosseguimento da minha jornada.

Gostaria de agradecer aos meus professores orientadores Luís Henrique Costa e Otto Carlos Duarte pela confiança, orientação, paciência e amizade durante todo o mestrado e doutorado. Todo o meu crescimento profissional é graças às muitas horas que eles dedicaram à correção das minhas falhas e dos meus pontos fracos. Espero, ao final da tese, ter correspondido ao menos em parte as suas expectativas.

Gostaria de agradecer à equipe do GTA, particularmente aos amigos Igor, Pedro Velloso, Daniel Cunha, Rafael Laufer, Bicudo, Aurélio, Pedro Espósito, Danilo, Marcelo, Natalia, Kléber, Carlos Henrique e Marcel por toda amizade e cooperação

durante toda a tese. Aos meus co-orientados Rafael, Rodrigo e Igor. Aos meus amigos fora do GTA Bruno, Daniel Veiga, Manoel, Felipe, Daniel Almeida, Raul, Mauro, Marcel, Mendes, Fernandão, Bruninho, Marcelle, Thiago, Léo e respectiva(o)s por compartilharem comigo durante muitos e muitos anos momentos felizes e momentos difíceis.

Gostaria ainda de agradecer aos professores Aloysio Pedroza, Célio Albuquerque, Marcelo Rubinstein e Nelson Fonseca pela presença na banca examinadora. Gostaria de agradecer aos professores Rezende e Leão que tiveram uma participação fundamental em minha formação acadêmica. Além de fazerem parte da minha banca, gostaria de agradecer novamente aos professores Marcelo Rubinstein e Célio Albuquerque pela amizade e companheirismo ao longo dos anos de tese.

Gostaria de agradecer também aos funcionários do Programa de Engenharia Elétrica da COPPE/UFRJ, Daniele, Rosa, Mauricio e Artur e à funcionária do registro da COPPE/UFRJ, Solange, pela presteza no atendimento e dedicação ao trabalho.

Por fim, gostaria de agradecer ao CNPq e à Faperj pelo financiamento da pesquisa.

Resumo da Tese apresentada à COPPE/UFRJ como parte dos requisitos necessários para a obtenção do grau de Doutor em Ciências (D.Sc.)

UM NOVO PROTOCOLO DE ROTEAMENTO PARA REDES EM MALHA
SEM FIO

Miguel Elias Mitre Campista

Dezembro/2008

Orientadores: Luís Henrique Maciel Kosmowski Costa

Otto Carlos Muniz Bandeira Duarte

Programa: Engenharia Elétrica

Atualmente, as redes em malha sem fio (RMSF) são consideradas a solução com a melhor relação custo-benefício para as redes de acesso. As RMSF são caracterizadas pela presença de um *backbone* estacionário, composto por roteadores sem fio, e a presença de um *gateway* para a Internet. Este trabalho aborda em paralelo dois problemas em aberto das redes em malha sem fio: (i) a conservação dos recursos da rede e (ii) a justiça no acesso ao meio sem fio. Considerando o primeiro problema, este trabalho propõe o protocolo de roteamento WPR (*Wireless-mesh-network Proactive Routing*) que é baseado em estados do enlace. O WPR explora as particularidades das RMSF para diminuir a sobrecarga de controle da rede ao mesmo tempo em que mantém as métricas dos enlaces mais utilizados sempre atualizadas. Assim, os recursos da rede são economizados e a vazão obtida aumenta. Considerando o segundo problema, este trabalho propõe o mecanismo RLF (*Route-Length-based Fairness*) para atribuir prioridade a pacotes na camada MAC (*Medium Access Control*). Pacotes que percorrem um número grande de saltos, chamados pacotes de vida longa, recebem uma maior prioridade no acesso ao meio. Os resultados obtidos demonstram que ambas as abordagens melhoram o desempenho das redes em malha sem fio.

Abstract of Thesis presented to COPPE/UFRJ as a partial fulfillment of the requirements for the degree of Doctor of Science (D.Sc.)

A NEW ROUTING PROTOCOL FOR WIRELESS MESH NETWORKS

Miguel Elias Mitre Campista

December/2008

Advisors: Luís Henrique Maciel Kosmowski Costa

Otto Carlos Muniz Bandeira Duarte

Department: Electrical Engineering

Currently, wireless mesh networks (WMN) are considered the most cost-effective solution for access networks. WMNs are characterized by a stationary backbone, composed by wireless routers, and the presence of an Internet gateway. This work addresses in parallel two issues in wireless mesh networks: (*i*) conservation of network resources, and (*ii*) fairness in wireless medium access. Concerning the former problem, this work proposes the link-state-based routing protocol WPR (Wireless-mesh-network Proactive Routing). WPR profits from the main WMN characteristics to reduce the network routing overhead while keeping updated the metrics for the frequently used links. Consequently, we save network resources and increase the aggregated throughput. Concerning the latter problem, this work proposes the RLF (Route-Length-based Fairness) mechanism to assign priority to packets at the MAC (Medium Access Control) layer. Packets that traverse a high number of hops, named long-living packets, receive a higher priority on medium access. The results obtained demonstrate that both solutions improve the wireless mesh network performance.

Sumário

Lista de Figuras	xi
Lista de Tabelas	xiii
1 Introdução	1
1.1 Motivação	1
1.2 Objetivos	5
1.3 Organização	6
2 Redes em Malha Sem Fio	7
2.1 Arquitetura da Rede	7
2.2 Desafios	9
2.2.1 Balanceamento da Vazão	9
2.2.2 Escassez de Recursos e Convergência do Tráfego	10
2.2.3 Mobilidade dos Usuários	11
2.2.4 Segurança	12
3 Trabalhos Relacionados	15
3.1 Encaminhamento por Múltiplos Saltos	15
3.2 Roteamento nas Redes em Malha Sem Fio	18
3.2.1 Métricas	18
3.2.2 Protocolos	25
4 RLF: <i>Route-Length-based Fairness</i>	36
4.1 Premissas	36
4.2 Operação do RLF	38
4.3 Resultados	41

4.3.1	Experimentos com Tráfego CBR	42
4.3.2	Experimentos com Tráfego FTP	45
5	WPR: <i>Wireless-mesh-network Proactive Routing protocol</i>	51
5.1	Premissas	51
5.2	Operação do Protocolo	52
5.2.1	Algoritmo de Controle de Inundação	53
5.2.2	Análise do Algoritmo de Controle de Inundação	57
5.2.3	Avaliação Comparativa	59
5.2.4	Algoritmo para o Cálculo do Conjunto AMPR	63
5.3	Análise da Complexidade dos Algoritmos Propostos	66
5.4	Ambiente de Simulações	69
5.4.1	Camada Física	70
5.4.2	Camada de Acesso ao Meio	71
5.4.3	Roteamento	72
5.4.4	Padrão de Tráfego e Cenário	73
5.5	Resultados das Simulações	74
5.5.1	Tráfego <i>Web</i>	75
5.5.2	Tráfego Misto	77
6	Conclusões	80
	Referências Bibliográficas	83

Lista de Figuras

2.1	Exemplo de uma rede em malha sem fio.	8
2.2	Categorias conforme o padrão IEEE 802.11s.	9
2.3	Exemplo de uma topologia em cadeia com um <i>gateway</i> e quatro nós roteadores (R1 a R4).	11
2.4	Exemplo do uso do NAT (<i>Network Address Translator</i>).	13
3.1	Exemplo de casos onde há interferência intra e interfluxos.	21
3.2	Exemplo de uma rede desconectada devido ao uso de múltiplos canais.	22
3.3	Métodos de inundação possíveis iniciados pelo nó i	28
3.4	Rede de testes do GTA.	30
3.5	Taxa de perda de pacotes.	31
3.6	Tempo de ida e volta.	31
3.7	Comprimento da rota.	31
4.1	Exemplo de uma topologia em cadeia com um <i>gateway</i> e quatro nós roteadores (R1 a R4).	37
4.2	Resultados obtidos para fontes CBR/UDP.	43
4.3	Distribuição de vazão entre os nós da cadeia usando fontes CBR/UDP.	44
4.4	Abordagem de melhor caso usando fontes CBR/UDP.	46
4.5	Resultados obtidos para fontes FTP/TCP.	48
4.6	Abordagem de melhor caso usando fontes FTP/TCP.	49
4.7	Distribuição de vazão entre os nós da cadeia usando fontes FTP/TCP.	50
5.1	Conjunto de ascendentes e de descendentes de i conforme o WPR.	53
5.2	Algoritmos de inundação controlada.	54

5.3	Proporção entre os períodos de envio de mensagens de inundação controlada e inundação.	59
5.4	Função de ajuste de inundação.	60
5.5	Cenário esparsos.	62
5.6	Cenário denso.	64
5.7	Topologia considerada.	67
5.8	Impacto do uso do módulo de perda de pacotes.	71
5.9	Impacto do uso do algoritmo de controle de taxa - ARF.	72
5.10	Tráfego <i>web</i> com carga baixa.	75
5.11	Tráfego <i>web</i> com carga alta.	77
5.12	Tráfego misto.	78

Lista de Tabelas

3.1	Características principais das métricas de roteamento.	24
3.2	Protocolos de roteamento e respectivas métricas.	34
4.1	Parâmetros usados na análise do melhor caso.	47
5.1	Parâmetros de camada física.	70

Capítulo 1

Introdução

A popularização das redes de comunicação e, particularmente, da Internet, exige que os usuários estejam conectados a qualquer momento e em qualquer lugar. Essa necessidade torna a ubiqüidade uma característica fundamental para as redes dos próximos anos. As redes sem fio atendem esse objetivo já que a sua forma de transmissão é em difusão por natureza. Além disso, esse tipo de rede possui vantagens quanto ao custo de instalação e ao suporte à mobilidade dos usuários.

1.1 Motivação

As redes sem fio estão se tornando cada vez mais populares graças às suas características de facilidade de acesso, suporte à mobilidade e simplicidade de instalação. Além disso, a infra-estrutura cabeada reduzida e a comercialização em larga escala da tecnologia sem fio resultam em uma redução acentuada dos custos de instalação e manutenção. Como consequência, um número crescente de provedores de Internet está oferecendo acesso sem fio na última milha, o que a médio/longo prazo pode resultar na Internet ubíqua.

Atualmente, o padrão para as redes sem fio mais utilizado é o IEEE 802.11 [1], comercialmente conhecido como Wi-Fi (*Wireless-Fidelity*). As redes que operam no padrão IEEE 802.11 podem operar em dois modos: infra-estruturado e ad hoc [2]. No modo infra-estruturado, toda comunicação deve ser intermediada por pontos de acesso, que atuam como elementos centralizadores de tráfego. Essa característica limita a área de cobertura da rede, pois um usuário deve permanecer dentro do

alcance de um ponto de acesso para se comunicar com outros usuários. Apesar das estações usarem transmissão sem fio, os pontos de acesso são normalmente interconectados por cabos, o que ainda resulta em custos de infra-estrutura. No modo ad hoc, por outro lado, as estações utilizam comunicações por múltiplos saltos aumentando assim o alcance da comunicação. Entretanto, o encaminhamento do tráfego depende da colaboração das estações participantes. Essa característica dispensa totalmente o emprego de fios, em oposição ao modo infra-estruturado. No modo ad hoc, todas as estações desempenham o mesmo papel, não havendo nem elementos centralizadores de tráfego nem tampouco pontos de interconexão com outras redes. O problema das comunicações por múltiplos saltos é que a rede pode não estar totalmente conectada, pois as estações são móveis e as condições de transmissão do meio sem fio variam dinamicamente. Caso a rede não esteja totalmente conectada, o funcionamento pode ser comprometido e a rede ad hoc pode se tornar uma coleção de redes isoladas.

As Redes em Malha Sem Fio (RMSF) [3, 4, 5] são uma alternativa de baixo custo para as redes de acesso. O objetivo principal é aumentar o alcance da comunicação mantendo a conectividade da rede apesar da dinamicidade do meio e da mobilidade dos usuários. As redes em malha sem fio são caracterizadas pela presença de um *backbone* composto por roteadores sem fio. Esse *backbone* é responsável por estender o alcance do acesso à rede cabeada além do alcance da transmissão de um único ponto de acesso. Para tal, os roteadores do *backbone* sem fio são encarregados de encaminhar o tráfego recebido através de múltiplos saltos vindo tanto de clientes quanto de outros roteadores. A presença do *backbone* sem fio torna as redes em malha um híbrido entre o modo infra-estruturado, já que as estações utilizam o *backbone* sem fio para se comunicar, e o modo ad hoc, já que o encaminhamento é realizado em múltiplos saltos. As redes em malha sem fio aumentam a conectividade da rede, interconectam redes isoladas e provêem acesso a redes cabeadas de banda larga. Ao mesmo tempo, as redes em malha sem fio evitam cabos de rede, o que reduz o custo da infra-estrutura. As redes em malha sem fio são utilizadas em zonas metropolitanas, ambientes industriais, *campi* universitários e em redes comunitárias [3, 4, 6, 7, 8].

Nas redes em malha sem fio, os roteadores do *backbone* são tipicamente esta-

cionários e apenas os usuários da rede são capazes de se deslocar. Conseqüentemente, as limitações de bateria ficam restritas aos usuários móveis, pois os roteadores da rede podem ser alimentados por fontes permanentes de energia. Como a conectividade da rede e a economia de energia não são mais consideradas problemas graves, tanto o roteamento quanto a camada de acesso ao meio (*Medium Access Control - MAC*), voltam o foco para questões como a qualidade de acesso [9, 10]. As métricas de roteamento, por exemplo, vêm sendo aprimoradas considerando a taxa de entrega de pacotes dos enlaces sem fio, ao invés de apenas o número de saltos, como era feito nas redes ad hoc.

Muito esforço tem sido realizado na camada MAC do padrão IEEE 802.11 para explorar novas técnicas de camada física como múltiplos canais, múltiplas interfaces, antenas direcionais e sistemas MIMO (*Multiple-Input Multiple-Output*) [11, 12, 13, 14]. O objetivo dessas técnicas é aumentar a capacidade da rede e/ou a robustez. Entretanto, em cenários onde há comunicação por múltiplos saltos, a melhoria do desempenho depende do protocolo de roteamento escolher a rota mais adequada de acordo com as condições da rede e, se possível, de acordo com as necessidades da aplicação. Portanto, o roteamento desempenha um papel fundamental nas redes em malha sem fio ao reunir informações das camadas inferiores para oferecer às camadas superiores o melhor serviço possível.

Diferentes propostas têm surgido para aumentar a eficiência do roteamento, incluindo novas métricas e protocolos. Tanto essas novas métricas quanto os protocolos são desenvolvidos considerando as características do meio sem fio para aumentar o desempenho. Adicionalmente, o padrão IEEE 802.11s [15, 16, 17], que encontra-se em fase de padronização, pretende definir as comunicações por múltiplos saltos na camada de enlace, fazendo as redes em malha sem fio serem vistas como uma rede local para os protocolos de roteamento de camada 3. Para garantir o bom funcionamento do roteamento nas redes em malha sem fio, não basta apenas propor novos protocolos e métricas de roteamento. Alguns problemas relacionados às limitações do meio sem fio e às comunicações por múltiplos saltos persistem e devem ser abordados. Dentre esses problemas podem ser destacadas [16] a justiça no acesso ao meio sem fio e a conservação dos recursos da rede.

Uma aplicação típica das redes em malha sem fio é o acesso à Internet. Nessa

aplicação, alguns roteadores assumem o papel de *gateways* para a infra-estrutura cabeada. Um problema chave que surge é a injustiça em termos de vazão de acordo com o número de saltos que um pacote percorre até alcançar o *gateway* [18, 19, 20, 21]. Uma vez que um cliente esteja conectado a um roteador distante do *gateway*, sua vazão é menor que a vazão alcançada por um cliente mais próximo. Assumindo que não há diferenciação entre os clientes, não há razão para que o desempenho seja dependente do posicionamento do cliente na rede. Esse problema origina-se no protocolo MAC do padrão IEEE 802.11, que garante aos nós dentro de uma mesma área de transmissão uma probabilidade aproximadamente igual de acessar o meio. Porém, nas redes sem fio de múltiplos saltos, a disputa pelo acesso ao meio físico ocorre a cada salto. Logo, quanto mais saltos tiver a comunicação, mais disputas a acesso ao meio são realizadas.

O emprego dos protocolos de roteamento propostos para as redes ad hoc nas redes em malha sem fio representa a solução trivial, visto que em ambas as redes as comunicações são realizadas por múltiplos saltos. Entretanto, características relacionadas à arquitetura da rede em malha e à sua matriz de tráfego levam os protocolos legados das redes ad hoc a sofrerem adaptações. Essas adaptações têm por objetivo conservar os recursos da rede, pois a largura de banda disponível no meio sem fio é limitada e a transmissão é em difusão, reduzindo o número de nós que podem acessar a rede ao mesmo tempo. Dentre as características da arquitetura e da matriz de tráfego estão o posicionamento estacionário dos roteadores do *backbone* e a presença de um *gateway* para a rede cabeada. Os protocolos de roteamento para as redes em malha atuais lidam com essas características com novas métricas de roteamento e com novos procedimentos de descobrimento e manutenção de rotas. Porém, essas novas métricas introduzem uma sobrecarga de controle extra, o que leva a maioria dos protocolos de roteamento das redes em malha a aplicarem mecanismos para a redução dessa carga. Embora alguns protocolos utilizem uma abordagem híbrida, eles não eliminam o problema da latência na descoberta de rotas, que é uma característica dos protocolos de roteamento ad hoc reativos. Outros protocolos utilizam uma abordagem completamente pró-ativa, ou seja, inundam a rede periodicamente com atualizações de rotas. Nesse caso, apesar dos protocolos empregarem mecanismos de controle de inundação, esses mecanismos não estão adaptados às

características das redes em malha.

1.2 Objetivos

O primeiro objetivo deste trabalho é aprimorar a alocação de recursos entre os nós do *backbone* de uma rede em malha sem fio. Para isso, procura-se balancear a vazão máxima que cada nó da rede pode alcançar compensando as deficiências do método de acesso ao meio para redes de múltiplos saltos. Neste trabalho, é proposto um novo mecanismo chamado RLF (*Route-Length-based Fairness*) [22, 23]. Esse mecanismo tem como principal finalidade reduzir a injustiça observada nas comunicações sem fio de múltiplos saltos. Prioridades são atribuídas aos pacotes dependendo do número de saltos que cada um deve percorrer para alcançar o *gateway*. Pacotes enviados por nós distantes um grande número de saltos do *gateway*, chamados pacotes de vida longa, recebem uma prioridade maior na camada MAC. Para conhecer na camada MAC o tamanho da rota de um pacote, uma técnica de otimização entre camadas [24, 25] é usada. Assim, é possível à sub-camada MAC obter informações de roteamento da camada superior. Ao atribuir prioridade na camada MAC, há uma redução da diferença de vazão entre os roteadores do *backbone*, aumentando a justiça da rede. Diferente de trabalhos anteriores [18, 21], não há necessidade dos nós calcularem periodicamente a vazão máxima permitida, considerando informações de outros nós da rede [18, 21]. Além disso, não são necessários novos pacotes de controle. Para garantir que pacotes com diferentes comprimentos de rota tenham suas prioridades respeitadas, o mecanismo proposto utiliza múltiplas filas na camada de enlace. Os pacotes são colocados em filas de acordo com o comprimento das suas rotas.

O segundo objetivo é reduzir o tráfego de controle para, conseqüentemente, aumentar a disponibilidade da rede para os fluxos de dados. Para alcançar esse objetivo, considera-se o tráfego de controle produzido pela camada de rede, já que a parcela dos recursos consumida pela sobrecarga dos protocolos de roteamento é elevada. Neste trabalho, é proposto o protocolo de roteamento WPR (*Wireless-mesh-network Proactive Routing*) [26, 27] cuja principal característica é a utilização de algoritmos para redução da sobrecarga de roteamento. Diferente dos protocolos encontrados

na literatura [28], o WPR utiliza um algoritmo de controle de inundação [29] que leva em consideração a matriz de tráfego comum das redes em malha, que concentra carga nos enlaces próximos ao *gateway* da rede cabeada. O WPR é um protocolo baseado em estado do enlace e, portanto, provê a atualização periódica das métricas de roteamento para evitar latência durante a descoberta de rotas. O algoritmo de controle de inundação trata a topologia da rede em malha como uma árvore, onde o *gateway* é a raiz. Como consequência, cada roteador encaminha somente as mensagens de controle originadas em roteadores que pertençam à sua rota até o *gateway* ou em roteadores que o utilizem para alcançar o *gateway*. Além do algoritmo de controle de inundação, o WPR ainda utiliza um algoritmo específico para a escolha de nós AMPR (*Adapted Multi-Point Relay*). Os nós AMPR são os únicos responsáveis pelo encaminhamento de mensagens de controle de roteamento. Assim, evita-se que as mesmas mensagens de controle sejam transmitidas de forma redundante.

1.3 Organização

Esta tese está organizada da seguinte forma. O Capítulo 2 descreve as principais características das redes em malha sem fio, bem como introduz os principais desafios desse tipo de rede. O Capítulo 3 revisa os principais trabalhos relacionados aos temas abordados. O Capítulo 4 apresenta o mecanismo proposto para melhorar a justiça em redes em malha sem fio, o RLF (*Route-Length-based Fairness*), e analisa através de simulações o seu desempenho. O Capítulo 5 apresenta o protocolo de roteamento *Wireless-mesh-network Proactive Routing* (WPR) dando ênfase nos dois algoritmos para redução da sobrecarga de controle. São apresentados ainda testes por simulação para avaliar o desempenho do WPR. Por fim, o Capítulo 6 conclui esta tese e indica possíveis direções futuras.

Capítulo 2

Redes em Malha Sem Fio

Neste capítulo, a arquitetura e as respectivas funções dos diferentes nós que compõem as redes em malha sem fio são apresentadas. Além disso, os principais desafios encontrados nesse tipo de rede são introduzidos.

2.1 Arquitetura da Rede

Assim como nas redes ad hoc, nas redes em malha sem fio, os roteadores do *backbone* se comunicam através de múltiplos saltos, conforme mostrado na Figura 2.1. Já os usuários portando dispositivos como computadores portáteis e PDAs (*Personal Digital Assitants*) se conectam ao *backbone* via roteadores que desempenham o papel de pontos de acesso. Logo, nas redes em malha sem fio, alguns nós possuem funções especializadas, enquanto no caso ad hoc, isso não ocorre. Nas redes em malha, os usuários também podem encaminhar tráfego. Nesse caso, porém, esses nós exercem as funções dos nós do *backbone* e por isso podem ser considerados parte dele.

Atualmente, uma extensão ao padrão IEEE 802.11 está sendo desenvolvida para as redes em malha sem fio [30]. O grupo de trabalho “s” é responsável pelo padrão IEEE 802.11s que definirá o encaminhamento de quadros em múltiplos saltos na camada de enlace. Assim, os nós que não pertencem à rede em malha sem fio, enxergam como um único enlace. Essa abordagem, apesar de ir contra o princípio de independência entre camadas, uma vez que as funções tradicionalmente atribuídas às camadas de rede e de enlace se misturam, pode facilitar a adoção das redes em malha, já que todas as funcionalidades necessárias estarão disponíveis e pré-configuradas no

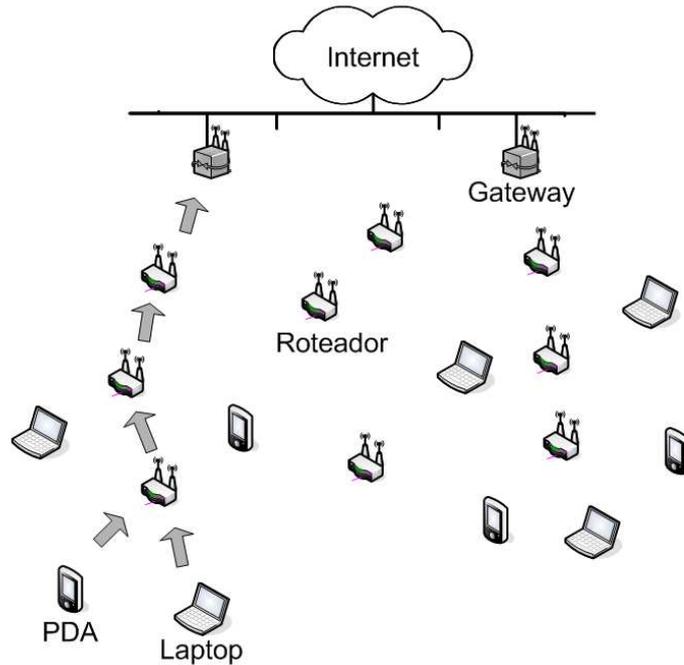


Figura 2.1: Exemplo de uma rede em malha sem fio.

equipamento adquirido pelo usuário.

O padrão IEEE 802.11s classifica os nós que compõem uma rede em malha sem fio em quatro categorias: estações (*stations - STA*), pontos da malha (*mesh points*), pontos de acesso da malha (*mesh access points*) e portais da malha (*mesh portal points*). A primeira categoria engloba os usuários da rede que não participam do roteamento. As estações apenas solicitam serviços da rede. A categoria de pontos da malha é formada pelos nós que participam do roteamento, mas não oferecem conexão às estações participantes. Em oposição, os pontos de acesso da malha além de participarem do roteamento, ainda funcionam como pontos de acesso às estações. Por fim, os portais da rede em malha são formados pelos nós responsáveis pela interconexão da rede. Logo, esses nós funcionam como *gateways* ou pontes para redes externas. Os portais da rede em malha possuem funcionalidades semelhantes aos pontos da malha e, portanto, não são utilizados como pontos de acesso para as estações. A topologia da rede e as diferentes categorias definidas pelo padrão IEEE 802.11s estão ilustradas na Figura 2.2.

As redes em malha sem fio têm duas peculiaridades importantes. Os roteadores, ou conforme a nomenclatura do padrão IEEE 802.11s, pontos da malha, pontos de acesso da malha e portal da malha, são tipicamente estacionários. Essa característica

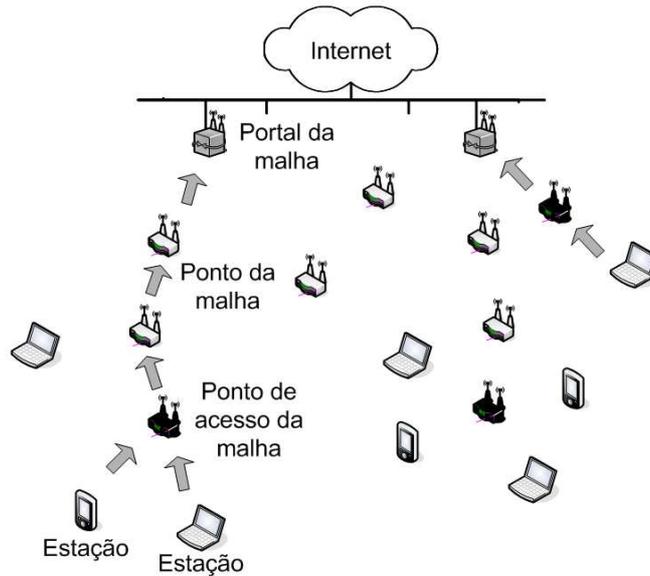


Figura 2.2: Categorias conforme o padrão IEEE 802.11s.

pode ser considerada no projeto dos protocolos usados nas diversas camadas. Por exemplo, as métricas de roteamento podem medir a qualidade dos enlaces sem fio, ao invés de apenas medir o número de saltos entre um nó fonte e um nó destino. A outra peculiaridade é que a maior parte do tráfego da rede flui na direção dos *gateways* ou portais da malha, já que o acesso à Internet é uma aplicação de caso comum nesse tipo de redes. A matriz de tráfego tende, portanto, a concentrar carga nos enlaces próximos aos *gateways*.

As semelhanças entre as redes em malha sem fio e as redes ad hoc fazem com que essas redes possuam muitos desafios em comum. Tais desafios, entretanto, podem ser acentuados pelas características peculiares das redes malha.

2.2 Desafios

Nesta seção, são destacados quatro dos desafios mais importantes das redes em malha sem fio.

2.2.1 Balanceamento da Vazão

De forma semelhante às redes ad hoc, os roteadores encaminham pacotes recebidos de outros nós e disputam o meio com os nós dentro da mesma área de contenção.

Assim, aumentar o número de saltos implica reduzir a vazão máxima alcançável dos nós mais distantes ao *gateway*, pois os pacotes desses nós disputam o meio mais vezes. Em redes em malha, esse problema pode ainda se tornar mais grave devido à infra-estrutura estacionária. Uma vez que não há mudanças na posição dos roteadores, os nós clientes que também não são móveis e que estão distantes do *gateway* vão sempre obter uma vazão máxima inferior a alcançada pelos clientes conectados aos roteadores mais próximos. Isso pode provocar desbalanceamentos no acesso aos recursos da rede.

Outro fator importante é o algoritmo de fila aplicado. No protocolo IEEE 802.11 original, todos os pacotes são colocados em uma única fila do tipo FIFO/Droptail. Nessas filas, o último pacote recebido é descartado caso a fila esteja cheia. Uma abordagem diferente é utilizada pelo IEEE 802.11e [31], que é a extensão do IEEE 802.11 que considera qualidade de serviço. No IEEE 802.11e, os quadros são colocados em filas diferentes de acordo com as suas prioridades. Os quadros mais prioritários são colocados em filas que podem possuir parâmetros IEEE 802.11 como o tamanho mínimo da janela de contenção e os intervalos entre quadros com valores menores. Ainda, os quadros de maior prioridade podem acessar o meio consecutivamente (*transmission opportunity* - TXOP) sem precisar entrar em contenção. Supondo o caso mais comum, que é o uso do IEEE 802.11 original, e supondo também a topologia em cadeia ilustrada na Figura 2.3, se todos os roteadores aumentarem sua carga oferecida igualmente, o roteador mais próximo do *gateway* (R1) tende a utilizar toda a capacidade do enlace entre ele e o *gateway*. Enquanto isso, os outros roteadores podem sofrer de inanição por não terem oportunidade de entregar seus pacotes ao *gateway* [32]. Na saturação, o roteador mais próximo enche sua fila de transmissão mais rápido do que transmite ou recebe pacotes. Logo, com a chegada de novos pacotes, ele é obrigado a descartá-los, independente do nó de origem. A vazão agregada da rede se torna injusta, pois o nó mais próximo ao *gateway* acaba tendo uma maior probabilidade de entrega dos pacotes que gera.

2.2.2 Escassez de Recursos e Convergência do Tráfego

As principais vantagens da tecnologia sem fio estão relacionadas com a transmissão por radiofrequência em difusão que dispensa cabos e permite mobilidade.

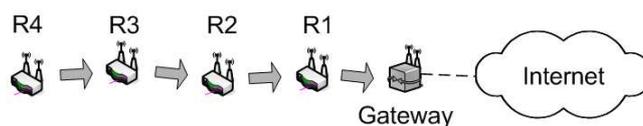


Figura 2.3: Exemplo de uma topologia em cadeia com um *gateway* e quatro nós roteadores (R1 a R4).

Entretanto, esse mesmo tipo de transmissão pode ser visto como o principal desafio dessas redes, uma vez que está sujeita a freqüentes variações, alta atenuação e ainda interferência. Adicionalmente, a largura de banda disponível é limitada, principalmente se comparada com as tecnologias de redes cabeadas, e há disputa durante o acesso ao meio com outras estações dentro do raio de alcance mútuo. Na tentativa de identificar o melhor possível as condições atuais do meio e assim tornar as comunicações confiáveis, muitos protocolos geram uma alta sobrecarga de controle. Essa sobrecarga consome parte relevante da capacidade da rede, a qual poderia ser utilizada para o tráfego de dados [33].

Atualmente, muitas das aplicações de redes em malha consideram o acesso à Internet. Nas redes em malha, isso resulta em convergência do tráfego na direção do *gateway* para a rede cabeada [34]. Mesmo aplicações par-a-par freqüentemente necessitam acessar a Internet para trocar informações de controle com servidores ou para se comunicar com pares em outras redes. Essa característica sobrecarrega os enlaces mais próximos ao *gateway*, podendo limitar a vazão de toda rede à capacidade desses enlaces.

2.2.3 Mobilidade dos Usuários

Um dos motivos do sucesso das redes sem fio é o suporte à mobilidade dos usuários. Essa característica, porém, é um desafio devido à alta variação da conectividade da rede, aos diferentes níveis de interferência e à freqüente reconfiguração dos protocolos. Esses problemas podem afetar o desempenho e ocasionar a queda da qualidade das aplicações. Nas redes em malha, embora a presença do *backbone* aumente a conectividade da rede, os usuários ainda estão sujeitos a freqüentes desconexões por *handoffs*. Durante os *handoffs*, os intervalos de ausência de conectividade

variam com o esquema de endereçamento e com a estratégia de encaminhamento utilizados. Caso os endereços usados sejam privados, há a necessidade de se utilizar tradução para endereços públicos (*Network Address Translator* - NAT). Com o uso do NAT, as estações da Internet não conseguem se comunicar diretamente com as estações da rede sem fio. Para isso, as estações da Internet devem se comunicar com as estações que realizam o NAT, para que estas estações encaminhem o tráfego aos nós da rede sem fio. O procedimento está ilustrado na Figura 2.4. Um pacote originado na estação sem fio é encaminhado até a estação que realiza o NAT para que esta mude o endereço IP de origem para o seu próprio. Conseqüentemente, ao receber o pacote de resposta vindo do servidor na Internet, ele deve trocar o endereço IP de destino para o endereço IP da máquina que requisitou o serviço. Nas redes sem fio, o impacto desse procedimento é que toda vez que um usuário sai do alcance da máquina que realiza o NAT, ele deve restabelecer suas conexões através da outra máquina que também realize o NAT. Esse procedimento pode levar tempo, deteriorando o desempenho principalmente de aplicações que utilizam o protocolo TCP (*Transmission Control Protocol*). Independentemente do uso de NATs, os endereços podem ser alterados após a mudança da sub-rede de acesso. Toda vez que um usuário se move, ele está sujeito a trocar de sub-rede e, como conseqüência, mudar de endereço IP para um endereço da faixa de endereços da nova rede. Esse procedimento pode acarretar desconexões temporárias para reconfiguração. Em um trabalho a parte, o desempenho de aplicações para distribuição de vídeo em redes par-a-par foi analisado em presença de *handoffs* em uma rede em malha [35]. Essa análise é tema de outro trabalho em andamento cujo um dos focos é avaliar o desempenho de diversas aplicações desse tipo [36].

2.2.4 Segurança

A transmissão em difusão dificulta o cumprimento de requisitos clássicos de segurança, principalmente os de privacidade, autenticidade e disponibilidade [37]. Isso ocorre porque é mais simples para usuários maliciosos acessarem os dados em trânsito e interferirem no desempenho das redes sem fio do que em redes cabeadas, uma vez que o meio sem fio opera em difusão.

Para aumentar a privacidade dos dados, mecanismos criptográficos podem ser

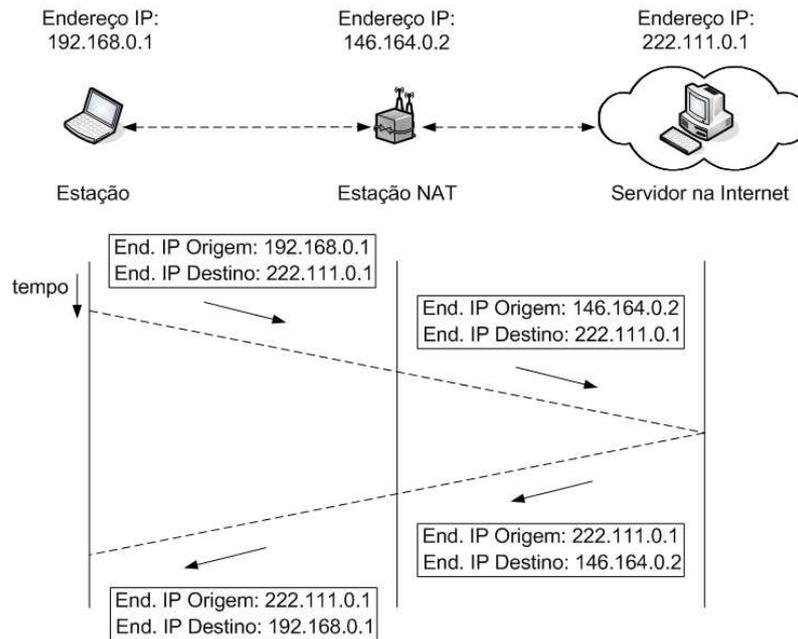


Figura 2.4: Exemplo do uso do NAT (*Network Address Translator*).

utilizados. Para isso, eles devem lidar com as limitações do *hardware* das estações. Nas redes em malha, as estações dos usuários possuem restrições de consumo de energia. Portanto, o emprego de sistemas criptográficos complexos ainda está limitado aos recursos disponíveis. Trabalhos atuais mencionam que sistemas de chaves simétricas com validade curta podem ser utilizados, já que essas chaves requerem um custo computacional mais baixo. Nas redes em malha, os nós do *backbone* também precisam de privacidade durante o tráfego de dados para que informações de topologia, por exemplo, não sejam facilmente obtidas. Nesse caso, sistemas de chaves assimétricas com validade mais longa podem ser utilizados, pois os nós do *backbone* não possuem as mesmas restrições de energia que as estações [38]. Entretanto, dependendo do *hardware*, os nós do *backbone* podem ainda estar limitados pelos recursos computacionais.

Além da privacidade, a autenticidade também é um requisito importante. Nas redes em malha, o encaminhamento dos dados é feito por múltiplos saltos. Para viabilizar esse tipo de comunicação são empregados protocolos de roteamento que devem se precaver contra a introdução de mensagens falsas ou alteradas. Tais mensagens podem anunciar rotas inválidas ou informações incorretas da topologia. Um ataque típico que forja as mensagens de roteamento para atrair tráfego e não encaminhá-lo é o buraco negro [39]. Garantir disponibilidade da rede em presença

de ataques de negação de serviço é outro desafio [40]. Em redes sem fio, a banda passante é limitada, o meio é em difusão e ataques do tipo *jamming* são difíceis de evitar. Nas redes em malha sem fio, as métricas de roteamento que consideram a qualidade dos enlaces podem contornar a área atacada e encontrar caminhos alternativos. Entretanto, o atacante obtém sucesso de qualquer forma já que ele interfere no funcionamento normal da rede.

Esta tese foca os dois primeiros desafios deste capítulo, ou seja, comunicações por múltiplos saltos e escassez de recursos e convergência do tráfego. Apesar dos desafios relacionados aos problemas da mobilidade e da segurança possuírem uma importância tão grande quanto a dos dois problemas abordados, eles estão fora do escopo desta tese.

Capítulo 3

Trabalhos Relacionados

Os dois desafios abordados são tratados nas camadas de enlace e de rede. A injustiça em termos de vazão dos nós e o acesso ao meio são aprimorados através de modificações do protocolo da camada de enlace. Já a sobrecarga de controle dos protocolos de roteamento é reduzida aproveitando a característica de convergência do tráfego nas redes em malha. Este capítulo revisa os principais trabalhos relacionados encontrados na literatura, nos dois temas onde foram realizadas as contribuições desta tese.

3.1 Encaminhamento por Múltiplos Saltos

Diferentes trabalhos tratam da justiça em redes sem fio de múltiplos saltos. Geralmente, as soluções propostas utilizam três tipos de abordagens: privilegiam alguns nós para evitar gargalos na rede [41, 42]; reservam recursos da rede através dos múltiplos saltos [18, 20, 21]; ou adotam diferentes estratégias de filas, principalmente no caso do protocolo TCP [43, 32, 44]. A maioria desses trabalhos considera a presença de um *gateway* para a Internet nas redes em malha sem fio.

Duffy *et al.* analisam o desempenho de aplicações com restrições de atraso em redes sem fio de múltiplos saltos [41]. É proposto um modelo analítico para verificar o desempenho das comunicações em múltiplos saltos. Adicionalmente, os autores propõem um mecanismo para atribuir maior prioridade aos roteadores agregadores de tráfego, evitando gargalos. No mecanismo proposto por Duffy *et al.*, o IEEE 802.11e é usado e a oportunidade de transmissão (*transmission opportunity*

- TXOP) de cada nó é ajustada baseada na quantidade de tráfego encaminhado. Quanto maior o tráfego encaminhado, maior é a oportunidade de transmissão. Em Raguin *et al.*, para acelerar as transmissões dos pacotes de dados, os nós que estão encaminhando tráfego em uma cadeia agregam em um único pacote o ACK e a requisição de transmissão (*Request To Send* - RTS) para o nó seguinte [42]. Assim, um nó que esteja encaminhando um pacote reconhece positivamente um pacote recebido ao mesmo tempo em que reserva o meio, evitando contenção para o próximo salto. A transmissão do pacote ACK/RTS é feita por nós sobrecarregados também para evitar gargalos. Essa proposta consegue acelerar o encaminhamento dos pacotes através da cadeia de nós, mas não elimina a probabilidade da injustiça de uma menor vazão de pacotes originados em nós distantes do *gateway*. Shi *et al.* aumentam o valor da janela de contenção mínima do nó mais próximo ao *gateway* para reduzir o problema da injustiça. Eles advogam que os nós mais distantes devem conseguir acessar o nó mais próximo ao *gateway* antes que este transmita. Assim, a justiça é alcançada colocando os pacotes de cada origem em filas separadas e servindo cada fila a partir de uma política como Round-Robin. Assim como o trabalho de Raguin *et al.*, Shi *et al.* [45] não garantem que os nós mais distantes alcancem a mesma vazão que os nós próximos tanto ao transmitirem dados na direção do *gateway* quanto no sentido reverso.

Gambiroza *et al.* propõem o IFA (*Inter-transit access points Fairness Algorithm*) para aumentar a justiça em redes de múltiplos saltos [18]. Com o IFA, cada nó calcula por enlace a quantidade de tempo que pode usar para efetuar suas transmissões, aumentando a justiça. O cálculo requer troca de informações de controle sobre a carga oferecida e a capacidade de cada enlace. Os nós enviam aos seus vizinhos a quantidade de recursos da rede que eles precisam para encaminhar o tráfego recebido. Após a troca de informações de controle, cada nó executa um algoritmo para calcular a máxima vazão permitida. Wang e Kar [20] propõem dois algoritmos para reduzir a injustiça em redes de múltiplos saltos. Os autores usam técnicas de otimização entre camadas para calcular a taxa ótima de transmissão na camada de transporte, de acordo com as condições detectadas no meio de transmissão. Eles consideram o ALOHA como método de acesso ao meio. Dong *et al.* propõem os algoritmos MMFA (*Max-Min Fair Allocation*) e TBFA (*Time-Based Fair Alloca-*

tion) [21]. O MMFA divide os recursos da rede entre os nós transmissores de modo que a vazão obtida por cada nó se torne equilibrada. Já o TBFA divide o tempo de transmissão para não prejudicar os nós que estão utilizando taxas mais altas. Em ambos os casos, os nós executam algoritmos adicionais e trocam informações de controle para relatar aos outros nós as suas condições atuais. Essas informações dizem respeito à vazão, no MMFA, e ao tempo de transmissão, no TBFA. Uma característica em comum das propostas de Gambiroza *et al.*, Wang e Kar, e Dong *et al.* é que elas precisam de troca de mensagens de controle para cálculo da vazão máxima permitida.

O padrão IEEE 802.11 originalmente usa o algoritmo FIFO/Droptail para gerenciar as filas de transmissão da camada MAC. Contudo, esse algoritmo mostrou-se ineficiente para o protocolo TCP, porque provoca grandes variações em sua janela de congestionamento, e para transmissões em múltiplos saltos. Desta forma, alguns trabalhos investigam diferentes algoritmos de escalonamento de filas para melhorar o desempenho do protocolo TCP em redes de múltiplos saltos. Fu *et al.* [43] usa o LinkRED (*Link Random Early Detection*) para manter a janela de congestionamento do TCP perto do valor ótimo, mesmo que haja congestionamento ou falhas de transmissões. Em transmissões em múltiplos saltos, usar uma fila FIFO/Droptail pode exaurir os recursos de nós afastados de mais de um salto do *gateway*. Então, Jun e Sichitiu [32] mostram que dividir o tráfego encaminhado e o originado pelo próprio nó em múltiplas filas e aplicar diferentes algoritmos de escalonamento, evita a exaustão de recursos. Eles advogam que apesar do custo, implementar uma fila por nó fonte é uma solução viável. Ferrero e Urvoy-Keller propõem o uso do LAS (*Least Attained Service*) [44] para aprimorar o desempenho do TCP. Uma prioridade é atribuída para cada fluxo de dados de acordo com o número de vezes que o fluxo foi servido até então. O fluxo cujos pacotes foram menos encaminhados aumenta de prioridade. Logo, sempre que a fila está cheia e um pacote de um fluxo prioritário é recebido, um pacote de um fluxo menos prioritário é descartado para dar lugar ao pacote recém chegado.

No Capítulo 4, será apresentado o mecanismo proposto nesta tese. Diferente das abordagens descritas, o mecanismo proposto privilegia os pacotes ao invés dos nós e não introduz sobrecarga adicional de controle. Por outro lado, o mecanismo

proposto continua utilizando múltiplas filas de transmissão.

3.2 Roteamento nas Redes em Malha Sem Fio

Muitas métricas e protocolos de roteamento vêm sendo propostos para as redes em malha [46, 47]. Esta seção descreve em detalhes as principais métricas e propõe uma classificação para os diferentes protocolos de roteamento [28].

3.2.1 Métricas

Nas redes ad hoc, a métrica mais utilizada é o número de saltos. Em tais redes, a utilização de métricas simples de calcular é mais freqüente, uma vez que a mobilidade dos usuários pode resultar em freqüentes quebras de enlaces. Portanto, é mais importante ter rapidamente uma rota para o destino do que ter uma rota de alta qualidade. Nas redes em malha sem fio, os roteadores são geralmente estacionários. Logo, as métricas de roteamento podem ser focadas na variação da qualidade dos enlaces ao invés de especificamente na quebra de enlaces. Esse tipo de métrica é conhecida por métrica ciente da qualidade [48].

Nos últimos anos, as métricas de roteamento têm sido continuamente aprimoradas. Uma das primeiras métricas propostas especificamente para as redes em malha sem fio é o Número Esperado de Transmissões (*Expected Transmission Count* - ETX) [49, 50]. O ETX calcula o número médio de vezes que um nó precisa enviar um pacote para um vizinho até que ele seja recebido com sucesso. Para calcular o ETX, cada nó envia sondas periodicamente em *broadcast* contendo o número de sondas recebidas de cada vizinho. O número de sondas recebidas é calculado no último intervalo de tempo T em uma janela deslizante. Um nó A calcula o ETX de um enlace para um nó B usando a taxa de entrega de sondas na direção direta (d_d) e na direção reversa (d_r). Essas taxas de entrega são, respectivamente, o número de sondas recebidas de A anunciado por B e o número de sondas recebidas de B , no mesmo intervalo de tempo T . O ETX do enlace AB é

$$ETX = \frac{1}{d_d \times d_r}. \quad (3.1)$$

O cálculo do ETX utiliza as taxas de entrega tanto na direção direta quanto na

reversa para considerar a transmissão dos dados e o seu respectivo reconhecimento positivo (*acknowledgement* - ACK), como é feito pelo padrão IEEE 802.11. A rota escolhida é aquela que apresentar a menor soma de ETX ao longo da rota até o destino. É importante ressaltar que enviar sondas em *broadcast* em uma rede com n nós gera um número de mensagens de controle da ordem de $O(n)$. Outra métrica baseada no envio de sondas para calcular a taxa de entrega é proposta por Passos *et al.* [51]. Ao invés de calcular o ETX, a métrica de Perda Mínima (*Minimum Loss* - ML) encontra a rota com a maior probabilidade de entrega fim-a-fim. Portanto, a métrica ML não é aditiva como o ETX, mas multiplicativa. Ela multiplica a taxa de entrega nas direções direta e reversa de todos os enlaces de uma rota para escolher a melhor rota possível. Os autores do ML advogam que o uso de métricas multiplicativas reduz o número de troca de rotas, aumentando o desempenho da rede.

A implementação do ETX apresenta duas deficiências: o envio de pacotes em *broadcast* é normalmente realizado na taxa básica de operação da rede e as sondas possuem um tamanho menor que o tamanho típico dos pacotes de dados. Portanto, exceto se a rede estiver operando em taxas baixas, o desempenho do ETX se torna insatisfatório porque a métrica nem distingue enlaces com diferentes larguras de banda, tampouco considera pacotes com tamanhos maiores, como podem ser os de dados. Para contornar essas deficiências, a métrica Tempo Esperado de Transmissão (*Expected Transmission Time* - ETT) foi proposta por Draves *et al.* [34, 52]. O ETT é o tempo médio que um pacote de dados precisa para ser entregue com sucesso para o próximo salto. Basicamente, o ETT ajusta o ETX levando em conta as taxas de transmissão empregadas em cada enlace e o tamanho do pacote. O cálculo do ETT é uma questão de escolha de implementação. Atualmente, existem duas abordagens principais. Em [34], o ETT é o produto entre o ETX e o tempo médio que um único pacote de dados precisa para ser entregue com sucesso. A expressão que define o ETT é

$$ETT = ETX \times t, \tag{3.2}$$

onde t é o tempo necessário para se enviar um quadro de dados. Para calcular t , os autores dividem um tamanho fixo de um pacote de dados (S) pela banda passante

estimada (B) do meio sem fio ($t = S/B$). Os autores preferem estimar a banda periodicamente a usar as taxas informadas pelo *firmware*. A técnica de par de pacotes é então utilizada para calcular a banda B de cada enlace. Essa técnica é conhecida das redes cabeadas e consiste da transmissão em seqüência de um trem de pacotes para estimar a largura de banda do gargalo da rede. Na implementação para redes sem fio de Draves *et al.*, dois pacotes são enviados seguidos em *unicast*, um pequeno e em seguida um grande, para estimar a banda do enlace para cada vizinho. Cada vizinho mede o intervalo de tempo entre a recepção dos dois pacotes e envia o resultado de volta para a fonte. A largura de banda calculada de cada enlace é então o tamanho do pacote maior da seqüência dividido pelo menor intervalo de recepção recebido. Em uma rede de n nós no qual cada nó possui v adjacências, estimar a banda gera um número de mensagens da ordem de $O(n.v)$. Outra abordagem para calcular o ETT é apresentada em [53, 54]. Os autores estimam a probabilidade de perda considerando que o IEEE 802.11 utiliza quadros de dados e de reconhecimento positivo. A idéia é calcular periodicamente a taxa de perda de dados e de reconhecimentos positivos (ACKs) para cada vizinho. A taxa de perda dos dados é estimada através do envio em *broadcast* de quadros com tamanhos semelhantes aos de quadros de dados típicos. Entretanto, cada pacote é enviado em uma das diferentes taxas de envio de dados definidas pelo padrão IEEE 802.11. Já a taxa de perda de reconhecimentos positivos é estimada enviando em *broadcast* pacotes do mesmo tamanho que quadros de ACK na taxa básica da rede. Essas diferenças se justificam pois os quadros de ACK são normalmente menores que os de dados e o IEEE 802.11 sempre envia quadros de controle na taxa básica da rede. Vale notar que enviar pacotes em *broadcast* em taxas diferentes da básica pode implicar modificações no *firmware*. De acordo com Aguayo *et al.*, o ETT é o inverso do produto entre a vazão máxima verificada (v_{max}) e a probabilidade de entrega de pacotes de ACK na direção reversa (p_{ACK}). Logo, o *ETT* também pode ser igual a

$$ETT = \frac{1}{v_{max} \times p_{ACK}}. \quad (3.3)$$

O cálculo do ETT em uma rede com n nós é de ordem $O(n.m)$, onde m é o número possível de taxas de dados. No IEEE 802.11g, por exemplo, o valor de m é 8, já que essa extensão do IEEE 802.11 pode assumir as taxas de 6, 9, 12, 18, 24, 36, 48

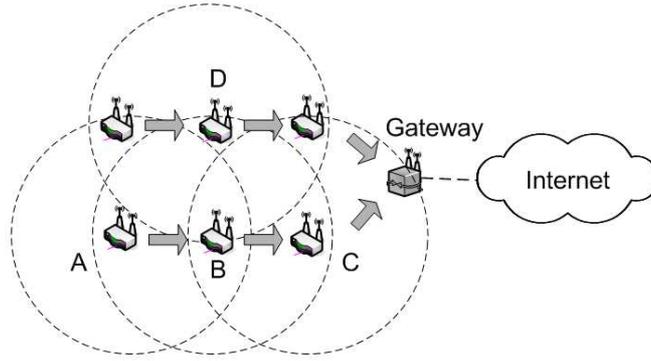


Figura 3.1: Exemplo de casos onde há interferência intra e interfluxos.

e 54 Mb/s. Semelhantemente ao ETX, a rota escolhida é aquela que apresenta a menor soma de ETTs desde a origem até o destino.

Atualmente, abordagens que utilizam otimização entre camadas [24, 25, 55, 56] estão recebendo atenção especial em redes em malha sem fio. Dentre as técnicas disponíveis, o emprego de múltiplos canais é o mais comum. Através de múltiplos canais, é possível aumentar a vazão obtida pelos nós da rede utilizando, simultaneamente, os canais disponíveis não sobrepostos definidos pelo padrão IEEE 802.11. Essa técnica, porém, precisa lidar com dois problemas para se tornar efetiva: a interferência intra e interfluxos. A interferência intrafluxos ocorre quando diferentes nós transmitindo pacotes pertencentes ao mesmo fluxo interferem. A Figura 3.1 ilustra os casos onde há interferência intra e interfluxos. Os nós A, B e C ocasionam interferência intrafluxo, pois são nós que encaminham os dados do mesmo fluxo desde o nó de origem A até o *gateway*. Como os raios de cobertura dos nós A-B-C, representados pelos círculos pontilhados, se sobrepõem, diz-se que ocorre interferência intrafluxo. No caso em que o alcance de um nó interfere na transmissão de outros nós que pertençam a fluxos diferentes, há o que é denominado interferência interfluxo. A interferência interfluxo é a interferência sofrida entre fluxos concorrentes. Um exemplo disso pode ser visto na Figura 3.1 na qual o nó D interfere na transmissão do nó B. Aumentar o número de canais não é trivial se for considerado que os nós devem manter conectividade. No exemplo da Figura 3.2, nota-se que os nós A e B não conseguem encaminhar seus dados até C porque o único nó intermediário é o nó I que está operando em um canal diferente do canal escolhido por A e B. Logo, a rede não está conectada. A métrica Tempo Esperado de Transmissão Cumulativo

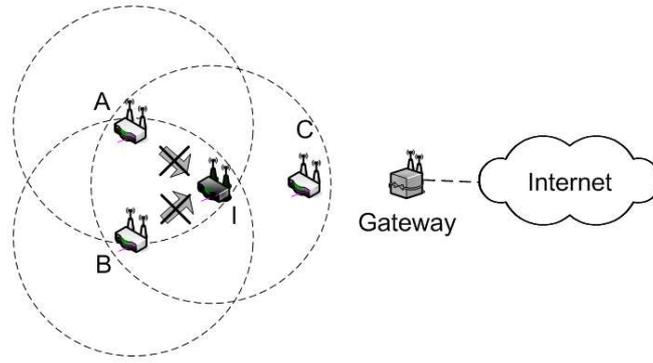


Figura 3.2: Exemplo de uma rede desconectada devido ao uso de múltiplos canais.

Ponderado (*Weighted Cumulative ETT* - WCETT) [34] altera o ETT para também considerar interferência intrafluxo. Essa métrica é a soma de dois componentes: o atraso fim-a-fim e a diversidade de canais. Um parâmetro ajustável é utilizado para combinar ambos os componentes ou priorizar um deles. Diferente do ETX e do ETT, o WCETT é uma métrica fim-a-fim. Portanto, seu resultado já é o valor calculado pela métrica para a rota e não para cada enlace. Essa métrica calcula valores fim-a-fim porque deve considerar todos os canais utilizados ao longo da rota para levar em conta a interferência intrafluxo. Entretanto, o WCETT não garante caminhos mais curtos e não evita interferência interfluxo [57]. Protocolos de roteamento baseados em estado do enlace necessitam de rotas de custos mínimos para serem livres de laços de roteamento. Além disso, não evitar interferência interfluxo pode levar o WCETT a escolher rotas em áreas congestionadas. A métrica MIC (*Metric of Interference and Channel-switching*) leva em conta esses problemas [57]. Primeiramente, cada nó considera o número de nós da vizinhança que possuem potencial para interferir em sua comunicação. Assim, a métrica estima a interferência interfluxo. Adicionalmente, o MIC usa um recurso de nós virtuais para garantir cálculo de rotas com custo mínimo. A métrica MIC também calcula seu valor a partir da métrica ETT.

Um problema crítico em redes sem fio é a rápida variação da qualidade dos enlaces. As métricas baseadas em valores médios calculadas sobre janelas de tempo, como o ETX, podem não refletir as variações dos enlaces ou gerar uma sobrecarga de controle excessiva. Além disso, métricas baseadas em médias podem não se adaptar tão rápido quanto o necessário às mudanças das condições do meio. Principalmente

em ambientes fechados, esse problema é ainda mais grave devido ao número de obstáculos, dispositivos sem fio interferentes, pessoas caminhando etc. que aumentam muito o dinamismo das condições dos enlaces sem fio. Para lidar com isso, foram propostas as métricas mETX (*modified ETX*) e ENT (*Effective Number of Transmissions*) [48]. Essas métricas consideram o desvio padrão além da variação média da qualidade dos enlaces. O objetivo principal é projetar as variações da qualidade do meio físico nas métricas de roteamento.

A métrica mETX é também calculada através do envio de sondas em *broadcast*. A diferença entre o mETX e o ETX é que ao invés de considerar perda de sondas, o mETX trabalha no nível de bit. A métrica mETX calcula a probabilidade de erro de bit (*Bit Error Rate* - BER) usando a posição do bit corrompido na sonda e a dependência desse erro nas transmissões seguintes. Isso é possível porque as sondas são compostas por uma seqüência conhecida de bits. A métrica ENT é uma alternativa ao mETX que mede o número sucessivo de retransmissões por enlace considerando a variância. A métrica ENT também envia sondas em *broadcast* e limita o cálculo de rotas aos enlaces que mostram um número aceitável de retransmissões de acordo com as requisições das camadas superiores. Se um enlace possui um número esperado de transmissões superior ao tolerado por um protocolo de camada superior, por exemplo o TCP, o ENT exclui esse enlace do cálculo de rotas atribuindo métrica infinita ao enlace. A métrica DBETX (*Distribution-Based Expected Transmission Count*) leva em conta a variação da qualidade dos enlaces considerando o desvanecimento do canal sem fio [58]. Para calcular o DBETX, cada nó estima a função de densidade de probabilidade da relação sinal-ruído do canal e, de acordo com a modulação utilizada, obtém a taxa de erro por pacote. Além disso, o DBETX considera o número máximo de retransmissões na camada de enlace para selecionar uma rota. Caso o número estimado de retransmissões de um enlace ultrapasse o número máximo permitido, esse enlace é excluído da topologia temporariamente. Outro exemplo é a métrica iAWARE (*Interference Aware Routing Metric*) [59]. Essa métrica usa a relação sinal-ruído (*Signal to Noise Ratio* - SNR) e a relação sinal-interferência-ruído (*Signal to Interference and Noise Ratio* - SINR) para continuamente avaliar a interferência da vizinhança nas métricas de roteamento. A métrica iAWARE estima o tempo médio que o meio sem fio está

Tabela 3.1: Características principais das métricas de roteamento.

Métrica	Ciente da qualidade	Taxa de dados	Tam. do pacote	Interf. intra-fluxo	Interf. inter-fluxo	Instabilidade do meio
Hop	×	×	×	×	×	×
ETX	✓	×	×	×	×	×
ML	✓	×	×	×	×	×
ETT	✓	✓	✓	×	×	×
WCETT	✓	✓	✓	✓	×	×
MIC	✓	✓	✓	✓	✓	×
mETX	✓	✓	✓	×	×	✓
ENT	✓	✓	✓	×	×	✓
DBETX	✓	✓	✓	✓	✓	✓
iAWARE	✓	✓	✓	✓	✓	✓

ocupado devido à transmissão de cada vizinho com potencial de interferir. Quanto maior a interferência, maior é o valor da métrica. Portanto, diferente do ENT e do mETX, o iAWARE considera interferência intra e interfluxo, instabilidade do meio e tempo de transmissão de dados.

Apesar de existir um número crescente de métricas de roteamento, um consenso sobre uma determinada métrica ainda não foi atingido. Geralmente, o número de características relacionadas a desempenho ou qualidade de serviço de uma métrica é inversamente proporcional a sua simplicidade. Até hoje, a maior parte dos protocolos de roteamento prefere simplicidade, por isso empregam o ETX ou o ETT. No escopo deste trabalho, é importante observar que as métricas de roteamento apresentadas introduzem sobrecarga de controle durante o envio de sondas. Essa característica é mencionada mais adiante. A Tabela 3.1 resume as principais características das métricas de roteamento apresentadas.

3.2.2 Protocolos

Os protocolos de roteamento ad hoc normalmente usam uma de três estratégias: reativa, pró-ativa ou híbrida. Na estratégia reativa, assim que um nó tem um pacote de dados para enviar, ele faz uma requisição de rota para o destino pretendido. Se um nó não possui pacote de dados para enviar a um determinado destino, ele jamais requisita uma rota para esse nó. A estratégia pró-ativa opera como nas redes cabeadas. Os nós mantêm rotas para cada possível destino da rede. Na estratégia híbrida, as estações realizam requisições periódicas de rotas para os destinos mais freqüentes.

Muitos protocolos de roteamento de redes em malha sem fio usam estratégias semelhantes às utilizadas pelas redes ad hoc para calcular rotas. Entretanto, elas são adaptadas às peculiaridades das redes em malha sem fio e usam uma das métricas cientes da qualidade apresentadas na Seção 3.2.1. Nesta tese, é proposta uma taxonomia para os principais protocolos das redes em malha sem fio [28]. Os protocolos são divididos em quatro classes: *protocolos legados das redes ad hoc*, *protocolos com controle de inundação*, *protocolos cientes do tráfego* e *protocolos oportunistas*. Esses protocolos diferem principalmente nos seus procedimentos de descoberta e manutenção de rotas. Nas redes em malha sem fio, a maioria dos protocolos de roteamento considera que a rede é somente composta por nós pertencentes ao *backbone* sem fio.

Protocolos legados das redes ad hoc

Os protocolos legados das redes ad hoc adaptam os protocolos de roteamento oriundos das redes ad hoc para o caso em malha. Além de utilizar métricas cientes da qualidade ao invés da métrica número de saltos, procura-se alterar os procedimentos de requisição e manutenção de rotas, com o objetivo de utilizar características das redes em malha sem fio. Por exemplo, é possível reduzir a sobrecarga de controle considerando que o destino preferencial da rede é o *gateway*, ou portal da malha. O protocolo LQSR (*Link Quality Source Routing*) [34] é um exemplo. O LQSR combina roteamento pró-ativo baseado em estado do enlace com a estratégia reativa das redes ad hoc. O LQSR é fundamentalmente um protocolo de roteamento baseado em estado do enlace e usa uma visão completa da topologia da rede para realizar

cálculo de menor caminho. Porém, o LQSR usa procedimento de descoberta de rotas como protocolos reativos para reduzir a sobrecarga de roteamento, que pode se tornar alta devido às freqüentes instabilidades do meio. Como a maior parte do tráfego é encaminhada na direção do *gateway* da rede, novos procedimentos de descoberta de rotas só são realizados quando a rota até o *gateway* for perdida ou quando houver necessidade de se comunicar com algum outro nó do *backbone*. Durante a descoberta de rotas, o LQSR obtém informações atualizadas sobre do estado dos enlaces atravessados, reduzindo a periodicidade das atualizações das métricas de roteamento. O protocolo SRcRR [53] é um outro exemplo de protocolo legado das redes ad hoc. Esse protocolo somente utiliza um procedimento de descoberta de rotas semelhante ao dos protocolos reativos para atualizar as informações de roteamento dos enlaces atravessados. Portanto, o SrcRR reduz ainda mais a sobrecarga de controle, mas pode calcular rotas com um visão reduzida da rede. Tanto o LQSR quanto o SrcRR utilizam o ETX e implementam procedimentos de descoberta de rotas baseados nos procedimentos do protocolo DSR (*Dynamic Source Routing*) [60]. Por conseguinte, o LQSR e o SrcRR utilizam roteamento por fonte. O protocolo *Mesh Distance Vector* (MeshDV) [61, 62] trata a mobilidade dos clientes das redes em malha e não somente considera os nós do *backbone*, como o LQSR e o SrcRR. Para isso, todos os nós do *backbone* mantêm uma tabela com os endereços IP dos clientes diretamente conectados e outra com os endereços IP dos clientes conectados a outros nós do *backbone*. O MeshDV executa o DSDV (*Destination-Sequenced Distance-Vector*) [63] no *backbone* e pode usar duas métricas, o número de saltos ou a taxa mínima de transmissão utilizada pelos enlaces da rota [64, 65, 66].

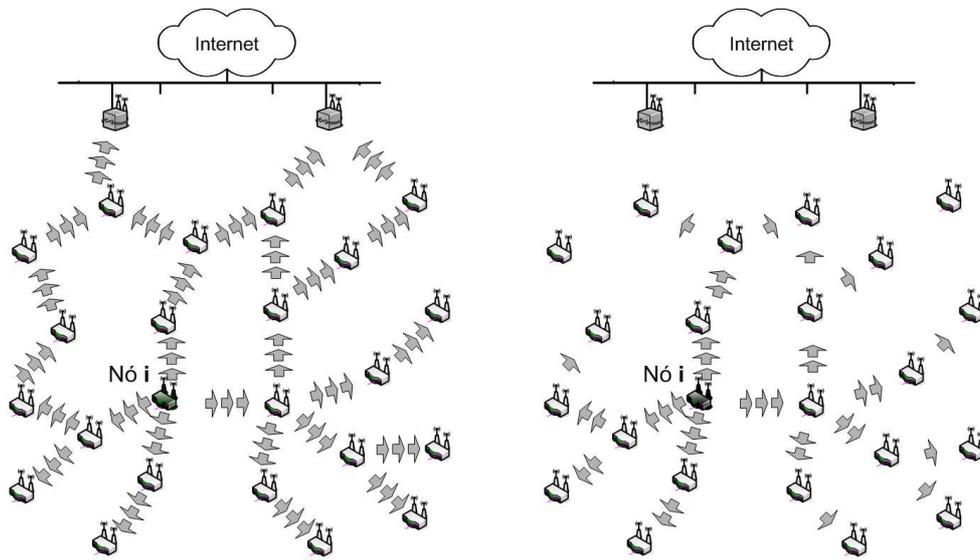
Um problema em aberto em redes sem fio é o emprego de informações advindas da camada física para aumentar a eficiência dos protocolos de roteamento. Para isso, é necessário o emprego de métodos de otimização entre camadas. O *Multi-Radio* LQSR (MR-LQSR) [34] é um exemplo de protocolo que utiliza esse tipo de otimização. O MR-LQSR adapta o LQSR para operar sobre múltiplos canais e múltiplas interfaces. O MR-LQSR utiliza a métrica de roteamento WCETT, apesar do uso dessa métrica não garantir caminhos de custo mínimo, como discutido na Seção 3.2.1. O MR-LQSR não introduz laços de roteamento pois utiliza roteamento por fonte. Outro exemplo é o protocolo DOLSR (*Directional Optimized Link-State Routing*) [67] que

emprega antenas direcionais para aumentar a eficiência do roteamento em redes em malha sem fio. O DOLSR utiliza métricas como o número de saltos e o ETX.

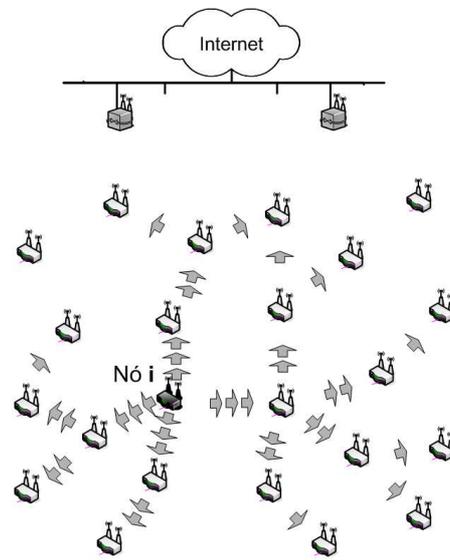
Protocolos com controle de inundação

A principal característica dos protocolos com controle de inundação é a utilização de algoritmos para reduzir a sobrecarga de controle. Inundar a rede com atualizações de roteamento ou com requisições de rota pode resultar em problemas de escalabilidade, especialmente se forem consideradas as freqüentes mudanças nas condições do meio sem fio e a escassez de banda passante. Este trabalho identifica duas abordagens básicas que podem ser adotadas para reduzir a sobrecarga de controle de roteamento introduzida pelo método clássico de inundação, visto na Figura 3.3(a). A Figura 3.3(b) ilustra o método de inundação temporal, comum em protocolos pró-ativos, no qual a periodicidade é ajustada de acordo com a distância do nó fonte. A Figura 3.3(c), por outro lado, mostra o método de inundação espacial, no qual os nós mais distantes recebem informações menos precisas ou menos detalhadas do nó fonte. Na prática, a maioria dos protocolos de roteamento se baseia em informações adquiridas em um escopo local. Os protocolos assumem que inundar a rede não é eficiente porque a maioria das comunicações nas redes sem fio ocorre entre nós próximos. Portanto, não é necessário enviar mensagens de controle para nós distantes com a mesma freqüência que para os nós próximos durante um processo de atualização de métricas ou requisição de rota. Outra forma de reduzir a sobrecarga de controle é limitar o número de nós responsáveis por inundar a rede, evitando redundâncias. Esses protocolos executam algoritmos para encontrar o conjunto mínimo de nós necessários para que as informações de roteamento alcancem todos os possíveis nós da rede.

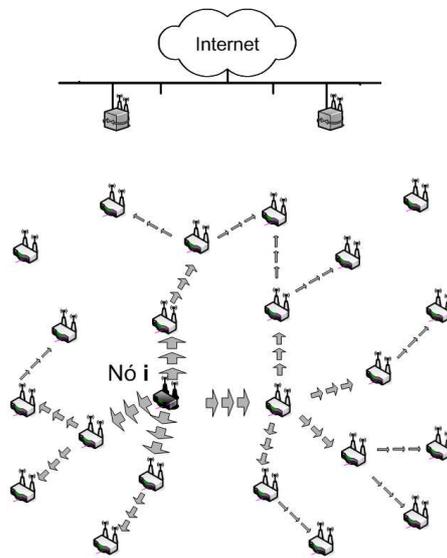
O Fisheye [68] foi um dos primeiros protocolos propostos para redes ad hoc que limita a disseminação dos pacotes de controle somente aos vizinhos. Para isso, o tempo de vida (*Time-To-Live* - TTL) das mensagens de controle é ajustado conforme o número de nós da rede que se pretende alcançar. Quanto menor o TTL, menor é o número de nós que recebem a mensagem. Alguns protocolos foram desenvolvidos para as redes em malha seguindo o mesmo princípio do Fisheye. O protocolo LOLS (*Localized On-demand Link State*) [69, 70] atribui um custo de longo-prazo



(a) Inundação clássica.



(b) Inundação temporal.



(c) Inundação espacial.

Figura 3.3: Métodos de inundação possíveis iniciados pelo nó i .

e um custo de curto-prazo aos enlaces. Os custos de longo-prazo e de curto-prazo representam, respectivamente, o custo médio e o custo instantâneo do enlace. Para reduzir a sobrecarga de controle de roteamento, os custos de curto-prazo são enviados com uma frequência maior aos vizinhos, enquanto os custos de longo-prazo são enviados em frequência menor. O protocolo LOLS calcula rotas usando a ETX ou a ETT. Outro exemplo típico é o protocolo MMRP (*Mobile Mesh Routing Protocol*) [71, 72, 73] desenvolvido pela MITRE Corporation [74]. O MMRP atribui idade às suas mensagens de roteamento assim como o protocolo de roteamento utilizado na Internet OSPF (*Open Shortest Path First*) [75]. Portanto, sempre ao enviar uma mensagem de controle de roteamento, o nó subtrai a idade da mensagem por uma estimativa do tempo necessário para encaminhá-la. Assim que a idade da mensagem expira, a mensagem é descartada, impedindo seu encaminhamento. O MMRP não especifica a métrica de roteamento a ser utilizada. O protocolo OLSR (*Optimized Link State Routing*) [76] foi originalmente projetado para redes sem fio ad hoc. O OLSR foi adaptado para usar o ETX como métrica de roteamento nas redes em malha. Esse protocolo pode também ser considerado como legado das redes ad hoc, porém, ele utiliza MultiPoint Relays (MPRs) que é uma técnica para controle de inundação. O OLSR limita o número de nós encarregados por encaminhar informações de roteamento para diminuir o número de mensagens redundantes. Logo, cada nó seleciona o seu conjunto de MPRs, que é composto pelos nós escolhidos para encaminhar informações de roteamento originadas no nó seletor. O conjunto de MPRs é composto pelo número mínimo de vizinhos de um salto capazes de alcançar todos os vizinhos de dois saltos. Há ainda uma implementação adicional do OLSR que emprega a métrica ML [51] e outra que implementa a métrica ETT [77, 78]. O protocolo OFLSR (*Optimized Fisheye Link-State Routing*) [79] tenta reduzir ainda mais a carga de controle do OLSR. O OFLSR combina o conjunto MPR do OLSR com o controle de disseminação por TTL do protocolo Fisheye. No OFLSR, os nós do conjunto MPR encaminham as mensagens de controle de roteamento com o campo TTL ajustado.

Foi desenvolvida durante esta tese uma extensão ao protocolo de roteamento OLSR. O protocolo OLSR original possui somente as métricas número de saltos e ETX implementadas. Neste trabalho, a métrica ETT foi adicionada ao OLSR

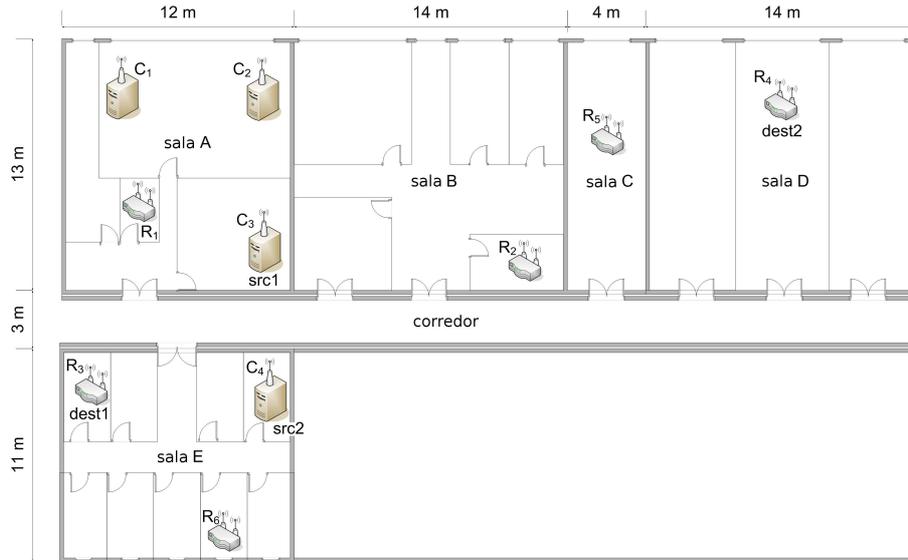
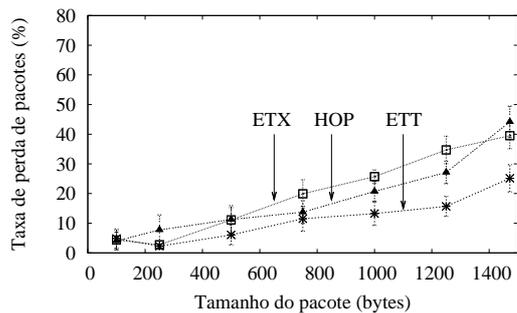
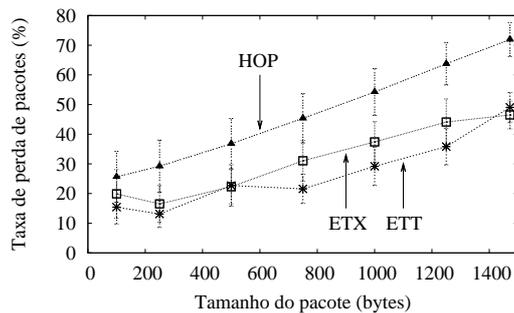


Figura 3.4: Rede de testes do GTA.

de acordo com a abordagem de Draves *et al.*. Para isso, desenvolveu-se um *plugin* para o OLSR com o objetivo de tornar a implementação a mais portátil possível. Assim, para utilizar a métrica ETT no OLSR, são necessárias apenas alterações de configuração [80]. Os experimentos realizados na rede de testes *indoor* do laboratório GTA demonstraram que o ETT apresenta de fato melhor desempenho que as métricas ETX e número de saltos (HOP) [77, 78]. A Figura 3.4 ilustra a rede de testes utilizada, enquanto as Figuras 3.5, 3.6 e 3.7 mostram os resultados obtidos respectivamente para a taxa de perda de pacotes, tempo de ida e volta (*Round-Trip-Time* - RTT) e comprimento de rotas. Foram realizados experimentos através do disparo de seqüências de *pings*, com o par origem-destino C_3-R_3 e depois com o par C_4-R_4 . Assim, apenas um par na rede estava se comunicando por vez. Observa-se que tanto a taxa de perda quanto o tempo de ida e volta obtidos com a métrica ETT são inferiores aos casos onde o ETX ou o HOP são usados. Isso ocorre, pois os enlaces escolhidos pelo ETT são de melhor qualidade, o que está refletido no comprimento das rotas. É conhecido que enlaces mais curtos possuem provavelmente taxas de transmissão mais elevadas e taxas de perdas menores. Em distâncias curtas, a relação sinal-ruído tende a ser mais bem preservada já que a atenuação do sinal é inferior [49, 50].

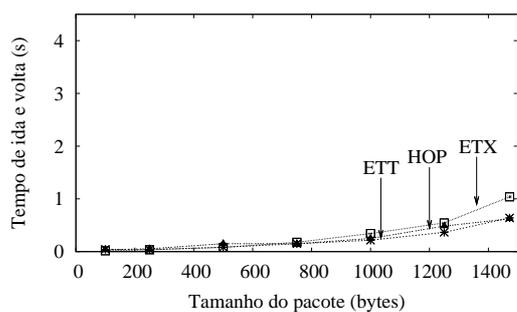


(a) Par C₃-R₃.

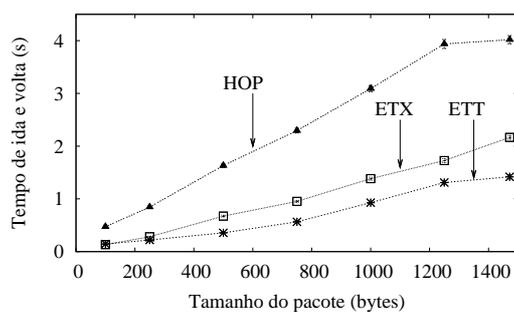


(b) Par C₄-R₄.

Figura 3.5: Taxa de perda de pacotes.

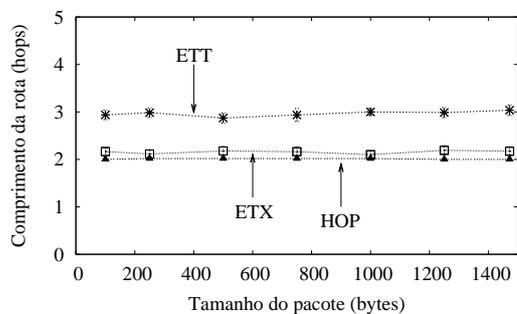


(a) Par C₃-R₃.

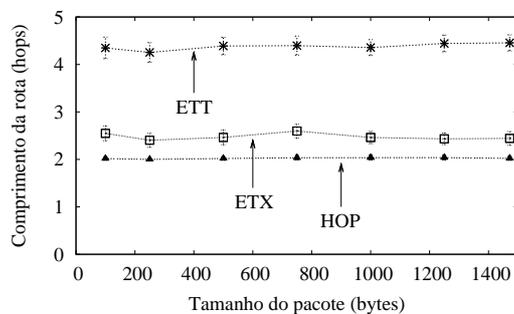


(b) Par C₄-R₄.

Figura 3.6: Tempo de ida e volta.



(a) Par C₃-R₃.



(b) Par C₄-R₄.

Figura 3.7: Comprimento da rota.

Protocolos cientes do tráfego

Os protocolos cientes do tráfego, ou protocolos baseados em árvore, se beneficiam da matriz de tráfego recorrente em redes em malha sem fio. Eles assumem que o acesso à rede cabeada de banda larga é a aplicação mais comum e, portanto, consideram que a topologia da rede é semelhante a uma árvore. Um exemplo é o protocolo AODV-ST (*Ad hoc On-demand Distance Vector-Spanning Tree*) [81]. Esse protocolo é a adaptação do protocolo reativo para redes ad hoc AODV (*Ad hoc On-demand Distance Vector*) [82]. No AODV-ST, o *gateway* periodicamente envia requisições de rota para todos os nós da rede para manter sua tabela de roteamento atualizada. Logo, o AODV-ST mantém uma árvore onde o *gateway* é a raiz. As comunicações que não incluem o *gateway* funcionam como no AODV original. O AODV-ST suporta tanto o ETX quanto o ETT. Raniwala e Chiueh também propuseram um protocolo de roteamento ciente de tráfego em [83]. Eles propuseram um algoritmo de roteamento baseado no protocolo *spanning tree* das redes cabeadas. O procedimento de manutenção de rotas é feito com mensagens de JOIN e LEAVE. Eles utilizam a métrica número de saltos e outras métricas para balanceamento de carga, não especificamente projetadas para as redes em malha sem fio.

Protocolos de roteamento oportunistas

Os protocolos de roteamento oportunistas exploram o fato de que as transmissões em radiofrequência são realizadas em difusão por natureza. Assim, eles escolhem sob demanda o próximo salto que oferece a melhor vazão, por exemplo. Os protocolos de roteamento clássicos calculam uma seqüência de saltos até o destino antes de enviar um pacote de dados, utilizando roteamento salto-a-salto ou pela fonte. No caso de falhas de enlaces, retransmissões sucessivas são realizadas na camada de enlace até que o pacote de dados seja corretamente encaminhado ao próximo salto ou até que o número máximo de retransmissões seja alcançado. Essa abordagem pode provocar um grande atraso e um desempenho pobre, pois os enlaces sem fio precisam de algum tempo para se recuperar de falhas. Os protocolos oportunistas, por outro lado, garantem que os dados são sempre encaminhados uma vez que haja pelo menos um próximo salto disponível. Além disso, a rota escolhida provavelmente

utiliza os enlaces de melhor qualidade, considerando as variações de curto-prazo.

O protocolo ExOR combina encaminhamento de pacotes com funcionalidades da camada de enlace como, por exemplo reconhecimento de recepção por salto [84]. Os nós enviam pacotes agregados em *broadcast* sem nenhum cálculo prévio de rota. Os pacotes são transmitidos agregados para reduzir a sobrecarga do protocolo, o que pode levar a subutilização dos recursos da rede. Além disso, enviar pacotes de dados em *broadcast* aumenta as chances de sucesso, pois é preciso que apenas um nó intermediário tenha escutado a transmissão. Entretanto, enviar em *broadcast* não garante que os pacotes tenham sido de fato recebidos, pois não há reconhecimento positivo (ACK) nesse caso. Logo, um mecanismo adicional é necessário para indicar corretamente a recepção de um pacote de dados. Entre os nós intermediários que escutam a transmissão, apenas um retransmite por vez. O nó fonte define uma lista de encaminhamento e adiciona a lista ao cabeçalho dos pacotes de dados. Essa lista contém os endereços dos vizinhos ordenados por prioridade de encaminhamento. Os nós vizinhos são organizados na lista de acordo com a proximidade até o destino, calculada a partir de uma métrica semelhante ao ETX. A métrica usada pelo ExOR somente considera a taxa de perda na direção direta, pois não há ACK na direção reversa. Ao receber um pacote de dados, o nó intermediário verifica a lista de encaminhamento. Caso o seu endereço esteja listado, ele espera a recepção completa de todo o agregado de pacotes. É possível, entretanto, que um nó não receba o agregado de pacotes inteiro. Para evitar esse problema, o ExOR opera como se segue. O nó com prioridade mais alta que recebeu pacotes os encaminha e indica para os nós com prioridade inferior quais os pacotes já foram enviados. Os nós com prioridade mais baixa transmitem, portanto, apenas os pacotes restantes, evitando o envio de pacotes duplicados. A transmissão é realizada até que o nó destino indique a recepção.

O protocolo ROMER (*Resilient Opportunistic MESH Routing*) [85] foca principalmente em robustez e alta vazão usando encaminhamento por múltiplos percursos. O ROMER combina as melhores rotas de longo-prazo, menor caminho ou latência mínima com ganhos oportunistas feitos sob-demanda para prover rotas robustas e para lidar com variações de curto-prazo na qualidade do meio. O protocolo ROMER calcula rotas de longo-prazo e oportunisticamente as expande ou as encurta

Tabela 3.2: Protocolos de roteamento e respectivas métricas.

Classe	Protocolos	Métricas
Legados das redes ad hoc	LQSR	ETX
	SrcRR	ETX
	MR-LQSR	WCETT
	MeshDV	#saltos ou taxa física
	DOLSR	#saltos ou ETX
Controle de inundação	LOLS	ETX ou ETT
	MMRP	Indefinido
	OLSR	#saltos, ETX, ML ou ETT
Cientes do tráfego	AODV-ST	ETX ou ETT
	Protocolo do Raniwala <i>et al.</i>	#saltos ou métricas de balanceamento de carga
Oportunísticos	ExOR	ETX unidirecional
	ROMER	Número de saltos ou Atraso

durante a sua utilização para explorar totalmente possíveis enlaces com qualidade momentaneamente superior. Essas rotas de longo-prazo são calculadas usando o número mínimo de saltos ou o menor atraso médio. Diferente do ExOR, o ROMER transmite na base de pacotes para possibilitar uma reação mais rápida às variações do meio. A rota com a maior vazão é escolhida de acordo com a taxa máxima de camada física como indicada pela camada de enlace.

A Tabela 3.2 apresenta os principais protocolos de roteamento de acordo com a taxonomia proposta e as principais métricas de roteamento utilizadas por cada um. É importante observar que os protocolos de roteamento possuem características de outras classes e que a taxonomia proposta neste trabalho não é a única possível.

O protocolo de roteamento proposto neste trabalho pode ser classificado como um protocolo legado das redes ad hoc, pois se baseia no OLSR; como um protocolo que realiza controle de inundação e ainda é ciente do tráfego, pois utiliza a premissa de convergência de carga nos enlaces próximos ao *gateway* para reduzir a sobrecarga

de controle. Além disso, observa-se na Seção 3.2.1 que muitas das métricas propostas para as redes em malha fazem uso de sondas para avaliar a qualidade dos enlaces. A inserção de sondas aumenta o controle da rede, o que reforça a necessidade de novos métodos de redução de carga de controle. O protocolo proposto nesta tese considera este problema, conforme é visto no Capítulo 5.

Capítulo 4

RLF: *Route-Length-based Fairness*

Neste capítulo, é apresentado o mecanismo de justiça proposto nesta tese, o *Route-Length-based Fairness* (RLF) que tem como principal objetivo distribuir de forma balanceada a vazão máxima alcançável por nó nas redes em malha sem fio. Resumidamente, uma maior prioridade é atribuída durante o acesso ao meio aos pacotes gerados por nós mais distantes do *gateway*. A distância de um nó até o *gateway* é calculada a partir de informações obtidas da camada de rede. Em seguida, o mecanismo proposto é descrito e analisado.

4.1 Premissas

Neste trabalho, assume-se que todo usuário deve receber nível de serviço semelhante da rede. Logo, os recursos devem ser igualmente distribuídos entre os usuários conectados. Adicionalmente, é considerado que os roteadores do *backbone* agregam o tráfego dos usuários da rede e que cada roteador oferece uma quantidade equivalente de tráfego vindo dos seus clientes. Portanto, a distribuição de recursos é realizada entre os roteadores do *backbone*, ao invés de entre os usuários.

A topologia analisada é uma cadeia de nós como vista na Figura 4.1. Uma rede em malha pode ser aproximada por uma coleção de cadeias que não se interferem [18]. Esse cenário, apesar de simplificar o problema, é usado para destacar o efeito dos múltiplos saltos na distribuição de recursos. Além disso, foi considerado que todos

os enlaces da rede têm a mesma capacidade. Para considerar enlaces com diferentes capacidades, no lugar do recurso vazão, o recurso tempo de transmissão poderia ser tratado [21], o que não é o objetivo deste trabalho.

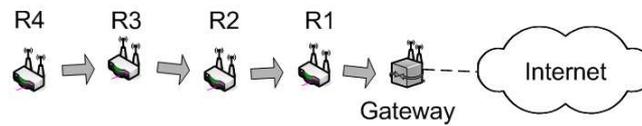


Figura 4.1: Exemplo de uma topologia em cadeia com um *gateway* e quatro nós roteadores (R1 a R4).

Outra premissa é que o RLF só pode ser utilizado em casos onde o protocolo de rede emprega roteamento pela fonte ou possui conhecimento de toda a topologia da rede. Essa premissa é necessária para se obter o comprimento da rota entre a origem do pacote e o destino. Utilizar roteamento pela fonte é mais conveniente para o mecanismo proposto, visto que a rota completa já está listada no cabeçalho do pacote. Entretanto, o RLF pode ser utilizado facilmente em protocolos baseados em estado do enlace. Nesses protocolos, cada roteador conhece o mapa completo da topologia da rede. Portanto, calcular o comprimento da rota de qualquer nó para qualquer outro é viável e só depende dos nós armazenarem o caminho completo entre eles e os outros nós da rede. O problema nesse caso é que o comprimento calculado por um nó pode não representar a rota real percorrida pelo pacote, já que os mapas dos nós podem não estar sincronizados. Já em protocolos baseados em vetores de distância, a adaptação do RLF é mais complexa porque os roteadores conhecem apenas a sua vizinhança e não têm informações da topologia completa. Nesse último caso, a aplicação do RLF necessita de maior investigação. Uma possível direção é armazenar a distância para cada nó da rede em uma memória cache. Essa distância poderia ser obtida a partir do campo TTL (*Time-To-Live*) dos pacotes recebidos de cada um dos nós da rede. Para tal, seria necessário que o valor inicial do TTL fosse sempre o mesmo para que a diferença entre ele e o TTL do pacote recebido represente o número de saltos percorridos. Essa solução assume que a rota entre a origem-destino e vice-versa é composta pelo mesmo número de saltos.

No mecanismo proposto são utilizadas múltiplas filas de transmissão. O obje-

tivo é evitar a exaustão dos recursos da rede por apenas um nó tratando de forma diferenciada os pacotes oriundos de rotas diferentes. Assim, os pacotes são enfileirados de acordo com o comprimento de suas rotas, evitando contenção entre pacotes originados localmente e pacotes recebidos de outros nós. As múltiplas filas são usadas para proteger os nós bem comportados da exaustão de recursos, causada por nós egoístas. Além disso, colocar pacotes de prioridades diferentes na mesma fila tornaria o mecanismo ineficiente, visto que um pacote de prioridade maior teria que esperar um de prioridade menor ser transmitido primeiro. Uma abordagem alternativa é utilizar a extensão para qualidade de serviço do padrão IEEE 802.11, o IEEE 802.11e [31], pois ele originalmente já implementa múltiplas filas para lidar com diferentes prioridades. Contudo, o número de filas definido pelo IEEE 802.11e é limitado a quatro, o que não seria apropriado para topologias com roteadores a mais de quatro saltos do *gateway*. Além disso, as prioridades são atribuídas numa camada mais elevada de acordo com as requisições da aplicação.

A implementação do mecanismo proposto exige algumas modificações em *firmware* para que informações do roteamento sejam obtidas na camada MAC e para que parâmetros também da camada MAC sejam alterados dinamicamente.

4.2 Operação do RLF

Este trabalho propõe um mecanismo para aumentar a justiça em redes sem fio de múltiplos saltos. Ao invés de atribuir prioridade a nós, o mecanismo RLF (*Route Length based Fairness*) atribui prioridade a pacotes, de acordo com o comprimento de rota até o destino. Essa prioridade é atribuída ajustando o tamanho da janela de contenção do pacote na camada MAC. Quanto mais longa for a rota, maior é a prioridade atribuída. Uma característica importante do mecanismo proposto é que não há necessidade de troca de mensagens de controle, que introduziria sobrecarga; nem tampouco é realizado cálculo de vazão máxima permitida, o que demandaria algoritmos adicionais [18, 21].

Ao receber um pacote de dados, os nós intermediários procuram primeiro a informação sobre o comprimento da rota no cabeçalho do pacote da camada de rede. Após analisar o cabeçalho, o pacote é enfileirado conforme o comprimento de

sua rota. Caso fosse usado um protocolo de roteamento que possui conhecimento da topologia da rede, o comprimento da rota poderia ser o comprimento da rota do nó intermediário até a fonte mais o comprimento da rota do nó intermediário até o destino. O RLF usa uma fila por comprimento de rota. Por conseguinte, dois nós a um mesmo número de saltos do *gateway* têm seus pacotes colocados na mesma fila, em um nó intermediário. Cada fila usa o algoritmo FIFO/Droptail, e as diferentes filas são servidas em *Round-Robin*.

No padrão IEEE 802.11, antes de encaminhar um pacote, todo nó precisa esperar um intervalo de tempo aleatório definido a partir do tamanho de sua janela de contenção. Portanto, priorizar um pacote significa diminuir esse tempo de espera, para que o nó privilegiado acesse o meio antes dos outros.

No mecanismo proposto, o nó reduz de uma parcela $f_{RLF}(l)$ o tamanho da janela de contenção do pacote a ser encaminhado, como visto na Expressão 4.1. A função $f_{RLF}(l)$ é então responsável por privilegiar os pacotes originados em nós distantes, os pacotes de vida longa, ao ajustar o tamanho da janela de contenção conforme o comprimento da rota do pacote. Quanto maior o comprimento da rota, menor é o tamanho da janela de contenção, privilegiando o pacote no acesso ao meio. Na Expressão 4.1, CW_{novo} é o tamanho da janela de contenção recalculado para o pacote sendo encaminhado, CW_i é o tamanho da janela de contenção atual como definido pelo padrão IEEE 802.11 e l é o comprimento da rota do pacote. No protocolo MAC do padrão IEEE 802.11, $CW_{i+1} = 2 \times CW_i + 1$, onde i é o número de retransmissões de um único pacote e $CW_0 = CW_{min}$ é o tamanho mínimo da janela de contenção. Além disso, quando CW_i alcança o tamanho máximo, CW_{max} , ele permanece nesse tamanho até ocorrer uma transmissão bem sucedida. O valor do CW_{novo} é igual a

$$CW_{novo} = CW_i - f_{RLF}(l), \quad (4.1)$$

onde $f_{RLF}(l)$ é dada por

$$f_{RLF}(l) = a \times \left\lfloor \frac{CW_i}{CW_{min}} \right\rfloor \times l. \quad (4.2)$$

Na Expressão 4.2, a é o *índice de agressividade*. Esse índice é usado para ajustar o nível de prioridade atribuído aos pacotes de vida longa. Um maior *índice de agressividade* aumenta a prioridade do pacote. Considerar a proporção entre CW_i e CW_{min}

aumenta a faixa de valores da função $f_{RLF}(l)$, acentuando ainda mais a prioridade dos pacotes de vida longa originados em nós distantes quando não ocorre uma transmissão bem sucedida. Na Seção 4.3, é demonstrado que a redução do tamanho da janela de contenção dos pacotes de vida longa representa um compromisso entre prioridade e vazão agregada da rede.

Uma importante observação é que a função $f_{RLF}(l)$ poderia considerar o número de saltos já percorridos ou o número de saltos a percorrer ao invés do tamanho completo da rota. Considerar o número de saltos já percorridos tem uma implementação direta nos protocolos de roteamento independente do algoritmo utilizado para o cálculo de rotas. É apenas necessário que a sub-camada MAC tenha acesso ao TTL (*Time-To-Live*) do pacote IP, assumindo que o TTL inicial seja conhecido, para saber o número de saltos percorrido pelo pacote. Essa abordagem, entretanto, não privilegia nós que estejam a números de saltos diferentes do *gateway*, caso eles sejam fontes de tráfego e compitam pelo meio. A outra opção, considerar o número de saltos que faltam para chegar no *gateway*, não privilegia os pacotes de vida longa em nós próximos do *gateway* e também tem limitações de implementação em protocolos baseados em vetor de distância. Outra importante observação importante é que o novo valor da janela de contenção deve ser calculado imediatamente antes de transmitir cada quadro. Como o valor da janela de contenção atual (CW_i) é utilizado em f_{RLF} , o RLF deve calcular o valor novo da janela de contenção a cada transmissão porque o valor de f_{RLF} não é constante a cada retransmissão. Isso representa uma maior complexidade de implementação que é diferente da maneira como o IEEE 802.11e funciona, por exemplo. No IEEE 802.11e, cada fila possui pré-definido o valor da janela de contenção mínima bem como outros parâmetros da sub-camada MAC. Uma alternativa para simplificar a implementação seria privilegiar os pacotes de vida longa utilizando sempre valores definidos pelo padrão IEEE 802.11 para a janela de contenção mínima. Ao invés de reduzir a janela de contenção de uma parcela através de uma expressão como f_{RLF} , cada fila teria um valor como 31, 63, 127, etc. fixo. Assim, a prioridade seria mantida e a implementação seria simples.

Supondo uma cadeia de cinco nós, como mostrada na Figura 4.1, quando o nó R4 transmite para o *gateway*, a rota pela fonte é $R4, R3, R2, R1, GW$. Ao receber o pacote vindo de R4, o nó R2 o enfileira de acordo com o número de saltos que o

pacote percorre na rede, $l = 4$. Supondo $a = 3$ e $CW_i = CW_{min} = 31$, antes de encaminhar o pacote, o nó R2 calcula o novo tamanho da janela de contenção para o pacote sendo transmitido, onde $CW_{novo} = 19$. Dessa forma, aumenta-se a prioridade no acesso ao meio deste pacote.

4.3 Resultados

O desempenho do RLF foi analisado em protocolos que utilizam roteamento pela fonte, por esse ser o caso mais conveniente para a aplicação do RLF. Neste trabalho, o protocolo utilizado é o DSR (*Dynamic Source Routing*) [60] que é comumente utilizado como base de protocolos desenvolvidos para as redes em malha sem fio, como visto no Capítulo 3. O simulador de redes ns-2 (*network simulator 2*) [86] foi utilizado e o RLF foi implementado como parte do módulo do IEEE 802.11. Foram realizados dois conjuntos de simulações. A Seção 4.3.1 mostra o desempenho do mecanismo proposto RLF utilizando fontes de tráfego CBR/UDP. Já na Seção 4.3.2, o RLF foi analisado com fontes FTP/TCP. O número de nós na cadeia foi variado para analisar a justiça e a vazão agregada da rede.

Como métrica de justiça foi utilizado o índice de justiça, também chamado de índice de Jain, denotado por J e definido na Expressão 4.3 [87]. Nessa expressão, V_i denota a vazão obtida pelo nó i e N o número de nós transmissores. Quando $J = 1$, a transmissão em múltiplos saltos é completamente justa, pois todos os nós alcançam a mesma vazão na rede. Por outro lado, em uma transmissão completamente injusta, $J = 1/N$. As fontes CBR enviam pacotes de 1500 bytes a 3 Mb/s sobre o UDP. Já as fontes FTP também enviam pacotes de 1500 bytes, sobre o TCP. Todos os nós produzem tráfego, exceto o *gateway*. Logo, em uma cadeia de n nós, há $n - 1$ nós transmissores e um *gateway* que é o destino comum de todos os tráfegos de dados na rede. A vazão agregada da rede é igual a soma das vazões alcançadas individualmente pelos nós e é igual a

$$J = \frac{(\sum_{i=0}^N V_i)^2}{N \times \sum_{i=0}^N V_i^2}, \text{ onde } 1/N \leq J \leq 1. \quad (4.3)$$

Para simular o padrão IEEE 802.11g, foi implementado um módulo para o ns-2. A taxa física do meio usada é igual à taxa máxima do padrão, ou 54 Mb/s.

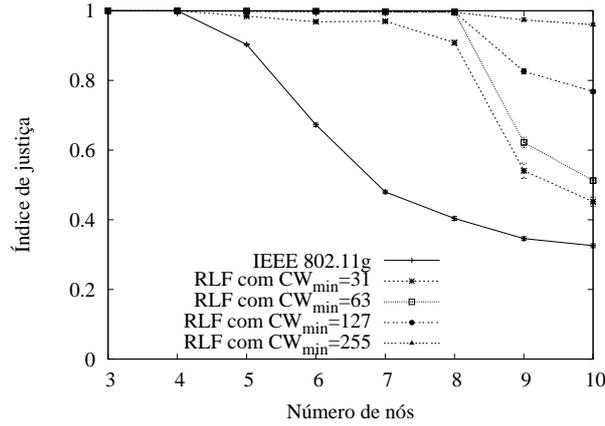
Além disso, o mecanismo RTS/CTS é sempre utilizado e o intervalo de confiança é de 95%. O RTS/CTS foi utilizado para evitar os efeitos do terminal escondido. Neste trabalho, foi assumido um índice de agressividade (a) igual a 3. O cenário de simulação é uma cadeia de encaminhamento como visto na Figura 4.1. O objetivo é isolar o efeito dos múltiplos saltos para não ser influenciado pela contenção de nós que estejam a um mesmo número de saltos do *gateway*.

A camada física usa o modelo de propagação de perda de percurso com $\beta = 3.9$ e $\sigma = 0$ para simular um ambiente interno, ou externo com obstáculos [88]. O raio de recepção dos nós é de aproximadamente 12,5 m, igual à distância física entre dois nós adjacentes, no cenário simulado. Já o raio de detecção de portadora é de aproximadamente 75 m. Um meio com taxa de erro de bit igual a zero foi usado.

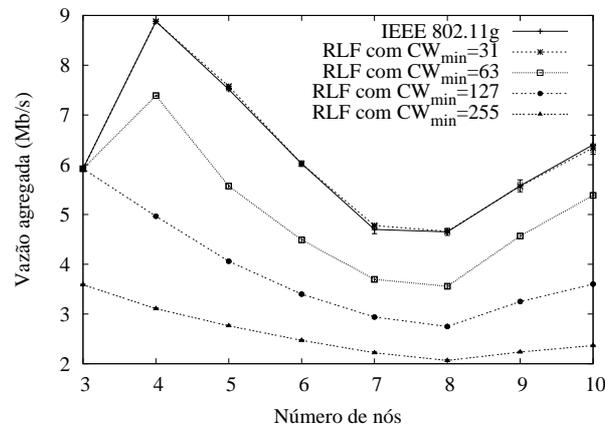
4.3.1 Experimentos com Tráfego CBR

A Figura 4.2(a) mostra o índice de justiça da topologia em cadeia com tráfego CBR/UDP. Aumentando o número de nós na cadeia, o RLF melhora a justiça da rede se comparado ao IEEE 802.11. Isso ocorre, pois toda vez que um pacote originado em um nó distante é enviado, a transmissão desse pacote é priorizada se comparada à de um pacote originado em um nó mais próximo. Logo, os pacotes de vida longa são enviados mais rapidamente a cada salto, não gastando o mesmo tempo em fila que os pacotes de vida mais curta.

A perda da justiça ocorre com o aumento da cadeia porque a prioridade atribuída pelo RLF aos nós mais distantes resulta em uma alta probabilidade de colisão. Isso ocorre porque ao diminuir a janela de contenção, reduz-se também o tempo que uma estação aguarda para começar a sua transmissão. Conseqüentemente, o início de sua transmissão tem uma maior probabilidade de coincidir com o início da transmissão de outro nó. Esse efeito é observado na Figura 4.2(a), quando se aumenta o número de nós na cadeia. Para privilegiar os pacotes de vida longa, o tamanho da janela de contenção é reduzido. Por exemplo, começando com $CW_{min} = 31$, CW_{novo} se torna igual a 3, assumindo uma rota de 9 saltos e um índice de agressividade igual a 3. Além da probabilidade de colisão, o reuso espacial pode agravar a injustiça. Por exemplo, no cenário simulado, quando existem mais de oito nós na cadeia, o último nó e o primeiro podem transmitir simultaneamente.



(a) Índice de justiça.

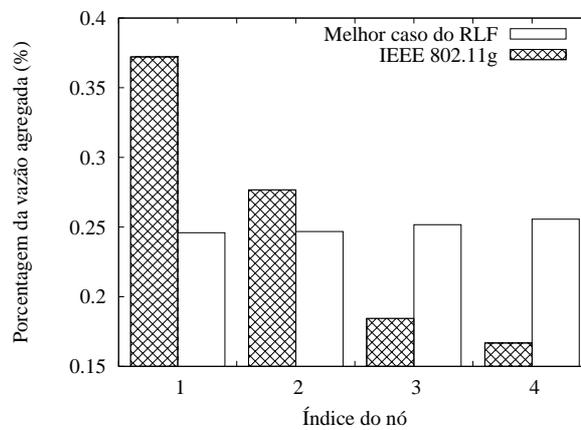


(b) Vazão agregada.

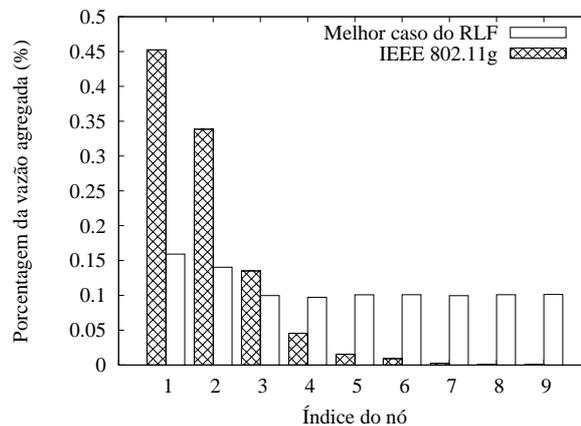
Figura 4.2: Resultados obtidos para fontes CBR/UDP.

Entretanto, quando o nó mais próximo do *gateway* transmite, ele impede que os nós da cadeia encaminhem seus próprios pacotes e os pacotes originados em nós mais distantes. Novamente, o nó mais próximo é beneficiado, diminuindo de forma mais agressiva o índice de justiça (J) da rede, como visto na Figura 4.2(a). Para reduzir esse problema, foram analisados diferentes tamanhos de janela mínima de contenção (CW_{min}). Usando maiores valores de CW_{min} , os pacotes de vida longa são mais privilegiados. Os pacotes enviados pelos nós mais distantes conseguem alcançar os nós que competem pelo meio com o nó mais próximo ao *gateway*, antes mesmo que o último comece a transmitir. Isso permite ainda que os nós intermediários possam enviar seus próprios pacotes e encaminhar os pacotes recebidos de outros nós, contornando o problema da injustiça causada pelo reuso espacial. Além disso, aumentar CW_{min} reduz a probabilidade de colisões, pois os nós mais próximos ao

gateway não ficam com a janela de contenção tão reduzida quanto ficavam quando $CW_{min} = 31$. A Figura 4.2(a) mostra que usar maiores tamanhos de CW_{min} melhora a justiça, superando os efeitos da probabilidade de colisão e do reuso espacial. Os resultados mostram que comparado ao IEEE 802.11, o índice de justiça (J) atingido pelo RLF passa de aproximadamente 0,3 para 0,95 usando $CW_{min} = 255$ numa cadeia de 10 nós. Mesmo mantendo $CW_{min} = 31$, o mecanismo proposto atinge $J=0,45$, que também é melhor que o apresentado pelo IEEE 802.11. A Figura 4.2(a) também mostra que dependendo do número de nós na cadeia e do tamanho do CW_{min} , o índice de justiça permanece próximo de 1.



(a) 5 nós.



(b) 10 nós.

Figura 4.3: Distribuição de vazão entre os nós da cadeia usando fontes CBR/UDP.

O compromisso do RLF é percebido na vazão agregada da rede, como visto na Figura 4.2(b). Note que o IEEE 802.11g atinge a maior vazão agregada. Entretanto, essa vazão agregada não reflete uma distribuição uniforme, pois dedica a maior parte

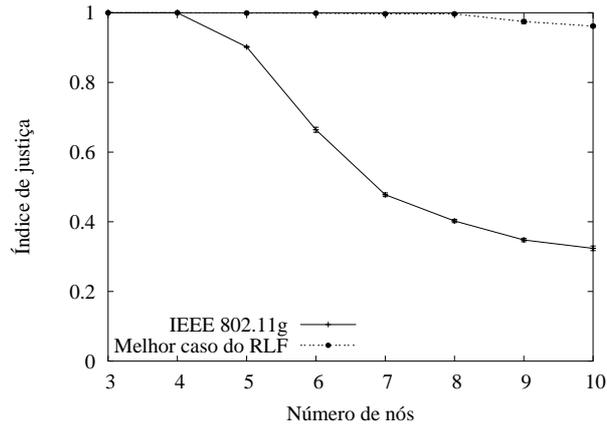
dos recursos da rede ao nó mais próximo ao *gateway*. Essa afirmação é comprovada nas Figuras 4.3(a) e 4.3(b), que ilustram a distribuição da vazão da rede entre os nós em uma cadeia de 5 e 10 nós, respectivamente. Nas Figuras 4.3(a) e 4.3(b), o eixo X representa o posicionamento do nó na cadeia, onde 1 é o nó mais próximo ao *gateway*. Já o eixo Y representa a porcentagem da vazão agregada que o nó está consumindo. As figuras mostram que os nós mais distantes não têm as mesmas oportunidades de enviar seus pacotes usando o IEEE 802.11g, o que não é uma característica desejável.

A Figura 4.2(b) mostra que o aumento de CW_{min} reduz a vazão agregada da rede. Isso acontece porque maiores tamanhos de CW_{min} resultam em maiores intervalos de tempo ociosos, diminuindo a vazão obtida pelos nós da rede. Usando $CW_{min} = 31$, a capacidade máxima da rede é obtida para cadeias com mais de 4 nós. Portanto, a vazão continua crescendo até uma cadeia de 4 nós, quando a rede fica sobrecarregada. Depois de 8 nós, a vazão agregada da rede aumenta, porque começa a haver reuso espacial.

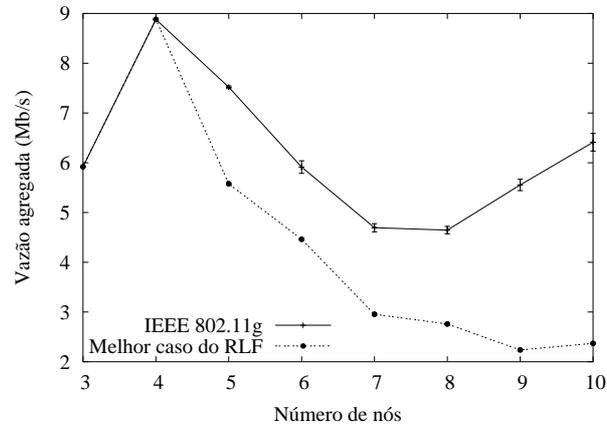
A Figura 4.4(a) mostra o índice de justiça para uma abordagem de melhor caso. Nessa abordagem, escolhe-se o tamanho de CW_{min} que oferece o melhor índice de justiça e máxima vazão agregada da rede, para cada número de nós na cadeia, como visto na Figura 4.2(a). Na simulação, os melhores tamanhos de CW_{min} foram ajustados manualmente, porém uma abordagem adaptativa merece maior investigação futura. A dificuldade da abordagem adaptativa é ajustar parâmetros do protocolo MAC de acordo com o número de nós da rede ou com a carga oferecida por nó. Os valores usados para o número de nós e CW_{min} correspondentes estão resumidos na Tabela 4.1. A Figura 4.4(b) mostra a vazão agregada alcançada na abordagem de melhor caso. É observado que o índice de justiça é aproximadamente igual a 1 independente do tamanho da cadeia e a vazão agregada da rede para cadeias com poucos nós é semelhante à alcançada pelo padrão IEEE 802.11g, caindo para cadeias mais longas.

4.3.2 Experimentos com Tráfego FTP

O protocolo TCP tenta utilizar a vazão máxima possível na rede. Além disso, o TCP possui um mecanismo de controle de congestionamento. Logo, o tráfego



(a) Índice de justiça do melhor caso.



(b) Vazão agregada do melhor caso.

Figura 4.4: Abordagem de melhor caso usando fontes CBR/UDP.

gerados pelas fontes FTP sofrem variações na taxa de envio para utilizar de forma mais eficiente os recursos disponíveis da rede, diferentemente das fontes CBR/UDP.

A Figura 4.5(a) mostra o índice de justiça das fontes FTP/TCP. De forma semelhante ao cenário com CBR/UDP, a justiça diminui conforme o número de nós da cadeia aumenta. Entretanto, um índice de justiça próximo a 1 é alcançado com $CW_{min} = 63$. Isso ocorre porque o TCP reage a colisões, ajustando o tamanho da sua janela de congestionamento. O protocolo TCP interpreta as colisões na camada de enlace como um indicativo de congestionamento da rede, reduzindo a taxa de envio de dados. Ao controlar a taxa de envio de dados, o TCP atenua o efeito negativo na justiça causado pelas colisões. Considerando a cadeia de 10 nós, a Figura 4.5(a) mostra que o índice de justiça atingido pelo RLF vai de aproximadamente 0,6 para 1, melhor que o IEEE 802.11g. Utilizando o tamanho mínimo do padrão IEEE 802.11

Tabela 4.1: Parâmetros usados na análise do melhor caso.

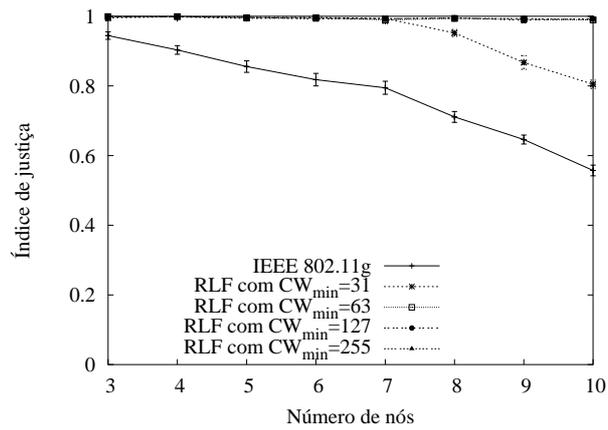
Número de nós na cadeia	CW_{min}
3 e 4	31
5 e 6	63
7 e 8	127
9 e 10	255

para janela de contenção ($CW_{min} = 31$), o índice de justiça passa de 0,6 para 0,8, ainda considerando a cadeia com 10 nós.

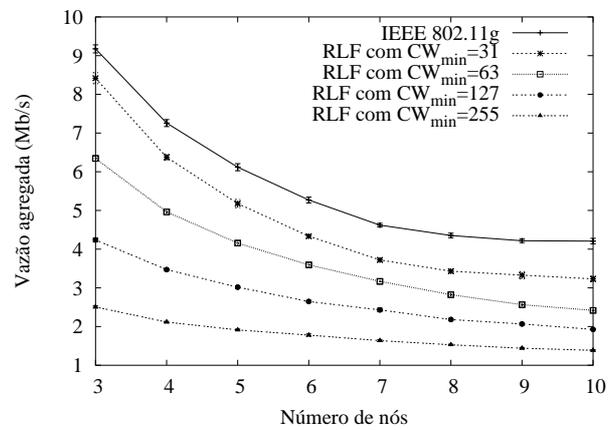
A Figura 4.5(b) mostra a vazão agregada da rede alcançada usando fontes FTP. Mais uma vez, a vazão do IEEE 802.11g é maior que a vazão alcançada pelo RLF, independentemente do tamanho da janela de contenção mínima usada. Note que com tráfego TCP a vazão diminui com o número de nós na cadeia. Isso ocorre porque o TCP regula a taxa de transmissão para que evitar congestionamentos e, conseqüentemente, perdas de pacotes. Principalmente perto do *gateway* da rede, para onde todo o tráfego é direcionado, o mecanismo de controle de congestionamento do TCP é mais presente. O mecanismo regula a taxa de transmissão para evitar gargalos, permitindo que nós mais distantes consigam uma parcela maior da banda passante disponível.

As Figuras 4.6(a) e 4.6(b) mostram, respectivamente, o índice de justiça e a vazão agregada da rede alcançadas pela abordagem de melhor caso. Em ambas as figuras a relação entre o número de nós na cadeia e o tamanho do CW_{min} mostrada na Tabela 4.1 é usada. De forma similar ao cenário com fontes CBR/UDP, o índice de justiça atingido permanece próximo a 1, não importando o número de nós na cadeia de encaminhamento.

As distribuições de vazão entre os nós da cadeia são mostradas nas Figuras 4.7(a) e 4.7(b) para 5 e 10 nós, respectivamente. Pode novamente ser comprovado que, apesar da vazão agregada ser maior no padrão IEEE 802.11g, os roteadores mais distantes transmitem pouco, o que prejudica os clientes da rede em malha distantes do *gateway*.

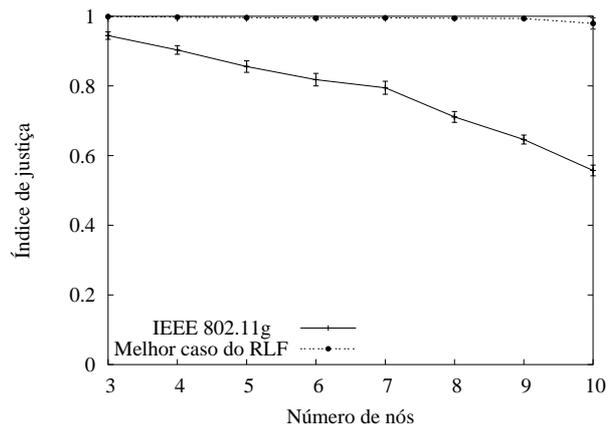


(a) Índice de justiça.

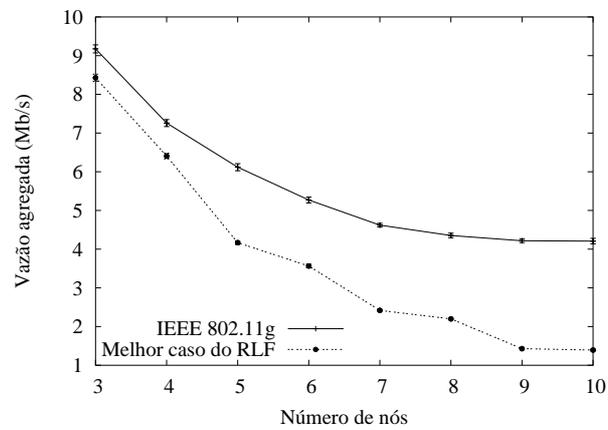


(b) Vazão agregada.

Figura 4.5: Resultados obtidos para fontes FTP/TCP.

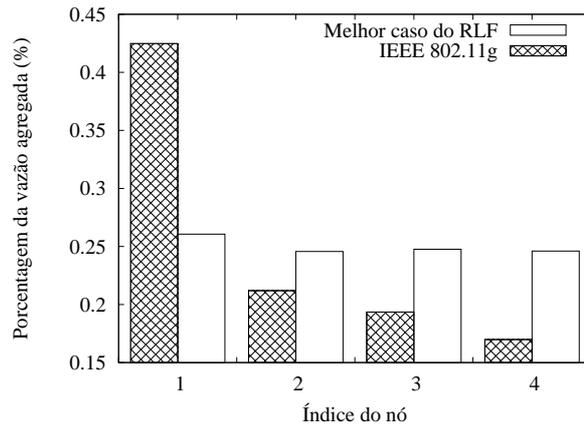


(a) Índice de justiça do melhor caso.

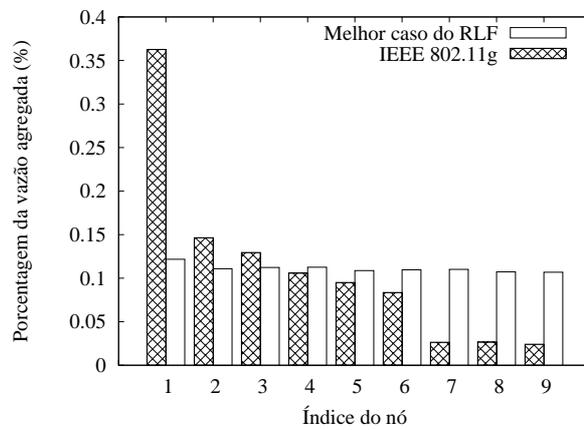


(b) Vazão agregada do melhor caso.

Figura 4.6: Abordagem de melhor caso usando fontes FTP/TCP.



(a) 5 nós.



(b) 10 nós.

Figura 4.7: Distribuição de vazão entre os nós da cadeia usando fontes FTP/TCP.

Capítulo 5

WPR: *Wireless-mesh-network* *Proactive Routing protocol*

Neste capítulo, é apresentado o protocolo de roteamento WPR (*Wireless-mesh-network Proactive Routing*). O protocolo WPR tem como principal objetivo aumentar a disponibilidade das redes em malha sem fio através da redução da sobrecarga de controle da rede. Para tal, ele utiliza dois algoritmos para controle de inundação que são cientes das características do tráfego da rede. O protocolo WPR é baseado no protocolo OLSR (*Optimized Link-State Routing*) e por isso seu desempenho é comparado a ele. Inicialmente, algumas premissas do WPR são apresentadas. Em seguida, os algoritmos utilizados no WPR são descritos e os resultados de simulação são apresentados.

5.1 Premissas

A primeira premissa deste trabalho é de que as aplicações que dependem do acesso à Internet são as mais comuns nas redes em malha [34]. Entretanto, dependendo do perfil dos usuários, outras aplicações podem gerar tráfego com origem e destino na própria rede em malha, como por exemplo aplicações par-a-par (P2P). Nesse caso, apesar da maior parte do tráfego ser entre usuários, deve-se ainda considerar que a arquitetura dessas aplicações pode ser híbrida, havendo o emprego de servidores na Internet. Dessa forma, também é analisado o desempenho do WPR com tráfego denominado “misto” onde convivem fluxos locais à rede em malha sem

fibra e fluxos de/para a Internet. A segunda premissa deste trabalho é que o protocolo de roteamento WPR conhece a topologia completa da rede. Para isso, o protocolo deve ser pró-ativo e baseado em estados do enlace. Algoritmos baseados em vetor de distâncias não atendem esse requisito e precisam de mais investigação, o que está fora do escopo deste trabalho. Note que a principal característica do protocolo OLSR, o conjunto de MPRs, também está ligada ao algoritmo de estados do enlace, já que é necessário conhecer os vizinhos de um e dois saltos. A terceira premissa é o conhecimento prévio dos *gateways* para a rede cabeada. O algoritmo de controle de inundação empregado pelo WPR precisa conhecer o endereço dos *gateways* para calcular os enlaces mais utilizados. Esse conhecimento não implica restrições, já que é comum definir os *gateways* em redes de acesso. Finalmente, é considerado que o protocolo de roteamento é executado somente pelos roteadores do *backbone*. Caso um usuário queira se conectar à rede, ele deve utilizar os roteadores como pontos de acesso conforme está sendo definido pelo padrão IEEE 802.11s.

5.2 Operação do Protocolo

O protocolo WPR possui duas características fundamentais: (i) o algoritmo de controle de inundação e (ii) o algoritmo de cálculo do conjunto dos nós AMPRs (*Adapted MultiPoint Relays*).

O WPR emprega um algoritmo de controle de inundação para redes em malha sem fio. Além disso, o WPR utiliza um algoritmo para o cálculo do conjunto de nós AMPRs, cuja função é equivalente ao conjunto de nós MPRs do OLSR. Vale mencionar novamente que o conjunto MPR de um nó qualquer é definido como o conjunto mínimo de vizinhos de um salto necessários para alcançar todos os vizinhos de dois saltos. Assim, evita-se a transmissão redundante de mensagens de controle. O conjunto de AMPRs também evita mensagens de controle redundantes, porém sua operação é adaptada ao algoritmo de controle de inundação utilizado. Com exceção dos algoritmos citados, a estrutura de pacotes e o funcionamento do protocolo WPR são intencionalmente semelhantes aos do OLSR para facilitar a sua implementação e adoção. Primeiramente, na Seção 5.2.1 o algoritmo de controle de inundação é apresentado e alguns dos seus parâmetros são avaliados. Na Seção 5.2.4, o algoritmo

para cálculo do conjunto AMPR é apresentado.

5.2.1 Algoritmo de Controle de Inundação

Nos protocolos baseados em estado do enlace, todos os nós conhecem o mapa completo da topologia. Para isso, cada nó periodicamente inunda a rede com os seus estados do enlace. Nas redes sem fio, isso acarreta múltiplos acessos ao meio compartilhado. Assim, a maioria dos protocolos com controle de inundação procura reduzir a frequência de envio de mensagens de controle pouco utilizadas ou redundantes [28].

Conforme uma das premissas básicas, o algoritmo de controle de inundação considera que os fluxos de dados são concentrados na direção do *gateway* para a rede cabeada. Logo, a parte da topologia mais utilizada é semelhante a uma árvore, na qual o *gateway* é a raiz. Baseado nessa topologia em árvore, o algoritmo de controle de inundação do WPR identifica como enlaces mais utilizados por um determinado nó i aqueles que pertencem a dois conjuntos distintos: o conjunto de nós ascendentes e descendentes de i na árvore. Denota-se \mathcal{A}_i como o conjunto de nós ascendentes de i e \mathcal{D}_i o conjunto de nós descendentes de i . A Figura 5.1 ilustra ambos os conjuntos, nos quais $\mathcal{A}_i = \{a_1, a_2, \dots, g\}$ e $\mathcal{D}_i = \{d_1, d_2, \dots\}$.

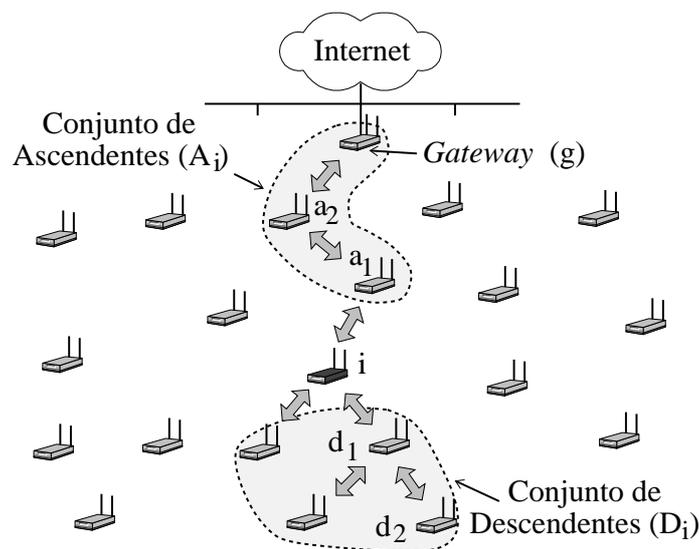


Figura 5.1: Conjunto de ascendentes e de descendentes de i conforme o WPR.

Determinados os conjuntos \mathcal{A}_i e \mathcal{D}_i , o algoritmo de controle de inundação do WPR reduz a sobrecarga de controle de roteamento ao encaminhar com maior

frequência as mensagens originadas apenas nos nós pertencentes aos conjuntos \mathcal{A}_i ou \mathcal{D}_i . Assim, encaminhando estados do enlace originados em \mathcal{A}_i , os nós de \mathcal{D}_i podem calcular rotas até o *gateway*. Por outro lado, encaminhando estados do enlace originados em \mathcal{A}_i , os nós de \mathcal{D}_i podem calcular rotas na direção reversa. Isso é necessário, pois as comunicações são bidirecionais. A Figura 5.2 ilustra a redução da carga de controle do WPR. Na Figura 5.2(a), os estados do enlaces originados em i são inundados na rede, como feito pelo OLSR com MPRs. Na Figura 5.2(b), uma mensagem de controle originada em i é encaminhada apenas pelos nós de \mathcal{A}_i , já que i é um descendente de \mathcal{A}_i ; e pelos nós de \mathcal{D}_i , já que i é um ascendente de \mathcal{D}_i . Portanto, i encaminha as mensagens de controle originadas no conjunto \mathcal{T}_i , onde $\mathcal{T}_i = \mathcal{A}_i \cup \mathcal{D}_i$, reduzindo a sobrecarga de controle total da rede.

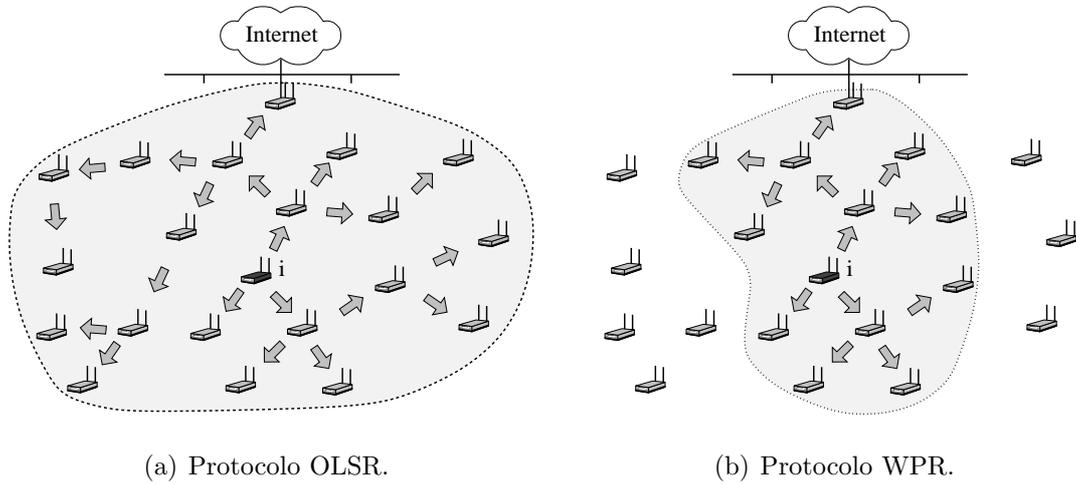


Figura 5.2: Algoritmos de inundação controlada.

O nó i determina o seu conjunto \mathcal{A}_i a partir da rota calculada até o *gateway*. Portanto, o conjunto \mathcal{A}_i é conhecido durante o processo de cálculo de rotas. Já o conjunto \mathcal{D}_i é conhecido através das mensagens HELLO. Nesse tipo de mensagem, todo nó lista os seus vizinhos de um salto e indica qual foi o escolhido como ascendente de um salto. Assim, o nó i conhece seus nós descendentes de um salto e pode encaminhar as mensagens deles. Recursivamente, toda mensagem de controle de roteamento originada em um nó qualquer pertencente a \mathcal{D}_i é encaminhada. Para tal, basta saber se o nó que a enviou por último é um descendente de um salto ou não. Como os descendentes de um salto só encaminham mensagens dos seus descendentes de um salto, assegura-se que a fonte da mensagem pertence a \mathcal{D}_i . Por exemplo, se uma mensagem de roteamento foi encaminhada por último por um nó descendente

de um salto, nó d_1 da Figura 5.1, assume-se somente um dos descendentes de d_1 originou a mensagem. Como os descendentes de d_1 estão também em \mathcal{D}_i , há uma propriedade recursiva simples para identificar nós descendentes. Outra opção seria calcular as rotas utilizadas por todos os nós da rede até o *gateway*, executando um algoritmo para busca do menor caminho (p. ex. Dijkstra). Assim, um determinado nó conheceria todas as rotas até o *gateway* das quais ele faz parte e, portanto, seus descendentes. Essa solução, porém, é custosa em termos computacionais e também depende fortemente da visão de todos os nós da rede ser a mesma em um determinado momento, o que nem sempre é o caso em redes sem fio. Isso ocorre porque a probabilidade de perda de pacotes é relativamente alta.

Em [29], dois tipos distintos de mensagens de controle são utilizados. As mensagens de inundação controlada, enviadas com maior frequência aos nós de \mathcal{A}_i e \mathcal{D}_i ; e mensagens de inundação, enviadas com menor frequência para toda a rede. Neste trabalho, a operação do algoritmo utiliza apenas uma mensagem de controle de topologia, e o tipo de encaminhamento necessário é identificado a partir de uma *flag* no cabeçalho. Assim, evita-se utilizar dois temporizadores, o que pode gerar informações redundantes quando os temporizadores expiram próximos. Além disso, o emprego de apenas uma mensagem torna a implementação do protocolo mais simples. No WPR, define-se o período de envio de mensagens de controle (T) e a proporção entre mensagens de inundação controlada e mensagens de inundação. Assim, após um número determinado de mensagens de inundação controlada, uma possui a *flag* de inundação para toda a rede ligada. É importante manter as mensagens de inundação, pois pode haver comunicações entre quaisquer nós do *backbone*, mesmo que sejam menos frequentes.

O Algoritmo 1 apresenta o funcionamento do controle de inundação do WPR, considerando a ação realizada por i ao receber a mensagem de controle m_c . No algoritmo, s é o nó que originou a mensagem de controle m_c , v é o nó vizinho que encaminhou m_c por último, g é o *gateway* de interconexão de rede e \mathcal{M}_v é o conjunto AMPR de v . Um nó somente encaminha uma mensagem de controle de roteamento se pertencer ao conjunto AMPR de v . Se essa condição for verdadeira, o nó i examina o tipo de mensagem de controle de roteamento recebida, como definido no cabeçalho de m_c . Se m_c for uma mensagem de inundação, o nó i simplesmente

encaminha m_c . Caso contrário, se m_c for uma mensagem de inundação controlada, o nó i usa duas funções para verificar se o nó v pertence ao seu conjunto \mathcal{T}_i . A função `eh_ascendente` verifica se s pertence ao conjunto \mathcal{A}_i de i considerando o *gateway* g . Já a função `eh_descendente` verifica se o nó v que encaminhou m_c é um descendente de um salto de i . Caso s e v não pertençam nem a \mathcal{A}_i nem a \mathcal{D}_i , o nó i não encaminha a mensagem.

Algoritmo 1 ENVIO DE MENSAGEM DE ROTEAMENTO EXECUTADO PELO NÓ i .

se $i \in \mathcal{M}_v$ **então**

se m_c é uma mensagem de inundação **então**

 encaminhar(m_c);

senão se m_c é uma mensagem de inundação controlada **então**

se `eh_ascendente`(s, i, g) **ou** `eh_descendente`(v, i, g) **então**

 encaminhar(m_c);

senão

 descartar(m_c);

fim do se

fim do se

fim do se

A proporção de envio entre mensagens de inundação controlada e mensagens de inundação é ajustada por cada nó, de acordo com a sua distância em número de saltos até o *gateway*. Quanto mais próximo do *gateway*, maior é o número de descendentes. Portanto, não há necessidade dos nós mais próximos do *gateway* inundarem a rede com a mesma frequência que os nós mais distantes, visto que eles já pertencem a um número maior de árvores (conjuntos \mathcal{T}_i). Cada nó WPR ajusta a proporção entre mensagens de inundação controlada e mensagens de inundação seguindo a expressão

$$p(l) = f(n) + g(l), \quad (5.1)$$

onde $p(l)$ é o número de mensagens de inundação controlada para cada mensagem de inundação, $f(n)$ é o número máximo de mensagens de inundação controlada para cada mensagem de inundação, calculado em função do número de nós (n) da rede e $g(l)$ é uma função que varia de acordo com o distância em número de saltos até o

gateway (l). O valor de n é conhecido uma vez que os nós possuem o mapa completo da topologia. Observa-se que quanto menor o valor de $p(l)$, menor é a proporção entre mensagens de inundação controlada e mensagens de inundação. Portanto, com maior frequência a rede é inundada.

5.2.2 Análise do Algoritmo de Controle de Inundação

O algoritmo de controle de inundação foi avaliado isoladamente tendo como medida o número de mensagens de controle enviadas por segundo, uma vez que o objetivo é reduzir a carga de controle da rede. Os resultados foram obtidos utilizando um simulador específico escrito em C++.

A análise está dividida em duas partes. A primeira avalia a influência dos parâmetros do algoritmo. Já na segunda parte, o desempenho do algoritmo proposto é comparado ao desempenho do OLSR e do algoritmo de inundação clássica. Na segunda parte, são considerados também cenários com e sem variação da qualidade do enlace. Nos cenários onde a qualidade do enlace varia, há o disparo de atualizações extras, aumentando ainda mais a carga de controle da rede. A escolha do OLSR para comparação se deve à importância do OLSR no padrão atualmente em desenvolvimento para redes em malha IEEE 802.11s. O padrão está definindo os algoritmos do OLSR como um dos protocolos base para o encaminhamento de pacotes nas redes em malha.

Na análise, considera-se que os nós recebem todos os pacotes de controle enviados pelos seus vizinhos e não há perda de mensagens de controle por falhas de transmissão. O encaminhamento, por sua vez, depende do algoritmo utilizado. No algoritmo proposto, o nó sempre encaminha o estado do enlace caso ele tenha sido originado por um nó pai ou filho pertencente ao seu conjunto \mathcal{T}_i ou quando a mensagem recebida é de inundação. Já no OLSR, o nó só encaminha caso ele seja um MPR do último nó que transmitiu a mensagem. No algoritmo de inundação, o nó sempre encaminha as mensagens recebidas. Independente do algoritmo utilizado, um mesmo pacote de controle só é transmitido uma única vez por cada nó, evitando a transmissão de pacotes duplicados por um único nó.

Nos resultados, o número de nós na rede é variado. Os nós são posicionados em uma grade $N \times N$, onde o *gateway* está localizado em um dos vértices. Todos os nós

geram mensagens de controle. É importante observar que as mensagens de controle são produzidas por todos os nós da rede, podendo haver transmissões simultâneas devido a reuso espacial. Porém, nos resultados não são considerados tempos de acesso ao meio ou colisões.

Avaliação de parâmetros

Nesta seção, é avaliado o desempenho dos principais parâmetros utilizados pelo algoritmo de controle de inundação. Neste cenário, cada nó possui no máximo 12 vizinhos, sendo esse um valor de densidade escolhido para os primeiros testes. É esperado, entretanto, que quanto mais densa for a rede, melhor será o comportamento do algoritmo de controle de inundação. Esse resultado é visto na Seção 5.2.3.

A Figura 5.3 mostra a carga de controle de roteamento enviada variando-se a proporção entre o período de envio de mensagens de inundação controlada e o período de envio de mensagens de inundação. No eixo X está o número de nós da rede e no eixo Y, a frequência de envio das mensagens de roteamento. É importante mencionar que nesses testes não há o uso da função que ajusta a proporção entre mensagens de inundação de acordo com a distância até o *gateway*, denotada por $p(l)$ na seção anterior (Seção 5.2.1). A intenção é isolar o efeito somente da variação da proporção entre os valores dos períodos. A legenda da Figura 5.3 mostra, respectivamente, o período utilizado para envio de mensagens de inundação controlada e o período de envio de mensagens de inundação em segundos. Pode-se notar que o período de inundação controlada afeta mais o número de mensagens de controle na rede que o período de inundação. Mantendo o período de inundação controlada igual a 4 s e variando o período de inundação de 100 para 500 s, há uma redução da carga de controle de até 20%. Por outro lado, mantendo o período de inundação de 500 s e variando o período de inundação controlada de 4 para 5 s, há uma redução também de até 20%. Logo, uma menor variação no período de inundação controlada provoca o mesmo aumento na carga de controle que uma variação bem maior no período de inundação.

Na próxima análise, duas possibilidades de funções para ajustar a proporção de envio entre mensagens de inundação controlada e mensagens de inundação de acordo com a distância do nó até o *gateway*, $p(l)$, são testadas. Deve ser observado

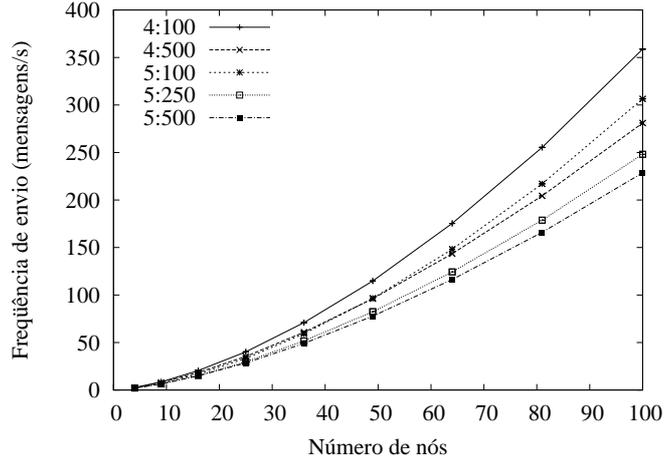


Figura 5.3: Proporção entre os períodos de envio de mensagens de inundação controlada e inundação.

que a função $p(l)$ ajusta o número máximo de mensagens de inundação por mensagem de inundação controlada ($f(n)$) de acordo com a distância até o gateway, $g(l)$. Conforme visto na Seção 5.2.1, $p(l) = f(n) + g(l)$. A função $g(l)$, dada pela Expressão 5.1, pode ser linear ou exponencial. A expressão linear utilizada é assumida igual a $g(l) = -(l + 20)$ e a exponencial é $g(l) = -l^2$. A proporção entre os períodos de inundação controlada e inundação é 5:100 s. Já a função $f(n)$ é considerada constante e igual a 200 s. Note que o objetivo dos testes é avaliar impacto do uso das diferentes funções $g(l)$ em termos relativos. Na avaliação a seguir é denominado algoritmo básico, aquele que não usa o ajuste de acordo com a distância do nó ao *gateway*.

A Figura 5.4 mostra que ambas as funções reduzem a carga de controle da rede em até 10%. Porém, a redução ao usar a função exponencial é ligeiramente maior, pois o valor de $p(l)$ cresce mais lentamente e, assim, na média um maior número de nós utiliza um período de inundação maior.

5.2.3 Avaliação Comparativa

Nesta seção, o algoritmo de controle de inundação é comparado ao algoritmo de controle de inundação do protocolo OLSR e ao algoritmo de inundação.

Na avaliação comparativa, o algoritmo proposto utiliza ajuste exponencial, no qual $f(n)=500$ s e a proporção entre os períodos de inundação controlada e inundação

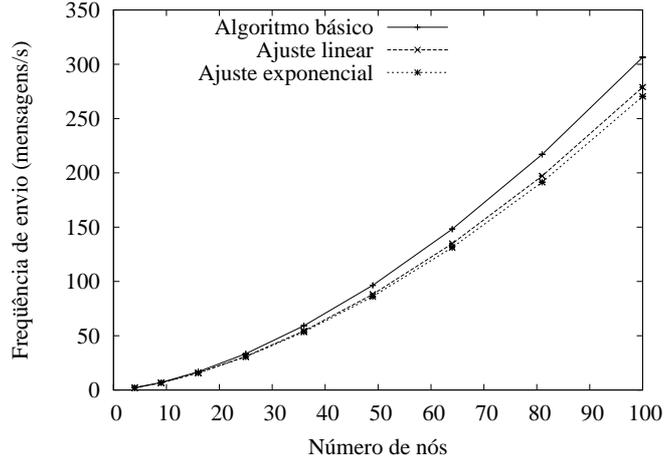


Figura 5.4: Função de ajuste de inundação.

é de 4:500s. Essa proporção foi escolhida por ter sido a que demonstrou os resultados intermediários de acordo com a Figura 5.3. Além disso, as mensagens de inundação são encaminhadas apenas por nós pertencentes ao conjunto MPR tanto no WPR quanto no OLSR. O conjunto MPR é calculado da mesma forma que no protocolo OLSR. As mensagens de inundação controlada, por sua vez, são encaminhadas por todos os nós pertencentes ao conjunto $\mathcal{T}_i = \mathcal{A}_i \cup \mathcal{D}_i$ de um nó i . Nesses testes, o conjunto AMPR ainda não é empregado. De qualquer maneira, espera-se reduzir o número de mensagens de controle enviadas a nós que não pertençam aos enlaces mais comumente utilizados e, assim, espera-se reduzir a quantidade de tráfego de controle na rede sem prejudicar as atualizações mais importantes. Portanto, apesar da redução da carga de controle global da rede, os estados dos enlaces de interesse são atualizados com frequência. Nos testes desta seção, é utilizado um período de 4s para o envio de mensagens de inundação controlada do algoritmo proposto. Isso aumenta a precisão dos nós no cálculo de rotas. Uma maior precisão no cálculo de rotas permite que as melhores rotas sejam escolhidas, aprimorando as condições de entrega de pacotes de dados da rede. Tanto o OLSR quanto o algoritmo de inundação utilizam um período de inundação igual a 5s, que é o período de inundação sugerido pela RFC 3626 do OLSR [89], e que é maior que o período utilizado pelo algoritmo proposto.

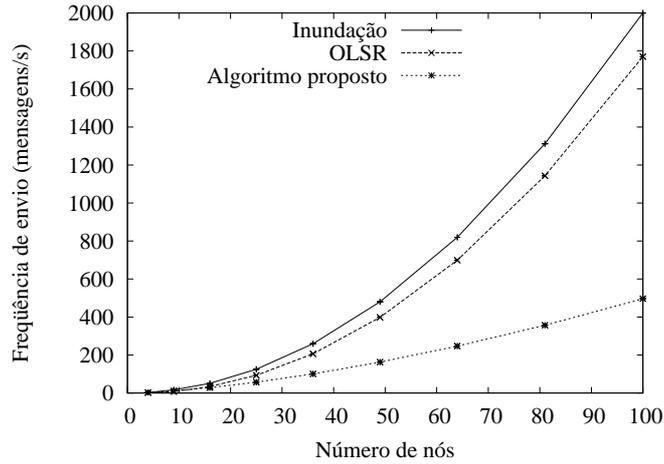
Nesta seção, são utilizados dois cenários, um esparsos e um denso, e cenários onde há ou não o disparo de atualizações em decorrência da variação das condições do meio. No cenário esparsos, cada nó da grade possui no máximo 4 nós vizinhos. Já

no cenário denso, cada nó possui no máximo 36 vizinhos. Nos cenários onde há disparos de atualizações de estados de enlace, considera-se a variação da qualidade dos enlaces. Sempre que ocorre um evento de variação, mensagens extras são enviadas. Tanto o OLSR quanto o algoritmo de inundação disseminam essas mensagens extras. Em oposição, o algoritmo proposto faz inundação controlada. Neste trabalho, foram considerados disparos de atualizações a cada 0,5s em média. Apesar das condições do meio poderem variar na ordem de milissegundos [48].

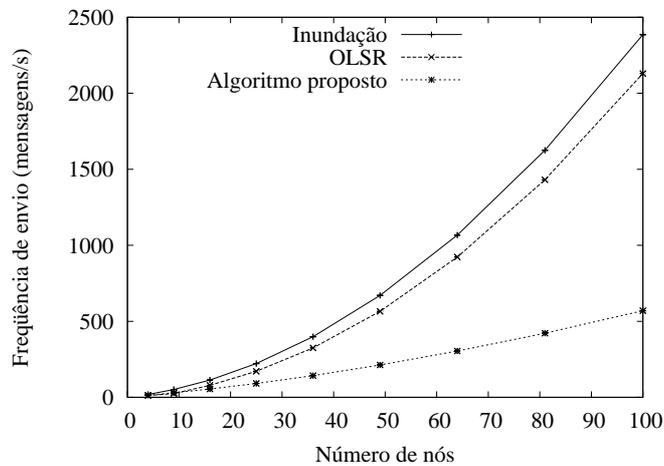
A Figura 5.5(a) mostra o número de mensagens de controle enviadas pelo algoritmo proposto, pelo OLSR e pelo algoritmo de inundação em um cenário esparsos sem variação na qualidade dos enlaces. Sem variação de qualidade, as únicas mensagens de controle transmitidas são as periódicas. Na Figura 5.5(a), nota-se um desempenho do OLSR muito próximo ao do algoritmo de inundação. Isso ocorre porque em cenários esparsos o mecanismo MPR não é eficiente. Não há muitas transmissões redundantes e, por conseguinte, quase todos os vizinhos de um salto devem ser eleitos MPR para que todos os de dois saltos recebam as mensagens de controle enviadas. Já no algoritmo proposto, o envio dos estados dos enlaces na direção do *gateway* é priorizado, reduzindo em até 73% o número de mensagens de controle em comparação ao OLSR.

Analisando o cenário esparsos onde há variação da qualidade dos enlaces, como visto na Figura 5.5(b), a diferença de sobrecarga de mensagens de controle entre o OLSR e o algoritmo proposto é maior. Essa diferença é de até 78% em grades com 100 nós. A diferença aumenta, pois com variação da qualidade dos enlaces, há o disparo de atualizações de controle, além das mensagens periódicas enviadas normalmente.

A Figura 5.6(a) mostra o número de mensagens de controle enviadas em um cenário denso sem variação de qualidade dos enlaces. Vale mencionar que a densidade é mantida constante. Para tal, sempre que o número de nós da rede aumenta, a área simulada também aumenta, mantendo a distância entre os nós sempre constante. Nota-se na figura que a eficiência do OLSR aumenta com a densidade da rede, pois o número de mensagens de controle torna-se consideravelmente menor que o número enviado pelo algoritmo de inundação por causa do uso do conjunto MPR. Quanto mais nós estiverem dentro da mesma área de transmissão, maior será



(a) Sem variação na qualidade dos enlaces.



(b) Com variação na qualidade dos enlaces.

Figura 5.5: Cenário esperso.

o número de transmissões redundantes. Conseqüentemente, a utilização do MPR é vantajosa. Mesmo assim, o algoritmo proposto continua sendo mais eficiente em número de mensagens de controle enviadas que o OLSR. Isso mostra que embora utilize um período de envio de mensagens de inundação controlada menor que o período de inundação usado pelo OLSR e pelo algoritmo de inundação (período de inundação controlada do WPR é de 4 s e de inundação do OLSR e do algoritmo de inundação é de 5 s), o desempenho da proposta é melhor em até 85% comparado ao OLSR. Uma maior frequência de envio de mensagens de controle mantém as métricas dos enlaces mais utilizados melhor atualizadas. Essa característica tem uma função importante, pois possibilita uma melhor escolha de rotas e, conseqüentemente, uma maior taxa de entrega de dados. Cenários mais densos favorecem também o algo-

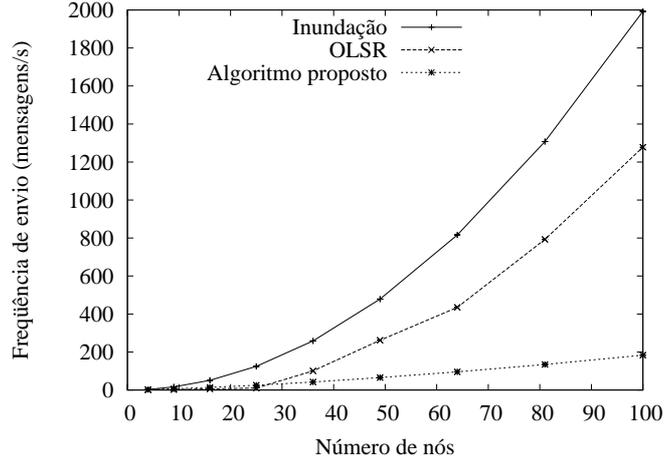
ritmo proposto, pois apenas os nós do conjunto MPR encaminham mensagens de controle de inundação.

Na Figura 5.6(b), é mostrado o desempenho dos algoritmos em um cenário denso, onde a qualidade dos enlaces varia. Novamente, a eficiência do algoritmo proposto é melhor que a do OLSR e a do algoritmo de inundação. O algoritmo proposto reduz a carga de roteamento em até 87%. Observa-se que apesar da melhora de desempenho do OLSR em relação ao cenário esparsos, a vantagem do algoritmo proposto é ainda mais acentuada. O elevado número de mensagens de controle enviadas por segundo ressalta a importância do algoritmo proposto. Em cenários reais, a carga de controle compete entre si e com os dados. Portanto, não enviar com sucesso todas as mensagens de controle prejudica o desempenho global da rede. Em vista disso, mais uma vez o algoritmo proposto para controle de inundação é mais eficiente que o OLSR e o algoritmo de inundação.

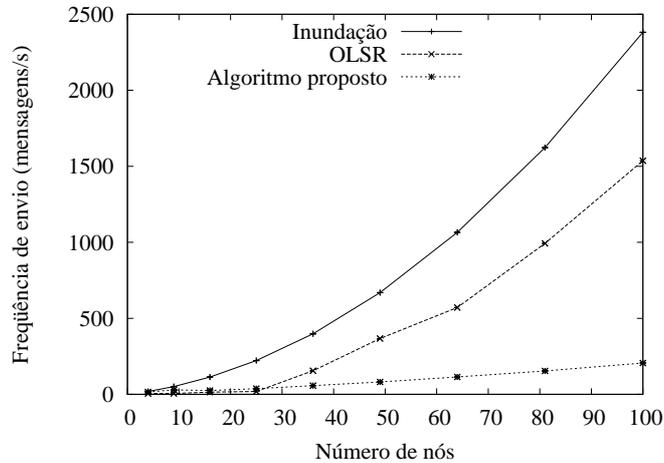
Os resultados obtidos mostram uma redução considerável na carga de controle de roteamento. Mesmo em cenários reais, o emprego do algoritmo de controle de inundação proposto mostra-se promissor, podendo melhorar a escalabilidade das redes em malha sem fio. A Seção 5.2.4 apresenta o outro algoritmo para a redução de carga de controle utilizado pelo WPR. A Seção 5.5, por sua vez, analisa o desempenho do WPR ao utilizar tanto o algoritmo de inundação controlada quanto o de cálculo de conjunto AMPR.

5.2.4 Algoritmo para o Cálculo do Conjunto AMPR

A segunda característica fundamental do WPR é o cálculo do conjunto AMPR (*Adapted Multi-Point Relay*) que tem por objetivo evitar mensagens de roteamento redundantes. O conjunto AMPR é uma versão adaptada do conjunto MPR do protocolo OLSR, que leva em consideração o algoritmo de inundação controlada do WPR. A idéia básica é encontrar os vizinhos de um salto pertencentes a \mathcal{T}_i necessários para alcançar todos os vizinhos de dois saltos também em \mathcal{T}_i . Como o WPR não faz somente inundações controladas, mas inunda a rede periodicamente, o conjunto AMPR é complementado com vizinhos de um salto que não estão em \mathcal{T}_i . Esse complemento é necessário para garantir, que todos os vizinhos de dois saltos que ainda não podem ser alcançados pelos nós já escolhidos para o conjunto



(a) Sem variação na qualidade dos enlaces.



(b) Com variação na qualidade dos enlaces.

Figura 5.6: Cenário denso.

AMPR, sejam alcançados. O cálculo do conjunto AMPR é semelhante ao cálculo do conjunto MPR do OLSR em duas etapas, conforme descrito no Algoritmo 2.

Em detalhes, o Algoritmo 2 funciona da seguinte forma. Seja \mathcal{M}_i o conjunto AMPR do nó i , $\mathcal{V}_{1,i}$ o conjunto de vizinhos de um salto de i e $\mathcal{V}_{2,i}$ o conjunto de vizinhos de dois saltos de i . Se $\mathcal{V}_{2,i}$ não estiver vazio, o algoritmo primeiro calcula o subconjunto de nós \mathcal{M}_i responsáveis por enviar as mensagens de inundação controlada aos vizinhos de dois saltos que pertencem também a \mathcal{T}_i , onde $\mathcal{T}_i = \mathcal{A}_i \cup \mathcal{D}_i$. Logo, o subconjunto dos nós que pertencem a $\mathcal{V}_{1,i}$ e a $\mathcal{V}_{2,i}$ e que também fazem parte de \mathcal{T}_i são passados como parâmetro para a função `calcula_AMPR`. Vale mencionar que $\mathcal{V}_{2,i}$ é deduzido a partir das mensagens HELLO enviadas por nós em $\mathcal{V}_{1,i}$. Se o conjunto AMPR permanecer vazio após a função `calcula_AMPR` ser executada, o

cálculo do conjunto AMPR se torna equivalente ao cálculo do conjunto MPR. Isso ocorre porque os parâmetros passados para a função `calcula_AMPR` são $\mathcal{V}_{1,i}$ e $\mathcal{V}_{2,i}$, o que resulta no conjunto de vizinhos de um salto capazes de alcançar todos os de dois saltos. Se \mathcal{M}_i não estiver vazio, por outro lado, o algoritmo exclui os nós em $\mathcal{V}_{2,i}$ que já são alcançados pelos nós em \mathcal{M}_i . A execução da função `exclui_nos` realiza essa tarefa e resulta no conjunto $\mathcal{V}'_{2,i}$, que é composto pelos nós vizinhos de dois saltos de i que ainda não foram alcançados por nós em \mathcal{M}_i . O algoritmo executa novamente a função `calcula_AMPR` para complementar o conjunto \mathcal{M}_i com os vizinhos de um salto necessários para alcançar todos os nós em $\mathcal{V}'_{2,i}$. Dessa vez, os vizinhos de um salto utilizados não estão em \mathcal{T}_i , visto que os vizinhos de um salto em \mathcal{T}_i já foram considerados na primeira etapa do algoritmo. A segunda vez que a função `calcula_AMPR` é executada garante que todos os vizinhos de dois saltos de i são alcançados durante uma inundação completa da rede. O conjunto AMPR final é a união dos nós encontrados na primeira e segunda vezes que a função `calcula_AMPR` é executada. Note que o vizinho de um salto pertencente ao conjunto \mathcal{A}_i deve estar sempre em \mathcal{M}_i . Caso contrário, uma mensagem de inundação controlada enviada por i nunca seria recebida por todos os nós ascendentes. Além disso, antes de encaminhar uma mensagem de inundação controlada, todo nó descendente deve verificar se pertence ao conjunto AMPR do nó que encaminhou a mensagem por último. Essa condição é testada na função `eh_descendente` do Algoritmo 1. Quando a mensagem é de inundação, todos os nós do conjunto AMPR devem encaminhar independentemente se estão ou não em \mathcal{A}_i ou \mathcal{D}_i .

O fato de o WPR calcular o conjunto AMPR em duas etapas faz com que o resultado final não seja necessariamente igual ao conjunto MPR do OLSR. Isso ocorre porque o OLSR é calculado levando em consideração todo o conjunto de vizinhos de um e dois saltos. Caso um determinado nó possua um grau de adjacência elevado e não pertença aos conjuntos \mathcal{A}_i e \mathcal{D}_i , ele é levado em consideração pelo OLSR para cálculo do conjunto de MPRs. Já o WPR só o leva em consideração na segunda etapa do cálculo do conjunto AMPR, podendo tornar o número de nós no conjunto final AMPR maior que o número final de nós no conjunto MPR do OLSR. O cálculo do AMPR leva em conta uma visão parcial nas duas etapas. Isso pode resultar em uma heurística menos eficiente do que o cálculo com a visão completa.

Algoritmo 2 CÁLCULO DO CONJUNTO AMPR EXECUTADO PELO NÓ i .

se $\mathcal{V}_{2,i} \neq \emptyset$ então
 $\mathcal{M}_i \leftarrow \text{calcula_AMPR}((\mathcal{V}_{1,i} \cap \mathcal{T}_i), (\mathcal{V}_{2,i} \cap \mathcal{T}_i));$
se $\mathcal{M}_i = \emptyset$ então
 $\mathcal{M}_i \leftarrow \text{calcula_AMPR}(\mathcal{V}_{1,i}, \mathcal{V}_{2,i});$
senão
 $\mathcal{V}'_{2,i} \leftarrow \text{exclui_nos}(\mathcal{M}_i, \mathcal{V}_{2,i});$
se $\mathcal{V}'_{2,i} \neq \emptyset$ então
 $\mathcal{M}_i \leftarrow \mathcal{M}_i \cup \text{calcula_AMPR}(\overline{(\mathcal{V}_{1,i} \cap \mathcal{T}_i)}, \mathcal{V}'_{2,i});$
fim do se
fim do se
fim do se

Apesar disso, o uso do conjunto AMPR evita o cálculo de dois conjuntos diferentes de MPRs, um para mensagens de inundação controlada e outro para mensagens de inundação, o que simplifica o algoritmo. Outra opção seria utilizar o conjunto MPR apenas para as mensagens de inundação [29]. Porém, essa opção implicaria em mensagens de inundação controlada redundantes.

A seção de resultados mostra que a taxa de entrega e a vazão agregada da rede que são obtidas com o WPR são superiores às do OLSR para diferentes tipos de tráfego. Isso ocorre porque o algoritmo de inundação controlada aliado ao algoritmo para cálculo do conjunto AMPR reduz a sobrecarga de controle sem afetar o desempenho do roteamento.

5.3 Análise da Complexidade dos Algoritmos Propostos

A complexidade do OLSR e do WPR é analisada em relação ao cálculo dos conjuntos MPR e AMPR. Em seguida, é avaliada a complexidade do algoritmo de controle de inundação em relação ao número de mensagens de controle enviadas. A notação utilizada é a mesma da Seção 5.2.

Lema 1 *Considere-se que $|\mathcal{V}_{1,i}|$ e $|\mathcal{V}_{2,i}|$ são respectivamente o número de vizinhos*

de um e dois saltos do nó i e $v = |\mathcal{V}_{1,i}| = |\mathcal{V}_{2,i}|/2$, como ilustrado na Figura 5.7. No pior caso, ou seja, quando todos os vizinhos de um salto pertencem ao conjunto de MPRs, a complexidade para um nó executando o protocolo OLSR calcular o seu conjunto MPR é $O(v^3)$.

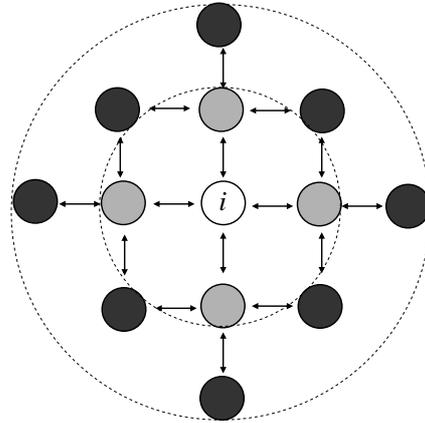


Figura 5.7: Topologia considerada.

Prova No OLSR, cada nó i precisa conhecer os seus vizinhos de um e dois saltos para calcular o seu conjunto MPR. A escolha de um nó pertencente ao conjunto MPR requer que o nó i encontre o seu vizinho de um salto com o maior grau de adjacência, considerando somente os seus vizinhos de dois saltos. O nó i então calcula o grau de adjacência que cada nó vizinho de um salto possui, levando em consideração todos os vizinhos de dois saltos. Essa operação leva $O(v^2)$ passos, onde cada passo é um teste de adjacência entre cada nó vizinho de um salto e cada nó vizinho de dois saltos, ou seja, $v \cdot 2v$ passos. Assim que um nó é escolhido para o conjunto MPR, ele é removido da lista de vizinhos de um salto. Adicionalmente, os vizinhos de dois saltos alcançados por esse novo nó MPR são removidos da lista de vizinhos de dois saltos. A seleção de nós para o conjunto MPR é um procedimento recursivo. Então, esse procedimento é repetido até que todos os vizinhos de dois saltos sejam alcançados por pelo menos um nó do conjunto MPR. No pior caso, calcular o conjunto MPR requer $\sum_{\xi=1}^v \xi^2$ passos, aumentando a complexidade para $O(v^3)$. ■

Lema 2 Considere-se que $v_{in} = |\mathcal{V}_{1,i} \cap \mathcal{T}_i| = |\mathcal{V}_{2,i} \cap \mathcal{T}_i|/2$ representa o número de vizinhos de um e dois saltos pertencentes ao conjunto \mathcal{T}_i e $v_{out} = |\overline{\mathcal{V}_{1,i} \cap \mathcal{T}_i}| = |\mathcal{V}'_{2,i}|$

o número de vizinhos de um salto e de dois saltos remanescentes que não estão em \mathcal{T}_i . O número de vizinhos de dois saltos remanescentes pode ser diferente de $|\overline{\mathcal{V}_{2,i} \cap \overline{\mathcal{T}_i}}|/2$, pois alguns nós mesmo não pertencendo a \mathcal{T}_i podem ser alcançados por nós em \mathcal{T}_i . Então, a complexidade para um nó executando o protocolo WPR calcular seu conjunto AMPR é $O(v_{in}^3 + v_{out}^3)$.

Prova No WPR, o cálculo do conjunto AMPR é similar ao cálculo do conjunto MPR em duas etapas. Entretanto, o conjunto de vizinhos de um e dois saltos usados em cada etapa são subconjuntos dos conjuntos de vizinhos de um e dois saltos usados pelo OLSR. O cálculo dos nós no conjunto AMPR responsáveis por encaminhar as mensagens de inundação controlada requer $\sum_{\xi=1}^{v_{in}} \xi^2$ passos, logo essa etapa possui complexidade $O(v_{in}^3)$. Semelhantemente, o cálculo dos nós do conjunto AMPR responsáveis por alcançar os vizinhos que não estão em \mathcal{T}_i é $O(v_{out}^3)$. Assim, o cálculo completo do conjunto AMPR é $O(v_{in}^3 + v_{out}^3)$. ■

Teorema 1 *A complexidade para calcular o conjunto AMPR é menor ou igual a necessária para calcular o conjunto MPR.*

Prova No Lema 1, define-se que o número de vizinhos de um salto de i é v e que de dois saltos é $2v$. Por outro lado, no Lema 2, $v_{in} + v_{out} \leq v$. Portanto, o número de passos necessários para calcular o conjunto MPR por um nó executando o protocolo OLSR é maior ou igual o número de passos que um nó executando o WPR requer para calcular o conjunto AMPR. Isso porque $v_{in}^3 + v_{out}^3 < v^3$, a não ser que $v_{out} = 0$ o que representaria uma cadeia de encaminhamento. ■

Lema 3 *Considere-se que n é o número total de nós da rede. O número de mensagens de controle de inundação enviadas por um nó executando o protocolo de roteamento OLSR é $O(n^2)$.*

Prova Considerando novamente que o conjunto MPR de um nó i é igual ao seu conjunto de vizinhos de um salto, o número de vezes que uma mensagem de i é encaminhada na rede é igual a n . Como todos os n nós inundam a rede periodicamente, o número de mensagens de inundação controlada é $O(n^2)$. ■

Lema 4 *O número de mensagens de inundação controlada enviadas por um nó executando o protocolo de roteamento WPR é $O((\sum_{i=1}^n (|\mathcal{A}_i| + |\mathcal{D}_i|)/n)^2)$.*

Prova Seja l_i o nível do nó i na topologia em árvore representada por \mathcal{T}_i , e $|\mathcal{A}_i|$ e $|\mathcal{D}_i|$ os números de nós em \mathcal{A}_i e \mathcal{D}_i , respectivamente. Logo, o número de vezes que uma mensagem de inundação controlada emitida por i é encaminhada é $\sum_{l=0}^{l_i-1} |\mathcal{A}_i| + \sum_{l=l_i}^{l_{max}} |\mathcal{D}_i| = l_i + \sum_{l=l_i}^{l_{max}} |\mathcal{D}_i|$. Note que $|\mathcal{A}_i|$ e $|\mathcal{D}_i|$ dependem do nível de i na árvore. Considerando que há n nós na rede, o número médio de ascendentes e descendentes na rede é $\sum_{i=1}^n |\mathcal{A}_i|/n$ e $\sum_{i=1}^n |\mathcal{D}_i|/n$, respectivamente. Então, o número de mensagens de inundação controlada é $O((\sum_{i=1}^n (|\mathcal{A}_i| + |\mathcal{D}_i|)/n)^2)$. ■

Teorema 2 *O protocolo WPR introduz menos sobrecarga de roteamento que o OLSR.*

Prova Para que o número de mensagens de inundação controlada seja menor ao usar o WPR, de acordo com os Lemas 3 e 4, deve-se garantir que

$$\left(\sum_{i=1}^n (|\mathcal{A}_i| + |\mathcal{D}_i|)/n\right) < n.$$

Portanto, para o WPR introduzir menos sobrecarga de controle que o OLSR basta que um nó i possua menos nós no seu conjunto de ascendentes e descendentes que o número total de nós da rede, ou seja, $|\mathcal{A}_i| + |\mathcal{D}_i| < n$. No caso de topologias do tipo cadeia de encaminhamento, isso não seria verdade pois $|\mathcal{A}_i| + |\mathcal{D}_i| = n$. ■

5.4 Ambiente de Simulações

O protocolo WPR proposto nesta tese é analisado através de simulações que utilizam o simulador de redes ns-2 em sua versão 31 [86]. Entretanto, como os módulos de camada física, de acesso ao meio e de roteamento são muito simplificados, uma série de alterações ao código foram realizadas para tornar os resultados obtidos por simulação mais próximos do cenário experimental. O emprego de técnicas para controle de inundação pode reduzir a robustez a erros da rede. Portanto, é importante avaliar o impacto dos algoritmos de controle de inundação proposto em um ambiente onde haja perda de mensagens de controle. Como os algoritmos propostos reduzem ainda mais o número de mensagens de controle em comparação ao OLSR, por exemplo, não é trivial se o desempenho do WPR é superior. Esta seção descreve as melhorias realizadas no código do simulador para torná-lo mais realista.

5.4.1 Camada Física

O simulador ns-2 original não considera a taxa de erro de bits (*Bit Error Rate* - BER) nas transmissões sem fio. Na distribuição padrão, o módulo da camada física calcula apenas o alcance máximo de recepção e interferência, conforme valores pré-definidos de potência de transmissão e recepção. Neste trabalho, o módulo de camada física desenvolvido por Xiuchao e Ananda [90] é adaptado para ser utilizado na versão 31 do ns-2. Nesse módulo, a taxa de erro de bits é obtida conforme a relação sinal-ruído (*Signal-to-Noise-Ratio* - SNR) do canal e a taxa física de transmissão. Para todo pacote recebido, é atribuída uma probabilidade de perda a partir da taxa de erro de bits calculada. É importante mencionar que o modelo de camada física foi desenvolvido para o IEEE 802.11b. Para definir o alcance de transmissão, o modelo de propagação de perda de percurso (*shadowing*) foi utilizado com os parâmetros obtidos experimentalmente também por Xiuchao e Ananda [91], listados na Tabela 5.1.

Tabela 5.1: Parâmetros de camada física.

Parâmetros	Valores
Potência de transmissão	$3,1622777 \times 10^{-2} \text{ W}$
Frequência de operação	2,472 GHz
Limiar de Detecção de Portadora	$3,1622777 \times 10^{-14} \text{ W}$
Limiar de Recepção	$3,1622777 \times 10^{-13} \text{ W}$
Ganho em antenas	1,0
Expoente do <i>shadowing</i>	4,0

Na Figura 5.8, pode-se observar a influência do uso do módulo de perda de pacotes no alcance máximo de transmissão. A Figura 5.8 é obtida por simulações onde a vazão máxima entre um par origem-destino é mostrada em função da distância entre eles. Para isso, utiliza-se uma fonte de tráfego constante igual a 11 Mb/s. Nota-se que o alcance de transmissão com o módulo de perda de pacotes é menor. Isso ocorre porque o módulo calcula a probabilidade da recepção do pacote em função da relação sinal-ruído do canal e da taxa de transmissão utilizada. Portanto, quanto menor a relação sinal-ruído e a taxa de transmissão, menor é a probabilidade de recepção do pacote com o aumento da distância. Utilizando a configuração padrão, a

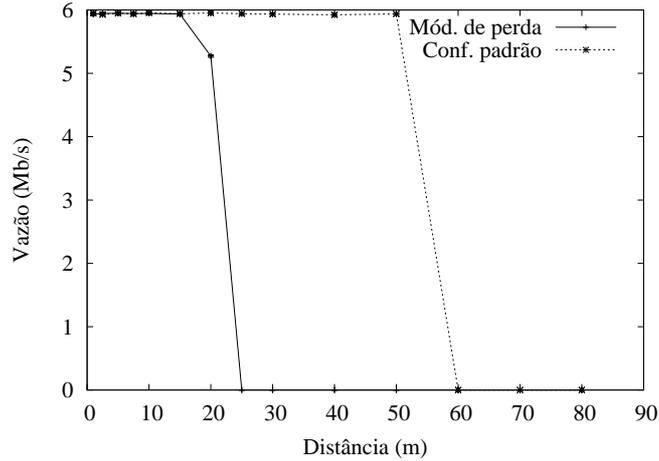


Figura 5.8: Impacto do uso do módulo de perda de pacotes.

probabilidade de recepção é de 100% enquanto a potência de recepção estiver acima de um limiar de potência mínimo. Esse limiar é o mesmo definido para taxas de transmissão de 1 Mb/s, o que torna o alcance máximo superior ao encontrado com o módulo de perda de pacotes. A atenuação é calculada conforme o modelo de perda de percurso e os parâmetros vistos na Tabela 5.1.

5.4.2 Camada de Acesso ao Meio

Apesar do padrão IEEE 802.11 definir múltiplas taxas físicas de transmissão, ele não define um algoritmo de controle para escolher a taxa mais apropriada para cada quadro a ser transmitido. Essa taxa depende das condições da rede e o algoritmo usado é deixado como uma opção para os fabricantes do *hardware*. Neste trabalho, o algoritmo ARF (*AutoRate Fallback*) [92] foi implementado no módulo do IEEE 802.11b. Esse algoritmo é simples e a sua operação é baseada no ajuste de dois contadores e de um temporizador. Basicamente, todo nó decresce sua taxa de transmissão para o valor mais baixo seguinte quando efetua duas retransmissões consecutivas. Em oposição, o nó aumenta a taxa de transmissão para o valor mais alto seguinte quando dez quadros são enviados consecutivamente com sucesso ou quando um temporizador de 60 ms expira. Sempre que um quadro é perdido, tanto o temporizador quanto o contador de pacotes enviados com sucesso são reiniciados. A implementação do ARF complementa o módulo de camada física. Sem um algoritmo de múltiplas taxas, a probabilidade de erro de bits do canal estaria somente

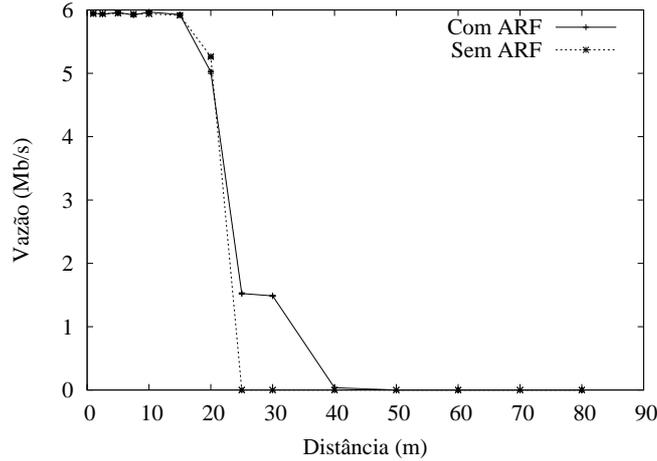


Figura 5.9: Impacto do uso do algoritmo de controle de taxa - ARF.

relacionada com a relação sinal-ruído, já que a taxa de transmissão seria constante.

A Figura 5.9 mostra o impacto do uso do algoritmo de controle de taxa ARF na vazão máxima obtida. Na Figura 5.9, repete-se o teste da Figura 5.8. Porém, dessa vez, o módulo de perda de pacotes é sempre utilizado. Pode-se observar na Figura 5.9 que o alcance aumenta com o uso do ARF. Isso ocorre porque com o uso do ARF, a taxa de transmissão é adaptada conforme a relação sinal-ruído do canal. Ao aumentar a distância entre os nós, a relação sinal-ruído decresce e a taxa de transmissão utilizada é menor que 11 Mb/s. Esse fato faz com que a transmissão se torne mais robusta ao aumento da distância e que a queda da vazão seja mais suave.

5.4.3 Roteamento

O protocolo de roteamento OLSR utilizado neste trabalho está disponível em [93]. Entretanto, para utilizá-lo, algumas alterações foram realizadas. Primeiramente, foi necessário portar o módulo à versão utilizada do simulador. Em seguida, o módulo do OLSR foi adaptado para utilizar como métrica o ETX, que é uma métrica específica das redes em malha sem fio. A implementação do ETX no simulador foi feita conforme a implementação do protocolo OLSR [94]. No OLSR, o ETX é calculado utilizando as mensagens de HELLO como sondas para estimar a qualidade dos enlaces. O cabeçalho das mensagens de HELLO é modificado para que os nós conheçam a fração de HELLOs recebidos numa determinada janela de tempo j por cada vizi-

no. O valor da janela j utilizada é 10 e é calculada como uma janela deslizante. No cabeçalho do HELLO, um campo é adicionado para indicar a fração de HELLOs recebidos (*Link Quality* - LQ) e outro para indicar a fração de HELLOs que o vizinho informou ter recebido (*Neighbor Link Quality* - NLQ). Um determinado nó calcula o $ETX = \frac{1}{LQ \times NLQ}$ de um enlace a partir da qualidade do enlace na direção direta (LQ) e na direção reversa (NLQ). Vale ressaltar que um modelo de camada física realista é fundamental para o funcionamento do ETX. Caso contrário, a métrica ETX seria função apenas das perdas por colisão, já que os enlaces seriam perfeitos em termos de taxa de erro binária.

A função $f(n)$ utilizada para ajustar a proporção de mensagens de inundação controlada e mensagens de inundação é $P_{min} + \sqrt{n}$, onde P_{min} é o número mínimo de mensagens de inundação controlada enviado a cada mensagem de inundação. Nas simulações, o número mínimo de mensagens de inundação controlada para cada mensagem de inundação é 13, a mesma usada pela extensão Fisheye do OLSR [94]. Como nas simulações deste trabalho são utilizados cenários em grade, torna-se conveniente usar $f(n)$ como função da raiz quadrada do número de nós da rede. Já a função $g(l) = -l$, uma vez que pode ser visto na Seção 5.2.2 que a diferença entre funções lineares e quadráticas não é tão relevante.

Nas simulações, o protocolo OLSR *sempre* utiliza a métrica ETX. Portanto, o OLSR utilizado é a versão alterada do OLSR que utiliza o ETX como métrica. A implementação do protocolo proposto nesta tese, o WPR, se baseia no módulo adaptado do OLSR e também usa a métrica ETX.

5.4.4 Padrão de Tráfego e Cenário

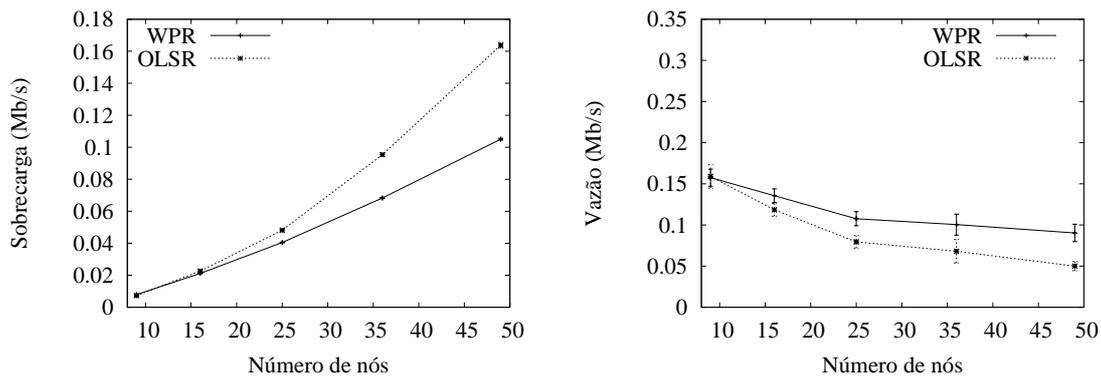
As simulações utilizam dois padrões de tráfego: tráfego *web* e tráfego misto. O tráfego *web* é modelado por requisições de páginas da Internet que geram uma resposta contendo os objetos da página solicitada. O tamanho da requisição é constante e igual a 1kbyte e o intervalo entre o envio de páginas diferentes é uma variável aleatória exponencial com média 10 s. Já o intervalo de envio entre os objetos de cada página é modelado por uma variável aleatória exponencial com média 10s cujo tamanho de cada objeto é uma variável aleatória com distribuição Pareto II com formato 1,2 e média 12kbytes [95]. O tráfego *web* é bidirecional e a requisição é sem-

pre iniciada pelos roteadores do *backbone* para o *gateway* da rede. Não é simulado o comportamento da rede cabeada, pois se assume que o gargalo é a rede de acesso sem fio. É importante mencionar que o tráfego *web* como modelado sempre utiliza o protocolo TCP. No tráfego denominado misto, além do tráfego *web*, há fontes CBR gerando tráfego entre pares origem-destino do *backbone*. Esses pares são escolhidos aleatoriamente, com exceção do *gateway*. Os fluxos CBR utilizam o protocolo UDP e têm duração segundo uma variável aleatória exponencial com média igual a 48 s. A duração de cada rodada de simulação é 90 s.

O cenário utilizado é uma grade de $N \times N$ nós, na qual o *gateway* está posicionado em um dos vértices. O número de nós na grade varia entre 9 e 49 e estão afastados de 20m. Assim, cada nó possui no máximo 20 vizinhos a 1 Mb/s e 8 vizinhos a 11 Mb/s. É utilizado apenas um *gateway* para a Internet. Caso η *gateways* fossem utilizados, o conjunto de ascendentes do nó i (\mathcal{A}_i) seria a união dos conjuntos de ascendentes para cada *gateway* ($\mathcal{A}_1 \cup \dots \cup \mathcal{A}_\eta$). Por outro lado, o conjunto de descendentes (\mathcal{D}_i) seria a união dos conjuntos de descendentes de cada conjunto em \mathcal{A}_i ($\mathcal{D}_1 \cup \dots \cup \mathcal{D}_\eta$). Com múltiplos *gateways* há maior sobrecarga de roteamento. Entretanto, no pior caso seria produzida a mesma sobrecarga do OLSR original, pois todos os vizinhos de dois saltos, ou pertenceriam ao conjunto de ascendentes ou ao conjunto de descendentes. Uma segunda forma de lidar com múltiplos *gateways* é considerar um nó pertencente a rede cabeada como o nó raiz da árvore \mathcal{T}_i . Assim, a estrutura em árvore permaneceria a mesma, pois o nó da rede cabeada seria visto como um *gateway* virtual e os múltiplos *gateways* seriam vistos como nós do *backbone*. Uma última forma de lidar com múltiplos *gateways* é criar critérios para que cada nó escolha apenas um *gateway* para a Internet e o utilize por um determinado período de tempo. Assim, a árvore utilizada é limitada a apenas uma e algoritmo proposto pode ser utilizado sem alterações.

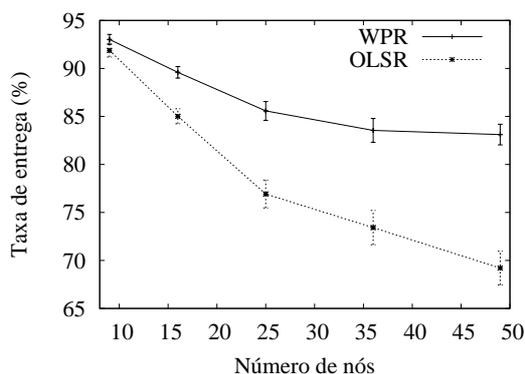
5.5 Resultados das Simulações

O desempenho do WPR foi comparado com o do OLSR. As métricas usadas para analisar o desempenho do WPR são: sobrecarga de roteamento, vazão agregada da rede e taxa de entrega de pacotes na camada de aplicação. Tanto o WPR quanto



(a) Sobrecarga de roteamento.

(b) Vazão.



(c) Taxa de entrega.

Figura 5.10: Tráfego *web* com carga baixa.

o OLSR enviam estados do enlace periodicamente a cada 5 s, como sugerido na RFC 3626 do OLSR. Já a proporção utilizada no WPR entre mensagens de difusão controlada e mensagens de difusão varia de 13:1 a 23:1, dependendo da distância em número de saltos do nó ao *gateway* (Seção 5.2). Todos os resultados possuem um intervalo de confiança de 95%, representado por barras de erro verticais.

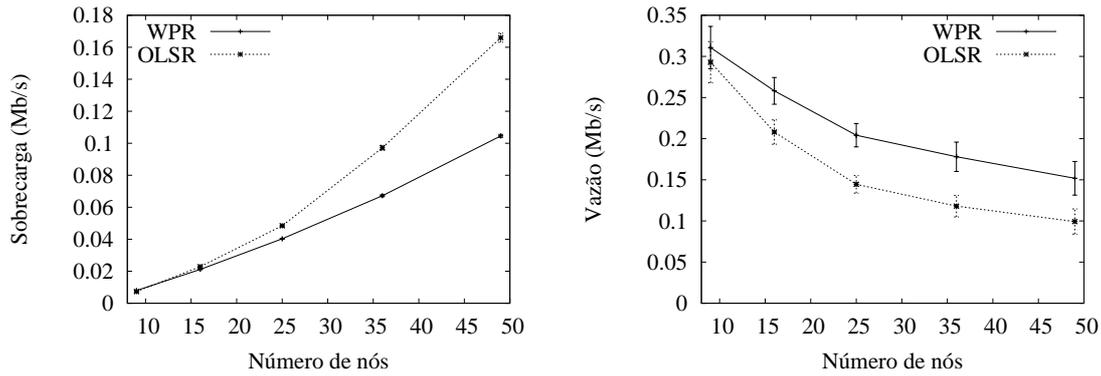
5.5.1 Tráfego *Web*

As simulações com tráfego *web* analisam o desempenho do WPR ao aumentar a carga de dados oferecida. Nesses testes, 75% dos nós da rede são escolhidos aleatoriamente para produzir tráfego na direção do *gateway* da Internet.

A Figura 5.10 mostra os resultados obtidos para carga baixa, na qual os nós que produzem tráfego iniciam 20 sessões *web* cada. Cada sessão representa uma seqüência de requisição de uma página e o recebimento dos objetos correspondentes. A Figura 5.10(a) apresenta a sobrecarga de controle de roteamento com o aumento

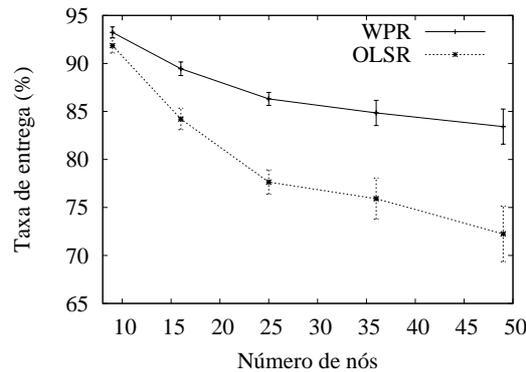
do número de nós. Pode ser visto que a redução da sobrecarga chega a até 36% se comparada ao OLSR. Essa redução aumenta com o número de nós, pois a média de saltos até o *gateway* também aumenta. Assim, o algoritmo de controle de inundação torna-se mais efetivo, já que a proporção entre os nós dos conjuntos \mathcal{A}_i e \mathcal{D}_i de um nó i qualquer diminui em comparação ao número total de nós da rede. Nota-se que a curva da sobrecarga de controle do WPR tem um crescimento mais lento que a curva de sobrecarga do OLSR. Esse resultado está de acordo com a análise de complexidade realizada na Seção 5.3, na qual verifica-se que o número de mensagens de controle do WPR possui complexidade inferior à do OLSR. A Figura 5.10(b) mostra a vazão agregada. Observa-se que a vazão alcançada com o WPR é maior que a alcançada pelo OLSR com o aumento do número de nós, já que a redução da sobrecarga de controle resulta em mais banda passante disponível para o tráfego de dados. Pode-se observar que a vazão agregada alcançada com o WPR é até 50% maior que a do OLSR. Outro efeito da redução da sobrecarga de controle pode ser visto na Figura 5.10(c). Essa figura mostra a taxa de entrega dos pacotes de dados. A taxa de entrega é a razão entre o número de pacotes de dados enviados e o número de pacotes recebidos na camada de aplicação. Pode-se observar que o decréscimo da sobrecarga de controle beneficia não somente o tráfego de dados, mas também o tráfego de controle da rede. Assim, a convergência dos algoritmos de roteamento torna-se mais rápida, evitando perda de pacotes. Observa-se ainda que a redução da taxa de perda é de até 10%.

A Figura 5.11 mostra os resultados obtidos ao duplicar a carga de dados. O objetivo é verificar o comportamento dos protocolos com o aumento da carga de dados oferecida. Pode-se perceber na Figura 5.11(a) que a sobrecarga de roteamento manteve-se a mesma vista na Figura 5.10(a). Isso acontece, pois as atualizações disparadas em virtude de quebras de rotas não são freqüentes. Esse efeito indica que a rede não está saturada e, portanto, não há quebra de rotas devido a congestionamento. É importante mencionar que o protocolo de roteamento só dispara atualização de métricas ao detectar quebra de rotas. Utilizando controle de taxa, o IEEE 802.11 reduz a sua taxa física de transmissão para evitar quedas de enlaces. A Figura 5.11(b) mostra que a vazão agregada da rede aumenta na mesma proporção que a carga oferecida se comparada com a vazão apresentada na Figura 5.10(b).



(a) Sobrecarga de roteamento.

(b) Vazão.



(c) Taxa de entrega.

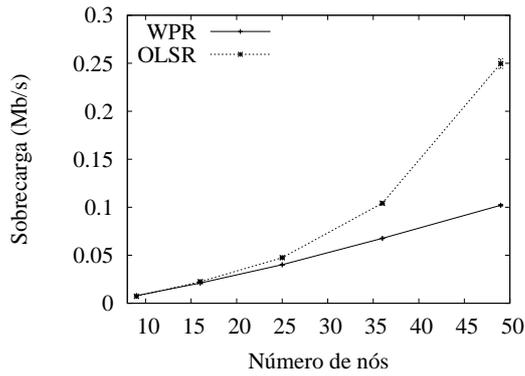
Figura 5.11: Tráfego *web* com carga alta.

Isso demonstra que a rede de fato não está saturada e que o WPR possui um desempenho melhor em tais condições. A taxa de entrega de pacotes de dados vista na Figura 5.11(c) também é semelhante à do cenário com carga mais baixa. Isso significa que o aumento da carga de dados ainda não foi suficiente para afetar a taxa de entrega de pacotes.

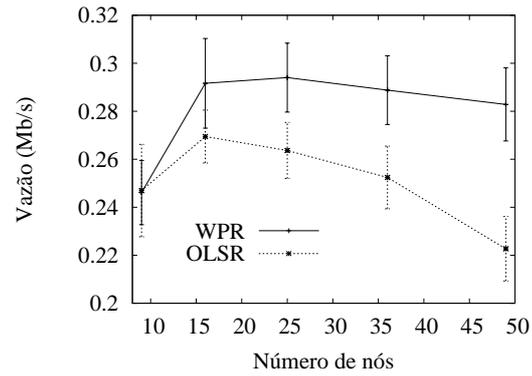
5.5.2 Tráfego Misto

Nas simulações com tráfego misto, 25% dos nós da rede utilizam tráfego *web* com o número de sessões igual a 20. Outros 25% dos nós são fontes de tráfego CBR a uma taxa de 56 kb/s. Tanto os nós *web* quanto as fontes e destinos do tráfego CBR foram escolhidos aleatoriamente, apenas evitando repetições. Nesses testes pretende-se avaliar o desempenho do WPR quando o tráfego não é em sua maior parte direcionado ao *gateway*.

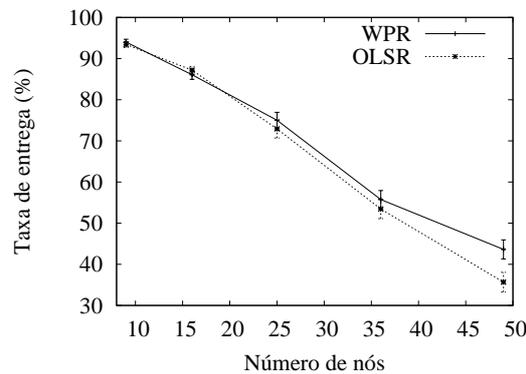
A Figura 5.12(a) mostra que a sobrecarga introduzida pelo OLSR continua su-



(a) Sobrecarga de roteamento.



(b) Vazão.



(c) Taxa de entrega.

Figura 5.12: Tráfego misto.

perior à introduzida pelo WPR, corroborando a análise de complexidade. Além disso, pode-se observar que a sobrecarga do WPR reduz é até 60% menor que a sobrecarga do OLSR. Nos testes com tráfego misto, observa-se que o OLSR utilizou mensagens de controle além da quantidade necessária nas simulações com tráfego *web*. O mesmo não ocorre com o WPR. Isso significa que houve um número maior de atualizações disparadas pelo OLSR. A Figura 5.12(b) mostra a vazão agregada obtida. Mais uma vez constata-se que a redução da sobrecarga de controle tem um impacto direto na vazão da rede. O WPR alcança resultados superiores aos do OLSR mesmo com premissa de convergência de tráfego na direção do *gateway* em cenários onde o tráfego não em sua maior parte direcionado ao *gateway*. O WPR supera em vazão o OLSR em até aproximadamente 24%. A Figura 5.12(c) mostra que a taxa de entrega da rede cai de forma acentuada se comparada aos resultados apenas com tráfego *web*. Isso ocorre porque há um aumento da carga oferecida à rede. O WPR oferece mesmo assim uma taxa de entrega superior à do OLSR em

até 22%. Com os resultados da Figura 5.12 conclui-se que o WPR é mais eficiente que o OLSR mesmo em cenários onde nem todo o tráfego é direcionado ao *gateway*.

Capítulo 6

Conclusões

Esta tese abordou dois dos principais desafios atuais das redes em malha sem fio que são a justiça no acesso ao meio e a conservação dos recursos da rede. Neste trabalho, as principais propostas existentes relacionadas a cada um dos desafios foram investigadas, com ênfase nos trabalhos relacionados ao roteamento em redes em malha. Nessa área, foram revisados as principais métricas e protocolos. Mais especificamente, foi proposta uma taxonomia para os protocolos de roteamento que os dividiu em quatro categorias de acordo com as suas características principais. Essa classificação dividiu os protocolos em legados do ad hoc, cientes do tráfego, com controle de inundação e oportunistas. Verificou-se que todos os protocolos têm como principal objetivo melhor utilizar os recursos das redes sem fio a partir de diferentes técnicas, como combinar estratégias pró-ativas e reativas, aproximar a topologia da rede a uma árvore, reduzir a sobrecarga de controle ou aumentar a confiabilidade no acesso ao meio. Além disso, verificou-se que a evolução das métricas cientes da qualidade acarreta um aumento de complexidade do protocolo de roteamento, principalmente em termos de número de mensagens de controle. Foi visto ainda que as métricas cientes da qualidade vêm sendo utilizadas pelos protocolos de roteamento propostos para as redes em malha em todas as categorias.

O problema da justiça no acesso ao meio em múltiplos saltos existente nas redes em malha sem fio é uma consequência da infra-estrutura estacionária e da presença de *gateways*, que se tornam destinos preferenciais da rede. Os nós mais distantes do *gateway* tendem a ter uma menor porção da vazão agregada da rede, ou até mesmo nula, se comparados aos nós mais próximos, pois tem que passar pelo processo de

disputa pelo meio um número maior de vezes. Essa característica é indesejável visto que idealmente os clientes conectados a uma rede em malha deveriam obter o mesmo desempenho da rede. Para aumentar a justiça em termos de vazão em tais redes, este trabalho propôs o mecanismo RLF (*Route-Length-based Fairness*), que atribui prioridade na camada MAC de acordo com o comprimento da rota dos pacotes gerados e encaminhados. O RLF privilegia pacotes de vida longa, que são os pacotes originados em nós distantes do *gateway*, no acesso ao meio. Nesta tese, o comprimento da rota é obtido pela camada MAC do cabeçalho do pacote de dados, através de técnicas de otimização entre camadas.

Os resultados de simulação mostraram que o RLF melhora a justiça da rede, mas possui um compromisso entre justiça e vazão agregada. Aumentar a justiça da rede implica diminuir a vazão agregada. Os resultados obtidos nesta tese mostram que o RLF pode alcançar um índice de justiça superior ao do IEEE 802.11g quando há transmissões de tráfego CBR/UDP. Quando a aplicação é FTP/TCP, a justiça também aumenta consideravelmente. Em ambas as aplicações, a justiça se mantém próxima de 1 com o aumento no número de nós em uma cadeia de encaminhamento, tornando a distribuição de vazão entre os nós da rede justa.

A redução da sobrecarga de controle nas redes em malha sem fio foi outro desafio considerado nesta tese. O protocolo de roteamento para redes em malha sem fio denominado WPR (*Wireless-mesh-network Proactive Routing*) foi proposto. O WPR possui algoritmos adaptados às redes em malha para reduzir a sobrecarga de controle de roteamento, e assim economizar banda passante para o tráfego de dados. A análise de complexidade realizada demonstrou que a sobrecarga de controle do WPR é inferior à introduzida pelo OLSR. Além disso, por meio de simulações foi mostrado que o desempenho do WPR é melhor que o do OLSR para tráfego *web* direcionado ao *gateway* da rede cabeada. Além disso, para tráfego misto, que é uma combinação de tráfego *web* e fontes CBR cujos pares origem-destino pertencem ao próprio *backbone*, o desempenho do WPR também foi superior. O WPR diminuiu a sobrecarga de controle em até 36% e 60% para tráfego *web* e misto, respectivamente. Para vazão agregada e taxa de entrega de pacotes, o WPR também obteve resultados superiores. Com tráfego *web* os ganhos foram de 50% na vazão e 10% na taxa de entrega. Já com tráfego misto, os resultados mostram que o WPR alcança

uma vazão agregada 24% maior e uma taxa de entrega 22% maior que o OLSR. Logo, apesar da operação do WPR assumir que as comunicações convergem para o *gateway*, seu desempenho mostrou-se superior mesmo em cenários com tráfego misto.

Há ainda muitas questões em aberto para melhorar o desempenho das redes em malha sem fio que vão desde rádios cognitivos até problemas de segurança. Uma direção é desenvolver abordagens que considerem técnicas de otimização entre camadas. Essa solução é promissora, pois muitos dos problemas das redes em malha sem fio estão diretamente ligados aos problemas do meio de transmissão que é muito dinâmico. Portanto, refletir as variações da camada física nas métricas de roteamento ou utilizar o espectro de frequências disponível de forma mais eficiente pode ser um caminho a se seguir.

Futuramente, planeja-se investigar a possibilidade de um RLF adaptativo e autônomo que ajuste o tamanho mínimo da janela de contenção conforme as condições da rede. Dentre essas condições é interessante utilizar o nível de congestionamento como parâmetro do RLF. Caso a rede esteja congestionada, não é claro se reduzir o tamanho da janela de contenção contribui ou não para o desempenho da rede mesmo em termos de justiça. A redução da janela de contenção em períodos de congestionamento pode aumentar o número de acessos ao meio e, conseqüentemente, de colisões. Uma forma de estimar o nível de congestionamento é medir o tempo médio que um determinado nó leva para acessar o meio ou o tamanho médio da janela de contenção utilizada. Com relação ao WPR, pretende-se implementar o protocolo em um protótipo real e analisar o seu desempenho experimentalmente. Além disso, planeja-se estender o algoritmo para o uso de múltiplos *gateways* para a Internet. Por fim, pretende-se implementar o RLF no WPR para que o protocolo reduza os problemas de injustiça nas redes em malha nativamente. Isso exige a adaptação do RLF para protocolos baseados em estados dos enlaces. Uma forma de alcançar esse objetivo é considerar o tamanho do caminho percorrido por um pacote igual a soma do tamanho da rota em número de saltos do nó intermediário até a fonte e do nó intermediário até o destino.

Referências Bibliográficas

- [1] IEEE, “IEEE Standard 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications”, Padrão.
- [2] RUBINSTEIN, M. G., MORAES, I. M., CAMPISTA, M. E. M., et al., “A Survey on Wireless Ad Hoc Networks”. Em: *IFIP IEEE International Conference on Mobile and Wireless Communication Networks (MWCN)*, pp. 1–34, Ago. 2006.
- [3] AKYILDIZ, I. F., WANG, X., “A Survey on Wireless Mesh Networks”, *IEEE Communications Magazine*, v. 43, n. 9, pp. S23–S30, Set. 2005.
- [4] AKYILDIZ, I. F., WANG, X., WANG, W., “Wireless Mesh Networks: A Survey”, *Computer Networks*, v. 47, n. 4, pp. 445–487, Março 2005.
- [5] BRUNO, R., CONTI, M., GREGORI, E., “Mesh Networks: Commodity Multihop Ad Hoc Networks”, *IEEE Communications Magazine*, v. 43, n. 3, pp. 123–131, Março 2005.
- [6] CHAVOUTIER, V., MANIEZZO, D., PALAZZI, C. E., et al., “Multimedia over Wireless Mesh Networks: Results from a Real Testbed Evaluation”. Em: *IFIP Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net)*, Junho 2007.
- [7] SUBRAMANIAN, A. P., GUPTA, H., DAS, S. R., “Minimum Interference Channel Assignment in Multi-Radio Wireless Mesh Networks”. Em: *IEEE Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, pp. 481–490, Junho 2007.

- [8] CAMPISTA, M. E. M., MORAES, I. M., ESPOSITO, P. M., et al., “The Ad Hoc Return Channel: A Low-Cost Solution for Brazilian Interactive Digital TV”, *IEEE Communications Magazine*, v. 45, n. 1, pp. 136–143, Jan. 2007.
- [9] CHENG, R.-G., WANG, C.-Y., LIAO, L.-H., et al., “Ripple: A Wireless Token-passing Protocol for Multi-hop Wireless Mesh Networks”, *IEEE Communications Letters*, v. 10, n. 2, pp. 123–125, Fev. 2006.
- [10] TSAI, T.-J., CHEN, J.-W., “IEEE 802.11 MAC Protocol over Wireless Mesh Networks: Problems and Perspectives”. Em: *International Conference on Advanced Information Networking and Applications (AINA)*, pp. 60–63, Março 2005.
- [11] RANIWALA, A., GOPALAN, K., CHIUEH, T.-C., “Centralized Channel Assignment and Routing Algorithms for Multi-Channel Wireless Mesh Network”, *ACM SIGMOBILE Mobile Computing and Communications Review*, v. 8, n. 2, pp. 50–65, Abril 2004.
- [12] MOSKO, M., ACEVES, J. J. G.-L., “Multipath Routing in Wireless Mesh Networks”. Em: *IEEE Workshop on Wireless Mesh Networks (WiMesh)*, Set. 2005.
- [13] ROBINSON, J., PAPAGIANNAKI, K., DIOT, C., et al., “Experimenting with a Multi-Radio Mesh Networking Testbed”. Em: *Workshop on Wireless Network Measurements (WinMee)*, Abril 2005.
- [14] KYASANUR, P., YANG, X., VAIDYA, N. H., “Mesh Networking Protocols to Exploit Physical Layer Capabilities”. Em: *IEEE Workshop on Wireless Mesh Networks (WiMesh)*, Set. 2005.
- [15] LEE, M. J., ZHENG, J., KO, Y.-B., et al., “Emerging Standards for Wireless Mesh Technology”, *IEEE Wireless Communications Magazine*, v. 13, n. 2, pp. 56–63, Abril 2006.

- [16] CAMP, J. D., KNIGHTLY, E. W., “The IEEE 802.11s Extended Service Set Mesh Networking Standard”, *IEEE Communications Magazine*, v. 46, n. 8, pp. 120–126, Ago. 2008.
- [17] SAADE, D. C. M., GOMES, A. G., CARRANO, R. C., et al., “Multihop MAC: Desvendando o Padrão IEEE 802.11s”, Em: *Minicursos do Simpósio Brasileiro de Redes de Computadores (SBRC)*, cap. 1, pp. 13–59, Sociedade Brasileira de Computação, Maio 2008.
- [18] GAMBIROZA, V., SADEGHI, B., KNIGHTLY, E. W., “End-to-End Performance and Fairness in Multihop Wireless Backhaul Networks”. Em: *ACM International Conference on Mobile Computing and Networking (MobiCom)*, pp. 287–301, Set. 2004.
- [19] DAS, S. M., PUCHA, H., HU, Y. C., “Symmetrical Fairness in Infrastructure Access in Multi-hop Wireless Networks”. Em: *IEEE Workshop on Wireless Networks and Mobile Computing (ICDCS)*, pp. 461–470, Junho 2005.
- [20] WANG, X., KAR, K., “Cross-layer Rate Optimization for Proportional Fairness in Multihop Wireless Networks with Random Access”, *IEEE Journal on Selected Areas in Communications*, v. 24, n. 8, pp. 1548–1559, Ago. 2006.
- [21] DONG, Q., BANERJEE, S., LIU, B., “Throughput Optimization and Fair Bandwidth Allocation in Multi-Hop Wireless LANs”. Em: *IEEE Conference on Computer Communications (INFOCOM)*, pp. 1–12, Abril 2006.
- [22] CAMPISTA, M. E. M., COSTA, L. H. M. K., DUARTE, O. C. M. B., “Um Mecanismo para Privilegiar Pacotes de Vida Longa em Redes Sem Fio de Múltiplos Saltos”. Em: *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)*, pp. 3–16, Maio 2007.
- [23] CAMPISTA, M. E. M., COSTA, L. H. M. K., DUARTE, O. C. M. B., “Privileging Long-life Packets in Multihop Wireless Networks”. Em: *IFIP/IEEE International Conference on Mobile and Wireless Communications Networks (MWCN)*, pp. 136–140, Set. 2007.

- [24] SRIVASTAVA, V., MOTANI, M., “Cross-Layer Design: A Survey and the Road Ahead”, *IEEE Communications Magazine*, v. 43, n. 12, pp. 112–119, Dez. 2005.
- [25] RAISINGHANI, V. T., IYER, S., “Cross-Layer Feedback Architecture for Mobile Device Protocol Stacks”, *IEEE Communications Magazine*, v. 44, n. 1, pp. 85–92, Jan. 2006.
- [26] CAMPISTA, M. E. M., COSTA, L. H. M. K., DUARTE, O. C. M. B., “WPR: Um Protocolo de Roteamento Pró-ativo Adaptado às Redes em Malha Sem Fio”. Em: *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)*, pp. 889–902, Maio 2008.
- [27] CAMPISTA, M. E. M., COSTA, L. H. M. K., DUARTE, O. C. M. B., “WPR: A Proactive Routing Protocol Tailored to Wireless Mesh Networks”. Em: *IEEE Globecom 2008 Ad Hoc, Sensor and Mesh Networking Symposium (GC AHSN)*, pp. 1–5, Nov. 2008.
- [28] CAMPISTA, M. E. M., PASSOS, D. G., ESPOSITO, P. M., et al., “Routing Metrics and Protocols for Wireless Mesh Networks”, *IEEE Network*, v. 22, n. 1, pp. 6–12, Jan.-Fev. 2008.
- [29] CAMPISTA, M. E. M., COSTA, L. H. M. K., DUARTE, O. C. M. B., “Um Algoritmo Eficiente de Disseminação dos Estados de Enlace para Redes em Malha Sem Fio”. Em: *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)*, pp. 751–764, Maio 2007.
- [30] CARRANO, R. C., SAADE, D. C. M., CAMPISTA, M. E. M., et al., “Multihop MAC: IEEE 802.11s Wireless Mesh Networks”, Em: *Encyclopedia on Ad Hoc and Ubiquitous Computing*, cap. 19, World Scientific Publishing, 2009.
- [31] IEEE 802.11E, “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Medium Access Control (MAC) Quality of Service Enhancements”, Extensão.

- [32] JUN, J., SICHITIU, M. L., “Fairness and QoS in Multihop Wireless Networks”. Em: *IEEE VTC-Fall*, pp. 2936–2940, Out. 2003.
- [33] BAUMANN, R., HEIMLICHER, S., LENDERS, V., et al., “Routing Packets into Wireless Mesh Networks”. Em: *Wireless and Mobile Computing, Networking and Communications, 2007. WiMOB 2007. Third IEEE International Conference on*, pp. 38–45, Out. 2007.
- [34] DRAVES, R., PADHYE, J., ZILL, B., “Routing in Multi-Radio, Multi-Hop Wireless Mesh Networks”. Em: *ACM International Conference on Mobile Computing and Networking (MobiCom)*, pp. 114–128, Set. 2004.
- [35] MORAES, I. M., CAMPISTA, M. E. M., DUARTE, J. L., et al., “On the Impact of User Mobility on Peer-to-Peer Video Streaming”, *IEEE Wireless Communications Magazine*, v. 15, n. 6, Nov.-Dez. 2008.
- [36] MORAES, I. M., CAMPISTA, M. E. M., MOREIRA, M. D. D., et al., “Distribuição de Vídeo sobre Redes Par-a-Par: Arquiteturas, Mecanismos e Desafios”, Em: *Minicursos do Simpósio Brasileiro de Redes de Computadores (SBRC)*, cap. 3, pp. 115–171, Sociedade Brasileira de Computação, Maio 2008.
- [37] FERNANDES, N. C., MOREIRA, M. D. D., VELLOSO, P. B., et al., “Ataques e Mecanismos de Segurança em Redes Ad Hoc”, Em: *Minicursos do Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg)*, cap. 2, pp. 49–102, Sociedade Brasileira de Computação, Ago. 2006.
- [38] SALEM, N. B., HUBUAX, J.-P., “Securing Wireless Mesh Networks”, *IEEE Wireless Communications Magazine*, v. 13, n. 2, pp. 50–55, Abril 2006.
- [39] FERNANDES, N. C., DUARTE, O. C. M. B., “CHARADAS: Uma proposta para uso de CHAve de grupo no Roteamento Através de Distribuição Assimétrica Segura”. Em: *XXV Simpósio Brasileiro de Telecomunicações (SBrT)*, Set. 2007.

- [40] GLASS, S., PORTMANN, M., MUTHUKKUMARASAMY, V., “Securing Wireless Mesh Networks”, *IEEE Internet Computing*, v. 12, n. 4, pp. 30–36, Jul.-Ago. 2008.
- [41] DUFFY, K., LEITH, D., LI, T., et al., “Improving Fairness in Multi-Hop Mesh Networks Using 802.11e”. Em: *International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks*, pp. 1–8, Abril 2006.
- [42] RAGUIN, D., KUBISCH, M., KARL, H., et al., “Queue-driven Cut-through Medium Access in Wireless Ad Hoc Networks”. Em: *IEEE WCNC*, pp. 1909–1914, Março 2004.
- [43] FU, Z., LUO, H., ZERFOS, P., et al., “The Impact of Multihop Wireless Channel on TCP Performance”, *IEEE Transactions on Mobile Computing*, v. 4, n. 2, pp. 209–221, Março 2005.
- [44] FERRERO, D., URVOY-KELLER, G., “A Size-based Scheduling Approach to Improve Fairness over 802.11 Wireless Networks”. Em: *ACM SIGCOMM*, Set. 2006.
- [45] SHI, J., GUREWITZ, O., MANCUSO, V., et al., “Measurement and Modeling of the Origins of Starvation in Congestion Controlled Mesh Networks”. Em: *IEEE Conference on Computer Communications (INFOCOM)*, pp. 1633–1641, Abril 2008.
- [46] BAUMANN, R., HEIMLICHER, S., LENDERS, V., et al., “Routing Packets into Wireless Mesh Networks”. Em: *IEEE Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pp. 38–45, Out. 2007.
- [47] WAHARTE, S., BOUTABA, R., IRAQI, Y., et al., “Routing Protocols in Wireless Mesh Networks: Challenges and Design Considerations”, *Multimedia Tools and Applications (MTAP) journal*, v. 29, n. 3, pp. 285–303, Junho 2006.

- [48] KOKSAL, C. E., BALAKRISHNAN, H., “Quality-Aware Routing Metrics for Time-Varying Wireless Mesh Networks”, *IEEE Journal on Selected Areas in Communications*, v. 24, n. 11, pp. 1984–1994, Nov. 2006.
- [49] COUTO, D. S. J. D., AGUAYO, D., BICKET, J., et al., “A High-Throughput Path Metric for Multi-Hop Wireless Routing”. Em: *ACM International Conference on Mobile Computing and Networking (MobiCom)*, pp. 134–146, Set. 2003.
- [50] DRAVES, R., PADHYE, J., ZILL, B., “Comparison of Routing Metrics for Static Multi-hop Wireless Networks”. Em: *ACM SIGCOMM*, pp. 133–144, Ago. 2004.
- [51] PASSOS, D., TEIXEIRA, D. V., MUCHALUAT-SAADE, D. C., et al., “Mesh Network Performance Measurements”. Em: *International Information and Telecommunicatios Technologies Symposium (I2TS)*, Dez. 2006.
- [52] BICKET, J., AGUAYO, D., BISWAS, S., et al., “Architecture and Evaluation of an Unplanned 802.11b Mesh Network”. Em: *ACM International Conference on Mobile Computing and Networking (MobiCom)*, pp. 31–42, Ago. 2005.
- [53] AGUAYO, D., BICKET, J., MORRIS, R., *SrcRR: A High Throughput Routing Protocol for 802.11 Mesh Networks (DRAFT)*, Rel. técnico, MIT, 2005.
- [54] DE COUTO, D. S. J., *High-Throughput Routing for Multi-Hop Wireless Networks*, Tese de Doutorado, MIT, 2004.
- [55] KYASANUR, P., VAIDYA, N. H., “Routing and Link-layer Protocols for Multi-Channel Multi-Interface Ad Hoc Wireless Networks”, *SIGMOBILE Mobile Computing and Communications Review*, v. 10, n. 1, pp. 31–43, Jan. 2006.
- [56] GOSSAIN, H., JOSHI, T., CORDEIRO, C., et al., “A cross-layer approach for designing directional routing protocol in MANETs”. Em: *IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1976–1981, Março 2005.

- [57] YANG, Y., WANG, J., KRAVETS, R., “Designing Routing Metrics for Mesh Networks”. Em: *IEEE Workshop on Wireless Mesh Networks (WiMesh)*, Set. 2005.
- [58] DE O. CUNHA, D., DUARTE, O. C. M. B., PUJOLLE, G., “An Enhanced Routing Metric for Fading Wireless Channels”. Em: *IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 2723–2728, Março 2008.
- [59] SUBRAMANIAN, A. P., BUDDHIKOT, M. M., MILLER, S. C., “Interference Aware Routing in Multi-Radio Wireless Mesh Networks”. Em: *IEEE Workshop on Wireless Mesh Networks (WiMesh)*, pp. 55–63, Set. 2006.
- [60] DAVID B. JOHNSON, D. A. M., BROCH, J., “Ad Hoc Networking”, cap. 5, pp. 139–172, *DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks*, Addison-Wesley, 2001.
- [61] IANNONE, L., FDIDA, S., “MeshDV: A Distance Vector Mobility-tolerant Routing Protocol for Wireless Mesh Networks”. Em: *IEEE ICPS Workshop on Multi-hop Ad hoc Networks: from theory to reality (REALMAN)*, pp. 103–110, Julho 2005.
- [62] IANNONE, L., KABASSANOV, K., FDIDA, S., “The MeshDVNet Wireless Mesh Network Test-bed”. Em: *International Workshop on Wireless Network Testbeds, Experimental evaluation and CHaracterization (WiNTECH)*, pp. 107–108, Set. 2006.
- [63] PERKINS, C., BHAGWAT, P., “Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers”. Em: *ACM SIGCOMM*, pp. 234–244, Ago. 1994.
- [64] IANNONE, L., FDIDA, S., “MRS: a Simple Cross-layer Heuristic to Improve Throughput Capacity in Wireless Mesh Networks”. Em: *International Conference On Emerging Networking Experiments And Technologies (ConeXt)*, pp. 21–30, Out. 2005.

- [65] IANNONE, L., KABASSANOV, K., FDIDA, S., “The Real Gain of Cross-Layer Routing in Wireless Mesh Networks”. Em: *IEEE ICPS Workshop on Multi-hop Ad hoc Networks: from theory to reality (REALMAN)*, pp. 15–22, Julho 2006.
- [66] IANNONE, L., KABASSANOV, K., FDIDA, S., “Evaluation of Cross-Layer Rate-Aware Routing in a Wireless Mesh Network Test Bed”, *EURASIP Journal on Wireless Communications and Networking*, v. 2007, pp. 1–10, 2007.
- [67] DAS, S. M., PUCHA, H., KOUTSONIKOLAS, D., et al., “DMesh: Incorporating Practical Directional Antennas in Multi-Channel Wireless Mesh Networks”, *IEEE Journal on Selected Areas in Communications*, v. 24, n. 11, pp. 2028–2039, Nov. 2006.
- [68] PEI, G., GERLA, M., CHEN, T.-W., “Fisheye State Routing in Mobile Ad Hoc Networks”. Em: *IEEE Workshop on Wireless Networks and Mobile Computing (ICDCS)*, pp. D71–D78, Abril 2000.
- [69] NELAKUDITI, S., LEE, S., YU, Y., et al., “Blacklist-Aided Forwarding in Static Multihop Wireless Networks”. Em: *IEEE Conference on Sensor and Ad Hoc Communications and Networks (SECON’05)*, pp. 252–262, Set. 2005.
- [70] WANG, J., LEE, S., ZHONG, Z., et al., “Localized On-Demand Link State Routing for Fixed Wireless Networks”. Em: *ACM SIGCOMM*, Ago. 2005.
- [71] MITRE CORPORATION, “Mobile Mesh Routing Protocol”, http://www.mitre.org/work/tech_transfer/mobilemesh/draft-grace-manet-mmrrp-00.txt, 2006.
- [72] MITRE CORPORATION, “Mobile Mesh Link Discovery Protocol”, http://www.mitre.org/work/tech_transfer/mobilemesh/draft-grace-manet-mmldp-00.txt, 2006.

- [73] MITRE CORPORATION, “Mobile Mesh Border Discovery Protocol”, http://www.mitre.org/work/tech_transfer/mobilemesh/draft-grace-manet-mmbdp-00.txt, 2006.
- [74] MITRE CORPORATION, <http://wiki.uni.lu/secan-lab/MobileMesh.html>, 2006.
- [75] MOY, J., “OSPF Version 2”, IETF Network Working Group RFC 2328, Abril 1998.
- [76] CLAUSEN, T., JACQUET, P., LAOUITI, A., et al., “Optimized Link State Routing Protocol”. Em: *IEEE International Multi Topic Conference (INMIC)*, pp. 62–68, Dez. 2001.
- [77] ESPOSITO, P. M., SCHILLER, F. O. S. B., CAMPISTA, M. E. M., et al., “Implementação da Métrica de Roteamento Tempo Esperado de Transmissão em Redes em Malha Sem Fio”. Em: *Workshop de Gerência e Operação de Redes e Serviços (WGRS)*, pp. 25–36, Maio 2007.
- [78] ESPOSITO, P. M., CAMPISTA, M. E. M., MORAES, I. M., et al., “Implementing the Expected Transmission Time Metric for OLSR Wireless Mesh Networks”. Em: *IFIP Network Control conference (Netcon) - Wireless Days Conference*, Nov. 2008.
- [79] CHEN, J., LEE, Y.-Z., MANIEZZO, D., et al., “Performance Comparison of AODV and OFLSR in Wireless Mesh Networks”. Em: *IFIP Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net)*, pp. 271–278, Junho 2006.
- [80] GTA, <http://www.gta.ufrj.br/wmn>, 2008.
- [81] RAMACHANDRAN, K. N., BUDDHIKOT, M. M., CHANDRANMENON, G., et al., “On the Design and Implementation of Infrastructure Mesh Networks”. Em: *IEEE Workshop on Wireless Mesh Networks (WiMesh)*, Set. 2005.

- [82] PERKINS, C. E., ROYER, E. B., “Ad-hoc On-Demand Distance Vector Routing”. Em: *IEEE Workshop on Mobile Computing Systems and Applications*, pp. 90–100, Fev. 1999.
- [83] RANIWALA, A., CHIUEH, T.-C., “Architecture and Algorithms for an IEEE 802.11-Based Multi-Channel Wireless Mesh Network”. Em: *IEEE Conference on Computer Communications (INFOCOM)*, pp. 2223–2234, Março 2005.
- [84] BISWAS, S., MORRIS, R., “ExOR: Opportunistic Multi-Hop Routing for Wireless Networks”. Em: *ACM SIGCOMM*, pp. 133–144, Ago. 2005.
- [85] YUAN, Y., YANG, H., WONG, S., et al., “ROMER: Resilient Opportunistic Mesh Routing for Wireless Mesh Networks”. Em: *IEEE Workshop on Wireless Mesh Networks (WiMesh)*, Set. 2005.
- [86] FALL, K., VARADHAN, K., *The ns Manual*, UC Berkeley, LBL, USC/ISI, and Xerox PARC, Maio 2008.
- [87] JAIN, R., *The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurement, Simulation, and Modeling*. Wiley-Interscience, Abril 1991.
- [88] CHEUNG, D., PRETTIE, C., *A Path Loss Comparison Between the 5 GHz UNII Band (802.11a) and the 2.4 GHz ISM Band (802.11b)*, Rel. técnico, Intel Labs, Jan. 2002.
- [89] CLAUSEN, T., JACQUET, P., “Optimized Link State Routing Protocol (OLSR)”, IETF Network Working Group RFC 3626, Out. 2003.
- [90] XIUCHAO, W., ANANDA, A. L., “Link Characteristics Estimation For IEEE 802.11 DCF Based WLAN”. Em: *IEEE Conference on Local Computer Networks (LCN)*, pp. 302–309, Nov. 2004.
- [91] XIUCHAO, W., *Simulate 802.11b Channel Within NS2*, Rel. técnico, National University of Singapore, 2004.

- [92] HOLLAND, G., VAIDYA, N. H., BAHL, P., “A Rate-Adaptive MAC Protocol for Multi-Hop Wireless Networks”. Em: *ACM International Conference on Mobile Computing and Networking (MobiCom)*, pp. 236–251, Julho 2001.
- [93] ROS, F. J., Acessado em <http://masimum.dif.um.es/um-olsr/html/>, 2005.
- [94] Acessado em <http://www.olsr.org>, 2007.
- [95] BAUMANN, R., HEIMLICHER, S., LENDERS, V., et al., “HEAT: Scalable Routing in Wireless Mesh Networks Using Temperature Fields”. Em: *IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM)*, pp. 1–9, Junho 2007.