DIFERENCIAÇÃO DE TRÁFEGO E CONTROLE DE ADMISSÃO
EM REDES AD HOC IEEE 802.11

Carlos Rodrigo Cerveira

DISSERTAÇÃO SUBMETIDA AO CORPO DOCENTE DA COORDENAÇÃO DOS PROGRAMAS DE PÓS-GRADUAÇÃO DE ENGENHARIA DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE EM CIÊNCIAS EM ENGENHARIA ELÉTRICA.

Aprovada por:

Prof. Luís Henrique Maciel Kosmalski Costa, Dr.

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

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

RIO DE JANEIRO, RJ - BRASIL

MARÇO DE 2007

CERVEIRA, CARLOS RODRIGO

Diferenciação de Tráfego e Controle de Admissão em Redes Ad Hoc IEEE 802.11 [Rio de Janeiro] 2007

XV, 81 p. 29,7 cm (COPPE/UFRJ, M.Sc., Engenharia Elétrica, 2007)

Dissertação - Universidade Federal do Rio de Janeiro, COPPE

1. Redes sem fio Ad Hoc

2. Qualidade de Serviço

3. Mobilidade

I. COPPE/UFRJ II. Título (série)

À minha esposa e filha, pela compreensão e carinho prestados enquanto me dediquei a este trabalho.

Agradecimentos

A Deus, por ter me dado oportunidade para iniciar e saúde para concluir este trabalho.

À minha família, principalmente a minha esposa Márcia e minha filha Helena por todo o amor, incentivo e compreensão, aos meus pais, por toda orientação, dedicação e apoio ao longo da minha vida.

Ao meu orientador Luís Henrique por toda a amizade, confiança e orientação, além de sempre estar presente, para dar conselhos e ajudar a superar todos os obstáculos.

A toda a equipe do GTA, em particular aos amigos, Henrique, Marcel, Igor, Miguel, Kleber, Ítalo pela amizade e pela boa convivência durante toda a dissertação.

Ao professor José Rezende por toda a ajuda, em especial no início do mestrado.

Aos professores Otto e Célio pela presença na banca examinadora.

À Marinha do Brasil pela liberação em tempo integral para o desenvolvimento deste trabalho e pelo estímulo ao constante aperfeiçoamento de seus profissionais.

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

DIFERENCIAÇÃO DE TRÁFEGO E CONTROLE DE ADMISSÃO
EM REDES AD HOC IEEE 802.11

Carlos Rodrigo Cerveira

Março/2007

Orientador: Luís Henrique Maciel Kosmalski Costa
Programa: Engenharia Elétrica

Neste trabalho é proposto um mecanismo que integra diferenciação de tráfego e controle de admissão para prover Qualidade de Serviço (QoS) em redes ad hoc IEEE 802.11. No mecanismo proposto, os fluxos das aplicações que possuem requisitos de Qualidade de Serviço, antes de serem admitidas na rede, passam pelo módulo do controle de admissão e só serão aceitas caso os recursos disponíveis sejam suficientes para atender a carga requisitada e não venham a interferir nos fluxos das aplicações do tipo QoS pré-existentes. O controle de admissão utiliza o período de tempo em que o meio permanece ocioso como estimativa dos recursos disponíveis e faz um cálculo da interferência intra-fluxo, o que permite maior precisão nos cálculos efetuados pelo controle de admissão para decidir a aceitação de um novo fluxo. Os fluxos das aplicações do tipo melhor-esforço (BE) possuem requisitos bem mais flexíveis do que as aplicações do tipo QoS, portanto as aplicações do tipo BE não passam pelo controle de admissão e são injetadas diretamente na rede. O acesso ao meio dos fluxos do tipo BE é controlado pelo protocolo padrão IEEE 802.11e, de forma a não degradar o desempenho das aplicações do tipo QoS. O mecanismo proposto é comparado ao SWAN, outro mecanismo proposto na literatura, e os resultados das simulações mostram ganhos de até 35% em termos de taxa de entrega e até 10 vezes em atraso fim-a-fim.

Abstract of Dissertation presented to COPPE/UFRJ as a partial fulfillment of the requirements for the degree of Master of Science (M.Sc.)

TRAFFIC DIFFERENTIATION AND ADMISSION CONTROL
FOR IEEE 802.11 AD HOC NETWORKS

Carlos Rodrigo Cerveira

March/2007

Advisor: Luís Henrique Maciel Kosmalski Costa

Department: Electrical Engineering

The aim of this work is to develop an integrated mechanism for traffic differentiation and admission control to provide Quality of Service (QoS) on IEEE 802.11 ad hoc networks. In the proposed mechanism, the incoming QoS traffic passes by the admission control component, and new flows will be accepted, in case there is enough resources to fulfill the request and not to havoc the pre-existing flows. The admission control uses the idle channel time to estimate the available resources and computes the intra-flow contention when it needs to decide on accepting or rejecting a new incoming flow. Best-Effort (BE) traffic requirements are more flexible than QoS traffic, therefore BE traffic don't passes by the admission control component, and are injected directly at the network. The standard protocol IEEE 802.11e is used to control the medium access of the BE traffic. The proposed mechanism is compared to SWAN, another service-differentiation mechanism found in the literature, and simulation results show performance gains of 35% on the packet delivery rate and up to 10 times on end-to-end delay.

Sumário

Resumo **v**

Abstract **vi**

Lista de figuras **x**

Lista de tabelas **xiii**

Lista de acrônimos **xiv**

1 Introdução **1**

1.1 Motivação 1

1.2 Trabalhos relacionados 3

1.3 Objetivos 4

2 As Redes IEEE 802.11 **7**

2.1 Camada Física 9

2.1.1 Subcamada de Convergência Física 10

2.1.2 Subcamada Dependente do Meio Físico 13

2.2 Subcamada de Controle de Acesso ao Meio 13

2.2.1 Função de Coordenação Distribuída 14

2.3 Efeitos da Detecção de Portadora na Qualidade de Serviço 17

2.4 Qualidade de Serviço no IEEE 802.11 19

3 Controle de Admissão **22**

3.1 Visão geral do protocolo AODV 23

3.1.1 Modificações do protocolo AODV 24

3.2 Controle de Admissão 25

3.2.1 TAC-AODV 26

3.2.1.1 Cálculo dos recursos disponíveis no TAC-AODV 26

3.2.1.2 Cálculo da interferência intra-fluxo no TAC-AODV . . 27

3.2.1.3 Estimativa dos recursos consumidos por um novo fluxo no TAC-AODV 28

3.2.2 TDAC-AODV 30

3.2.3 Cálculo dos recursos disponíveis no TDAC-AODV 31

3.3 Cálculo da interferência intra-fluxo no TDAC-AODV 36

3.4 Operação do Controle de Admissão do TDAC-AODV 39

3.4.1 Cálculos efetuados pelo Controle de Admissão do TDAC-AODV 40

3.5 Violação de QoS 42

3.5.1 Implementação do Controle de Violação de QoS no TDAC-AODV 45

4 Diferenciação de Tráfego **47**

4.1 IEEE 802.11e 47

5 Simulações **52**

5.1 Modificações realizadas no NS-2 53

5.2 Avaliação 53

5.3 SWAN (*Stateless Wireless Ad Hoc Networks*) 54

5.3.1 Controle de Taxa dos Fluxos BE 54

5.3.2 Controle de Admissão dos Fluxos QoS 55

5.4 Métricas 55

5.5 Considerações Iniciais 57

5.6 Primeira fase das simulações 59

5.7 Resultados da segunda fase das simulações 70

5.8 Resultados da terceira fase das simulações 72

6 Conclusões **76**

Referências Bibliográficas **78**

Lista de Figuras

2.1 Arquitetura de uma rede infra-estruturada. 8

2.2 Exemplo de uma BSS independente. 9

2.3 Exemplo de uma rede ad hoc de múltiplos saltos. 10

2.4 Formato da PPDU longa. 11

2.5 Formato da PPDU curta. 12

2.6 O esquema básico de acesso no mecanismo distribuído. 15

2.7 O problema do terminal escondido. 16

2.8 O mecanismo de acesso ao meio distribuído com RTS e CTS. 16

2.9 Estimativa de recursos disponíveis de um nó. 18

2.10 Interferência intra-fluxo. 19

3.1 *backoff* médio. 27

3.2 Armazenamento das mensagens *Hello* 33

3.3 O nó E está dentro do alcance-CS do nó A mas está escondido para o mesmo. 34

3.4 O círculo pontilhado representa o alcance-TX e o círculo cheio o alcance-CS do nó A. 34

3.5 O nó E está fora do alcance-CS do nó A 36

3.6 Cadeia de Encaminhamento de um fluxo de 9 saltos 37

3.7 Mecanismo implementado na camada de rede. 43

3.8 Violação de QoS por mobilidade. 44

4.1 Camada MAC do IEEE 802.11e. Figura adaptada de [1] 48

4.2 Relações dos intervalos entre-quadros no IEEE 802.11e. 50

5.1 Taxa de Entrega. 61

5.2 Taxa de Entrega do TDAC e TDAC-mod. 62

5.3 Pacotes descartados na camada MAC e fila de transmissão da camada MAC devido a colisões. 63

5.4 Pacotes descartados na camada MAC por transbordo de fila. 63

5.5 Pacotes descartados na camada de rede. 64

5.6 Atraso fim-a-fim. 64

5.7 Atraso fim-a-fim do TDAC e TDAC-mod. 65

5.8 Taxa de Entrega com inibição de quebra de rota. 66

5.9 Atraso fim-a-fim com inibição de quebra de rota. 66

5.10 Taxa de sobrecarga. 67

5.11 Vazão Agregada dos Fluxos QoS. 68

5.12 Vazão Agregada dos Fluxos BE. 68

5.13 Vazão média dos Fluxos QoS. 69

5.14 Vazão média dos Fluxos QoS sem quebra de rota. 70

5.15 Taxa de Entrega. 71

5.16 Atraso fim-a-fim. 71

5.17 Vazão Agregada dos Fluxos QoS. 72

5.18 Vazão média dos Fluxos QoS. 72

5.19 Vazão média dos Fluxos QoS sem quebra de rota. 73

5.20 Cenário com mobilidade. 73

5.21 Vazão dos Fluxos sem o mecanismo de controle de violação de QoS. . . . 74

5.22 Vazão dos Fluxos com o mecanismo de controle de violação de QoS. . . . 75

Lista de Tabelas

3.1 Pacotes/Quadros incluídos no cálculo de T_o durante uma transmissão entre o nó fonte A e o nó destino B. 31

4.1 Tipos de tráfegos e *ACs* associadas. 49

4.2 Valores de CW_{min}, CW_{max}, $AIFSN$ e $TXOPLimit$ utilizados pelas ACs. 51

5.1 Parâmetros da simulação primeira fase. 60

5.2 Configuração dos mecanismos avaliados. 61

Lista de acrônimos

Alcance-TX : *A*lcance de transmissão;

Alcance-CS : *Alcance de detecção da portadora*;

AODV : *Ad hoc On-demand Distance Vector*;

BSS : *Basic Service Set*;

BE : *Best-Effort*;

CC : *Contention Count*;

CCK : *Complementary Code Keying*;

CRC : *Cyclic Redundant Check*;

CSMA/CA : *Carrier Sense Multiple Access and Collision Avoidance*;

CSMA/CD : *Carrier Sense Multiple Access and Collision Detection*;

CTS : *Clear to Send*;

CW : *Contention Window*;

DBPSK : *Differential Binary Phase Shift Keying*;

DCF : *Distributed Coordination Function*;

DIFS : *DCF InterFrame Space*;

DQPSK : *Differential Quadrature Phase Shift Keying*;

DSDV : *Destination-Sequenced Distance Vector*;

DSR : *Dynamic Source Routing*;

DSSS : *Direct Sequence Spread Spectrum*;

EIFS : *Extended InterFrame Space*;

FCS : *Frame Check Sequence*;

FHSS : *Frequency Hopping Spread Spectrum*;

HR/DSSS : *High Rate Direct Sequence Spread Spectrum*;

IBSS : *Independent Basic Service Set*;

IEEE : *Institute of Electrical and Electronics Engineers*;

IP : *Internet Protocol*;

MAC : *Medium Access Control*;

MPDU : *MAC Protocol Data Unit*;

NAV : *Network Allocation Vector*;

ns : *Network Simulator*;

OLSR : *Optimized Link State Routing*;

PBCC : *Packet Binary Convolutional Coding*;

PCF : *Point Coordination Function*;

PLCP : *Physical Layer Convergence Procedure*;

PMD : *Physical Medium Dependent*;

PPDU : *PLCP Protocol Data Unit*;

PSDU : *PLCP Service Data Unit*;

QoS : *Quality of Service*;

QPSK : *Quadrature Phase Shift Keying*;

RREP : *Route Reply*;

RREQ : *Route Request*;

RTS : *Request to Send*;

SFD : *Start Frame Delimiter*;

SIFS : *Short InterFrame Space*.

Capítulo 1

Introdução

O rápido crescimento no número de usuários de dispositivos de comunicação sem fio que utilizam interfaces de rede IEEE 802.11 [2] tem atraído em muito a atenção da comunidade científica. As redes sem fio permitem a mobilidade, proporcionando uma maior flexibilidade. Além disso, a ausência de fios permite uma redução no tempo e custo da instalação de uma rede assim como sua utilização em regiões onde seria inviável a instalação de redes cabeadas, como por exemplo em cenários militares ou de resgate.

1.1 Motivação

As redes sem fio podem ser divididas em dois tipos: redes com infra-estrutura e redes ad hoc. No primeiro tipo, toda comunicação ocorre entre os nós usuários e um ponto de acesso. Este ponto de acesso é um elemento centralizador que também pode servir como ponte para outras redes sem fio ou cabeadas. Já nas redes ad hoc, estudadas neste trabalho, não se precisa de nenhuma infra-estrutura prévia, os nós se comunicam diretamente uns com os outros. Se o nó de destino não estiver no raio de alcance de transmissão do nó fonte, ainda assim pode-se ter uma comunicação entre eles, com o uso dos nós intermediários propagando os pacotes até o destino. Desta forma, os nós pertencentes a uma rede ad hoc são clientes e roteadores e devem cooperar uns com os outros, a fim de prover o roteamento em uma rede ad hoc.

Uma grande vantagem das redes ad hoc é sua flexibilidade. Em áreas onde existe pouca ou nenhum tipo de infra-estrutura de comunicação ou ainda, onde a instalação desta infra-estrutura seria muito cara, mesmo assim seria possível que usuários de rede sem fio pudessem se comunicar através da formação de uma rede ad hoc. Assim, são inúmeras as aplicações para redes ad hoc: operações militares, reuniões não planejadas, situações de emergência como enchentes, terremotos ou furacões (quando a infra-estrutura pára de funcionar), etc.

Em contraste com as tradicionais redes cabeadas, as redes ad hoc sem fio possuem como características importantes o suporte a mobilidade, o compartilhamento do meio e a descentralização. A natureza dinâmica da topologia, devido à mobilidade, faz com que ocorram quebras de rotas tornando imprecisa a informação do estado da rede. Além disso, não existe garantias que os recursos permanecerão disponíveis. A largura de banda disponível pode diminuir, por exemplo, no caso de dois nós pertecentes a fluxos distintos se aproximarem, causando interferência mútua. O compartilhamento do meio faz com que uma estação tenha que disputar os recursos da rede com outras estações. Ainda deve-se levar em conta que, a alocação de recursos a uma determinada estação, afeta os recursos disponíveis de todas as outras estações que disputam o meio. Por fim, a descentralização faz com que seja difícil estabelecer uma seqüência de transmissão entre as estações com o objetivo de garantir taxa de entrega de pacotes constante. Estas características tornam a provisão de garantias de Qualidade de Serviço (*Quality of Service* - QoS), em uma rede ad hoc, um problema complexo.

A utilização em redes ad hoc de aplicações multimídias (VoIP, Vídeo-Conferência, *Chat*) que exigem garantias de QoS em termos de largura de banda, atraso e variação de atraso (*jitter*), tem sido tema de muitos trabalhos [3, 4, 5, 6, 7, 8, 9].

Diferentes tecnologias foram propostas e implementadas que dão suporte à construção de redes ad hoc. Uma das tecnologias que vem obtendo grande êxito comercial é o padrão IEEE 802.11, que define um conjunto de normas para redes locais sem fio. As principais vantagens do IEEE 802.11 são: o baixo custo dos dispositivos de rede e a grande flexibilidade, pois pode ser utilizado tanto para redes com infra-estrutura como para redes ad hoc. O IEEE 802.11 possui atualmente crescente sucesso comercial. Desta forma, a análise

realizada nesta dissertação se concentra no padrão IEEE 802.11.

1.2 Trabalhos relacionados

A pesquisa na área de QoS em redes ad hoc abrange diversos tópicos que incluem roteamento com QoS [10, 11], modelos de QoS [12], sinalização [13], QoS na subcamada de controle de acesso ao meio [7, 8] e controle de admissão [3, 4, 5, 6]. Bharghavan *et al.* [10] propuseram um protocolo de roteamento (*Core-Extraction Distributed Ad hoc Routing* - CEDAR) capaz de prover QoS em redes ad hoc. O CEDAR é baseado na eleição de líderes responsáveis por realizar o roteamento e anunciar os enlaces mais estáveis para os nós mais distantes e os enlaces menos estáveis ou de menor capacidade para os nós mais próximos. O núcleo da rede é formado pelos nós líderes que devem executar um algoritmo para descoberta de uma rota que satisfaça a banda passante requerida. No CEDAR, assume-se que a largura de banda disponível é conhecida e o seu cálculo não é investigado. Ge *et al.* [11] propuseram uma extensão com QoS ao protocolo de roteamento OLSR (*Optimized Link State Routing*) [14], onde o objetivo do mecanismo é encontrar a rota com maior largura de banda disponível. Nesta proposta a mobilidade dos nós não foi considerada. Xiao *et al.* [12] propuseram um modelo flexível de QoS para redes móveis ad hoc (*Flexible QoS Model for Mobile Ad Hoc Networks* - FQMM), que combina os modelos DiffServ (*Differentiated Services*) e IntServ (*Integrated Services*). O tráfego de maior prioridade recebe a provisão de QoS por fluxo (IntServ) e o tráfego menos prioritário recebe provisão de QoS por classe (DiffServ). Na solução proposta no FQMM, as características inerentes das redes ad hoc, como o suporte a mobilidade e o compartilhamento do meio, não foram consideradas. O INSIGNIA, proposto por Campbell *et al.* [13], é um protocolo de sinalização que provê suporte a QoS em redes ad hoc. Nesse modelo, em caso dos recursos disponíveis não serem mais suficientes para atender a requisição da aplicação, os tráfegos não são interrompidos ocasionando desperdícios de recursos e energia.

No padrão IEEE 802.11e [8] os fluxos são agrupados em diferentes categorias de acesso ao meio (*Access Category* - AC) que possuem prioridades de transmissão diferen-

tes. São atribuídos diferentes valores de AIFS (*Arbitration Inter-Frame Space*) e janelas de contenção (*Contention Window* - CW) para as diferentes categorias, provendo uma diferenciação de serviço na camada MAC (*Medium Access Control*). O IEEE 802.11e pode prover diferenciação de serviço entre tráfegos, porém não pode garantir que um determinado nível de serviço seja atendido, já que não existe nenhum tipo de controle na admissão de fluxos nem reserva de recursos. Kravets e Yang [4] propuseram um controle de admissão (*Contention-Aware Admission Control for Ad Hoc Networks* - CACP) para redes ad hoc. O mecanismo proposto no CACP não provê nenhuma estratégia para controlar a perda de garantias de QoS devido à mobilidade dos nós. Chakeres e Belding-Royer também propuseram um controle de admissão (*Perceptive Admission Control for Mobile Wireless Networks* - PAC). Nos cálculos efetuados pelo controle de admissão do PAC, não são considerados os efeitos da interferência intra-fluxo. Tanto no CACP quanto no PAC não é realizada diferenciação de serviço, todos os fluxos têm a mesma prioridade. O SWAN (*Stateless Wireless Ad Hoc Networks*) [3] utiliza um algoritmo de controle distribuído com o objetivo de prover diferenciação de serviços em uma rede ad hoc. O SWAN implementa um controle de admissão para os fluxos com requisitos de QoS e um controle de taxa de transmissão para gerenciar os fluxos de melhor esforço (*Best-Effort* - BE). O objetivo do controle de taxa é evitar que os fluxos BE degradem o desempenho dos fluxos de QoS. O SWAN não considera modificações na camada MAC, como a nova funcionalidade de QoS criada pela extensão IEEE 802.11e. Os cálculos realizados pelo o controle de admissão do SWAN não levam em conta a largura de banda consumida pelos nós situados entre o alcance de transmissão e o alcance de detecção da portadora e ainda, o efeito da interferência intra-fluxo. Maiores detalhes de sua implementação serão descritas no Capítulo 5.

1.3 Objetivos

O principal objetivo deste trabalho é implementar um mecanismo que seja capaz de prover garantias de QoS em redes ad hoc IEEE 802.11 em cenários estáticos ou de baixa mobilidade. Em cenários onde a topologia da rede muda rapidamente, a informação de estado da rede está constantemente desatualizada, tornando-se muito difícil prover garan-

tias de QoS. Além disso, consideram-se aplicações que suportam uma perda temporária no atendimento aos seus requisitos de QoS. Por exemplo, a perda de alguns quadros em um fluxo de vídeo, devido à quebra de rotas ocasionadas pela mobilidade dos nós, não é suficiente para comprometer a percepção do usuário com relação ao conteúdo da informação audiovisual. Em contrapartida, enquanto as rotas permanecerem estabelecidas e a capacidade do canal não sofrer mudanças drásticas, o mecanismo tem de garantir o atendimento aos requisitos de QoS das aplicações. Se os requisitos mínimos não puderem ser satisfeitos, os dados transmitidos não serão aproveitados e assim, serão desperdiçados recursos da rede e energia dos nós. Nestes casos, a transmissão dos fluxos não deveria ser iniciada. Na primeira parte deste trabalho é proposto um controle de admissão (*Time-based Admission Control* - TAC-AODV) [15], o qual é baseado em uma precisa estimativa dos recursos disponíveis e na interferência intra-fluxo para decidir se admite ou não novos fluxos que exigem requisitos de QoS. Adaptamos o controle de admissão ao protocolo de roteamento AODV (*Ad-hoc On-Demand Distance Vector Routing*) [16], um dos protocolos ad hoc mais conhecidos. Em seguida foram feitas profundas modificações nos cálculos realizados pelo controle de admissão do TAC-AODV para permitir o seu funcionamento em redes, onde operam tanto aplicações que possuem requisitos de QoS quanto aplicações do tipo BE. Para suportar ambos os tipos de aplicações em redes ad hoc, é necessário prover garantia de QoS ao tráfego de tempo real. O mecanismo proposto foi batizado de TDAC-AODV (*Traffic Differentiation and Admission Control* - AODV).

Para prover QoS, o TDAC-AODV possui três componentes essenciais [17]. Primeiro, o controle de admissão que é feito na camada de rede, com o objetivo de impedir a entrada de novos fluxos QoS que venham a congestionar a rede e deteriorar o desempenho dos fluxos QoS pré-existentes. Segundo, o mecanismo realiza diferenciação de tráfego na camada MAC com o objetivo de prover garantias para os tráfego de QoS na presença de tráfegos do tipo BE. O protocolo padrão IEEE 802.11e [18] foi escolhido para efetuar esta diferenciação. O terceiro componente está relacionado a como o mecanismo proposto reage a violações de QoS, devido principalmente à mobilidade dos nós ou à degradação da capacidade do meio. Neste sentido, o TDAC-AODV utiliza mensagens ICMP (*Internet Control Message Protocol*) para sinalização de perda de QoS.

A avaliação do mecanismo foi realizada através de simulações sendo dividida em

três partes. Na primeira e na segunda partes é analisado o caso de redes ad hoc sem mobilidade, sendo as fases diferenciadas pelo tráfego oferecido à rede. Na terceira parte, é analisada a eficiência do mecanismo de controle de violação de QoS proposto no TDAC-AODV em cenários com mobilidade.

Este trabalho está organizado da seguinte forma. O Capítulo 2 descreve as principais características do padrão IEEE 802.11. O Capítulo 3 descreve o funcionamento do controle de admissão e as modificações implementadas no protocolo AODV. O Capítulo 4 descreve as técnicas utilizadas pelo protocolo IEEE 802.11e para realizar a diferenciação de serviço entre tráfegos. O Capítulo 5 detalha as simulações realizadas. Por fim, o Capítulo 6 conclui este trabalho e apresenta direções para trabalhos futuros.

Capítulo 2

As Redes IEEE 802.11

O padrão IEEE 802.11 [2] especifica a subcamada de controle de acesso ao meio (*Medium Access Control* - MAC) da camada enlace assim como diferentes camadas físicas. Este capítulo descreve as principais características da camada física, os métodos de acesso ao meio e a provisão de qualidade de serviço no IEEE 802.11.

O IEEE 802.11 prevê dois modos de operação: infra-estruturado e ad hoc. No modo infra-estruturado, as estações se comunicam através de um dispositivo centralizador, chamado de ponto de acesso. Um nó, ainda que se encontre próximo a outro nó, não se comunica diretamente com este outro, mas tem de efetuar a comunicação através de um ou mais pontos de acesso. Desta forma, a rede, ou *Basic Service Set* - BSS, é limitada à região no alcance do ponto de acesso. Os pontos de acesso podem ser interconectados, através de um sistema de distribuição. As redes infra-estruturadas possuem maior simplicidade que as redes ad hoc, já que o ponto de acesso concentra a maior parte da funcionalidade da rede, deixando os clientes sem fio bastante simples. O ponto de acesso é responsável por exemplo pelo controle de acesso ao meio e por achar uma caminho até o destino. A arquitetura de uma rede infra-estruturada pode ser vista na Figura 2.1.

As redes ad hoc, por outro lado, não possuem nenhum elemento centralizador, as estações se comunicam diretamente umas com as outras. Numa configuração ad hoc, uma rede, ou *independent BSS* - IBSS, pode ser composta simplesmente por duas estações em alcance mútuo. A Figura 2.2 mostra uma IBSS composta por três nós. As circunferências

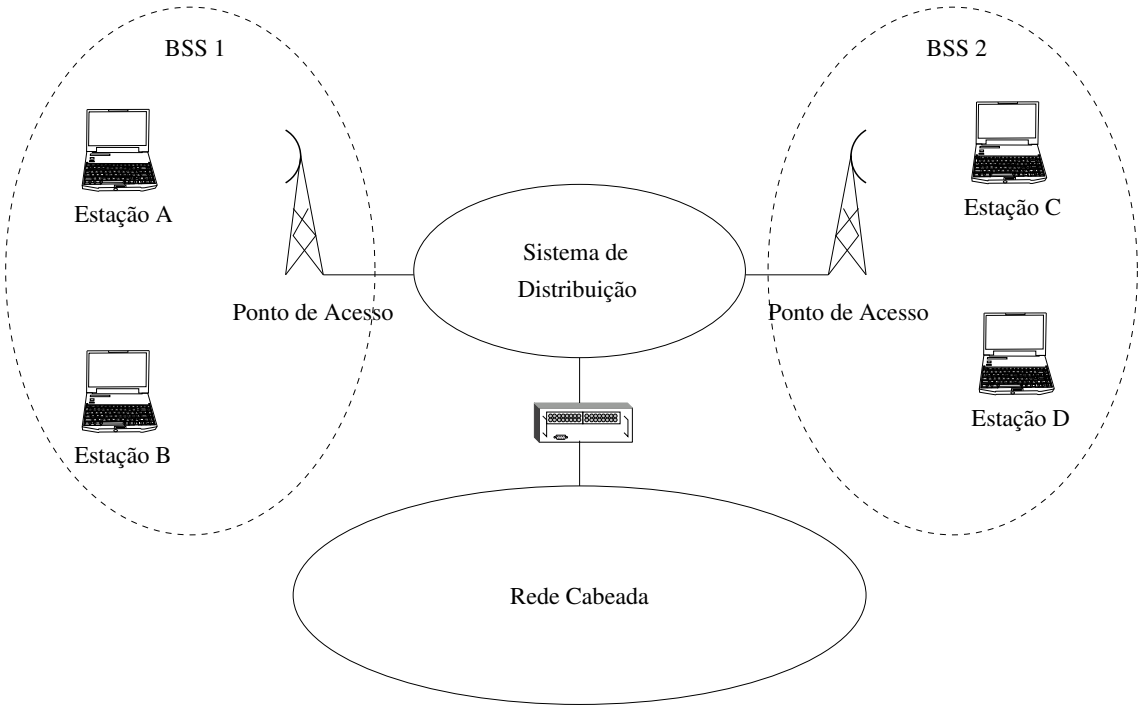


Figura 2.1: Arquitetura de uma rede infra-estruturada.

pontilhadas representam os alcances das estações localizadas nos seus respectivos centros.

Caso as estações fonte e destino não estejam no alcance, elas ainda assim podem se comunicar, utilizando transmissões em múltiplos saltos. Portanto, deve haver outros nós móveis ou não dispostos a cooperar na comunicação, formando uma rota que permita à fonte alcançar o destino. Assim, na Figura 2.3, a estação A é capaz de se comunicar com a estação C, fazendo uso da estação B. A complexidade de redes ad hoc é maior, já que cada nó precisa implementar o controle de acesso ao meio e também o roteamento de pacotes.

O padrão IEEE 802.11 define duas camadas físicas com taxas de transmissão de dados iguais a 1 e 2 Mbps na banda de 2,4 GHz. Posteriormente, foram lançadas extensões ao padrão original. A extensão conhecida como IEEE 802.11b [19] possibilita a transmissão de dados a 1, 2, 5,5 e 11 Mbps na mesma banda de 2,4 GHz. A segunda extensão desenvolvida ficou conhecida como IEEE 802.11a [20] e possibilita a transmissão de dados a até 54 Mbps na banda de 5 GHz, não sendo, portanto, compatível com dispositivos que trabalham na banda de 2,4 GHz. Já o IEEE 802.11g [21] possibilita a transmissão

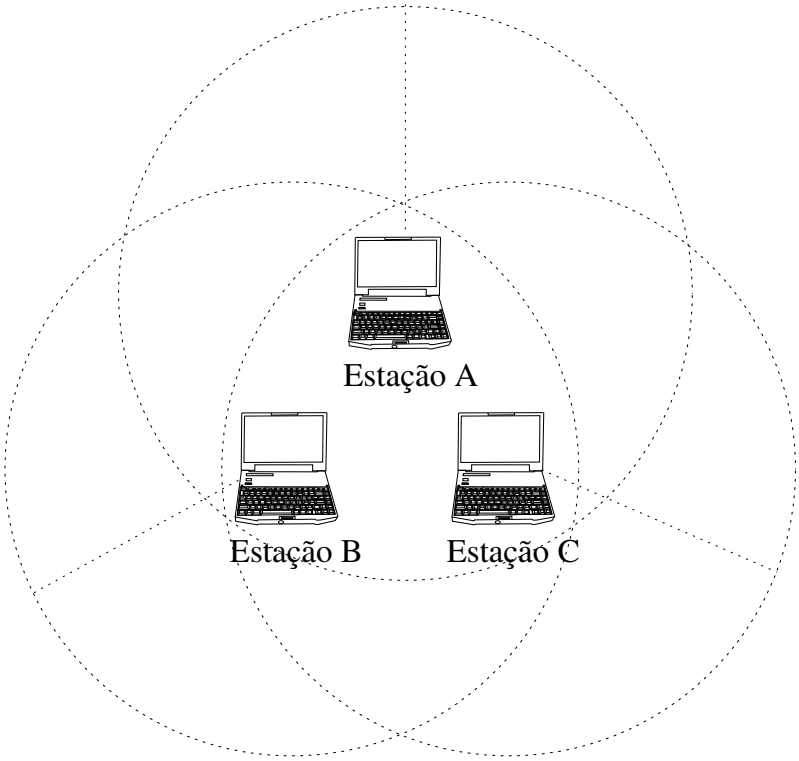


Figura 2.2: Exemplo de uma BSS independente.

de dados a 54 Mbps na banda de 2,4 GHz, permitindo assim, a compatibilidade com equipamentos mais antigos (802.11 e 802.11b).

2.1 Camada Física

O padrão IEEE 802.11 original define três possíveis técnicas de transmissão: transmissão por infra-vermelho, espalhamento de espectro por salto de freqüência (*Frequency-Hoping Spread Spectrum* - FHSS) e espalhamento de espectro por seqüência direta (*Direct Sequence Spread Spectrum* - DSSS). A camada física do IEEE 802.11 define um sinal de avaliação de canal livre (*Clear Channel Assessment* - CCA) que é utilizado pela subcamada de acesso ao meio (Seção 2.2) para verificar se o meio está ocioso ou ocupado.

O protocolo da camada física é dividido em Protocolo da Subcamada Dependente do Meio Físico (*Physical Medium Dependent* - PMD) e Protocolo da Subcamada de Convergência Física (*Physical Layer Convergence Protocol* - PLCP). Os detalhes mais relevantes

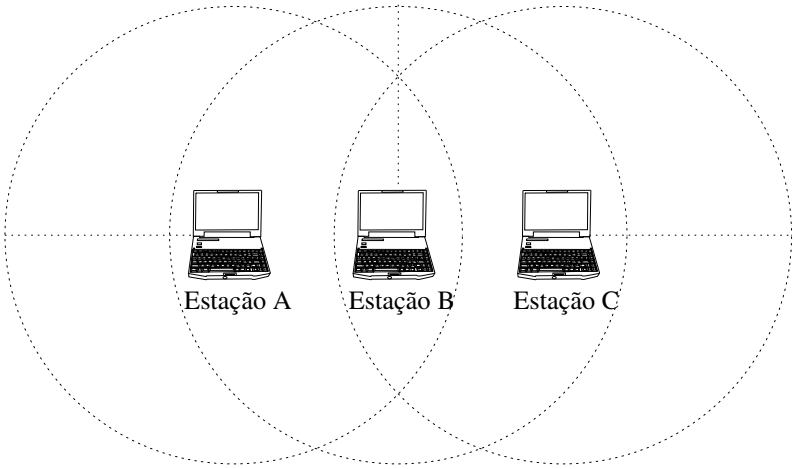


Figura 2.3: Exemplo de uma rede ad hoc de múltiplos saltos.

destas subcamadas são destacados nas Seções 2.1.1 e 2.1.2.

2.1.1 Subcamada de Convergência Física

Esta subcamada é suportada pelo procedimento de convergência de camada física (*Physical Layer Convergence Procedure* - PLCP), que define o mapeamento das unidades de dados de protocolo da subcamada MAC (MPDU) num formato de quadro adequado à transmissão e recepção usando o sistema PMD associado. Desta forma, a camada física troca unidades de dados de protocolo da camada física (PPDU) que contêm unidades de dados do serviço PLCP (PSDU). Como a subcamada de acesso ao meio utiliza o serviço da camada física, cada MPDU corresponde a uma PSDU carregada numa PPDU. A subcamada PLCP possibilita à subcamada de acesso ao meio operar com o mínimo de dependência da subcamada PMD.

Para efetuar a transmissão de dados, um preâmbulo e um cabeçalho PLCP devem ser acrescentados à PSDU. Estes preâmbulo e cabeçalho trazem informações necessárias à demodulação da PSDU. Existem dois tipos de preâmbulos e cabeçalhos possíveis: o preâmbulo e cabeçalho longos que são obrigatórios e compatíveis com a especificação IEEE 802.11 original, e o preâmbulo e cabeçalho curtos que são opcionais e projetados para aplicações que exijam alta vazão e dispensem a compatibilidade com equipamentos legados.

A Figura 2.4 mostra o formato da PPDU longa. O preâmbulo PLCP contém dois campos, um para sincronização (*Synchronization* - SYNC) e outro para delimitação de início de quadro (*Start Frame Delimiter* - SFD). O cabeçalho PLCP possui quatro campos: SINAL, SERVIÇO, TAMANHO e CRC (*Cyclic Redundant Check*).

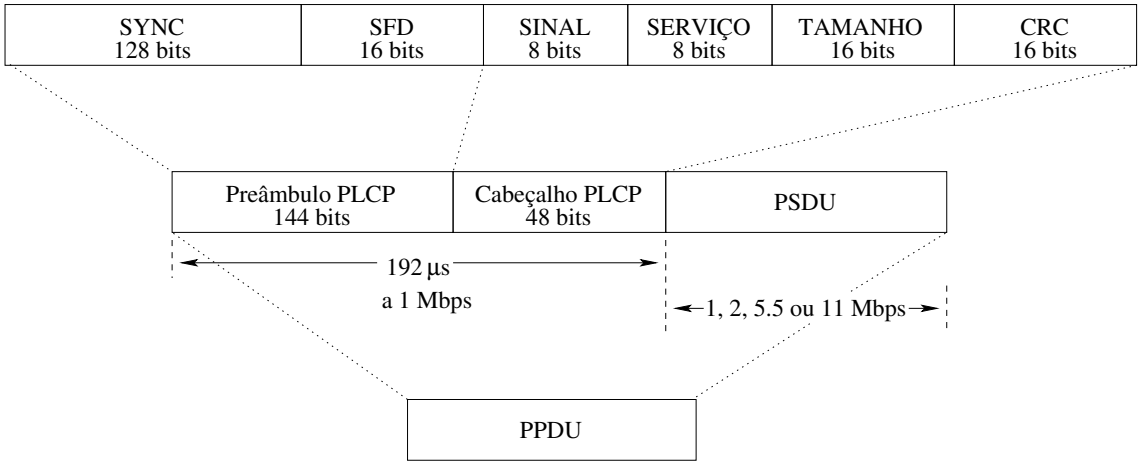


Figura 2.4: Formato da PPDU longa.

São transmitidos ao todo 192 bits de preâmbulo mais cabeçalho. Como a taxa de transmissão do preâmbulo e cabeçalhos longos é de 1 Mbps no IEEE 802.11, a duração da transmissão dos 192 bits é de 192 μs.

O campo SINAL define a taxa de transmissão utilizada para a PSDU. A taxa de transmissão é igual ao valor indicado no campo SINAL multiplicado por 100 kbps. Quando utilizado o preâmbulo longo, este campo pode representar uma das quatro taxas obrigatórias: 1, 2, 5,5 ou 11 Mbps.

O campo SERVIÇO foi definido já na especificação original para suportar extensões ao padrão IEEE 802.11. O bit 7 deste campo serve como complementação para o campo TAMANHO, como será visto a seguir. O bit 3 indica se a modulação utilizada é CCK (*Complementary Code Keying*) ou PBCC (*Packet Binary Convolutional Coding*). O bit 2 é utilizado para indicar se a freqüência de transmissão e o relógio dos símbolos são derivados do mesmo oscilador.

O campo TAMANHO é um número inteiro sem sinal de 16 bits que expressa em microssegundos o tempo de transmissão necessário para transmitir a PSDU. Como há

uma ambigüidade no número de *bytes* descritos por um número inteiro de microssegundos para taxas acima de 8 Mbps, o bit 7 do campo SERVIÇO é utilizado para complementar este campo, eliminando a ambigüidade.

O campo CRC contém uma seqüência de verificação de quadro (*Frame Check Sequence* - FCS) que protege os campos SINAL, SERVIÇO e TAMANHO. A FCS é o complemento a um do resto gerado pela divisão módulo 2 dos campos protegidos pelo polinômio $x^{16} + x^{12} + x^5 + 1$.

O preâmbulo curto foi definido como opcional e visa reduzir a sobrecarga adicionada na camada física e, desta forma, aumentar a vazão da rede. O formato da PPDU curta é mostrado na Figura 2.5. O campo de sincronização (ShortSYNC) possui menos bits que o seu equivalente do preâmbulo longo enquanto que o conteúdo do campo delimitador de início de quadro (ShortSFD) é o mesmo do campo SFD para o preâmbulo longo com a ordem dos bits invertida. Os campos do cabeçalho PLCP possuem os mesmos tamanhos e codificações, a exceção do campo SINAL que passa a possibilitar a transmissão do PSDU apenas nas taxas 2, 5.5 e 11 Mbps.

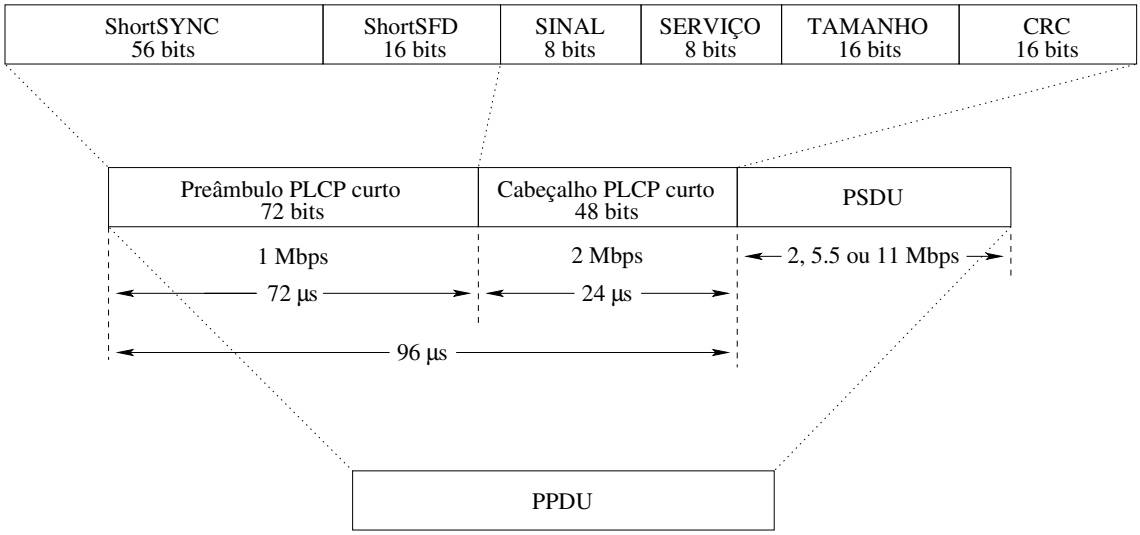


Figura 2.5: Formato da PPDU curta.

Neste caso, o preâmbulo PLCP possui 72 bits que são transmitidos a 1 Mbps em 72 μs e o cabeçalho PLCP possui os mesmos 48 bits do preâmbulo longo que agora são transmitidos a 2 Mbps, ou seja, em 24 μs. No total, a utilização do preâmbulo curto

implica uma sobrecarga de 96 μs na transmissão de um quadro, metade da sobrecarga imposta pela utilização do preâmbulo longo.

2.1.2 Subcamada Dependente do Meio Físico

A subcamada PMD é responsável pela codificação, decodificação e modulação dos sinais. O IEEE 802.11, empregando o DSSS, opera na taxa de 1 Mbps utilizando a modulação DBPSK (*Differential Binary Phase Shift Keying*) e na taxa de 2 Mbps utilizando a modulação DQPSK (*Differential Quadrature Phase Shift Keying*).

O padrão IEEE 802.11b [19] define uma extensão ao DSSS, denominada (*High Rate DSSS* - HR/DSSS), que utiliza uma técnica de modulação de chaveamento de código complementar (*8-chip Complementary Code Keying* - CCK) em conjunto com DSSS, permitindo a transmissão de dados em taxas de 5,5 Mbps e 11 Mbps.

2.2 Subcamada de Controle de Acesso ao Meio

De maneira diferente do que ocorre na redes IEEE 802.3 [22], o IEEE 802.11 não implementa a detecção de colisão. A capacidade de detectar colisões exigiria a capacidade de enviar e receber a sua própria transmissão para verificar se as transmissões de outras estações estão interferindo na sua transmissão, o que pode ser muito caro. Além disto, mesmo que houvesse a detecção de colisão no emissor ainda assim podem ocorrer colisões no receptor que não é possível detectar nas transmissões por rádio. Dadas essas dificuldades para que o nó emissor detecte colisões nas redes sem fio, foi desenvolvido um protocolo que visa à prevenção de colisões (*Carrier-Sense Multiple Access with Collision Avoidance* - CSMA/CA) em vez da detecção e recuperação de colisões (*Carrier-Sense Multiple Access with Collision Detection* - CSMA/CD).

O padrão IEEE 802.11 utiliza o mecanismo CSMA/CA e define dois métodos de acesso ao meio. O primeiro método de acesso, denominado Função de Coordenação Distribuída (*Distributed Coordination Function* - DCF), é distribuído e pode ser utilizado tanto na configuração infra-estruturada quanto na configuração ad hoc. O segundo mé-

todo de acesso, denominado Função de Coordenação em um Ponto (*Point Coordination Function* - PCF), é opcional e centralizado, podendo ser utilizado apenas em redes infra-estruturadas. Como o método DCF é o único que se aplica às redes ad hoc, este método será detalhado na Seção 2.2.1.

2.2.1 Função de Coordenação Distribuída

No mecanismo de acesso ao meio distribuído cada terminal da rede deve escutar o meio antes de iniciar uma transmissão. Caso o meio esteja ocioso, o terminal aguarda um certo intervalo de tempo (*Inter-Frame Space* - IFS). Após este intervalo de tempo, se o meio ainda estiver ocioso, o terminal pode começar a transmissão. O valor deste intervalo de tempo é determinado pelo tipo de quadro a ser transmitido (Figura 2.6).

Os quadros de reconhecimento (*Acknowledgment* - ACK) utilizam um intervalo de tempo chamado de SIFS (*Short Inter-Frame Space*) e têm prioridade sobre os pacotes de dados, que usam o intervalo DIFS (*Distributed Inter-Frame Space*). Além disto, para tentar evitar as colisões, um terminal deve esperar, além do tempo DIFS, por um tempo aleatório (*backoff*). No caso de vários terminais possuírem um quadro para ser transmitido, aquele que tiver sorteado o menor tempo de *backoff* irá transmitir primeiro. Este tempo é calculado a partir de um fator que depende do número de vezes consecutivas de tentativas de transmissão de um quadro multiplicado por um número aleatório (Equações 2.1 e 2.2). O tempo de *backoff* é usado para iniciar um temporizador que vai sendo decrementado enquanto o meio está ocioso. Quando o temporizador de *backoff* chega a zero, o terminal realiza sua transmissão. Caso, enquanto um terminal estiver decrementando o seu *backoff*, detectar que o meio não está mais ocioso, o terminal interrompe o contador de *backoff* e só volta a decrementá-lo após o meio ficar ocioso por um intervalo DIFS.

A cada vez que uma estação não recebe um ACK considera-se que houve uma colisão e desta forma o quadro deve ser retransmitido. Para minimizar a probabilidade de ocorrerem futuras colisões, o valor da janela de *backoff* é aumentado para a próxima potência de 2 menos 1, até um limite máximo predefinido. Este mecanismo é conhecido

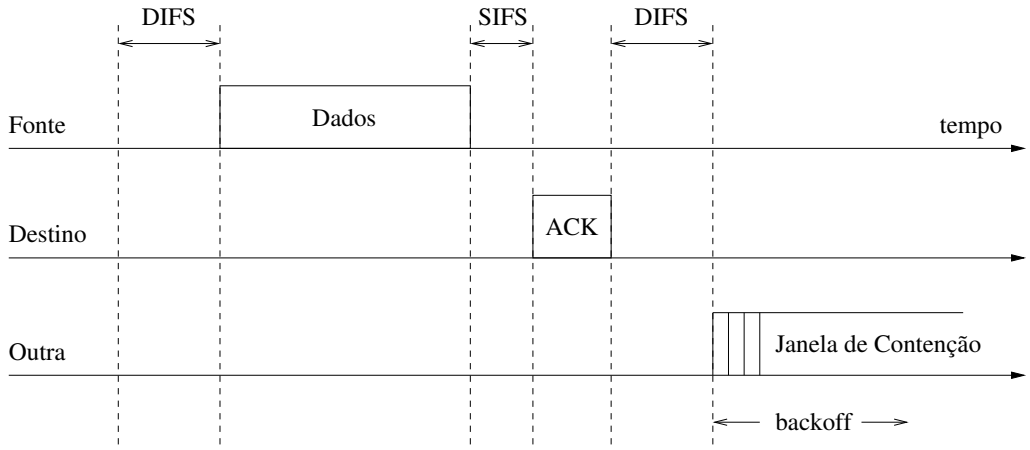


Figura 2.6: O esquema básico de acesso no mecanismo distribuído.

como *backoff* exponencial binário. Uma conseqüência deste método de acesso é que as estações que obtiveram sucesso na última transmissão são favorecidas, pois possuirão tamanhos de janela de *backoff* menores que as estações que não conseguiram transmitir. Este problema é agravado quando a rede está com uma alta carga, pois a probabilidade de ocorrerem colisões é maior.

O terminal escondido é um outro problema que ocorre neste tipo de acesso ao meio. A Figura 2.7 ilustra um cenário onde pode ocorrer este problema. As estações A e C estão fora do raio de alcance mútuo e alcançam apenas a estação B, enquanto que B alcança A e C. Considere que A comece a transmitir para B. Em seguida, C realiza detecção de portadora e verifica que o meio está livre. C também começa a transmitir para B, tendo em vista que C não é capaz de perceber que B já está recebendo informações de A. Neste cenário, ocorrerá uma colisão em B e apenas esta estação perceberá. As estações A e C só perceberão a colisão após a expiração do tempo de espera para o recebimento do ACK de B.

Para aliviar este problema, o IEEE 802.11 define o mecanismo opcional RTS (*Request To Send*) / CTS (*Clear To Send*). A Figura 2.8 ilustra a transmissão de um pacote utilizando o mecanismo RTS/CTS. Uma estação envia um RTS antes de cada transmissão de pacote para reservar o canal. Se o destino está pronto para receber, responde com um CTS, sinalizando que o nó fonte pode iniciar a transmissão e reservando o meio no entorno do receptor. Todas as estações que escutarem o RTS ou CTS devem atualizar o

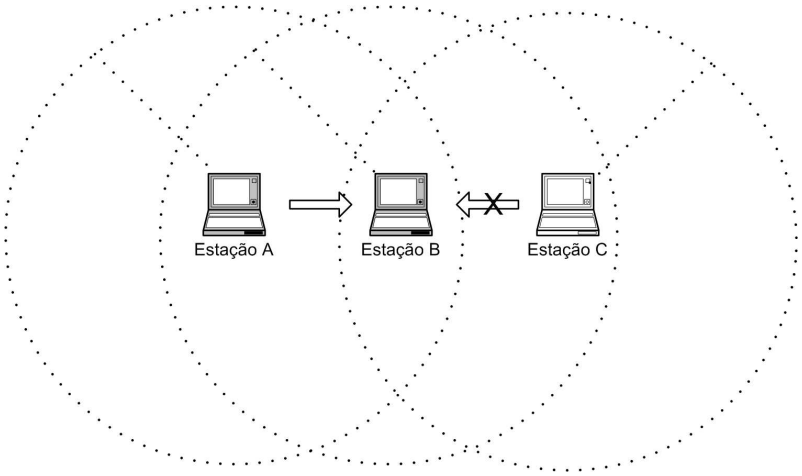


Figura 2.7: O problema do terminal escondido.

valor do seu vetor de alocação de rede (*Network Allocation Vector* - NAV). O conteúdo do campo NAV informa o período de tempo em que o meio permanecerá ocupado com aquela transmissão.

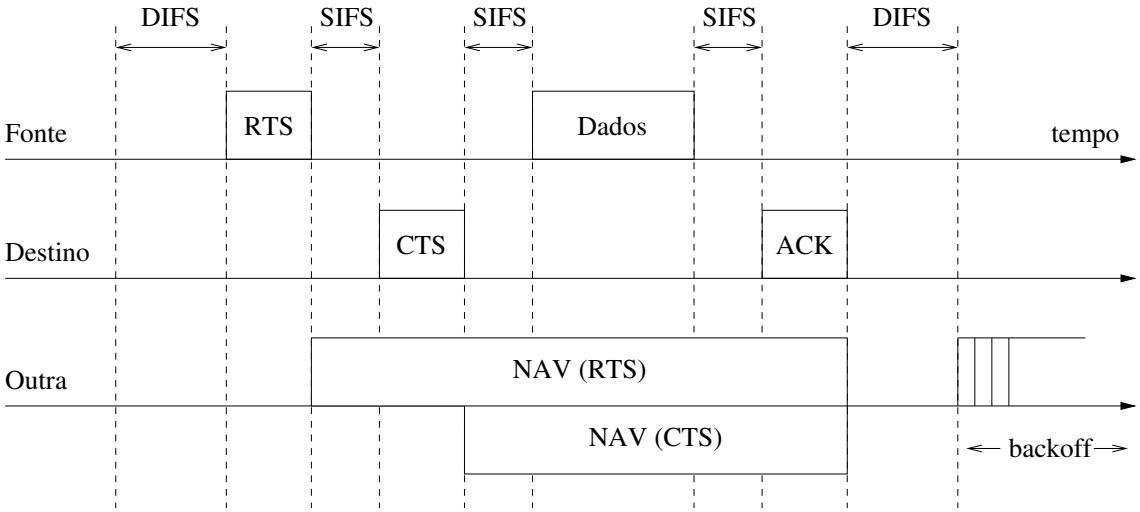


Figura 2.8: O mecanismo de acesso ao meio distribuído com RTS e CTS.

Por um lado, este mecanismo aumenta a eficiência da rede por minimizar o número de colisões e por garantir que as colisões ocorram apenas entre quadros de RTS, que são menores e não transportam dados. Por outro lado, o mecanismo acrescenta uma sobrecarga de controle ao DCF, conseqüentemente diminuindo a capacidade da rede.

2.3 Efeitos da Detecção de Portadora na Qualidade de Serviço

Nesta seção, analisamos as conseqüências dos chamados alcance de transmissão e alcance de detecção da portadora em redes IEEE 802.11.

Nas redes IEEE 802.11 dois ou mais nós não podem acessar o meio simultaneamente. Se um nó estiver detectando a transmissão de um outro nó, ele terá que esperar esta transmissão terminar, para tentar acessar o meio e transmitir o seu pacote. O alcance de transmissão (*Transmission Range*)[1] (i.e. alcance-TX) é menor que o alcance de detecção da portadora (*Carrier Sensing Range*) [2] (i.e. alcance-CS) [23]. Sendo assim, dois nós que não podem se comunicar diretamente podem ainda assim disputar os mesmos recursos. Conseqüentemente, um nó para saber o quanto de recursos disponíveis possui, precisa conhecer o total de recursos ocupados por todos os nós pertencentes à sua área de detecção de portadora (*Carrier Sensing Area*). A obtenção desta informação não é trivial já que, um nó pode disputar recursos com um outro nó e não ser capaz de comunicar-se diretamente com ele, caso este nó esteja localizado além do alcance de transmissão mas dentro do alcance de detecção de portadora.

Yang and Kravets [4] demonstraram quantitativamente através de simulação o efeito da detecção de portadora na estimativa de recursos disponíveis. O cenário utilizado foi o da Figura 2.9, onde o alcance de transmissão dos nós é de 250 m e o alcance de detecção de portadora é de 550 m. Inicialmente, o fluxo AB consome 45% da largura de banda do canal. Após um intervalo de tempo, o fluxo CD é iniciado e consome outros 45% da largura de banda do canal. Até este momento, na visão dos nós A e C, 90% da largura de banda do canal está sendo consumida e por isso ambos os fluxos conseguem obter uma vazão bem próxima da carga oferecida. Em seguida, o fluxo EF é iniciado com uma carga equivalente também à 45% da largura de banda do canal. O fluxo AB continua obtendo uma uma vazão igual a carga oferecida, já que os nós A e E estão separados por

[1] Distância na qual, os pacotes recebidos referentes a transmissão de um outro nó podem ser decodificados.

[2] Distância na qual, um nó é capaz de detectar a transmissão de um outro nó, mas não sendo possível decodificar os pacotes recebidos

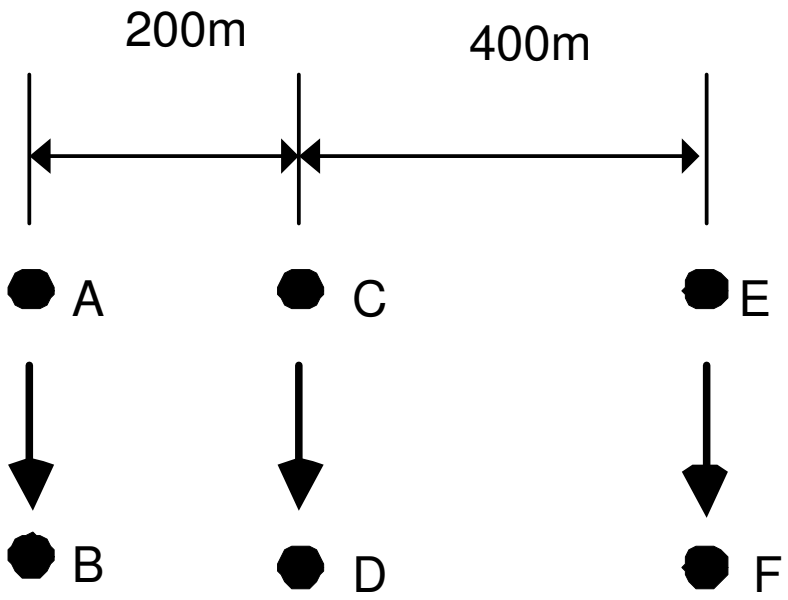


Figura 2.9: Estimativa de recursos disponíveis de um nó.

uma distância maior que o alcance de detecção da portadora (não disputam os mesmos recursos). Já o nó C, está dentro do alcance de detecção da portadora do nó E e com isso, os seus recursos passam a ser compartilhados com o fluxo EF. Como conseqüência o desempenho do fluxo CD sofre uma degradação devido ao fato da rede estar saturada na visão do nó C (carga oferecida à rede de 135%).

Outro fator importante ocasionado pela detecção de portadora e que deve ser levado em consideração, quando um nó for verificar se possui recursos disponíveis para suportar um fluxo de QoS, é a chamada interferência intra-fluxo (*intra-flow contention*) [4].

A interferência intra-fluxo é a interferência causada entre os nós que encaminham pacotes pertencentes a um mesmo fluxo em uma comunicação de múltiplos saltos [23]. Este fenômeno é agravado pelo fato de que normalmente a área de detecção da portadora é maior que a área de alcance de transmissão. Um nó da cadeia de encaminhamento terá os seus recursos divididos pelo número de nós pertencentes à cadeia de encaminhamento situados dentro do seu alcance de detecção de portadora, como ilustrado no exemplo a seguir.

Suponha o cenário com 5 saltos da Figura 2.10, onde os círculos de linha cheia representam o alcance de transmissão e os círculos de linha pontilhada representam o alcance

de detecção de portadora dos nós 1 e 5. Suponha um fluxo entre o nó 1 (fonte) e o nó 6 (destino). O nó 3 está dentro do alcance de detecção de portadora dos nós 1 e 5 e também está dentro do alcance de transmissão dos nós 2 e 4. Desta forma, o nó 3 não pode efetuar transmissões simultâneas com os nós 1, 2, 4 e 5, tendo os seus recursos disponíveis reduzidos em 5 vezes. Sendo assim, além do cálculo da estimativa de recursos disponíveis, um nó para decidir se é capaz ou não de suportar um fluxo que exige QoS, deve calcular o quanto este fluxo irá consumir caso aceito. Este valor depende da carga injetada na rede pela aplicação somado ao efeito da interferência intra-fluxo.

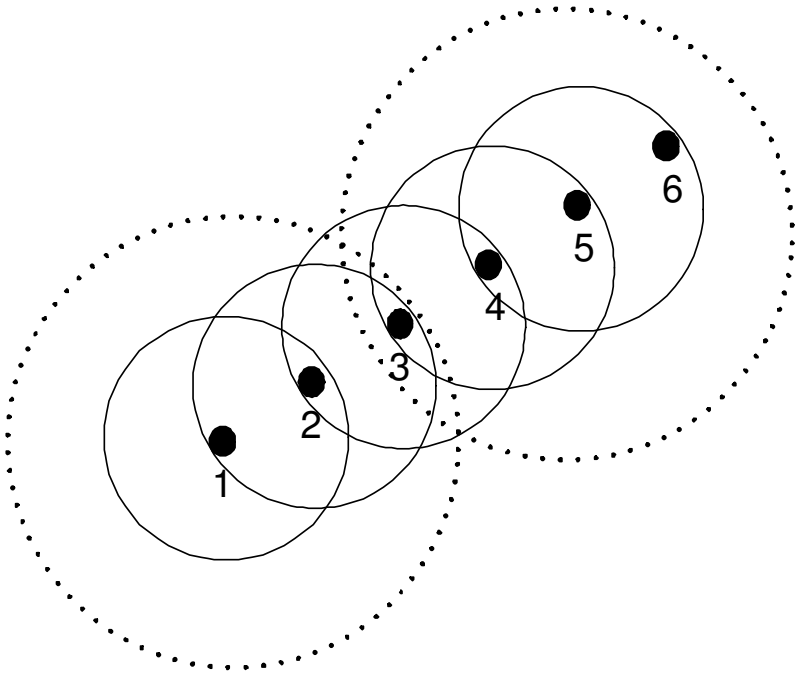


Figura 2.10: Interferência intra-fluxo.

O cálculo da estimativa de recursos disponíveis e o cálculo da interferência intra-fluxo de um nó (*contention count* - CC) realizados pelo TDAC-AODV são descritos no Capítulo 3.

2.4 Qualidade de Serviço no IEEE 802.11

Para prover garantias de QoS em redes IEEE 802.11 uma alternativa é realizar diferenciação entre os serviços executados pelas estações. Esta diferenciação pode ser feita

por diferentes prioridades no acesso ao meio para as diferentes estações ou tipos de tráfegos [24].

Os trabalhos relacionados à provisão de QoS em redes baseadas no padrão IEEE 802.11 podem ser divididos em duas categorias [25]. A primeira delas engloba propostas que realizam o fornecimento de QoS através do mecanismo centralizado e associadas às redes sem fio com infra-estrutura [26]. Na outra categoria, os trabalhos [8, 27, 28] visam prover QoS usando o mecanismo de acesso distribuído (DCF) e podem abranger tanto as redes sem fio com infra-estrutura como as redes ad hoc.

Em redes ad hoc baseadas no padrão IEEE 802.11, o mecanismo de acesso ao meio obrigatório é o distribuído, já que o PCF exige a presença de uma infra-estrutura. Existem três técnicas para oferecer diferenciação de serviço em redes ad hoc baseadas no IEEE 802.11 [7]. Estas técnicas consistem, basicamente, na variação de três parâmetros do mecanismo DCF para prover qualidade de serviço estatística ou determinística em redes ad hoc.

A primeira técnica consiste em alterar o valor do atraso aleatório (*backoff*). Esta técnica se baseia na variação da função que gera o *backoff*, alterando-se o fator multiplicativo ou o valor da janela do *backoff*, de maneira que cada terminal possa ter uma função diferente, de acordo com a qualidade de serviço requerida. As estações com maior prioridade teriam um fator multiplicativo menor, ou uma janela de tempo (*Contention Window* - CW) menor, que as estações com menor prioridade, acarretando um menor tempo de espera no acesso ao meio. A fórmula da função que gera o *backoff* pode ser expressa da seguinte maneira:

$$CW = ((CW_{min} + 1) * 2^{i-1}) - 1, \tag{2.1}$$

onde i representa o número de tentativas de transmissão.

Já o tempo de *backoff* é dado por:

$$backoff = random(CW) \times st, \tag{2.2}$$

onde, $random(CW)$ é uma função aleatória uniformemente distribuída entre $(0, CW)$ e st é uma fatia de tempo (*slot-time*).

A segunda técnica consiste na mudança do valor do DIFS. A idéia é usar valores de DIFS diferentes de acordo com a prioridade de cada estação, desta maneira, as estações com maior prioridade de acesso ao meio teriam um DIFS menor. Esta técnica também gera um menor tempo de espera no acesso ao meio.

A última técnica baseia-se na modificação do tamanho máximo do quadro a ser transmitido. Neste caso, as estações com maior prioridade poderiam transmitir quadros maiores que as demais estações. Esta técnica garante a diferenciação da qualidade de serviço ao permitir a transmissão de uma maior quantidade de informação a cada quadro, ao invés de fornecer prioridade no acesso ao meio, como as duas anteriores [7].

Capítulo 3

Controle de Admissão

Os protocolos de roteamento *ad hoc* podem ser divididos em dois grandes grupos: os protocolos pró-ativos e os sob-demanda, ou reativos.

De forma semelhante aos protocolos de roteamento na Internet, os protocolos pró-ativos constroem rotas para todos os nós da rede, mesmo sem tráfego de dados. Desta forma, quando um pacote necessitar de encaminhamento, a rota já é conhecida e pode ser utilizada imediatamente. Neste caso, os nós mantêm uma ou mais tabelas com informações referentes à rede e respondem a mudanças da topologia propagando atualizações, de modo a manter a conectividade da rede e a consistência do roteamento. Estas atualizações são feitas periodicamente, o que faz com que haja sempre um número constante de transmissões de pacotes de controle, mesmo quando o algoritmo de cálculo de rotas convergiu e mesmo sem carga. Dentre os protocolos pró-ativos para redes *ad hoc* móveis podem-se destacar o *Destination-Sequenced Distance Vector* (DSDV) [29] e o *Optimized Link State Routing* (OLSR) [14].

Os protocolos de roteamento sob-demanda, por outro lado, constroem as rotas apenas quando estas são necessárias, ou seja, quando uma rota é requerida o protocolo de roteamento inicia um procedimento de descoberta de rota. Desta forma, o processo de descoberta de rotas é disparado por um pacote de dados necessitando encaminhamento. Como a chegada de um pacote de dados é o evento que dispara a descoberta de rotas, estes protocolos não trocam mensagens a intervalos regulares, visando economizar banda

passante e energia. O volume de tráfego de controle de roteamento varia de acordo com a utilização da rede. Em contrapartida, estes protocolos apresentam uma maior latência no encaminhamento das mensagens, uma vez que a transmissão de dados só pode ser efetuada após a construção de uma rota para o destino. Dois dos protocolos reativos mais difundidos para redes móveis *ad hoc* são o *Dynamic Source Routing* (DSR) [30] e o *Ad-hoc On-Demand Distance Vector Routing* (AODV) [16]. Ambos os protocolos são compatíveis com o uso da tecnologia IEEE 802.11 e a maioria das propostas para prover QoS na camada de rede, são com a utilização de protocolos reativos [4, 5, 6, 31]

Neste capítulo é proposto um mecanismo de controle de admissão implementado na camada de rede, através da modificação do protocolo de roteamento AODV. As principais modificações são no processo de descobrimento de rotas e no anúncio de vizinhos pela mensagem *Hello*. Nos protocolos reativos, geralmente, o controle de admissão é implementado durante o processo de descoberta de rotas [4, 6, 31]. O principal papel do controle de admissão é verificar se o nó possui recursos suficientes para suportar a transmissão ou o reencaminhamento de um fluxo QoS, sem interferir nos fluxos QoS pré-existentes.

3.1 Visão geral do protocolo AODV

O protocolo AODV é um protocolo para descoberta de rotas sob demanda baseado em tabelas de roteamento, ou seja, os nós só descobrem uma rota para algum outro nó no momento em que a rota se faz necessária. Para operar corretamente, o protocolo AODV precisa do conhecimento da conectividade local. Para tanto, um mecanismo periódico de difusão local de mensagens *Hello* pode ser utilizado, ou o AODV pode apoiar-se em mensagens da camada MAC para identificar os nós vizinhos. O AODV utiliza, ainda, números de seqüência para controlar a idade das rotas e, desta forma, evitar a formação de *loops*. Quando é necessária a descoberta de uma rota, o nó fonte envia em difusão uma mensagem de pedido de rota (*Route Request* - RREQ) contendo, entre outros campos, o endereço do nó fonte e um identificador (*broadcast_id*), que juntos identificam unicamente um procedimento de descoberta de rota. Sempre que uma fonte inicia um novo

procedimento de descoberta de rota, o valor do identificador é incrementado. Os nós intermediários vão incrementando o contador de saltos da mensagem RREQ e reenviando-a para seus vizinhos, até que este pedido de rota atinja o destino, ou algum nó intermediário que possua uma entrada válida em sua tabela de roteamento para o nó destino. Ao reenviar um RREQ para seus vizinhos, o nó intermediário precisa armazenar o endereço IP da fonte e do destino, o identificador, o número de saltos do caminho reverso e o número de seqüência da fonte, para o caso de uma eventual requisição de rota para o nó fonte, que pode ser satisfeita por esta rota reversa. Cada nó intermediário processa e reenvia apenas uma vez cada RREQ, descartando os RREQs redundantes que provêm de inundações dos vizinhos. Para um nó intermediário estar apto a responder um RREQ, ele precisa ter uma entrada válida na tabela de roteamento com número de seqüência do destino mais recente que o enviado pela fonte. O nó intermediário com uma entrada ativa na tabela, ou o nó destino, envia em *unicast* uma resposta de rota (*Route Reply* - RREP) com, entre outros campos, o contador de saltos e o número de seqüência conhecido para o destino. O RREP retorna pelo caminho reverso do RREQ original, e vai estabelecendo apontadores para o nó que o enviou. Ao receber um segundo RREP para a mesma rota, o nó só o propaga se este contiver um número de seqüência do destino maior que os anteriores (rota mais nova) ou o mesmo número de seqüência com um contador de saltos menor (rota mais curta).

A tabela de roteamento possui, no máximo, uma entrada para cada destino, e cada entrada está associada a um temporizador que é o tempo sem utilização após o qual a entrada será considerada inválida. Cada entrada possui, ainda, uma lista com todos os vizinhos ativos através dos quais são recebidos pacotes para o destino em questão. O número de seqüência das entradas ativas da tabela é utilizado para distinguir mensagens de resposta e assim evitar a formação de *loops* que poderiam ocorrer com a utilização de informações desatualizadas.

3.1.1 Modificações do protocolo AODV

Na Seção 2.3, foram mostradas os efeitos da interferência intra-fluxo em uma comunicação de múltiplos saltos. Quanto maior for o número de nós pertencentes à cadeia de encaminhamento situados dentro do alcance de detecção da portadora do nó, menor será a

quantidade de recursos disponíveis deste nó. No protocolo AODV, os nós intermediários processam e reenviam apenas uma vez cada RREQ, descartando os RREQs redundantes que provêm da inundação da rede. As mensagens de RREQ são transmitidas em difusão e não são retransmitidas pela camada MAC em caso de colisão. Na camada MAC das redes IEEE 802.11 os quadros são transmitidos após esperarem por um tempo DIFS mais um tempo sorteado aleatoriamente (*backoff*). Portanto, não se pode garantir que a rota que será formada entre o nó fonte e o nó destino será a rota com o menor número de saltos. Para melhorar a eficiência do protocolo AODV e conseqüentemente do controle de admissão proposto neste trabalho, modificamos o mecanismo utilizado pelo protocolo AODV ao receber mensagens de RREQ com o mesmo endereço do nó fonte e mesmo identificador (*broadcast_id*). Antes de descartar o RREQ, o nó deve verificar se o valor do campo contador de saltos é menor do que o valor contido na tabela de roteamento associado ao nó fonte. Caso seja menor, a rota para o nó fonte deve ser atualizada, caso contrário a mensagem RREQ é descartada.

Para permitir o funcionamento do controle de admissão proposto neste trabalho, foram inseridos novos campos nas mensagens RREQ, RREP e *Hello* do protocolo AODV. Estes novos campos e sua utilização serão explicados nas próximas seções.

3.2 Controle de Admissão

O objetivo do controle de admissão é verificar se existem recursos disponíveis suficientes para atender aos requisitos de QoS exigidos pela aplicação e garantir que a entrada na rede deste novo fluxo não irá interferir nos fluxos QoS pré-existentes. O controle de admissão utiliza 3 componentes para decidir se aceita ou não a entrada de um novo fluxos: a estimativa dos recursos disponíveis, o cálculo da interferência intra-fluxo e o total de recursos que o novo fluxo irá consumir.

3.2.1 TAC-AODV

O TAC-AODV (*Time-based Admission Control - AODV*) [15] foi baseado no AAC-AODV (*Adaptive Admission Control - AODV*) [6], com uma modificação no cálculo dos recursos disponíveis. No AAC-AODV, Renesse *et al.* consideram que em uma rede IEEE 802.11b, a máxima largura de banda disponível é igual a 3,6 Mb/s (vazão de saturação da rede). Este valor corresponde à vazão de saturação da rede, quando é utilizado pela aplicação pacotes de aproximadamente 1024 bytes. Obviamente esta aproximação reduz a flexibilidade do protocolo, diminuindo a eficiência do mesmo quando são utilizados pacotes menores que 1024 bytes. Para superar esta deficiência, foi proposto neste trabalho o cálculo do consumo de banda em função do tempo de ocupação do meio. Este cálculo visa evitar que a saturação da rede seja atingida, qualquer que seja o tamanho de pacote utilizado pelas aplicações ativas na rede.

3.2.1.1 Cálculo dos recursos disponíveis no TAC-AODV

A estimativa de recursos disponíveis se baseia no chamado Cálculo de Tempo Ocupado (T_o). Para um nó estimar o período de tempo em que o meio está ocupado, T_o, somam-se os tempos em que o meio permanece ocupado com a transmissão, recepção e a detecção de pacotes $RTS, CTS, ACK e Data$ por um período de tempo de 1 segundo.

O tempo total ocupado (T_T) durante um período de 1 segundo, pode ser calculado pela seguinte equação:

$$T_T = To + (DIFS + 3 * SIFS + Backoff) \times NPD \tag{3.1}$$

onde NPD é o número de pacotes de dados transmitidos, recebidos ou detectados, T_o é o tempo em que o meio ficou ocupado pela transmissão de pacotes $RTS + CTS + ACK + Data$.

Uma questão importante é o cálculo do valor médio do *backoff*. Foram feitas simulações com diferentes valores de janela de tempo inicial (*CWmin*) e variando-se o número de nós disputando o acesso ao meio, para medir o número de fatias de tempo gastas em

uma transmissão. Os resultados da Figura 3.1 mostram que a partir de 5 nós, o número de fatias de tempo gastas torna-se constante. Este valor foi considerado nas simulações descritas no Capítulo 5.

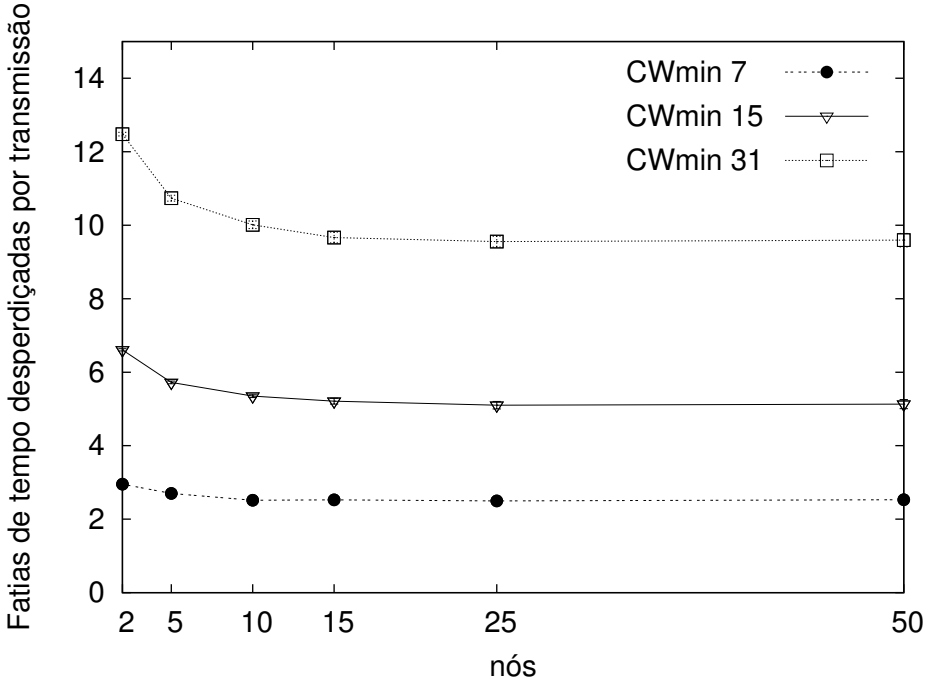


Figura 3.1: *backoff* médio.

Finalmente, para calcularmos o Tempo Livre (T_L) visto por um nó em 1 segundo, basta subtrairmos T_T:

$$T_L \;=\; 1 - T_T \; . \tag{3.2}$$

3.2.1.2 Cálculo da interferência intra-fluxo no TAC-AODV

O TAC-AODV utiliza o mecanismo proposto no AAC-AODV para o cálculo da interferência intra-fluxo de um nó (*Contention Count - CC*). No AAC-AODV, os autores assumem que todo nó em um caminho de múltiplos saltos interfere no máximo com os 2 nós anteriores e os 2 nós seguintes da cadeia de encaminhamento, ou seja, o alcance-CS é considerado igual a 2 vezes o alcance-TX de dados. Renesse *et al.* [6] utilizam o campo contador de saltos das mensagens RREQ e RREP do protocolo AODV. À medida que a mensagem RREQ vai sendo propagada pelos nós intermediários durante o processo

de descobrimento de rota, o valor do campo contador de saltos vai sendo incrementado. Nesta fase do descobrimento de rota, o campo contador de saltos da mensagem RREQ armazena o número de saltos entre o nó fonte e o nó que está propagando o RREQ. Já na fase em que a mensagem RREP foi transmitida pelo nó de destino, o valor do campo contador de saltos armazena o número de saltos entre o nó de destino e o nó que está propagando o RREP.

Sejam h_{req} e h_{rep} o número de saltos obtidos dos campos contador de saltos das mensagens RREQ e RREP, respectivamente. De acordo com [6], a interferência intra-fluxo de um nó (*CC*) é definida como:

$$\begin{cases} \text{se } h_{req} > 2 \rightarrow h_{req} = 2 \\ \text{se } h_{rep} > 3 \rightarrow h_{rep} = 3 \\ \qquad CC = h_{req} + h_{rep} \ . \end{cases} \tag{3.3}$$

A equação 3.3 mostra que o maior valor da interferência intra-fluxo de um nó (*CC*) é igual a cinco, ou seja, os dois nós anteriores, os dois nós posteriores e o próprio nó.

3.2.1.3 Estimativa dos recursos consumidos por um novo fluxo no TAC-AODV

O nó fonte de um fluxo, ao receber o pacote gerado na camada de roteamento verifica a taxa de geração de pacotes pela aplicação e o tamanho do pacote. Com essas informações é possível calcular o tempo que será consumido na transmissão dos pacotes desta aplicação, em 1 segundo.

O tempo T para transmitir um pacote de dados na rede IEEE 802.11 pode ser resumido da seguinte forma:

$$\begin{aligned} T = \quad & DIFS + backoff + RTS + SIFS + \\ & CTS + SIFS + \\ & Data + SIFS + ACK \ , \end{aligned} \tag{3.4}$$

onde $DIFS$ é 50 μs, que $3 * SIFS$ é 30 μs, *backoff* é obtido pelo produto de um valor aleatório de 0 a 31 pelo *slot-time* de 20 μs, e portanto o *backoff* médio é de $15,5 * 20\mu s$,

ou 310 μs. O Preâmbulo longo e o cabeçalho dos quadros possuem 192 bits transmitidos na taxa de 1 Mb/s. Os quadros $RTS + CTS + ACK$ possuem 48 bytes, ou 384 bits, que transmitidos na taxa básica de 1 Mb/s consomem 384 μs. $Data$ é o tamanho do pacote de dados, mais 48 bytes referentes aos acréscimos dos cabeçalhos IP e MAC. Assim, temos que o tempo médio de pacote T_{med} em μs, em uma rede 802.11b, pode ser calculado como:

$$T_{med(\mu s)} = 1542 + \frac{8 \times (tam+48)}{11} \tag{3.5}$$

onde tam é o tamanho de pacote originado pela aplicação.

O tempo de que será consumido na transmissão dos pacotes pertencentes a um fluxo (T_{tx}) em uma rede 802.11b, no período de 1 segundo, é calculado pela equação:

$$T_{tx(s)} = \frac{num}{1000000} * (1542 + \frac{8*(tam+48)}{11}) \, , \tag{3.6}$$

onde num é o número de pacotes gerados pela aplicação em 1 segundo, calculado pela razão entre a taxa da aplicação e o tamanho do pacote.

Em seguida o nó verifica se o tempo livre que possui é suficiente para atender a solicitação da aplicação. A mensagem RREQ só será enviada se o próprio nó puder atender os requisitos desejados pela aplicação. Foram incluídos dois novos campos nas mensagens RREQ e RREP, do AODV, contendo a taxa e o tamanho do pacote gerado pela aplicação.

Os nós intermediários, ao receberem as mensagens RREQ e RREP, irão verificar se podem ou não atender a solicitação do nó fonte. Os nós intermediários realizam o cálculo da equação (3.6) utilizando as informações sobre taxa e tamanho do pacote, contidas nas mensagens RREQ e RREP. É importante notar que a interferência intra-fluxo do nó, explicada na Seção 3.2.1.2, deve ser contabilizada e multiplicada pelo T_{tx}. A interferência é calculada através do campo *Hop Count* das mensagens RREQ e RREP. O fluxo só será admitido se:

$$T_L - CC * T_{tx} > 0 \, . \tag{3.7}$$

Caso o nó não possa atender a requisição, ele descarta a mensagem RREQ ou RREP interrompendo a descoberta de rota.

3.2.2 TDAC-AODV

O TDAC-AODV (*Traffic Differentiation and Admission Control - AODV*) combina mecanismos de controle de admissão e de diferenciação de serviços no protocolo AODV. No entanto, o controle de admissão do TDAC-AODV difere do TAC-AODV [15] principalmente no cálculo da estimativa de recursos disponíveis e no cálculo da interferência intra-fluxo. Em ambos mecanismos, o período de tempo em que o meio permanece ocioso é utilizado como estimativa dos recursos disponíveis. O controle de admissão proposto no TAC-AODV não realiza diferenciação de serviço e calcula os recursos disponíveis através da monitoração passiva da atividade do meio, utilizando-se da detecção física da portadora, de forma semelhante a outros mecanismos de controle de admissão encontrados na literatura [4, 5, 6]. O TAC-AODV não realiza diferenciação de serviço porque, através da monitoração passiva da atividade do meio não é possível decodificar e conseqüentemente diferenciar as transmissões de tráfegos do tipo QoS dos tráfegos do tipo BE, efetuadas por nós situados entre o alcance-TX e o alcance-CS. Em contrapartida, o controle de admissão do TDAC-AODV realiza diferenciação de serviço e para isso, faz o cálculo dos recursos disponíveis de forma ativa, pois cada nó da rede anuncia para os seus vizinhos os recursos consumidos por suas transmissões QoS e BE (Seção 3.2.3).

Outra modificação foi o aperfeiçoamento na precisão do cálculo da interferência intra-fluxo de um nó. Para realizar o cálculo de forma mais precisa do valor da interferência intra-fluxo de um nó em redes IEEE 802.11b, é necessário conhecer a identidade de todos os nós situados dentro do alcance-CS, o que não é possível somente através da escuta do meio.

No controle de admissão do TDAC-AODV, somente os procedimentos de descoberta de rota para aplicações que exigem garantias de QoS passam pelo módulo do controle de admissão. Considera-se que as aplicações do tipo BE possuem requisitos bem mais flexíveis do que as aplicações do tipo QoS, desta forma os procedimentos de descoberta de

rota para aplicações BE não passam pelo controle de admissão e são injetados diretamente na rede. A utilização do protocolo IEEE 802.11e na camada MAC pelo TDAC-AODV garante que as transmissões efetuadas pelos fluxos BE não irão interferir no desempenho dos fluxos QoS.

3.2.3 Cálculo dos recursos disponíveis no TDAC-AODV

O cálculo dos recursos disponíveis no TDAC-AODV é baseado em uma variável chamada Tempo Ocupado (T_o). Cada nó da rede estima seu T_o, através do tempo em que o meio está ocupado com as transmissões feitas pelo próprio nó, são somados mensagens de roteamento, quadros de dados de fluxos QoS, e seus respectivos quadros de RTS/CTS (quando utilizados), e ACK, somando-se DIFS, SIFS e o tempo gasto com o *backoff*, durante um intervalo de tempo de 1 segundo.

A Tabela 3.1 mostra os pacotes/quadros incluídos no cálculo de T_o em uma transmissão entre o nó fonte (A) e o nó de destino (B). Para efeito de cálculo o tempo ocioso gasto com DIFS, SIFS e *backoff* são incluídos no tempo gasto pelo nó fonte do tráfego.

Pacote/Quadro	Nó A	Nó B
Hello	X	X
RREQ	X	--
RREP	--	X
RTS	X	--
CTS	--	X
DATA	X	--
ACK	--	X

Tabela 3.1: Pacotes/Quadros incluídos no cálculo de T_o durante uma transmissão entre o nó fonte A e o nó destino B.

Não é incluído no cálculo de T_o o tempo gasto com as transmissões efetuadas de tráfegos do tipo BE. A idéia principal do mecanismo é que os fluxos BE somente ocupem os recursos da rede não utilizados pelos fluxos QoS. Para tanto, consideramos que os

fluxos BE utilizam o protocolo TCP, o qual vai incrementando sua janela de transmissão até ocupar toda a largura de banda não utilizada na rede. Portanto os recursos consumidos pelos fluxos BE podem ser reduzidos a qualquer momento com a admissão de um novo fluxo QoS. Assim, os recursos consumidos pelos fluxos BE não são contabilizados pelo controle de admissão ao decidir se aceita ou rejeita um novo fluxo QoS.

Na camada MAC, assumimos a utilização do IEEE 802.11e. Pode-se utilizar o padrão 802.11e para que os tráfegos de maior prioridade (fluxos QoS) acessem o meio mais rápido do que os tráfegos de menor prioridade (fluxos BE). Para tal o 802.11e controla o acesso ao meio e, conseqüentemente, reduz a largura de banda consumida pelos fluxos BE.

Em redes que utilizam o CSMA/CA para controle de acesso ao meio, os recursos ocupados de um nó correspondem a toda a largura de banda consumida por todos os nós situados dentro de seu alcance-CS (Seção 2.3). Os experimentos realizados em [32] mostram que o alcance-CS é aproximadamente duas vezes o alcance-TX para a taxa de transmissão de 2 Mb/s. Portanto, para calcularmos o Tempo Total Ocupado de um nó (T_T) é necessário obter o T_o de todos os nós vizinhos de 1 e 2 saltos considerando o alcance-TX para a taxa de 2 Mb/s.

No IEEE 802.11b [19], os quadros de difusão são transmitidos na taxa básica de 2 Mb/s. A mensagem de controle *Hello* do AODV possui um tempo de vida (*Time to Live* - TTL) igual a 1, ou seja, só alcança os seus vizinhos de 1 salto. Desta forma é possível conhecer os vizinhos diretos de um nó, porém não os vizinhos de 2 saltos.

Assim, para obter o valor de T_T, foram incluídos dois novos campos na mensagem *Hello* do AODV. O primeiro contém o T_o do nó e o seu tempo gasto com a transmissão de fluxos do tipo BE (T_{be}). O segundo campo contém uma lista com os endereços dos seus vizinhos, com seus respectivos T_o e T_{be}. Conseqüentemente, um nó ao receber as mensagens *Hello* transmitidas pelos seus vizinhos terá a informação do T_o dos mesmos e o T_o de todos os vizinhos dos seus vizinhos.

De posse destas informações, o Tempo Total Ocupado de um nó (T_T) é calculado pela soma de três parcelas (Equação 3.8). A primeira parcela é o T_o do próprio nó. A segunda

parcela é a soma dos T_o de todos os seus vizinhos (T_{o1}) ou seja, os nós situados dentro do seu alcance-TX. A terceira parcela é a soma dos T_o dos nós vizinhos dos seus vizinhos (T_{o2}), e que ainda não foram incluídos no cálculo da primeira e segunda parcelas.

$$T_T \quad = \quad T_o + T_{o1} + T_{o2}. \tag{3.8}$$

Considere o exemplo da Figura 3.2. Neste cenário o nó A recebe mensagens *Hello* dos nós B e C, os quais anunciam os seu próprios T_o e T_{be} e ainda os T_o e T_{be} dos seus vizinhos. A Figura 3.2 também mostra a estrutura de como o nó A armazena as informações recebidas nas mensagens *Hello*. Para o nó A estimar o seu T_T, primeiro ele calcula o T_o dele mesmo (T_o(A)). Depois somam-se os valores dos T_o dos seus vizinhos B e C (T_{o1}(B) + T_{o1}(C)) e, por fim, acrescenta-se somente o valor de T_o do nó D (T_{o2}(D)), o qual é seu vizinho de 2 saltos e ainda não havia sido contabilizado no cálculo das duas primeiras parcelas.

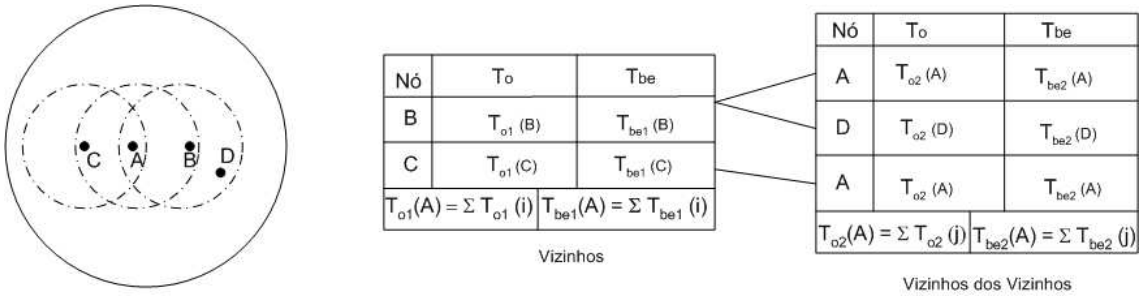


Figura 3.2: Armazenamento das mensagens *Hello*

Chen e Heinzelman [31] mostram que a estimativa de T_T pode ser incorreta devido ao problema do terminal escondido. Considere na Figura 3.3 o nó E, o qual está fora do alcance-TX do nó A e de seus vizinhos, mas está dentro do alcance-CS do nó A. O nó A e seus vizinhos escutam as transmissões de E, mas não são capazes de decodificar os quadros. Com isso, o nó A não terá conhecimento das transmissões efetuadas pelo nó E, apesar de sofrer interferência delas.

Como os fluxos do tipo BE não são incluídos no cálculo de T_o, as transmissões efetuadas pelos nós escondidos irão causar um erro no cálculo de T_T somente se o nó escondido transmitir tráfego do tipo QoS. Para resolver esse problema assumiu-se que todos fluxos transmitidos por um nó escondido são considerados como do tipo QoS, uma solução conservadora.

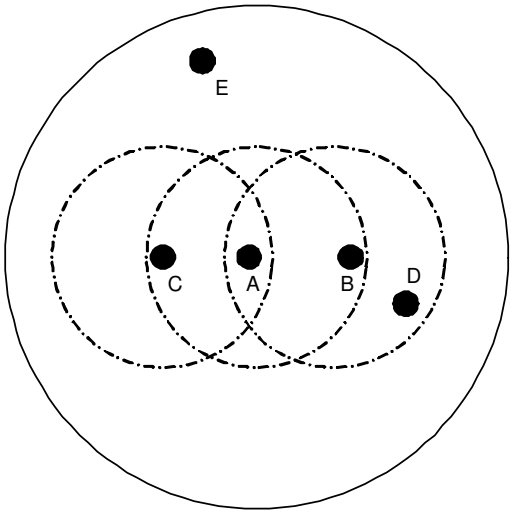


Figura 3.3: O nó E está dentro do alcance-CS do nó A mas está escondido para o mesmo.

Com isto, o cálculo do T_T foi modificado. O cálculo da primeira e segunda parcelas, correspondentes ao tempo consumido pelo próprio nó e pelos nós situados dentro do seu alcance-TX, permaneceram inalterados. Para estimar o T_o dos nós situados na região entre o alcance-TX e o alcance-CS (T_{o2}), são somados os tempos gastos com a detecção da portadora de todos os pacotes que a camada física não foi capaz de decodificar (T_{cs}), ou seja, todas as transmissões efetuadas nesta região, menos o tempo gasto com as transmissões de fluxos do tipo BE (T_{be2}) anunciadas nas mensagens *Hello* pelos vizinhos de 2 saltos (Equação 3.9).

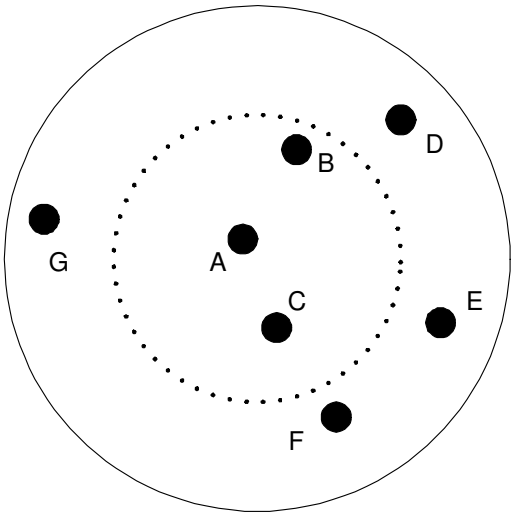


Figura 3.4: O círculo pontilhado representa o alcance-TX e o círculo cheio o alcance-CS do nó A.

Na Figura 3.4, o T_{cs} do nó A é o tempo total gasto com todas as transmissões efetuadas pelos nós D, E, F e G. O T_{be2} é o tempo gasto somente por transmissões de fluxos BE originadas pelos nós D, E, F e G. Desta forma, o tempo ocupado pelos vizinhos de 2 saltos (T_{o2}) de um nó é definido por

$$T_{o2} \quad = \quad T_{cs} - T_{be2} \; . \tag{3.9}$$

Assim o Tempo Total Ocupado (T_T) de um nó durante o período de 1 segundo é definido por

$$T_T \quad = \quad (T_o + T_{o1}) + (T_{cs} - T_{be2}) \; . \tag{3.10}$$

Esta escolha torna o controle de admissão mais restritivo, podendo impedir a entrada de um novo fluxo QoS na rede caso o nó escondido esteja transmitindo um fluxo BE e o controle de admissão o considerou um fluxo QoS. Em contrapartida, garante-se que a rede não irá saturar com a admissão errônea de um novo fluxo, prejudicando os fluxos pré-existentes.

O Tempo Livre Disponível (T_L) em 1 segundo de um nó é dado por

$$T_L \quad = \quad 1 - T_T \; . \tag{3.11}$$

A característica principal de um controle de admissão é garantir que ao admitir um novo fluxo QoS, este fluxo não venha a interferir nos fluxos QoS pré-existentes. Considere o cenário da Figura 3.5, onde as linhas pontilhadas representam o alcance-TX e as linhas cheias representam o alcance-CS dos nós A e C. O fluxo DE consome 100% dos recursos, sendo 80% consumidos pelo nó D com a transmissão de quadros RTS e Dados e 20% consumidos pelo nó E com a transmissão dos quadros CTS e ACK. Suponha que o nó A queira transmitir um fluxo para o nó B e este fluxo viesse a consumir 15% dos recursos. Pelo mecanismo proposto, o nó A, ao calcular os seus recursos disponíveis, somente contabiliza os recursos consumidos pelo nó D no fluxo DE, pois o nó E está a 3 saltos do nó A. Sendo assim, o nó A concluirá que possui recursos suficientes e admitirá o fluxo

AB, embora na realidade não existam recursos suficientes.

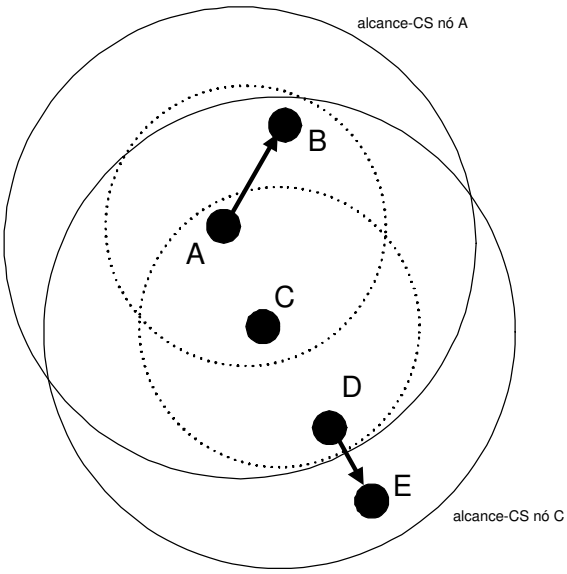


Figura 3.5: O nó E está fora do alcance-CS do nó A

A admissão deste fluxo ocasionará colisões no nó D (quadros do fluxo AB com os quadros CTS/ACK do nó E), degradando assim o desempenho do fluxo DE. Para evitar este problema, o T_L de um nó deve ser baseado no mínimo do T_L do nó e de todos os seus nós vizinhos de um salto. Foi necessária a inclusão de um terceiro campo na mensagem *Hello* do AODV que contém o T_L do próprio nó, calculado através da Equação 3.11. No exemplo da Figura 3.5 o T_L do nó A será o min (T_L(A), T_L(B), T_L(C)). Como o T_L(C) é igual a zero, o nó C recebe os recursos consumidos pelos nós D 80% (1 salto) e E 20% (2 saltos), conseqüentemente o T_L do nó A será igual a zero e o fluxo AB não poderá ser admitido pela rede. Desta forma o T_L de um nó é calculado por

$$T_L(i) \quad = \quad min\left(T_L(i), T_L(j)\right), \tag{3.12}$$

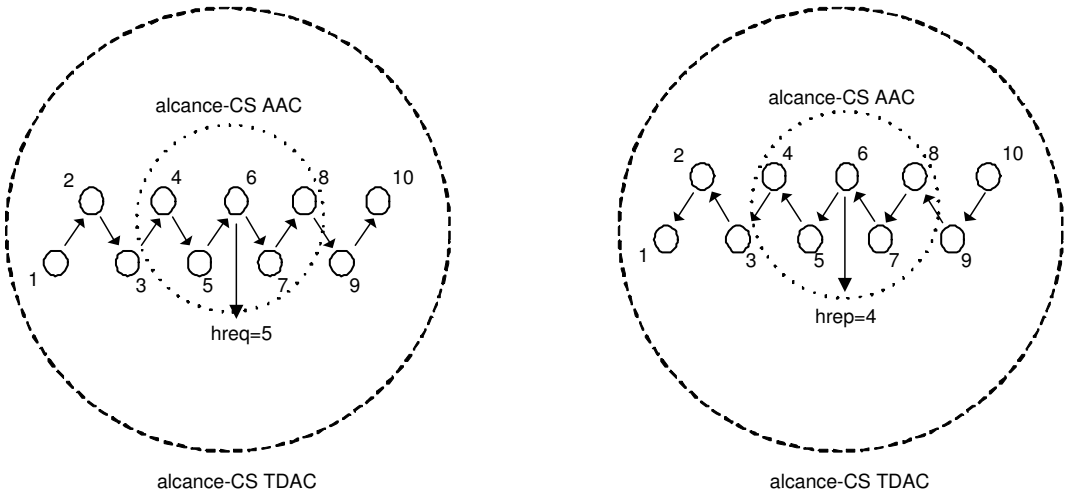
para todo nó j vizinho de 1 salto do nó i.

3.3 Cálculo da interferência intra-fluxo no TDAC-AODV

Kravets e Yang [4] definem a interferência intra-fluxo de um nó (*CC*) como o número de nós pertencentes à cadeia de encaminhamento situados dentro do alcance-CS do

referido nó.

O CACP (*Contention-Aware Admission Control for Ad Hoc Networks*) [4] é um mecanismo de controle de admissão proposto para redes ad hoc IEEE 802.11. O CACP, assim como o AAC-AODV [6], também assume que o alcance-CS é duas vezes o alcance-TX. Desta forma, a transmissão de um nó interfere no máximo em 2 nós anteriores e 2 nós posteriores em uma cadeia de encaminhamento. Esta afirmação é correta se a rede utiliza a taxa de transmissão de dados de 2 Mb/s. O CACP utiliza o protocolo de roteamento DSR, o qual realiza o roteamento pela fonte. O uso deste protocolo permite aos nós conhecerem todos os nós anteriores e posteriores a ele na cadeia de encaminhamento. Durante o descobrimento de rota, ao receber um RREQ, o nó adiciona a uma lista o endereço dos últimos dois nós que propagaram a mensagem. Durante a fase de encaminhamento do RREP o mesmo procedimento é executado. Ao final, o nó pode calcular o valor de seu *CC* de acordo com a informações contidas na lista.



(a) Pedido de rota para o destino.

(b) Resposta de rota para o fonte.

Figura 3.6: Cadeia de Encaminhamento de um fluxo de 9 saltos

Na Figura 3.6, considere o nó 1 como sendo o nó fonte e o nó 10 o nó de destino da comunicação. O círculo pontilhado representa o alcance-CS assumido pelo AAC [6] e pelo CACP [4]. Aplicando-se a Equação 3.3 ao sexto nó da cadeia de encaminhamento, obtemos que o valor de *CC* é igual a 5.

Os mecanismos propostos por Kravets e Yang [4] e Renesse *et al.* [6] para o cálculo de

CC não são apropriados quando o protocolo IEEE 802.11b é utilizado. Os experimentos realizados em [33] mostram que o alcance-CS é aproximadamente 6 vezes o alcance-TX para a taxa de transmissão de dados de 11 Mb/s. Vale ressaltar que o alcance-CS independe da taxa de dados usada, sendo exclusivamente dependente da potência de transmissão e da sensibilidade da interface de rede do receptor. Portanto, vizinhos a 3 ou mais saltos em um caminho de múltiplos saltos podem estar dentro do alcance-CS quando a taxa de transmissão utilizada é de 11 Mb/s. Portanto, ao aplicarmos a Equação 3.3 podemos obter um valor errôneo do *CC* de um nó visto que os vizinhos de 3 ou mais saltos, pertencentes a um caminho de múltiplos saltos, podem estar dentro do alcance-CS quando a taxa de transmissão utilizada é de 11 Mb/s.

Para lidar com este problema, no TDAC-AODV foi introduzido um novo campo nas mensagens de pedido de rota (RREQ) e resposta de rota (RREP) do protocolo AODV. Quando uma mensagem RREQ é transmitida pelo nó fonte ou é reencaminhada pelos nós intermediários, cada nó adiciona o seu próprio endereço a este campo. Quando o nó de destino recebe a mensagem RREQ, ele copia o conteúdo do campo para a mensagem RREP e transmite a mesma. Para o cálculo da interferência intra-fluxo, é necessário que o nó conheça todos os nós anteriores e seguintes a ele na cadeia de encaminhamento entre o nó fonte e o nó destino. Para evitar que algum nó intermediário que possua uma rota para o destino transmita uma mensagem RREP em resposta ao RREQ, impedindo o armazenamento da rota completa, o *flag* "D" [1] do cabeçalho da mensagem RREQ deve estar setado.

Na seção 3.2.3, foi mostrado que um nó após receber as mensagens *Hello* de todos os seus vizinhos de 1 salto, conhece todos os nós com os quais ele pode se comunicar e que estão dentro do seu alcance-CS. Assim, cada nó da cadeia de encaminhamento pode calcular o valor de *CC* ao receber o RREP, através da equação

$$CC = \#(CSN \cap P)\,, \tag{3.13}$$

onde CSN é o conjunto de nós situados dentro do alcance-CS, obtido através do recebimento das mensagens *Hello* e P é o conjunto de nós pertencentes à cadeia de encaminha-

[1] Somente o nó de destino pode responder a uma mensagem RREQ.

mento entre o nó fonte e o nó de destino.

Portanto, no exemplo da Figura 3.6b (o círculo tracejado representa o alcance-CS no TDAC-AODV) quando a taxa de transmissão de dados é igual a 11 Mb/s, o nó 1 até o nó 10 estão dentro do alcance-CS do nó 6. Aplicando-se a Equação 3.13, o valor correto de *CC* do nó 6 é igual a 9.

Um outro ponto importante a ressaltar, além do problema já citado no cálculo do *CC* realizado pelos mecanismos [4, 6] em redes IEEE 802.11b é que, estes mecanismos ainda podem cometer erros no cálculo do *CC* em redes IEEE 802.11 que operam na taxa de transmissão de dados de 2 Mb/s. Estes mecanismos consideram em seus cálculos que o algoritmo de caminho mais curto de *Dijkstra* foi utilizado durante o estabelecimento da rota entre os nós fonte e destino. Ambos os mecanismos utilizam protocolos de roteamento reativos que inundam a rede com mensagens de difusão RREQ na tentativa de encontrar uma rota para o destino. Em cenários com uma alta densidade de nós, a probabilidade de colisão destas mensagens cresce. Portanto, nem sempre a rota com menor número de saltos é formada, fazendo com que seja possível existirem mais de dois nós anteriores ou posteriores, pertencentes à cadeia de encaminhamento, dentro do alcance-CS do nó.

Após calcular o valor de *CC*, cada nó verifica se os recursos disponíveis são suficientes para suportar uma carga equivalente a $CC * Taxa$ (onde $Taxa$ é a carga gerada pela aplicação). Em caso afirmativo o processo de descoberta de rota prossegue, caso contrário o nó descarta a mensagem RREQ ou RREP.

3.4 Operação do Controle de Admissão do TDAC-AODV

O controle de admissão do TDAC-AODV é dividido em duas fases. A primeira, denominada controle de admissão parcial, é realizada durante a fase em que os nós recebem as mensagens RREQ e a segunda, denominada controle de admissão completo, é realizada durante a fase em que os nós recebem as mensagens RREP. A Seção 3.3 mostra que o cálculo preciso do valor de *CC* só pode ser feito após o recebimento da mensagem

RREP. Na primeira fase, os nós não conhecem a rota completa para o nó de destino conseqüentemente, o valor de *CC* obtido da Equação 3.13 é parcial. Entretanto, o objetivo de realizar-se o controle de admissão desta fase é reduzir o número de inundações de mensagens RREQ desnecessárias, onde não existe recursos disponíveis para suportar o tráfego requisitante, mesmo considerando o valor parcial de *CC*.

Quando a camada de roteamento de um nó fonte recebe um pacote da camada superior para iniciar um tráfego, primeiro é verificado o tipo de tráfego (QoS ou BE). Caso seja um tráfego do tipo QoS, a requisição tem de passar primeiro pelo módulo do controle de admissão, antes de transmitir uma mensagem RREQ. No controle de admissão, o nó verifica se os recursos disponíveis são suficientes para atender a requisição de carga considerado os efeitos da interferência intra-fluxo. Caso afirmativo, o nó fonte transmite a mensagem RREQ. Caso contrário, como não há recursos suficientes, a mensagem RREQ é descartada e o fluxo não será iniciado. Este processo é feito por todos nós intermediários envolvidos no descobrimento de rota, antes de propagar ou transmitir um RREQ ou RREP.

Agora caso o tráfego seja de tipo BE, o processo de descobrimento de rota não passa pelo controle de admissão. As mensagens RREQ e RREP são enviadas diretamente para a camada MAC para serem transmitidas.

3.4.1 Cálculos efetuados pelo Controle de Admissão do TDAC-AODV

O primeiro passo efetuado pelo controle de admissão do TDAC-AODV, assim como no TAC-AODV, é verificar a taxa de transmissão da aplicação e o tamanho do pacote gerado pela aplicação. Com essas informações é possível calcular o total de recursos que serão consumidos por segundo, para transmitir este novo fluxo.

Da mesma forma que no TAC-AODV, é calculado o tempo gasto na transmissão de um pacote. Porém, com relação ao TAC-AODV, a taxa básica passou de 1 Mb/s para 2 Mb/s, de acordo com IEEE 802.11b [19]. Assim, temos que o tempo de transmissão médio de um pacote T_{med} em μs, em uma rede 802.11b, pode ser calculado como:

$$T_{med(\mu s)} = 50 + 30 + backoff + 576 + \frac{8\times(tam+48)}{11} \quad (3.14)$$

ou

$$T_{med(\mu s)} = 656 + backoff + \frac{8\times(tam+48)}{11}\ , \quad (3.15)$$

onde tam é o tamanho do pacote originado pela aplicação.

Caso o mecanismo de RTS/CTS não esteja sendo utilizado o T_{med} em μs fica reduzido a:

$$T_{med(\mu s)} = 454 + backoff + \frac{8\times(tam+48)}{11} \quad (3.16)$$

Um nó pode calcular o tempo que será consumido para a transmissão de um fluxo QoS (T_{tx}) na taxa de 11 Mb/s durante o período de 1 segundo, através das seguintes equações:

$$T_{tx(s)} = \frac{num}{1000000} \times (656 + backoff + \frac{8\times(tam+48)}{11})\ , \quad (3.17)$$

ou

$$T_{tx(s)} = \frac{num}{1000000} \times (454 + backoff + \frac{8\times(tam+48)}{11})\ , \quad (3.18)$$

onde num é o número de pacotes gerados pela aplicação em 1 segundo, calculado pela razão entre a taxa de transmissão da aplicação pelo o tamanho do pacote. Mais uma vez, a Equação 3.17 considera o uso de RTS/CTS enquanto a Equação 3.18 não.

Para permitir que os nós vizinhos, ao receberem a mensagem RREQ ou RREP, saibam identificar se aquela requisição é para um tráfego QoS ou BE, utilizamos o campo *Type of Service* do cabeçalho IP para diferenciar uma requisição da outra.

Os dois novos campos que foram adicionados às mensagens RREQ e RREP no TAC-AODV, os quais contêm a taxa de transmissão e o tamanho do pacote gerado pela aplicação, são também utilizados no TDAC-AODV. O conteúdo destes campos são utilizados pelos controles de admissão dos nós intermediários no cálculo das Equações 3.17 ou 3.18. A interferência intra-fluxo é calculada (Equação 3.13) e multiplicada por T_{tx}. O fluxo é

aceito e conseqüentemente o processo de descobrimento de rotas não é interrompido apenas se:

$$T_L - CC * T_{tx} > 0 \, . \tag{3.19}$$

Nas redes IEEE 802.11, a vazão agregada diminui após a saturação da rede [34]. A precisão dos cálculos efetuados pelo controle de admissão de um nó durante o processo de descobrimento de rota está diretamente ligada ao correto recebimento das mensagens *Hello* de seus vizinhos. As mensagens *Hello* são transmitidas em difusão e não são retransmitidas em caso de colisão. Portanto, o controle de admissão de um nó pode eventualmente efetuar seus cálculos com informações defasadas e com isso, o nó admita um fluxo erroneamente.

Por isso, na Equação 3.19, justifica-se a utilização de uma reserva de recursos que tem como objetivo tentar evitar que o total de carga admitida não seja superior ao ponto de saturação da rede. Desta forma, preveni-se que a rede sature devido a erros na estimativa dos recursos disponíveis. Assim sendo, a Equação 3.19 ficaria desta forma:

$$T_L - CC * T_{tx} > T_R \, , \tag{3.20}$$

onde T_R representa uma largura de banda reservada.

Outra vantagem é que utilizando o tempo de reserva (T_R), os fluxos QoS não ocuparão todos os recursos da rede, evitando assim inanição dos fluxos BE.

A Figura 3.7 mostra o funcionamento da camada de rede de um nó proposta pelo mecanismo.

3.5 Violação de QoS

A mobilidade é uma característica intrínseca das redes ad hoc e pode, naturalmente, levar a uma mudança de cenário que altere a quantidade de recursos utilizados em uma

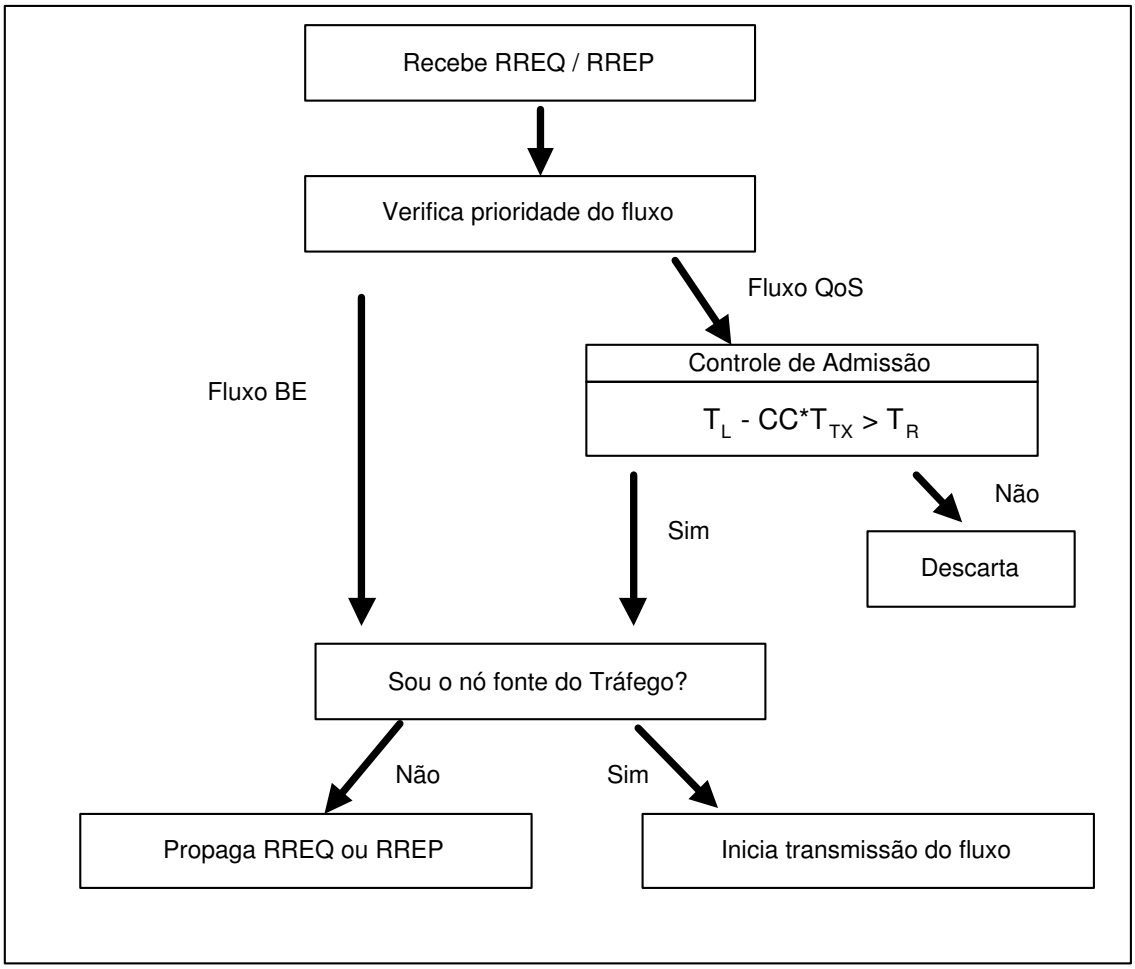
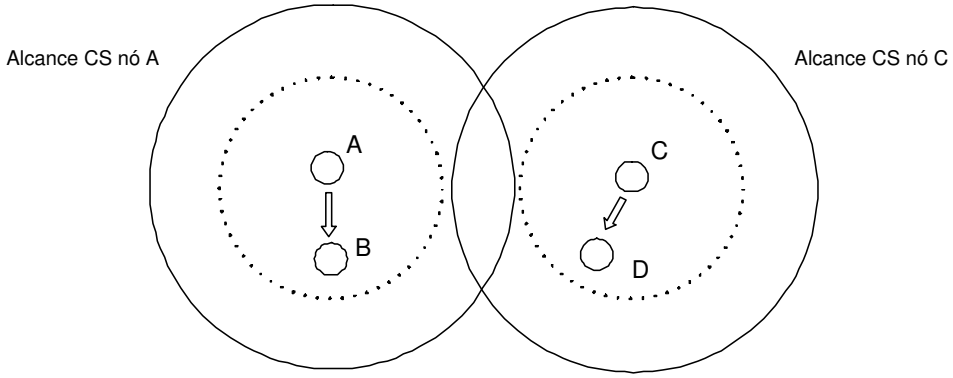


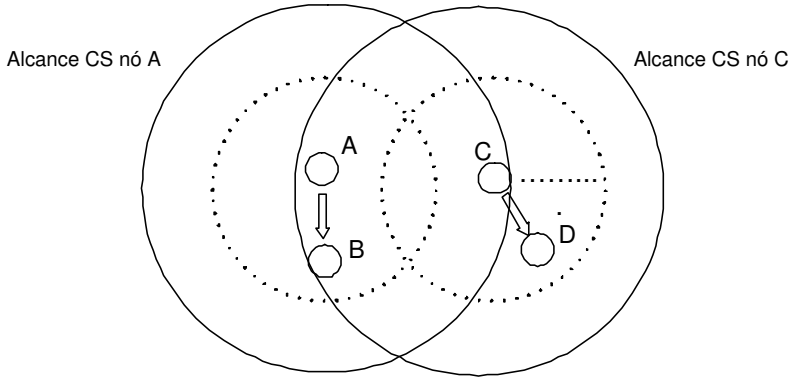
Figura 3.7: Mecanismo implementado na camada de rede.

determinada região. Suponha que dois nós estejam roteando dois fluxos QoS e não estejam disputando os mesmos recursos da rede. Em um determinado instante, os nós movimentam-se para dentro da área de interferência em comum e passam a disputar os mesmos recursos. A Figura 3.8 ilustra os 2 cenários. O T_L de cada nó será reduzido e com isso os nós podem não ser mais capazes de suportar os fluxos QoS, previamente aceitos, com o nível qualidade de serviço exigido pela aplicação.

Além da mobilidade, "falsas admissões" podem causar violações de QoS. A falsa admissão pode ocorrer quando vários nós fontes iniciam simultaneamente um procedimento de descobrimento de rotas, compartilhando caminhos e nós intermediários entre a fonte e o destino. Durante o descobrimento de rotas, os nós intermediários não realizam qual-



(a) O nó C não interfere no fluxo AB.



(b) O nó C passa a interferir no fluxo AB.

Figura 3.8: Violação de QoS por mobilidade.

quer reserva de recursos, portanto, um nó fonte pode receber uma mensagem de RREP indicando que existe uma rota com recursos suficientes para atender os requisitos do novo fluxo, quando na realidade pode não existir.

Além disso, reduções automáticas na taxa de transmissão de dados ocasionadas pela degradação das condições de recepção fazem com que a relação sinal-ruído cresça aumentando a perda de pacotes. Conseqüentemente, as taxas de transmissão de dados são automaticamente reduzidas para uma das possíveis taxas: 5,5 Mb/s, 2 Mb/s e 1 Mb/s. Ao melhorar as condições de propagação e diminuindo a taxa de erro de pacotes, as taxas voltam a ser incrementadas. Desta forma, foi definido um mecanismo de controle de violação de QoS no TDAC-AODV, visando adaptar o mecanismo a estas variações da rede.

3.5.1 Implementação do Controle de Violação de QoS no TDAC-AODV

Com o objetivo de evitar a perda de garantias QoS pelos motivos citados, todos os nós da rede periodicamente verificam se o seu T_L é maior que um limiar de segurança (T_S). Este limiar de segurança é menor que o valor de T_R utilizado pelo controle de admissão durante o processo de descobrimento de rotas. Se T_L for menor que T_S, assume-se que a saturação da rede é iminente e, neste caso, algum fluxo QoS deve ser interrompido com o intuito de preservar o desempenho dos outros fluxos QoS. Perkins *et al.* [35] adicionaram extensões à tabela de roteamento dos nós para permitir que os nós intermediários associem cada fluxo que estejam roteando com o nó fonte do tráfego.

No protocolo AODV, quando um nó recebe uma mensagem RREP durante o processo de descoberta de rota, ele adiciona a sua tabela de roteamento, caso não exista, uma rota para o nó de destino do tráfego a ser admitido (o nó que originou o RREP). A esta nova rota são adicionadas extensões que incluem um identificador do fluxo, o endereço do nó fonte do fluxo e a quantidade de recursos consumidos pelo fluxo.

Um nó, ao verificar uma perda de garantia de qualidade de serviço, envia uma mensagem *ICMP QoS Lost* [35] para o nó fonte de um tráfego QoS que ele esteja roteando, informando que não é possível mais atender a requisição. Nesta mensagem é incluído o identificador do fluxo para que cada nó pertencente à cadeia de encaminhamento do fluxo, ao receber a mensagem, possa verificar junto à sua tabela de roteamento a quantidade de recursos que este fluxo consumia e atualizar a informação de T_o desconsiderando a existência deste fluxo. Após esta atualização, cada nó deve transmitir imediatamente uma mensagem *Hello* com um código diferente no cabeçalho indicando que aquele *Hello* foi transmitido devido ao recebimento de uma mensagem *ICMP QoS Lost*. Um nó ao receber esta mensagem *Hello*, transmite uma mensagem *Hello* imediatamente com as informações atualizadas dos recursos consumidos pelos seus vizinhos de 1 salto. O objetivo é que o estado da rede seja atualizado o mais rápido possível.

Suponha no cenário da Figura 3.8 que após o nó C entrar no alcance de detecção de portadora do nó A, ambos verifiquem que seu Tempo Livre Disponível (T_L) é menor do que T_S e interrompam os dois fluxos. Esta situação não é a ideal já que bastaria que

um dos fluxos fosse interrompido. Para reduzir este problema, além da utilização do código diferente no cabeçalho da mensagem *Hello*, que tem como objetivo fazer com que a informação atualizada de T_o de um nó seja propagada o mais rápido possível para seus vizinhos, um outro artifício foi implementado. O intervalo de tempo em que as medições são efetuadas pelos nós para verificar seu T_L é feito de forma aleatória. Cada nó sorteia um valor dentro de um intervalo de forma a aumentar a probabilidade de a rede atualizar suas informações antes de um segundo nó disparar uma nova mensagem *ICMP QoS Lost*.

Os nós da cadeia de encaminhamento, ao receberem a mensagem *ICMP QoS Lost*, removem de suas tabelas de roteamento a rota associada ao fluxo que será interrompido. Desta forma os pacotes que ainda estiverem em trânsito serão descartados na camada de roteamento. Após receber a mensagem *ICMP QoS Lost* o nó fonte interromperá o tráfego e transmitirá um novo pedido de rota para descobrir um novo caminho com recursos suficientes.

Capítulo 4

Diferenciação de Tráfego

No capítulo anterior foi mostrado que o objetivo do controle de admissão é garantir que um fluxo que exija QoS só será admitido na rede, caso existam recursos disponíveis suficientes para atender a sua requisição e não interferir nos fluxos QoS pré-existentes. Como o pedido de rota para fluxos BE não passa pelo controle de admissão, cabe à camada MAC prover algum mecanismo de forma a priorizar os tráfegos QoS em relação aos do tipo BE.

4.1 IEEE 802.11e

De acordo com Imad [7], podemos obter uma diferenciação de serviço entre tráfegos no IEEE 802.11 quando utilizando o mecanismo DCF, através das técnicas citadas na seção 2.4.

O IEEE 802.11 convencional não suporta o conceito de diferenciação de serviço. Basicamente, utilizando o mecanismo DCF todas as estações que disputam o acesso ao meio têm uma probabilidade igual de sucesso ao tentarem transmitir um quadro. Entretanto, esta probabilidade de acesso ao meio igual para todas as estações não é o ideal se deseja-se transmitir tráfegos com diferentes prioridades.

O protocolo IEEE 802.11e [18] é uma extensão do IEEE 802.11 que introduz meca-

nismos de provisão de QoS na camada MAC. O IEEE 802.11e oferece melhor suporte a QoS do que o 802.11. No IEEE 802.11e, dentro de uma mesma estação várias instâncias do DCF são executadas em paralelo, como se fossem "MACs virtuais" (Figura 4.1). Essas instâncias, definidas como categorias de acesso (*Access Categories* - ACs), executam o procedimento de *backoff* independentemente umas das outras, e competem entre si pelas oportunidades de transmissão.

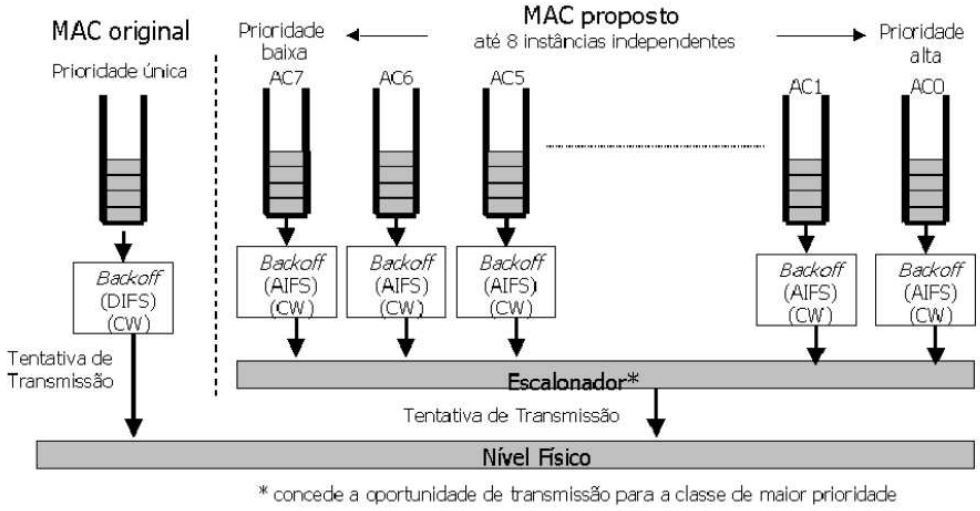


Figura 4.1: Camada MAC do IEEE 802.11e. Figura adaptada de [1]

O padrão IEEE 802.11e aperfeiçoou a subcamada MAC do IEEE 802.11 introduzindo o *Hybrid Coordination Function* (HCF), o qual inclui 2 métodos de acesso ao meio: o *Hybrid Controlled Channel Access* (HCCA) e o *Enhanced Distributed Channel Access* (EDCA). O HCCA é centralizado e gerencia o acesso ao meio usando um Ponto de Acesso com QoS (*QoS Access Point* - QAP), sendo apenas utilizado em redes infra-estruturadas. Já o EDCA é distribuído e pode ser usado em redes ad hoc, as quais são o foco deste trabalho.

O EDCA provê diferenciação e acesso distribuído ao meio utilizando 8 tipos diferentes de prioridades de tráfego, os quais são associados a 4 diferentes tipos de *ACs*. Desta forma um ou mais tipos de tráfegos podem ser associados à mesma *AC*.

A tabela 4.1 mostra os diferentes tipos de tráfego e as *ACs* às quais os tráfegos são associados [18].

UP	Designação	AC	Tipo
1	BK	AC_BK	*Background*
2	-	AC_BK	*Spare*
0	BE	AC_BE	*Best Effort*
3	EE	AC_BE	*Excellent Effort*
4	CL	AC_VI	*Controlled Load*
5	VI	AC_VI	*Video*
6	VO	AC_VO	*Voice*
7	NC	AC_VO	*Network Control*

Tabela 4.1: Tipos de tráfegos e *ACs* associadas.

Basicamente, cada *AC* possui um conjunto de parâmetros $AIFS$ [*AC*], CW_{min} [*AC*] e CW_{max} [*AC*] ao invés de $DIFS$, CW_{min} e CW_{max} usados no DCF para controlar o acesso ao meio. A diferenciação entre *ACs* é obtida variando-se estes parâmetros, fazendo com que as *ACs* mais prioritárias acessem o meio mais rápido do que as de menor prioridade.

Cada *AC* dentro de uma estação disputa o acesso ao meio independentemente e inicia o decremento do *backoff* após o meio ficar ocioso por um período de tempo $AIFS$ (*Arbitration Inter-frame Space*). O $AIFS$ é pelo menos igual a $DIFS$ para a categoria de mais alta prioridade, e pode ser aumentado individualmente para as *ACs* de menor prioridade. A Figura 4.2 ilustra as relações dos valores de $AIFS$ com os outros intervalos entre-quadros já definidos.

O valor de $AIFS$ de uma categoria de acesso é calculado pela equação

$$AIFS[AC] \;=\; AIFSN[AC] * SlotTime + SIFS\,, \tag{4.1}$$

onde $AIFSN[AC]$ é uma constante individual de cada *AC*, 1 $SlotTime$ é igual a $20\mu s$ e $SIFS$ é igual a $10\mu s$ de acordo com [19].

Apesar de cada *AC* ter diferentes conjuntos de parâmetros que controlam o acesso ao meio, existe a possibilidade de duas ou mais *ACs* tentarem transmitir simultaneamente,

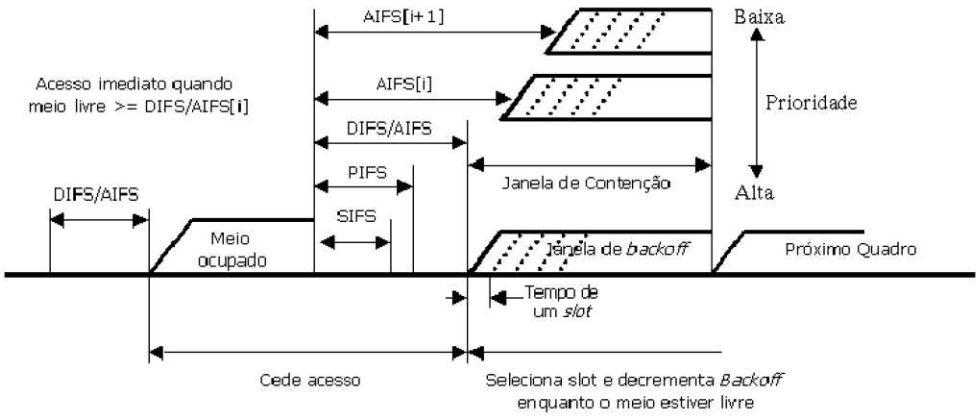


Figura 4.2: Relações dos intervalos entre-quadros no IEEE 802.11e.

ocasionando uma "colisão virtual" na estação. O IEEE 802.11e evita esta colisão interna através do escalonador (Figura 4.1), o qual garante o acesso ao meio à *AC* de maior prioridade. As *ACs* de menor prioridade comportam-se como se tivesse ocorrido uma colisão no meio, incrementando seus contadores de *backoff* e aguardando um novo período $AIFS$ [*AC*] para começar a decrementá-los.

Um conceito importante no 802.11e é o de oportunidade de transmissão (*Transmission Opportunity* - TXOP). Durante uma TXOP (a estação conseguiu acessar o meio), a estação pode enviar vários quadros em rajada, separados por SIFS, sem ter que disputar o meio quadro a quadro. O intervalo de tempo em que a estação pode permanecer transmitindo os quadros não pode exceder o parâmetro *TXOP Limit* definido para cada *AC*(Tabela 4.2). A *TXOP Limit* maior que 0 (zero) significa que a estação pode transmitir múltiplos quadros desde que estas transmissões não se estendam além do *TXOP Limit*. A *TXOP Limit* igual 0 (zero) implica que a estação só pode enviar um quadro de cada vez.

Uma outra diferença entre o DCF e o EDCA é como o *backoff* é decrementado. No EDCA o primeiro slot é decrementado no final do intervalo de tempo $AIFS$ [*AC*]. Já no DCF o primeiro decremento só ocorre no final do primeiro slot após o intervalo $DIFS$. Esta modificação faz com que as estações de mais alta prioridade que utilizam o EDCA, consigam acessar o meio na frente de estações que utilizam o DCF, quando ambas possuem o mesmo número de fatias de tempo a ser decrementado após um período $AIFS$ ou $DIFS$.

A Tabela 4.2 mostra os parâmetros utilizados pelo EDCA, quando utilizada a camada física DSSS do IEEE 802.11b.

	AC	$AIFSN$	CW_{min}	CW_{max}	$TXOPLimit$
Alta prioridade ⇓ Baixa prioridade	AC_VO	2	7	15	3.264ms
	AC_VI	2	15	31	6.016ms
	AC_BE	3	31	1023	0
	AC_BK	7	31	1023	0

Tabela 4.2: Valores de CW_{min}, CW_{max}, $AIFSN$ e $TXOPLimit$ utilizados pelas ACs.

No IEEE 802.11e os pacotes de controle do protocolo de roteamento são associados a *AC* de mais alta prioridade (AC_VO).

No TDAC os tráfegos que exigem QoS são associados à *AC* de mais alta prioridade (AC_VO) e os tráfegos BE são associados à *AC* de mais baixa prioridade (AC_BK). Os valores de CW_{min} e CW_{max} da categoria de acesso AC_VO são iguais a 7 e 15 respectivamente (Tabela 4.2). Desta forma, esta *AC* só possui dois estágios de *backoff* fazendo com que a janela de contenção (CW) não seja incrementada caso ocorra mais de uma colisão na tentativa de transmitir um quadro.

Capítulo 5

Simulações

O objetivo principal das simulações realizadas é obter e avaliar os resultados do mecanismo proposto e compará-lo com outros mecanismos encontrados na literatura.

A ferramenta de simulação empregada foi o *Network Simulator* (NS) [36]. O *Network Simulator* é um simulador orientado a eventos, desenvolvido no Projeto VINT (*Virtual InterNetwork Testbed*) com o suporte da DARPA (*Defense Advanced Research Projects Agency*), e com a colaboração de pesquisadores de centros de pesquisa e universidades como UCB (*University of California at Berkeley*), LBL (*Lawrence Berkeley National Laboratory*), USC/ISI (*University of Southern California / Information Sciences Institute*), e Xerox PARC (*Palo Alto Research Center*). O núcleo do simulador é escrito em C++. Uma outra linguagem orientada a objetos chamada OTcl é utilizada para estabelecer uma interface de comando e configuração. Essa linguagem auxiliar é interpretada, permitindo que os *scripts* de simulação sejam escritos e modificados sem necessidade de recompilar todo o código do simulador.

O NS é um simulador baseado em eventos. O escalonador seleciona o próximo evento agendado, executa-o inteiramente e retorna para executar o próximo evento. O simulador executa somente um evento de cada vez, isto é, em qualquer instante de tempo, somente um evento estará sendo executado. Se mais de um evento estiver programado para executar no mesmo tempo, o primeiro evento agendado será realizado e em seguida o outro.

O modelo de propagação via rádio utiliza o modelo de atenuação *Free-space* para cur-

tas distâncias e uma aproximação para o modelo *Two Ray Ground* para grandes distâncias. É utilizada, também, uma antena omnidirecional.

O pacote do NS-2 disponibiliza um programa gerador de cenários (*setdest*), que utiliza o modelo de mobilidade *random way point*. Neste modelo, cada nó escolhe aleatoriamente um destino, dentro da área de simulação, para o qual ele deve se dirigir a uma velocidade uniformemente distribuída dentro do intervalo entre zero e um valor máximo determinado. Após a chegada ao destino, o nó deve aguardar por um determinado intervalo de tempo, denominado tempo de pausa, previamente definido. Após o tempo de pausa o nó escolhe um novo destino e uma nova velocidade, com a qual ele se movimentará, e assim por diante.

5.1 Modificações realizadas no NS-2

Ao implementarmos o TDAC-AODV no simulador, foi necessário a modificação de algumas partes do código. Para implementar o controle de admissão as principais modificações ocorreram no código do protocolo AODV. Na implementação do IEEE 802.11e, utilizamos o código elaborado por Wiethölter e Hoene [37]. A camada física do NS-2 foi modificada para que fosse possível obter diferentes alcances de transmissão para as taxas de 2 Mb/s e 11 Mb/s. Os valores atribuídos foram obtidos dos resultados experimentais em [33] e estão descritos na Tabela 5.1.

5.2 Avaliação

A versão do NS-2 utilizada foi a 2.27. Todos os nós são equipados com interface de redes IEEE 802.11b operando a 11 Mbps para a transmissão de dados e a 2 Mbps para as mensagens de difusão. As simulações foram realizadas em três fases. Na primeira e segunda fases, os nós são estáticos e posicionados de forma aleatória. Foram realizadas 75 rodadas e em cada rodada o posicionamento dos nós é alterado. Nestas fases o TDAC foi comparado com o SWAN [3] e com a implementação do IEEE 802.11e para o NS-2 disponibilizada pelo Grupo de Redes e Telecomunicações da Universidade de Berlin [37].

Tanto no TDAC quanto no IEEE 802.11e o $TXOPLimit$ para todas as *ACs* foi configurado para 0 (zero) de forma que apenas um quadro é transmitido por TXOP. Na terceira fase foi verificada a eficiência do mecanismo de controle de violação de QoS do TDAC, sendo comparado o desempenho do TDAC com e sem o mecanismo de controle de violação de QoS implementado. Em todas as fases os gráficos plotados contêm barras de erros correspondentes a um de intervalo de confiança de 95% em relação à média das medidas.

Neste trabalho consideramos que os fluxos de QoS são fluxos que utilizam o UDP (*User Datagram Protocol*) e os fluxos BE utilizam o TCP (*Transport Control Protocol*) como protocolos de transporte respectivamente e, só existe dois tipos de tráfego na rede: QoS ou BE.

5.3 SWAN (*Stateless Wireless Ad Hoc Networks*)

O SWAN [3] utiliza um algoritmo de controle distribuído para prover diferenciação de serviço. Um controle de admissão baseado no nó fonte é responsável por gerenciar os fluxos QoS. Já para os fluxos BE, existe um controle de taxa para regular a taxa de transmissão destes fluxos, de forma prevenir que os fluxos BE degradem o desempenho dos fluxos QoS.

5.3.1 Controle de Taxa dos Fluxos BE

O SWAN utiliza um controle de taxa AIMD (*Additive Increase, Multiplicative Decrease*) que opera em função do intervalo de tempo entre a transmissão de um quadro e o recebimento do respectivo reconhecimento (ACK). Um nó vai aumentando sua taxa de transmissão (*Additive Increase*) até que o controle de taxa detecte que o intervalo de tempo entre a transmissão e o recebimento do reconhecimento de um quadro está acima de um valor pré-definido. Neste caso, o nó reduz sua taxa de transmissão (*Multiplicative Decrease*). O principal objetivo do controle de taxa é tentar evitar que os fluxos BE interfiram nos fluxos QoS.

5.3.2 Controle de Admissão dos Fluxos QoS

No SWAN, os nós intermediários não participam da decisão de controle de admissão. A decisão é feita exclusivamente pelo nó fonte do tráfego QoS. O controle de admissão do nó fonte envia uma mensagem (*probing request packet*) para o nó de destino, com o objetivo de obter o valor da largura de banda fim-a-fim disponível. Cada nó intermediário entre o nó fonte e o nó de destino, ao receber a mensagem, atualiza o valor do campo *bottleneck bandwidth* da mensagem, caso a sua largura de banda disponível seja menor que o valor contido no campo. O nó de destino, ao receber a mensagem, envia uma mensagem de resposta para o nó fonte, com o valor do campo *bottleneck bandwidth* copiado da mensagem *probing request*. Ao receber a mensagem enviada pelo nó de destino, o controle de admissão do nó fonte pode decidir se aceita ou não a entrada de um novo fluxo QoS, simplesmente comparando a largura de banda fim-a-fim disponível com a carga requisitada pela aplicação. Porém, os cálculos realizados pelo o controle de admissão do SWAN não levam em conta a largura de banda consumida pelos nós situados entre o alcance-TX e o alcance-CS (Figura 3.4) e o efeito da interferência intra-fluxo na carga requisitada pela aplicação.

5.4 Métricas

Diferentes métricas de desempenho são utilizadas nas simulações. A primeira métrica utilizada é a Taxa de Entrega (T_E), definida como a razão entre o número de pacotes recebidos pela camada de aplicação do nó de destino (R) e o número de pacotes entregues à camada MAC do nó fonte (T) e, portanto, é dada por

$$T_E \;=\; \tfrac{R}{T}\,. \tag{5.1}$$

São contabilizados em T, apenas os pacotes pertencentes aos fluxos que efetivamente possuam uma rota para o destino. Estes pacotes podem ser descartados por transbordos da fila de transmissão da camada MAC (*Interface Queue*), caso a rede esteja operando na saturação, ou seja, admitindo mais carga do que a rede pode suportar ou por atingir

o número máximo de tentativas de transmissão. Os pacotes descartados na camada de roteamento devido aos fatores citados no item 1 da Seção 5.5 não são considerados.

A segunda métrica é o atraso médio fim a fim, definido como a diferença entre o instante de chegada de um pacote na camada de aplicação do nó de destino e o tempo em que o pacote foi gerado pela camada de aplicação no nó de origem. Conseqüentemente, apenas os pacotes que efetivamente chegaram ao destino são levados em conta.

A terceira métrica é o "*Overflow*" (O_f) definido como a razão entre o número de pacotes descartados na camada MAC (D_M), devido ao transbordo de fila, e o número de pacotes entregues à camada MAC do nó fonte (E_M). O objetivo desta métrica é medir o nível de congestionamento da rede e é expressa por

$$O_f = \frac{D_M}{E_M} . \tag{5.2}$$

A quarta métrica é a vazão agregada dos fluxos QoS (V_Q) definida pela razão entre o número de bits recebidos na camada de aplicação de todos os nós de destino de fluxos QoS (R_Q), por um período de tempo em segundos (t), sendo expressa por

$$V_Q = \frac{R_Q(bits)}{t(segundos)} . \tag{5.3}$$

A vazão agregada da rede é uma das métricas mais importantes para avaliar o desempenho de uma rede. Um controle de admissão conservativo aumenta a taxa de entrega mas diminui a vazão agregada da rede.

Vale ressaltar que no caso de ocorrerem quebras de rotas por falhas sucessivas de transmissão, o intervalo de tempo em que a transmissão do fluxo é interrompida (entre a sinalização da quebra de rota pela camada MAC e o restabelecimento da rota pelo nó fonte), não é subtraído do período de medição t.

A quinta métrica é a vazão agregada dos fluxos BE (V_{BE}) definida como a razão entre o número de bits recebidos na camada de aplicação dos nós de destino de fluxos BE (R_{BE}), por um período de tempo em segundos (t). Esta métrica é dada por

$$V_{Be} \quad = \quad \frac{R_{BE}(bits)}{t(segundos)} \; . \tag{5.4}$$

A sexta métrica é a vazão média dos fluxos QoS admitidos na rede (V_{MQ}) definida pela razão entre V_Q e o número de fluxos QoS admitidos pela rede (N_Q). O objetivo desta métrica é verificar o número médio de bits entregues por cada fluxo QoS, sendo expressa por

$$V_{MQ} \quad = \quad \frac{V_Q}{N_Q} \; . \tag{5.5}$$

Nesta métrica, mesmo que um fluxo seja interrompido por uma sinalização de quebra de rota, este fluxo é incluído em N_Q.

5.5 Considerações Iniciais

Para melhor compreensão dos resultados expostos nos gráficos obtidos nas simulações, devem ser ressaltados alguns pontos importantes.

1. Quando uma aplicação é iniciada, os pacotes gerados são enviados para a camada de roteamento do nó fonte, onde são armazenados em uma fila até a conclusão do processo de descobrimento de rota, realizado pelo protocolo de roteamento AODV. O nó fonte, ao receber a mensagem de resposta do pedido de rota (RREP), cria uma rota para o nó de destino e envia todos os pacotes armazenados na fila da camada de roteamento para a fila de transmissão da camada MAC, para serem transmitidos. Caso ocorra um atraso grande no estabelecimento da rota ou o nó fonte não receba a mensagem de resposta de rota devido ao nó de destino estar inalcançável ou ainda, no caso do TDAC, o processo de descobrimento de rota ter sido interrompido pela inexistência de recursos suficientes para atender a requisição da aplicação, os pacotes gerados pela aplicação serão descartados na camada de roteamento por transbordo de fila (*overflow*). Isto ocorre porque a fila na camada de rede tem um tamanho finito e porque não é implementada no simulador NS-2 uma sinalização

da camada de roteamento para a camada de aplicação, informando que não foi encontrada uma rota para o destino para que com isso a aplicação interrompesse a geração de pacotes.

2. A camada MAC de um nó, após atingir o número máximo de tentativas (*retry limit*) de transmissão de um quadro e não obter sucesso, descarta o quadro e sinaliza para a camada de rede informando que a transmissão do respectivo quadro falhou. O protocolo AODV, ao receber esta sinalização, interpreta como se tivesse ocorrido uma quebra de rota. Imediatamente o protocolo AODV desativa a rota associada ao nó de destino do quadro, descarta todos os pacotes endereçados ao nó de destino que estão armazenados na fila de transmissão da camada MAC e envia uma mensagem de erro de rota (*Route Error* - RERR) para o nó fonte do quadro. Os nós vizinhos ao receberem a mensagem de erro de rota também desativam as suas rotas para o nó de destino do fluxo e descartam os pacotes endereçados ao nó de destino que estão armazenados em sua fila de transmissão da camada MAC. Já o nó fonte, ao receber a mensagem de erro de rota, além de realizar as ações já citadas, inicia um novo processo de descobrimento de rota para o nó de destino. Desta forma, podemos concluir que mesmo em cenários estáticos podem ocorrer "falsas sinalizações" de quebras de rotas ocasionadas por sucessivas colisões, principalmente em cenários onde a carga da rede está próxima da saturação e o número de estações disputando o acesso ao meio é alto.

3. Em situações em que a carga na rede é alta e é grande o número de nós disputando o acesso ao meio, o desempenho da categoria de acesso (*AC*) de mais alta prioridade (*AC_VO*) sofre uma forte degradação, devido ao alto número de colisões ocasionadas pelo fato de que os valores $CWmin$ e $CWmax$ são pequenos. Essas colisões fazem com que o *AC_VO* tenha um alto índice de descarte de pacotes.

4. A utilização de valores pequenos para $CWmin$ e $CWmax$ é necessária para prover diferenciação de serviço. Entretanto, há um compromisso entre a vazão da rede e a diferenciação de serviço provocado pelos altos índices de colisão.

5. Como no 802.11e os pacotes de controle são associados à *AC_VO*, estes pacotes também sofrem muito com o alto índice de colisões em situações em que a rede

está saturada. Como conseqüência, alguns dos procedimentos de descobrimento de rota podem sofrer um grande atraso. Este atraso pode ocasionar um transbordo de fila na camada de roteamento (item 1).

6. Em cenários onde a carga na rede é baixa, o papel de CW_{max} na diferenciação de serviço é menos significante comparado com CW_{min}. Entretanto, à medida que a carga na rede e o número de nós disputando o acesso ao meio aumenta, a probabilidade de colisões se eleva muito. Portanto, valores mais altos de CW_{max} para as *AC* de mais alta prioridade podem reduzir em muito a probabilidade de colisões e aumentar a desempenho da rede.

   Nas simulações realizadas foi incluída uma versão do TDAC, onde o valor de CW_{max} da *AC* associado aos tráfegos do tipo QoS foi aumentado para 255. Essa versão do TDAC foi chamada de TDAC-mod.

5.6 Primeira fase das simulações

Nesta fase, foram utilizadas oito fontes de tráfego, sendo 4 fontes CBR (QoS) e 4 fontes TCP (BE). A carga oferecida à rede por cada fonte de dados CBR varia de 100 até 400 kbps.

As tabelas 5.1 e 5.2 mostram os parâmetros utilizado na primeira fase das simulações e a configuração dos mecanismos avaliados. Diferentemente do TDAC-AODV, o SWAN e o 802.11e não utilizam em suas implementações a mensagem de controle *Hello* do protocolo AODV, diminuindo assim a sobrecarga na rede.

A Figura 5.1 demonstra a eficiência do controle de admissão proposto pelo TDAC-AODV. Na métrica Taxa de Entrega, somente os pacotes entregues à camada MAC do nó fonte são contabilizados. Os pacotes sem rota para o destino, devido à ação do controle de admissão, não são contabilizados. Na carga oferecida de 100 kbps o comportamento dos protocolos é similar. À medida que incrementa-se a carga oferecida, o número de fluxos QoS rejeitados pelo controle de admissão do TDAC aumenta. Isto evita que a rede sature e como conseqüência, sustenta a taxa de entrega acima de 95%. A alteração do valor de

Número de nós	100
Área de simulação	300 x 300m
Alcance de transmissão 11 Mbps	30m
Alcance de transmissão 2 Mbps	90m
Alcance de detecção da portadora	180m
Protocolo de Roteamento	AODV
Fonte de Tráfego QoS	CBR
Número de Fontes CBR	4
Fonte de Tráfego BE	FTP
Número de Fontes TCP	4
Tamanho do pacote CBR	512 bytes
Tamanho do pacote FTP	1000 bytes
Número de corridas	75

Tabela 5.1: Parâmetros da simulação primeira fase.

CW_{max} implementada no TDAC-mod faz com que a sua Taxa de Entrega seja maior que a do TDAC, porque a probabilidade de sucessivas colisões diminui e conseqüentemente, diminui o número de pacotes descartados na camada MAC e na fila de transmissão da camada MAC devido ao estouro do número de tentativas de transmissão de um quadro (Figura 5.3). A Figura 5.2 traz uma ampliação da Figura 5.1 onde mostra, em detalhes, a diferença entre os resultados obtidos pelo TDAC e TDAC-mod.

Com o aumento da carga na rede, a Taxa de Entrega tanto do SWAN quanto do 802.11e decresce. Isto acontece porque o 802.11e não faz controle de admissão. Já o SWAN realiza controle de admissão, mas não leva em conta os recursos consumidos pelos nós situados entre o alcance-TX e o alcance-CS na estimativa dos recursos disponíveis, nem o efeito da interferência intra-fluxo. Como conseqüência, ambos aceitam mais carga do que a rede pode suportar.

O 802.11e utiliza uma janela de contenção (CW) pequena e não incrementa após sucessivas colisões, isso faz com que ocorram muitas colisões quando a rede está saturada, ocasionando sucessivas falhas de transmissão e conseqüentemente provocando um alto

Configuração	TDAC	SWAN	802.11e
RTS/CTS	NÃO	NÃO	NÃO
Protocolo MAC	802.11e	802.11	802.11e
Uso mensagem *Hello* do AODV	Sim	NÃO	NÃO
Quebra de rota pela camada MAC	SIM	SIM	SIM
Controle de Admissão	SIM	SIM	NÃO

Tabela 5.2: Configuração dos mecanismos avaliados.

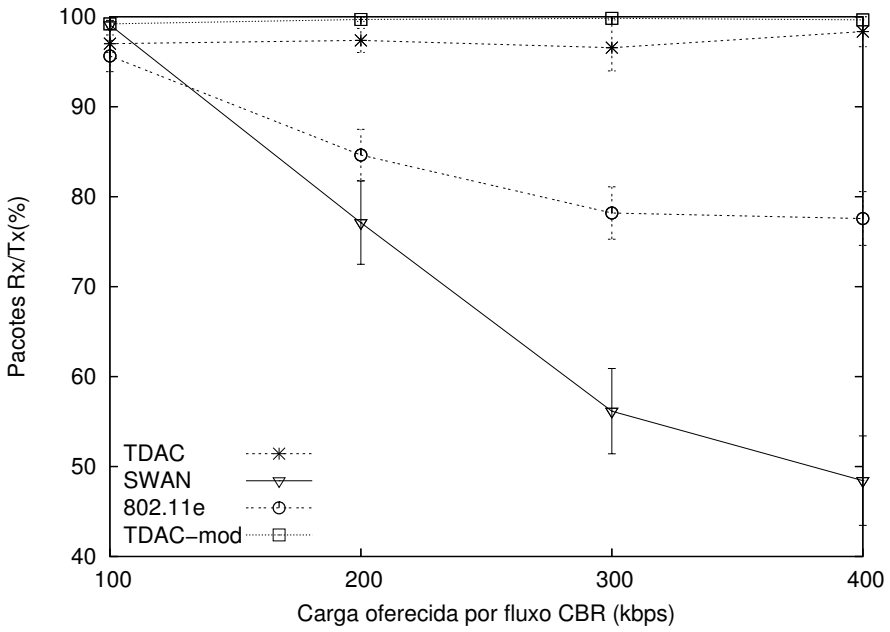


Figura 5.1: Taxa de Entrega.

número de descartes de pacotes na camada MAC e na fila de transmissão da camada MAC, como pode ser observado na Figura 5.3.

Já no SWAN, o número de colisões é bem menor que no 802.11e (Figura 5.3). Isto acontece devido ao SWAN utilizar janelas de contenção maiores, o que diminui em muito a probabilidade de colisões. A grande perda de pacotes no SWAN está relacionada diretamente ao transbordo da fila de transmissão da camada MAC (*overflow*), como pode ser observado na Figura 5.4.

O baixo número de pacotes descartados por transbordo da fila de transmissão da camada MAC no 802.11e (Figura 5.4) deve-se ao fato de que o alto número de colisões

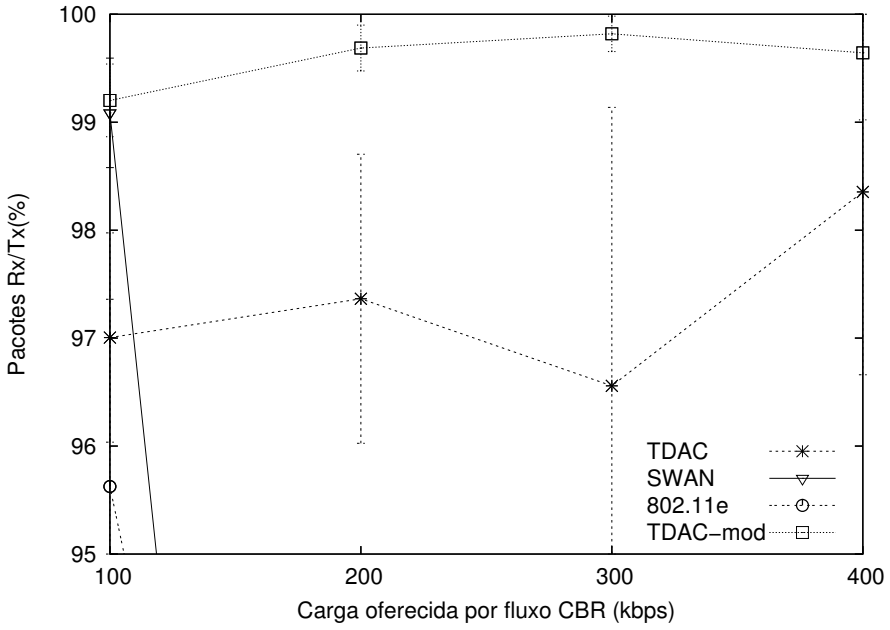


Figura 5.2: Taxa de Entrega do TDAC e TDAC-mod.

sofridas pela *AC_VO* faz com que os pacotes associados a essa *AC* armazenados na fila de transmissão da camada MAC, sejam descartados constantemente e conseqüentemente, não há tempo suficiente para a fila de transmissão da camada MAC transbordar.

A grande diferença de desempenho do 802.11e em relação ao SWAN deve-se ao fato de que o número de colisões no 802.11e é tão grande que em muitos casos o processo de descobrimento de rotas sofre um atraso muito grande para ser concluído. Este atraso faz com que pacotes sejam descartados por transbordo de fila na camada de rede ao invés de serem descartados na fila de transmissão da camada MAC (item 1 da Seção 5.5). A Figura 5.5 mostra a razão entre os pacotes descartados na camada de roteamento dos nós fontes devido à ausência de rotas pelo número de pacotes gerados na aplicação. O alto número de pacotes descartados pelo TDAC é devido a ação do controle de admissão. Pode-se verificar que o 802.11e, mesmo sem a presença de um controle de admissão, tem um número bem maior do que o SWAN de pacotes descartados por ausência de rota para o destino.

A Figura 5.6 mostra que o atraso fim-a-fim obtido com o TDAC permanece abaixo de 60 ms, devido ao controle de admissão não permitir que a rede sature. Um importante ponto que deve ser notado nessa figura é que o atraso fim-a-fim do TDAC-mod não cresceu

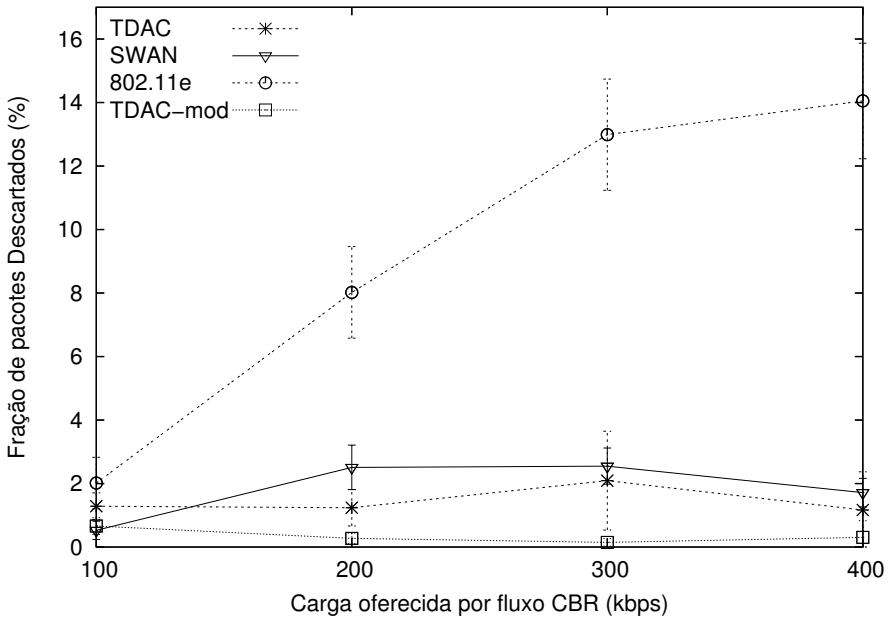


Figura 5.3: Pacotes descartados na camada MAC e fila de transmissão da camada MAC devido a colisões.

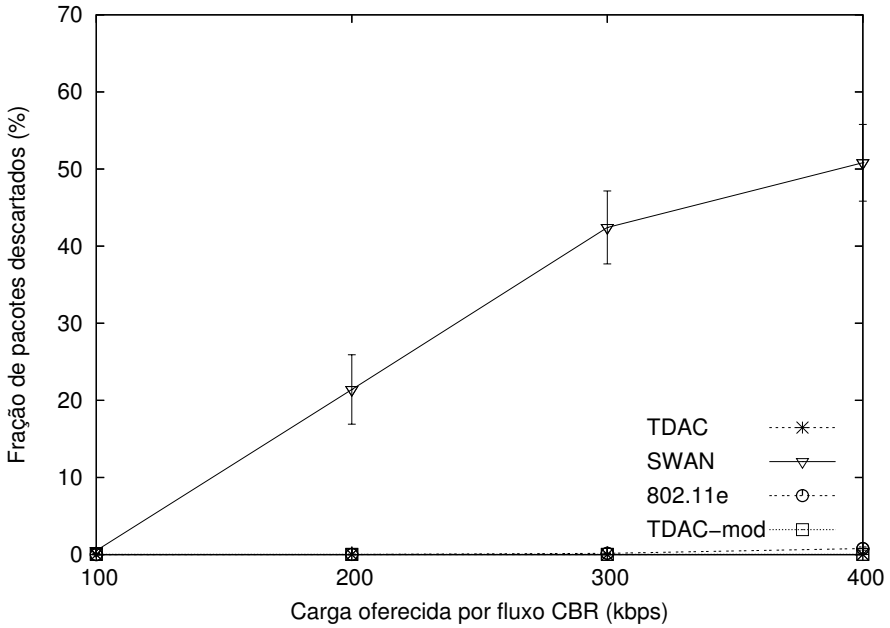


Figura 5.4: Pacotes descartados na camada MAC por transbordo de fila.

em relação ao TDAC (Figura 5.7), mesmo com a alteração do valor de CW_{max}, que aumenta o tempo médio de *backoff* para transmitir um pacote. O aumento no valor de CW_{max} diminui a probabilidade de colisões sucessivas, fazendo com que o número médio de tentativas de transmissão de um pacote no TDAC-mod seja menor que no TDAC.

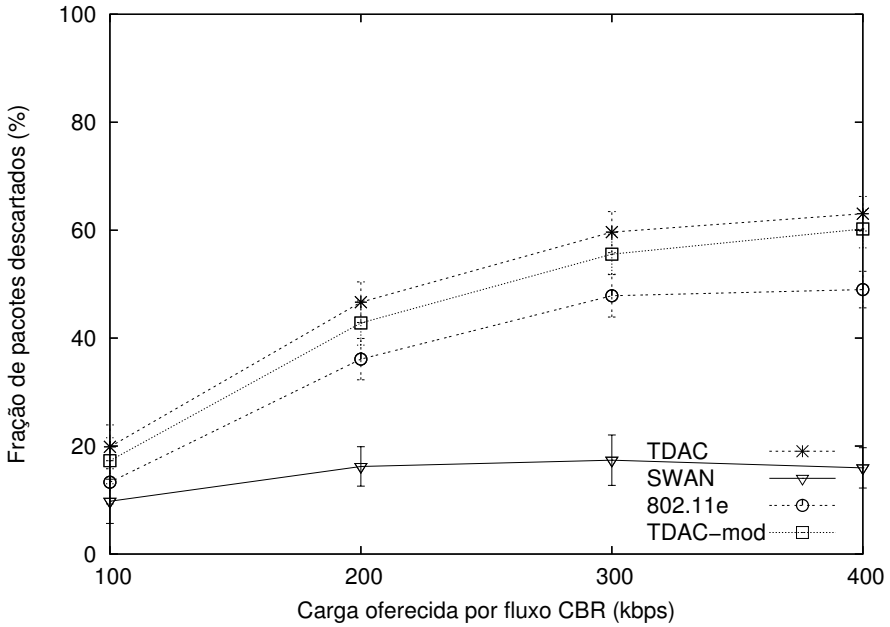


Figura 5.5: Pacotes descartados na camada de rede.

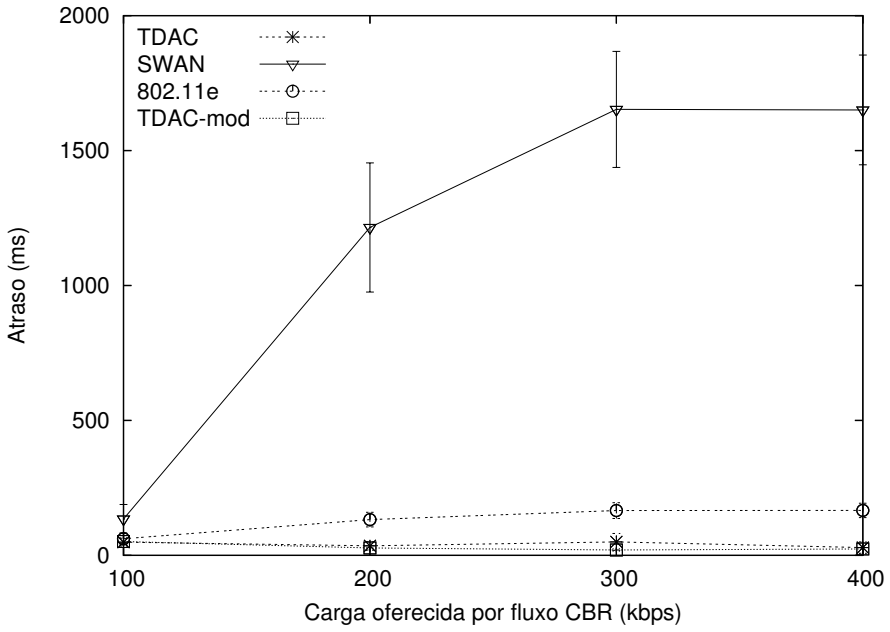


Figura 5.6: Atraso fim-a-fim.

O atraso fim-a-fim do SWAN cresce de forma acentuada devido ao total de carga admitida na rede ser superior à sua capacidade, o que provoca acúmulo de pacotes em filas. Novamente, a grande diferença dos resultados obtidos nesta métrica pelo SWAN e pelo 802.11e deve-se ao fato do alto número de colisões no 802.11e e não ao mecanismo de diferenciação de serviços implementado no 802.11e. Com a saturação da rede, tanto

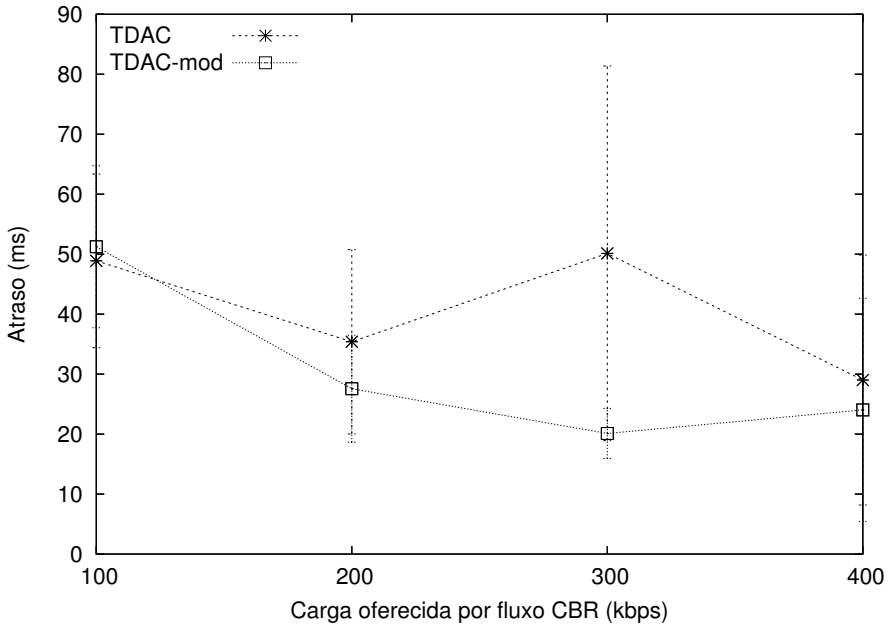


Figura 5.7: Atraso fim-a-fim do TDAC e TDAC-mod.

o SWAN como o 802.11e acumulam pacotes na fila de transmissão da camada MAC. A diferença é que no 802.11e, devido ao alto número de falhas de transmissão, a fila de transmissão da camada MAC "esvaziam" com uma freqüência muito maior que no SWAN (Figura 5.3) e, conseqüentemente, os atrasos dos pacotes que estavam armazenados não são contabilizados.

Devido à grande influência das sucessivas falhas de transmissão nos resultados das métricas Taxa de Entrega e Atraso fim-a-fim, principalmente no 802.11e, e pelo fato do TDAC utilizar o protocolo 802.11e em sua camada MAC, o que poderia também estar influenciando os seus resultados, foram realizadas simulações com o mesmo cenário mas com a inibição de quebras de rota. Após atingir o número máximo de tentativas de transmissão, sem sucesso, o pacote é descartado mas a camada MAC não sinaliza para a camada de rede (item 2 da Seção 5.5).

As Figuras 5.8 e 5.9 mostram que a desempenho do TDAC e do TDAC-mod estão diretamente ligados à eficiência do controle de admissão proposto, visto que não ocorreram mudanças nos seus resultados. Em contrapartida, o 802.11e teve o seu desempenho degradado nas duas métricas por não existir mais descartes de pacotes na camada de rede por atraso no restabelecimento de rotas (Taxa de Entrega) e não haver mais descartes de

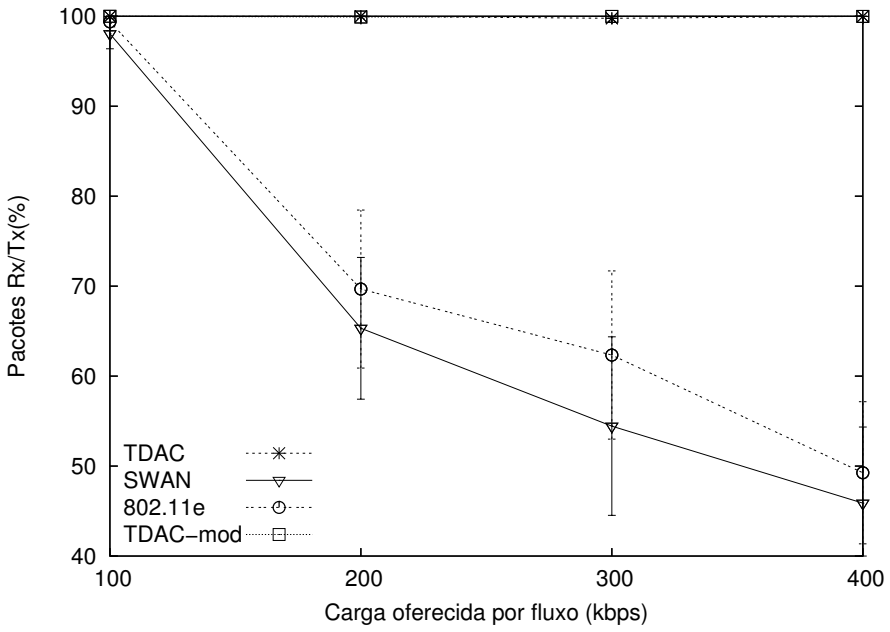


Figura 5.8: Taxa de Entrega com inibição de quebra de rota.

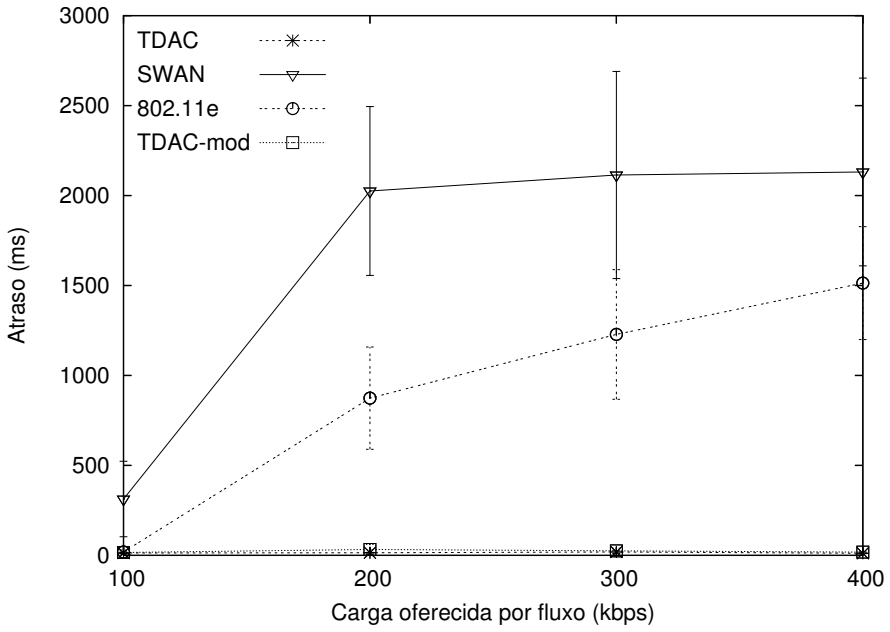


Figura 5.9: Atraso fim-a-fim com inibição de quebra de rota.

pacotes na fila de transmissão da camada MAC devido a “falsas sinalizações” de quebras de rota (Atraso fim-a-fim). Ainda assim, o mecanismo de diferenciação de serviço do 802.11e obteve um resultado melhor que o controle de taxa de transmissão dos fluxos BE proposto no SWAN.

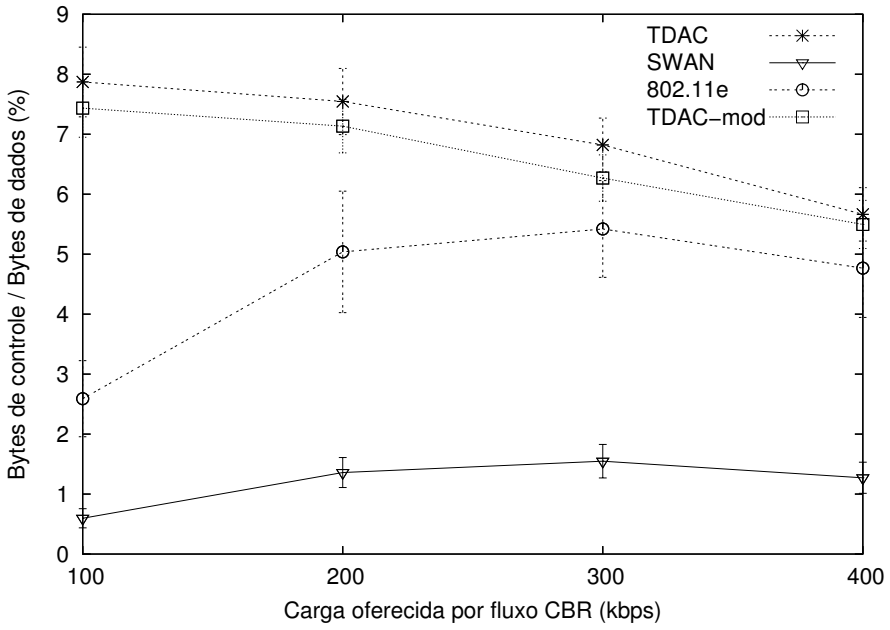


Figura 5.10: Taxa de sobrecarga.

A Figura 5.10 mostra a sobrecarga na rede. O funcionamento do controle de admissão do TDAC exige o uso da mensagem *Hello* do AODV para disseminar as informações sobre o tempo ocupado por transmissões e ainda, a utilização de novos campos nas mensagens de pedido de rota (RREQ) e resposta de rota (RREP) do AODV. Por outro lado, à medida que a carga oferecida vai sendo incrementada, o controle de admissão do TDAC restringe a entrada de novos fluxos (Figura 5.5) reduzindo a transmissão desnecessária de mensagens RREQ e RREP e fazendo com que a taxa de sobrecarga diminua. No 802.11e, o número de colisões cresce com o aumento da carga oferecida à rede, portanto o número de quebras de rotas cresce e conseqüentemente, aumenta o número de transmissões de mensagens de erro de rota (REER) e de descobrimento de rota (para restabelecer as rotas), aumentando a sobrecarga da rede. No SWAN, somente durante o estabelecimento de uma rota é que os pacotes de controle do mecanismo são utilizados. Como o número de quebras de rotas do SWAN é bem inferior ao 802.11e, a sobrecarga provocada pelo SWAN é pequena.

A Figura 5.11 mostra a vazão agregada dos fluxos QoS. Os resultados do TDAC-mod foram superiores aos dos TDAC em até 15%, mostrando que o incremento de CW após sucessivas colisões aumenta a probabilidade de sucesso na transmissão de um pacote, sem

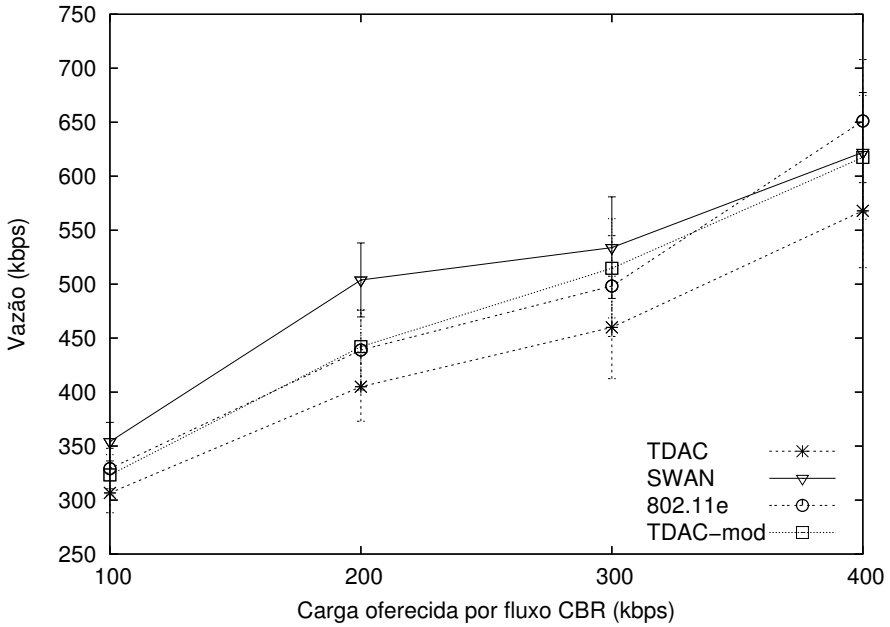


Figura 5.11: Vazão Agregada dos Fluxos QoS.

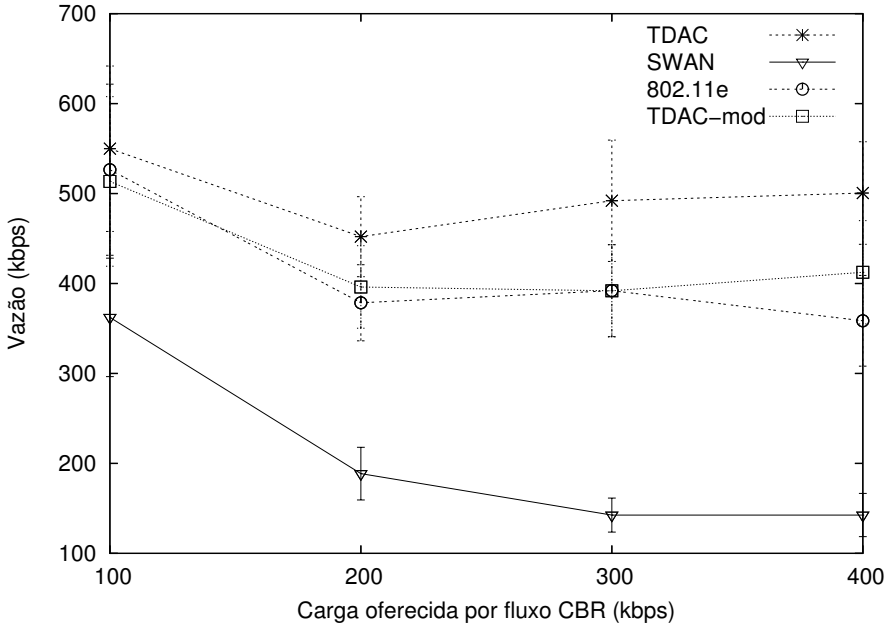


Figura 5.12: Vazão Agregada dos Fluxos BE.

prejudicar o atraso fim-a fim (Figura 5.7). O controle de admissão do TDAC, faz com que um número maior de fluxos QoS sejam rejeitados em comparação com o SWAN, pois o cálculo de recursos disponíveis é mais preciso (Figura 5.5). Em contrapartida, a rejeição maior de fluxos QoS faz com que mais recursos estejam disponíveis para os fluxos BE, como pode ser visto na Figura 5.12. No SWAN, o controle de admissão mais

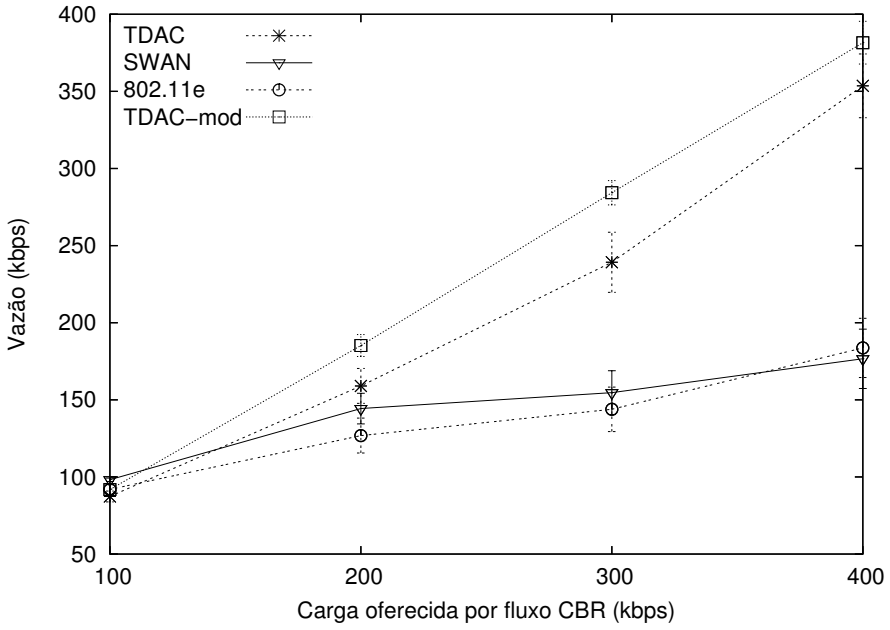


Figura 5.13: Vazão média dos Fluxos QoS.

frouxo resulta em uma vazão agregada maior (Figura 5.11), mas sem garantias de que os fluxos QoS admitidos irão atingir o nível de serviço desejado. Isto pode ser comprovado através da Figura 5.13, que mostra a vazão média dos fluxos QoS admitidos pela rede. Os resultados do TDAC são superiores principalmente quando aumenta-se a carga oferecida.

Apesar de o cenário ser estático, ocorrem falsas sinalizações de quebras de rotas, sinalizadas pela camada MAC devido ao estouro no número de tentativas de transmissão de um pacote. Após uma quebra de rota, não existe garantia de que este fluxo será readmitido pela rede ou ainda quanto tempo levará para este fluxo ser readmitido devido a colisões de mensagens de roteamento ou temporizadores utilizados para restringir o número de tentativas de descobrimento de rotas. Estes fatores fazem com que a vazão média obtida pelo TDAC fique um pouco abaixo do valor da carga oferecida pelos fluxos. A Figura 5.14 mostra a mesma métrica, em um cenário com inibição das quebras de rotas. Pode-se constatar que os valores alcançados pelo TDAC são iguais à carga oferecida pelos fluxos, neste caso.

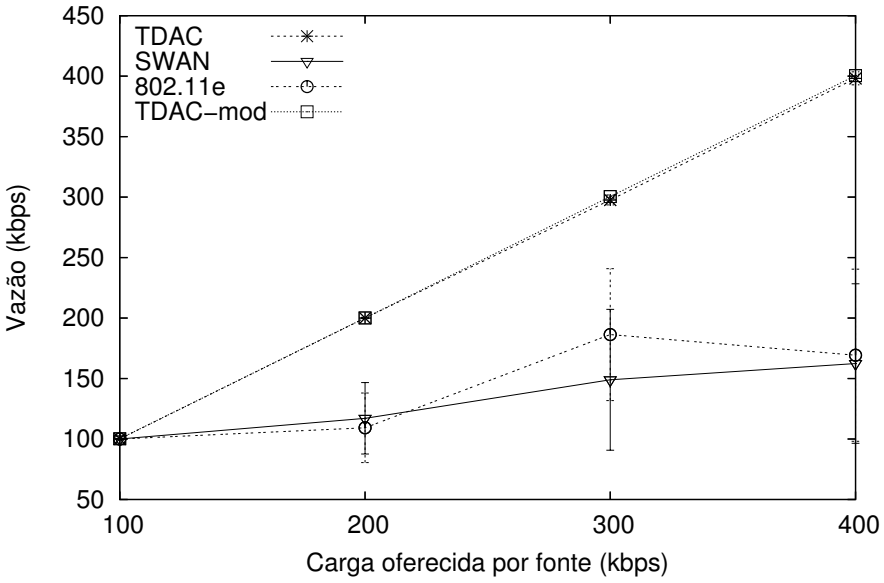


Figura 5.14: Vazão média dos Fluxos QoS sem quebra de rota.

5.7 Resultados da segunda fase das simulações

O objetivo desta fase é verificar se o provisionamento de QoS do TDAC sofre perdas no seu desempenho quando variamos o número de fontes de tráfego BE oferecido à rede. Na primeira fase a razão de fluxos QoS sobre BE era de 1/1 (4 fontes CBR (QoS) e 4 fontes FTP (BE)). Os parâmetros utilizados nesta fase são os mesmos da Tabela 5.1. No cenário utilizado, manteve-se o número de fontes CBR e variou-se o número de fontes FTP de dois (2) até doze (12). A carga oferecida por fonte de fluxo QoS foi fixada em 250 kbps.

As Figuras 5.15 e 5.16 mostram que o desempenho tanto do TDAC quanto do TDAC-mod não sofrem degradações com o aumento do número de fontes de tráfego do tipo BE, mostrando a eficiência do controle de admissão proposto. Pelo fato do controle de admissão restringir a entrada de fluxos CBR (QoS) caso não haja recursos suficientes, a razão efetiva entre o número de fontes CBR e TCP pode ser menor do que a indicada nas figuras. A Figura 5.17 mostra que na razão 1/3, a vazão agregada dos fluxos QoS varia em torno de 500 Kbps ou seja, em média dois (2) fluxos foram admitidos na rede.

A Figura 5.18 mostra a vazão média dos fluxos QoS admitidos pela rede. Mais uma

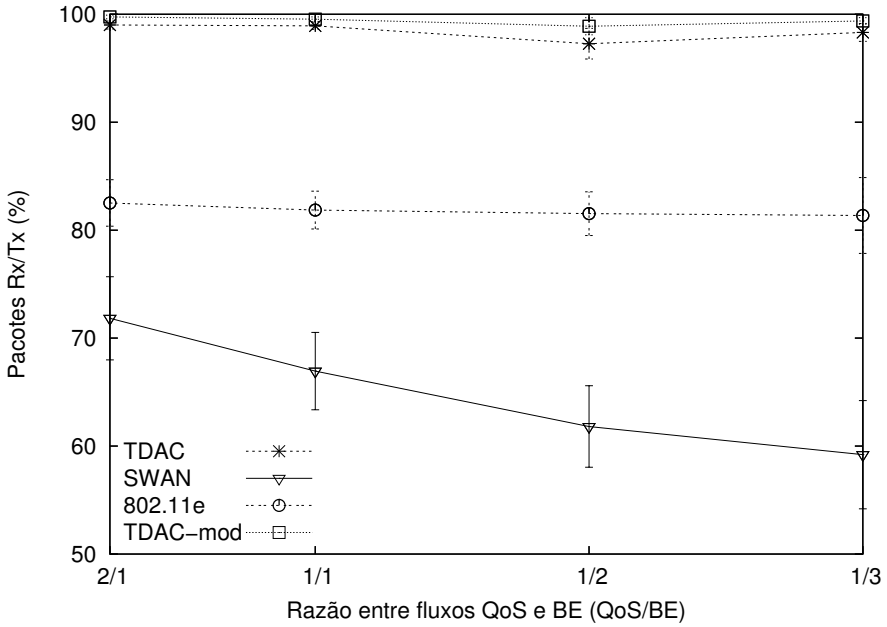


Figura 5.15: Taxa de Entrega.

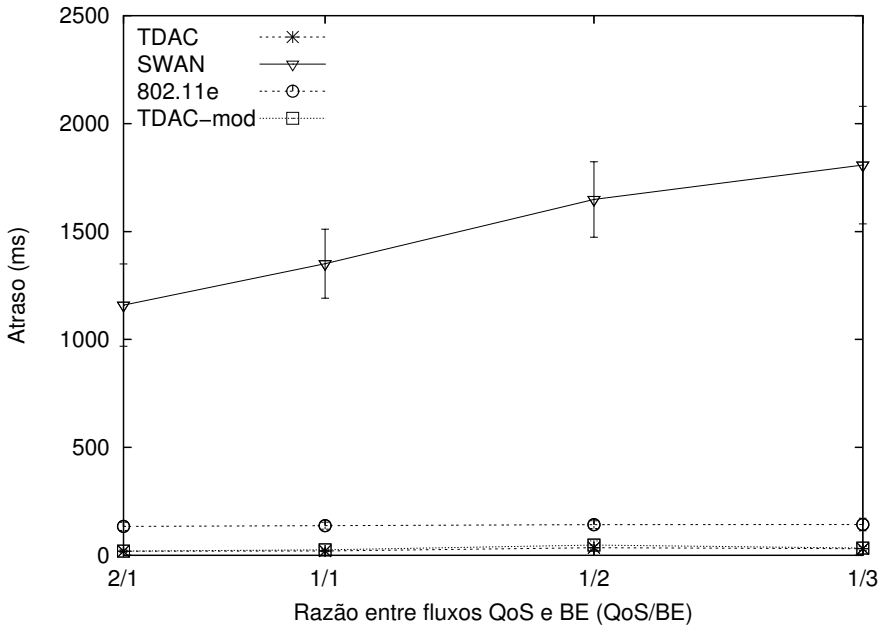


Figura 5.16: Atraso fim-a-fim.

vez, o TDAC-mod teve um desempenho melhor que do TDAC, porém ambos tiveram uma perda à medida que o número de fontes TCP aumentou. Essa perda deve-se mais uma vez as falsas sinalizações de quebra de rota como pode ser comprovado através da Figura 5.19 (com inibição de quebra de rota). Nesta Figura, a vazão média é igual à carga oferecida por cada fonte CBR, comprovando a eficiência do mecanismo proposto.

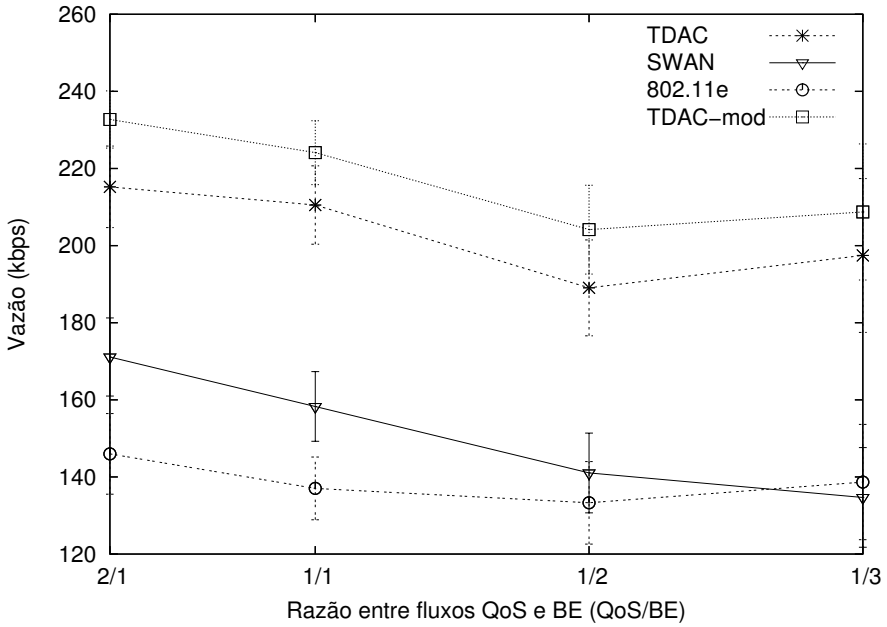


Figura 5.17: Vazão Agregada dos Fluxos QoS.

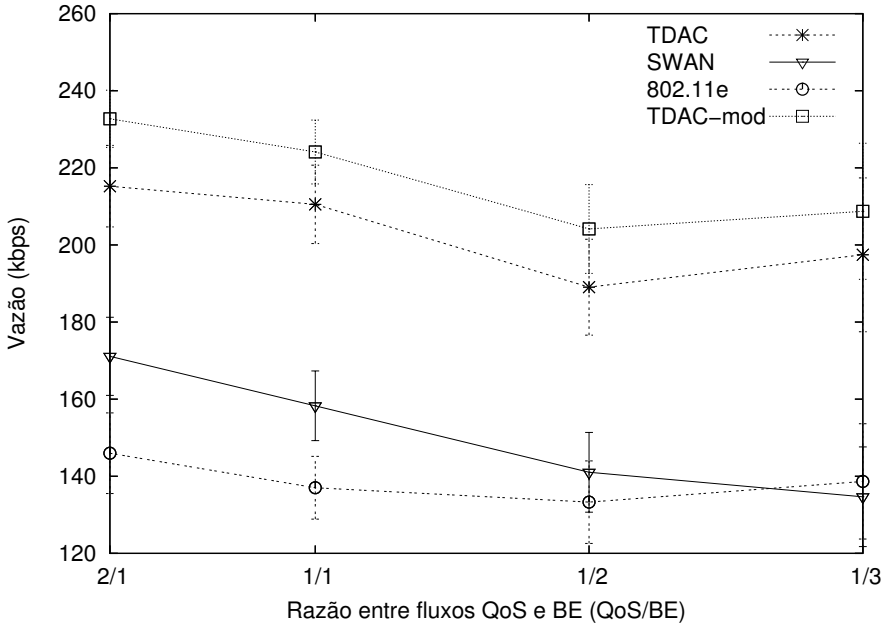


Figura 5.18: Vazão média dos Fluxos QoS.

5.8 Resultados da terceira fase das simulações

Nesta fase o objetivo é verificar a eficiência do mecanismo de controle de violação de QoS proposto no TDAC. A Figura 5.20 mostra o cenário utilizado.

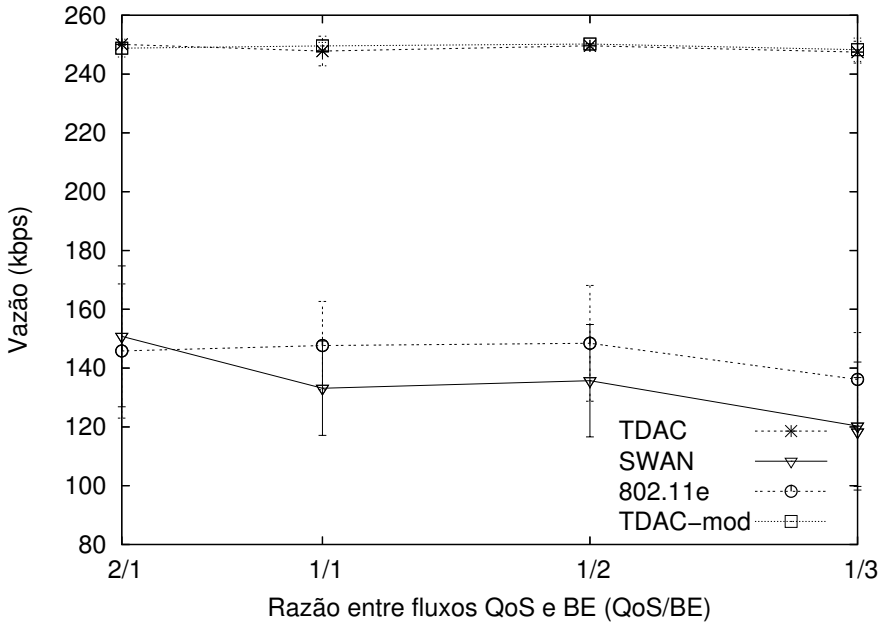


Figura 5.19: Vazão média dos Fluxos QoS sem quebra de rota.

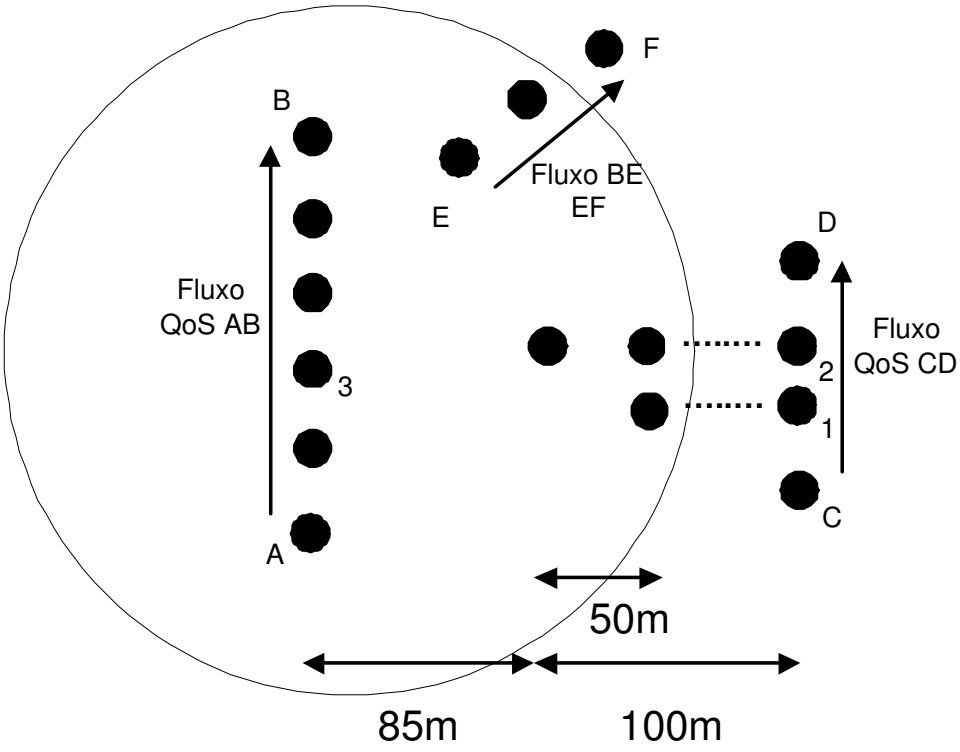


Figura 5.20: Cenário com mobilidade.

Os fluxos QoS AB e CD oferecem uma carga à rede de 1200 kbps e 500 kbps, res-

pectivamente. Inicialmente estes fluxos não disputam os mesmos recursos (O círculo representa o alcance-CS do nó 3). O fluxo *best-effort* EF disputa recursos com ambos os fluxos QoS. Em um determinado instante (20s), os nós intermediários 1 e 2 do fluxo QoS CD movem-se em direção aos nós pertencentes ao fluxo QoS AB. A partir deste momento, os fluxos AB e CD passam a disputar os mesmos recursos. Posteriormente (50s), os nós 1 e 2 afastam-se dos nós pertencentes ao fluxo AB, fazendo com que os fluxos não mais disputem os mesmos recursos.

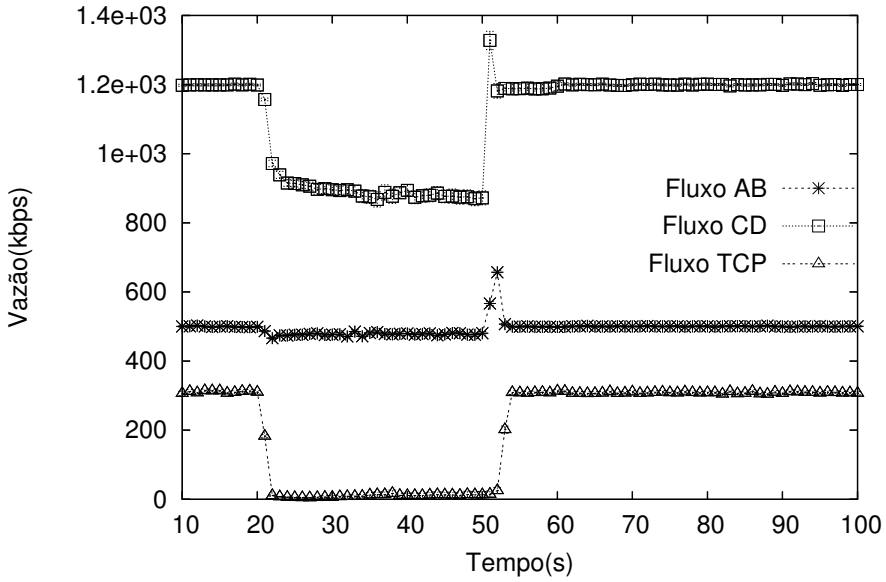


Figura 5.21: Vazão dos Fluxos sem o mecanismo de controle de violação de QoS.

A Figura 5.21 mostra a vazão dos fluxos em função do tempo sem o mecanismo de controle de violação de QoS implementado. Até 20s, os fluxos QoS AB e CD obtêm uma vazão igual à carga oferecida. A partir de 20s, os fluxos QoS passam a interferir um com o outro, fazendo com que sua vazão sofra degradação. O desempenho do fluxo EF sofre degradação porque, até 20s, os fluxos QoS não disputavam recursos e isso significa que ambos podem transmitir simultaneamente, aumentando o tempo livre disponível do fluxo EF. Com a interferência entre os fluxos QoS, não ocorrem transmissões simultâneas e com isso diminui o tempo livre disponível do fluxo EF. Após 50s, os nós 1 e 2 voltam a sua posição original e as vazões dos fluxos voltam a ser iguais ao momento anterior à primeira movimentação.

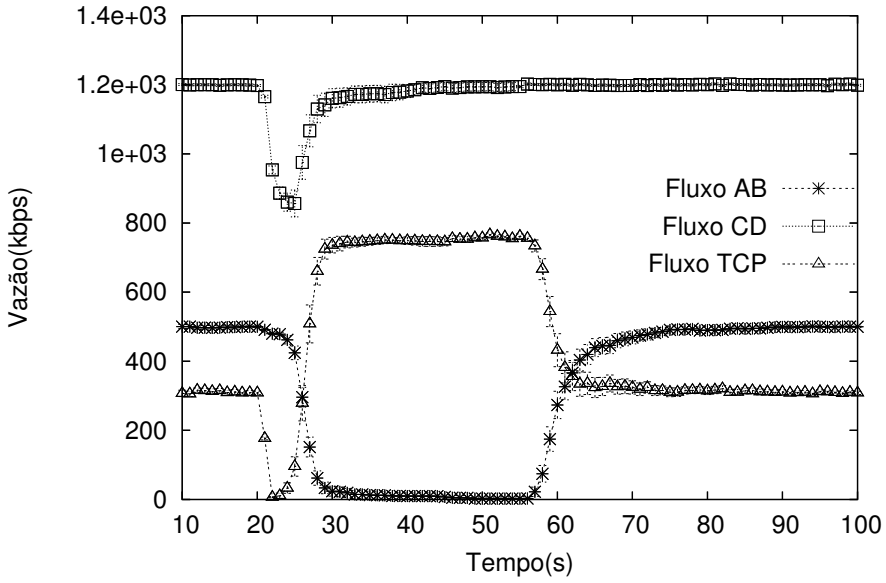


Figura 5.22: Vazão dos Fluxos com o mecanismo de controle de violação de QoS.

A Figura 5.22 mostra a vazão dos fluxos em função do tempo com o mecanismo de controle de violação de QoS implementado. A partir de 20s, as informações da rede são atualizadas de acordo com a nova topologia. Durante o intervalo de tempo entre a atualização da rede e o disparo do mecanismo de violação de QoS, todos os fluxos sofrem uma degradação. Um dos nós pertencentes ao fluxo AB verifica que não suporta mais a carga requisitada e interrompe o fluxo AB, evitando desperdício de recursos. A partir deste momento o fluxo QoS CD volta a entregar a carga oferecida pela sua fonte e o fluxo *Best-Effort* EF aumenta a sua taxa de transmissão, aproveitando um maior número de recursos disponibilizados na rede. A partir de 50s, uma nova atualizacão é feita e os nós pertencentes ao fluxo AB verificam que existe recursos suficientes para suportar o fluxo e o mesmo é readmitido na rede.

Capítulo 6

Conclusões

As redes ad hoc são mais flexíveis e robustas que as redes infra-estruturadas. No entanto, estas redes sem fio possuem características importantes como suporte a mobilidade, o compartilhamento do meio e a descentralização. Estas características tornam a provisão de garantias de Qualidade de Serviço (QoS), em uma rede ad hoc, um problema complexo.

Neste trabalho foi proposto um mecanismo que é capaz de prover garantias de QoS em redes ad hoc IEEE 802.11 em cenários estáticos ou de baixa mobilidade. Na primeira parte deste trabalho é proposto um controle de admissão (*Time-based Admission Control* - TAC-AODV) [15] baseado em uma precisa estimativa dos recursos disponíveis e na interferência intra-fluxo, para admissão ou não de fluxos que exigem requisitos de QoS. O controle de admissão foi adaptado ao protocolo de roteamento AODV. Em seguida foram feitas modificações nos cálculos realizados pelo controle de admissão do TAC-AODV para permitir o seu funcionamento em redes onde coexistem tanto aplicações do tipo QoS com aplicações do tipo melhor esforço (*Best-Effort* - BE). O mecanismo proposto foi batizado de TDAC-AODV (*Traffic Differentiation and Admission Control* - AODV).

O controle de admissão, a diferenciação de tráfego e a monitoração da violação de QoS são componentes chaves para garantir QoS em redes ad hoc IEEE 802.11. O mecanismo proposto no TDAC-AODV combina estes três componentes. A principal contribuição do mecanismo proposto refere-se ao cálculo dos recursos disponíveis quando existem

fluxos que exigem garantias de QoS e melhor esforço na rede e o aperfeiçoamento do cálculo da interferência intra-fluxo em redes IEEE 802.11.

Os resultados de simulação mostraram que o controle de admissão proposto é eficiente, mantendo a Taxa de Entrega muito próxima de 100% e o atraso-fim-a-fim pequeno e aproximadamente constante mesmo em cenários onde a carga da rede era alta. O TDAC-AODV provê com maior eficiência garantias de QoS em relação ao SWAN e o IEEE 802.11e. Os ganhos obtidos pelo TDAC-AODV foram superiores em até 35% em termos de Taxa de Entrega e 10 vezes em atraso fim-a-fim. A modificação no valor de CW_{max} da categoria de acesso de maior prioridade do IEEE 802.11e (TDAC-mod) aumentaram ainda mais esta eficiência, diminuindo o número de sucessivas falhas de transmissão.

O controle de violação de QoS do TDAC mostrou-se eficiente, interrompendo um fluxo QoS o qual não era mais possível atender com o nível de serviço desejado. Esta interrupção assim como a rejeição de novos fluxos QoS, realizados pelo controle de admissão economiza recursos e melhora o desempenho dos fluxos BE.

Como trabalhos futuros, inclui-se implementar no controle de admissão diferentes classes de tráfegos QoS, oferecendo compatibilidade com IEEE 802.11e. Uma investigação mais detalhada sobre os valores de $AIFS$, CW_{min} e CW_{max} atribuídos as categorias de acesso no IEEE 802.11e, com o objetivo de tentar reduzir o número de sucessivas falhas de transmissão devido ao alto número de colisões em cenários onde a carga de fluxos QoS na rede é alta.

Referências Bibliográficas

[1] DE MELO FILHO, J. C. Mecanismos de Controle de Qualidade de Serviço em Redes IEEE 802.11. Tese de Mestrado, Programa de Pós-Graduação de Engenharia de Sistemas e Computação - COPPE/UFRJ, 2003.

[2] IEEE. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. Standard 802.11, 1999.

[3] AHN, G.-S., CAMPBELL, A. T., VERES, A., E SUN, L.-H. Supporting Service Differentiation for Real-Time e Best-Effort Traffic in Stateless Wireless Ad Hoc Networks. Em *IEEE Transactions on Mobile Computing, vol. 1, no. 3, páginas 192-207* (julho de 2002).

[4] KRAVETS, R., E YANG, Y. Contention-Aware Admission Control for Ad Hoc Networks. Em *IEEE Transactions on Mobile Computing, vol. 4, no.4, páginas 363-377* (julho de 2005).

[5] CHAKERES, I. D., E BELDING-ROYER, E. M. Perceptive Admission Control for Mobile Wireless Networks. Em *IEEE QShine* (Dallas, EUA, outubro de 2004).

[6] RENESSE, R., GHASSEMIAN, M., FRIDERIKOS, V., E AGHVAMI, A. Adaptive Admission Control for Ad Hoc and Sensor Networks Providing Quality of Service. Relatório técnico, Center for Telecommunications Research, King's College, Londres, Inglaterra, maio de 2005.

[7] AAD, I., E CASTELLUCCIA, C. Differentiation Mechanisms for IEEE 802.11. Em *IEEE Infocom* (Anchorage, Alasca, abril de 2001).

[8] MANGOLS, S., CHOI, S., MAY, P., KLEIN, O., HIERTZ, G., E STIBOR, L. IEEE 802.11e Wireless Lan for Quality of Service. Em *Proc. European Wireless, vol. 1, páginas 32-39* (Florença, Itália, fevereiro de 2002).

[9] LOHIER, S., E SENOUCI, S.-M. A Reactive QoS Routing Protocol For Ad Hoc Networks. Em *European Symposium on Ambient Intelligence* (novembro de 2003).

[10] SIVAKUMAR, R., SINHA, P., E BHARGHAVAN, V. CEDAR: A Core-Extraction Distributed Ad Hoc Routing Algorithm. Em *IEEE Infocom* (Nova Iorque, EUA, março de 1999).

[11] YING GE, THOMAS KUNZ, L. L. Quality of Service Routing in Ad Hoc Networks Using OLSR. Em *Hawaii International Conference on System Sciences* (Hawaii, USA, 2003).

[12] XIAO, H., SEAH, W. K. G., LO, A., E CHUA, K. C. A flexible Quality of Service Model for Mobile Ad-Hoc Networks. Em *IEEE Vehicular Technology Conference (VTC Spring 2000)* (Tóquio, Japão, maio de 2000).

[13] LEE, S.-B., E CAMPBELL, E. T. INSIGNIA: In-Band Signaling Support for QoS in Mobile Ad Hoc Networks. Em *5th International Workshop on Mobile Multimedia Communications (MoMuC98)* (Berlim, Alemanha, outubro de 1998).

[14] CLAUSEN, T., JACQUET, P., LAOUITI, A., MUHLETHALER, P., QAYYUM, A., E VIENNOT, L. Optimized Link State Routing Protocol. Em *IEEE INMIC* (dezembro de 2001).

[15] CERVEIRA, C. R., E COSTA, L. H. M. K. A Time-based Admission Control Mechanism for IEEE 802.11 Ad Hoc Networks. Em *8th Mobile Wireless Communications Network, páginas 217-228* (Santiago, Chile, agosto de 2006).

[16] PERKINS, C. E., BELDING-ROYER, E. M., E DAS, S. Ad Hoc On-Demand Distance Vector Routing. Em *IETF RFC 3561* (1999).

[17] KRAVETS, R., E YANG, Y. Distributed Qos Guarantees for Realtime Traffic in Ad Hoc Networks. Em *IEEE International Conference on Sensor and Ad Hoc Communications e Networks* (California, EUA, outubro de 2004).

[18] IEEE. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. Standard 802.11e, 2005.

[19] IEEE. *Supplement to part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. Standard 802.11b, 1999.

[20] IEEE. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. Standard 802.11a, 1999.

[21] IEEE. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. Standard 802.11g, 2003.

[22] IEEE. *Carrier Sense with Multiple Access and Colision Detection and Physical Layer (PHY) Specifications*. Standard 802.3, 1998.

[23] VILLELA, B. A. M., E DUARTE, O. C. M. B. Calculating the Maximum Throughput in Multihop Ad Hoc Networks. Em *Lecture Notes in Computer Science - Networking pp. 223-234, vol. 3042, Springer-Verlag* (maio de 2004).

[24] RUBINSTEIN, M. G., E DE REZENDE, J. F. Qualidade de Serviço em Redes 802.11. Em *XX Simpósio Brasileiro de Redes de Computadores (SBRC2002)* (Búzios, RJ, Brasil, maio de 2002).

[25] VELLOSO, P. B., RUBINSTEIN, M. G., E DUARTE, O. C. M. B. Transmissão de Voz em Redes Ad Hoc. Em *Workshop em Qualidade de Serviço e Mobilidade (WQoSM)* (Angra dos Reis, RJ, Brasil, maio de 2003).

[26] VEERARAGHAVAN, M., COCKER, N., E MOORS, T. Support of Voice Services in IEEE 802.11 Wireless LANs. Em *IEEE Infocom* (Anchorage, Alasca, abril de 2001).

[27] BARRY, M. G., CAMPBELL, E. T., E VERES, E. Distributed Control Algorithms for Service Differentiation in Wireless Packet Networks. Em *IEEE Infocom* (Anchorage, Alasca, abril de 2001).

[28] KANG, S.-S., E MUTKA, M. W. Provisioning Service Differentiation in Ad Hoc Networks by the Modification of Backoff Algorithm. Em *Int'l Conference on Com-*

puter Communication e Network (ICCCN) (Scottsdale, Arizona, EUA, outubro de 2001).

[29] BROCH, J., MALTZ, D. A., JOHNSON, D. B., HU., Y. C., E JETCHEVA, J. A performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols.

[30] PERKINS, C. *Ad Hoc Networking, cápitulo 5, páginas 139-172,*. Addison-Wesley Company, 2001.

[31] CHEN, L., E HEINZELMAN, W. B. Qos-Aware Routing Based on Bandwidth Estimation for Mobile Ad Hoc Networks. Em *IEEE Journal on Selected Area in Communications, vol. 23, no. 3, páginas 561-572* (março de 2005).

[32] DHOUTAUT, D., E LASSOUS, I. Experiments with 802.11b in Ad Hoc Configurations. Em *14th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, páginas 1618-1622* (Beijing, China, 2003).

[33] ANASTASI, G., BORGIA, E., CONTI, M., E GREGORI, E. Wi-Fi in Ad Hoc Mode: A Measurement Study. Em *IEEE International Conference on Pervasive Computing and Communications (PerCom 2004), páginas 145-154* (EUA, março de 2004).

[34] BIANCHI, G. Performance Analisys of the IEEE 802.11 Distributed Coordination Function. Em *IEEE Journal on Selected in Communications, vol. 18 no. 3, páginas 535-547* (março de 2000).

[35] PERKINS, C. Quality of Service for Ad Hoc On-Demand Distance Vector Routing, 2003.
http://people.nokia.net/charliep/txt/aodvid/qos.txt - último acesso em 20/12/2006.

[36] NS-2. The network simulator - ns-2, 2005.
http://www.isi.edu/nsnam/ns/ - último acesso em 10/10/2006.

[37] WIETHÖLTER, S., EMMELMANN, M., HOENE, C., E WOLISZ, A. TKN EDCA Model for ns-2. Relatório técnico, Telecommunication Networks Group, Technische Universität, Berlim, Alemanha, 2006.