Carlos Eduardo Seo

Análise Comparativa Entre Protocolos de Camada MAC para Redes Ad-Hoc Sem Fio

Dissertação de Mestrado apresentada à Faculdade de Engenharia Elétrica e de Computação como parte dos requisitos para obtenção do título de Mestre em Engenharia Elétrica. Área de concentração: Telecomunicações.

Orientador: Prof. Dr. Michel Daoud Yacoub
Co-Orientador: Prof. Dr. Paulo Cardieri

Campinas, SP
2007

FICHA CATALOGRÁFICA ELABORADA PELA
BIBLIOTECA DA ÁREA DE ENGENHARIA E ARQUITETURA - BAE - UNICAMP

Seo, Carlos Eduardo
Se61a Análise comparativa entre protocolos de camada MAC para redes ad-hoc sem fio / Carlos Eduardo Seo. -- Campinas, SP: [s.n.], 2007

Orientadores: Michel Daoud Yacoub, Paulo Cardieri
Dissertação (Mestrado) - Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação.

1. Redes de computação - Protocolos. 2. Sistemas de comunicação sem fio. 3. Sistemas de comunicação móvel. I. Yacoub, Michel Daoud. II. Cardieri, Paulo. III. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. IV. Título.

Título em Inglês:	Comparative analysis between MAC-Level protocols for ad-hoc wireless networks
Palavras-chave em Inglês:	Ad-hoc networks, Mobile communications, Network protocols, MAC layer, IEEE 802.11
Área de concentração:	Telecomunicações e Telemática
Titulação:	Mestre em Engenharia Elétrica
Banca Examinadora:	Ailton Akira Shinoda, Hélio Waldman, Maurício Ferreira Magalhães
Data da defesa:	30 de julho de 2007
Programa de Pós-Graduação:	Engenharia Elétrica

COMISSÃO JULGADORA - TESE DE MESTRADO

Candidato: Carlos Eduardo Seó

Data da Defesa: 30 de julho de 2007

Título da Tese: "Análise Comparativa entre Protocolos de Camada MAC para Redes Ad Hoc Sem Fio"

Prof. Dr. Michel Daoud Yacoub (Presidente): _____

Prof. Dr. Ailton Akira Shinoda: _____

Prof. Dr. Hélio Waldman: _____

Prof. Dr. Mauricio Ferreira Magalhães: _____

Resumo

Este trabalho visa o estudo de redes *ad hoc* sem fio, em especial, os protocolos da subcamada MAC do modelo OSI. Neste tipo de rede sem controle centralizado, o acesso ao meio se torna uma parte crítica no processo de comunicação entre terminais. Assim sendo, a principal motivação deste trabalho é investigar como os protocolos da subcamada MAC podem afetar o desempenho da rede do ponto de vista das aplicações, em especial, tráfego VoIP e de dados. Para tal, foram feitas análises comparativas entre diversos protocolos, baseadas em resultados de simulações feitas no simulador de redes ns-2. Tais resultados mostram que a maior parte das alternativas ao protocolo padrão IEEE 802.11 ainda precisam amadurecer para que possam tornar-se comercialmente viáveis. Um protocolo, no entanto, se destaca dos demais em cenários de tráfego misto (voz e dados), apresentando melhoria de desempenho em relação ao IEEE 802.11: o IEEE 802.11e, variante do IEEE 802.11 com funções de suporte a QoS.

Palavras-chave: Redes ad-hoc, comunicações móveis, protocolos de rede, camada MAC, IEEE 802.11.

Abstract

This work presented here is focused on studying ad hoc wireless networks, in particular, the MAC sublevel protocols from the OSI reference model. In these networks, the lack of a centralized control makes the medium access control a critical part in the communication process between network terminals. Thus, the main objective of this work is to investigate how the MAC sublevel protocols may interfere in network performance from the application point of view, in particular, VoIP and data transmission. In order to accomplish this goal, several comparative analysis between protocols have been made, based on simulation results from the ns-2 network simulator. The results show that the alternatives to the IEEE 802.11 standard suggested so far aren't mature enough to be commercially viable, although there is one protocol that is very promising: the IEEE 802.11e, a variant of IEEE 802.11 with QoS support functions.

Keywords: Ad-hoc networks, mobile communications, network protocols, MAC layer, IEEE 802.11.

Agradecimentos

Ao meu orientador, Prof. Dr. Michel Daoud Yacoub, e meu co-orientador, Prof. Dr. Paulo Cardieri, sou grato pela orientação.

Ao Prof. Élvio João Leonardo, pela ajuda no decorrer dos estudos dos protocolos MAC, ferramentas de simulação e elaboração de artigos.

Aos colegas Álvaro Medeiros e David Muñoz, pela ajuda ao longo deste trabalho.

A minha família e amigos pelo apoio durante esta jornada.

À minha família, colegas e professores da
Faculdade de Engenharia Elétrica e
de Computação da Unicamp

Sumário

Lista de Figuras **xi**

Lista de Tabelas **xiii**

Glossário **xv**

Lista de Símbolos **xvii**

Trabalhos Publicados Pelo Autor **xix**

1 Introdução **1**
1.1 Contribuições 2
1.2 Estrutura da Dissertação 3

2 Mecanismo de Acesso ao Meio **5**
2.1 Problemas a Serem Contornados Durante o Projeto de um Protocolo MAC 5
2.1.1 Eficiência Espectral 5
2.1.2 Suporte à Qualidade de Serviço (QoS) 6
2.1.3 Terminal Escondido e Terminal Exposto 6
2.1.4 Erros na transmissão devido à natureza do canal sem fio 7
2.2 Alguns Protocolos MAC 7
2.2.1 Padrão IEEE 802.11 8
2.2.2 TDMA-W 11
2.2.3 Distributed Priority Scheduling 11
2.2.4 Multiple Access Collision Avoidance with Piggy-Backed Reservation 13
2.2.5 IEEE 802.11e 16

3 O simulador de redes ns-2 **19**
3.1 Breve Histórico 19
3.2 Arquitetura 19
3.3 Formato dos Dados de Saída 20
3.4 Considerações Finais a Respeito do ns-2 21

4 Simulações e Resultados Comparativos entre IEEE 802.11, DPS e MACA-PR para um Arranjo Linear de Nós **23**
4.1 Topologia . . . 23
4.2 Camada Física . . . 24
4.3 Camada MAC e Roteamento . . . 24
4.4 Modelos de Tráfego . . . 25
4.5 Resultados das Simulações . . . 25
4.5.1 Tráfego CBR . . . 26
4.5.2 Tráfego FTP . . . 28
4.6 Conclusões . . . 30

5 Simulações e Resultados Comparativos entre IEEE 802.11 e IEEE 802.11e em WMN **33**
5.1 Topologia . . . 33
5.2 Camada Física . . . 33
5.3 Camada MAC e Roteamento . . . 34
5.4 Modelos de Tráfego . . . 35
5.5 Resultados das Simulações . . . 36
5.5.1 Um *Gateway*, Apenas Tráfego CBR . . . 36
5.5.2 Cinco *gateways*, apenas tráfego CBR . . . 37
5.5.3 Tráfego misto com um *gateway* . . . 39
5.6 Conclusões . . . 41

6 Análise da Influência da Carga Oferecida e do Alcance de Interferência no Desempenho do IEEE 802.11 em WMN **43**
6.1 Influência da Carga Oferecida . . . 43
6.2 Influência do Alcance de Transmissão e do Alcance de Interferência . . . 45
6.3 Conclusões . . . 46

7 Análise da Influência do Mecanismo de Handshaking RTS/CTS no Tráfego VoIP para o IEEE 802.11 em WMN **49**
7.1 Requisitos do Tráfego VoIP e QoS . . . 49
7.2 Cenários de Simulação . . . 50
7.3 Resultados das Simulações . . . 51
7.3.1 Apenas um *gateway* . . . 51
7.3.2 Rede com Dois *Gateways* . . . 51
7.3.3 Rede com Quatro *Gateways* . . . 54
7.4 Conclusões . . . 56

8 Simulações e Resultados Comparativos entre IEEE 802.11 e IEEE 802.11e em WMN com Tráfego VoIP **59**
8.1 Cenários de Simulação . . . 59
8.2 Resultados . . . 60
8.2.1 Desempenho do IEEE 802.11b - Apenas Tráfego VoIP . . . 60
8.2.2 Desempenho do IEEE 802.11e - Apenas Tráfego VoIP . . . 62

8.2.3 Desempenho do IEEE 802.11b - Tráfego VoIP e FTP 64
8.2.4 Desempenho do IEEE 802.11e - Tráfego VoIP e FTP 65
8.3 Conclusões 67

9 Conclusão **69**
9.1 Conclusões Gerais 69
9.2 Trabalhos Futuros 71

Referências bibliográficas **72**

A Apêndice A **75**
A.1 Algoritmo de geração de tráfego VoIP 75
A.2 Exemplo de simulação: grid 7x7, tráfego VoIP 76

Lista de Figuras

1.1 Exemplo de rede *ad hoc*. 2

2.1 Problema do terminal escondido: os terminais A e C não se enxergam, mas ambos enxergam B. 6
2.2 Problema do terminal exposto: o terminal B está transmitindo para A. O terminal C deseja transmitir para D, mas percebe o meio como ocupado e inibe sua transmissão. No entanto, uma transmissão de C para D não causaria colisões. 7
2.3 IEEE 802.11 DCF. 9
2.4 Mecanismo de RTS/CTS do IEEE 802.11. 10
2.5 Acesso ao meio no DPS: mecanismo de *piggyback* associado ao *handshake* de 4 vias do IEEE 802.11. 12
2.6 Mecanismo de acesso ao meio do MACA-PR: tráfego não sensível ao atraso. 14
2.7 Mecanismo de acesso ao meio do MACA-PR: tráfego sensível ao atraso. 15

4.1 Topologia do tipo cadeia linear de nós. 23
4.2 Atraso médio para o tráfego CBR. 26
4.3 Vazão média para o tráfego CBR. 26
4.4 Variação do atraso para o tráfego CBR. 27
4.5 Taxa de perdas para o tráfego CBR. 27
4.6 Vazão média para o tráfego FTP. 29
4.7 Atraso médio para o tráfego FTP. 29
4.8 Variação do atraso para o tráfego FTP. 30
4.9 Taxa de perdas para o tráfego FTP. 30

5.1 Topologia do tipo grade de nós 7x7 com um *gateway*. 34
5.2 Topologia do tipo grade de nós 7x7 com cinco *gateways*. As setas indicam quais nós se comunicam com cada *gateway*. 35
5.3 Vazão por nó para o caso de um *gateway*. 36
5.4 Atraso médio por enlace para o caso de um *gateway*. 37
5.5 Vazão por nó para o caso de cinco *gateways*. 38
5.6 Atraso médio por enlace para o caso de cinco *gateways*. 38
5.7 Topologia do tipo grade de nós 7x7 com um *gateway* e tráfego de fundo FTP. Os nós azuis são os geradores de tráfego CBR e se comunicam com o *gateway*. Os pares de nós coloridos são os que se comunicam via FTP. 39
5.8 Vazão por nó para o caso de um *gateway* e tráfego misto. 40

5.9 Atraso médio por enlace para o caso de um *gateway* e tráfego misto. 40

6.1 Vazão da rede em função da carga oferecida. 44
6.2 Atraso médio na rede em função da carga oferecida. 44
6.3 Resultados para o tráfego CBR. 45
6.4 Resultados para o tráfego FTP. 46

7.1 Cenário para a simulação com um *gateway*. 52
7.2 Atraso médio em ms para o cenário com um *gateway*. 52
7.3 Variação do atraso em ms para o cenário com um *gateway*. 53
7.4 Taxa de perdas para o cenário com um *gateway*. 53
7.5 Cenário para a simulação com dois *gateways*. 54
7.6 Atraso médio em ms para o cenário com dois *gateways*. 54
7.7 Variação do atraso em ms para o cenário com dois *gateways*. 55
7.8 Taxa de perdas para o cenário com dois *gateways*. 55
7.9 Cenário para a simulação com quatro *gateways*. 56
7.10 Atraso médio em ms para o cenário com quatro *gateways*. 56
7.11 Variação do atraso em ms para o cenário com quatro *gateways*. 57
7.12 Taxa de perdas para o cenário com quatro *gateways*. 57

8.1 Atraso médio fim-a-fim por enlace para o 802.11b com tráfego VoIP. 61
8.2 Taxa de perdas por enlace para o 802.11b com tráfego VoIP. 61
8.3 Atraso médio fim-a-fim por enlace para o 802.11e com tráfego VoIP. 63
8.4 Taxa de perdas por enlace para o 802.11e com tráfego VoIP. 63
8.5 Atraso médio fim-a-fim por enlace para o 802.11b com tráfego misto. 64
8.6 Taxa de perdas por enlace para o 802.11b com tráfego misto. 65
8.7 Atraso médio fim-a-fim por enlace para o 802.11e com tráfego misto. 66
8.8 Taxa de perdas por enlace para o 802.11e com tráfego misto. 66

Lista de Tabelas

5.1 Valores médios para o cenário de um *gateway* com tráfego CBR. 36
5.2 Valores médios para o cenário de cinco *gateways* com tráfego CBR. 38
5.3 Valores médios para o cenário de um *gateway* com tráfego misto. 41

6.1 Grupos de usuários ativos. 43

8.1 Atribuição de prioridades na MAC para a simulação do IEEE 802.11e. 65

Glossário

AC - Access Category
ACK - Acknowledgement
AIFS - Arbitration Inter-Frame Space
AODV - Ad Hoc On-Demand Distance-Vector
CBR - Constant Bit Rate
CONSER - Collaborative Simulation for Education and Research
CSMA/CA - Carrier Sense Multiple Access/Collision Avoidance
CTS - Clear to Send
CW - Contention Window
DARPA - Defense Advanced Research Projects Agency
DCF - Distributed Coordination Function
DIFS - DCF Inter-Frame Spacing
DPS - Distributed Priority Scheduling
DSDV - Destination-Sequenced Distance Vector
DSR - Dynamic Source Routing
EDCF - Enhanced Distributed Coordination Function
EDF - Earliest Deadline First
FTP - File Transfer Protocol
HCF - Hybrid Coordination Function
HMM - Horário de Maior Movimento
HOL - Head of Line
IEEE - Institute of Electrical and Electronics Engineers
ISM - Industrial, Scientific and Medical
ITU-T - International Telecommunication Union - Telecommunication Standardization Sector
LAN - Local Area Network
LBL - Lawrence Berkeley National Laboratory
MAC - Medium Access Control
MACA-PR - Multiple Access Collision Avoidance with Piggy-Backed Reservation
MACAW - Multiple Access Collision Avoidance for Wireless LANs
MSDU - MAC Service Data Unit
NAV - Network Allocation Vector
NSF - National Science Foundation
OSI - Open Systems Interconnection
PARC - (Xerox) Palo Alto Research Center
PCF - Point Coordination Function
PCM - Pulse Code Modulation
QoS - Quality of Service
RF - Rádio-freqüência

RT - Reservation Table
RTS - Request to Send
SAMAN - Simulation Augmented by Measurement and Analysis for Networks
SIFS - Short Inter-Frame Spacing
s-slot - Transmit/Send Slot
TCP - Transmission Control Protocol
TDMA - Time Division Multiple Access
TTL - Time To Live
TXOP - Transmission Oportunity
UCB - University of California, Berkeley
UDP - User Datagram Protocol
UP - User Priority
USC/ISI - University of Southern California/Information Sciences Institute
VoIP - Voice over IP
Wi-Fi - Wireless Fidelity
WissTek - Wireless Technlogy Laboratory
WLAN - Wireless Local Area Network
WMN - Wireless Mesh Network
w-slot - Wakeup Slot

Lista de Símbolos

CW_{min} - Tempo mínimo da janela de contenção da DCF do IEEE 802.11.
CW_{max} - Tempo máximo da janela de contenção da DCF do IEEE 802.11.
d_{CS} - Alcance máximo de interferência.
d_{Tx} - Alcance máximo de transmissão.
$f(S_j)$ - Função distribuição do tempo de *back-off* no DPS.
P_i - Índice de prioridade do pacote a ser transmitido no DPS.
r_j - Posição ocupada pelo terminal j na tabela de agendamento no DPS.
S_j - Tabela de agendamento do terminal j no DPS.
$U[a, b]$ - Distribuição uniforme entre a e b.

Trabalhos Publicados Pelo Autor

1. D.M. Gallego, A.M. Medeiros, P. Cardieri, M.D. Yacoub, C.E. Seo, E.J. Leonardo. "Capacity and QoS of Wireless Mesh Networks". *4th International Information and Telecommunication Technologies Symposium* (I2TS 2005), Florianópolis, Santa Catarina, Brasil, Dezembro de 2005.

2. D.M. Gallego, A.M. Medeiros, P. Cardieri, M.D. Yacoub, C.E. Seo, E.J. Leonardo. "Capacidade das redes WMN em ambientes com desvanecimento". *XXII Simpósio Brasileiro de Telecomunicações,* (SBrT '05), Campinas, São Paulo, Brasil, Setembro de 2005.

3. C.E. Seo, E.J. Leonardo, P. Cardieri, M.D. Yacoub, D.M. Gallego, A.M. Medeiros. "Performance of IEEE 802.11 in Wireless Mesh Networks". *International Microwave and Optoelectronics Conference* (IMOC 2005), Brasília, Distrito Federal, Brasil, Julho de 2005.

Capítulo 1

Introdução

A expressão *ad hoc* significa "para um determinado propósito e ocasião específicos" [1]. Este é um dos princípios que fundamentam as redes ad hoc sem fio: redes descentralizadas, sem a necessidade de infra-estrutura, nas quais os terminais podem se comunicar entre si. Tais redes, justamente por não necessitarem de infra-estrutura e controle centralizado, possuem custo baixo e podem ser facilmente instaladas e desinstaladas, sendo bastante úteis em situações bem específicas, como por exemplo comunicação militar em território inimigo, suporte em operações de resgate e emergência, reuniões, convenções ou redes de sensores para coleta de informações em lugares inóspitos [2, 3]. Outro ponto importante de ser citado em redes ad hoc é o fato de haver possibilidade de se estabelecer conexões compostas de múltiplos saltos (*multihop*), nas quais os nós da rede podem repassar informações até que estas cheguem ao seu destino final (figura 1.1). Esta característica difere de uma rede celular, na qual a comunicação se estabelece em apenas um *hop* entre o móvel e a estação rádio-base (ou vice-versa) e não há repasse de informação por parte dos terminais [4]. Isto confere às redes *ad hoc* uma topologia dinâmica e flexível, tornando a comunicação menos vulnerável a falhas de conexão, pois ao se detectar falha em algum enlace, uma nova rota pode ser utilizada, e ainda oferece maior mobilidade aos usuários.

Certamente existem também algumas desvantagens, como por exemplo a complexidade dos terminais, que devem apresentar um mecanismo complexo de acesso ao meio (camada MAC) a fim de evitar problemas relacionados à colisão de pacotes, o roteamento adequado de pacotes utilizando protocolos dinâmicos de roteamento apropriados, a alta latência devido à comunicação *multihop* e o fato de a rede *ad hoc* ser inerentemente insegura, gerando uma preocupação maior com o tratamento da segurança das informações transmitidas. Adicionam-se ainda todos os problemas inerentes às redes sem fio: baixa taxa de transmissão, alta probabilidade de erro, a grande variabilidade das condições do meio de transmissão [5] e a limitação no consumo de energia por parte dos terminais, visto que nessas redes eles são geralmente alimentados por fontes de energia limitadas (baterias),

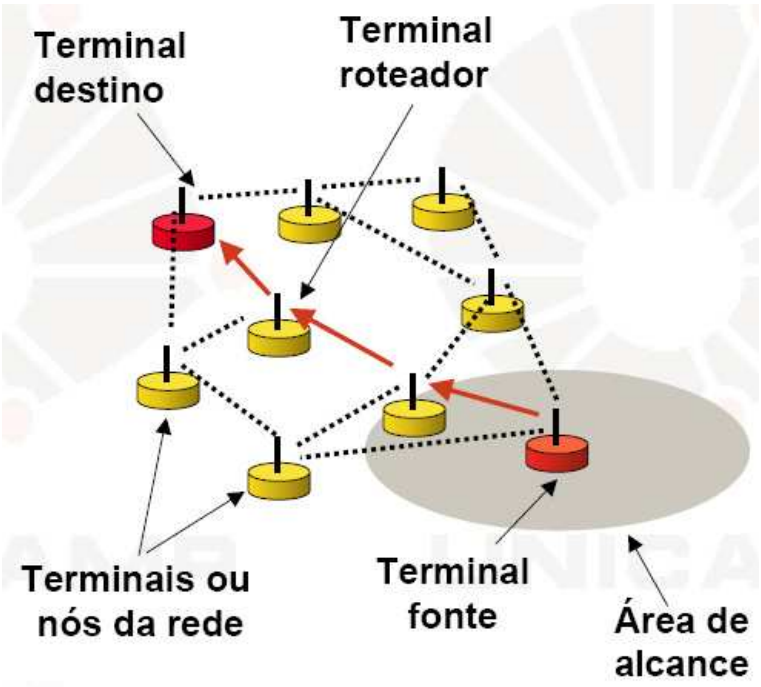

Fig. 1.1: Exemplo de rede *ad hoc*.

resultando em uma capacidade reduzida de processamento local.

Os pontos críticos citados anteriormente fazem com que ainda existam muitos desafios nessa área. Um dos pontos cruciais para o bom funcionamento das redes *ad hoc* reside nos protocolos de acesso ao meio, que deve garantir a eqüidade na alocação dos recursos do canal rádio compartilhado para todos os terminais.

1.1 Contribuições

Este trabalho tem como objetivo avaliar o mecanismo de controle de acesso ao meio nessas redes, através do estudo de alguns protocolos MAC disponíveis para o simulador ns-2 e análise comparativa da influência desses no desempenho de tráfego de voz em uma rede ad hoc através de simulações utilizando o simulador de redes ns-2. Traz como contribuições uma análise detalhada da influência do protocolo MAC IEEE 802.11 no desempenho de redes *ad hoc*, especialmente WMN, comparações de desempenho através de simulações entre o padrão IEEE 802.11 e outros protocolos sugeridos pelo meio acadêmico e pelo próprio IEEE, um estudo dos diferentes usos possíveis das prioridades do IEEE 802.11e e uma análise da viabilidade comercial do uso das redes WMN na implementação de serviços de telefonia VoIP.

1.2 Estrutura da Dissertação

O restante desta dissertação está estruturado da seguinte forma: o capítulo 2 traz uma descrição sobre o mecanismo de controle de acesso ao meio em redes, os problemas a serem contornados ao se projetar um protocolo MAC e uma descrição detalhada dos protocolos MAC mais citados na literatura. Em seguida, o capítulo 3 traz um histórico e uma descrição do simulador de redes ns-2, que foi utilizado em todas as simulações computacionais deste trabalho. Exemplos de códigos-fonte para o ns-2 estão disponíveis no Apêndice A. No capítulo 4, são mostradas as primeiras simulações realizadas no ns-2, em um cenário simples, a fim de comparar o desempenho de alguns protocolos: IEEE 802.11, DPS e MACA-PR. Devido aos resultados pouco promissores para os protocolos DPS e MACA-PR, o trabalho muda seu foco para o protocolo IEEE 802.11e que, segundo a literatura, se apresenta bastante promissor. Visando uma simulação mais próxima da realidade, o capítulo 5 traz um cenário mais real e complexo, do tipo grade de nós com *gateway* para escoamento de tráfego, simulando uma WMN, para a comparação de desempenho entre o IEEE 802.11 e o IEEE 802.11e. Para enriquecer mais este trabalho, foi feita uma análise mais profunda sobre o funcionamento do IEEE 802.11 nos capítulos 6 e 7, visto que esse protocolo é a base do IEEE 802.11e. No capítulo 6 é feita uma análise da influência da carga oferecida e do alcance de interferência no desempenho do IEEE 802.11. Já no capítulo 7, é analisada a relevância do mecanismo de *handshaking* RTS/CTS do IEEE 802.11 no desempenho da rede quando temos tráfego VoIP. Nesse mesmo capítulo é mostrado um algoritmo de geração de tráfego VoIP para o ns-2 que foi desenvolvido a fim de possibilitar as simulações. O capítulo 8 faz uma comparação do desempenho do IEEE 802.11 e do IEEE 802.11e com tráfego VoIP e discute a viabilidade prática de se utilizar redes do tipo WMN para implementação de telefonia VoIP. Por fim, o capítulo 9 traz as conclusões deste trabalho.

Capítulo 2

Mecanismo de Acesso ao Meio

Em uma rede *ad hoc* sem fio os terminais, em geral, compartilham um canal de rádio comum. Como o espectro é limitado, a banda disponível para a comunicação na rede também é limitada. O acesso a esse meio compartilhado deve ser devidamente controlado de tal forma que exista eqüidade na disponibilidade dos recursos do canal para cada um dos nós. Como as redes *ad hoc* apresentam características bastante peculiares tais como mobilidade, banda limitada, canal mais sucetível a erros, limitações de potência e problemas de terminal escondido e terminal exposto (descritos a seguir), os protocolos de controle de acesso ao meio (MAC) para essas redes apresentam características bem particulares. A seguir serão citadas algumas questões que devem ser exploradas quando se projeta um protocolo MAC para redes *ad hoc* sem fio [4].

2.1 Problemas a Serem Contornados Durante o Projeto de um Protocolo MAC

2.1.1 Eficiência Espectral

Alguns aspectos estão diretamente relacionados ao uso do espectro em redes *ad hoc* [6]:

1. A natureza descentralizada, que faz com que o acesso ao meio seja controlado através da troca de pacotes de controle entre os nós;
2. A troca de pacotes de controle a fim de manter o sincronismo necessário para o funcionamento de alguns protocolos, como os baseados em TDMA, por exemplo;
3. O espectro limitado que é compartilhado entre todos os nós da rede.

Visando a uma utilização eficiente do espectro, qualquer protocolo MAC deve minimizar o *overhead* de controle do protocolo e maximixar a carga útil na rede.

2.1.2 Suporte à Qualidade de Serviço (QoS)

Devido à natureza das redes *ad hoc* sem fio, em que pode existir mobilidade dos nós, prover QoS é muito difícil. A mobilidade afeta diretamente a vazão da rede [5]: em uma rede *ad hoc* sem fio com nós móveis, a topologia da rede é constantemente alterada e as reservas de canal e troca de mensagens de controle tornam-se ineficientes. Adiciona-se ainda o fato de haver constantes quebras de conexão devido à mobilidade e tem-se um cenário bastante adverso para a provisão de QoS, que é essencial em transmissões nas quais o tempo de trânsito dos pacotes entre fonte e destino é limitado, como transmissão de voz, por exemplo.

O protocolo MAC deve possuir algum tipo de mecanismo de reserva de recursos que leve em consideração a mobilidade dos nós e a natureza do canal sem fio a fim de prover QoS para tais serviços.

2.1.3 Terminal Escondido e Terminal Exposto

Esses dois problemas são exclusivos de redes sem fio. O problema do terminal escondido [6, 7] se refere à situação em que ocorre colisão de pacotes num nó receptor devido à transmissão simultânea de pacotes de dois ou mais nós que enxergam o receptor, porém estão fora de alcance entre si. Esta situação é mostrada na figura 2.1.

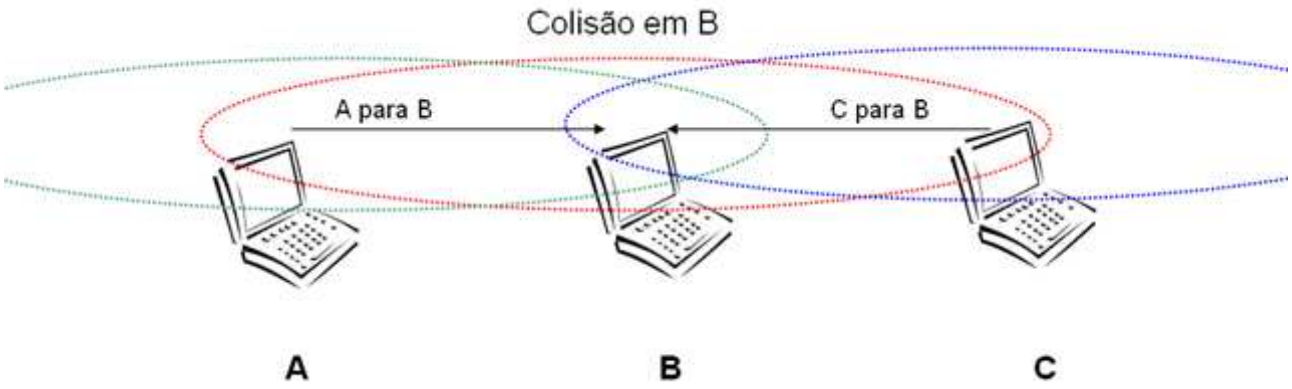

Fig. 2.1: Problema do terminal escondido: os terminais A e C não se enxergam, mas ambos enxergam B.

Já o problema de terminal exposto [6] se refere à incapacidade de um nó de transmitir sua informação devido ao bloqueio no acesso ao meio causado por uma transmissão próxima (dentro de seu alcance), porém para um destinatário diferente (ver figura 2.2).

É desejável que o protocolo MAC tenha algum tipo de mecanismo a fim de evitar ambos os problemas que podem causar queda significativa na vazão da rede.

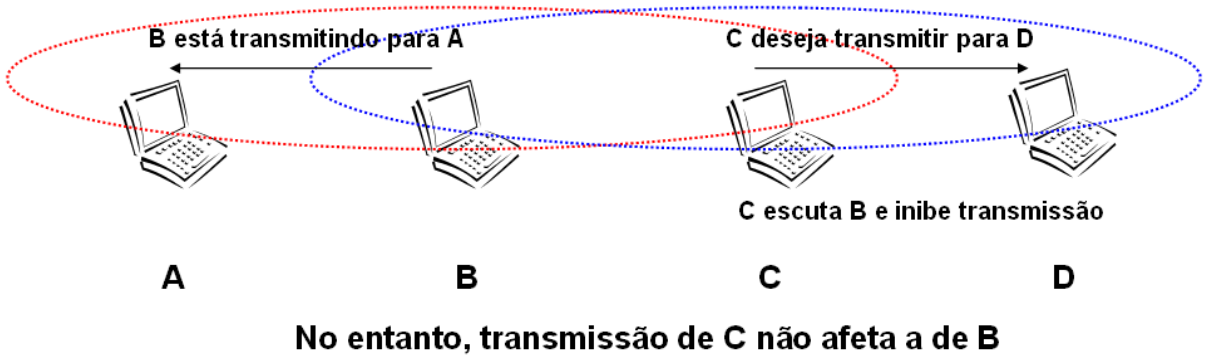

Fig. 2.2: Problema do terminal exposto: o terminal B está transmitindo para A. O terminal C deseja transmitir para D, mas percebe o meio como ocupado e inibe sua transmissão. No entanto, uma transmissão de C para D não causaria colisões.

2.1.4 Erros na transmissão devido à natureza do canal sem fio

Em comunicações sem fio, quando um nó transmite uma mensagem, esta é recebida por todos os nós dentro de sua área de alcance. Quando um nó está recebendo dados, nenhum outro nó na vizinhança, exceto a fonte, deve transmitir por questões de interferência [4]. Um nó só deve acessar o meio compartilhado quando sua transmissão não afeta nenhuma outra já em andamento. No entanto, existe a possibilidade de vários nós acessarem o canal simultaneamente e, com isso, a probabilidade de ocorrerem colisões de pacotes é relativamente alta em redes sem fio. O protocolo MAC deve garantir o acesso ao meio de tal forma que as colisões sejam minimizadas. Além disso, o protocolo deve garantir a eqüidade no acesso ao meio a todos os nós [8]. Em uma rede *ad hoc* sem fio, cada um dos nós pode gerar e encaminhar tráfego, havendo uma disputa de acesso ao meio entre o tráfego gerado e o repassado. A eqüidade representa a alocação justa dos recursos de forma a equilibrar o uso do canal entre o tráfego gerado e o encaminhado.

2.2 Alguns Protocolos MAC

Tendo em mente todos os problemas mencionados na seção anterior a serem contornados, pode-se fazer uma melhor análise dos protocolos MAC disponíveis atualmente. Nesta seção, serão apresentados alguns protocolos MAC escolhidos para estudo no decorrer deste trabalho. Todos apresentam implementação para o simulador ns-2, embora alguns tenham limitações que serão citadas mais adiante.

2.2.1 Padrão IEEE 802.11

O padrão IEEE 802.11 [9] é predominante em redes sem fio atualmente. Sua versão 802.11b, comercialmente conhecida como *Wi-Fi*, é amplamente difundida no mercado. O padrão engloba a Camada Um (camada física) e uma das subcamadas da Camada Dois (subcamada MAC) do modelo de rede OSI. Além disso, existem dois modos de operação suportados pelo padrão: infra-estrutura (no qual os nós se comunicam com um ponto de acesso fixo) e *ad hoc* (no qual os nós comunicam-se entre si, sem a necessidade de controle centralizado). A seguir será apresentada uma descrição do mecanismo de acesso ao meio, ou seja, da subcamada MAC para o modo de operação *ad hoc* [9].

O método de acesso utilizado pelo 802.11 no modo ad hoc é através de uma função de coordenação distribuída (DCF). Essa função é baseada numa versão do CSMA/CA. A seguir, é feita uma breve descrição do mecanismo de acesso ao meio do 802.11:

1. Se o meio está ocioso por um intervalo de tempo chamado DIFS, o nó acessa o meio para iniciar a transmissão. Logo, pode-se afirmar que em situações de carga leve, o atraso de acesso ao canal é igual a DIFS.
2. Caso o meio esteja ocupado após a duração de DIFS, o nó espera um intervalo de tempo aleatório chamado tempo de *back-off*, cujo valor é escolhido dentro de um intervalo chamado de janela de contenção (CW), que varia de CW_{min} até CW_{max}. Inicialmente, a CW tem duração aleatória escolhida entre 0 e CW_{min}. Pequenas CWs implicam em intervalos de *back-off* muito próximos um dos outros, fazendo com que a probabilidade de colisão seja alta. Logo, para cada colisão que ocorre, a CW tem a sua duração duplicada, sendo essa duração limitada por CW_{max}. Quando uma transmissão é efetuada com sucesso, a duração da CW é reiniciada, ou seja, volta a ser um valor aleatório escolhido entre 0 e CW_{min}.
3. Após a escolha do valor de *back-off*, um contador entra em ação e vai sendo decrementado até que se chegue em zero, quando o nó ganha o acesso ao meio e transmite seu dado. Neste momento, todos os nós que ouvirem a transmissão atualizam seus respectivos NAVs, os quais determinam o instante de tempo mais próximo em que um nó pode iniciar uma transmissão.
4. Durante o procedimento de *back-off*, se o nó detecta o meio ocupado, o contador de *back-off* é paralisado e este só volta a ser decrementado quando o nó detecta o meio ocioso por um intervalo de tempo igual a DIFS.
5. Cada um dos nós executa o procedimento de *back-off* pelo menos uma vez entre toda transmissão bem-sucedida.

É importante notar que nesse mecanismo a chance que cada um dos terminais tem de transmitir um dado na próxima tentativa é sempre igual para todos, independente do tempo total de espera para a transmissão. Além disso, devido ao mecanismo de funcionamento da CW, nós que já efetuaram uma transmissão com sucesso possuem uma CW menor que os nós que ainda não transmitiram. Conseqüentemente, o tempo de *back-off* para os nós que já conseguiram transmitir é menor.

Logo, tal mecanismo não garante a eqüidade no acesso ao meio. Em outras palavras, o mecanismo de acesso ao meio do 802.11 favorece os terminais que já executaram uma transmissão com sucesso, em detrimento daqueles que tentam acessar o meio a fim de transmitir sua informação. Numa situação ideal, desejar-se-ia que os nós que esperaram mais para transmitir tenham prioridade maior.

Outro mecanismo importante no 802.11 é a transmissão de pacotes de confirmação (ACK). Tais pacotes precisam ser enviados após a recepção de um dado para garantir que sua entrega tenha sido bem sucedida. Após a recepção do dado, o nó receptor espera um intervalo de tempo chamado de SIFS e envia um pacote ACK. Os outros nós devem então esperar por DIFS mais o tempo de *back-off*, reduzindo a probabilidade de colisão, já que a prioridade de um pacote ACK é maior pois o SIFS é menor que a soma de DIFS com o tempo de *back-off*. Caso não haja a recepção de um pacote de ACK por parte do nó origem, este tenta retransmitir o dado até que, ou receba um ACK, ou o número de tentativas de retransmissão chegue no limite e a camada MAC informe a camada superior que a transmissão falhou. Na figura 2.3, é mostrado um esquema completo de fucionamento da DCF.

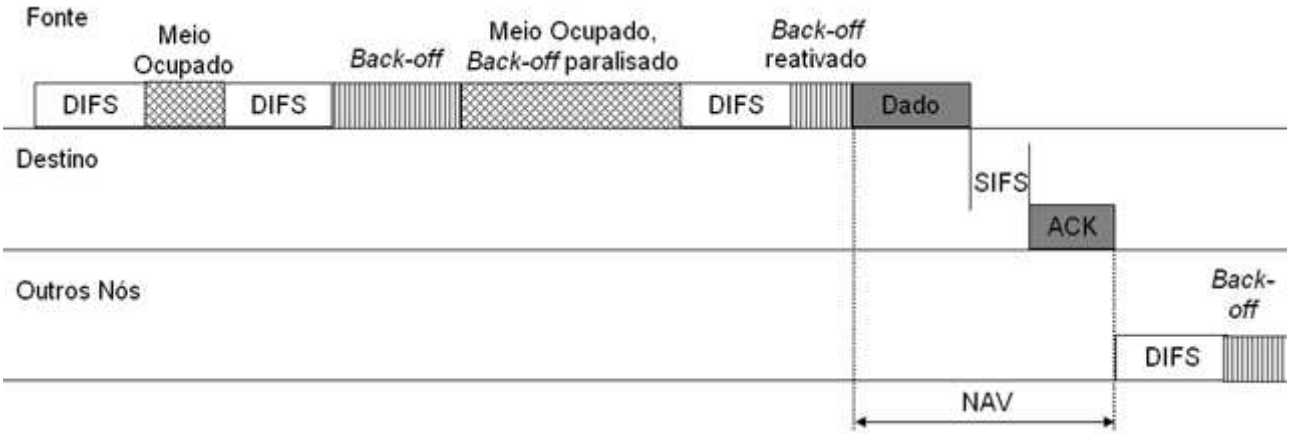

Fig. 2.3: IEEE 802.11 DCF.

Para tentar minimizar o problema de terminal escondido, o 802.11 possui um mecanismo opcional de *handshaking* RTS/CTS descrito a seguir e ilustrado na figura 2.4:

1. O transmissor envia um pacote RTS para o receptor. O pacote inclui informação sobre o destinatário do próximo pacote de dados a ser transmitido e o tempo total da transmissão do dado. O RTS é recebido por todos os nós dentro do raio de alcance do

transmissor.

2. Cada um dos nós que recebeu o RTS atualiza seu NAV.

3. Depois de esperar SIFS, o receptor envia um pacote CTS se estiver apto a receber o dado. O pacote contém informações sobre a duração da transmissão. O CTS é recebido por todos os nós e dentro do raio de alcance do receptor.

4. Todos os nós que receberam o CTS atualizam seus NAVs. Como o conjunto de nós que recebeu o RTS não é necessariamente o mesmo que recebeu o CTS, fica evidente a existência de alguns terminais escondidos.

5. Depois que o CTS é recebido pelo transmissor, todos os nós ao redor do transmissor e do receptor ficam cientes que o meio está reservado exclusivamente para apenas um transmissor. O transmissor então espera SIFS e inicia a transmissão do dado.

6. O receptor, depois de receber o dado, espera SIFS e envia um ACK.

7. Depois da conclusão da transmissão, o NAV de todos os nós envolvidos no processo indica que o meio está livre (exceto no caso que algum desses nós tenha recebido algum outro RTS ou CTS durante o processo).

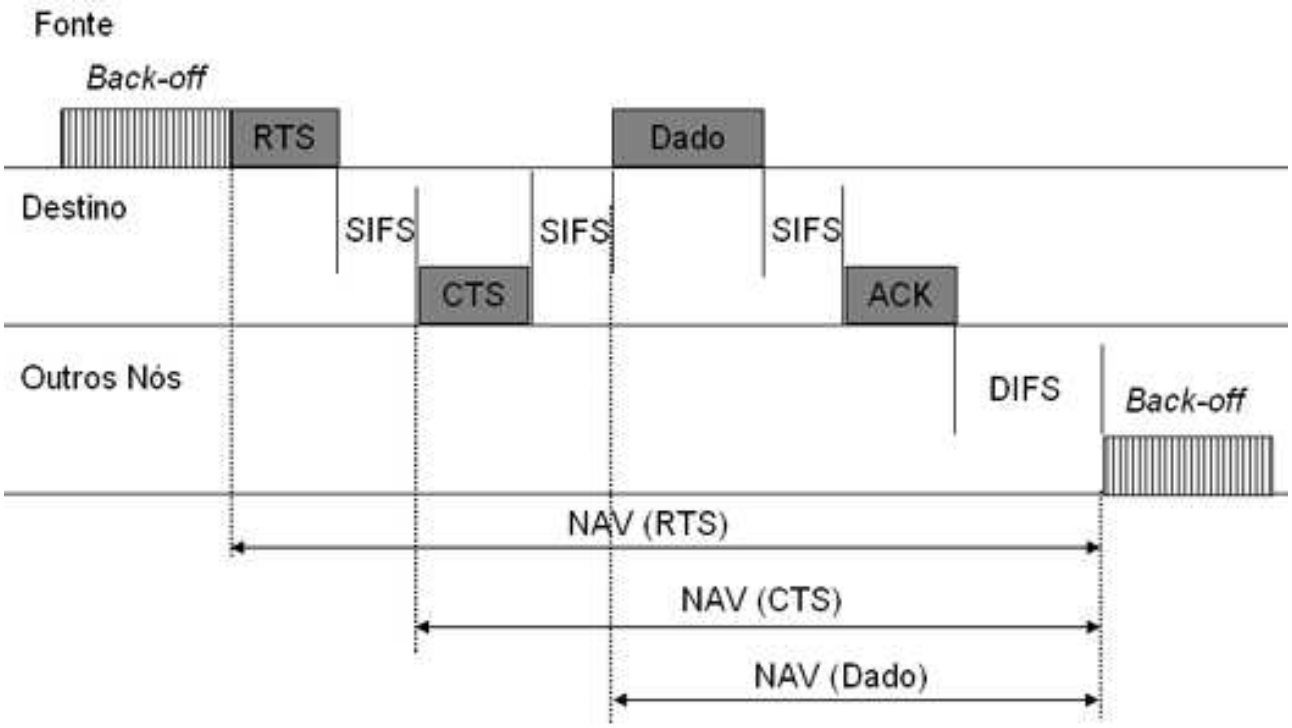

Fig. 2.4: Mecanismo de RTS/CTS do IEEE 802.11.

É importante notar que pacotes RTS e CTS são como quaisquer outros pacotes e podem ocorrer colisões envolvendo qualquer um dos dois. Também se nota que existe a inclusão de um *overhead*

não desprezível ao se usar esse mecanismo. O que se faz é adotar um limiar baseado no tamanho do pacote para habilitar ou desabilitar o mecanismo: se o tamanho do pacote é maior que o limiar, o mecanismo é habilitado; caso contrário, é desabilitado.

O IEEE 802.11 DCF está completamente implementado no ns-2 e é um dos protocolos escolhidos para as simulações.

2.2.2 TDMA-W

O TDMA-W [10] é um protocolo MAC baseado na mesma técnica de acesso TDMA utilizada pelo sistema IS-136 em redes celulares. Neste protocolo, são designados dois *time slots* de um quadro TDMA para cada um dos nós: o s-slot e o w-slot. Cada um dos nós monitora o canal durante o w-slot e transmite no s-slot se necessário.

Durante uma transmissão, apenas os destinatários escutam o transmissor. Os outros nós podem desligar seus circuitos de RF para economizar energia. Para ativar um nó, o transmissor envia um pacote de *wakeup* ao destinatário. Ao receber o pacote, o destinatário identifica o transmissor e começa a escutá-lo dutante o s-slot associado ao nó origem.

Este protocolo é mais utilizado em redes de sensores, uma das aplicações práticas do conceito de redes *ad hoc*, visto que numa rede desse tipo a taxa de transmissão é baixa e, como existem muitos slots disponíveis, a probablidade de dois nós selecionarem o mesmo slot como sendo seu s-slot ao mesmo tempo é muito baixa.

O protocolo possui uma implementação bastante limitada no ns-2, podendo ser utilizado apenas para redes com comunicação de um salto (*single-hop*). Devido a essa limitação, este protocolo não será utilizado nas análises.

2.2.3 Distributed Priority Scheduling

O DPS [11] é um protocolo baseado no MAC do 802.11 que trabalha com um esquema de agendamento distribuído no qual cada nó constrói uma tabela de agendamento baseada em informações recebidas por ele. As informações necessárias para a construção da tabela estão presentes nos pacotes de controle e dados transmitidos pelos terminais vizinhos. Em especial, os pacotes de dados devem carregar informações (*piggyback*) a respeito da situação do nó transmissor. A seguir, é descrito o funcionamento deste mecanismo, ilustrado na figura 2.5:

1. Fonte e destino trocam pacotes de RTS e CTS antes da transmissão do dado. Os terminais que recebem tais pacotes utilizam as informações contidas nesses para atualizar suas tabelas de agendamento. As informações de controle são: fonte, destino, duração do pacote de dados e índice de prioridade P_i do pacote de dados a ser transmitido.

2. Ocorre então a transmissão do dado seguida de um ACK. Ambas as transmissões também carregam informações de controle, informando a existência de um possível pacote na fila do terminal fonte (pacote HOL). Essas informações também são usadas pelos nós vizinhos para atualização de suas tabelas de agendamento.

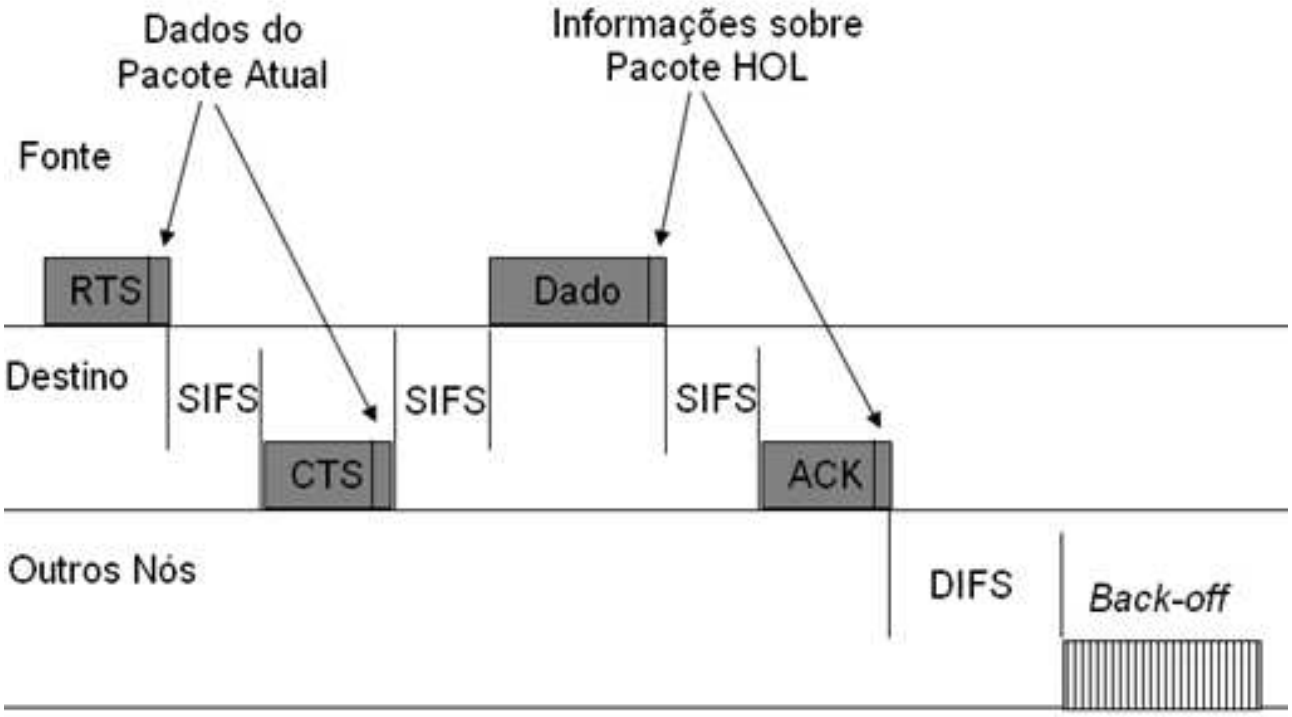

Fig. 2.5: Acesso ao meio no DPS: mecanismo de *piggyback* associado ao *handshake* de 4 vias do IEEE 802.11.

As tabelas de agendamento são baseadas em índices de prioridade, que são calculados com base nas informações dos terminais e no fluxo de dados em questão. Ou seja, a prioridade é calculada levando-se em conta apenas o estado do terminal e o estado do seu fluxo, desprezando-se o estado dos terminais vizinhos. Para o cálculo do índice de prioridade, é utilizado o método EDF, que define o índice de prioridade como sendo $t + d$, com t sendo o tempo de chegada do pacote e d, o limite de atraso tolerado pela aplicação que gerou o pacote.

A construção das tabelas de agendamento é feita levando-se em conta a ordem decrescente dos índices de prioridade. A tabela estabelece uma classificação das transmissões futuras, incluindo a do próprio terminal e de seus vizinhos. Considere um dado terminal j, que ocupa a posição r_j de sua própria tabela S_j. Com base nessa posição, o terminal determinará a distribuição de *back-off* $f(S_j)$ a ser adotada por ele:

$$f(S_j) = \begin{cases} U[0, 2^l CW_{min} - 1] & r_j = 1 \quad l < m \\ \alpha CW_{min} + U[0, \gamma CW_{min} - 1] & r_j > 1 \quad l = 0 \\ U[0, 2^l \gamma CW_{min} - 1] & r_j > 1 \quad l \geq 1 \end{cases}$$

em que $U[a, b]$ indica uma distribuição uniforme entre a e b, α e γ são constantes, l indica o número de tentativas de retransmissão e m é o número máximo de retransmissões permitidas.

O DPS possui implementação para o ns-2 feita pela equipe do *WissTek* e é um dos três protocolos escolhidos para análise.

2.2.4 Multiple Access Collision Avoidance with Piggy-Backed Reservation

O MACA-PR [12] é um protocolo utilizado para prover suporte a tráfego em tempo real, como voz, por exemplo, em redes sem fio *multihop*. É composto por três protocolos: um protocolo MAC baseado no MACAW [3], um protocolo de reserva e um protocolo de roteamento com suporte a QoS, baseado no DSDV [13]. O MACA-PR distingue pacotes *real-time* (voz, por exemplo) de pacotes *best-effort* (dados, por exemplo) e tem como objetivo o compromisso de garantir o acesso ao canal sempre que necessário numa transmissão *real-time* e ao mesmo tempo fazer com que a transmissão dos pacotes *best-effort* seja confiável (sem erros). Para isso, o tempo é dividido em *time slots*. Tais slots são definidos pelas reservas feitas em cada um dos nós, fazendo com que possuam natureza assíncrona, com diferentes tamanhos. Em cada nó existe uma tabela de reserva (RT) que armazena todas as janelas/slots de transmissão/recepção de todos os nós dentro de seu alcance de transmissão.

Quando um pacote de dados (ou qualquer outra aplicação que não seja sensível ao atraso) é transmitido, o protocolo MAC ilustrado na figura 2.6, é utilizado:

1. O nó origem espera por um slot livre na RT (ou seja, quando o meio está livre) e, quando encontra um, espera por um intervalo de tempo aleatório (da mesma ordem de grandeza que o atraso de uma viagem ida e volta de um enlace).
2. Se o meio estiver ocupado, o nó repete o passo 1.
3. Se o meio ainda estiver livre, o nó transmite um RTS, que é respondido pelo nó destino com um CTS.
4. Ao receber o CTS, o nó origem transmite o dado e, se a transmissão ocorrer sem erros, o nó destino envia um ACK.

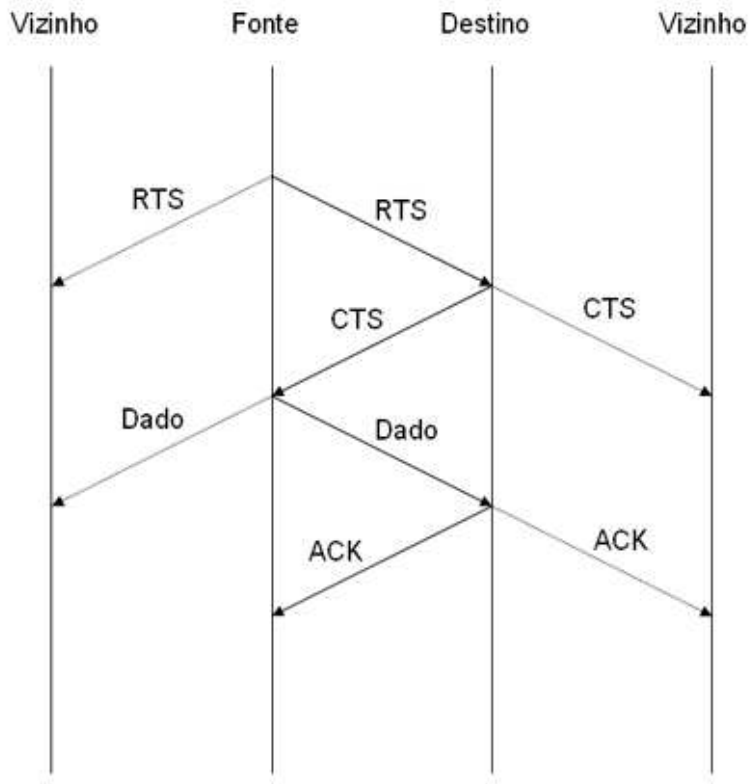

Fig. 2.6: Mecanismo de acesso ao meio do MACA-PR: tráfego não sensível ao atraso.

Os pacotes de RTS e CTS contêm a duração da transmissão do dado. Os nós vizinhos que ouvirem esses pacotes evitam iniciar uma transmissão durante aquele intervalo de tempo.

Já na transmissão de um pacote de voz (ou em qualquer outra aplicação sensível ao atraso), é utilizado o protocolo de reserva, ilustrado na figura 2.7:

1. Considera-se que o transmissor envia um pacote a cada período de tempo chamado de CYCLE.
2. O primeiro pacote é transmitido exatamente da mesma forma que um pacote *best-effort*. No entanto, é incluida (*piggy-backed*) no pacote que contém o dado a informação de reserva do próximo dado a ser transmitido (que é agendado para ser transmitido após o período CYCLE).
3. Ao receber o primeiro dado, o receptor atualiza sua tabela de reserva com a informação inclusa naquele pacote e envia um ACK de volta ao transmissor para confirmar o recebimento da informação de reserva contida no dado.
4. Todos os vizinhos que escutaram o pacote de dados e/ou o ACK atualizam suas tabelas de reserva com as informações contidas nesses pacotes e evitam iniciar uma transmissão durante os instantes de tempo reservados.

5. Ao contrário do protocolo MAC, o protocolo de reserva não utiliza mais o mecanismo de RTS/CTS na transmissão dos pacote de dados subseqüentes. A transmissão ocorre a cada intervalo de tempo CYCLE e o dado carrega a informação de reserva para o próximo pacote. Logo, a transmissão de pacotes *real-time* ocorre numa série de trocas dado-ACK.
6. Caso o transmissor não receba um ACK, o pacote é marcado como perda e não é retransmitido. Pode-se dizer que o ACK funciona como um mecanismo de renovação da reserva: caso o nó transmissor não receba um ACK após um certo número consecutivo de pacotes de dados, ele assume que a reserva foi perdida e reinicia a sessão *real-time* com uma troca de pacotes RTS/CTS que pode ocorrer num outro slot no mesmo enlace, ou em um outro enlace, caso o enlace atual tenha sido rompido.

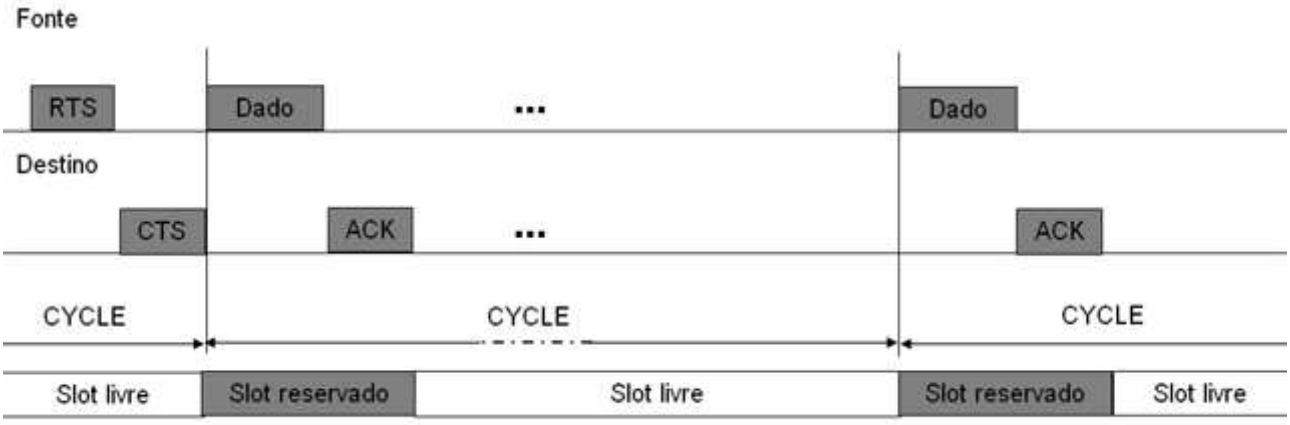

Fig. 2.7: Mecanismo de acesso ao meio do MACA-PR: tráfego sensível ao atraso.

É importante notar que, em ambos os casos (*real-time* ou *best-effort*), para se transmitir um RTS, o nó origem deve encontrar um slot que esteja livre em ambos os extremos da comunicação. Para que haja consistência nas informações a respeito dos slots livres em todos os nós, o MACA-PR adota um esquema de troca periódica de tabelas de reserva. Essa troca elimina por si só o problema de terminal escondido, visto que um terminal escondido nunca irá transmitir ao mesmo tempo que um outro devido à reserva.

O MACA-PR é um dos protocolos com implementação para ns-2 escolhidos para as simulações. A implementação para o ns-2 possui algumas diferenças em relação ao mecanismo descrito nesta seção: quando utilizado o protocolo de reserva, as reservas são feitas de forma independente por enlace, e não para o caminho todo fim-a-fim; além disso, só estão implementados o protocolo MAC e o protocolo de reserva, não havendo a implementação do protocolo de roteamento. Os impactos dessas diferenças serão analisados posteriormente neste trabalho.

2.2.5 IEEE 802.11e

O IEEE 802.11e [14] é uma extensão do padrão 802.11 que visa o suporte a QoS apresentando soluções para a camada MAC. Dois mecanismos foram propostos para esse fim: a EDCF, descrita a seguir, uma evolução da DCF [9] do 802.11, e a HCF [14], uma função de coordenação híbrida.

A EDCF provê acesso ao meio diferenciado e distribuído. Cada quadro da camada superior possui uma prioridade de usuário (UP). Ao receber um quadro, a camada MAC mapeia este em uma categoria de acesso (AC). Cada AC possui uma prioridade diferente no acesso ao meio e pode estar associada à uma ou mais UPs. Podem existir oito ACs e oito UPs. Cada uma das ACs é uma variante melhorada do DCF. Fluxos que caem dentro da mesma AC possuem a mesma prioridade. O nó sempre acessa o meio baseado na AC do quadro a ser transmitido. Cada um dos nós aguarda por oportunidades de transmissão (TXOPs) através da utilização de um conjunto de parâmetros EDCF de acesso ao meio que são únicos para a AC do pacote a ser transmitido. O TXOP é definido como o intervalo de tempo durante o qual o terminal tem direito a iniciar uma transmissão. Dependendo da duração do TXOP, o nó pode transmitir uma ou mais MSDUs, o tamanho do quadro MAC. A prioridade de uma AC se refere à mais baixa UP associada àquela AC.

Durante cada período de contenção, cada AC (com prioridade i) do terminal espera por TXOP e inicia um contador de *back-off* após detectar o canal como ocioso após um intervalo de tempo chamado de AIFS[i]:

$$\text{AIFS}[i] = \text{SIFS} + \text{AIFSN}[i] \times \text{duração do slot}$$

AIFSN[i] é o número de *time slots* em que o terminal precisa detectar o meio como ocioso antes de iniciar o procedimento de *back-off* para uma dada prioridade i. Obrigatoriamente é maior que zero.

Classes com maior prioridade possuem baixos valores de AIFSN associados a elas. Depois de esperar por AIFS[i], cada contador de *back-off* é iniciado em um valor inteiro selecionado entre:

$$[1, \text{CW}[i]+1] \text{ para cada classe } i \text{ com AIFSN}[i] = 1;$$

$$[0, \text{CW}[i]] \text{ para outras classes } i \text{ com AIFSN}[i] > 1.$$

A razão de se criar um intervalo diferente para classes com AIFSN[i]=1 é evitar que transmissões iniciadas por terminais que estão operando no modo EDCF colidam com pacotes de *polling* do modo HCF (descrito mais adiante).

É importante notar que, em um mesmo terminal, as ACs funcionam como MACs virtuais e colisões entre diferentes ACs são tratadas internamente.

A HCF combina as características da EDCF e da PCF (do padrão 802.11) [9] de forma a prover capacidade de manipular seletivamente as MSDUs de tal maneira que haja compatiblidade com ambos DCF e PCF. Este modo é utilizado em redes do tipo infraestrutura, enquanto o EDCF é utilizado em redes *ad hoc*.

Capítulo 3

O simulador de redes ns-2

O ns-2 [15] é um simulador de rede de eventos discretos que cobre um grande número de tipos de redes, protocolos, elementos de redes e modelos de tráfego. Trata-se de um *software* de código aberto que possui várias extensões desenvolvidas pelo meio acadêmico e é amplamente usado em pesquisas com redes *ad hoc*.

3.1 Breve Histórico

O desenvolvimento de sua primeira versão começou em 1989, como uma variante do REAL network simulator [16]. Em 1995, seu desenvolvimento passou a ser suportado pelo DARPA através do Projeto VINT [15], desenvolvido na Xerox PARC, LBL, UCB e USC/ISI, culminando no lançamento da versão 2. Atualmente, seu desenvolvimento é feito pelo DARPA através do projeto SAMAN [15] e pela NSF através do CONSER [15], ambos com apoio de outros grupos de pesquisadores, tais como *Sun Microsystems*, Projeto UCB Daedelus e Projeto CMU Monarch. A versão 3 começou a ser desenvolvida no dia 1 de julho de 2006 e tem previsão para ficar pronta em quatro anos.

Existe ainda uma lista de discussões (*ns mailing list* [17]) na qual os usuários podem trocar experiências e discutir aperfeiçoamentos para o *software*.

3.2 Arquitetura

Atualmente, o simulador é baseado em duas linguagens de programação: um núcleo orientado a objeto escrito em C++ e um interpretador OTcl (uma extensão orientada a objeto da linguagem Tcl), utilizado para executar os *scripts* de comando e configuração do usuário.

O uso de duas linguagens de programação é justificado através das duas diferentes tarefas que o simulador deve executar. De um lado, está a simulação detalhada de protocolos, que requer uma

linguagem capaz de manipular de forma eficiente bytes, cabeçalhos de pacotes e implementar algoritmos que sejam executados sobre grandes massas de dados. Para essa tarefa, o tempo de execução é prioridade e, assim sendo, o C++ torna-se uma excelente opção. Por outro lado, o estudo de redes quase sempre requer mudanças constantes de parâmetros e acesso rápido a diferentes topologias. Como a configuração é executada apenas uma vez, o tempo de execução deixa de ser prioridade e o tempo de iteração passa a ser mais importante. Nesse caso, o OTcl é a linguagem mais adequada.

O simulador possui uma ampla biblioteca de objetos de rede e de protocolos. Existem duas classes hierárquicas para cada objeto: a compilada em C++ e a interpretada em OTcl, sendo que existe correspondência um para um entre elas. A classe compilada em C++ permite alcançar eficiência nas simulações e menores tempos de execução. É bastante útil na definição e operação de protocolos, permitindo a redução do tempo de processamento de pacotes e eventos. Já no *script* OTcl de usuário, pode-se definir uma topologia de rede, os protocolos e aplicações a serem simulados e a forma do arquivo de saída do simulador. O OTcl pode fazer uso dos objetos compilados em C++ através de uma ligação OTcls feita usando o TCtcl, que cria um par OTcl para cada um dos objetos C++.

3.3 Formato dos Dados de Saída

Para este trabalho em particular será utilizado apenas o modo *Wireless*, que possui um formato de saída particular e pouco inteligível à primeira vista, o *wireless trace*, mostrado no exemplo abaixo:

Exemplo de arquivo *wireless trace*:

```
s -t 0.267662078 -Hs 0 -Hd -1 -Ni 0 -Nx 5.00 -Ny 2.00 -Nz 0.00
-Ne -1.000000 -Nl RTR -Nw -- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 0.255
-Id -1.255 -It message -Il 32 -If 0 -Ii 0 -Iv 32
s -t 1.511681090 -Hs 1 -Hd -1 -Ni 1 -Nx 390.00 -Ny 385.00 -Nz
0.00 -Ne -1.000000 -Nl RTR -Nw -- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is
1.255 -Id -1.255 -It message -Il 32 -If 0 -Ii 1 -Iv 32
s -t 10.000000000 -Hs 0 -Hd -2 -Ni 0 -Nx 5.00 -Ny 2.00 -Nz 0.00
-Ne -1.000000 -Nl AGT -Nw -- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 0.0
-Id 1.0 -It tcp -Il 1000 -If 2 -Ii 2 -Iv 32 -Pn tcp -Ps 0 -Pa
0 -Pf 0 -Po 0
r -t 10.000000000 -Hs 0 -Hd -2 -Ni 0 -Nx 5.00 -Ny 2.00 -Nz 0.00
-Ne -1.000000 -Nl RTR -Nw -- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 0.0
-Id 1.0 -It tcp -Il 1000 -If 2 -Ii 2 -Iv 32 -Pn tcp -Ps 0 -Pa
0 -Pf 0 -Po 0
r -t 100.004776054 -Hs 1 -Hd 1 -Ni 1 -Nx 25.05 -Ny 20.05 -Nz
```

```
0.00 -Ne -1.000000 -Nl AGT -Nw -- -Ma a2 -Md 1 -Ms 0 -Mt 800
-Is 0.0 -Id 1.0 -It tcp -Il 1020 -If 2 -Ii 21 -Iv 32 -Pn tcp
-Ps 0 -Pa 0 -Pf 1 -Po 0
s -t 100.004776054 -Hs 1 -Hd -2 -Ni 1 -Nx 25.05 -Ny 20.05 -Nz
0.00 -Ne -1.000000 -Nl AGT -Nw -- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is
1.0 -Id 0.0 -It ack -Il 40 -If 2 -Ii 22 -Iv 32 -Pn tcp -Ps 0
-Pa 0 -Pf 0 -Po 0
```

Cada linha iniciada por `<letra> -t` corresponde a um evento. A letra que antecede o campo `-t` define o tipo de evento: s = envio de pacote, f = encaminhamento de pacote, r = recepção de pacote e d = perda de pacote. Em cada linha, os campos contêm informações tais como: instante de acontecimento do evento, nó origem, nó destino, identificação do fluxo, próximo nó dentro da conexão de múltiplos enlaces, tipo de pacote e outros. Todos estes parâmetros estão descritos de forma detalhada no manual [15]. A fim de extrair os dados necessários para a análise, esses arquivos de *trace* foram processados utilizando *parsers* escritos em perl e awk, duas linguagens de programação muito eficientes para se manipular *strings* de texto. Com esses *parsers*, consegue-se extrair do *wireless trace* as seguintes informações: vazão da rede, atraso médio dos pacotes, variação do atraso e taxa de perdas de pacotes.

3.4 Considerações Finais a Respeito do ns-2

Uma observação importante a ser feita é que o ns-2 é um software bastante exigente em termos de poder computacional (processamento intenso), espaço e velocidade de escrita em disco (gera muitos dados de saída rapidamente). Logo, a máquina a ser utilizada tem papel fundamental no tempo gasto para se executar uma simulação e é bastante comum uma simulação demorar várias horas para ser executada. Além disso, como os arquivos-texto de saída são muito grandes (facilmente chegando na casa dos GB), a eficiência de programação dos *parsers* (programas que filtram arquivos de texto baseados em procura de padrões) influencia muito no tempo de processamento dos resultados. Recomenda-se que o usuário tome cuidado ao escrever o *parser* utilizado para extração dos dados desejados, a fim de otimizar ao máximo o tempo de processamento.

Para facilitar a familiarização do leitor com o simulador de redes, são mostrados alguns códigos-fonte exemplo no *Apêndice A*, escritos em Tcl.

Capítulo 4

Simulações e Resultados Comparativos entre IEEE 802.11, DPS e MACA-PR para um Arranjo Linear de Nós

Para esta etapa do trabalho, foi escolhido um cenário simples para a análise comparativa entre os protocolos MAC IEEE 802.11, DPS e MACA-PR, a fim de facilitar a familiarização com o simulador de redes e verificar como é feita a simulação dos protocolos no ns-2. O cenário de simulação é descrito a seguir:

4.1 Topologia

Foi escolhida uma cadeia linear composta por nove nós separados por uma distância de 200 m, mostrada na figura 4.1.

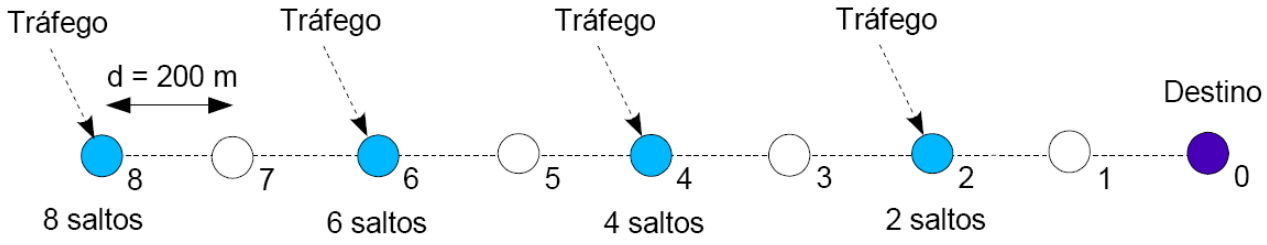

Fig. 4.1: Topologia do tipo cadeia linear de nós.

Na topologia em cadeia, o terminal mais à direita (terminal 0) é o *gateway da rede*. No caso de tráfego FTP, o gateway é a fonte de tráfego para todos os outros terminais, simulando uma transferên-

cia de um arquivo infinito. Para tráfego CBR, uma simulação preliminar de tráfego de voz, o gateway é o destino do tráfego dos outros terminais. Dos outros oito terminais, quatro deles (terminais 2, 4, 6 e 8) geram tráfego, enquanto que os outros quatro atuam apenas como encaminhadores nas rotas *multihop* estabelecidas. Desta forma, temos as situações de rotas *multihop* com dois, quatro, seis e oito saltos. Decidiu-se por apenas quatro terminais geradores de tráfego pois a situação em que todos os terminais geram tráfego tem baixa probabilidade de ocorrência no mundo real quando se trata de tráfego telefônico.

Apesar deste cenário ser simples e certamente não representar casos típicos encontrados na prática, o uso do mesmo facilita a análise e o entendimento do comportamento dos protocolos de comunicação no simulador ns-2.

4.2 Camada Física

Na camada física, o simulador permite o acerto da freqüência a ser utilizada, a escolha do modelo de propagação (Espaço Livre, Terreno Plano ou Sombreamento) e o ajuste do raio de transmissão e do raio de interferência (*Carrier Sensing*) dos terminais.

Tais raios estão diretamente relacionados à dois limiares de recepção utilizados nos protocolos baseados em CSMA: um limiar de recepção e um limiar de *carrier sensing*. Ao receber um pacote, o receptor verifica o nível deste em relação aos limiares. Se o sinal estiver abaixo do limiar de *carrier sensing*, o receptor ignora a transmissão; caso o sinal esteja entre os dois limiares, o receptor detecta a tentativa de transmissão, porém não repassa a informação recebida para a camada superior; por último, se o sinal está acima do limiar de recepção, a informação é considerada recebida corretamente e é repassada para a camada superior.

O alcance de transmissão de cada nó foi ajustado para 250 m, de tal forma que cada nó enxergue somente seus vizinhos imediatos. Além disso, o alcance de interferência foi ajustado em 550 m. Ambos os ajustes de alcance são feitos através da atribuição do nível de potência do sinal recebido na distância desejada, utilizando-se as equações do modelo de propagação escolhido. A freqüência utilizada foi de 800 MHz e o modelo de propagação adotado foi o de terreno plano.

4.3 Camada MAC e Roteamento

Conforme já foi mencionado, foram utilizados três protocolos MAC nestas simulações: IEEE 802.11, DPS e MACA-PR (protocolo MAC baseado no MACAW e protocolo de reserva). A taxa de transmissão máxima do canal foi ajustada em 2 Mbits/s.

Em relação ao roteamento, alguns cuidados foram tomados, visto que o roteamento é fator bastante crítico em redes *multihop*. Nas primeiras análises do simulador, foi feito um teste para verificar o efeito dos diferentes protocolos de roteamento disponíveis (DSR, AODV, DSDV e TORA) tanto no cenário linear, quanto no arranjo na forma de grade. Mantiveram-se parâmetros fixos para todas as camadas e foi-se alterando o protocolo de roteamento. Os resultados mostraram que a diferença no desempenho geral da rede entre os protocolos foi desprezível, considerando como parâmetros de avaliação a vazão média, atraso médio, variação do atraso média e taxa média de perda de pacotes. Concluiu-se então que, para os protocolos de roteamento implementados na versão utilizada do ns-2, não existe impacto significativo desses na análise do desempenho em relação a varição do parâmetros da camada MAC. Por essa razão, para todas as simulações feitas ao longo deste trabalho, fixou-se um protocolo de roteamento em cada uma delas.

O protocolo de roteamento escolhido é o DSR. É importante salientar que no caso do MACA-PR, não existe implementação do protocolo de roteamento com suporte a QoS baseado no DSDV e isso terá impacto significativo no desempenho do protocolo, conforme será visto adiante.

4.4 Modelos de Tráfego

Para estas análises, decidiu-se empregar apenas os modelos de tráfego das aplicações FTP e CBR. A razão da escolha é a distinção entre ambos nos requisitos de qualidade de serviço e tipo de protocolo de transporte (TCP e UDP, respectivamente).

Para o tráfego FTP, foi suposta a transferência de um arquivo de tamanho infinito (enquanto a simulação durar) a partir do gateway. O tamanho dos pacotes TCP foi ajustado para 512 bytes, com janelas do TCP de 32 bytes. Para o tráfego CBR, a taxa de transmissão foi ajustada para 50 kbits/s, com pacotes de 125 bytes, o que equivale a um pacote a cada 20 ms. Este valores correspondem a uma modelagem preliminar de um tráfego de voz.

4.5 Resultados das Simulações

Para a análise comparativa entre os três protocolos MAC, foram escolhidos os parâmetros: vazão média em kbits/s, atraso médio na transmissão de pacotes por terminal, variação do atraso na transmissão de pacotes por terminal e taxa de perda de pacotes por terminal. Todos os resultados apresentados a seguir são uma média dos resultados obtidos em 10 simulações de 180 segundos de tráfego em cada uma delas.

4.5.1 Tráfego CBR

As Figuras 4.2, 4.3, 4.4 e 4.5 apresentam os resultados para atraso, vazão, variação do atraso e perdas, respectivamente, em função da distância (em número de saltos) do terminal ao gateway, para os protocolos MAC IEEE 802.11, DPS e MACA-PR. Deve-se notar que, para o tráfego CBR, o gateway é o destino de todo o tráfego. Deve ser observado que o resultado é dado em função do número de saltos até o gateway, que coincide com o índice do terminal.

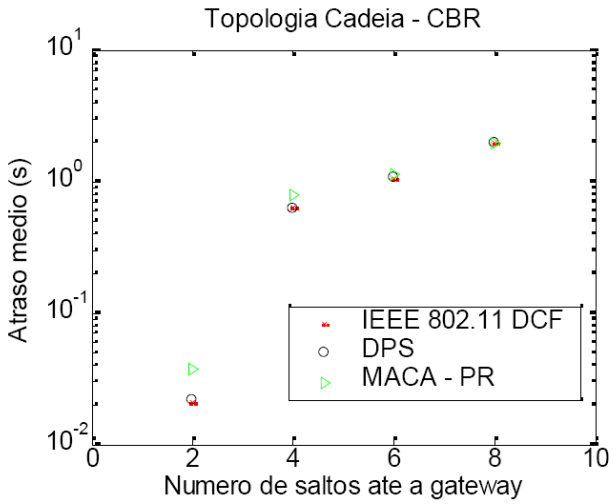

Fig. 4.2: Atraso médio para o tráfego CBR.

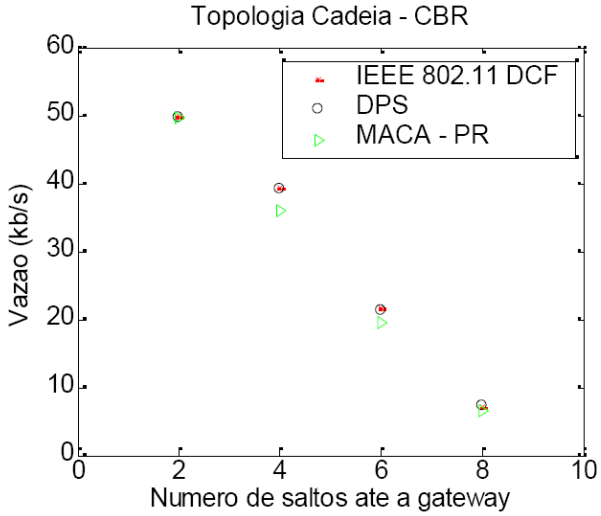

Fig. 4.3: Vazão média para o tráfego CBR.

Independente do protocolo usado, o desempenho dos terminais degrada com o aumento do comprimento do enlace entre a fonte e o destino. O atraso e a variação do atraso observados no

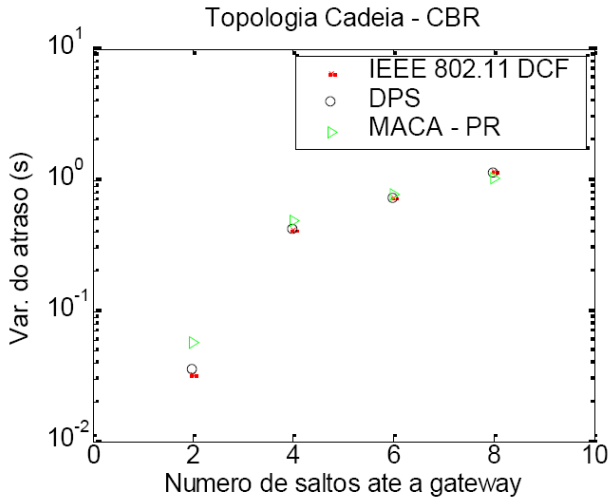

Fig. 4.4: Variação do atraso para o tráfego CBR.

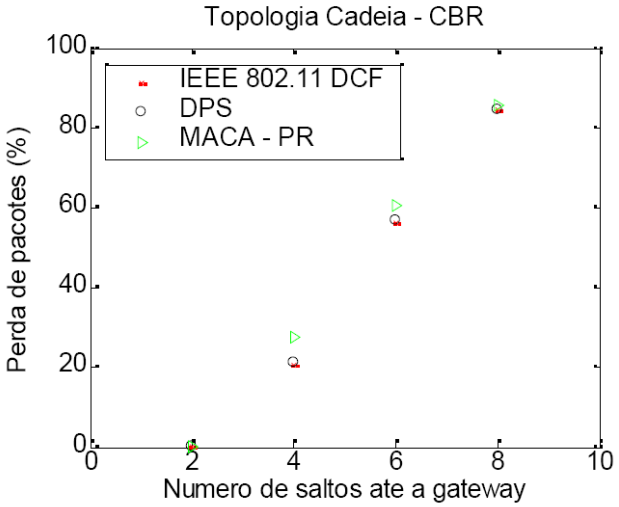

Fig. 4.5: Taxa de perdas para o tráfego CBR.

terminal mais próximo ao gateway (a dois saltos do gateway) têm valores aceitáveis para aplicações como, por exemplo, tráfego de voz. No entanto, o aumento em dois saltos no enlace já leva a valores inaceitáveis de atraso. Observa-se também uma grande semelhança entre os resultados para os três protocolos, mostrando que os mecanismos para melhora de desempenho apresentados pelo DPS e pelo MACA-PR não surtiram o efeito planejado.

Os resultados de vazão mostram que apenas o terminal mais próximo do gateway consegue transmitir na taxa de geração de tráfego (50 kbits/s), indicando um grau de ineqüidade entre os terminais. Este resultado é corroborado pelos valores de perda de pacotes observados. Note-se que em aplicações do tipo CBR, que emprega o protocolo de transporte UDP, não há retransmissão de pacotes

perdidos.

Estes resultados mostram que a estratégia de atribuir prioridade aos pacotes (mecanismo DPS), ou a estratégia de reservar o canal (mecanismo MACA-PR), na forma que foram implementadas, não surtiram o efeito esperado. Quanto ao mecanismo MACA-PR, dois possíveis motivos para o baixo desempenho podem ser identificados. O primeiro é o fato de a reserva ser feita por enlace e de forma independente, e não para todo o enlace fim-a-fim. Assim, se um pacote não encontrar reservas em todos os enlaces que compõem o seu caminho da fonte ao destino, deverá acionar, em vez do mecanismo de reserva, o protocolo MAC, que se resume ao mecanismo do MACAW. Outro motivo é o *overhead* elevado neste mecanismo, devido a troca de tabelas de reserva entre os terminais vizinhos. A degradação devido ao *overhead* pode reduzir eventuais ganhos do mecanismo. Em relação ao mecanismo DPS, a diferenciação de pacotes nas simulações acima ocorreu apenas em função da origem do pacote, dado que havia apenas pacotes CBR. Portanto, atribuir maior prioridade ao terminais que têm pacotes de outros nós para encaminhar parece não ser adequado. Uma outra questão importante no mecanismo DPS é o aumento do tamanho das mensagens de controle e de dados necessário para a implementação da tabela de prioridade. Este aumento pode degradar o desempenho da rede devido ao correspondente aumento do overhead. Portanto, uma investigação mais profunda deve ser conduzida com o objetivo de determinar as reais diferenças entre o ganho devido à atribuição de prioridades e a perda devido ao aumento do *overhead*.

Os valores de perda de pacotes observados são bastante elevados (até 80%, para o terminal 8) . No entanto, este valor é consistente com os outros resultados da simulação e com o fato de não haver retransmissão no protocolo UDP.

4.5.2 Tráfego FTP

As Figuras 4.6, 4.7, 4.8 e 4.9 apresentam os resultados de atraso, vazão, variação do atraso e perdas para aplicação do tipo FTP.

Aqui também, como no caso do tráfego CBR, observa-se uma grande semelhança entre os desempenhos obtidos com os três protocolos. No entanto, como já citado anteriormente, esta proximidade dos desempenhos era esperada, pois os mecanismos MACA-PR e DPS se resumem ao mecanismos do IEEE 802.11 no caso tráfego FTP, lembrando que o MACAW é muito similar ao 802.11.

A Figuras 4.6 e 4.7 mostram que os terminais 4, 6 e 8 praticamente não conseguem escoar seus fluxos de tráfego, enquanto que o terminal 2, que é o mais próximo do gateway, apresenta valores aceitáveis de atraso e vazão. Este resultado mostra o alto grau de ineqüidade entre os terminais quando o IEEE 802.11 é empregada em uma rede ad hoc multihop. Esta ineqüidade foi discutida por Xu e Saadawi em [18], no qual eles argumentam que o mecanismo de *backoff* empregado no IEEE 802.11

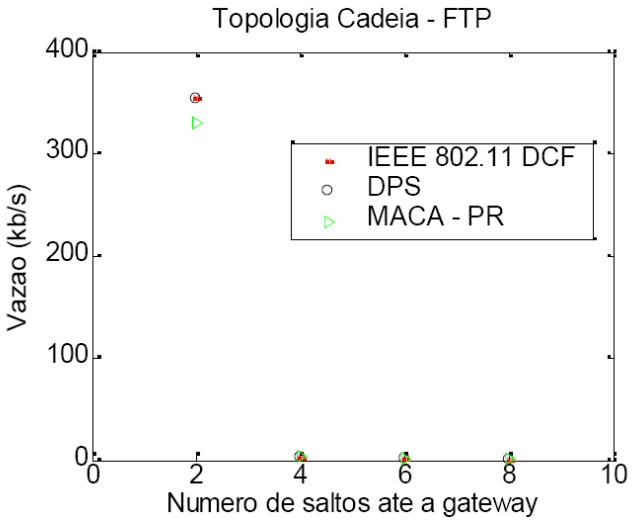

Fig. 4.6: Vazão média para o tráfego FTP.

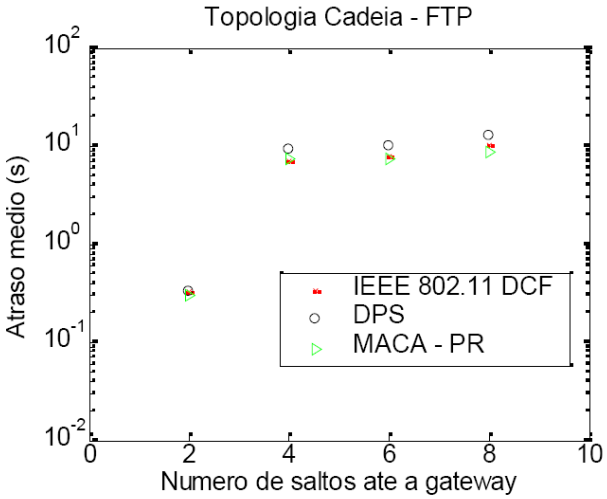

Fig. 4.7: Atraso médio para o tráfego FTP.

favorece terminais que concluíram com sucesso uma transmissão, em detrimento aos terminais que estejam tentando acessar o canal. Desta forma, um terminal pode capturar o canal, o que de fato ocorre nas simulações com o terminal 2.

Os valores bastante elevados de atraso para os terminais 4, 6 e 8 (aproximadamente 10 s, maior que os atraso observados no caso de tráfego CBR) deve-se ao fato da existência de um mecanismo de *handshaking* e de retransmissões no protocolo TCP. Um pacote será considerado transmitido apenas se for recebido corretamente. Caso contrário, será retransmitido. Portanto, alto atraso é consistente com relativa baixa taxa de perda de pacotes (quando comparamos com o caso de tráfego CBR, em que não há retransmissão).

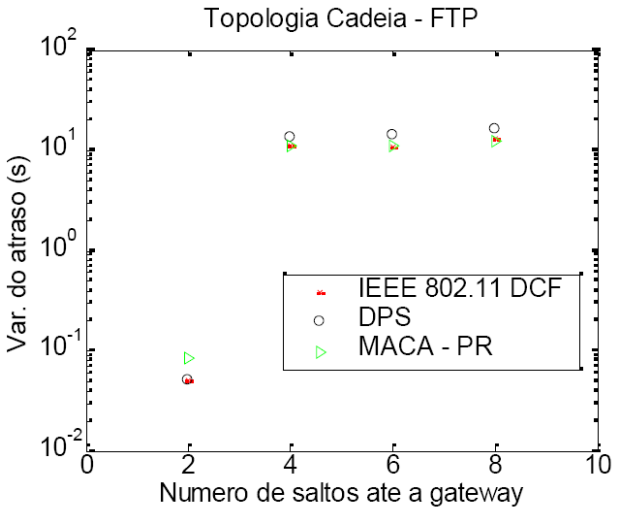

Fig. 4.8: Variação do atraso para o tráfego FTP.

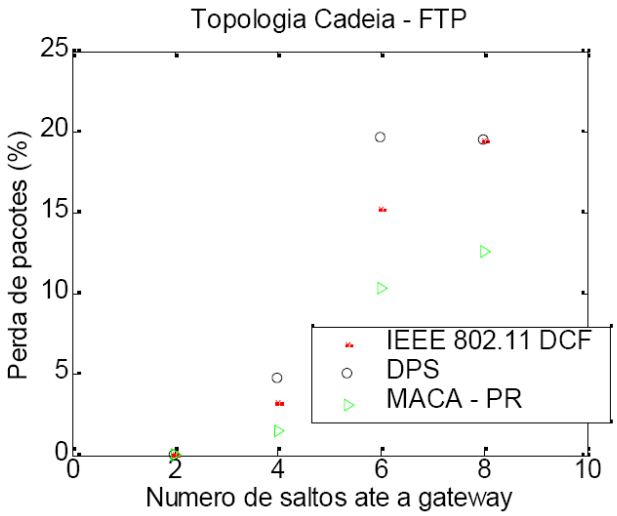

Fig. 4.9: Taxa de perdas para o tráfego FTP.

4.6 Conclusões

Os resultados obtidos até o momento mostram que o protocolo DPS, apesar da tentativa de melhorar o desempenho atribuindo classes de prioridades para os pacotes, adiciona um *overhead* de controle bastante significativo, tornando seu desempenho praticamente igual ao do IEEE 802.11 no caso de tráfego CBR e, pior que este no caso de tráfego FTP. Já o MACA-PR apresentou desempenho pior que o 802.11 no caso de tráfego CBR, justamente quando o protocolo de reserva deveria melhorar o desempenho. Isso ocorreu devido ao motivo citado na seção anterior, ou seja, a maneira que ele foi implementado no ns-2. Possivelmente, no futuro, quando houverem implementações mais refinadas

deste protocolo, deveremos verificar melhoras no desempenho. Já no caso de tráfego FTP, o MACA-PR utiliza o protocolo MAC baseado no MACAW, que é bastante similar ao IEEE 802.11. Logo, o desempenho de ambos é praticamente o mesmo, conforme o esperado.

Devido ao desempenho bastante ruim dos protocolos MACA-PR e DPS em relação ao IEEE 802.11, que é atualmente o padrão de referência em redes ad hoc, na próxima etapa do trabalho, os dois serão substituídos por um protocolo que se tem mostrado bastante promissor nas publicações científicas até o momento: o IEEE 802.11e, descrito na seção 2.2.5.

Capítulo 5

Simulações e Resultados Comparativos entre IEEE 802.11 e IEEE 802.11e em WMN

Para esta etapa, foi escolhido um cenário do tipo grade de nós com *gateway* para o escoamento de tráfego para uma rede externa para a análise comparativa entre os protocolos IEEE 802.11 e IEEE 802.11e. Esse tipo de rede é conhecido como *mesh*. O cenário é descrito a seguir.

5.1 Topologia

Foi escolhido um arranjo do tipo grade de nós 7x7, ou seja, 49 nós, separados entre si por uma distância de 200 metros, conforme mostra a figura 5.1.

Esse arranjo foi escolhido como modelo de uma situação real de rede de pequeno porte, como por exemplo em uma pequena comunidade ou em ambiente rural. Na figura 5.1, os nós coloridos representam os terminais que geram e recebem tráfego, enquanto aqueles em branco atuam apenas como *relays*. O código de cores identifica as diferentes prioridades do 802.11e: vermelho = máxima prioridade, verde = prioridade média, azul = prioridade mínima. As prioridades foram escolhidas de tal forma que os nós mais distantes do *gateway* tenham prioridade maior, visto que o número de saltos na comunicação é maior do que os que estão mais próximos. Além disso, também foi escolhido um outro arranjo do tipo grade 7x7, porém com cinco *gateways*, mostrado na figura 5.2, a fim de se observar o efeito de múltiplos pontos de escoamento de tráfego no desempenho da rede.

5.2 Camada Física

Na camada física, o alcance de transmissão de cada nó foi ajustado para 250 m, de tal forma que cada nó exergue somente quatro de seus vizinhos. Além disso, o alcance de interferência

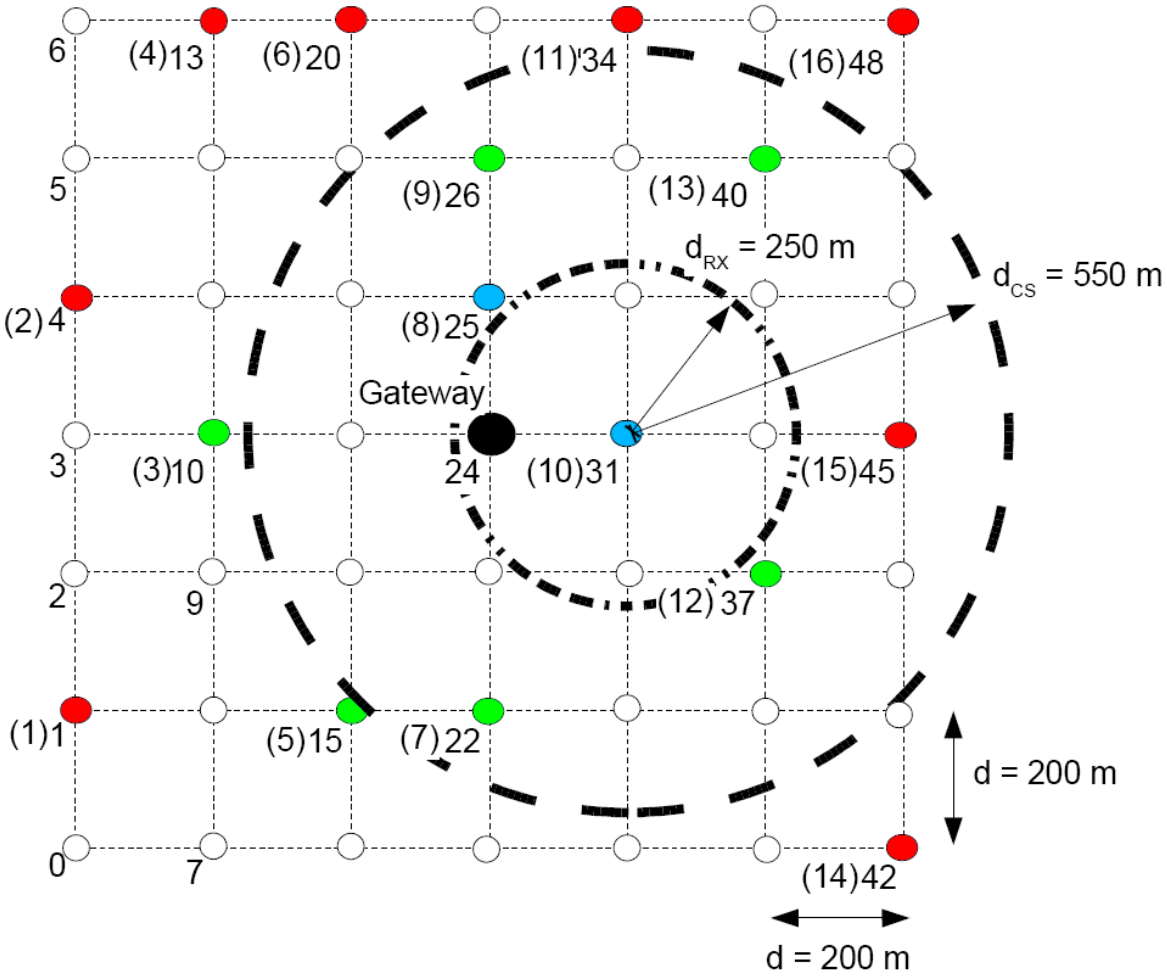

Fig. 5.1: Topologia do tipo grade de nós 7x7 com um *gateway*.

foi ajustado em 550 m. Ambos os ajustes de alcance são feitos através da atribuição do nível de potência do sinal recebido na distância desejada, utilizando-se as equações do modelo de propagação escolhido. A freqüência utilizada foi de 2,4 GHz e o modelo de propagação adotado foi o de Terreno Plano [19].

5.3 Camada MAC e Roteamento

Conforme já foi mencionado, foram utilizados dois protocolos MAC nestas simulações: IEEE 802.11 e IEEE 802.11e. A taxa de transmissão máxima do canal foi ajustada em 2 $Mbits/s$ e o mecanismo de RTS/CTS está ativo. O protocolo de roteamento utilizado é o DSR [4].

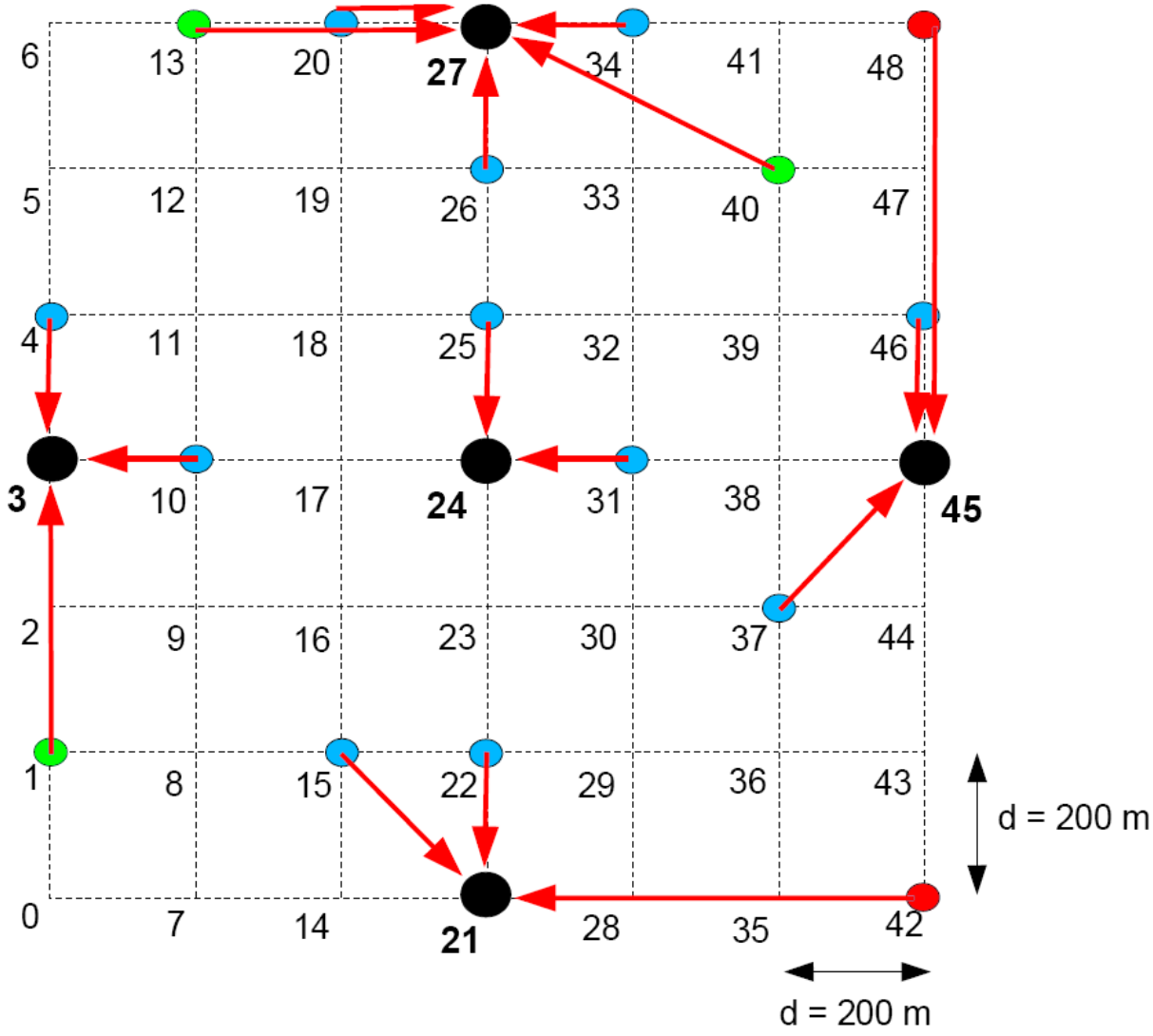

Fig. 5.2: Topologia do tipo grade de nós 7x7 com cinco *gateways*. As setas indicam quais nós se comunicam com cada *gateway*.

5.4 Modelos de Tráfego

Para as simulações a seguir, foi usado tráfego CBR contínuo de 50 kbits/s com pacotes de 125 bytes, o que resulta em um pacote transmitido a cada 20 ms. O tráfego CBR é utilizado aqui como uma modelagem preliminar do tráfego de voz.

Além das simulações com apenas tráfego CBR, no caso de um *gateway* foi feita a análise para o caso de tráfego CBR com tráfego de fundo FTP, a fim de verificar o efeito das prioridades do IEEE 802.11e para diferentes tipos de pacotes.

Para o tráfego FTP em questão, foi suposta a transferência de um arquivo de tamanho infinito (enquanto a simulação durar) entre os pares de nós mostrados na figura . O tamanho dos pacotes TCP foi ajustado para 512 bytes, com janelas de recepção do TCP de 32 bytes.

5.5 Resultados das Simulações

5.5.1 Um *Gateway*, Apenas Tráfego CBR

Para o cenário com um único *gateway*, foram obtidos os resultados das figuras 5.3 e 5.4, que correspondem a uma média de 20 simulações executadas no ns-2, e da tabela 5.1, que apresenta a média dos resultados entre os terminais.

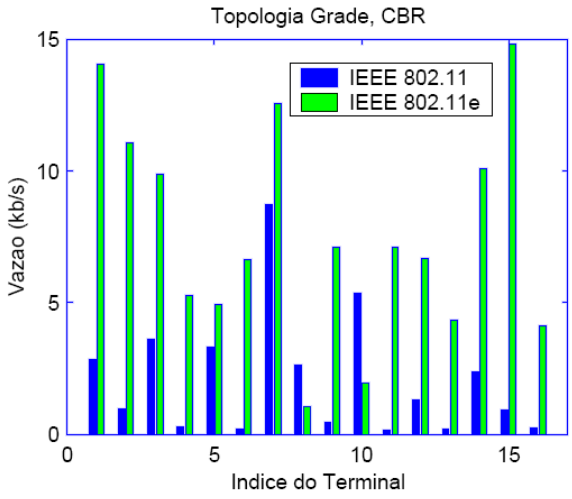

Fig. 5.3: Vazão por nó para o caso de um *gateway*.

Parâmetro	*IEEE 802.11*	*IEEE 802.11e*
Vazão [*kbits/s*]	$2,10$	$7,80$
Atraso [s]	$8,05$	$9,73$

Tab. 5.1: Valores médios para o cenário de um *gateway* com tráfego CBR.

Para o tráfego CBR, o IEEE 802.11e apresenta um desempenho melhor na vazão, com $7,80\ kbits/s$ contra $2,10\ kbits/s$ do IEEE 802.11. Se observarmos a figura 5.3, nota-se o problema da ineqüidade no acesso ao meio no 802.11: os terminais mais próximos ao *gateway* conseguem transmitir primeiro e, com isso, são favorecidos pelo mecanismo de cálculo da CW, conforme foi mostrado no capítulo

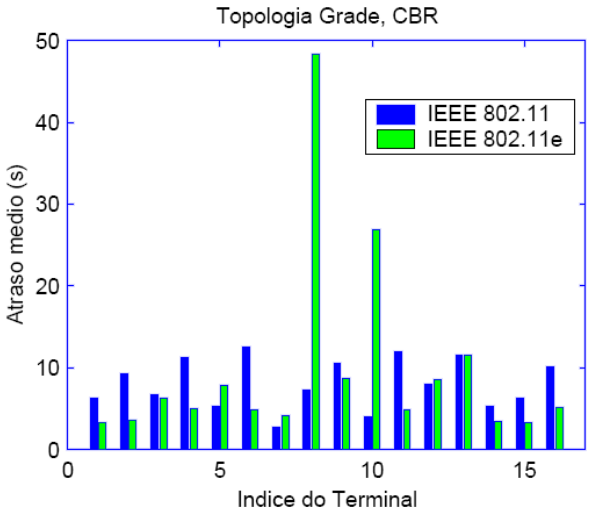

Fig. 5.4: Atraso médio por enlace para o caso de um *gateway*.

2. Com a introdução de prioridades maiores para os nós mais distantes no 802.11e, o problema da ineqüidade foi minimizado, resultando em maiores vazões para os nós mais distantes. No entanto, os nós 8 e 10 (os mais próximos do *gateway*) apresentaram desempenho pior, pois a prioridade do tráfego gerado nestes é menor do que a do tráfego sendo encaminhado por eles.

No entanto, no atraso médio, o IEEE 802.11 leva vantagem. Isso ocorreu devido aos dois terminais mais próximos do *gateway* apresentarem altos níveis de contenção por causa da baixa prioridade atribuída a esses no 802.11e (lembrando que no caso do 802.11e, os terminais mais distantes do *gateway* apresentam prioridade maior). No geral, os outros terminais apresentaram atrasos menores quando é utilizado o 802.11e. Também foi observado na simulação que a taxa de perda de pacotes no IEEE 802.11e é menor que no IEEE 802.11 padrão.

É importante citar que, os resultados, apesar de serem bastante ruins para uma aplicação prática, correspondem a um cenário bastante estressante, uma situação de pior caso (apenas um *gateway*). Um cenário prático mais realista envolve mais de um *gateway*, visando melhor distribuição de tráfego, redundância a a diminuição do número de saltos na comunicação. A seguir será mostrada a mesma análise para um cenário com cinco *gateways*.

5.5.2 Cinco *gateways*, apenas tráfego CBR

Serão mostrados agora os resultados para o cenário da figura 5.2, com cinco *gateways*. Observou-se um ganho significativo de desempenho em relação ao caso de apenas um *gateway*, devido principalmente à redução de gargalos e diminuição do número de saltos. Os resultados estão apresentados nas figuras 5.5 e 5.6, e na tabela 5.2. Novamente, correspondem à média de 20

realizações.

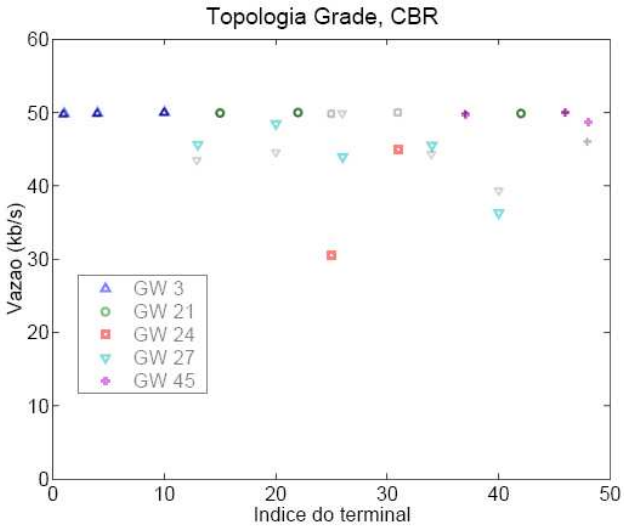

Fig. 5.5: Vazão por nó para o caso de cinco *gateways*.

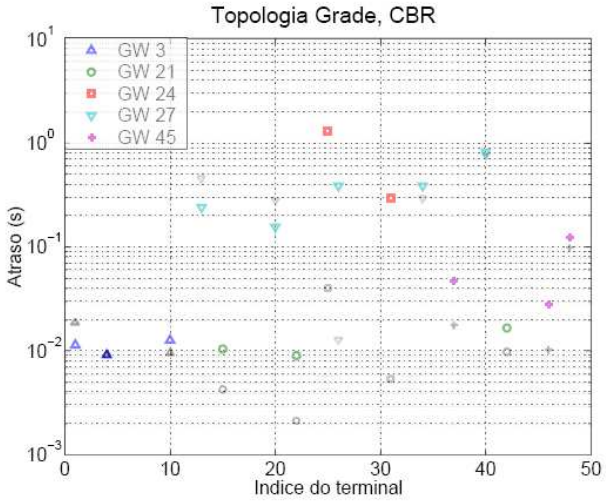

Fig. 5.6: Atraso médio por enlace para o caso de cinco *gateways*.

Parâmetro	*IEEE 802.11*	*IEEE 802.11e*
Vazão [*kbits/s*]	48, 48	46, 20
Atraso [ms]	87, 74	257, 00

Tab. 5.2: Valores médios para o cenário de cinco *gateways* com tráfego CBR.

Neste caso, o desempenho do IEEE 802.11e é, na média, pior que o do IEEE 802.11. Isso ocorreu devido ao desempenho ruim dos terminais 25 e 31, que apresentam prioridades menores. Exceto por esse fato, o desempenho dos dois protocolos se apresentou bastante similar, não deixando claro quais as vantagens dos mecanismos de suporte a QoS do IEEE 802.11e quando esses são utilizados para dar maior prioridade aos nós mais distantes do gateway. Nota-se ainda que o IEEE 802.11 padrão apresentou um número maior de terminais que atingiram um valor de atraso médio dentro dos padrões de QoS usualmente adotados (abaixo de $250\ ms$) [5].

5.5.3 Tráfego misto com um *gateway*

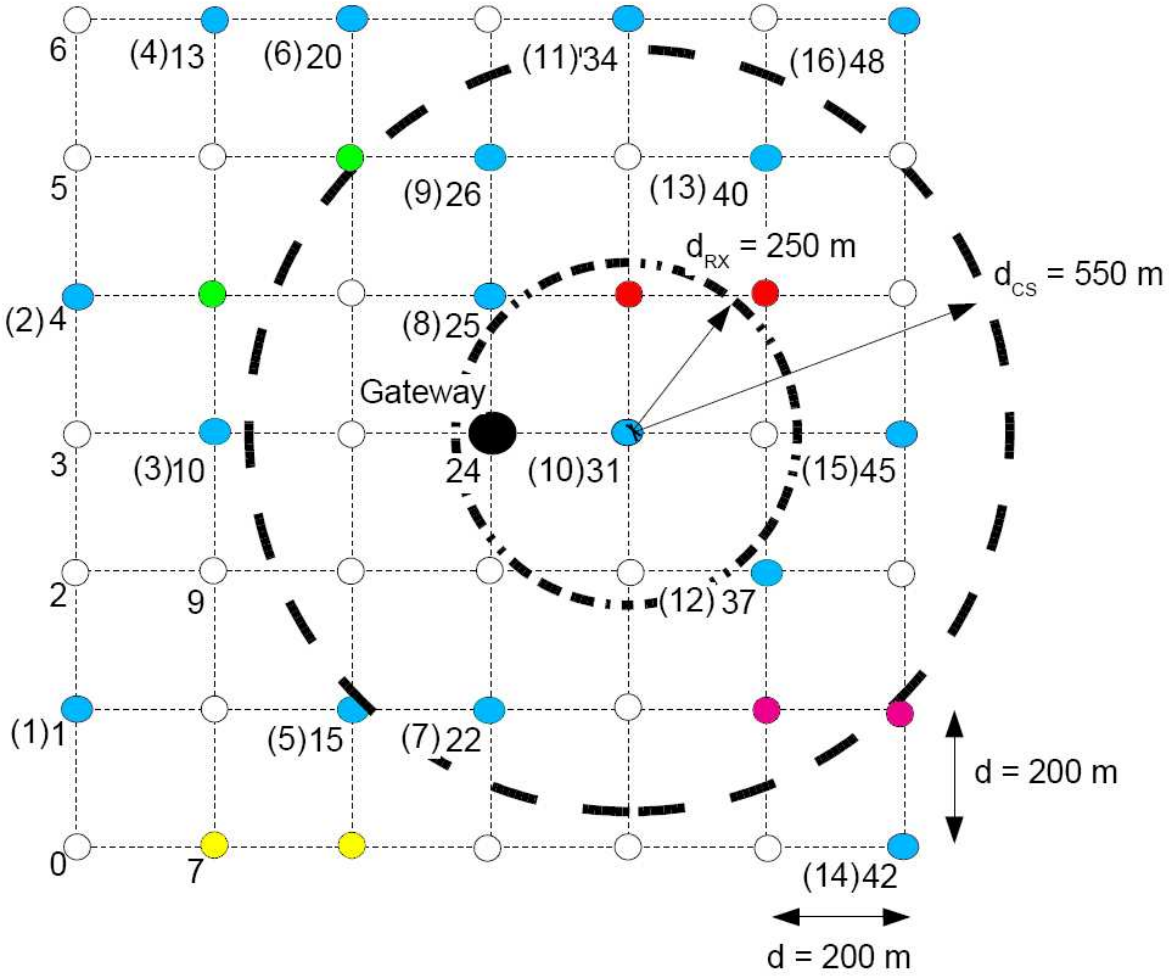

Fig. 5.7: Topologia do tipo grade de nós 7x7 com um *gateway* e tráfego de fundo FTP. Os nós azuis são os geradores de tráfego CBR e se comunicam com o *gateway*. Os pares de nós coloridos são os que se comunicam via FTP.

Esta seção mostra a influência do mecanismo de suporte a QoS do IEEE 802.11e quando

é utilizado para atribuir prioridades distintas a diferentes tipos de tráfego. Neste caso, foi utilizado o cenário de um *gateway* com 16 terminais gerando tráfego CBR, porém com mais quatro pares de terminais transmitindo dados via FTP entre si, conforme mostra a figura 5.7. O fluxo de dados via FTP atua como tráfego de fundo e o desempenho medido é em relação ao tráfego CBR.

Os resultados são mostrados nas figuras 5.8, 5.9 e na tabela 5.3.

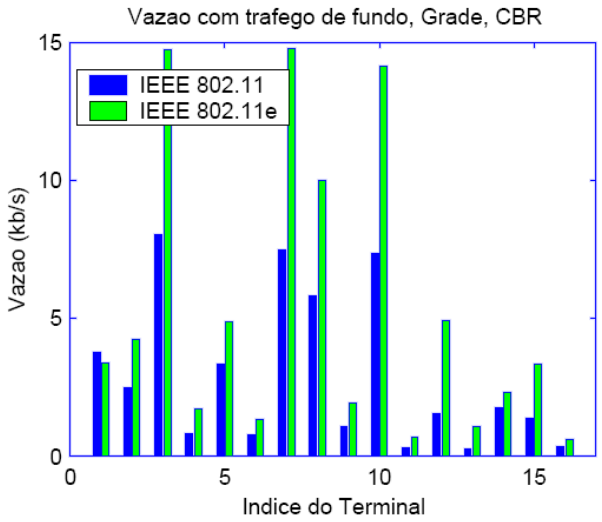

Fig. 5.8: Vazão por nó para o caso de um *gateway* e tráfego misto.

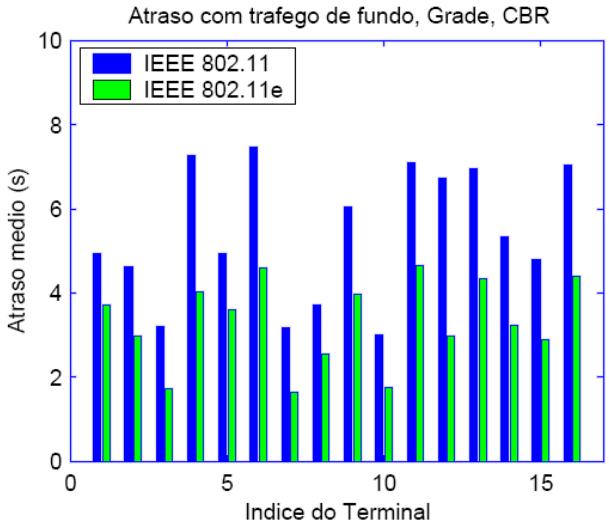

Fig. 5.9: Atraso médio por enlace para o caso de um *gateway* e tráfego misto.

Utilizando a EDCF para atribuir diferentes prioridades para os tipos de tráfego distintos, nota-se uma clara superioridade do IEEE 802.11e em relação ao IEEE 802.11 padrão, e consegue-se per-

Parâmetro	*IEEE 802.11*	*IEEE 802.11e*
Vazão [*kbits/s*]	$2,90$	$5,20$
Atraso [s]	$5,30$	$3,10$

Tab. 5.3: Valores médios para o cenário de um *gateway* com tráfego misto.

ceber a melhora trazida pela EDCF em relação a DCF quando se tem tipos de tráfego diferentes.

5.6 Conclusões

As simulações realizadas neste capítulo investigaram duas aplicações do mecanismo de atribuição de prioridades do IEEE 802.11e e compararam o seu desempenho em relação ao IEEE 802.11 padrão.

Primeiramente, as prioridades foram utilizadas numa tentativa de melhorar o desempenho em uma rede *multihop*, fazendo com que os terminais mais distantes do *gateway* apresentem prioridade maior. Para apenas um *gateway* foi observado que, em geral, o desempenho de ambos os protocolos é muito similar, com ligeira vantagem para o IEEE 802.11e, que utilizando seu mecanismo de suporte a QoS, consegue distribuir melhor os recursos entre os terminais. No entanto, em alguns casos, o IEEE 802.11e tem um desempenho pior que o IEEE 802.11 padrão, devido à atribuição de prioridade menor para os terminais mais próximos do destino. Já para o caso de cinco *gateways*, o IEEE 802.11 padrão possui desempenho melhor no geral. Com base nos resultados obtidos, pode-se concluir que não é muito vantajoso utilizar as classes de prioridades do IEEE 802.11e para tentar alocar melhor os recursos da rede.

Posteriormente, as prioridades foram utilizadas para distinguir tipos de tráfego diferentes. Neste caso, mostrou-se clara a vantagem do IEEE 802.11e em relação ao IEEE 802.11 padrão. O mecanismo EDCF é bem mais eficiente que o DCF ao lidar com tipos de tráfego diferentes e, nesse caso, as classes de prioridades devem ser utilizadas para melhorar o desempenho da rede.

No geral, o IEEE 802.11e se mostrou um protocolo MAC bastante promissor na área de redes ad hoc sem fio, principalmente no caso de diferentes tipos de tráfego, situação na qual as diferentes classes de prioridades funcionam muito bem.

Capítulo 6

Análise da Influência da Carga Oferecida e do Alcance de Interferência no Desempenho do IEEE 802.11 em WMN

Neste capítulo será feita uma análise da influência da carga oferecida e do alcance de interferência no desempenho da rede ao se utilizar o IEEE 802.11 na camada MAC. Para isso, será utilizado o mesmo cenário de um *gateway* do capítulo anterior (ver figura 5.1), com os mesmos parâmetros de camada física, MAC e roteamento.

6.1 Influência da Carga Oferecida

Para esta primeira análise, foram determinados quatro grupos de nós ativos, aumentando progressivamente a carga oferecida na rede, conforme mostra a tabela 6.1. Nessa simulação foi utilizado o tráfego CBR de 50 kbits/s do capítulo anterior.

Grupo	*No. de nós ativos*	*No. dos nós*	*Carga oferecida*
G1	1	1	50 $kbits/s$
G2	2	1, 48	100 $kbits/s$
G3	3	1, 26, 48	150 $kbits/s$
G4	5	1, 4, 26, 37, 48	250 $kbits/s$
G5	16	ver fig. 5.1	800 $kbits/s$

Tab. 6.1: Grupos de usuários ativos.

Para esse cenário em particular, podemos observar que o desempenho em aplicações sensíveis ao atraso é aceitável quando temos até dois nós ativos, pois o desempenho de rede cai rapi-

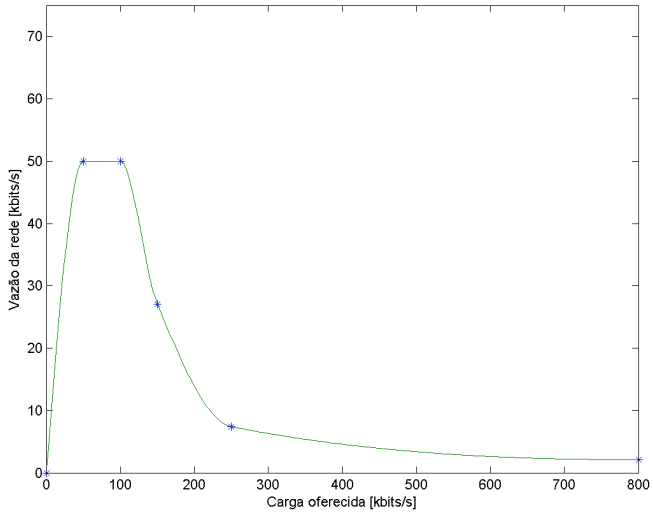

Fig. 6.1: Vazão da rede em função da carga oferecida.

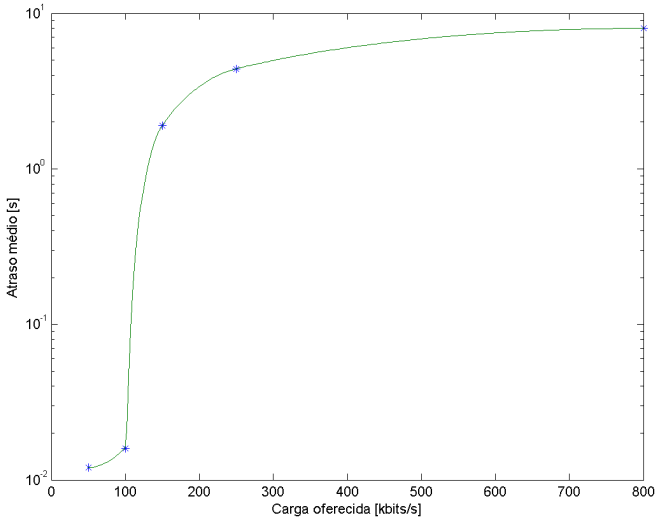

Fig. 6.2: Atraso médio na rede em função da carga oferecida.

damente quando o número de nós aumenta além disso (figura 6.2). No caso da vazão, observamos que a rede não consegue escoar todo o tráfego mesmo quando temos apenas dois nós transmitindo tráfego CBR contínuo (figura 6.1). Tal queda na vazão ocorre devido ao alto número de pacotes perdidos por colisão ou por descarte no *buffer* da MAC, o que mostra que o IEEE 802.11 não é eficaz no encaminhamento de pacotes em redes *multihop*, pois muitos dos pacotes a serem encaminhados acabam sendo perdidos, principalmente por descarte no *buffer* da camada MAC.

6.2 Influência do Alcance de Transmissão e do Alcance de Interferência

O bom desempenho de uma rede *ad hoc multihop* sem fio depende da capacidade do protocolo de camada MAC permitir o reuso espacial do canal e de evitar colisões. Esses dois atributos estão diretamente ligados ao alcance de transmissão (d_{Tx}), que é a máxima distância a partir da antena transmissora que o pacote pode ser recebido corretamente, e ao alcance de interferência, ou *carrier sensing* (d_{CS}), que é a máxima distância que um nó consegue interferir na transmissão dos outros nós).

Nesta análise, o desempenho da rede é observado como uma função do alcance de transmissão e do alcance de interferência. Os cenários de simulação são os seguintes:

1. d_{Tx} = 250 m e d_{CS} = 550 m: os mesmos valores utilizados em todas as simulações deste capítulo e do capítulo anterior (d_{CS}/d_{Tx} = 2,2);
2. d_{Tx} = 320 m e d_{CS} = 704 m: nesse caso, oito nós vizinhos estão dentro do alcance de transmissão, mantendo a mesma razão d_{CS}/d_{Tx} = 2,2;
3. d_{Tx} = 320 m e d_{CS} = 320 m: novamente temos oito nós dentro do alcance de transmissão, mas com d_{CS}/d_{Tx} = 1.

São analisados ambos os tipos de tráfego (CBR e dados via FTP). Os resultados são mostrados nas figuras 6.3 e 6.4.

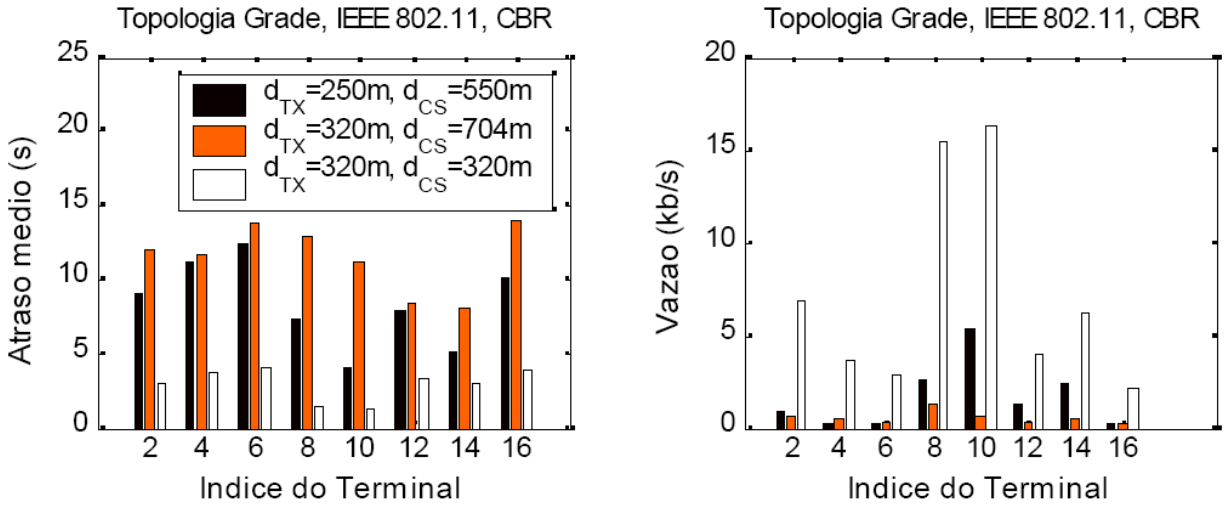

Fig. 6.3: Resultados para o tráfego CBR.

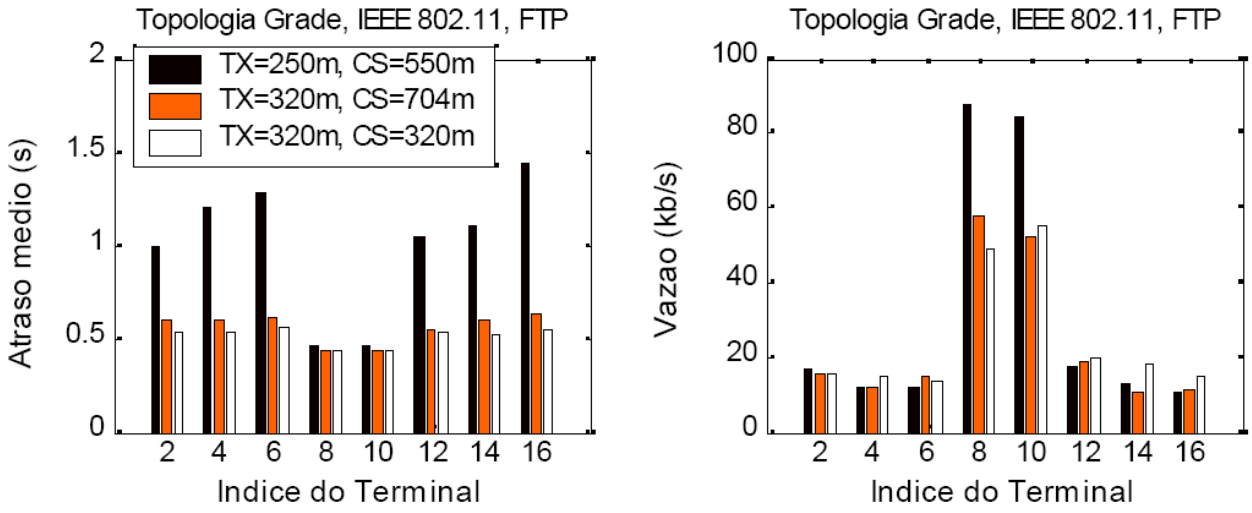

Fig. 6.4: Resultados para o tráfego FTP.

Como pode ser observado, os melhores resultados para o tráfego CBR são obtidos quando d_{CS}/d_{Tx} = 1, ou seja, se aumentarmos o alcance de transmissão a fim de diminuirmos o número de saltos, devemos diminuir o alcance de interferência. Resultados similares foram obtidos em [20]. Também podemos observar que quando d_{CS}/d_{Tx} = 2,2, o desempenho da rede é pior quando o alcance de transmissão e o de interferência são maiores, pois o reuso do canal é reduzido (maior nível de interferência implica em maior nível de contenção na MAC), resultando em maior atraso e menor vazão.

Para o tráfego de dados via FTP, os resultados são ligeiramente diferentes. Para o atraso, temos melhor desempenho com d_{CS}/d_{Tx} = 1; já para a vazão, a razão d_{CS}/d_{Tx} = 2,2 apresenta melhores resultados, com d_{CS} = 550 m e d_{Tx} = 250 m. No caso do FTP, existe o mecanismo do TCP por trás, que é um protocolo de transporte com garantia de entrega, permitindo retransmissão de dados em caso de falha na trasmissão. Logo, ao aumentarmos o alcance de transmissão, diminuindo o número de saltos, o atraso médio diminui, pois a soma do tempo de transmissão do dado, mais o atraso de *buffer* na MAC diminui. Porém, o atraso causado pelas retransmissões do TCP não necessariamente diminuem também, o que faz com que o desempenho em relação ao atraso seja similar nas duas situações em que o alcance de transmissão é de 320m.

6.3 Conclusões

Na primeira parte deste capítulo foi constatado que o IEEE 802.11 possui desempenho muito ruim em redes *multihop* conforme a carga de tráfego aumenta, seja pela sua influência negativa no encaminhamento de pacotes, ou pela sua incapacidade de prover eqüidade no acesso ao canal.

Por esse motivo, se espera que tal protocolo sempre irá apresentar desempenho ruim em situações de tráfego intenso.

Na segunda parte do capítulo, foi mostrado que o aumento do alcance de transmissão pode ser uma solução para diminuir o número de saltos e, conseqüentemente, aumentar o desempenho da rede. No entanto, isso só se torna uma alternativa viável se diminuirmos também o alcance de interferência.

Capítulo 7

Análise da Influência do Mecanismo de Handshaking RTS/CTS no Tráfego VoIP para o IEEE 802.11 em WMN

Diversos estudos na área de redes ad hoc sem fio utilizam o protocolo IEEE 802.11 como padrão para o controle de acesso ao meio, mesmo sabendo que este é muito ineficiente [18] e tem seu desempenho muito dependente da configuração da rede, principalmente no modo multihop. Neste capítulo é investigada a influência do mecanismo de RTS/CTS no desempenho geral de uma rede do tipo WMN. O objetivo principal desta análise é verificar o quanto o *overhead* provocado por esse mecanismo influencia no desempenho em uma rede WMN e se é possível abrir mão desse recurso que evita o problema do terminal escondido e ainda assim atingir QoS em transmissões de voz. Neste estudo é utilizado um cenário do tipo grade de nós com diferentes configurações de transmissores e receptores.

7.1 Requisitos do Tráfego VoIP e QoS

Em uma transmissão de pacotes de voz, alguns requisitos devem ser satisfeitos para a garantia da inteligibilidade da conversação. Tais requisitos são definidos pelos parâmetros: atraso máximo por pacote, variação máxima do atraso por pacote e máxima taxa de perda de pacotes. O mais crítico deles é o tempo de atraso, pois conforme ele cresce, a perda de interatividade aumenta. A ITU-T, através da recomendação G.114 [21], define que um atraso total fim-a-fim de 400 ms é inaceitável para transmissão de voz. A faixa de 150 ms a 400 ms é aceitável, embora exista alguma perda de interatividade. O ideal é que o atraso esteja abaixo dos 150 ms.

Em redes *ad-hoc* e WMN, a maior parte dos atrasos é causada pela natureza dos protocolos

MAC, como o IEEE 802.11 e suas extensões, que são baseados em contenção. Nesses protocolos, os pacotes esperam pela transmissão em um *buffer* na camada MAC, resultando em atrasos. Além disso, é comum ocorrer *overflow* nos *buffers*, o que causa perda de pacotes. Uma taxa de perda de pacotes pequena (5% ou menos é um valor comum na literatura) é aceitável e não compromete a inteligibilidade da conversa. Altas taxas de perda produzem cortes na comunicação que são bastante incômodos para o ouvinte. Isso é mais perceptível ainda quando os pacotes perdidos são consecutivos.

O atraso e a perda de pacotes estão bastante ligados ao mecanismo de *handshaking* RTS-CTS do 802.11. Embora ele minimize as colisões de terminal escondido, seu *overhead* diminui a eficiência do mecanismo da MAC. Por esse motivo, existe um limiar (em bytes) para o tamanho do pacote que será transmitido usando o RTS-CTS. Para valores menores que esse limiar, os pacotes são transmitidos sem o mecanismo de *handshaking*. Um limiar de 250 bytes é adotado na literatura como ótimo para WLANs [22]. Já roteadores WiFi comerciais adotam um valor padrão de 2347 bytes. Pacotes de voz VoIP geralmente possuem tamanho de 160 bytes devido à recomendação da ITU-T G.711, μ-Law, que é um padrão para codificação de voz PCM 64 kbits/s na América do Norte e no Japão. Por esse motivo, são transmitidos sem o mecanismo RTS-CTS.

A variação do atraso pode interferir na qualidade da comunicação, pois sinais de voz precisam ser reproduzidos continuamente no terminal de destino. No entanto, esse não é um problema muito comum, já que dispositivos e *softwares* VoIP geralmente possuem um *buffer* de recepção para armazenar os pacotes de voz antes de serem reproduzidos para o ouvinte.

Com base nos fatos citados, para as simulações, foram adotados como requisitos de QoS um atraso médio de até 250 ms e uma taxa de perdas máxima de 5%.

7.2 Cenários de Simulação

Nesta seção serão apresentados os cenários de simulação e os detalhes de configuração de cada cenário. Todas as simulações foram realizadas no simulador de redes ns-2. A taxa de transmissão na camada física é de 11 Mbits/s, operando na faixa ISM de 2,4 GHz, conforme o padrão 802.11b, comercialmente conhecido como WiFi. O modelo de propagação utilizado é o de terreno plano (*Two-ray Ground*) e o protocolo de roteamento utilizado é o DSR.

O cenário adotado em todas as simulações é o do tipo grade de nós 7x7, com espaçamento de 200m entre cada nó. Cada um dos nós possui alcance de transmissão de 250m e alcance de interferência de 300m.

Para a simulação das conversas telefônicas, foi elaborado um modelo baseado em uma Cadeia de Markov de dois estados, explicado a seguir: cada terminal pode assumir um dos dois estados possíveis (*on* ou *off*) e, enquanto um está *on*, o outro está *off*, e vice versa. O tempo de permanência

em cada estado é definido por uma variável aleatória com distribuição exponencial de média igual a 2 segundos. O estado *on*, representando atividade no canal, é modelado por uma fonte de tráfego CBR, cujos parâmetros são os da recomendação de codificação de voz G.711, μ-LAW [23] (taxa de 64 kbits/s e pacotes de 160 bytes). Já no estado *off*, nenhum tipo de tráfego é gerado. A implementação para ns-2 em tcl está inclusa no *Apêndice A*.

Foi escolhido um tempo de simulação de 5 minutos e o tempo de início de cada uma das conversações telefônicas é aleatório, uniformemente distribuído entre 0 e 10 segundos.

Os resultados de simulação a seguir representam a média dos resultados de 10 simulações executadas, considerando-se tanto o enlace direto quanto o enlace reverso.

7.3 Resultados das Simulações

7.3.1 Apenas um *gateway*

Neste cenário, foi escolhido o nó central da grade para atuar como *gateway* da rede. Parte-se do pressuposto que todas as ligações telefônicas serão para terminais de outras redes. Logo, toda a comunicação passa pelo *gateway*. Foram escolhidos arbitrariamente 16 terminais ativos para esta simulação, conforme mostra a figura 7.1. O *gateway* está assinalado em preto e os terminais ativos, em vermelho. Os enlaces estão numerados de acordo com a ordem crescente do índice dos nós (por ex: nó 0 corresponde ao enlace 1; nó 2, enlace 2; nó 4, enlace 3; e assim por diante).

As simulações mostram que o mecanismo de RTS/CTS prejudica o desempenho em transmissões de voz, conforme mostram as figuras 7.2, 7.3 e 7.4. O *overhead* provocado pelo *handshaking* ocasiona maiores atrasos, variação do atraso e perdas.

Apesar do desligamento do mecanismo de RTS/CTS melhorar bastante o desempenho da rede, não se conseguiu atingir valores que garantissem QoS. Logo, para a topologia analisada, não é possível garantir QoS com apenas um *gateway*. Apesar disso, deve-se levar em conta que este é um cenário bastante estressante e que representa a situação de pior caso em uma rede real. Na prática, dificilmente se utiliza apenas um *gateway*. Geralmente é usado mais de um por redundância. As análises seguintes irão abordar os casos de utilização de dois e quatro gateways, respectivamente.

7.3.2 Rede com Dois *Gateways*

Nesta análise, é utilizado a mesma grade de nós do item anterior, porém com dois gateways, representadas pelos nós em preto na figura 7.5. A linha tracejada na figura determina a fronteira entre as duas regiões de influência dos *gateways*: nós ativos (assinalados em vermelho) acima da linha tracejada se comunicam se comunicam com o *gateway* de número 40, enquanto o restante se

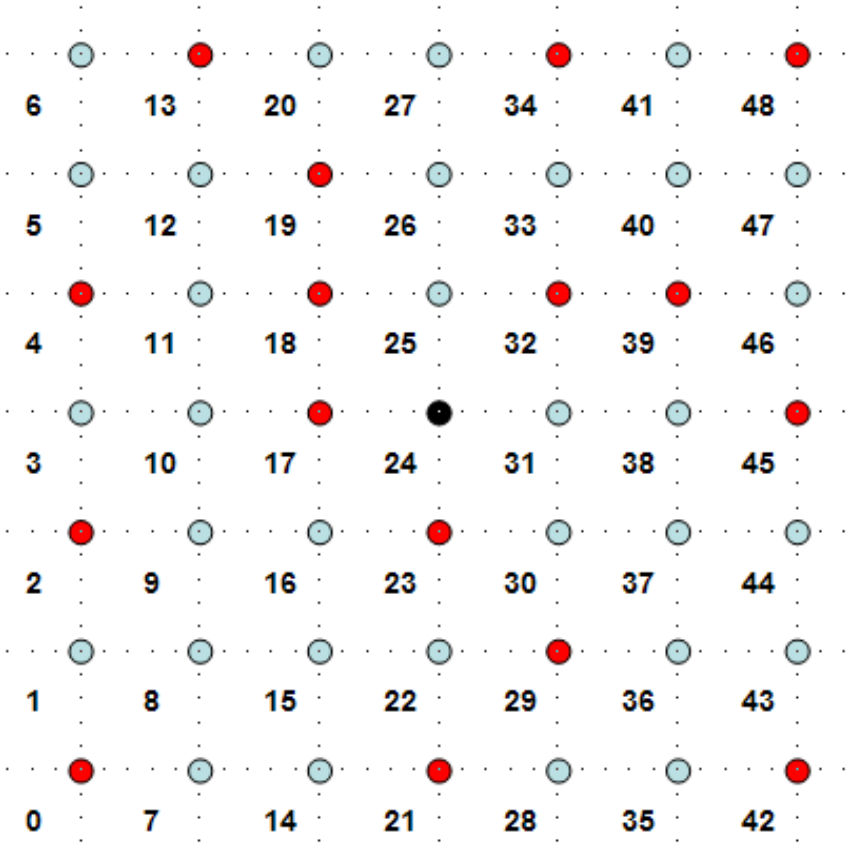

Fig. 7.1: Cenário para a simulação com um *gateway*.

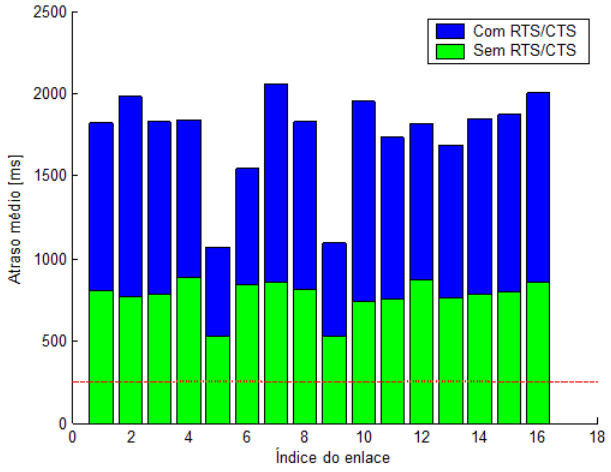

Fig. 7.2: Atraso médio em ms para o cenário com um *gateway*.

comunica com o *gateway* de número 8. Todos os parâmetros de simulação foram mantidos em relação à análise para um *gateway*.

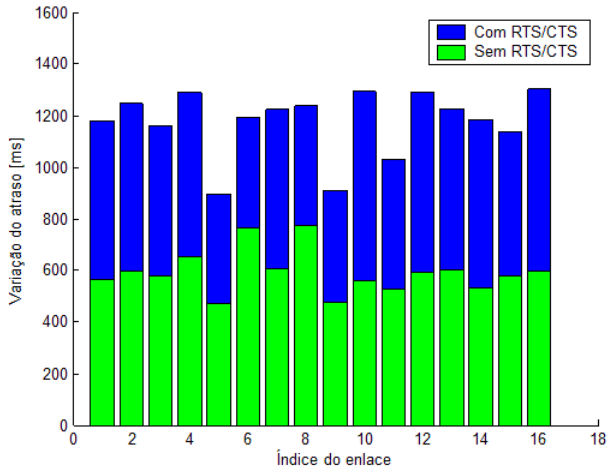

Fig. 7.3: Variação do atraso em ms para o cenário com um *gateway*.

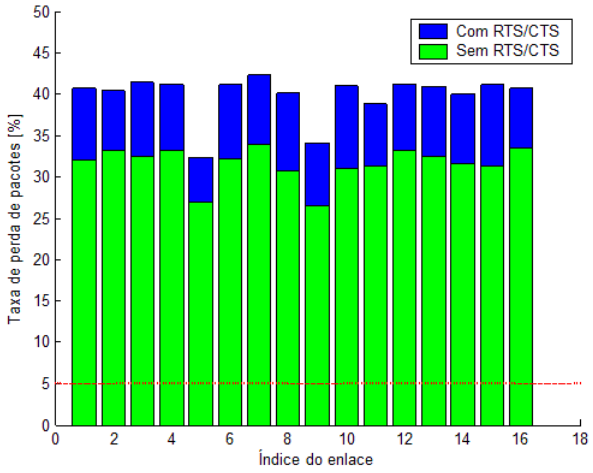

Fig. 7.4: Taxa de perdas para o cenário com um *gateway*.

Nessas simulações, pode-se notar que em sete dos terminais se conseguiu atingir as metas de QoS com o mecanismo de RTS/CTS desabilitado, conforme pode ser visto nas figuras 7.6, 7.7 e 7.8. Pode-se inferir que ao se adicionar mais alguns *gateways*, as condições de QoS serão satisfeitas para todos os terminais ativos, visto que a capacidade por *gateway* aumenta e o número de saltos por enlace diminui. Tal fato será abordado na seção seguinte.

É importante observar que apesar do atraso médio dos nós que atingiram QoS estar baixo, a variação do atraso tem valor em torno de 200 ms, que é alto para transmissão de voz. Isso mostra que a capacidade dos gateways ainda está abaixo do necessário para escoar todo o tráfego.

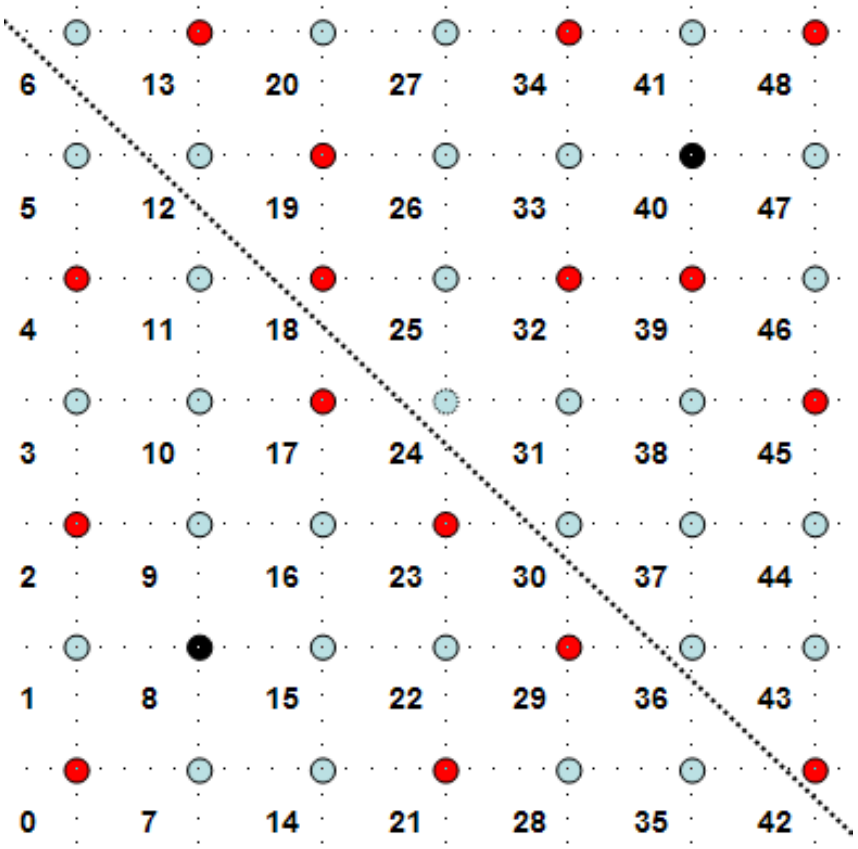

Fig. 7.5: Cenário para a simulação com dois *gateways*.

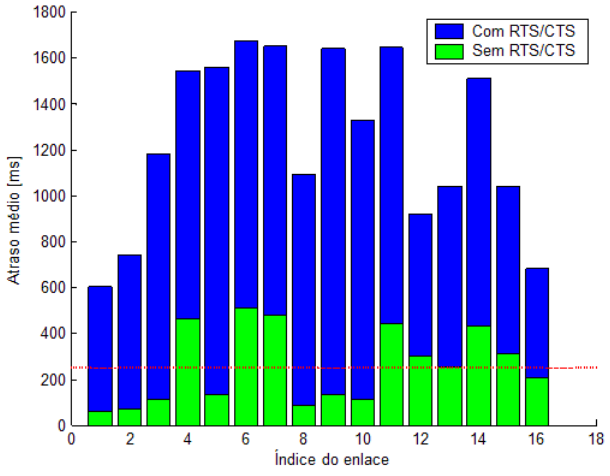

Fig. 7.6: Atraso médio em ms para o cenário com dois *gateways*.

7.3.3 Rede com Quatro *Gateways*

Ainda mantendo a mesma configuração, são utilizados quatro *gateways*, conforme mostra a figura 7.9. Neste caso existem quatro regiões distintas, contra duas do item anterior. Novamente, os

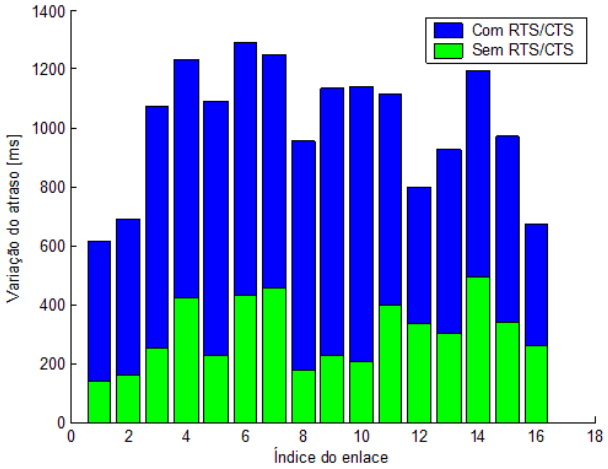

Fig. 7.7: Variação do atraso em ms para o cenário com dois *gateways*.

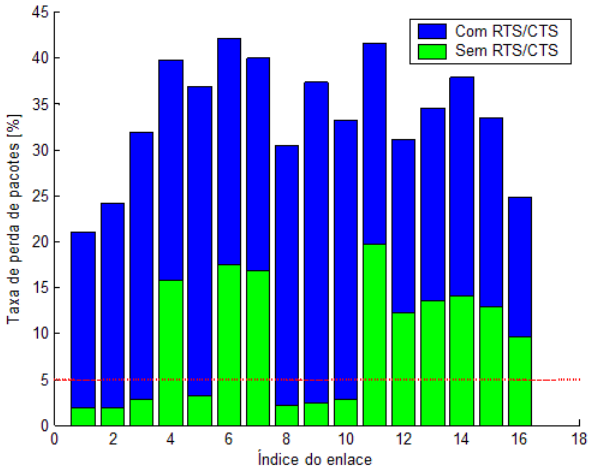

Fig. 7.8: Taxa de perdas para o cenário com dois *gateways*.

nós que se localizam dentro de cada região se comunicam com o *gateway* correspondente.

Os resultados das figuras 7.10, 7.11 e 7.12 mostram novamente que, apesar de todos os nós satisfazem requisitos de QoS em ambas as situações, o desempenho com o mecanismo de *handshaking* desabilitado é melhor, com taxa zero de perdas em todos os terminais ativos, exceto os de número 3 e 5.

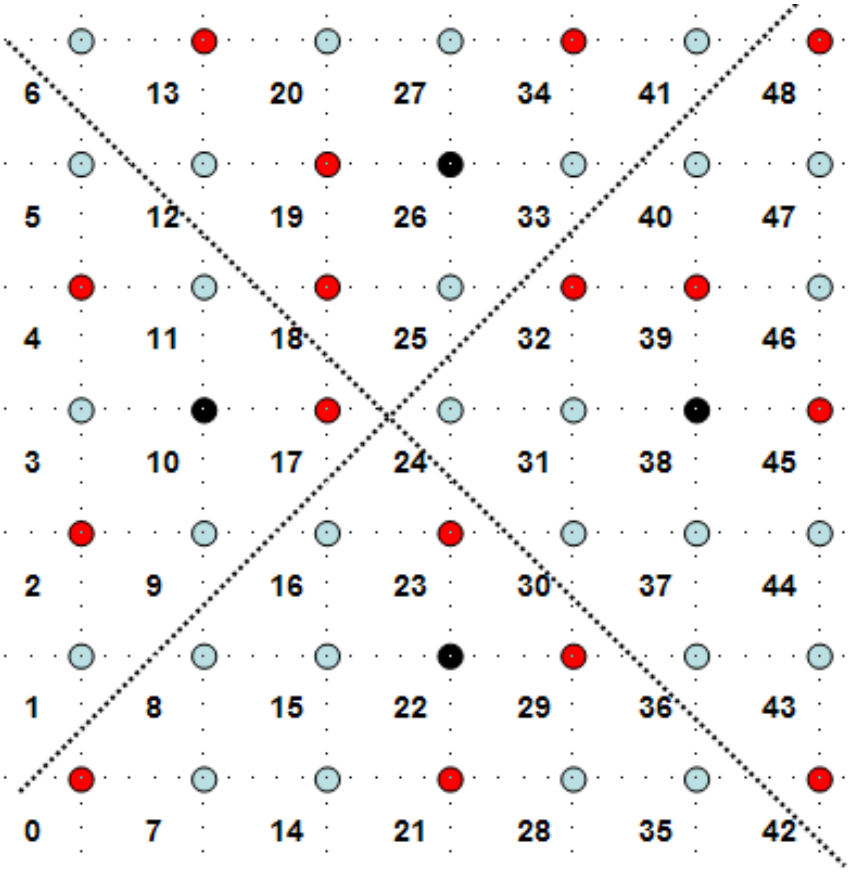

Fig. 7.9: Cenário para a simulação com quatro *gateways*.

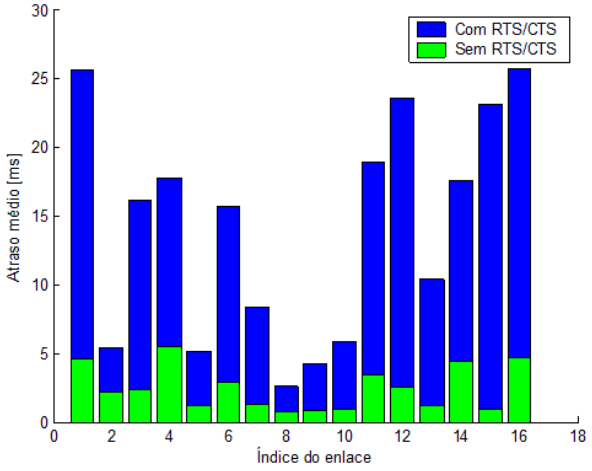

Fig. 7.10: Atraso médio em ms para o cenário com quatro *gateways*.

7.4 Conclusões

O principal objetivo deste capítulo foi analisar o impacto do mecanismo de *handshaking* do IEEE 802.11 no desempenho de uma rede ad hoc transmitindo pacotes de voz. A análise abrange um

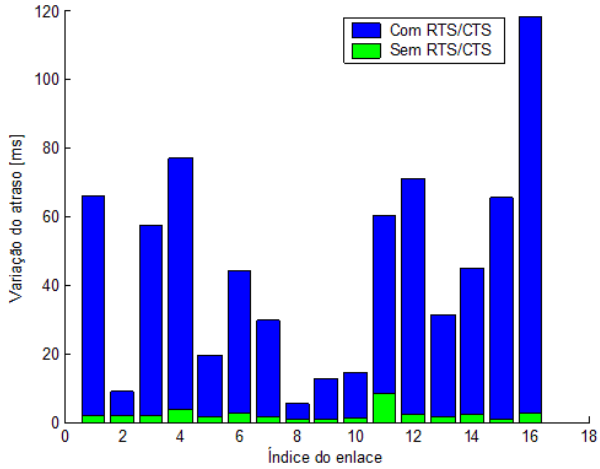

Fig. 7.11: Variação do atraso em ms para o cenário com quatro *gateways*.

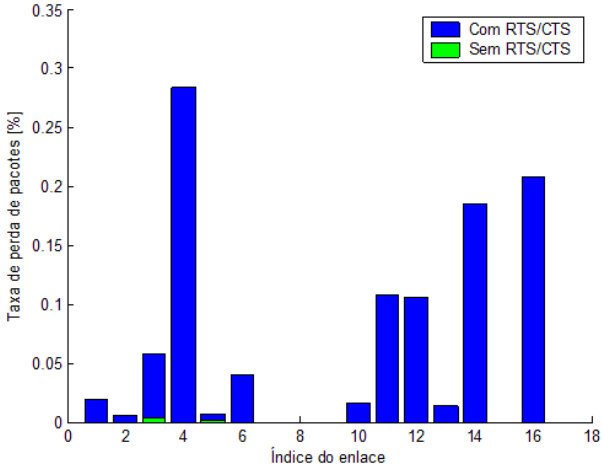

Fig. 7.12: Taxa de perdas para o cenário com quatro *gateways*.

cenário de múltiplos saltos e comunicação tanto no enlace direto quanto no enlace reverso. Para tal análise, foram realizadas simulações em ns-2 a fim de avaliar o grau de influência do mecanismo de RTS/CTS no desempenho da rede. Os resultados mostraram que tal mecanismo provoca um overhead bastante prejudicial ao desempenho e que a adoção deste mecanismo para evitar colisões não compensa no caso de transmissão de voz, visto que o tempo gasto no handshaking é maior que o tempo de transmissão de um pacote de voz. De fato, existiram situações nas quais não houve uma colisão sequer mesmo com o *handshaking* desabilitado, comprovando que, assim como em WLANs com controle centralizado, o mecanismo de RTS/CTS é bastante prejudicial em transmissões de voz em redes ad hoc *multihop*.

Capítulo 8

Simulações e Resultados Comparativos entre IEEE 802.11 e IEEE 802.11e em WMN com Tráfego VoIP

Após a implementação de um algoritmo gerador de tráfego VoIP e a análise sobre o RTS-CTS feita no capítulo anterior, temos material suficiente para aprofundarmos o estudo em WMN. O principal objetivo deste capítulo é analisar o desempenho de uma rede do tipo *mesh* em uma situação próxima de um cenário real. Essa análise é importante pois visa avaliar a viabilidade de se usar a tecnologia de redes WMN na provisão de serviços de telefonia VoIP. As redes *mesh* são redes *ad hoc* conectadas a uma infraestrutura fixa através de *gateways*. Tais redes podem ser utilizadas para prover serviços de voz e dados em áreas onde a base de assinantes não seja grande o suficiente para justificar o custo de uma infraestrutura fixa, como por exemplo em áreas rurais ou pequenas comunidades.

A seguir será descrito o cenário de simulação utilizado para fazer tal análise.

8.1 Cenários de Simulação

Para as simulações deste capítulo, usaremos primeiro o IEEE 802.11b nas camadas física e MAC. Conforme já foi mencionado neste texto, o 802.11b oferece taxas de transmissão de até 11 Mbits/s e opera na faixa ISM de 2,4 GHz. Será feita a comparação de desempenho com o protocolo IEEE 802.11e, que utiliza a EDCF e a discriminação de serviços na camada MAC. O protocolo de roteamento utilizado é o DSR.

A topologia de rede utilizada ainda é a grade de nós 7x7 do capítulo anterior, com 49 terminais uniformemente distribuídos em um quadrado com 1200 m de lado (7.1). Foi utilizado um alcance de transmissão de 250 m e um alcance de interferência de 300 m.

O tráfego VoIP é modelado exatamente da mesma forma que no capítulo anterior, ou seja, uma cadeia de Markov de dois estados (*on-off*). Quando o terminal está no estado *on*, o tráfego é modelado como uma fonte CBR de 64 kbits/s, enviando pacotes de 160 bytes, simulando uma transmissão de voz PCM de acordo com a recomendação G.711, μ-Law da ITU-T. Quando o terminal está no estado *off*, não envia nenhum pacote. A duração de cada estado é determinada por uma variável aleatória exponencial com média igual a 2 segundos. Tal valor foi adotado como a duração média de uma frase que uma pessoa fala ao telefone.

Para simularmos diferentes cargas de tráfego, foram utilizadas três configurações de *gateways* diferentes. Para simular tráfego pesado, utilizou-se um único *gateway* recebendo tráfego de 16 terminais ativos (pontos vermelhos na figura 7.1), o que resulta em uma atividade de 33%. Um segundo cenário com dois *gateways* para os mesmos 16 terminais ativos (16% de atividade) é utilizado para simular uma situação de HMM (ver figura 7.5). O último cenário apresenta quatro *gateways* para 16 terminais ativos (8% de atividade), simulando uma situação de tráfego leve (ver figura 7.9). Cada conversa telefônica simulada possui um tempo de início aleatório, uniformemente distribuído entre 0 e 10 segundos, a fim de evitarmos o início de simulação simultâneo em todos os nós. O tempo total de simulação é de 300 segundos.

Nas simulações deste capítulo, os pacotes de voz possuem um tempo de vida de 440 ms. Não devemos confundir esse tempo com o TTL tipicamente adotado em redes, que é mais utilizado para contagem de saltos no trajeto fim-a-fim (terminal para o *gateway* e vice-versa). Quaisquer pacotes recebidos com um atraso maior que 400 ms é descartado e considerado uma perda. O atraso total fim-a-fim é a soma do tempo de espera no *buffer* de transmissão com o tempo de transmissão propriamente dito. Os atrasos de codificação de voz, geração de pacote e no *buffer* de recepção não são considerados.

Os parâmetros de QoS utilizados são aqueles discutidos no capítulo anterior: taxa máxima de perda de 5% e um atraso máximo fim-a-fim de 400 ms. Os resultados apresentados são uma média de 10 simulações.

8.2 Resultados

8.2.1 Desempenho do IEEE 802.11b - Apenas Tráfego VoIP

As primeiras simulações nos mostram o desempenho do tráfego VoIP quando utilizamos as especificações do IEEE 802.11b nas camadas física e MAC. Nas figuras 8.1 e 8.2, temos os resultados por enlace para as diferentes cargas de tráfego.

Os resultados são bons na situação de tráfego leve, com uma taxa média de perdas de 2,4%,

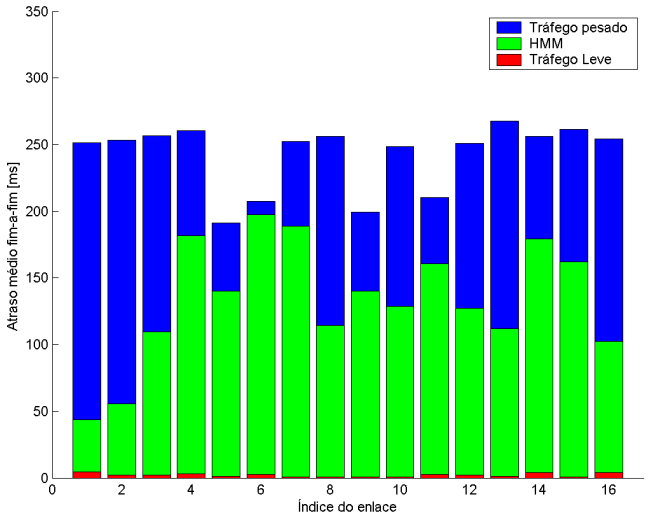

Fig. 8.1: Atraso médio fim-a-fim por enlace para o 802.11b com tráfego VoIP.

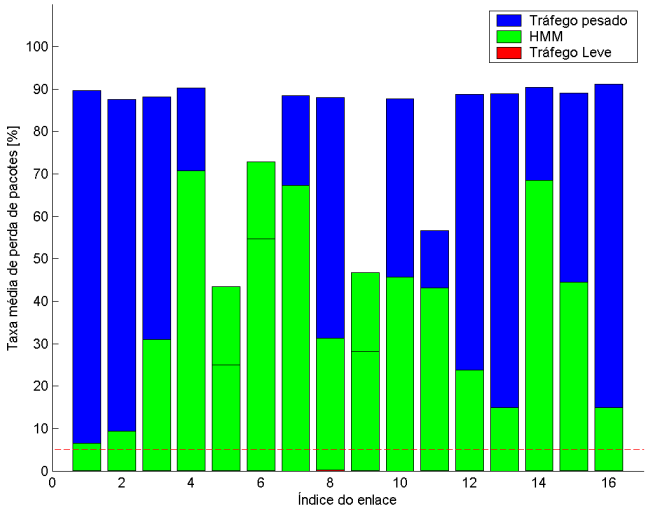

Fig. 8.2: Taxa de perdas por enlace para o 802.11b com tráfego VoIP.

atraso médio fim-a-fim de 2,1 ms e uma variação média do atraso de 1,2 ms, mostrando que o 802.11b é viável em situações de tráfego leve.

Em HMM, o atraso médio fim-a-fim é aceitável (134 ms, com variação média de 49 ms), mas a taxa média de perdas é muito alta, acima de 39%. Verificando o desempenho individual de cada terminal, percebemos que aqueles próximos a um *gateway*, apesar de não atingirem a meta de QoS, apresentam taxas baixas de perda de pacotes, enquanto aqueles mais distantes de um *gateway* apresentam taxas de perda altíssimas, geralmente acima de 40%. A mesma situação é observada no

caso de tráfego pesado, quando temos um atraso médio fim-a-fim de 242 ms e uma variação média do atraso de 26 ms. A taxa de perdas média é ainda pior que aquela registrada em HMM: 77%. Em alguns casos, em especial os terminais mais distantes do *gateway*, as perdas ultrapassam 90%.

A alta taxa de perdas pode ser explicada através de dois fatores: a já conhecida ineqüidade na alocação dos recursos no 802.11 e colisões de pacotes. Já é conhecido da literatura que o mecanismo MAC do 802.11 para redes *ad hoc* favorece os terminais que já efetuaram uma transmissão com sucesso, em detrimento àqueles que ainda estão tentando acessar o canal de rádio. Por causa disso, os terminais mais próximos aos *gateways* geralmente conseguem efetuar uma transmissão com sucesso mais cedo que os demais, ganhando preferência e, com isso, causando a degradação do desempenho global da rede conforme o tráfego aumenta [18]. As colisões podem ser explicadas através da ocorrência do problema do terminal escondido, já que o mecanismo RTS-CTS está desabilitado para o tráfego VoIP (ver capítulo anterior). Por outro lado, por causa do tempo de vida dos pacotes, mesmo se o *handshaking* estivesse habilitado, as perdas ainda seriam altas pois a maioria dos pacotes iria ser descartada nos *buffers* de transmissão, devido ao tempo de espera até que o terminal consiga acesso ao canal. Por causa disso, conclui-se que a ineqüidade na alocação dos recursos de rádio é o aspecto mais influente na alta taxa de perda de pacotes no IEEE 802.11 quando temos uma situação de alto tráfego. Logo, esse padrão é inadequado para prover serviços VoIP em áreas populosas, como cidades, por exemplo.

8.2.2 Desempenho do IEEE 802.11e - Apenas Tráfego VoIP

O IEEE 802.11e é uma tentativa muito promissora de melhorar o desempenho do padrão IEEE 802.11 em redes *ad hoc*. Como já foi mencionado no capítulo 2, o 802.11e introduz algumas modificações para a provisão de QoS no 802.11. Nessa simulação, as funções de suporte a QoS não estão sendo usadas, apenas o mecanismo melhorado de acesso ao meio. Os resultados observados nas figuras 8.3 e 8.4 nos mostram que essa MAC melhorada sozinha já garante melhora de desempenho em relação aos resultados obtidos para o 802.11b

Em situações de tráfego leve, embora o 802.11b tenha tido um bom desempenho, o 802.11e mostra resultados ainda melhores, com um atraso médio fim-a-fim de 2 ms, variação do atraso de 0,9 ms e uma taxa de perdas de apenas 0,5 %.

Na simulação de HMM, embora nenhum terminal tenha atingido a meta de QoS de 5% de perdas, o 802.11e também apresentou um desempenho melhor que o 802.11b, com uma média de 27% de pacotes perdidos. Os valores médios obtidos para o atraso e variação do atraso (65 ms e 34 ms, respectivamente) também foram significativamente mais baixos que aqueles obtidos na simulação anterior. Novamente, os terminais mais distantes dos *gateways* tiverem desempenho ruim. A taxa de perdas média global caiu 12% em relação àquela obtida para o 802.11b, mas ainda assim está muito

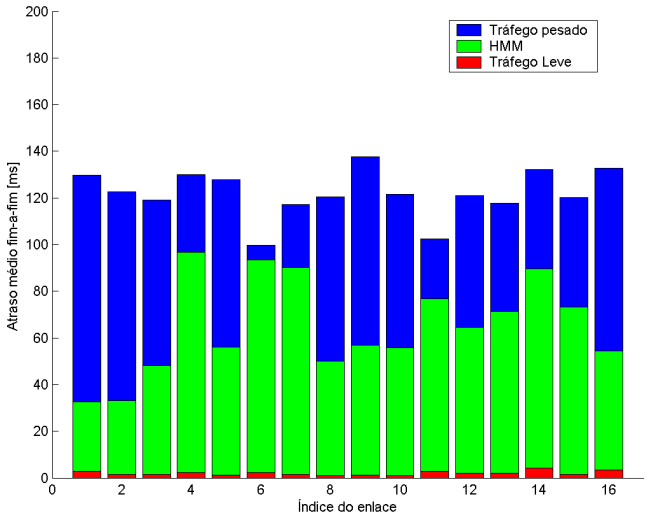

Fig. 8.3: Atraso médio fim-a-fim por enlace para o 802.11e com tráfego VoIP.

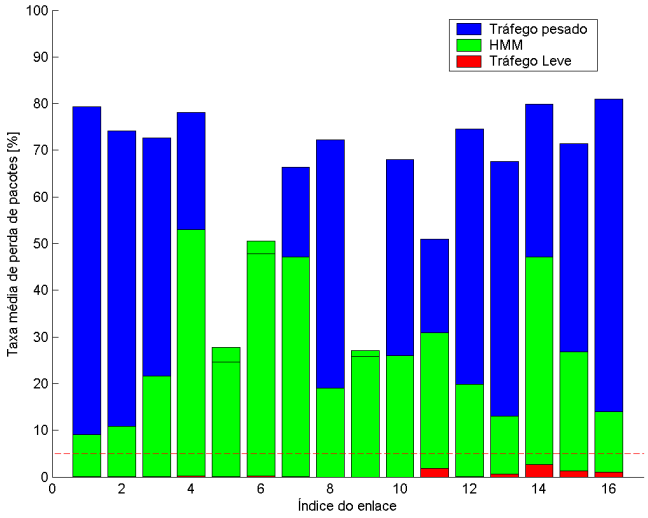

Fig. 8.4: Taxa de perdas por enlace para o 802.11e com tráfego VoIP.

alta.

Na situação de tráfego pesado, observamos novamente uma melhora em relação ao 802.11b, mas ainda assim as perdas estão muito altas, em torno de 64%.

Embora as melhoras observadas não sejam muito significativas no geral, podemos perceber claramente que a MAC do 802.11e é melhor, reduzindo o atraso médio fim-a-fim, a variação do atraso e a taxa de perda de pacotes. As grandes diferenças entre os dois protocolos ficarão mais claras na próxima simulação, na qual temos os cenários aqui apresentados com a adição de tráfego de fundo

FTP.

8.2.3 Desempenho do IEEE 802.11b - Tráfego VoIP e FTP

Como ambos os protocolos analisados neste capítulo não atingiram os requisitos de QoS nas situações de HMM e tráfego pesado, decidiu-se manter o foco na situação de tráfego leve. Esse cenário reproduz bem as condições de tráfego encontradas em áreas rurais e pequenas comunidades, onde a aplicação comercial das redes WMN é mais promissora.

A fim de sobrecarregar ainda mais os protocolos, foi introduzido um tráfego de fundo FTP, simulando algumas conexões de dados entre as transmissões VoIP. Esse tráfego é representado por enlaces de comunicação estabelecidos entre os seguintes pares de nós: 11 e 12, 15 e 15, 33 e 40 (ver o posicionamento dos nós na figura 7.9).

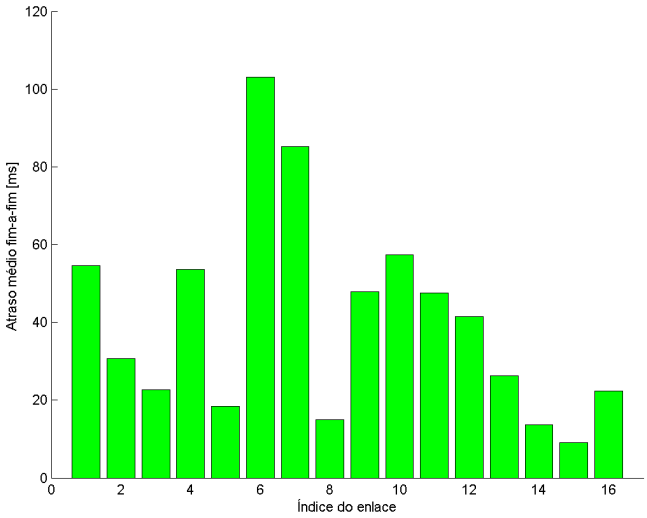

Fig. 8.5: Atraso médio fim-a-fim por enlace para o 802.11b com tráfego misto.

Nesse cenário de tráfego misto, podemos notar que o desempenho da rede é consideravelmente pior que aquele observado no cenário com tráfego VoIP apenas (figuras 8.5 e 8.6). Com a introdução do tráfego FTP e a ausência de um mecanismo de discriminação de serviços, o 802.11b apresenta um valor de atraso médio cerca de 20 vezes maior (41 ms) e uma variação do atraso 30 vezes maior (30 ms) que aqueles obtidos anteriormente. A taxa de perdas é ligeiramente alta (uma média de 10%) e o 802.11b não atinge as metas de QoS. Na próxima seção, veremos que o 802.11e apresenta um desempenho melhor, principalmente em relação ao atraso médio e a variação média do atraso.

A explicação dos motivos que levaram ao aumento no atraso, na variação do atraso e na taxa de perda de pacotes é feita na seção seguinte, na qual é feita a comparação entre os dois protocolos.

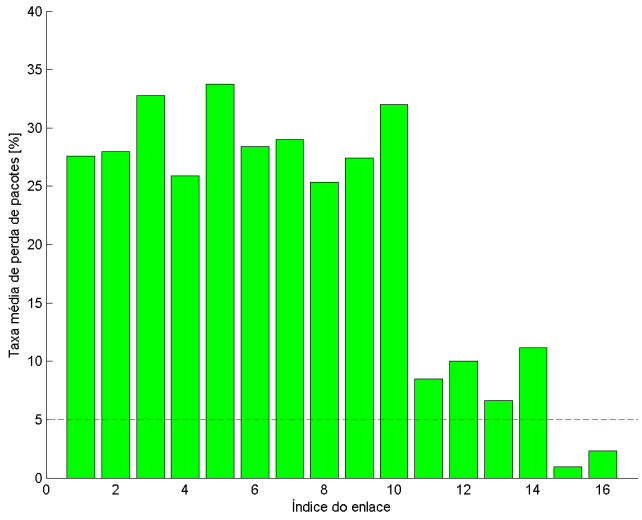

Fig. 8.6: Taxa de perdas por enlace para o 802.11b com tráfego misto.

8.2.4 Desempenho do IEEE 802.11e - Tráfego VoIP e FTP

Para essa simulação, as prioridades do IEEE 802.11e estão configuradas conforme mostra a tabela 8.1. Além da discriminação de serviços (voz e dados), as prioridades da MAC foram utilizadas para distingüir diferentes fluxos de tráfego VoIP de acordo com o número de saltos entre o terminal de origem e o *gateway*, de tal forma a reduzir o problema da ineqüidade na alocação dos recursos já mencionado anteriormente. Os terminais mais distantes dos *gateways* têm prioridade maior do que os mais próximos e, claro, todo o tráfego VoIP tem prioridade sobre o tráfego de dados e pacotes de roteamento.

VoIP - 3 ou mais saltos	*VoIP - 2 saltos*	*VoIP 1 salto*	*FTP e roteamento*
Máxima	Média	Mínima	Extra-mínima

Tab. 8.1: Atribuição de prioridades na MAC para a simulação do IEEE 802.11e.

Nesse cenário podemos ver claramente as vantagens do 802.11e sobre o 802.11b. Com a introdução do tráfego de fundo FTP, as funções de suporte a QoS ajudaram a reduzir o atraso médio fim-a-fim e a variação do atraso para os terminais mais distantes dos *gateways* (figuras 8.7 e 8.8). A taxa de perda de pacotes, no entanto, é ruim, apesar de ser melhor que no caso do 802.11b. No caso de apenas tráfego VoIP, tínhamos uma taxa de perdas média de apenas 0,5%. Agora, com o tráfego de fundo, a taxa média subiu para 9,8%. Embora as funções de suporte a QoS tenham funcionado, a introdução de seis novos nós ativos aumentou bastante a interferência. O 802.11e, assim como o

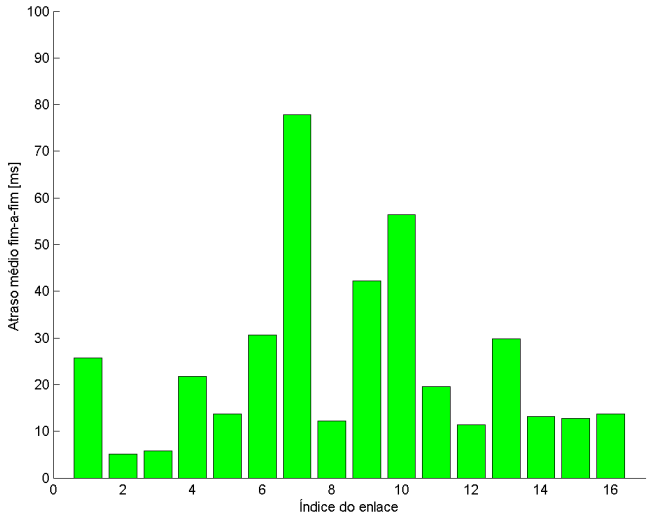

Fig. 8.7: Atraso médio fim-a-fim por enlace para o 802.11e com tráfego misto.

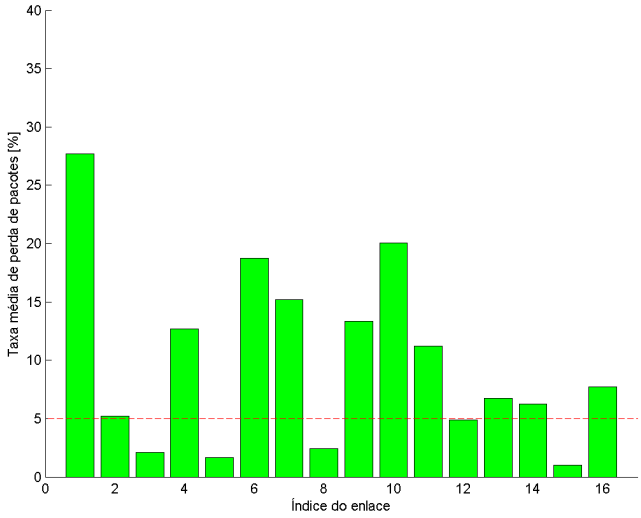

Fig. 8.8: Taxa de perdas por enlace para o 802.11e com tráfego misto.

802.11b, é um protocolo MAC baseado em contenção. Ou seja, quando um nó está transmitindo, todos os nós em seu raio de interferência identificam o meio como ocupado e não podem acessá-lo [9]. Em uma situação de grande interferência, tal fato faz com que o tempo de espera no *buffer* de transmissão aumente e, como temos um tempo de vida para cada pacote, a taxa de perdas aumenta também. Essa situação piora conforme o número de terminais ativos aumenta. Por esse motivo, quando aumentamos o número de terminais ativos para esse cenário, a taxa de perdas aumentou bastante quando comparada àquela obtida para o tráfego VoIP apenas, mesmo mantendo o tráfego

por *gateway* em valores baixos.

8.3 Conclusões

Neste capítulo foi feita uma análise comparativa de desempenho com tráfego VoIP entre dois protocolos de camada MAC. Os resultados mostram que o padrão comercial IEEE 802.11b apresenta um desempenho ruim em situações de tráfego pesado. Na tentativa de melhorar os resultados, o grupo IEEE 802.11e introduziu um novo protocolo MAC com funções de suporte a QoS, que pareceu ser bastante promissor. As simulações mostraram que o mecanismo aperfeiçoado de acesso ao meio do 802.11e sozinho já consegue melhorar o desempenho de rede em relação ao 802.11b. Quando utilizamos as funções de discriminação de serviços, as diferenças entre os dois protocolos são ainda mais evidentes, principalmente em relação ao atraso médio fim-a-fim e a variação média do atraso. Em relação à taxa de perda de pacotes, o 802.11e leva uma pequena vantagem em relação ao 802.11b.

Apesar de nenhum dos dois protocolos apresentar desempenho razoável em situações de tráfego intenso, o IEEE 802.11e aparenta ser bastante promissor na provisão de serviços VoIP em áreas de tráfego baixo. Com o uso de uma topologia de rede e potência de transmissão adequadas, pode ser uma tecnologia comercialmente viável para prover serviços de telefonia em áreas onde o número de assinantes é muito baixo para justificar o custo de uma infraestrutura de telefonia fixa.

Capítulo 9

Conclusão

9.1 Conclusões Gerais

Este trabalho apresentou um estudo detalhado sobre redes *ad hoc* e a influência dos protocolos de camada MAC no desempenho da rede através de simulações com o simulador de redes ns-2, que foi apresentado no capítulo 3.

Foram mostrados os desafios ao se projetar um protocolo de camada MAC para redes *ad hoc* e foram apresentados em detalhes diversos protocolos, tais como o padrão da indústria IEEE 802.11, uma de suas evoluções, o IEEE 802.11e, e também algumas sugestões do meio acadêmico visando melhorar o desempenho na camada MAC, como o DPS e o MACA-PR.

As primeiras simulações, em cenários simples, nos mostraram que o protocolo DPS, apesar da tentativa de melhorar o desempenho atribuindo classes de prioridades para os pacotes, adiciona um *overhead* de controle bastante significativo, tornando seu desempenho praticamente igual ao do IEEE 802.11 no caso de tráfego CBR e, pior que este no caso de tráfego FTP. O MACA-PR, em vez de apresentar melhor desempenho que o 802.11, apresentou resultados piores, justamente quando o mecanismo de reserva deveria mostrar o contrário (tráfego CBR). Da análise feita, é possível dizer que tal desempenho ruim foi causado pela maneira que o protocolo foi implementado no ns-2, que não corresponde 100% a sua descrição na literatura.

Após os resultados desfavoráveis obtidos para os protocolos DPS e MACA-PR, este estudo foi focado em um protocolo mais promissor: o IEEE 802.11e, que apresenta uma MAC aprimorada em relação ao 802.11 padrão e também funções de suporte a QoS. Foram feitas simulações em um cenário do tipo grade de nós, simulando uma rede do tipo WMN, a fim de comparar o desempenho entre o IEEE 802.11 e o IEEE 802.11e. Para essa comparação, as prioridades do IEEE 802.11e foram utilizadas tanto para diferenciar tipos de tráfego, como também para aumentar a prioridade do tráfego de terminais com maior número de saltos na comunicação. Os resultados mostraram que, no

caso de um tipo de tráfego apenas, utilizar prioridades em função do número de saltos pode não ser muito vantajoso, já que em alguns casos o 802.11e apresentou desempenho pior que o 802.11 padrão. Já quando usamos as prioridades para discriminação de serviços, ficou clara a vantagem do IEEE 802.11e sobre o 802.11 padrão. Devido aos resultados obtidos no capítulo 5, decidiu-se aprofundar o estudo na comparação entre o IEEE 802.11 e o IEEE 802.11e em WMN.

Foi feita ainda uma análise da influência da carga oferecida e dos alcances de transmissão e interferência no desempenho do IEEE 802.11. Foi mostrado que o IEEE 802.11 apresenta desempenho bastante ruim conforme a carga oferecida aumenta, confirmando que esse protocolo é inadequado para aplicações de tráfego intenso. Já em relação aos alcances de transmissão e interferência, foi mostrado que o aumento do alcance de transmissão pode ser uma solução para diminuir o número de saltos e, conseqüentemente, aumentar o desempenho da rede. No entanto, isso só se torna uma alternativa viável se diminuirmos também o alcance de interferência.

No capítulo 7, foi criado um algoritmo de geração de tráfego VoIP para o ns-2, a fim de tornar as simulações deste trabalho mais realistas. Além disso, através da análise feita sobre a influência do mecanismo de *handshaking* RTS-CTS no desempenho da rede, foi definido que, para o tráfego VoIP, devemos transmitir os pacotes sem utilizar o mecanismo, pois a sua capacidade de evitar o problema do terminal escondido não compensa o *overhead* que ele introduz na rede.

Com base no que foi obtido no desenvolvimento do capítulo 7, foi elaborado um último cenário de simulação, de tal forma a simular algumas situações próximas da realidade e, com isso, podermos avaliar a viabilidade do uso das redes WMN na provisão de serviços de voz para o usuário final. Novamente, a análise foi feita com base na comparação de desempenho entre os protocolos IEEE 802.11 e IEEE 802.11e, só que dessa vez, ambos os usos mencionados anteriormente para as prioridades foram implementados simultaneamente. Os resultados mostraram que nenhum dos dois protocolos apresenta desempenho satisfatório em situações de tráfego intenso. No entanto, em situações de tráfego leve, o IEEE 802.11e mostrou ser um protocolo bastante promissor. Nas primeiras simulações, sem diferenciação de serviços, foi mostrado que apenas a MAC aperfeiçoada do 802.11e sozinha é capaz de melhorar o desempenho de rede em relação ao 802.11 padrão. Quando introduzimos o tráfego misto, as prioridades mostraram que cumprem o papel para as quais foram designadas, mostrando melhoras significativas no atraso médio fim-a-fim e na variação média do atraso em relação ao resultados obtidos com o IEEE 802.11.

Com os resultados obtidos até então, pode-se afirmar que o IEEE 802.11e é um protocolo que merece atenção no estudo de redes *ad hoc*, principalmente quando nos referimos a provisão de serviços VoIP em áreas de tráfego baixo, como zonas rurais e pequenas comunidades. Com uma topologia de rede e potência de transmissão adequadas, a tecnologia pode ser comercialmente viável em áreas em que a base de assinantes não seja grande o suficiente para justificar o custo de uma

infraestrutura de telefonia fixa.

9.2 Trabalhos Futuros

As conclusões deste trabalho abrem caminho para novos pesquisas em redes *ad-hoc* e WMN. Um primeiro tema a ser considerado é a sugestão de melhorias para os protocolos de camada MAC, em especial o IEEE 802.11e, visando melhorar o desempenho geral da rede em situações de tráfego mais intenso. Uma possível solução para o problema seria um melhor controle das filas das diferentes categorias de acesso do 802.11e, visto que boa parte das perdas de pacotes ocorrem devido ao atraso causado pelo tempo de espera nas filas. O uso das prioridades também deve ser investigado mais a fundo, pois pode ser bastante útil na melhora do desempenho global da rede quando temos diferentes tipos de tráfego. O aprimoramento do MACA-PR também pode vir a ser uma solução viável para os problemas de desempenho. No entanto, até o presente momento, não existe uma implementação fiel e completa do protocolo para o ns-2, impossibilitando simulações do protocolo nesta ferramenta. A implementação completa do MACA-PR para o ns-2 seria de grande valia para a comunidade acadêmica, possibilitando estudos mais aprofundados sobre esse protocolo.

Referências Bibliográficas

[1] . Língua Portuguesa. Página da internet, Maio 2005. `http://educaterra.terra.com.br/sualingua/index2.htm`.

[2] Jie Wu, Ivan Stojmenovic. Guest Editor's Introduction: Ad Hoc Networks. *IEEE Computer*, 37:29–31, Fevereiro 2004.

[3] Visda Vokhshoori. A Survey Paper on Mobile Ad Hoc Networks. Class Project ELEN 6951, Columbia University, 2002.

[4] C. Siva Ram Murthy, B.S. Manoj. *Ad Hoc Wireless Networks: Architectures and Protocols*. Prentice Hall, 2004.

[5] Pedro Braconnot Velloso, Marcelo G. Rubinstein, Otto Carlos M.B. Duarte. Uma Avaliação da Capacidade de Transmissão de Voz em Redes 802.11 no Modo Ad Hoc. *Revista da Sociedade Brasileira de Telecomunicações*, 18(2), Outubro 2003.

[6] S. Kumar, V.S. Raghavan, J. Deng. Medium Access Control protocols for ad hoc wireless networks: a survey. Survey paper, Science Direct, Outubro 2004. `http://www.sciencedirect.com`.

[7] R. Jurdak, C.V. Lopes, P. Baldi. A Survey, Classifcation and Comparative Analysis of Medium Access Control Protocols for Ad Hoc Networks. *IEEE Communications Surveys and Tutorials*, 2004.

[8] J. Jun, M.L. Sichitiu. The Nominal Capacity of Wireless Mesh Networks. *IEEE Wireless Communications*, Outubro 2003.

[9] IEEE Computer Society LAN-MAN Standards Committee. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifcations. Std. 802.11, IEEE, New York, 1997.

[10] Z. Chen, A. Khokhar. Self Organization and Energy Effcient TDMA MAC Protocol by Wake Up for Wireless Sensor Networks. University of Illinois at Chicago, USA, 2004.

[11] V. Kanodia, C. Li, A. Sabharwal, B. Sadeghi, E. Knightly. Distributed Priority Scheduling and Medium Access in Ad Hoc Networks. *Wireless Networks*, 8(455-456), 2002.

[12] Z. Ying, A.L. Ananda, L. Jacob. A QoS Enabled MAC Protocol for Multi-hop Ad Hoc Wireless Networks. *Proc. IEEE Int. Conf. Perform., Comput., Commun.*, 8(149-156), Abril 2003.

[13] C.E. Parkins, P. Bhagwat. Highly Dinamic Destination-Sequenced Distance Vector Routing (DSDV) for Mobile Computers. Procedings of ICUPC 1998 Vol. 1, ICUPC, Outubro 1998.

[14] S. Wiethölter, C. Hoene. Design and Verifcation of an IEEE 802.11e EDCF Simulation Model in ns-2.26. Technical report series, Technical University Berlin, Telecommunication Networks Group.

[15] K. Fall, K. Varadhan. *The ns Manual*. UC Berkley, LBL, USC/ISI and Xerox PARC, Abril 2002.

[16] S. Keshav. REAL 5.0 Overview. Página da internet, Cornell University, Agosto 1997. `http://www.cs.cornell.edu/skeshav/real/overview.html`.

[17] . The Network Simulator ns-2: Mailing Lists. Página da internet, Maio 2005. `http://www.isi.edu/nsnam/ns/ns-lists.html`.

[18] S. Xu, T. Saadawi. Does the IEEE 802.11 MAC Protocol Work Well in Multihop Wireless Ad Hoc Networks? *IEEE Communications Magazine*, pages 130–137, Junho 2001.

[19] M.D. Yacoub. *Foundations of Mobile Radio Engineering*. CRC Press, 1993.

[20] J. Deng, B. Liang, P.K. Varshney. Tuning the carrier sensing range of IEEE 802.11 MAC. *IEEE Global Telecommunications Conference*, 5:2987–2991, 2004.

[21] ITU-T. Recommendation G.114 - One-Way Transmission Time. Recom. g.114, ITU-T, março 1996.

[22] B.P. Crow, F.I. Widjaja, J.G. Kim, P.T. Sakai. IEEE 802.11 wireless local area networks. *IEEE Communications Magazine*, 35(9):116–126, setembro 1997.

[23] ITU-T. Recommendation G.711 - Pulse Code Modulation (PCM) of Voice Frequencies. Recom. g.711, ITU-T, novembro 1988.

Apêndice A

Apêndice A

Neste apêndice são apresentados alguns códigos-fonte escritos em tcl para uso no simulador de redes ns-2.

A.1 Algoritmo de geração de tráfego VoIP

```
# VoIP Traffic Algorithm
#---------------------------------------------------------------
proc rand_start {} {
    set rng1 [new RNG]
    $rng1 seed 0
    $rng1 uniform 0 10
}

proc rand_phrase {} {
    set rng2 [new RNG]
    $rng2 seed 0
    $rng2 exponential 2
}

#Creates 16 conversations
for {set i 0} {$i < 16} {incr i} {
    puts "================================================"
    puts "Begin of conversation $i"
    puts "================================================"
    set count [rand_start]     ;#set call start time
    set m $i                   ;#set calling node
    set flag 0
    while {$flag == 0} {
```

```
#Set phrase start time
    $ns_ at $count "$cbr($m) start"
    puts "Node $m transmitting at $count"
#Set valid phrase duration
    set delta [rand_phrase]
        set count [expr $count + $delta]
    if {$count < $stoptime_} {
        $ns_ at $count "$cbr($m) stop"
    #Changes transmitting node
        if {$m == $i} {
        set m [expr int([expr $i + 16])]
        } else {
        set m $i
        }
    } else {
        set count $stoptime_
        set flag 1
        $ns_ at $count "$cbr($m) stop"
    }
    }
}
```

A.2 Exemplo de simulação: grid 7x7, tráfego VoIP

```
# Beginning of script

#===================================================================================
# Definitions
#===================================================================================
set val(chan)           Channel/WirelessChannel    ;#channel type
set val(prop)           Propagation/TwoRayGround   ;#propagation model
set val(netif)          Phy/WirelessPhy            ;#network interface type
set val(mac)            Mac/802_11_WT              ;#MAC protocol
set val(ifq)            CMUPriQueue                ;#queue type
set val(ll)             LL                         ;#link layer type
set val(ant)            Antenna/OmniAntenna        ;#antenna type
set val(ifqlen)         50e+6                      ;#max no. of packets in ifq
set val(nn)             49                         ;#number of nodes
set val(rp)             DSR                        ;#routing protocol
set val(x)              8000                       ;#x dimension
set val(y)              8000                       ;#y dimension
```

```
#===================================================================
# Main program
#===================================================================
# Global variables
#-------------------------------------------------------------------
set stoptime_ 180                          ;#simulation end time
set datarate 11e6                          ;#channel capacity


# Beginning simulation
#-------------------------------------------------------------------
set ns_         [new Simulator]
puts "stoptime=$stoptime_"
$ns_ use-newtrace                           ;#use  new trace
set tracefd [open grid_cbr.tr w]            ;#create wireless-trace
$ns_ trace-all $tracefd


# Physical layer parameters
#-------------------------------------------------------------------
Phy/WirelessPhy set RXThresh_ 3.65262e-10 ;#transmission range 250m
Phy/WirelessPhy set CSThresh_ 1.76149e-10 ;#interference range 300m
Phy/WirelessPhy set Pt_ 0.281838          ;#transmission power
Phy/WirelessPhy set freq_ 2.4e+9          ;#frequency
Phy/WirelessPhy set L_ 1.0                ;#system loss


# Mac layer parameters
#-------------------------------------------------------------------
Mac/802_11_WT set dataRate_ $datarate
Mac/802_11_WT set PLCPDataRate_ 1Mb;
Mac/802_11_WT set RTSThreshold_ 0;

# Setup topography
#-------------------------------------------------------------------
set topo [new Topography]
$topo load_flatgrid $val(x) $val(y)       ;#simulation area (m x m)

# Criar GOD
#-------------------------------------------------------------------
 create-god $val(nn)
```

```
# Setup nodes
#-------------------------------------------------------------------------------
$ns_ node-config  \
    -adhocRouting $val(rp) \
    -llType $val(ll) \
    -macType $val(mac) \
    -ifqType $val(ifq) \
    -ifqLen $val(ifqlen) \
    -antType $val(ant) \
    -propType $val(prop) \
    -phyType $val(netif) \
    -topoInstance $topo \
    -agentTrace ON \
    -routerTrace OFF \
    -macTrace OFF \
    -movementTrace OFF \
    -channel [new $val(chan)]

# Create nodes - 7x7 square grid
#-------------------------------------------------------------------------------
set n 0
for {set i 1} {$i < 8} {incr i} {
    for {set j 1} {$j < 8} {incr j} {
        set node_($n) [$ns_ node]
        set xpos [expr $i * 200]            ;#grid step 200m
        set ypos  [expr $j * 200]
        $node_($n) set X_ $xpos
        $node_($n) set Y_ $ypos
        $node_($n) set Z_ 0
        $node_($n) random-motion 0          ;#disable random motion
        $ns_ at 0 "$node_($n) setdest $xpos $ypos 0.0"
        incr n
    }
}

# Setup traffic
#-------------------------------------------------------------------------------
Agent/UDP set packetSize_ 256

for {set i 0} {$i < 32} {incr i} {
    set udp($i) [new Agent/UDP]
    $udp($i) set class_ 1
```

```
    $udp($i) set fid_ $i
    set cbr($i) [new Application/Traffic/CBR]
    $cbr($i) set packetSize_ 160
    $cbr($i) set random_ false
    $cbr($i) set rate_ 64e+3                    ;#bit rate
    $cbr($i) attach-agent $udp($i)
}

#Uplink
$ns_ attach-agent $node_(0) $udp(0)
$ns_ attach-agent $node_(2) $udp(1)
$ns_ attach-agent $node_(4) $udp(2)
$ns_ attach-agent $node_(13) $udp(3)
$ns_ attach-agent $node_(17) $udp(4)
$ns_ attach-agent $node_(18) $udp(5)
$ns_ attach-agent $node_(19) $udp(6)
$ns_ attach-agent $node_(21) $udp(7)
$ns_ attach-agent $node_(23) $udp(8)
$ns_ attach-agent $node_(29) $udp(9)
$ns_ attach-agent $node_(32) $udp(10)
$ns_ attach-agent $node_(34) $udp(11)
$ns_ attach-agent $node_(39) $udp(12)
$ns_ attach-agent $node_(42) $udp(13)
$ns_ attach-agent $node_(45) $udp(14)
$ns_ attach-agent $node_(48) $udp(15)

#Downlink
$ns_ attach-agent $node_(24) $udp(16)
$ns_ attach-agent $node_(24) $udp(17)
$ns_ attach-agent $node_(24) $udp(18)
$ns_ attach-agent $node_(24) $udp(19)
$ns_ attach-agent $node_(24) $udp(20)
$ns_ attach-agent $node_(24) $udp(21)
$ns_ attach-agent $node_(24) $udp(22)
$ns_ attach-agent $node_(24) $udp(23)
$ns_ attach-agent $node_(24) $udp(24)
$ns_ attach-agent $node_(24) $udp(25)
$ns_ attach-agent $node_(24) $udp(26)
$ns_ attach-agent $node_(24) $udp(27)
$ns_ attach-agent $node_(24) $udp(28)
$ns_ attach-agent $node_(24) $udp(29)
$ns_ attach-agent $node_(24) $udp(30)
$ns_ attach-agent $node_(24) $udp(31)
```

```
for {set i 0} {$i < 32} {incr i} {
    set sink($i) [new Agent/Null]
}

#Uplink
$ns_ attach-agent $node_(24) $sink(0)
$ns_ attach-agent $node_(24) $sink(1)
$ns_ attach-agent $node_(24) $sink(2)
$ns_ attach-agent $node_(24) $sink(3)
$ns_ attach-agent $node_(24) $sink(4)
$ns_ attach-agent $node_(24) $sink(5)
$ns_ attach-agent $node_(24) $sink(6)
$ns_ attach-agent $node_(24) $sink(7)
$ns_ attach-agent $node_(24) $sink(8)
$ns_ attach-agent $node_(24) $sink(9)
$ns_ attach-agent $node_(24) $sink(10)
$ns_ attach-agent $node_(24) $sink(11)
$ns_ attach-agent $node_(24) $sink(12)
$ns_ attach-agent $node_(24) $sink(13)
$ns_ attach-agent $node_(24) $sink(14)
$ns_ attach-agent $node_(24) $sink(15)

#Downlink
$ns_ attach-agent $node_(0) $sink(16)
$ns_ attach-agent $node_(2) $sink(17)
$ns_ attach-agent $node_(4) $sink(18)
$ns_ attach-agent $node_(13) $sink(19)
$ns_ attach-agent $node_(17) $sink(20)
$ns_ attach-agent $node_(18) $sink(21)
$ns_ attach-agent $node_(19) $sink(22)
$ns_ attach-agent $node_(21) $sink(23)
$ns_ attach-agent $node_(23) $sink(24)
$ns_ attach-agent $node_(29) $sink(25)
$ns_ attach-agent $node_(32) $sink(26)
$ns_ attach-agent $node_(34) $sink(27)
$ns_ attach-agent $node_(39) $sink(28)
$ns_ attach-agent $node_(42) $sink(29)
$ns_ attach-agent $node_(45) $sink(30)
$ns_ attach-agent $node_(48) $sink(31)

for {set i 0} {$i < 32} {incr i} {
    $ns_ connect $udp($i) $sink($i)
```

```
}

# VoIP Traffic Algorithm
#---------------------------------------------------------------------------
proc rand_start {} {
    set rng1 [new RNG]
    $rng1 seed 0
    $rng1 uniform 0 10
}

proc rand_phrase {} {
    set rng2 [new RNG]
    $rng2 seed 0
    $rng2 exponential 2
}

#Creates 16 conversations
for {set i 0} {$i < 16} {incr i} {
    puts "================================================"
    puts "Begin of conversation $i"
    puts "================================================"
    set count [rand_start]    ;#set call start time
    set m $i                  ;#set calling node
    set flag 0
    while {$flag == 0} {
#Set phrase start time
        $ns_ at $count "$cbr($m) start"
        puts "Node $m transmitting at $count"
#Set valid phrase duration
        set delta [rand_phrase]
        set count [expr $count + $delta]
        if {$count < $stoptime_} {
            $ns_ at $count "$cbr($m) stop"
        #Changes transmitting node
            if {$m == $i} {
                set m [expr int([expr $i + 16])]
            } else {
                set m $i
            }
        } else {
            set count $stoptime_
            set flag 1
            $ns_ at $count "$cbr($m) stop"
```

```
        }
    }
}


# Simulation end time
#-------------------------------------------------------------------------
$ns_ at $stoptime_ "finish"
$ns_ at [expr $stoptime_ + 0.0001] "puts \"NS STOPPING...\" ; $ns_ halt"
proc finish {} {
    global ns_ tracefd
    $ns_ flush-trace
    close $tracefd
}

puts "NS Starting ..."
$ns_ run

#### End of script #############
```