MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA
INSTITUTO MILITAR DE ENGENHARIA
CURSO DE MESTRADO EM SISTEMAS E COMPUTAÇÃO

MARCOS GOMES PINTO FERREIRA

UMA ABORDAGEM DE ACESSO EM REDES MESH BASEADA EM CONCEITO DE REPUTAÇÃO

Rio de Janeiro
2008

INSTITUTO MILITAR DE ENGENHARIA

MARCOS GOMES PINTO FERREIRA

UMA ABORDAGEM DE ACESSO EM REDES MESH BASEADA EM CONCEITO DE REPUTAÇÃO

Dissertação de Mestrado apresentada ao Curso de Mestrado em Sistemas e Computação do Instituto Militar de Engenharia, como requisito parcial para obtenção do título de Mestre em Sistemas e Computação.

Orientadores: Prof. Edison Ishikawa - D.Sc.
Prof. Artur Ziviani - Dr.

Rio de Janeiro
2008

INSTITUTO MILITAR DE ENGENHARIA
Praça General Tibúrcio, 80-Praia Vermelha
Rio de Janeiro-RJ CEP 22290-270

F383 Ferreira, M. G. P.

Uma Abordagem de Acesso em Redes Mesh Baseada em Conceito de Reputação/ Marcos Gomes Pinto Ferreira. – Rio de Janeiro: Instituto Militar de Engenharia, 2008.

92 p.: il., graf., tab.

Dissertação (mestrado) – Instituto Militar de Engenharia – Rio de Janeiro, 2008.

1. Redes de computadores. 2. Medições em redes. I. Título. II. Instituto Militar de Engenharia.

CDD 004.6

INSTITUTO MILITAR DE ENGENHARIA

MARCOS GOMES PINTO FERREIRA

UMA ABORDAGEM DE ACESSO EM REDES MESH BASEADA EM CONCEITO DE REPUTAÇÃO

Dissertação de Mestrado apresentada ao Curso de Mestrado em Sistemas e Computação do Instituto Militar de Engenharia, como requisito parcial para obtenção do título de Mestre em Sistemas e Computação.

Orientadores: Prof. Edison Ishikawa - D.Sc.
Prof. Artur Ziviani - Dr.

Aprovada em 08 de Agosto de 2008 pela seguinte Banca Examinadora:

Prof. Edison Ishikawa - D.Sc. do IME - Presidente

Prof. Artur Ziviani - Dr. do LNCC

Prof. Antônio Tadeu Azevedo Gomes - D.Sc., do LNCC

Prof. Morganna Carmem Diniz - D.Sc., da UNIRIO

Rio de Janeiro
2008

Dedico este trabalho

Ao meu Pai Chico Netto “in memoriam”porque sei o quanto de magia existia em sua vida e o quanto seus filhos significavam para ele.

À minha mãe, Thereza, que sempre foi para mim o maior exemplo de vida, esperança e superação e com sua simplicidade soube plantar em meu coração a fé em Deus e a confiança necessária para buscar a realização dos meus sonhos.

À minha esposa, Lucia e à minha filha, Luisa, meus maiores tesouros, que trazem tanta luz e gosto à minha vida, um amor especial ... obrigado pelo carinho e paciência que demonstraram durante estes anos.

À toda minha família e à Conceição ... somos uma família abençoada.

Marcos Gomes Pinto Ferreira

AGRADECIMENTOS

Antes e acima de tudo, agradeço a Deus, pois Ele é o meu pastor e nada me falta. Suas bênçãos me acompanham ao longo de toda a minha vida. "Porque dele, por meio dele e para ele são todas as coisas e a Ele, toda a glória e para sempre."Rm.11.36.

Sei que o meu muito obrigado não é capaz de exprimir com toda a propriedade o meu sentimento de gratidão àquelas pessoas que em especial o destino colocou em meu caminho ao longo deste curso. Este sentimento destaca-se além da mera formalidade, pois alcança no sentido e na essência a verdadeira solidariedade.

Para exprimir melhor a percepção do que tudo isto significa, é fundamental mencionar que o IME em meus tempos de graduação sempre foi um sonho inalcançável, pois a vida me impunha uma jornada dura, onde era importante conciliar o trabalho, necessário para ajudar no sustento de casa, com os estudos noturnos, nem sempre de qualidade. Mas a vida é magnífica e o destino quis que meu currículo fosse aceito no IME e eu submetido a mais esta prova de fé. O caminho para chegar até aqui não foi breve e nem fácil, ao contrário, se caracterizou como uma travessia que parecia não ter fim, onde as forças se esgotavam e o desespero chegava ao extremo, a ponto de achar em muitos momentos, que o melhor a fazer era desistir. Tudo isto principalmente causado pela falta de base acadêmica das minhas formações anteriores e por algumas sérias intercorrências pessoais, que mexeram muito com a minha forma de ver e de viver a vida. O que agora, com a distância de passado, vislumbro que todos estes percalços só aumentaram o brilho desta vitória.

Tudo isto só foi possível pela força da fé em Deus e na capacidade de realização do homem, pela esperança na vida e que apesar de tudo nos mantém firmes e de pé e pela generosa solidariedade dos verdadeiros e valorosos amigos que descobri nesta trajetória do mestrado.

Agradeço a todos que de alguma forma contribuíram com o desenvolvimento desta dissertação, com críticas, idéias, sugestões, ou qualquer outra forma de auxílio. Em especial, eu quero também agradecer algumas pessoas que se tornaram fundamentais ao

longo deste trabalho, às quais dedico algumas palavras, a seguir:

Ao meu orientador Artur Ziviani, uma pessoa muito especial e que sempre demonstrou acreditar em mim. Sua proximidade como pessoa valorizou em muito a convivência do nosso grupo e pude realmente conhecer na essência o que significa ser um verdadeiro mestre. Ao meu orientador Edison Ishikawa agradeço profundamente por ter assumido a orientação desta tese, tendo-me brindado com sua confiança e com importantes colaborações na discussão do trabalho.

Ao Professor Ronaldo Salles, também sou imensamente grato pela amizade e os incentivos recebidos ao longo do curso.

Sou profundamente grato também aos grandes amigos André Castelucio, Bruno Correa e Emanuel Freire, juntos e somente pela grandiosa contribuição de cada um de vocês é que me foi possível chegar até aqui e alcançar este título de Mestre. Sem a força deste time, sem a amizade vivida e consolidada, sem o apoio nos momentos difíceis, sem a cumplicidade nas provações, sem alegria nos bons momentos e sem a ajuda de cada um de vocês eu não teria conseguido. Obrigado.

Quero também agradecer e homenagear os amigos que por diversos motivos ficaram ao longo do caminho e que não puderam chegar até aqui. Um outro momento mais favorável, um outro destino, algo de bom, o bom Deus há de reservar para cada um deles.

Há muito mais a quem agradecer ... A todos aqueles que, embora não nomeados, me ajudaram de alguma forma.

Por fim, agradeço a todos os professores e funcionários do IME - Instituto Militar de Engenharia, em especial do nosso Departamento de Engenharia de Computação (SE/8).

Todos vocês são co-autores deste trabalho e merecedores da minha eterna gratidão.

Marcos Gomes Pinto Ferreira

SUMÁRIO

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

GLOSSÁRIO

ACK	*Acknowledgment*
AODV	*Ad Hoc On-Demand Distance Vector*
AODV_D	*Ad Hoc On-Demand Distance Vector - Drop*
AP	*Access Point*
BSA	*Basic Service Area*
BSS	*Basic Service Set*
CBR	*Constant Bit Rate*
CCK	*Complementary Code Keying*
CDF	*Cumulative Distribution Function*
CS	*Carrier Sense*
CSMA/CA	*Carrier Sense Multiple Access With Collision Avoidance*
CSMA/CD	*Carrier Sense Multiple Access With Collision Detection*
CTS	*Clear To Send*
CW	*Contention Window*
CWD	*Contention Window Differentiation*
CWMax	*Contention Window - Maximum*
CWMin	*Contention Window - Minimum*
DARPA	*Defense Advanced Research Project Agency*
DBPSK	*Differential Binary Phase Shift Keying*
DCF	*Distributed Coordination Function*
DFWMAC	*Distributed Foundation Wireless MAC*
DIFS	*Distributed Inter Frame Space*
DQPSK	*Differential Quadrature Phase Shift Keying*
DSSS	*Direct Sequence Spread Spectrum*
ERP	*Effective Radiation Power*
ESA	*Extended Service Area*
ESS	*Extended Service Set*

FHSS	*Frequency Hopping Spread Spectrum*
GFSK	*Gaussian Frequency Shift Keying*
GPS	*Global Positioning System*
HR/DSSS	*High Rate Direct Sequence Spread Spectrum*
IEEE	*Institute of Electrical and Electronic Engineers*
IFS	*Inter Frame Space*
IME	*Instituto Militar de Engenharia*
IP	*Internet Protocol*
ISO	*International Standardization Organization*
LAN	*Local Area Network*
LLC	*Logical Link Control*
MAC	*Medium Access Control*
MAN	*Metropolitan Area Network*
MANETs	*Mobile Ad-Hoc Networks*
MIMO	*Multiple Input, Multiple Output*
MIT	*Massachusetts Institute of Technology*
NAM	*Network Animator*
NAV	*Network Allocation Vector*
NS	*Network Simulator*
OFDM	*Orthogonal Frequency Division Multiplexing*
OSI	*Open Systems Interconnection*
PCF	*Point Coordination Function*
PIFS	*Priority Inter Frame Space*
QoS	*Quality of Service*
RERR	*Route Error*
RREP	*Route Reply*
RREQ	*Route Request*
RTS	*Request To Send*
SIFS	*Short Inter Frame Space*
TCL	*Tool Command Language*

TCP	*Transmission Control Protocol*
UCSB	*University of California, Santa Barbara*
WAN	*World Area Network*
WEP	*Wired Equivalent Privacy*
WiFi	*Wireless Fidelity*
WIMAX	*Worldwide Interoperability for Microwave Access*
WLAN	*Wireless Local Area Network*
WMN	*Wireless Mesh Network*

RESUMO

As redes mesh se originaram das redes sem fio *ad-hoc* com mecanismos mais robustos de segurança e garantia de qualidade de serviço. Os terminais podem funcionar como roteadores, encaminhando pacotes advindos de seus terminais vizinhos, estabelecendo uma comunicação entre outros nós, mesmo que estes nós não sejam diretamente alcançáveis. A comunicação, nestes casos, se dá através de múltiplos saltos, utilizando nós intermediários da rede.

Por todas estas características, as redes mesh passaram a despertar um maior interesse, pois a tecnologia possui diversos benefícios em comparação com a topologia de redes com infra-estrutura. Entre os benefícios pode-se destacar: escalabilidade, menor custo de construção, compatibilidade com outras tecnologias, qualidade de serviço, robustez, reconstrução de rotas e crescimento orgânico.

A proposta deste trabalho é avaliar o impacto da cooperação entre os nós em uma rede mesh de arquitetura híbrida. A cooperação entre os nós de uma rede mesh, na estrutura do *backbone* sem fio, é compulsória e construída quando na concepção da rede, porém, avaliamos além da estrutura do *backbone*, onde os nós podem não querer, de forma espontânea, disponibilizar seus recursos computacionais e de comunicação. Outra proposta é avaliar, de acordo com o nível de cooperação, o efeito da diferenciação de acesso ao meio com base na manipulação da janela de contenção e do mecanismo de *backoff*.

Os resultados alcançados neste trabalho demonstram que a cooperação traz reais benefícios para a rede como um todo e ainda mostram que a manipulação do algoritmo de *backoff* é um mecanismo útil para garantir a diferenciação de prioridade no acesso ao meio e com isto, proporcionar uma melhoria na quantidade total de pacotes transmitidos pela rede.

ABSTRACT

Mesh networks are originated from ad-hoc wireless networks, but with stronger mechanisms of security and quality of service. In these networks hosts can operate as routers forwarding packets from other neighbors establishing a direct communication among hosts on the network. It happens even if the destination host is out of the range of the source host. This kind of communication happens using multiple hops between the intermediate network hosts.

Due to these characteristics, mesh networks started to stir up more interest, since the technology presents several benefits when compared to networks with infrastructure topology. Among these benefits we can highlight: scalability, lower construction prices, compatibility with other technologies, quality of service, strength, reconstruction of routes and organic growth.

The proposal of this work is to evaluate the impact of the cooperation between the nodes in a mesh network with hybrid architecture. The cooperation between the nodes in a mesh network, in a wireless backbone structure, is mandatory and built when the network is projected, however, we didn't only evaluate the backbone structure, where the nodes may not want to dispose their computer and communication resources spontaneously. Another proposal is to evaluate, according to the cooperation levels, the effect of access differentiation to the medium based on the manipulation of the contention window and the backoff mechanism. The results obtained in this work demonstrate that the cooperation brings real benefits to the networks as a whole and show that the manipulation of the backoff algorithm is a helpful mechanism to guarantee the differentiation of access priorities to the medium, and to grant an improvement on the total number of sets to be transmitted through the network.

1 INTRODUÇÃO

A tecnologia de redes de malha sem fio (WMNs - *Wireless Mesh Networks*) (AKYILDIZ, 2005), ou simplesmente redes mesh, teve origem nos Estados Unidos no DARPA (*Defense Advanced Research Project Agency*) e é fundamentada no padrão WiFi (*Wireless Fidelity*) de acordo com as normas do IEEE 802.11 (CORSON, 1999) (WALKE, 2006). Inicialmente, as redes mesh foram propostas para fins militares, devido à necessidade de redes sem fio com características como: (i) comunicação fim-a-fim utilizando o IP (*Internet Protocol*), (ii) capacidade de transmissão de dados, voz e imagens em banda larga, (iii) comunicação direta entre os nós, sem a necessidade de uma infra-estrutura gerenciada por um nó central ou servidor, (iv) garantia de qualidade de serviço na comunicação entre os nós móveis e (vi) roteamento por múltiplos caminhos minimizando congestionamentos e garantindo robustez à rede.

As redes sem fio utilizam os produtos de comunicação de dados via rádio, de baixo custo e que trazem a potencialidade de utilização em larga escala. Dependendo da área geográfica coberta, as redes sem fio podem ser classificadas em redes locais de computadores (LAN - *Local Area Network*), redes de área metropolitana de computadores, que podem até interligar mais de uma cidade (MAN - *Metropolitan Area Network*) e redes de longa distância (WAN - *Wide Area Network*). A maioria destas redes existentes, porém, é formada por topologias do tipo estrela, composta de uma infra-estrutura que necessita de um AP (*Access Point*), que exerce o controle centralizado da rede e por ele faz fluir todo o tráfego.

No caso das redes mesh, estas não utilizam a topologia estrela e sim o modo *ad-hoc* de se organizar, o que significa que todos os terminais se organizam de forma aleatória e podem funcionar como roteadores, encaminhando pacotes advindos de seus terminais vizinhos estabelecendo comunicação direta com outros nós. Inicialmente o modo *ad-hoc* de organização de uma rede foi concebido para conexões pontuais. Somente com a evolução dos padrões, com mecanismos mais robustos de segurança é que este modelo passou a

despertar maior interesse, pois possui diversos benefícios em comparação com a topologia de redes infra-estruturadas.

A principal característica de uma rede mesh é o fato de um nó origem poder transmitir a um nó destino, que está fora de seu alcance, utilizando um nó intermediário da rede. Para isto é necessário que este nó intermediário disponibilize voluntariamente uma parte de seus recursos de processamento, comunicação e energia. Para que se obtenha uma conexão fim-a-fim, os nós intermediários precisam colaborar. Uma possibilidade de se aumentar a colaboração é o uso de um mecanismo de reputação (ROCHA, 2006), que dê prioridade aos nós que disponibilizem seus recursos e restrinja o acesso aos nós egoístas, que objetivam somente seus interesses individuais.

O trabalho aqui proposto considera as redes mesh estruturadas de forma hierárquica, onde existam roteadores sem fio mesh em lugares pré-determinados, para fornecer serviço a outros dispositivos móveis WiFi. A largura de banda total de tráfego desta rede fica limitada à capacidade do *backbone* mesh instalado.

O objetivo é conseguir uma ampliação da capacidade de transmissão em uma rede mesh, aproveitando uma das suas principais características, que é a possibilidade de comunicação direta entre os nós. Como os nós são móveis e com a necessidade de acesso à *Internet* ou à *Intranet*, dependendo da densidade de participantes e as características de mobilidade do grupo de nós que compõem a rede, é possível afirmar que se os participantes cooperassem entre si, assumindo também o papel de nós intermediários, a comunicação seria otimizada e a banda total da rede cresceria na proporção da quantidade de nós participantes, além de uma ampliação do perímetro coberto.

A proposta deste trabalho é avaliar o impacto do nível de cooperação dos nós de uma rede mesh de arquitetura híbrida e propor um controle de acesso baseado no conceito de reputação (ROCHA, 2006). Este controle fará com que um determinado participante desta rede tenha as suas requisições de acesso ao meio atendidas, com maior prioridade de acordo com o seu nível de cooperação, em busca de maior disponibilidade do meio.

Os resultados alcançados neste trabalho demonstram que a cooperação traz reais benefícios para a rede como um todo e ainda mostram que a manipulação do algoritmo de *backoff* (PANG, 2004), com a variação da janela de contenção, é um mecanismo útil para

garantir a diferenciação de prioridade no acesso ao meio e com isto, proporcionar uma melhoria na quantidade total de pacotes transmitidos pela rede.

1.1 CONTRIBUIÇÕES

As contribuições deste trabalho são:

- A proposta aborda redes mesh utilizando um conceito de reputação com a geração da motivação necessária, para que os participantes da rede disponibilizem seus recursos, para em troca ter prioridade de acesso ao meio;
- O trabalho avalia o impacto do nível de cooperação dos nós em uma rede mesh, onde se avaliou que a cooperação é relevante na performance de transmissão total de pacotes. Os resultados demonstram que existe realmente uma relação direta entre o nível de cooperação dos nós da rede e a quantidade de pacotes transmitidos com sucesso;
- Implementação e simulação de um mecanismo que exerce um controle da reputação dos nós, para identificá-los e escaloná-los numa lista segundo a quantidade de pacotes transmitidos de seus vizinhos. O objetivo foi aferir níveis diferentes de prioridades de acesso ao meio, através do controle do mecanismo de *backoff*;
- O trabalho demonstra a possibilidade que projetos de redes mesh possam ser feitos com menor número de roteadores na infra-estrutura básica do *backbone*;
- Outra contribuição é a possibilidade de comunicação direta entre os participantes da rede sem sobrecarregar o *backbone*, propiciando um aumento substancial da largura de banda passante total da rede.

1.2 MOTIVAÇÃO

A grande motivação para este trabalho se deu pela conjunção de duas premissas. A primeira é tecnológica. A tecnologia de redes mesh tem um enorme potencial para viabilizar novas aplicações. As características de robustez, possibilidade de recomposição

de rotas, múltiplos caminhos, baixo custo dos equipamentos, entre outras características, são diferenciais positivos em relação a outros tipos de redes.

A segunda grande premissa tem relação com cooperação e reputação. "E isto é exatamente como concebemos a multidão: singularidade somada a cooperação, reconhecimento da diferença e do benefício de uma relação comum."(HARDT, 2008). Ou seja, em uma rede mesh é fundamental que exista cooperação em prol do benefício maior do grupo.

Originalmente os protocolos de rede tendem, em seus projetos, a buscar a preservação dos recursos computacionais dos nós, tanto para preservação dos recursos de energia, como para alcançar a máxima capacidade de transmissão de dados. O que propomos neste trabalho é utilizar a característica egoísta dos nós em prol da otimização da rede, com um aumento da taxa total de transmissão. E isto é possível em redes mesh, através de novos estudos com novas abordagens em redes mesh.

1.3 METODOLOGIA DA PESQUISA

Este trabalho teve o objetivo de alcançar a natureza de uma pesquisa avançada, ou seja, objetivou gerar conhecimento para contribuir com aplicações práticas, propondo uma solução e abrindo novas possibilidades para tratar um problema específico em redes mesh, aproveitando a característica egoísta dos nós, inerente aos protocolos existentes para este tipo de rede.

A pesquisa teve uma abordagem quantitativa, pois buscamos traduzir em números se a cooperação entre os nós de uma rede mesh é vantajosa ou não, quando trata-se dos resultados da rede como um todo e não apenas de um determinado nó. Objetivamos saber ainda em que proporção a cooperação pode interferir na capacidade total de transmissão de pacotes, considerando determinadas condições e cenários.

Quanto aos objetivos da pesquisa, esta teve o caráter explicativo, buscando aprofundamento e utilizando o método experimental. Buscamos entender quais fatores são determinantes na forma com que os nós se relacionam no encaminhamento de pacotes. Tendo em vista que este tipo de rede tem como característica básica a possibilidade de múltiplos saltos, para transmitir pacotes de um nó origem a um nó destino, utilizando nós intermediários.

Quanto aos procedimentos, para as experimentações, foram selecionadas variáveis capazes de influenciar a experimentação e foram definidas formas de controle e ferramentas para ajudar na produção e na obtenção dos resultados. Para isto foi implementado um programa que permitiu avaliar os efeitos da cooperação com diversos níveis de cooperadores em uma rede mesh.

1.4 RESUMO DO CAPÍTULO

Este capítulo apresentou as principais motivações para este trabalho, uma introdução sobre redes mesha e a metodologia aplicada à pesquisa. O restante deste trabalho é apresentado da seguinte forma: no Capítulo 2, apresentamos os trabalhos relacionados. No Capítulo 3, apresentaremos o padrão IEEE 802.11, que é a base da tecnologia de redes mesh (AKYILDIZ, 2005). No Capítulo 4 apresentamos as redes mesh.com suas principais características e funcionalidades, e ainda o protocolo de roteamento AODV, utilizado nas simulações, para obtenção dos resultados. O Capítulo 5 descreve o desenvolvimento da solução e as implementações necessárias para este trabalho. Já no Capítulo 6 são apresentadas as simulações e os resultados.

2 REVISÃO DA LITERATURA

Este capítulo apresenta alguns estudos realizados sobre redes sem fio, o padrão IEEE 802.11 e suas variações, redes mesh e conceitos de reputação aplicados às redes de computadores. O objetivo foi pesquisar a literatura existente para situar o tema proposto junto aos trabalhos já publicados, no intuito de facilitar a leitura e o entendimento quanto a solução analisada por este trabalho.

2.1 TRABALHOS RELACIONADOS

Nos estudos realizados até o momento, não foi encontrado nenhum trabalho que tratasse diretamente a utilização de rede mesh vinculada ao conceito de reputação, que avaliasse a cooperação entre os nós.

Neste trabalho, utilizamos para redes mesh o conceito de reputação apresentado em (ROCHA, 2006), "que é uma medida de confiabilidade e justiça de um nó em relação a seus pares". A reputação é utilizada em caso de congestionamento da rede, levando à disputa pelo meio. Quando mais de um nó quer transmitir pacotes ao mesmo tempo que outro, cada nó terá maior ou menor chance de ter acesso ao meio dependendo da sua reputação, comparado com seus pares, em relação à quantidade de pacotes encaminhados de seus vizinhos. Os nós que mais encaminharem pacotes de outros nós terão prioridade de acesso ao meio e os nós que menos encaminharem pacotes de seus vizinhos serão penalizados, com uma baixa probabilidade de terem sucesso na disputa do meio.

Analisando-se a literatura a respeito, verifica-se que os trabalhos relacionados não apresentam uma abordagem que relacione redes mesh ao conceito de reputação ou ao controle de acesso ao meio com a utilização do mecanismo de *backoff*. Os trabalhos abordam as questões sob uma determinada ótica específica, ou abordando as características de simples controle de acesso ao meio, ou com uma abordagem de mecanismos de reputação, ou outros baseados em teoria dos jogos, outros ainda em protocolos de roteamento para redes de múltiplos saltos, ou apenas sobre redes mesh. Por este motivo os trabalhos re-

lacionados podem ser agrupados nos trabalhos a redes mesh, trabalhos relacionados ao controle de reputação e trabalhos sobre controle de acesso ao meio.

Na literatura, existem vários trabalhos utilizando a teoria dos jogos com o objetivo de gerar modelos baseados na característica egoísta dos nós. Em (BANDYOPADHYAY, 2005) são propostos alguns dos mecanismos de punição e regulação para os nós que não cooperam em encaminhar pacotes de outros nós.

Em (ZHONG, 2003) é proposto um sistema de recibos que contabiliza a quantidade de serviços prestados e utilizados por cada nó. Já (ILERI, 2005) trata o relacionamento dos nós da rede com o ponto de acesso, através de regras de um jogo como um sistema de contabilização de créditos.

Em (VIKRAM, 2003) é necessário impor regras que estabeleçam incentivos como uma contrapartida à cooperação, pois o conceito de reputação é uma métrica de confiabilidade de um nó em relação aos seus vizinhos. Considerando a característica racional dos nós de uma rede, que tendem a ignorar o que não atenda aos seus objetivos, estes buscam o máximo de recursos para satisfazer suas necessidades cedendo a menor quantidade possível de seus recursos.

Em (HE, 2004), sem que haja a necessidade de um mecanismo de controle centralizado, cada nó pode calcular a probabilidade com que os seus vizinhos encaminham pacotes, sem a necessidade de inundar a rede com as informações de reputação de cada nó.

Em (ROCHA, 2006) a utilização da teoria dos jogos objetiva prover um mecanismo que otimize a utilização de redes sobrepostas, aproveitando as características racionais e egoístas dos nós. Já em (LAI, In Workshop on Economics of Peer-toPeer Systems, 2003) a idéia é obter a otimização global da rede através de decisões locais.

Em (PANG, 2004) é proposto a garantia de qualidade de serviço utilizando-se o algoritmo de *backoff*, com algumas alterações. Eles propõem o CWD (*Contention Window Differentiation*), cuja proposta mostra que classes de tráfegos diferentes poderiam ser submetidas a diferentes intervalos de janela de contenção. Dado que o valor que alimenta o algoritmo de *backoff* é um número aleatório e uniformemente distribuído entre o valor do tamanho mínimo e máximo da janela de contenção, as duas classes de tráfego podem ser diferenciadas. Desta forma, é proposto um mecanismo para modificar os valores mínimos

e máximos da janela de contenção, de tal forma que para tráfegos de baixa prioridade os valores propostos são maiores que os valores para tráfegos de alta prioridade.

Em (AKYILDIZ, 2005) são apresentadas as redes mesh. Elas são redes sem fio auto-configuráveis e de comunicação direta entre os nós, sem a necessidade de infra-estrutura de pontos de acesso ou de redes cabeadas. Operam através de múltiplos saltos, onde é possível que os nós da rede se alcancem sem que estejam na mesma área de cobertura.

Atualmente existem diversas iniciativas em desenvolvimento de projetos com base na tecnologia de redes mesh, tanto na área acadêmica como pela iniciativa privada. A maioria destes projetos restringe a utilização da tecnologia de redes mesh ao *backbone*. A última milha (conexão com os usuários) é feita através de redes com tecnologia WiFi ou *Ethernet* (redes cabeadas).

A UFF (*Universidade Federal Fluminense*) desenvolve o projeto Remesh (SCHARA, 2007), que se caracteriza por interligar através de um *backbone* mesh o topo de diversos edifícios ao redor da universidade. A partir deste *backbone* a conexão aos usuários desta rede é feita através de rede cabeada e com tecnologia *ethernet*.

Na UFPA (*Universidade Federal do Pará*) existe um projeto (AGUIAR, 2007) que interliga os 10 prédios do campus, através de um *backbone* de roteadores mesh. Simulações já foram realizadas com transmissões simultâneas de Voz e Dados.

Em Tiradentes, Minas Gerais, existe um projeto com tecnologia Mesh da Cisco (CISCO). O projeto interliga através de um *backbone* mesh 8 escolas do município, telecentros, postos de saúde, hospitais e órgãos públicos. O projeto ainda prevê o acesso gratuito pela comunidade através de conexões WiFi.

Em Cambridge no MIT (*Massachusetts Institute of Technology*) existe um projeto denominado Roofnet (BICKET, 2005) constituído por um *backbone* de 37 nós distribuídos ao longo de quatro quilômetros quadrados de uma área urbana. A rede oferece aos usuários uma performance média de 627 kbps, com percurso médio de três saltos, porém, o principal objetivo é o estudo de características de enlaces.

Na Grécia há o projeto VMesh (TSARMPOPOULOS, 2005) desenvolvido na universidade de Thessaly. O projeto tem os objetivos de estudar a construção de redes sem fio de baixo custo, protocolos de comunicações ad-hoc e experiências com mobilidade em redes

Mesh.

Na UCSB (*University of California, Santa Barbara*) está sendo desenvolvido o projeto MeshNet (RAMACH, 2005). Este projeto é constituido de uma rede sem fio com tecnologia mesh, implantado no campus da UCSB. A rede é composta de 25 nós distribuídos em cinco andares do prédio de Engenharia.

2.2 RESUMO DO CAPÍTULO

Este capítulo apresentou alguns estudos realizados sobre redes sem fio, com foco em melhorias de desempenho decorrentes da cooperação entre os participantes da rede. O objetivo foi investigar as relações entre os trabalhos com redes mesh aqui mencionados. Todos os projetos com base na tecnologia de redes mesh restringem a utilização da tecnologia somente ao *backbone*. Nos estudos realizados não encontramos até o momento, nenhum trabalho que utilizasse redes mesh na última milha (conexões com os usuários) e nem que relacionassem redes mesh com o conceito de reputação, com objetivo de aumentar a cooperação. Desta forma entendemos ter valia esta investigação, principalmente devido a característica de múltiplos saltos suportada pela tecnologia. A seguir, no Capítulo 3, apresentaremos o padrão IEEE 802.11, que é a base da tecnologia de redes mesh. No Capítulo 4 apresentamos as redes mesh.com suas principais características e funcionalidades, e ainda o protocolo de roteamento AODV, utilizado nas simulações, para obtenção dos resultados. O Capítulo 5 descreve o desenvolvimento da solução e as implementações necessárias para este trabalho. Já no Capítulo 6 são apresentadas as simulações e os resultados.

3 IEEE 802.11

Este capítulo descreve o padrão de redes sem fio, o IEEE 802.11. O objetivo é introduzir o tema das redes WLAN (*Wireless Local Area Network*) e aprofundar esse entendimento até o ponto de como o padrão trata a disputa do meio compartilhado, que os nós móveis exercem em uma rede sem fio.

A disputa pelo meio gera o problema de contenção, que é causado quando mais de um nó pretende fazer uso do meio, para transmitir ao mesmo tempo que outro. O padrão IEEE 802.11 define o mecanismo de *backoff* para tratar a contenção de acesso ao meio e minimizar ao máximo possível as colisões. A diferenciação de prioridades para acesso ao meio, através da diferenciação da contenção pelo mecanismo de *backoff* é a base teórica da solução que é proposta neste trabalho.

3.1 O PADRÃO IEEE 802.11

Definido como padrão de redes sem fio pelo IEEE (*Institute of Eletrical and Eletronics Engineers*), o IEEE 802.11 (CORSON, 1999) (WALKE, 2006) é parte do IEEE 802 que engloba padrões aplicados à construção de redes locais - LANs (*Local Area Network*) e redes metropolitanas - MANs (*Metropolitan Area Network*). Membros destacados desta família são, por exemplo, os padrões IEEE 802.3 (*Ethernet*) e IEEE 802.5 (*Token Ring*) assim como uma série de padrões mais recentes ou emergentes como o IEEE 802.15 (*Bluetooth*) ou IEEE 802.16 - WiMax (*Worldwide Interoperability for Microwave Access*).

Um dos objetivos principais do IEEE ao criar o padrão 802.11 foi o de permitir a interligação da rede sem fio com redes cabeadas que seguem o padrão *Ethernet* IEEE 802.3. As redes sem fio inicialmente eram vistas como extensão de uma rede cabeada. A decisão de interligação das redes sem fio com as redes cabeadas resultou na necessidade de uma série de mecanismos apropriados para a compatibilização das partes com fio e sem fio de uma rede local. A popularização das redes sem fio e seu uso cada vez mais intenso motivou novas propostas na direção de aumentar a largura de banda disponível (como

as emendas a, b e g, e recentemente o *draft* n), para tornar a rede mais segura (IEEE 802.11i), para auxiliar a mobilidade (*draft* r), para suportar qualidade de serviço (IEEE 802.11e) e para desenvolver as redes mesh de múltiplos saltos, para o qual foi criado um Grupo de Trabalho (IEEE 802.11s) que tem o objetivo de adequar este tipo de rede ao padrão existente.

3.1.1 ARQUITETURA DO PADRÃO IEEE 802.11

O padrão IEEE 802.11 (ERGEN, 2002) foi projetado para prover uma rede sem fio definindo métodos de transmissão e outros aspectos de transferência de dados, com suporte à mobilidade de modo transparente para as camadas superiores do modelo OSI (*Open Systems Interconnection*) da ISO (*International Standardization Organization*).

Esse padrão especifica as funções da camada física (*PHY*) e de enlace -MAC (*Medium Access Control*) (BHARGHAVAN, 1994),contendo uma série de emendas que ampliam ou aperfeiçoam suas capacidades. A Figura 3.1, situa o Padrão 802.11 no contexto do modelo *OSI-ISO*.

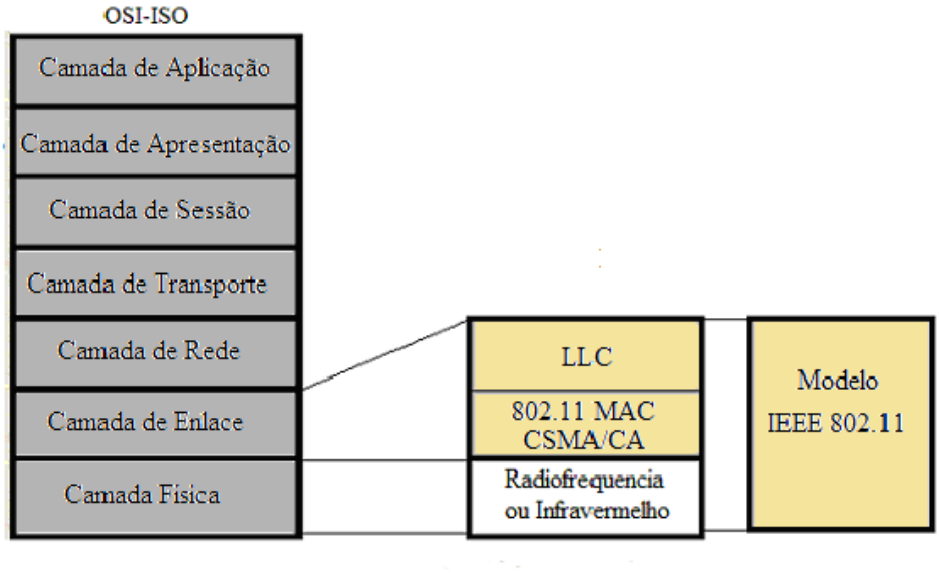

FIG. 3.1: Padrão 802.11, modelo *OSI-ISO*

O padrão IEEE 802.11 define a arquitetura baseado na divisão da área coberta pela rede em BSAs (*Basic Service Area*) ou células de cobertura, tal como na Figura 3.2, cujo

tamanho depende das características do ambiente e da potência dos rádios usados como estações de transmissão e recepção. Outros elementos ainda compõem a arquitetura:

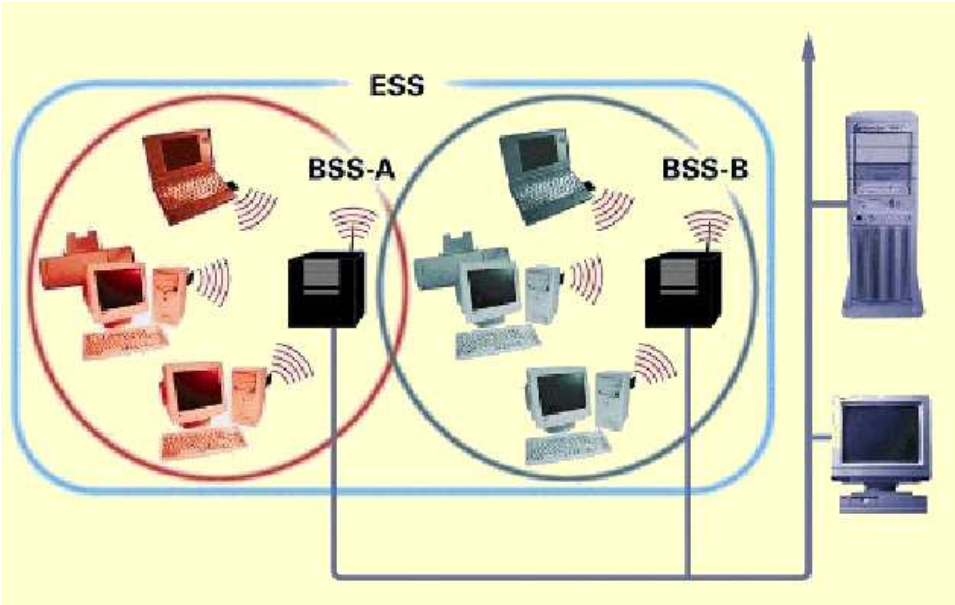

FIG. 3.2: Arquitetura

- BSS (*Basic Service Set*) - é o conjunto básico de serviço, que é composto de um grupo de estações de rádio que se comunicam em uma BSA (*Basic Service Area*);
- Ponto de acesso (AP - *Access Point*) - são estações centrais de uma rede infra-estruturada que controlam e centralizam todas as funcionalidades da rede dentro de uma BSA e ainda se comunicam com outras BSAs, através de um sistema de distribuição;
- Sistema de distribuição - é o *backbone*, infra-estrutura de comunicação entre células que viabiliza a interligação entre múltiplas BSAs, com o objetivo de ampliar a cobertura de uma rede;
- ESA (*Extended Service Area*) - é a área de serviço estendida pela interligação de vários BSAs através dos APs;
- ESS (*Extended Service Set*) - é o conjunto de serviço estendido e representa um

conjunto de estações formado por vários BSSs conectados por um sistema de distribuição.

No 802.11 são definidos dois arranjos de redes sem fio: redes sem infra-estrutura e redes infra-estruturadas. Em redes sem infra-estrutura, também chamadas de redes *ad hoc*, as estações podem se comunicar diretamente sem a necessidade de APs para centralizar as comunicações. Já nas redes infra-estruturadas, é necessária uma estação que centralize a comunicação e que possa prover a interconexão de vários BSSs, formando um ESS. A infra-estrutura é caracterizada pelos APs e pelo sistema de distribuição que faz a interligação dos APs. O sistema de distribuição pode ainda prover os recursos necessários para interligação da rede sem fio a outras redes sem fio ou redes cabeadas (fios de cobre ou cabos de fibra óptica). A Figura 3.3 ilustra os dois tipos de topologia, a *ad-hoc* e a com infra-estrutura.

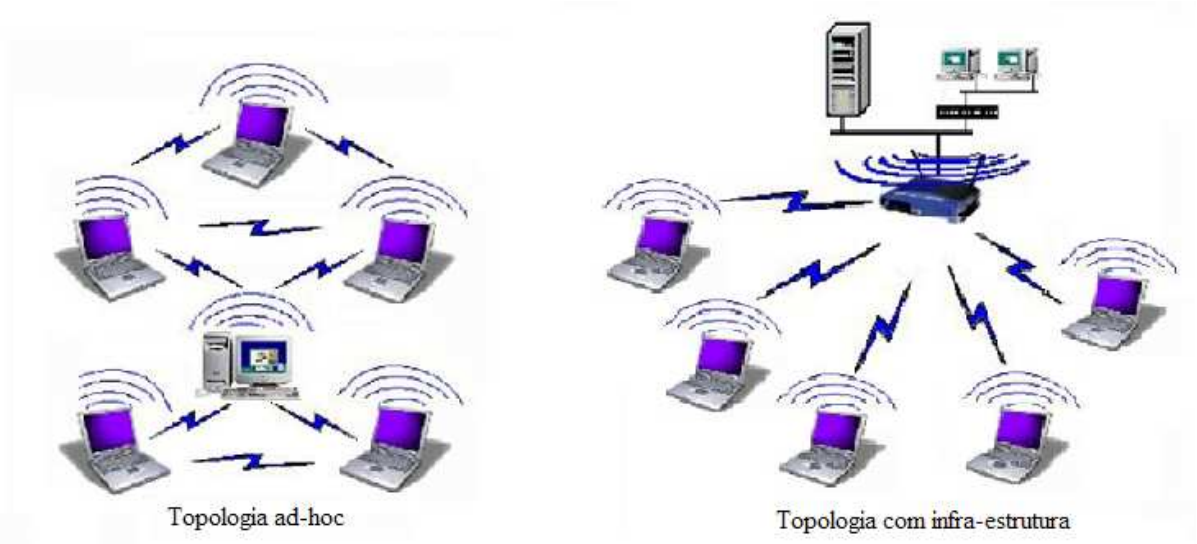

FIG. 3.3: Topologia *ad-hoc* e topologia com infra-estrutura

3.1.2 EVOLUÇÃO DO PADRÃO IEEE 802.11

A evolução do padrão IEEE 802.11 (WALKE, 2006) teve como motivações o aumento da capacidade de transmissão, a melhoria na garantia da qualidade de serviços, uma maior e melhor cobertura e aproveitamento do espectro de freqüência, a otimização de energia,

melhores mecanismos de segurança, a interação com obstáculos e facilidade de expansão, tal como descrito a seguir:

- Padrão IEEE 802.11 - Lançado em 1997 e originou todos os demais padrões. Ele define a camada MAC, na faixa de freqüência de 2.4 a 2.5Ghz e descreve o formato de modulação FHSS (*Frequency Hopping Spread Spectrum*) e DSSS (*Direct Sequence Spread Spectrum*), padronizando a velocidade de transmissão em 1 e 2 Mbps;

- Padrão IEEE 802.11a - Emenda aprovada em 1999 como padrão para camada física na faixa de freqüência de 5.15 a 5.8Ghz, com modulação OFDM (*Orthogonal Frequency Division Multiplexing*), com 8 canais de rádio e suporte a velocidade de largura de banda de até 54Mbps. Introduzida ao padrão 802.11 em 2007;

- Padrão IEEE 802.11b - Emenda aprovada em 1999 como padrão para a camada física na faixa de freqüência de 2.4 a 2.5Ghz, com modulação HR/DSSS (*High Rate Direct Sequence Spread Spectrum*), com especificação de 3 canais de rádio e suporte a velocidade de largura de banda de até 11Mbps;

- Padrão IEEE 802.11d - Emenda aprovada em 2001 e define o suporte às questões regulatórias internacionais (canais de comunicação permitidos, níveis de potência aceitáveis, etc.), com o objetivo de buscar compatibilidade à grande variedade de normais internacionais;

- Padrão IEEE 802.11e - Emenda aprovada em 2005, que complementa a camada MAC e define classes de serviços com níveis gerenciáveis de qualidade de serviço (QoS - *Quality of Service*), destinadas para aplicações LAN, a serem aplicados aos padrões 802.11a, 802.11b e 802.11g, com objetivo de atender as demandas de multimídia (dados, voz e vídeo);

- Padrão IEEE 802.11f - Esta emenda teve como objetivo regulamentar a interoperabilidade entre APs de fabricantes diferentes. O trabalho foi desenvolver um protocolo que permitisse interconexão entre pontos de acesso, o que permitiria que dispositivos móveis se conectassem a vários pontos de acesso de fabricantes diferentes;

- Padrão IEEE 802.11g - Emenda aprovada em 2003, com padrão para a camada física nas faixas de freqüência de 2.4Ghz e 5Ghz, com modulação ERP (*Effective Radiation Power*) / DSSS / CCK (*Complementary Code Keying*) / OFDM , com 3 canais de rádio e com suporte a velocidade de largura de banda de até 54Mbps. Introduzida ao padrão 802.11 em 2007;

- Padrão IEEE 802.11h - Emenda aprovada em 2004 com o objetivo de buscar compatibilidade do 802.11a (faixa de freqüência de 5Ghz) com as normas regulatórias da União Européia, que exigem produtos com controle de potência e seleção de canais de freqüência de forma dinâmica;

- Padrão IEEE 802.11i - Emenda aprovada em 2004 e define novos mecanismos de segurança objetivando mais proteção e confiabilidade na comunicação entre os dispositivos dos padrões 802.11a, 802.11b e 802.11g, com novos métodos criptografia e procedimentos de autenticação (WEP - *Wired Equivalent Privacy*);

- Padrão IEEE 802.11j - Emenda aprovada em 2004 com o objetivo de buscar compatibilidade com as normas regulatórias japonesas;

- Padrão IEEE 802.11-2007 - Incorpora todas as emendas acima ao padrão original;

- Padrão IEEE 802.11n (*draft*) - Grupo de trabalho com o objetivo de avaliar e propor métodos para vazões superiores a 100Mbps, com modulação OFDM. A tecnologia MIMO (*Multiple Input, Multiple Output*) está associada a este grupo de trabalho;

- Padrão IEEE 802.11r (*draft*) - Grupo de trabalho com o objetivo avaliar e propor métodos para aprimoramento de *handoff*, que atendam com resposta satisfatória à mobilidade de mais alta velocidade;

- Padrão IEEE 802.11s (*draft*) - Grupo de trabalho com o objetivo de adequar o padrão existente às redes mesh;

- Padrão IEEE 802.11x - Emenda que propõe a regulamentação do controle de acesso de estações na rede e aplicados aos padrões 802.11a, 802.11b e 802.11g;

- Padrão IEEE 802.11p - Emenda que propõe um padrão para diferenciação de tráfego em classes de prioridade e filtros de multicasta, com suporte à níveis de serviço (QoS) e é parte importante da proposta do padrão 802.11e. Aplicado aos padrões 802.11a, 802.11b e 802.11g.

3.2 A CAMADA FÍSICA

As principais funções dessa camada são: a codificação e decodificação de sinais, a geração e remoção de parâmetros para sincronização, a recepção e transmissão de sinais digitais, a especificação do meio de transmissão e a codificação para comunicações sem fio, sendo os mais comuns: DSSS - espalhamento de espectro por seqüência direta e FHSS - espalhamento de espectro por salto de freqüência.

O método FHSS divide a largura de banda em vários canais de freqüência e faz com que os rádios (transmissor e o receptor) permaneçam em um desses canais por uma certa fração de tempo e depois saltem para outro canal, o que possibilita a coexistência de várias redes numa mesma área geográfica de espectro de freqüência, individualizando-as por diferentes padrões pseudo-aleatórios de uso do canal no tempo, evitando colisões na disputa do acesso ao meio. A modulação de freqüência utilizada no FHSS é a GFSK (*Gaussian Frequency Shift Keying*).

O DSSS é uma técnica de espalhamento de espectro por seqüência direta com separação de códigos. O DSSS utiliza a modulação diferencial binária por chaveamento de fase - DBPSK (*Differential Binary Phase Shift Keying*) e a modulação diferencial quaternária por chaveamento de fase - DQPSK (*Differential Quadrature Phase Shift Keying*). Atualmente o DSSS é a técnica mais usada no desenvolvimento dos novos equipamentos de redes sem fio, pois possibilitam uma taxa de transferência superior a técnica FHSS, apesar desta ser mais imune a interferências.

A evolução dos padrões, na busca de maiores taxas de transmissão proporcionou diversas propostas de alterações no padrão original do 802.11, principalmente utilizando a técnica DSSS. Uma das propostas é o uso do chaveamento de código complementar (CCK) e outra é a multiplexação por divisão ortogonal em freqüência (OFDM).

3.3 A SUBCAMADA MAC DO NÍVEL DE ENLACE DE DADOS

O padrão IEEE 802.11 define duas camadas separadas, o LLC (*Logical Link Control*) e a camada MAC, para a camada de enlace de dados do modelo OSI da ISO.

As principais funções da camada MAC são:

- Transmissão de dados - formar pacotes de dados com endereços e campos para detecção e controle de erro;
- Recepção de dados - abrir e reconhecer os endereços dos pacotes e tratar os erros;
- Controle de acesso ao meio - gerenciar o uso compartilhado do meio.

As principais funções da camada LLC são:

- Prover a conexão com as camadas superiores;
- Controlar o fluxo de dados;
- Controlar os erros de pacotes.

3.4 PROTOCOLO MAC DO PADRÃO IEEE 802.11

Além dos mecanismos de transmissão (camada física) que utilizam a radiofreqüência ou infravermelho, o IEEE definiu um mecanismo de acesso ao meio, denominado de DFW-MAC (*Distributed Foundation Wireless* MAC), prevendo dois métodos de acesso (funções de coordenação). Ambas as funções de coordenação se destinam a definir quando uma estação pode ou não transmitir, são estas funções:

- Função de coordenação distribuída - DCF (*Distributed Coordination Function*): é o método de acesso distribuído básico, onde a decisão de que uma estação pode ou não transmitir é realizada individualmente pelas próprias estações da rede, com a possibilidade de ocorrer colisões;
- Função de coordenação pontual - PCF (*Point Coordination Function*): é o método de acesso com controle centralizado, onde a decisão de transmitir é centralizada

em uma estação, que determina qual estação pode transmitir e em que momento, minimizando assim a possibilidade de colisões.

Em ambos os métodos de acesso existem parâmetros para regular o tempo necessário de espera antes de liberar o acesso ao meio para uma estação, pois o meio pode estar ocupado com a transmissão de quadros de dados, com quadros de controle ou ainda estar disponível, para que alguma estação possa tomar o meio de transmissão. A Figura 3.4, apresenta o funcionamento do controle de acesso DFWMAC.

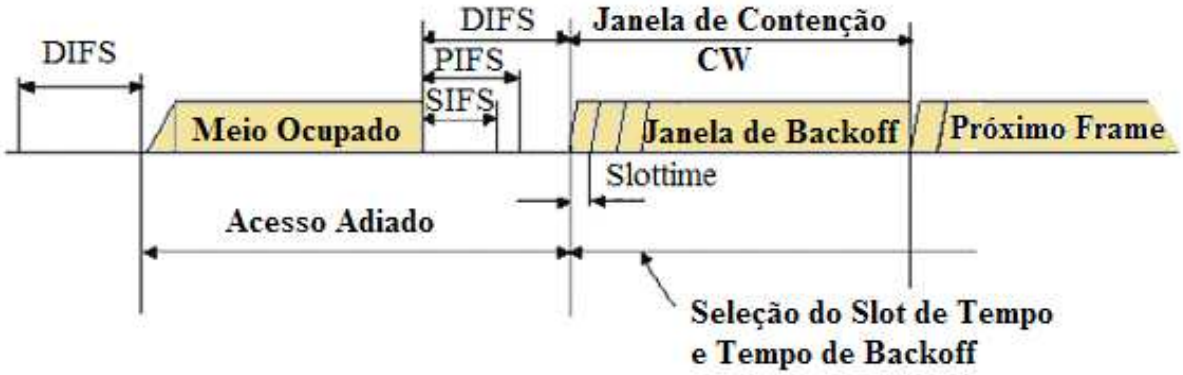

FIG. 3.4: Controle de acesso DFWMAC

Para uma estação ter acesso ao meio e assim poder transmitir, ela deve "ouvir" se o meio está livre por um período de silêncio mínimo, IFS (Inter Frame Space), antes de utilizá-lo. O DFWMAC define três prioridades de acesso ao meio, através de diferentes períodos de tempo:

- DIFS (*Distributed Inter Frame Space*) - parâmetro que indica o maior tempo de espera aguardando um intervalo de silêncio mínimo para ter o acesso ao meio, para transmitir dados (menor prioridade) e é definido pelo espaço distribuído entre quadros da função de coordenação distribuída (DCF);

- PIFS (*Priority Inter Frame Space*) - é um espaço de tempo intermediário entre o DIFS e o SIFS (prioridade média), pois é usado por uma estação que controla outras estações e por isto tem maior prioridade que as estações comuns e é definido pelo espaço entre os quadros da função de coordenação pontual (PCF);

- SIFS (*Short Inter Frame Space*) - é o espaço de tempo de espera para funções de maior prioridade. Em geral são transmissões de quadros que contém respostas curtas como, por exemplo, os pacotes ACK (*Acknowledgment*).

3.4.1 FUNÇÕES DE COORDENAÇÃO

Existem duas funções de coordenação, a função de coordenaão de pontual (PCF), que é uma função opcional que pode ser agregada ao protocolo DFWMAC e a função de coordenação distribuída (DCF).

No caso de redes sem fio numa arquitetura ad-hoc é utilizada a função de coordenação distribuída. A função DCF é o mecanismo que no padrão 802.11 regula a disputa do acesso múltiplo compartilhado com detecção de portadora, com o objetivo de evitar colisões. Esta função é denominada CSMA/CA (*Carrier Sense Multiple Access With Collision Avoidance*) com reconhecimento positivo, que tem como objetivo evitar colisões, enquanto a função CSMA/CD (*Carrier Sense Multiple Access With Collision Detection*), utilizada em redes cabeadas (IEEE 802.3), somente controla as colisões quando elas ocorrem.

Como no método CSMA/CA podem ocorrer colisões, não havendo garantia da entrega dos pacotes, uma estação após transmitir um quadro, necessita de uma confirmação de recebimento pelo destino, um aviso de recebimento (ACK), enviado pela estação destino, após esperar um tempo SIFS, assim nenhuma outra estação estará acessando o meio ao mesmo tempo causando uma colisão. Caso o aviso de recebimento (ACK) não retorne a estação de origem, esta realiza novamente o processo de transmissão do quadro.

Pela função de coordenação distribuída, quando uma estação quer transmitir, tanto nas redes não infra-estruturadas como nas redes infra-estruturadas, primeiramente a estação "ouve" o meio no intuito de detectar a portadora ou não, para determinar se outra estação já está utilizando o meio, com alguma transmissão. Caso o meio esteja livre (sem nenhuma outra estação transmitindo) há pelo menos um intervalo de tempo DIFS, a estação pode transmitir sem problemas.

Caso o meio esteja ocupado por alguma outra estação, o processo de transmissão é adiado para não atrapalhar a estação que já está transmitindo, iniciando-se assim um processo de *backoff*, que se refere ao tempo em que um dispositivo de transmissão de dados

aguarda para realizar uma nova transmissão após a ocorrência de colisão na primeira tentativa, no qual um tempo aleatório uniformemente distribuído entre zero e o tamanho máximo da janela de contenção - CW (*Contention Window*) é escolhido e através de um temporizador de *backoff*, buscando-se evitar as colisões. Se ao término do tempo de *backoff* a estação encontrar o meio livre, há pelo menos um intervalo de tempo DIFS, ela poderá transmitir.

O temporizador de *backoff* é determinado de acordo com a quantidade de colisões ocorridas na rede. Com pouca carga (poucas colisões) o tempo de *backoff* estimado é da ordem de 7ms, submetendo assim os quadros a poucos atrasos. Com muita carga, o tempo de *backoff* vai dobrando a cada ocorrência de colisão até chegar ao limite máximo de 255ms. Quanto menor o limite, maior será a chance de duas estações escolherem o mesmo tempo de *backoff*, provocando uma colisão.

Além do CSMA/CA, que é obrigatório no padrão, existe um outro mecanismo de controle do DCF e que utiliza pedidos de permissão para transmissão de dados, denominado mecanismo de RTS (*Request To Send*) / CTS (*Clear To Send*). A Figura 3.5, apresenta o funcionamento do CDF utilizando RTS e CTS.

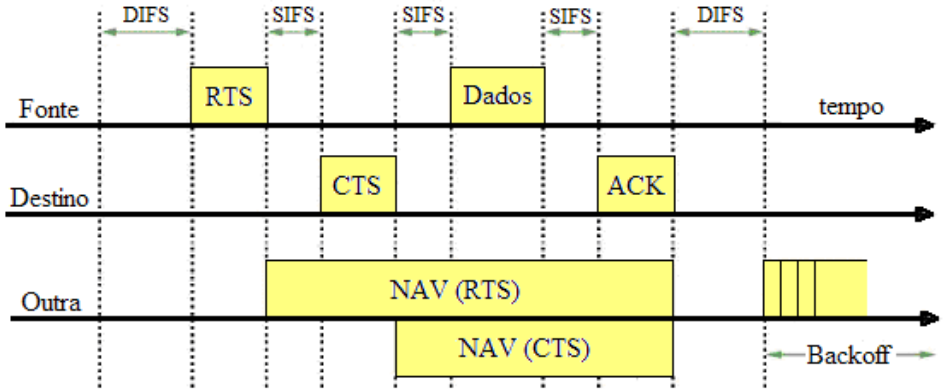

FIG. 3.5: CDF utilizando RTS e CTS

O processo ocorre quando uma estação, após aguardar o tempo DIFS, antes de efetivamente transmitir o quadro de dados, transmite um quadro de controle RTS, que leva a informação da estimativa da duração da transmissão do quadro de dados que se pretende transmitir.

A estação de destino quando receber o RTS ajusta o seu vetor de alocação de rede -

NAV (*Network Allocation Vector*), que é utilizado para a detecção virtual da portadora, indicando quando poderá haver uma nova tentativa de acesso ao meio. A estação destino então, em resposta ao RTS, envia um CTS avisando que está pronto para receber o quadro de dados e que também serve para informar as demais estações, que uma transmissão vai ocorrer, provocando que todas as demais estações atualizem seus vetores NAV. Com isto, todas as estações irão aguardar o tempo da transmissão terminar para tentar acessar o meio novamente.

3.5 ALGORITMO DE *BACKOFF*

O algoritmo de *Backoff* é o mecanismo do IEEE 802.11 para evitar as colisões sucessivas que podem ocorrer quando as estações tentam transmitir ao mesmo tempo, isto é: Após a transmissão de um quadro bem sucedida e o período de tempo DIFS transcorrido, qualquer estação pode tentar tomar o meio, e caso nenhuma outra estação esteja também disputando o meio, transmitir. A Figura 3.6 apresenta o funcionamento da técnica de *backoff* exponencial binária e mostra que após o período DIFS, segue-se o período de contenção também denominado de janela de *backoff*, que é dividida em *slots* de tempo. Um slot de tempo corresponde ao tempo de propagação de ida e volta dentro de uma BSA, necessário para uma estação detectar se o meio está ocupado por alguma outra estação.

O meio é determinante no comprimento do *slot* de tempo, desta forma as camadas físicas de mais alta velocidade utilizam *slots* de tempo menores e as camadas físicas de mais baixa velocidade utilizam *slots* de tempo maiores.

No processo de disputa do meio, as estações escolhem um valor entre 0 (zero) e CW, que é o valor mínimo da janela de contenção. Assim as estações que desejam transmitir, selecionam um intervalo de tempo aleatório iniciando um contador (*backoff time*) para uma próxima tentativa de transmissão. O *backoff time* regula as transmissões e as estações somente podem transmitir quando o contador chega a zero. O *backoff time* se comporta da seguinte forma:

- O contador de tempo é decrementado quando o meio está livre;
- O contador é paralisado quando há colisão, isto é, quando uma transmissão é de-

tectada no canal;

- O contador é reativado quando por um período maior do que um DIFS o canal permanece livre.

O método de acesso, cuja função de coordenação de transmissão (aquela que define quando uma estação pode ou não transmitir) é a função de coordenação distribuída (DCF). A técnica de *backoff* utilizada é a exponencial binária. Se alguma colisão ocorre a estação altera o valor da janela de contenção corrente para o valor da próxima potência de 2, menos 1, desta forma a cada tentativa de retransmissão, a janela de contenção é duplicada até o valor máximo de 1023 *slots* de tempo.

Após várias tentativas de retransmissão sem sucesso e alcançando o número máximo de retransmissões, com o CW no valor máximo (1023 *slots*), o contador de *backoff* é reinicializado ao seu valor mínimo, com o descarte do pacote, sendo necessário a reinicialização do processo de transmissão.

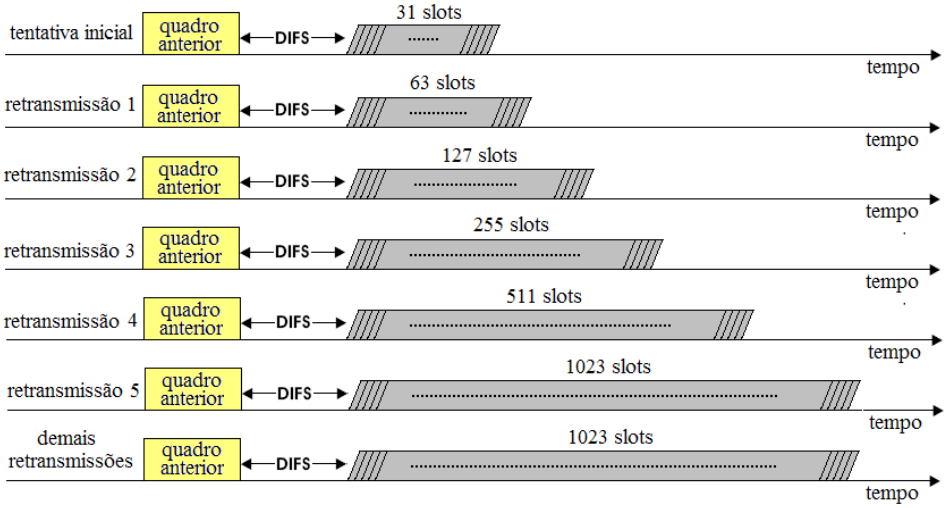

FIG. 3.6: Técnica de *backoff* exponencial binária

3.6 RESUMO DE CAPÍTULO

Este capítulo apresentou o padrão de redes sem fio, o IEEE 802.11 com suas características, arquitetura e evolução, e aprofundou na camada de enlace, especificamente no

controle de acesso ao meio, com a função de coordenação distribuída. Um dos objetivos foi discutir o algoritmo de *backoff*, que será utilizado na metodologia para solução proposta neste trabalho.

Uma das evoluções do padrão IEEE 802.11 vista neste capítulo, foi a do Grupo de Trabalho IEEE 802.11s, que tem o objetivo de desenvolver as redes mesh, que apresentaremos a seguir no Capítulo 4 e que utilizamos em nossas simulações.

4 REDES MESH

Neste capítulo se descreve a tecnologia de redes em malha ou como é mais usualmente tratada na literatura, redes mesh. O objetivo é apresentar as principais características e funcionalidades e com isto destacar a importância deste tipo de infra-estrutura no cenário atual, frente à grande demanda pela universalização do acesso à Internet.

Apresentaremos aqui também o protocolo de roteamento AODV (*Ad-Hoc On-Demand Distance Vector*), o qual utilizamos em nossas simulações para produção dos resultados.

A escolha do protocolo de roteamento AODV foi motivada por ser um protocolo reativo, próprio para redes com mobilidade, pois atua sob demanda. O AODV é um dos protocolos mais estudados e ainda como em (AGUIAR, 2007) é apresentado um estudo comparativo dos principais protocolos de roteamento para redes mesh e o protocolo AODV é o que apresentou os melhores resultados.

4.1 REDES MESH E REDES *AD-HOC*

As redes mesh (AKYILDIZ, 2005), (WANG, 2008), (MESH, 2008) são redes que evoluíram a partir das redes móveis *ad-hoc*, as MANETs (*Mobile Ad-hoc Networks*) (Zang, 2007) e apresentam uma topologia dinâmica, variável e de crescimento escalável, constituídas por nós cuja comunicação, no nível físico, é baseado no padrão IEEE 802.11.

Redes *ad-hoc* são redes geradas de forma espontânea, sem nenhuma infra-estrutura prévia e de auto-organização. Os nós são responsáveis por descobrir quais são os outros nós vizinhos que podem se comunicar diretamente a eles. Redes *ad-hoc* se aplicam a situações onde existe ausência absoluta da possibilidade de construção de infra-estrutura ou em casos de emergência, tais como: redes temporárias, desastres, catástrofes, e que não necessitem de segurança ou qualidade de serviço - QoS (*Quality of service*).

O pouco incentivo aos participantes de uma rede *ad-hoc* em compartilhar seus recursos computacionais e de comunicação é o que torna limitado o seu uso, quando comparado às redes mesh. Nas redes mesh há o compartilhamento compulsório dos recursos para

formação do *backbone* principal da rede, que é sem fio. Esta é uma das principais diferenças entre redes *ad-hoc* e redes mesh. Nas redes *ad-hoc* não existe a caracterização de uma estrutura de *backbone*, já em redes mesh existe o *backbone* sem fio e o acesso dos nós clientes (última milha) ao *backbone* pode ser com ou sem fio.

Os nós do *backbone* de uma rede mesh podem ter localização fixa ou mobilidade limitada e por isto, não ter limitação de energia, devido a possibilidade de estarem conectados diretamente à rede elétrica, eliminando assim, algumas das restrições das redes *ad-hoc*.

4.2 CARACTERÍSTICAS BÁSICAS

A tecnologia de redes mesh - WMNs (*Wireless Mesh Network*) teve origem nos Estados Unidos na DARPA (*Defense Advanced Research Project Agency*), onde se buscava, para fins militares uma rede sem fio que fosse flexível, dinâmica, escalável e que possibilitasse uma comunicação com suporte IP fim a fim com as seguintes características técnicas:

- Capacidade de transmissão de dados em banda larga;
- Comunicação direta entre os nós, sem a necessidade de comunicação com um nó central;
- Capacidade de transmissão de dados, voz e imagens;
- Suporte para geo-localização, sem a utilização de GPS (*Global Positioning System*);
- Capacidade de conexão a nós móveis.

Em uma rede mesh, cada nó pode ser qualquer dispositivo móvel com uma interface de comunicação sem fio padrão WiFi (*Wireless Fidelity*), assumindo a função de *host* ou *router* quando necessário. Este tipo de topologia também propicia estender o alcance da rede. Toda a comunicação é feita através de comutação de pacotes, onde estes podem seguir caminhos distintos, de acordo com a capilaridade e disponibilidade existente em cada rota, possibilitando assim, a comunicação por múltiplos caminhos. Este tipo de comunicação possibilita evitar rotas congestionadas e supera perdas de conexão. A Figura 4.1 apresenta a topologia de uma rede mesh.

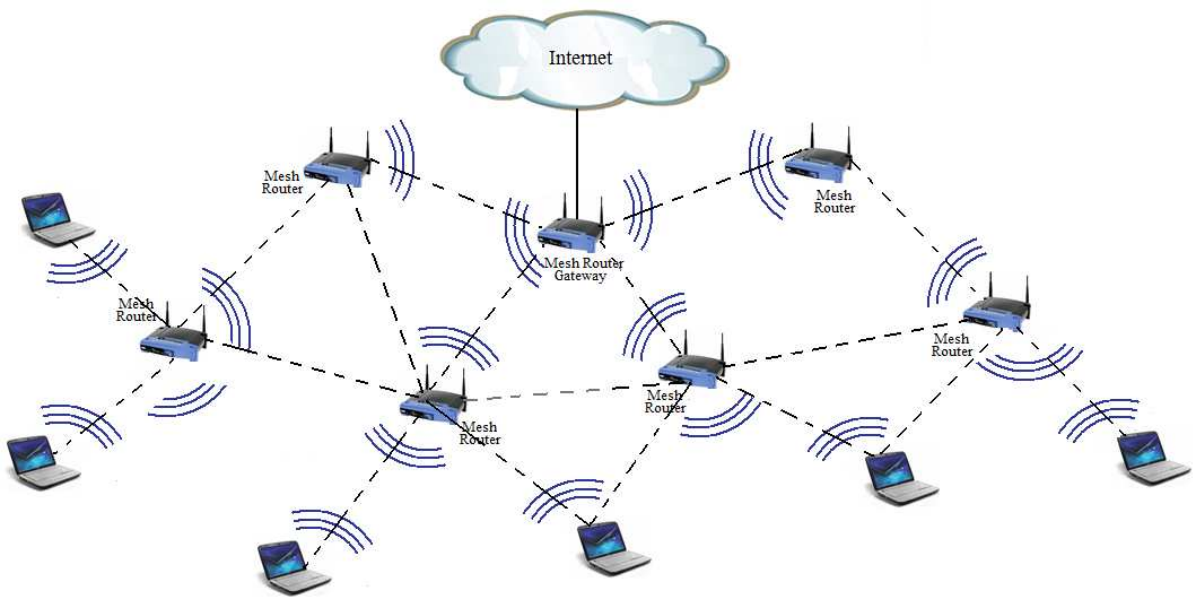

FIG. 4.1: Redes mesh

A transmissão de dados de um nó de origem ao último nó de destino, mesmo fora da área de cobertura do nó de origem, é possível através de múltiplos saltos, porém é necessário ter disponíveis todas as informações de endereçamento até o destino final, o que é possível através das características do roteamento, ou seja, os nós que exercem papel de roteadores trocam informações em suas redes próximas e reportam todas as rotas conhecidas. O nó de origem que quer transmitir a um nó destino se comunica com seu nó roteador correspondente ou *gateway*, que se comunica aos nós que desempenham papéis de roteadores intermediários até o *gateway* do destino, que entrega o pacote ao nó destinatário final.

Em redes sem fio, o meio é um recurso compartilhado. Em redes mesh este recurso pode ser compartilhado não só com dispositivos mesh, como também com dispositivos WiFi. Nas redes mesh a comunicação pode ocorrer entre múltiplos dispositivos que estejam próximos (vizinhos diretos) ou com vizinhos indiretos (vizinhos dos vizinhos), através de múltiplos saltos.

O suporte de segurança em redes sem fio mesh, que contempla múltiplos saltos, é mais complexo do que em redes infra-estruturadas, pois a relação direta entre os dispositivos, sem um controle centralizado, faz com que nem sempre os relacionamentos entre

os nós sejam confiáveis, pois entre a origem e o destino podem existir vários caminhos e contemplar múltiplos saltos até o destino final.

4.3 ARQUITETURA MESH

A arquitetura de redes mesh é composta por dois tipos de nós: roteadores e clientes. Diferente de um roteador WLAN convencional, um roteador mesh contém funções adicionais de roteamento para suprir a gestão de redes mesh, podendo inclusive ser equipado com múltiplas *interfaces* de comunicação sem fio. Em uma rede mesh os nós podem acessar uns aos outros através de diversos caminhos e sem nenhuma hierarquia, já em uma rede WiFi, composta por um AP, todas as conexões são centralizadas e reguladas pelo AP.

Tal como apresentado no capítulo anterior, as redes sem fio se caracterizam pelo tipo de arquitetura adotada. O padrão IEEE 802.11 define a arquitetura de redes sem fio em BSAs e o que melhor representa uma rede mesh é a arquitetura ESS, que é um conjunto de serviço estendido e pode representar um grupo de estações formado por vários BSSs e conectados por um sistema de distribuição. Em redes mesh o sistema de distribuição representa o *backbone* sem fio, pois é formado apenas por roteadores mesh.

As redes mesh também podem ser caracterizadas pelo tipo de hierarquia. Em redes cujos nós estejam numa mesma estrutura sem hierarquia, todos os dispositivos da rede sem fio têm função e capacidade de suportar tráfego de múltiplos pontos e podem enviar e receber pacotes de si mesmo e de seus vizinhos, funcionando assim como nós intermediários da rede mesh (DRAVES, 2004). No caso das redes com níveis de hierarquia diferentes, onde existam nós com a tecnologia mesh e outros não, apenas os nós compatíveis com mesh é que poderão fornecer serviço aos nós que não são compatíveis e que se associam à rede, porém estes últimos não têm capacidade de retransmissão.

A arquitetura de redes mesh pode ser classificada em três grupos com base na funcionalidade dos nós:

- Arquitetura com infra-estrutura WMN de *backbone*: neste tipo de arquitetura os roteadores mesh exercem a função de *gateway*, podendo ser conectados à Internet,

formando um *backbone* em malha capaz de se auto-organizar e auto-configurar dinamicamente, mantendo as conexões automaticamente entre eles. Isto proporciona conectividade para os clientes convencionais do tipo WiFi e ainda a integração com outras redes sem fio existentes;

- Arquitetura com infra-estrutura WMN de clientes: os clientes mesh podem estabelecer conexões ponto a ponto entre os dispositivos. Este tipo de arquitetura é formado apenas por nós móveis que executam roteamento e auto-configuração. A comunicação entre os nós pode ser feita através de múltiplos saltos. Um pacote destinado a um nó na rede pode passar por diversos nós para alcançar o destino;

- Arquitetura com infra-estrutura WMN híbrida: esta arquitetura é a de melhor aplicação pois faz a combinação de infra-estrutura de *backbone* e infra-estrutura cliente, desta forma, provê conexão à Internet a outros tipos de rede e aos clientes mesh, que podem acessar a rede através dos roteadores mesh, como também se conectando diretamente com outros clientes da rede.

4.4 MÉTRICAS DE ROTEAMENTO

Em redes sem fio, as métricas de roteamento (BROCH, 1998) que devem ser consideradas para a seleção do caminho são diferentes das métricas utilizadas em redes cabeadas, pois não existe a premissa da estabilidade na topologia, dada a mobilidade dos nós.

O roteamento em redes mesh e redes *ad-hoc* é feito de forma semelhante, porém com métricas distintas. Redes mesh oferecem suporte à qualidade de serviço (voz, dados e imagens), largura de banda mínima necessária à transmissão (avaliação do estado dos *links*), latência (escolha do caminho não necessariamente pelo mais curto, ou seja, com o menor número de saltos), segurança, níveis de congestionamento, disponibilidade de canais de freqüência, ganho de antena, energia de transmissão, níveis de ruído e erro. Todas estas métricas devem ser consideradas e podem variar mesmo em curto espaços de tempo, podendo inviabilizar diversas aplicações suportadas pela tecnologia mesh.

4.5 CONTROLE DE ACESSO AO MEIO

O controle de acesso ao meio (MAC) em redes mesh deve ser feito através de um mecanismo que seja eficiente e atrativo para os participantes dessas redes. Estas características devem estar presentes para que os nós da rede possam ter prioridade de acesso ao meio quando quiserem transmitir seus pacotes. Em troca desta prioridade, devem ceder seus recursos computacionais e servirem de nós intermediários para outros nós, que queiram transmitir para algum nó, que esteja fora de sua área de cobertura direta.

Os protocolos de camada MAC são caracterizados por operar em *Half-Duplex*. Os terminais geram interferência quando transmitem, que é percebida pelo receptor do próprio terminal, fazendo com que a detecção de colisões não seja possível enquanto os dados são enviados. Por este motivo, o controle de acesso ao meio em redes *ad-hoc* usa a estratégia baseada na tentativa de evitar a colisão, o que pode gerar desperdício do canal, pois as colisões são detectadas apenas ao final da transmissão. O mecanismo de controle de acesso ao meio deve ter condições ainda de tratar as variações do sinal recebido, pois o sinal sofre variações no tempo e com desvanecimento, o que faz com que o sinal recebido seja o somatório das cópias atenuadas do sinal transmitido.

Como numa rede mesh não há um ponto central ou servidor para controlar o acesso ao meio, os terminais "ouvem" o canal antes de iniciarem as suas transmissões, com o objetivo de verificar se seus vizinhos estão utilizando o canal. Caso o canal esteja desocupado ao seu redor, o terminal pode iniciar a sua transmissão. Esta estratégia diminui a chance de ocorrer uma colisão, mas leva aos problemas de terminal escondido e terminal exposto.

As redes sem fio mesh podem ser consideradas como a soma de várias redes vizinhas de um salto se sobrepondo de forma contínua, na qual existe a possibilidade de troca de informações entre nós que não estão ao alcance direto uns dos outros. Desta forma é necessário um maior controle, por parte dos nós, de seus canais de acesso para cobrir uma área maior, utilizando para isto as informações dos nós vizinhos.

4.6 POSSIBILIDADE DE INTERFERÊNCIA DEVIDO AO TERMINAL OCULTO

Em redes mesh o fenômeno do terminal oculto deve ser levado em consideração, devido ao fato de que transmissões podem não ser detectadas utilizando o CS (*Carrier Sense*). Um terminal da rede mesh poder ter somente alguns nós vizinhos diretos, mas muitos indiretos que podem não ter conhecimento mútuo. Portanto, somente os terminais intermediários podem informar a vizinhança indireta sobre a existência destes terminais ocultos.

Uma forma de minimizar o problema do terminal oculto é o *handshake* que estabelece a reserva do canal pela transmissão de mensagens curtas entre o transmissor e o receptor, antes da transmissão de dados. No IEEE 802.11 utiliza-se o RTS/CTS. O RTS enviado ao transmissor contém a duração da transmissão dos dados que serão enviados. O receptor responde transmitindo CTS que contém o mesmo valor de duração de transmissão. Qualquer dispositivo na vizinhança de ambos é notificado para evitar o congestionamento.

Como demonstrado na Figura 4.2, onde o terminal C não pode perceber a transmissão de A para B e supondo que o terminal A quer transmitir para o terminal B, C não receberá RTS de A, mas C receberá CTS de B. Neste caso, uma colisão pode ocorrer no envio de RTS por parte de A e C, sendo ambos endereçados para B.

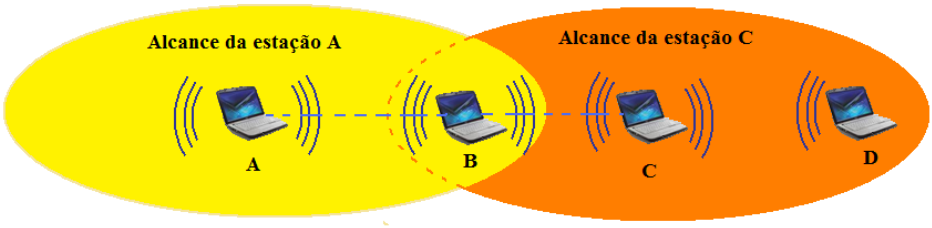

FIG. 4.2: Terminal oculto

4.7 CAPACIDADE NÃO UTILIZADA DEVIDO AO TERMINAL EXPOSTO

Um nó pode ser caracterizado como um terminal exposto se, de acordo com o protocolo aplicado, o nó decidir que o canal não está disponível, mesmo que sua transmissão simultânea a outra transmissão não cause uma interferência negativa. Como os terminais

expostos não são prejudiciais a outros dispositivos, a maior parte dos padrões de redes sem fio não os levam em consideração, mesmo que haja a perda de capacidade. No caso das redes mesh, o problema do terminal exposto deve ser considerado, já que a comunicação por múltiplos saltos torna o espectro de freqüência muito mais ocupado do que em outros tipos de rede de comunicação por um único salto. Isto gera perda de capacidade, como no caso do terminal oculto.

Na Figura 4.3 pode-se observar que nem todos os terminais estão ao alcance dos demais. Ainda assim, o terminal C não transmite para D se o terminal B estiver transmitindo para A, pois o terminal B terá enviado o RTS primeiro. O terminal C, querendo transmitir para D, deverá enviar o RTS depois para evitar uma suposta colisão, pois o RTS de B era endereçado para A e o terminal C não recebeu o CTS do terminal A e A enviará o reconhecimento de um quadro correto.

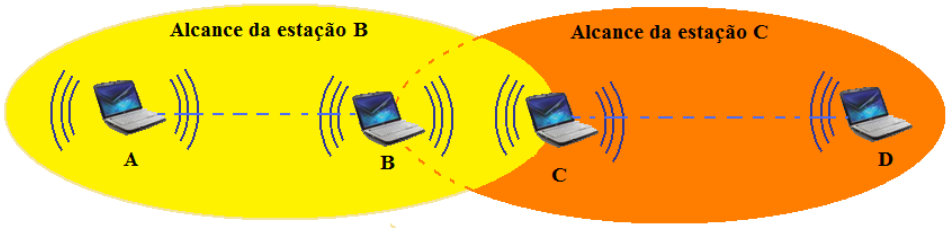

FIG. 4.3: Terminal exposto

4.8 PROTOCOLO DE ROTEAMENTO AODV

O protocolo AODV é um protocolo de roteamento proposto por (PERKINS, 1997) e é um dos protocolos utilizados no roteamento de redes móveis com alta mobilidade, pois se caracteriza por apresentar uma rápida adaptação às condições dos *links*, baixo processamento, baixa utilização de memória, menor número de pacotes de controle e a possibilidade de *loop* é mínima.

Na modalidade de um protocolo reativo, as rotas não são guardadas previamente em nenhuma tabela, somente são buscadas quando existe necessidade e as informações de rotas baseadas no vetor de distância são guardadas pelos próprios nós, que tem a capacidade de enviar, receber e transmitir pacotes nos modos *unicast* e *broadcast*, com a

premissa de que todos os nós que compõem a rede são de boa fé. A Figura 4.4 apresenta o protocolo AODV.

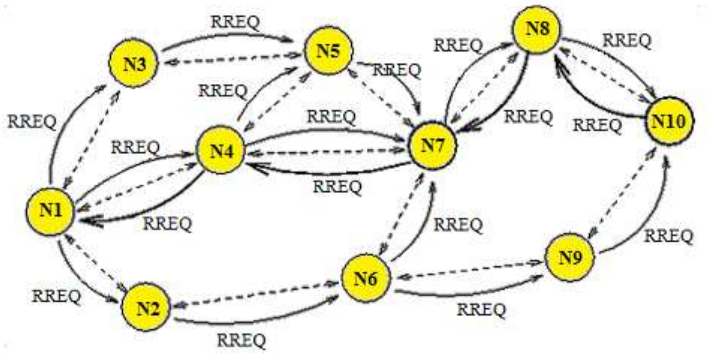

FIG. 4.4: AODV

O protocolo AODV se originou do algoritmo de vetor de distância (algoritmo de *Bellman-Ford*). Muitos protocolos originados deste algoritmo são pró-ativos, ou seja, os nós que compõem estas redes trocam constantemente informações sobre suas tabelas de roteamento, o que é muito dispendioso em termos de processamento para redes com muita mobilidade.

Já o protocolo AODV trabalha de forma reativa, ou seja, sob demanda, descobrindo as rotas somente quando são necessárias. Esta forma de descoberta de rotas toma mais tempo, comparado aos protocolos pró-ativos, quando em redes de baixa mobilidade, porém consomem menos processamento, pois não requer que os dispositivos guardem tabelas de rotas para todos os nós, mesmo as que não são necessárias.

As principais mensagens utilizadas neste protocolo são:

- Requisição de Rota - RREQ (*Route Request*): Este pacote é utilizado quando um dispositivo necessita enviar dados para algum outro dispositivo e este não está em sua tabela de roteamento como um nó de comunicação ativa;

- Resposta de Rota - RREP (*Route Replie*): Este pacote é a resposta a uma requisição de rota, sendo este nó o destino da requisição ou um nó intermediário do caminho até o destino final. Esta resposta é endereçada ao nó origem da requisição;

- Erros de Rota - RERR (*Route Error*): Este pacote é utilizado quando existe a perda

de algum *link* válido, com o objetivo de anunciar a necessidade de busca de uma nova rota, para todos os nós que utilizavam este caminho.

A tabela de roteamento deste protocolo guarda apenas as informações das conexões ativas, ou seja, dos caminhos que estão sendo utilizados em alguma comunicação. Como este protocolo é baseado no algoritmo de vetor de distância, são necessárias apenas as informações de distância e do próximo salto, não sendo necessário o armazenamento de todo o caminho. A otimização desta tabela torna o protocolo mais escalável e de fácil gerenciamento pelo processador, pois cada nó armazena somente o registro de quem fez a requisição, possibilitando a recomposição do caminho de volta, quando se alcança o destino desejado.

Quando o pacote de requisição de rota, retorna ao nó de origem, fica formado o caminho de ida e o nó que deseja enviar pacotes àquele destino armazena o caminho descoberto. No caso da chegada de várias respostas de rotas, será utilizada a que contiver o caminho mais curto e ao final de um certo tempo, as rotas que não chegam ao seu destino ou não são utilizadas, são descartadas.

Cada requisição de rota é composta da direção do nó de destino e do nó de origem e um identificador da direção é necessário, pois se um nó recebe uma requisição e não tem como atendê-la, a encaminha adiante aos seus vizinhos. Se a mesma requisição, porém, retorna a este nó intermediário, esta é ignorada para evitar a inundação da rede. Compõem também a requisição de rota, a hora lógica da última rota conhecida para aquele destino, para garantir que não sejam anunciadas rotas desatualizadas.

O funcionamento do protocolo AODV se dá quando existe a necessidade de comunicação entre nós em que a rota não é conhecida ou motivada por uma queda de link. Esta requisição de rota (RREQ) se dá através de um *broadcast* para toda a rede. Os nós, ao receberem a requisição de rota, verificam se eles próprios são os dispositivos para os quais se destina a rota requisitada, e caso não sejam, verificam se eles detêm uma rota atualizada para o nó a que se destina aquela requisição. Em caso afirmativo, o nó envia um pacote de resposta de rota (RREP) para o nó que gerou a requisição da rota. Caso contrário, o nó intermediário atualizará sua tabela e encaminhará a requisição para seus nós vizinhos, que deverão fazer o mesmo procedimento.

Devido à mobilidade que este tipo de rede prevê, os nós fazem o monitoramento constante dos *links* (somente das comunicações ativas) com seus vizinhos. Na ocorrência de algum problema, esta informação é repassada aos nós que utilizam estes caminhos, para que novas rotas sejam requisitadas. Desta maneira nenhum nó tem as informações de rotas de toda a rede, pois cada nó guarda para cada destino usado somente o primeiro salto por onde vai encaminhar os pacotes.

4.9 RESUMO DO CAPÍTULO

Neste capítulo apresentamos a tecnologia de redes mesh, com suas principais características e funcionalidades e sua importância frente à grande demanda de acesso a Internet. As redes mesh podem utilizar dispositivos WiFi, de baixo custo e bastante difundidos. Para aplicação em larga escala, além dos limites do *backbone* fixo, é necessário que outros nós participantes da rede, estejam dispostos a ceder seus recursos computacionais e de comunicação, para servirem de nós intermediários, ampliando assim a capacidade e a cobertura da rede.

O protocolo de roteamento AODV também foi apresentado com mais detalhes, pois é a base utilizada nas simulações para produção dos resultados. Nosso objetivo é o de investigar o impacto da cooperação entre os nós em uma rede mesh, e ainda, mostrar que a diferenciação de prioridades no acesso ao meio, para os nós cooperadores, traz melhoria na capacidade total da rede. No capítulo a seguir apresentamos a metodologia utilizada no desenvolvimento da solução proposta neste trabalho.

5 METODOLOGIA DE DESENVOLVIMENTO

Este capítulo descreve o desenvolvimento da solução e as implementações necessárias para este trabalho. Primeiramente é apresentada a estratégia da solução proposta. Em seguida, é apresentada a metodologia do desenvolvimento para simular o comportamento egoísta dos nós. Posteriormente é apresentada a implantação de prioridades na camada MAC. Ao final deste capítulo é apresentada a implementação da ferramenta Gresult, que gera a análise e a aferição do nível de cooperação dos nós, que compõem a rede mesh.

5.1 DESENVOLVIMENTO DA SOLUÇÃO

Em uma rede mesh estruturada de forma hierárquica, onde existam APs fixos funcionando como roteadores sem fio mesh em lugares pré-determinados, para fornecer serviço a outros dispositivos móveis WiFi, a banda total de tráfego desta rede fica limitada à capacidade do *backbone* mesh instalado.

Todo o desenvolvimento objetivou conseguir uma ampliação da capacidade de transmissão em uma rede mesh, aproveitando a possibilidade de comunicação direta entre os nós. Devido a mobilidade dos nós e com a necessidade de acesso à *Internet* ou à *Intranet* e dependendo da quantidade de nós na rede é possível afirmar que se os participantes cooperassem entre si, assumindo também o papel de nós intermediários, a comunicação seria otimizada e a banda total da rede pode crescer na proporção da quantidade de nós participantes, além de uma ampliação da área inicialmente coberta.

Devido aos nós terem características racionais, eles nunca tomam nenhuma ação contra seus próprios interesses, e por terem características egoístas, eles buscam apenas satisfazer seus interesses próprio (ROCHA, 2006). Com isso, as ações dos nós não visam, de forma alguma, alcançar o bem comum na rede, pois sua única motivação é alcançar seus objetivos individuais. Desta forma, seus protocolos estão voltados para obter o máximo de recursos da rede, com o menor dispêndio de recursos possíveis, só cedendo seus recursos computacionais e de comunicação se disso retirarem algum benefício. Neste trabalho

avaliamos a cooperação dos nós por meio de um mecanismo de aferição desta reputação, para que os nós que mais cedam seus recursos possam ter prioridade de acesso ao meio, com o objetivo de acesso à *Internet* ou à *Intranet*, em relação aos nós que cedam menos seus recursos ou não os cedam.

Para aferição dos nós que mais cooperam na rede, foi implementado um mecanismo que mede a quantidade de pacotes que cada nó (desempenhando o papel de nó intermediário) transmite de seus vizinhos. O mecanismo gera uma lista ordenada, para aferir mais prioridade aos nós que mais cooperam, de tal forma que quem necessita de muito acesso ao meio tem que ceder muito mais os seus recursos do que um nó que necessita de acesso esporádico.

Nas simulações foram consideradas as seguintes métricas:

- Nível de serviço provido aos nós cooperadores: o objetivo desta métrica foi avaliar a qualidade de serviço para acesso ao meio e sua evolução, para os nós participantes da rede que se dispõem a cooperar;

- Nível de serviço provido aos nós oportunistas: o objetivo desta métrica foi avaliar o quanto o mecanismo será eficiente em detectar e isolar os nós oportunistas, minimizando a qualidade de serviço para acesso ao meio e sua evolução, para os nós participantes da rede que não se dispõem a cooperar;

- *Throughput*: o objetivo desta métrica foi avaliar a capacidade de transmissão da rede, com e sem o mecanismo proposto.

As métricas foram analizadas utilizando-se o arquivo *trace* do simulador ns-2. O arquivo contém todas informações necessárias para o estudo e traz os resultados da quantidade de pacotes transmitidos e recebidos por cada um dos nós colaboradores e egoístas, pacotes descartados, tempos de transmissão e retardo, etc.

A Figura 5.1 apresenta um fluxograma da metodologia adotada na proposta, apresentando em módulos as diversas etapas do desenvolvimento da solução.

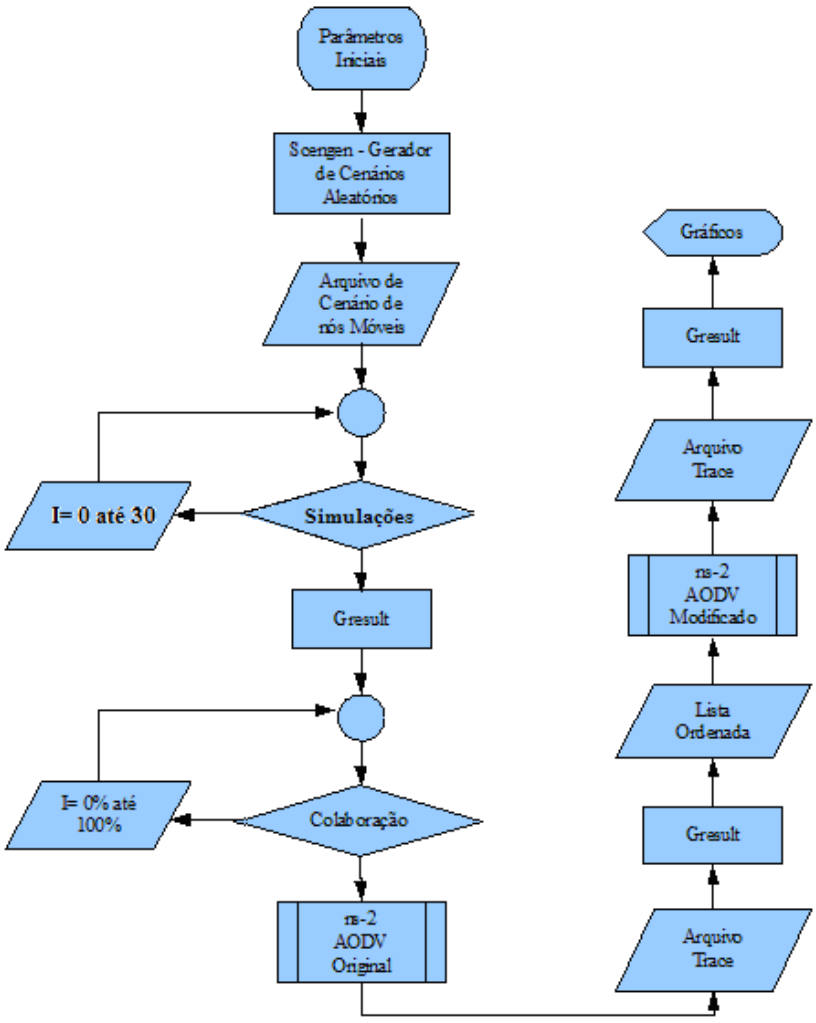

FIG. 5.1: Diagrama da metodologia

5.1.1 DESENVOLVIMENTO PARA SIMULAR O COMPORTAMENTO EGOÍSTA

Para utilização do mecanismo, foram feitas algumas alterações no protocolo original do AODV (NS). O protocolo de roteamento modificado foi denominado AODV_D (*Ad Hoc On-Demand Distance Vector - Drop*), que em relação ao AODV traz algumas alterações substanciais para que pudéssemos simular no ns-2 a diferenciação dos nós egoístas dos nós que cooperam.

As modificações feitas para gerar o AODV_D tiveram como objetivo o descarte de todos os pacotes recebidos dos nós vizinhos que um nó tentasse transmitir através de um outro nó intermediário com comportamento egoísta. As Figuras 5.2, 5.3 e 5.4

mostram a transmissão de um pacote através de um nó intermediário, com todas as estações utilizando o AODV.

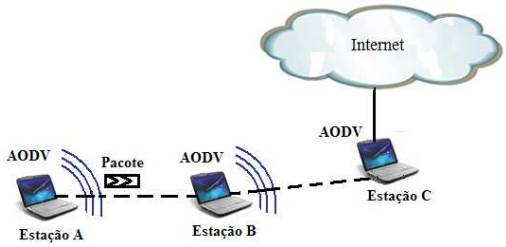

FIG. 5.2: Estação A quer transmitir para a estação C

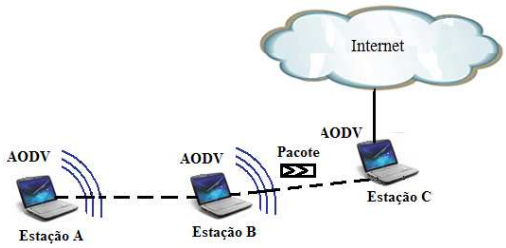

FIG. 5.3: A transmissão só é possível através da estação B (nó intermediário)

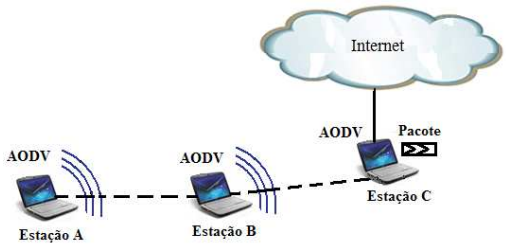

FIG. 5.4: Estação C recebe a transmissão da estação A com sucesso

Em (AL-SHURMAN, 2004) é apresentada a teoria do buraco negro (*Blackhole*) e em (LI, In International Conference on Ad-Hoc Networks and Wireless, Cancun, Mexico, 2008) é apresentada a teoria do buraco cinza, que foram a inspiração para gerar o comportamento não cooperativo através do descarte dos pacotes dos nós vizinhos. O objetivo

era simular um comportamento egoísta e seletivo com a possibilidade de privilegiar alguns nós, para obtermos uma melhoria no desempenho de uma rede mesh.

As Figuras 5.5 e 5.6 o comportamento egoísta, quando uma estação tenta transmitir um pacote através de um nó intermediário que utiliza o AODV_D.

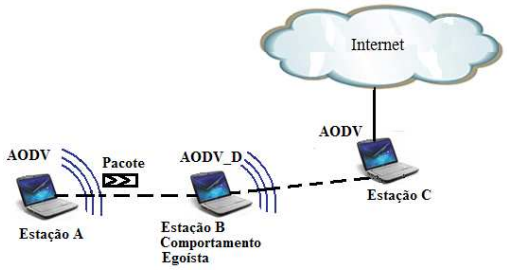

FIG. 5.5: Estação A quer transmitir para a estação C

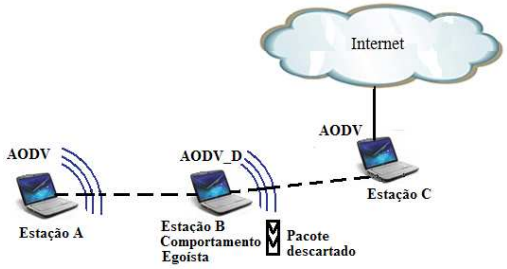

FIG. 5.6: A estação B descarta o pacote que deveria transmitir para C

As redes mesh trazem em si, como premissa, a característica de confiança entre os vizinhos para o encaminhamento dos pacotes a destinos além de seu alcance direto, porém um vizinho malicioso ou egoísta (ROCHA, 2006), pode atrair as rotas e encaminhar seletivamente apenas alguns pacotes, caracterizando uma espécie de sumidouro para a rede - buraco cinza. O nó egoísta, quando desempenhando o papel de nó intermediário para algum nó de sua vizinhança que deseja encaminhar pacotes a um outro destino, pode não encaminhar alguns ou todos os pacotes. Outro caso é quando um nó com comportamento egoísta informar que a rota existe e simplesmente não encaminhar os pacotes ou mesmo não informar a existência da rota, caracterizando um comportamento egoísta e não contribuindo para o melhor funcionamento possível da rede.

Uma forma de encaminhamento seletivo de pacotes é aquele que caracteriza o comportamento egoísta, no qual o nó não encaminha os pacotes de seus vizinhos, transmitindo apenas os seus próprios pacotes. Isto não necessariamente caracteriza um comportamento egoísta e sim pode significar um comportamento não cooperativo, com o objetivo de preservar seus recursos computacionais ou de energia.

Já a teoria do buraco negro, que não é objeto de estudo deste trabalho, é a situação extrema do encaminhamento seletivo, onde todos os pacotes são descartados pelo nó que está atraindo todos os pacotes da rede.

O protocolo AODV_D teve como base o AODV e inicialmente agirá da mesma forma que o protocolo original. As modificações no protocolo foram implementadas usando C++ e com o objetivo de estar apto para usar *scripts* TCL para simulações no ns-2. Todos os passos para criação do AODV_D estão descritos no Apêndice.

5.1.2 IMPLEMENTAÇÃO DE PRIORIDADES NA CAMADA MAC

Com o objetivo de diferenciar os nós da rede em quatro níveis de prioridade, implementamos novos protocolos MAC, aqui no código, chamados 802_11x, 802_11y e 802_11z. Esses novos protocolos serão similares ao 802_11, com algumas diferenças no procedimento de *backoff*. A tabela 5.1 apresenta as características de cada um dos protocolos com prioridades diferenciadas que propomos para a simulação.

TAB. 5.1: Protocolos com prioridades diferenciadas

Protocolo	Quantidade	CWinicial	CWmax	Incremento
Prioridade Categoria 1	20% dos nós	15	301	CW = CW+50
Prioridade Categoria 2	20% dos nós	31	501	CW= CW+100
Categoria Sem Prioridade	40% dos nós	31	1023	CW = CW x 2
Categoria Penalizada	20% dos nós	257	4097	CW = CW x 4

Os arquivos do protocolo 802_11 estão no diretório mac dentro do diretório base do ns-2. Os arquivos principais são mac-802_11.h / mac-802_11.cc e são usadas classes definidas em *mac-timers.h* e *mac-timers.cc*.

Todos os passos para a criação desses novos protocolos estão descritos no Apêndice.

5.1.3 IMPLEMENTAÇÃO DA FERRAMENTA GRESULT

Com a implementação do AODV_D funcionando no ns-2, possibilitando a diferenciação dos nós egoístas dos nós cooperadores em níveis percentuais de cooperação e com a criação dos protocolos de acesso ao meio com prioridade diferenciada, implementamos uma ferramenta para análise e aferição do nível de cooperação dos nós. A ferramenta mede a quantidade de pacotes que cada nó transmite de seus vizinhos, e gera uma lista ordenada do nível de cooperação.

O Gresult inicia a simulação de uma rede mesh no ns-2 com o cenário dado, variando a quantidade percentual de nós cooperadores. Para facilitar a análise dos resultados, os níveis de cooperação foram fixados em 0%, 25%, 50%, 75% e 100%.

O Gresult utiliza o arquivo trace de saída do ns-2, analisa e gera uma lista ordenada pelos nós que mais cooperam. A partir daí, a própria ferramenta afere para cada grupo de nós, segundo o nível de cooperação, um protocolo de prioridade diferenciada e reinicia a simulação, agora com as devidas diferenciações nas janelas de contenção dadas pelos diferentes algoritmos dos protocolos. Após esta nova simulação, o Gresult analisa novamente o arquivo trace de saída do ns-2, para comparação com os arquivos originais.

Assim pode ser dada mais prioridade de acesso ao meio àqueles nós que mais cooperam e os nós que menos cooperam podem inclusive ser penalizados, de tal forma que quem necessita de muito acesso ao meio, deve ter prioridade, e com isto há uma melhoria na quantidade total de pacotes transmitidos na rede como um todo.

O processo pode funcionar de forma dinâmica e recorrente, se automodelando até ser alcançada a melhor otimização da rede dado um determinado cenário.

5.2 RESUMO DO CAPÍTULO

Este capítulo apresentou as implementações necessárias para este trabalho. Apresentamos a metodologia do desenvolvimento para simular, no ns-2, o comportamento egoísta dos nós em uma rede mesh, a implementação de prioridades na camada MAC e a ferramenta Gresult. Esta ferramenta permite avaliar o nível de cooperação entre os nós, manipular as prioridades de acesso ao meio e gerar os resultados da simulação.

Todo o desenvolvimento objetivou avaliar o impacto da cooperação em uma rede mesh e possibilitou a obtenção dos resultados através das simulações, as quais apresentamos a seguir no Capítulo 5.

6 SIMULAÇÃO E RESULTADOS

O capítulo descreve as simulações e tudo o que foi utilizado para produzir os resultados deste trabalho: O simulador e as métricas utilizadas para avaliação do desempenho dos protocolos no ns-2, o cenário utilizado nas simulações e o programa gerador dos cenários, o modelo de tráfego, as características e os parâmetros da simulação, o intervalo de confiança dos resultados, os gráficos e os resultados alcançados.

6.1 SIMULAÇÃO NO NS-2

Todas as simulações foram feitas no simulador ns (*Network Simulator*) (NS2, 2008). O simulador ns-2 fornece suporte a redes sem fio, modelando o padrão IEEE 802.11 na camada física e na camada de enlace (MAC) usando o modo DCF.

O ns é um simulador para eventos discretos, utilizado para simulação de redes, pois provê suporte para simulações do TCP (*Transmission Control Protocol*), roteamento IP e alguns outros protocolos para redes locais. O ns-2 é um interpretador de *scripts TCL* orientado a objeto e contém uma biblioteca, com objetos de temporização de eventos, objetos de componentes de rede e módulos de suporte à configuração de redes. Após uma rodada de simulação, o ns produz arquivos em texto com as informação detalhada e relativa aos resultados da simulação, que podem ser visualizada através do NAM (*Network Animator*), que permite analisar os resultados da simulação através de uma interface gráfica amigável, permitindo controlar diversos fatores tal como velocidade.

As métricas utilizadas para comparar o desempenho dos protocolos foram:

- Quantidade de pacotes entregues - razão entre o número de pacotes entregues no destino e o número de pacotes gerados pela aplicação;
- Atraso de pacotes (dados) - inclui os possíveis atrasos causados na descoberta de rotas, propagação dos dados, retransmissões e tempo de transferência. Foram considerados os tempos a partir do instante que o pacote está pronto para transmitir e

quando ele é dado como recebido no destino pelo simulador;

- Número de pacotes (roteamento) - foram medidos os números de pacotes de roteamento dos protocolos AODV e AODV_D durante a simulação.

- Número de pacotes entregues (dados) - foram medidos os números de pacotes de dados entregues no destino.

6.1.1 GERAÇÃO DE CENÁRIOS

Para a simulação, utilizamos o programa *Scengen* (SCENGEN), que é um gerador de cenários aleatórios de mobilidade. O *Scengen* é um programa implementado em C++ e é capaz de gerar arquivos de movimentação aleatória de nós móveis (*trace*) em um padrão compatível com o simulador ns-2, podendo gerar os modelos de mobilidade (CAMP, 2002) do tipo *Waypoint, Fixed Waypoint, Brownian Motion, Mobility Model, Pursue Motion Model* e *Column Motion Model*.

Os parâmetros para geração dos modelos são definidos nos arquivos de configuração do *Scengen*:

- *Model-spec*: parâmetros admitidos por cada modelo;

- *Scen-spec*: parâmetros referentes ao cenário a ser simulado

  - Parâmetros globais: tamanho e forma da área de simulação e tempo de início e de término da simulação;

  - Parâmetros de definição dos grupos de mobilidade.

O cenário utilizado foi um campo na forma de quadrado com dimensões de 2000m x 2000m, divididos em 4 sessões iguais, com distribuição dos nós em 4 grupos, cada grupo formado por nós móveis e um nó fixo, além de nós móveis que ultrapassavam os limites de cada sessão.

Uma imagem instantânea de um dos cenários utilizados na simulação é mostrado na figura 6.1.

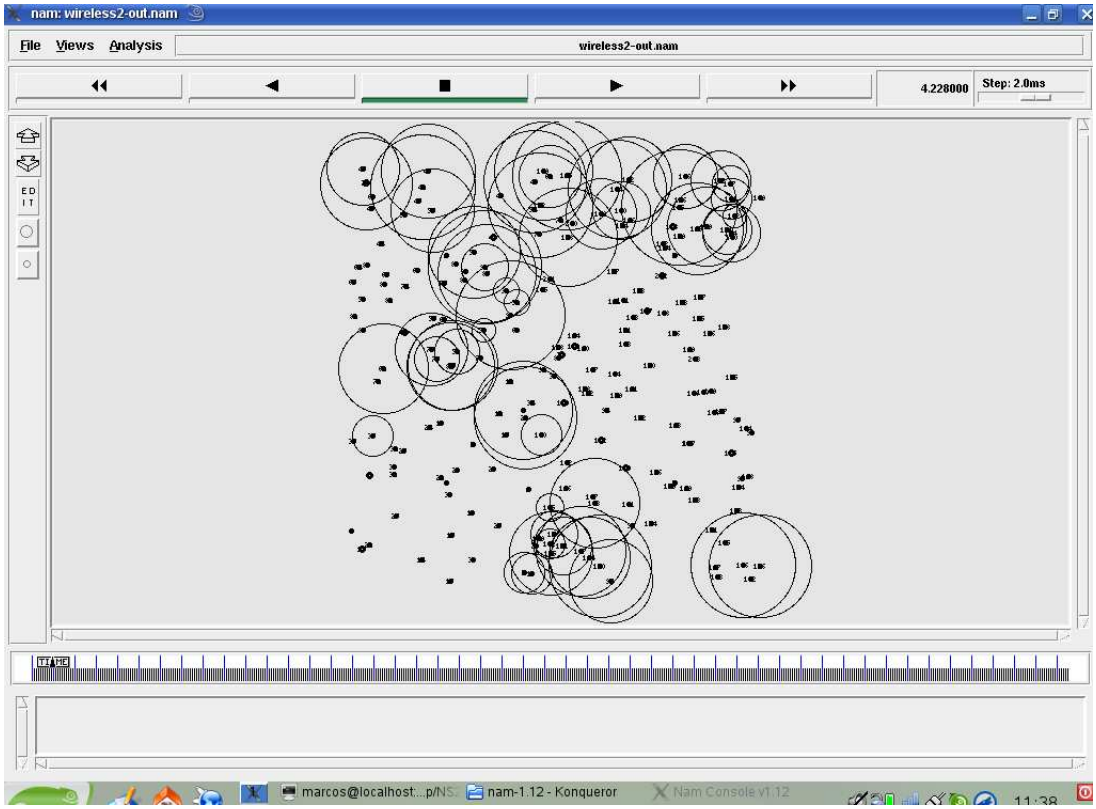

FIG. 6.1: Cenário da simulação

6.1.2 MODELO DE MOBILIDADE

Os modelos de mobilidade (CAMP, 2002) buscam representar a movimentação dos dispositivos móveis na rede. Existem os modelos de mobilidade individual, que representam a movimentação dos nós móveis de forma independente do restante dos nós da rede e os modelos de mobilidade em grupo (HONG, ACM/IEEE MSWiM'99, Seattle, WA, 1999), que representam a movimentação de um grupo como um todo, ou seja, o movimento de cada nó é dependente do movimento dos outros nós da rede.

Como sabemos que o desempenho de um protocolo depende diretamente do modelo de mobilidade, escolhemos para a simulação um modelo de mobilidade que pudesse representar o comportamento dos nós móveis no cenário desejado, ou seja, de comportamento espontâneo e aleatório. Por isto foi escolhido um modelo de mobilidade individual para avaliar o desempenho dos algoritmos de roteamento.

Para a simulação foi utilizado o modelo de mobilidade individual *Waypoint* para todos

os nós da rede. O modelo de mobilidade é definido no arquivo (*scen-spec*) do gerador do cenário *Scengen*.

O modelo de mobilidade *Random Waypoint* gera o percurso de um determinado nó móvel ligando dois pontos fixos no espaço, dentro dos limites do cenário. Desta forma, os nós permanecem parados por um determinado intervalo de tempo e segue para um outro ponto escolhido aleatoriamente, com velocidade uniformemente distribuída dentro do intervalo [Vmin,Vmax].

A movimentação dos nós não ultrapassou as bordas do cenário, ou seja, foram definidos os valores limites para a posição inicial e final dos nós e o modelo sempre irá gerar valores de posição dentro dos limites, respeitando a fronteira da área de simulação no ns2, não sendo necessário nenhum tratamento de regras de borda.

6.1.3 MODELO DE TRÁFEGO

A simulação foi baseada em fontes de tráfego CBR (*Constant Bit Rate*), com o objetivo de facilitar a análise dos resultados, tendo em vista que o tráfego TCP possui um mecanismo de controle de congestionamento, que implicaria em distorções na avaliação dos resultados da simulação (KUROSE, 2000).

A tabela 6.1 apresenta as características do tráfego CBR utilizado nas simulações. Onde X é um número aleatório entre 0 e 100 e Y é um número aleatório entre 0 e 50.

TAB. 6.1: Tráfego CBR

Descrição	Parâmetros	Intervalo
Inicio da Transmissão	Inicio_TX = X	[0 - 100] %
Fim da Transmissão	Fim_TX = X + Y + 20	[20 - 170] %
Tempo de Transmissão	T_TX = Fim_TX - Inicio_TX	[20 - 170] %

6.1.4 CARACTERÍSTICAS E PARÂMETROS DA SIMULAÇÃO

No mecanismo TCL implementado (*wless.200cbr4.0.06.tcl*) para simulação no ns-2, o intervalo de tempo de transmissão entre pacotes foi de 0.06s e o tamanho dos pacotes é fixo em 250 bytes. Foram utilizadas 4 faixas de prioridades, sendo denominadas de 802.11

(original do algoritmo) e 3 faixas de prioridades que foram criadas: 802.11++, 802.11+ e 802.11-. A 802.11+, como prioridade de categoria 2, que é algo melhor do que o 802.11 (original) e pior do que de prioridade de categoria 1, denominada 802.11++, e enquanto a categoria penalizada é a 802.11-, que é pior do que o 802.11 (original). A diferenciação das prioridades é feita através da manipulação da janela de contenção do mecanismo de *backoff*, tal como pode ser visto na Figura 6.2.

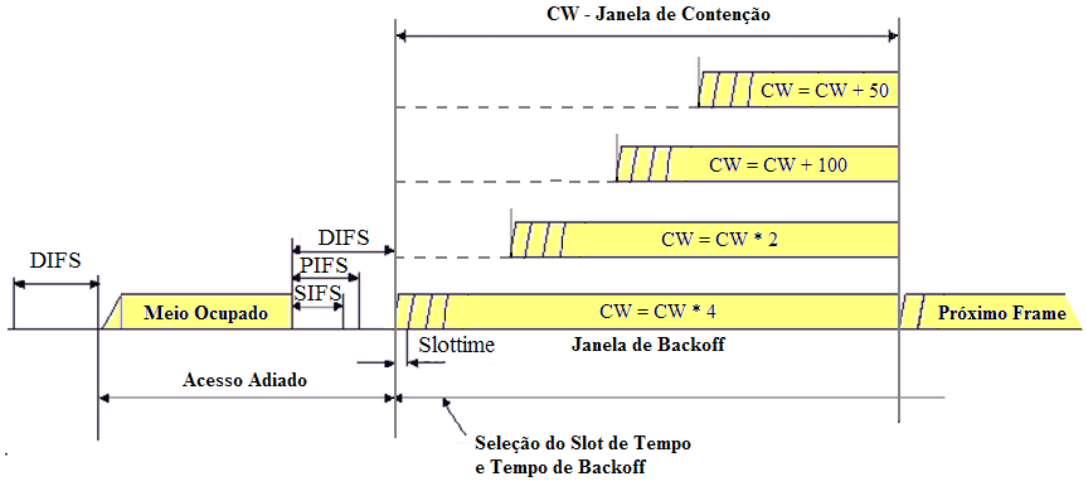

FIG. 6.2: Diferenciação de prioridade de acesso ao meio

Parâmetros da simulação:

- Tipo de rede: mesh;
- Número de nós móveis na rede: 200 (divididos em 4 grupos);
- Movimentação dos nós: A velocidade dos nós é determinada pelo gerador de cenários no intervalo de [5,15]m/s. O arquivo (*scen-spec*) do gerador de cenário tem como parâmetros defindos o $member\_model.V\_min = 5$ e o $member\_model.V\_max = 15$, que são os valores mínimos e máximos de velocidade do movimento. O *scengen*, no modelo *Waypoint*, usa uma distribuição uniforme para escolher valores dentro do intervalo especificado;
- Número de nós fixos: 4 (formando 4 grupos de mobilidade);
- Número de nós transmitindo: 100 (com tempo de inicio e término aleatórios);

- Área de simulação: 2000 m x 2000 m;
- Posição inicial dos nós: aleatoriamente posicionados (gerador de cenários);
- Trajetórias: aleatórias (gerador de cenários);
- Número de simulações: 30 rodadas;
- Tempo de simulação: 200 s (suficiente para satisfazer as métricas, pois o período transiente nesta configuração não influenciou os resultados da simulação (DUNCAN, 2006));
- Protocolo de roteamento: AODV e AODV_D;
- Intervalo entre os pacotes: 0,06s (BONFIGLIO, 2008);
- Tamanho dos pacotes: Fixo de 250 bytes (BONFIGLIO, 2008);
- Tipo de tráfego: CBR (*Constant Bit Rate*) uniformemente distribuído;
- Taxa de transmissão dos nós: fixa em 1Mbps independente da distância e definida no arquivo ns-mac.tcl (os pacotes de controle são definidos por Mac/802_11 set basicRate_ 1Mb e os pacotes de dados por Mac/802_11 set dataRate_ 1Mb), com tempo de inicio e término aleatórios;
- Número máximo de saltos de um nó origem até o destino (Nó ou AP): Para o AODV e AODV_D é de 7 hops (aodv/aodv.h: #define TTL_THRESHOLD 7);

6.2 INTERVALO DE CONFIANÇA

A análise estatística dos dados da simulação possibilitou determinar o grau de confiança, expresso pelo intervalo de confiança, ou seja, um intervalo de valores em torno da estimativa que contenha o valor com uma dada probabilidade.

Para este trabalho avaliamos a média de uma distribuição normal com variância desconhecida, ou seja, avaliamos a quantidade de pacotes transmitidos de seus vizinhos por cada um dos nós, como tendo uma distribuição normal e objetivamos fazer a inferência sobre a média que é desconhecida, obtendo um intervalo de confiança.

Em nossas simulações um certo número de nós foi selecionado aleatoriamente e teve a quantidade de pacotes transmitidos de seus vizinhos calculados a partir dos dados obtidos no arquivo de saída do ns-2. O intervalo de confiança para média desta distribuição normal, tendo sua média desconhecida é apresentado na tabela 6.2.

TAB. 6.2: Intervalo de confiança

Nível de Cooperação	Algoritmo de Backoff	Taxa de Sucesso Média	Desvio Padrão	Intervalo de Confiança 90%	Intervalo de Confiança 95%	Intervalo de Confiança 99%
0%	Normal	18,27%	2,19%	0,66%	0,78%	1,03%
0%	Modificado	18,45%	2,23%	0,67%	0,80%	1,05%
25%	Normal	23,13%	2,30%	0,69%	0,82%	1,08%
25%	Modificado	25,28%	2,67%	0,80%	0,96%	1,26%
50%	Normal	28,99%	2,77%	0,83%	0,99%	1,30%
50%	Modificado	31,62%	3,18%	0,96%	1,14%	1,50%
75%	Normal	34,20%	2,39%	0,72%	0,86%	1,13%
75%	Modificado	38,39%	2,24%	0,67%	0,80%	1,05%
100%	Normal	38,66%	2,17%	0,65%	0,78%	1,02%
100%	Modificado	42,58%	3,02%	0,91%	1,08%	1,42%

6.3 GRÁFICOS

Os gráficos a seguir foram resultados de 30 rodadas de simulações com nós colaboradores de 0% até 100%, *backoff* normal e *backoff* diferenciado.

No gráfico da figura 6.3 os primeiros resultados são apresentados na forma do gráfico dados pela função de distribuição cumulativa - CDF (*Cumulative Distribution Function*) e apresenta 10 curvas na mesma imagem, para uma melhor comparação. Ele mostra os resultados para 100 nós transmitindo com taxa de sucesso de 0% a 100% com e sem o mecanismo de priorização (*backoff* normal e *backoff* diferenciado).

O gráfico foi gerado com os resultados colhidos da simulação com 200 nós, sendo apenas 100 nós transmissores. As duas primeiras curvas quase não apresentam diferença, isto é, com 0% de colaboração, praticamente pouca diferença faz entre mudar o *backoff* ou não. Para os 4 pares de curvas restantes, a versão 2 com o *backoff* diferenciado para os nós cooperadores, apresentam resultados melhores, principalmente para os casos com 50% e 75% de nós colaboradores.

Na primeira rodada da simulação os nós atuam normalmente de acordo com as características do algoritmo original, o mecanismo analisa o arquivo de saída do ns-2 e gera uma

lista ordenada com a quantidade de pacotes encaminhados de seus vizinhos por cada um dos nós, desta forma o mecanismo afere diferentes protocolos a grupos de nós de acordo com a quantidade de pacotes encaminhados. Por convenção, os 20% dos nós que mais encaminharam pacotes dos outros, receberam a prioridade de categoria 1, que incrementa a janela de contenção com o fator 50%, os 20% seguintes receberam a prioridade de categoria 2, os 120 nós do meio da lista (40% dos nós) receberam a prioridade original do 802.11 e os 40 últimos (20% dos nós) a de prioridade z, com o objetivo de simular uma penalização.

O gráfico mostram a evolução da taxa de sucesso na medida em que o percentual de nós que cooperam aumenta, e ainda mostra que existe uma melhoria significativa da primeira para a segunda rodada, que é quando é aplicado o mecanismo de diferenciação do *backoff* com a alteração das regras na janela de contenção, quando há colisões. Pode-se ainda concluir que em todas as segundas rodadas chegaram mais pacotes ao destino do que nas primeiras rodadas.

No gráfico cada curva é feita com 100 pontos, pois apenas 100 nós transmitiram dados e os outros 100 nós poderiam encaminhar pacotes, caso fossem colaboradores.

Um ponto a ser notado é que essa curva "esconde" um pouco o resultado, pois não apresenta o volume total de dados que cada nó transmitiu, apenas a taxa de sucesso. Essa taxa nada mais é do que o total de bytes transmitidos com sucesso (que chegaram ao destino) sobre o total de *bytes* transmitidos por um determinado nó N.

O gráfico da figura 6.3 mostra os resultados para 100 nós transmitindo com taxa de sucesso de 0% a 100% com e sem o mecanismo de priorização (*backoff* normal e *backoff* diferenciado).

Para explicitar melhor o resultado do mecanismo foram gerados mais dois grupos de gráficos para cada simulação com diferentes percentuais de nós colaboradores. O primeiro gráfico mostra os resultados na forma de um histograma, ou seja, o tamanho de cada linha vertical representa a quantidade de dados transmitidos por cada nó. O eixo y indica o número total de pacotes transmitidos e o eixo x indica apenas o número do nó. Os resultados mostram que os nós transmitiram mais dados após a alteração do *backoff*.

Já o segundo grupo de gráficos representam o mesmo resultado, porém os valores foram

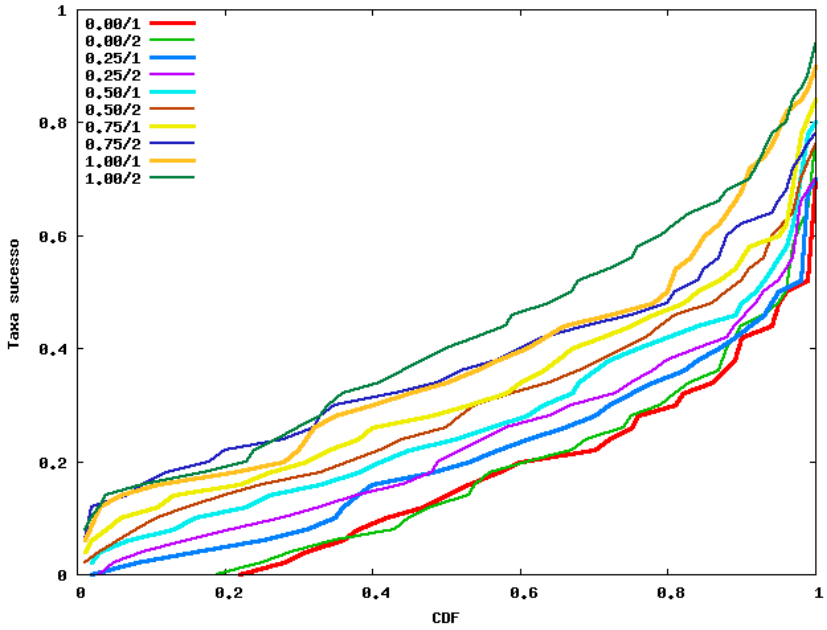

FIG. 6.3: Taxa de sucesso com 100 nós transmitindo de 0% a 100% de colaboradores

ordenados em ordem crescente. Perde-se desta forma a visão de cada nó, mas pode-se observar melhor o ganho na performance da rede com a aplicação do mecanismo.

O gráfico da figura 6.4 mostra os resultados na forma de histograma com taxa de 0% de nós colaboradores, simulação com 100 nós transmitindo, que demonstra um aumento efetivo total de 2,98% na taxa de transmissão da rede.

O gráfico da figura 6.5 mostra os resultados com taxa de 0% de nós colaboradores, simulação com 100 nós transmitindo, que demonstra um aumento efetivo total de 2,98% na taxa de transmissão da rede.

O gráfico da figura 6.6 mostra os resultados na forma de histograma com taxa de 25% de nós colaboradores, simulação com 100 nós transmitindo, que demonstra um aumento efetivo total de 9,38% na taxa de transmissão da rede.

O gráfico da figura 6.7 mostra os resultados com taxa de 25% de nós colaboradores, simulação com 100 nós transmitindo, que demonstra um aumento efetivo total de 9,38% na taxa de transmissão da rede.

O gráfico da figura 6.8 mostra os resultados na forma de histograma com taxa de 50% de nós colaboradores, simulação com 100 nós transmitindo, que demonstra um aumento efetivo total de 9,25% na taxa de transmissão da rede.

O gráfico da figura 6.9 mostra os resultados com taxa de 50% de nós colaboradores, simulação com 100 nós transmitindo, que demonstra um aumento efetivo total de 9,25% na taxa de transmissão da rede.

O gráfico da figura 6.10 mostra os resultados na forma de histograma com taxa de 75% de nós colaboradores, simulação com 100 nós transmitindo, que demonstra um aumento efetivo total de 13,60% na taxa de transmissão da rede.

O gráfico da figura 6.11 mostra os resultados com taxa de 75% de nós colaboradores, simulação com 100 nós transmitindo, que demonstra um aumento efetivo total de 13,60% na taxa de transmissão da rede.

O gráfico da figura 6.12 mostra os resultados na forma de histograma com taxa de 100% de nós colaboradores, simulação com 100 nós transmitindo, que demonstra um aumento efetivo total de 9,91% na taxa de transmissão da rede.

O gráfico da figura 6.13 mostra os resultados com taxa de 100% de nós colaboradores, simulação com 100 nós transmitindo, que demonstra um aumento efetivo total de 9,91% na taxa de transmissão da rede.

6.4 RESUMO DO CAPÍTULO

A tabela 6.3 apresenta o resumo dos resultados obtidos nas simulações de acordo com a quantidade percentual de nós colaboradores. São apresentados os resultados utilizando o mecanismo de backoff original e também os resultados quando é utilizado o mecanismo de backoff modificado, onde são priorizados os nós mais colaboradores, avaliados na primeira rodada de simulação. Os resultados mostram que com a utilização do mecanismo de backoff modificado, pode-se observar a melhoria de performance da rede, com o aumento da transmissão total de pacotes.

A diferença na evolução da taxa de 9,91% com 100% de colaboradores, comparada a taxa de 13,60% com 75% de nós colaboradores, foi causada pelo fato de que se todos cooperam a diferenciação de prioridades no aceeso ao meio, já não causa tanta diferença, apesar de que a quantidade total de *bytes* transferidos foi maior.

TAB. 6.3: Totais de *bytes* transferidos na rede

Colaboradores	*Backoff* Original	*Backoff* Modificado	Melhoria
0% dos nós	32.133KB	33.092KB	2.98%
25% dos nós	40.352KB	44.139KB	9.38%
50% dos nós	50.966KB	55.680KB	9.25%
75% dos nós	60.317KB	68.520KB	13.60%
100% dos nós	70.443KB	77.422KB	9.91%

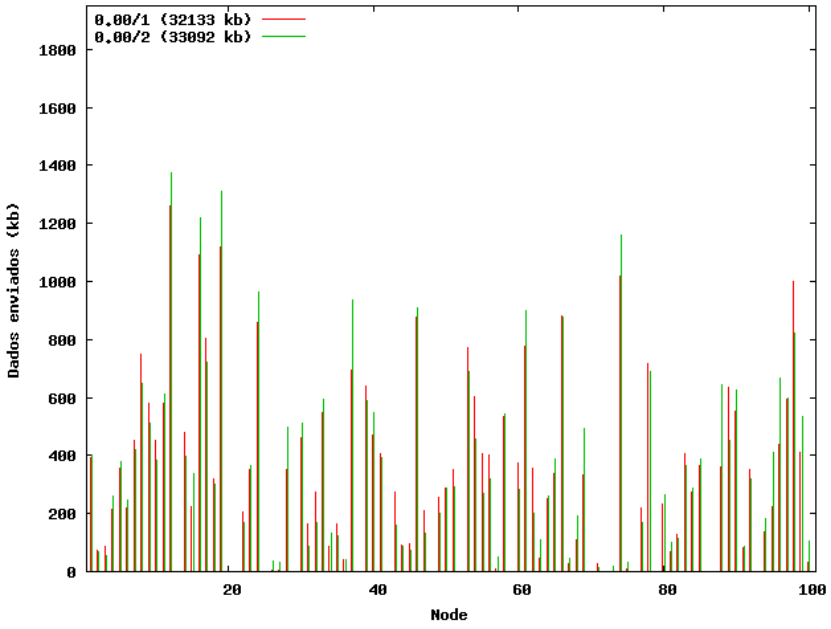

FIG. 6.4: Histograma com 0% de nós colaboradores

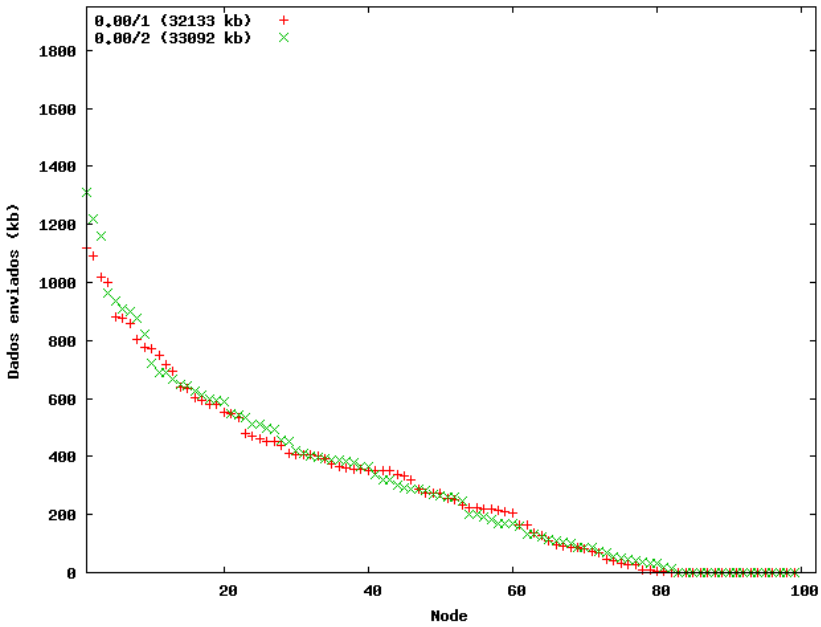

FIG. 6.5: Distribuição de dados enviados com 0% de nós colaboradores

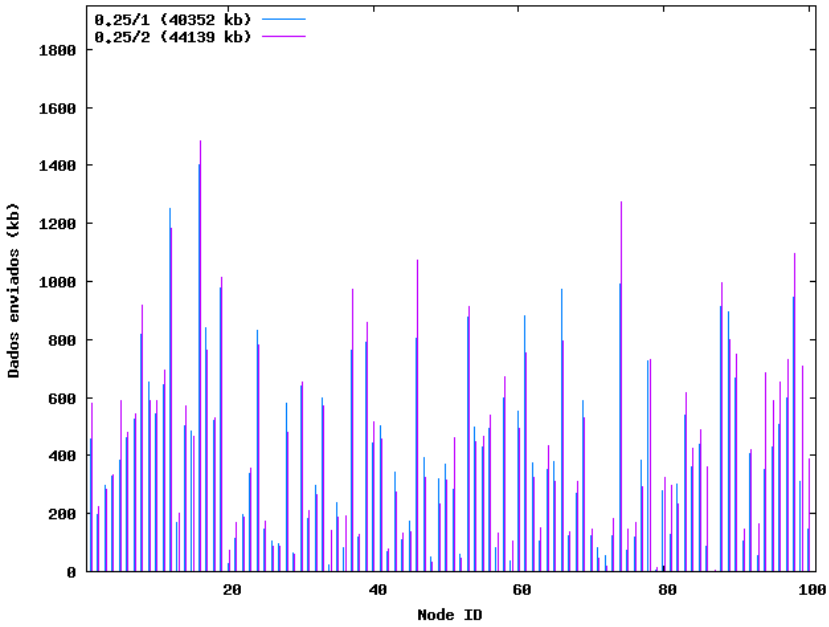

FIG. 6.6: Histograma com 25% de nós colaboradores

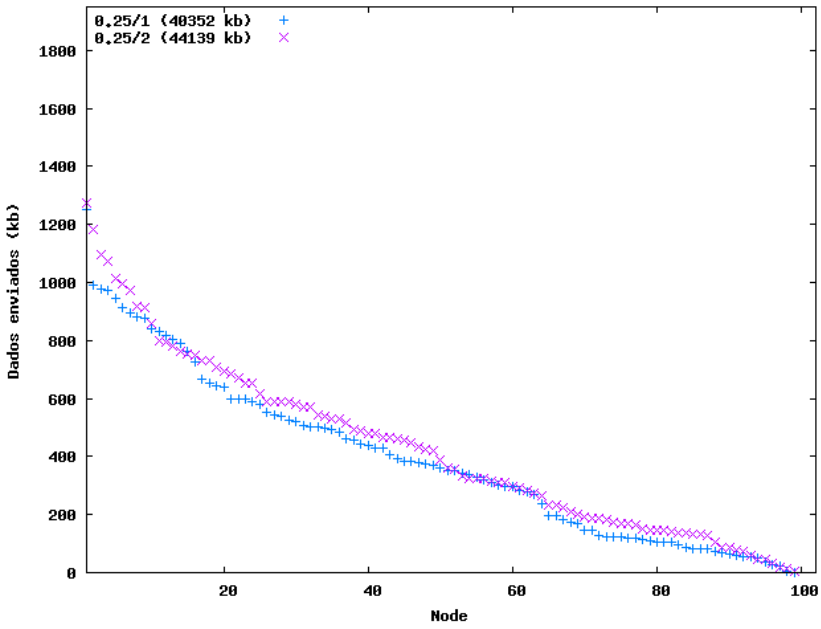

FIG. 6.7: Distribuição de dados enviados com 25% de nós colaboradores

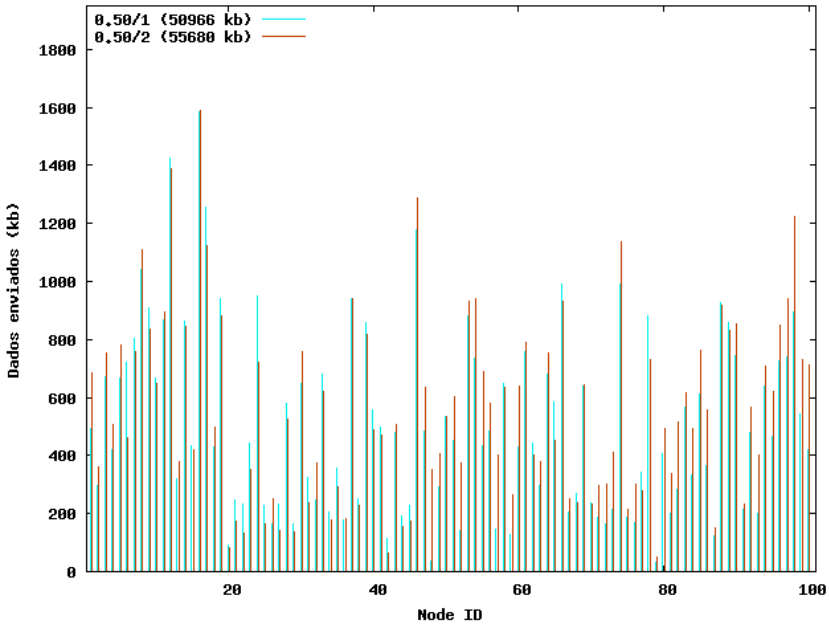

FIG. 6.8: Histograma com 50% de nós colaboradores

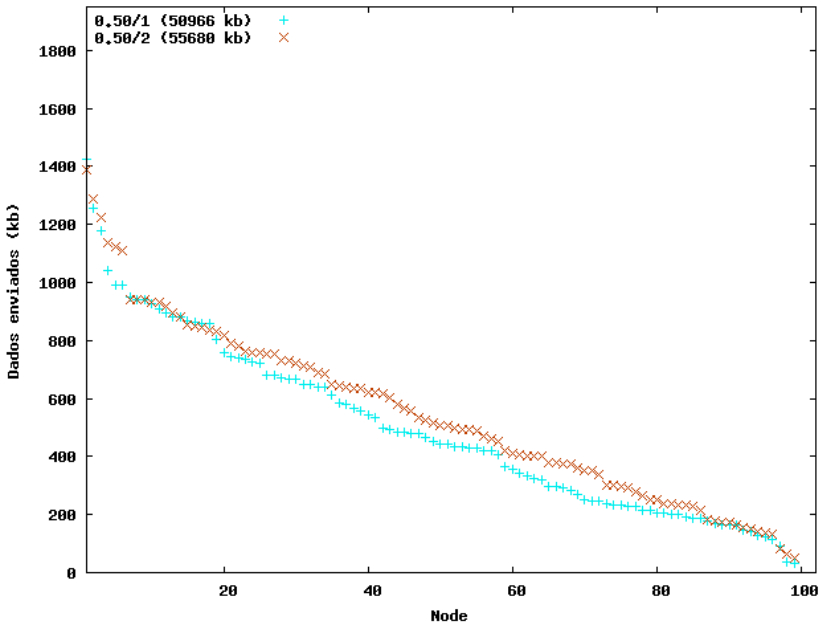

FIG. 6.9: Distribuição de dados enviados com 50% de nós colaboradores

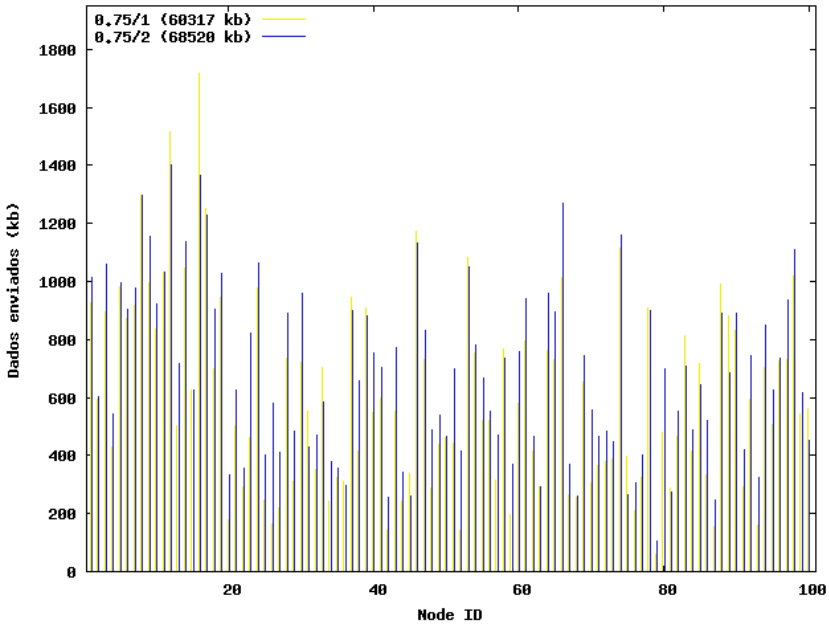

FIG. 6.10: Histograma com 75% de nós colaboradores

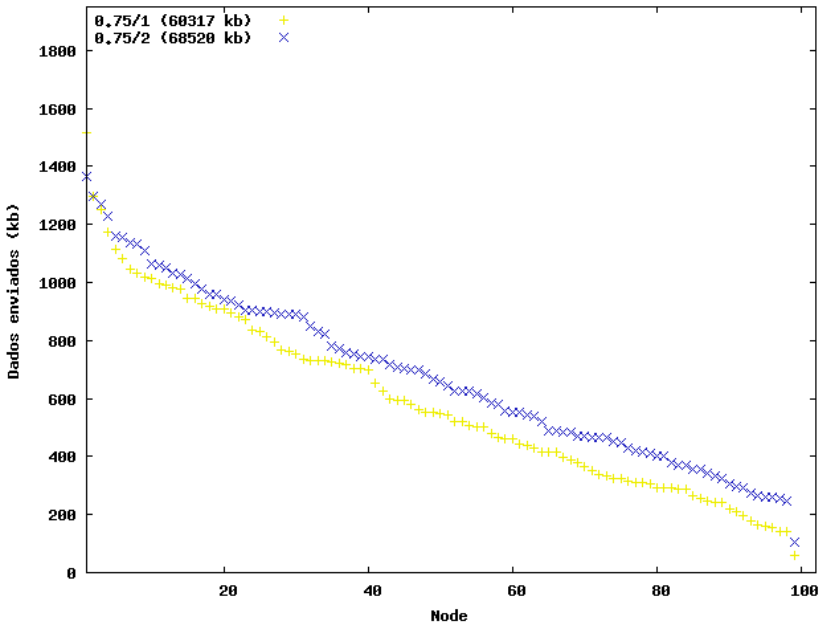

FIG. 6.11: Distribuição de dados enviados com 75% de nós colaboradores

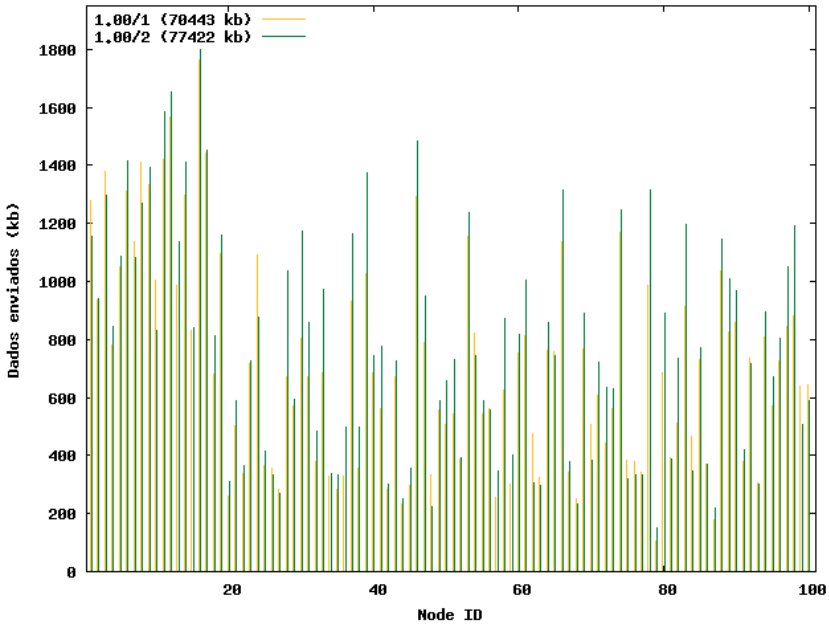

FIG. 6.12: Histograma com 100% de nós colaboradores

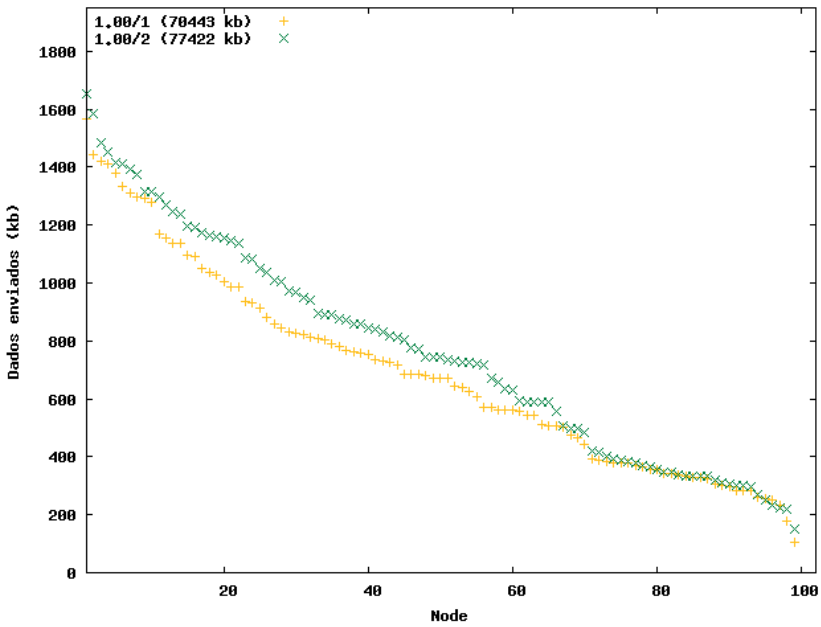

FIG. 6.13: Distribuição de dados enviados com 100% de nós colaboradores

7 CONSIDERAÇÕES FINAIS

A proposta de uma nova abordagem para redes mesh se mostrou viável. Aproveitando a característica egoísta dos nós, com a geração da motivação necessária através de conceito de reputação, com os participantes da rede disponibilizando seus recursos, para em troca ter prioridade de acesso ao meio, apresentou resultados satisfatórios.

As redes mesh passam a ser uma alternativa viável. A maioria das redes existentes é formada por topologias do tipo estrela composta de infra-estrutura centralizada. Em redes mesh os equipamentos existentes, do tipo WiFi, agregam a possibilidade de redes maiores, geograficamente falando, de menor custo de implantação e com uma capacidade de transmissão muito além da capacidade do *backbone*, uma vez que existe a possibilidade de transmissão através de múltiplos caminhos, em múltiplos saltos e da comunicação direta entre os nós e com mecanismos mais robustos de segurança. Há ainda, a possibilidade de se auto-organizar dinamicamente quando em crescimento, por conta, por exemplo, da entrada de novos nós na rede, ou quando há quebra de alguma rota ou a saída de algum nó da rede.

Este trabalho aproveitou a característica de uma rede mesh que é o fato de um nó origem poder chegar a um nó destino através de múltiplos saltos e por múltiplos caminhos, podendo utilizar os nós intermediários da rede em malha.

O primeiro objetivo deste trabalho foi avaliar o impacto do nível de cooperação dos nós em uma rede mesh, onde se avaliou a cooperação entre os participantes de uma rede é relevante ou não na performance de transmissão total de pacotes nesta rede e em que proporção. Os resultados alcançados neste trabalho, através das simulações feitas, demonstram que existe realmente uma relação direta entre o nível de cooperação dos nós da rede e a quantidade de pacotes transmitidos com sucesso. Mesmo em um ambiente de mobilidade, à medida que a cooperação aumenta entre os participantes de uma rede mesh, a quantidade total de pacotes transmitidos aumenta também, aumentando a capacidade total de transmissão da rede.

O segundo objetivo deste trabalho foi o de implementar e simular um mecanismo que pudesse exercer um controle da reputação dos nós móveis de uma rede mesh, para identificá-los e escaloná-los numa lista segundo a quantidade de pacotes transmitidos de seus vizinhos, os nós mais cooperadores de forma espontânea; e num segundo momento, aferir níveis diferentes de prioridades de acesso ao meio para os participantes da rede que mais disponibilizem os seus recursos, dando a estes uma maior prioridade de acesso ao meio, através do controle do mecanismo de *backoff*, e ainda restringir o acesso aos nós egoístas que objetivam somente seus interesses individuais.

A seleção e o controle de prioridades aqui propostos se aplicam a redes de ambientes com perfil definido por uma identidade como: universidades, centros de convenções, prédios inteligentes e parques industriais. Os resultados demonstram que o mecanismo implementado, aferindo prioridades diferentes de acesso ao meio, pode induzir os participantes à cooperação em redes mesh e os resultados comprovam ainda que através deste mecanismo é possível obter melhorias significativas na capacidade total de transmissão de pacotes da rede superiores a 13%.

Por fim, o trabalho demonstra a possibilidade que projetos de redes mesh possam ser feitos com menor número de roteadores na infra-estrutura básica do *backbone*, pois a totalidade da cobertura poderia se dar através dos nós intermediários, que surgirão de forma espontânea na rede através da cooperação motivada por uma maior prioridade de acesso ao meio. Outro benefício é a possibilidade de comunicação direta entre os participantes da rede sem sobrecarregar o *backbone*, propiciando um aumento substancial da largura de banda passante total da rede.

7.1 TRABALHOS FUTUROS

Os resultados e conclusões deste trabalho abrem a possibilidade de alguns desdobramentos em trabalhos futuros, tais como:

- Aplicação no mecanismo proposto de algoritmos apresentados em diversos trabalhos baseados na teoria dos jogos para controle através do conceito de reputação dos nós egoístas, como estratégia para aumentar a confiabilidade e justiça no compartilhamento dos recursos em redes mesh;

- Aprimoramento dos níveis de prioridade propostos neste trabalho, tornando-os dinâmicos e lineares de acordo com o nível de cooperação entre os nós de uma rede mesh;
- Definir novas aplicações possíveis em redes mesh que atendam outras características de distribuição geográfica de cenários, com a possibilidade de ampliação da área de cobertura ou da ampliação da capacidade do *backbone*, através de mecanismos de incentivo com a manipulação do *backoff*;
- Avaliar a melhor relação entre disponibilidade e cobertura de uma rede mesh com o controle de reputação investigado.

8 REFERÊNCIAS BIBLIOGRÁFICAS

AGUIAR, E., BITTENCOURT, P., MOREIRA, W. e ABELÉM, A. G. **Estudo comparativo de protocolos de roteamento para redes mesh na região amazônica**. Em SBRC Belém, 2007.

AKYILDIZ, I., WANG, X. e WANG, W. **Wireless mesh networks: A survey**. p. 445–487, Phoenix, AZ, USA, 2005. Computer Networks, 47. ISBN Computer Networks, 47.

AL-SHURMAN, Mohammad, YOO, Seong-Moo e PARK, Seungjin. **Black hole attack in mobile ad hoc networks**. Em ACM-SE 42: Proceedings of the 42nd annual Southeast regional conference, p. 96–97, New York, NY, USA, 2004. ACM. ISBN 1-58113-870-9.

BANDYOPADHYAY, Seema e BANDYOPADHYAY, Subhajyoti. **A game-theoretic analysis on the conditions of cooperation in a wireless ad hoc network**. Em WiOpt, p. 54–58, 2005.

BHARGHAVAN, Vaduvur, DEMERS, Alan, SHENKER, Scott e ZHANG, Lixia. **Macaw: a media access protocol for wireless lan's**. Em SIGCOMM '94: Proceedings of the conference on Communications architectures, protocols and applications, p. 212–225, New York, NY, USA, 1994. ACM. ISBN 0-89791-682-4.

BICKET, John, AGUAYO, Daniel, BISWAS, Sanjit e MORRIS, Robert. **Architecture and evaluation of an unplanned 802.11b mesh network**. Em MobiCom '05: Proceedings of the 11th annual international conference on Mobile computing and networking, p. 31–42, New York, NY, USA, 2005. ACM. ISBN 1-59593-020-5.

BONFIGLIO, D., MELLIA, M., MEO, M., RITACCA, N. e ROSSI, D. **Tracking down skype traffic**. p. 261–265, Phoenix, AZ, USA, 2008. INFOCOM 2008. The 27th Conference on Computer Communications. IEEE Publication. ISBN 10.1109/INFOCOM.2008.61.

BROCH, Josh, MALTZ, David A., JOHNSON, David B., HU, Yih-Chun e JETCHEVA, Jorjeta. **A performance comparison of multi-hop wireless ad hoc network routing protocols**. Em Mobile Computing and Networking, p. 85–97, 1998. URL `citeseer.ist.psu.edu/broch98performance.html`.

CAMP, T., BOLENG, J. e DAVIES, V. **A survey of mobility models for ad hoc network research**. Wireless Communications and Mobile Computing (WCMC): Special issue on Mobile Ad Hoc Networking: Research, Trends and Applications, v. 2, n. 5, p. 483–502, 2002. URL `http://citeseer.ist.psu.edu/camp02survey.html`.

CISCO. **Rede Mesh na cidade de Tiradentes, MG**. http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns348/ns621/networking_solution_case_study_tiradentes_brazil_vod.html.

CORSON, S. e MACKER, J. **Mobile ad hoc networking (manet): Routing protocol performance issues and evaluation considerations**. p. 445–487, United States, 1999. RFC Editor. ISBN RFC.

DRAVES, Richard, PADHYE, Jitendra e ZILL, Brian. **Routing in multi-radio, multi-hop wireless mesh networks**. Em MobiCom '04: Proceedings of the 10th annual international conference on Mobile computing and networking, p. 114–128, New York, NY, USA, 2004. ACM. ISBN 1-58113-868-7.

DUNCAN, I. B. **Modelagem e análise do protocolo ieee 802.11**. Em SBRC, 2006.

ERGEN, M. **Ieee 802.11 tutorial**, 2002. URL `http://citeseer.ist.psu.edu/article/ergen02wtrpwireless.html`.

HARDT, Michael e NEGRI, Antonio. **O que é a multidão?** Em WiOpt, p. 16, 2008. URL `http://www.cebrap.org.br/imagens/Arquivos/o_que_e_a_multidao.pdf`.

HE, Yifeng, STIMPSON, Brad, LEE, Ivan, GU, Xijia e GUAN, Ling. **Adaptive peer to peer streaming over hybrid wireless networks**. Int. J. Intell. Syst. Technol. Appl., v. 3, n. 3/4, p. 257–276, 2004. ISSN 1740-8865.

HONG, X., GERLA, M., PEI, G. e CHIANG, C. **A group mobility model for ad hoc wireless networks**, ACM/IEEE MSWiM'99, Seattle, WA, 1999. URL `citeseer.ist.psu.edu/hong99group.html`.

ILERI, Omer, MAU, Siun-Chuon e MANDAYAM, Narayan B. **Pricing for enabling forwarding in self-configuring ad hoc networks**. IEEE Journal on Selected Areas in Communications, v. 23, n. 1, p. 151–163, 2005. URL `http://jmvidal.cse.sc.edu/library/ileri05a.pdf`.

KUROSE, James F. e ROSS, Keith W. **Computer Networking: A Top-Down Approach Featuring the Internet Package**. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2000. ISBN 0201477114.

LAI, K., FELDMAN, M., STOICA, I. e CHUANG, J. **Incentives for cooperation in peer-to-peer networks**, In Workshop on Economics of Peer-toPeer Systems, 2003. URL `citeseer.ist.psu.edu/lai03incentives.html`.

LI, Zhenjiang e GARCIA-LUNA-ACEVES, J.J. **Enhancing the security of on-demand routing in ad hoc networks**, In International Conference on Ad-Hoc Networks and Wireless, Cancun, Mexico, 2008. URL `citeseer.ist.psu.edu/li05enhancing.html`.

MESH, 2008. **Redes Mesh: Mobilidade, Qualidade de Serviço e Comunicação**. `www.midiacom.uff.br/schara/publications/Minicurso-Mesh-completo.pdf`.

NS. **Tutorial of 802.11 Implementation in ns-2**. http://www.winlab.rutgers.edu/ zhibinwu/pdf/tr_ns802_11.pdf .

NS2, 2008. **The Network Simulator NS-2**. http://www.isi.edu/nsnam/ns/ns-documentation.html.

PANG, Qixiang, LIEW, Soung C., LEE, Jack Y. B. e LEUNG, Victor C. M. **Performance evaluation of an adaptive backoff scheme for wlan: Research articles**. Wirel. Commun. Mob. Comput., v. 4, n. 8, p. 867–879, 2004. ISSN 1530-8669.

PERKINS, C. **Ad hoc on demand distance vector (aodv) routing**, 1997. URL citeseer.ist.psu.edu/article/perkins99ad.html.

RAMACH, Krishna N., BUDDHIKOT, Ran Milind M., CH, Girish, MILLER, Scott, BELDING-ROYER, Elizabeth M. e ALMEROTH, Kevin C. **On the design and implementation of infrastructure mesh networks**. Em in IEEE Workshop on Wireless Mesh Networks (WiMesh, 2005.

ROCHA, Bruno Gusmão, ALMEIDA, Virgilio e GUEDES, Dorgival. **Increasing qos in selfish overlay networks**. IEEE Internet Computing, v. 10, n. 3, p. 24–31, 2006. ISSN 1089-7801.

SCENGEN. **The Scenario Generator Scengen**. http://isis.poly.edu/ qiming/scengen/index.html.

SCHARA, L. C., MARTINS, R. R. e CARRANO, R. C. **The ruca project and digital inclusion**. Em Network Operations and Management Symposium, LANOMS, Latin American, 2007.

TSARMPOPOULOS, N., KALAVROS, I. e LALIS, S. **A low-cost and simple-to-deploy peer-to-peer wireless network based on open source linux routers**. Em Testbeds and Research Infrastructures for the Development of Networks and Communities, Tridentcom, 2005.

VIKRAM, Srinivasan, NUGGEHALLI, Pavan, CHIASSERINI, Carla-Fabiana e RAO, Ramesh R. **Cooperation in wireless ad hoc networks**. Em INFOCOM, In San Francisco, California, USA, 2003.

WALKE, B., MANGOLD, S. e BERLEMANN, L. **IEEE 802 Wireless Systems: Protocols, Multi-Hop Mesh/Relaying, Performance and Spectrum Coexistence**. John Wiley, Sons, Nov 2006. ISBN 0-470-01439-3. URL http://www.comnets.rwth-aachen.de.

WANG, Xudong e LIM, Azman O. **Ieee 802.11s wireless mesh networks: Framework and challenges**. Ad Hoc Netw., v. 6, n. 6, p. 970–984, 2008. ISSN 1570-8705.

ZHONG, Sheng, CHEN, Jiang e YANG, Yang Richard. **Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks**. Em INFOCOM, In San Francisco, California, USA, 2003.

9 ANEXOS

9.1 DESENVOLVIMENTO PARA SIMULAR O COMPORTAMENTO EGOÍSTA

O primeiro passo foi a criação de um diretório chamado aodvd dentro do diretório base do ns-2 para armazenamento dos arquivos do novo protocolo. Não existe um número nem um padrão de nomes para os arquivos do diretório, mas é comum no caso de um protocolo chamado aaa, encontrar pelo menos os seguintes arquivos: aaa.h, aaa.cc, aaa_packet.h, aaa_rtable.h e aaa_rtable.cc. Tomando como base o protocolo AODV original, temos em seu diretório os seguintes arquivos:

- aodv.h/aodv.cc - arquivo de cabeçalho e implementação que define os temporizadores, agentes de roteamento, funções para as chamadas TCL e outras funções necessárias para as funcionalidades do protocolo;
- aodv_packet.h - especificação de todos os tipos de pacotes utilizados pelo protocolo;
- aodv_rtable.h/aodv_rtable.cc - arquivo de cabeçalho e implementação da tabela de roteamento do protocolo;
- aodv_rqueue.h/aodv_rqueue.cc - arquivo de cabeçalho e implementação das regras de enfileiramento de pacotes do protocolo;
- aodv_logs.cc - arquivo de implementação das funções de log;
- aodv.tcl - arquivo com *scripts* TCL de inicialização.

Para a implementação do novo protocolo de roteamento no ns-2 foi criado um agente derivado da classe *Agent*. De acordo com a documentação do ns-2, agentes são pontos de origem ou destino para pacotes do nível de rede e são usados na implementação de protocolos de outras camadas. Em outras palavras, o agente é a principal classe de um protocolo de roteamento e faz a interface com o código TCL das simulações. O agente de roteamento deve manter um estado interno e uma tabela de roteamento. No caso do AODV, a tabela de roteamento é representada por uma nova classe, chamada aodv_rtable. Além disso, um novo protocolo deve definir pelo menos um tipo de pacote para seu tráfego de controle. Esses novos tipos de pacote estão definidos no arquivo

aodv_packet.h. Também é necessário que o protocolo faça um envio periódico de pacotes ou um envio certo tempo após a ocorrência de algum evento. Neste caso, é necessário ter uma classe temporizadora (*timer class*) no protocolo.

O AODV implementa cinco classes temporizadoras:

- *BroadcastTimer*;
- *HelloTimer*;
- *NeighborTimer*;
- *RouteCacheTimer*;
- *LocalRepairTimer*.

Foi ainda necessário que o agente implementasse algumas funções especificadas na documentação do ns-2, entre elas uma função chamada command() e outra chamada recv(). O método recv() é chamado sempre que o agente de roteamento recebe um pacote. Os pacotes têm um cabeçalho comum definido no arquivo common/packet.h dentro do diretório do ns-2 para a correta identificação do seu tipo. No caso do AODV, a função recv() verifica o cabeçalho recebido e chama o método indicado para o tratamento do pacote. No caso de um pacote AODV é chamada a função recvAODV(), no caso de um pacote de dados, são chamadas funções para o encaminhamento (*forward*) ou descarte (*drop*) do pacote. A função *forward* é que irá verificar o endereço de destino e receber ou encaminhar o pacote.

Neste caso, fizemos um novo protocolo de roteamento chamado AODV_D. Na verdade, ele não vai ser um novo protocolo, mas um protocolo similar ao AODV com a característica de não encaminhar pacotes de dados originados em outros nós da rede. Desta forma, não é necessário a criação de um novo tipo de pacote, o AODV_D vai usar o mesmo tipo de pacote do AODV, possibilitando a interoperação dos dois protocolos.

Para a inclusão do protocolo AODV_D, são necessárias algumas alterações na biblioteca TCL do ns-2. No arquivo tcl/lib/ns-packet.tcl o nome do protocolo precisa ser adicionado na lista *prot*.

```
foreach prot {
...
AODVD
...
}
```

No arquivo tcl/lib/ns-lib.tcl é necessário definir os procedimentos para a criação de um nó com o AODV_D como protocolo de roteamento. O método *node* quando usado para criar nós wireless no ns-2 chama o método *create-wireless-node* da biblioteca TCL. Esse método precisa ser modificado para possibilitar a criação de nós AODV_D.

```
Simulator instproc create-wireless-node args {
...
   switch -exact $routingAgent_ {
   ...
      AODVD {
         set ragent [$self create-aodvd-agent $node]
      }
   ...
   }
...
}
```

O método *create-aodvd-agent* também deve ser definido no arquivo.

```
Simulator instproc create-aodvd-agent { node } {
        #  Create AODV routing agent
        set ragent [new Agent/AODVD [$node node-addr]]
        $self at 0.0 "$ragent start"
        $node set ragent_ $ragent
        return $ragent
}
```

Após essas alterações globais no ns-2, pode-se partir para a criação do protocolo. Neste caso foram copiados os seguintes arquivos do diretório aodv para o diretório aodvd e mudar em cada um deles todas as ocorrências de AODV para AODV_D.

```
aodvd.cc
aodvd.h
aodvd.tcl
aodvd_logs.cc
```

Os arquivos aodv_packet.h, aodv_rtable.h e aodv_rtable.cc não são necessários no AODV_D pois como já mencionado anteriormente, ele não define um tipo de pacote. Para a tabela de roteamento do AODV_D, as classes definidas nos arquivos aodv_rtable.h e aodv_rtable.cc no diretório aodv podem ser usadas após as seguintes modificações.

```
class aodv_rt_entry {
        friend class aodv_rtable;
        friend class AODV;
        friend class AODVD;
...
}

class AODV_Neighbor {
        friend class AODV;
        friend class AODVD;
...
}
```

Com essas modificações o ns-2 pode ser compilado, mas o protocolo AODV_D teria o mesmo comportamento do AODV. A mudança desejada no AODV_D, para ele não encaminhar pacotes de dados originados em outros elementos da rede, mas continuar encaminhando os pacotes AODV pode ser feita na função *forward*() do arquivo aodvd.cc.

```
AODVD::forward(aodv_rt_entry *rt, Packet *p, double delay) {
```

```
...
 if(ih->ttl_ == 0) {
 ...
 }
 if (ch->ptype() != PT_AODV && ch->direction() == hdr_cmn::UP) {
  drop(p, DROP_RTR_TTL);
  return;
 }
...
}
```

Finalmente, antes de compilar o ns-2, é necessário alterar o arquivo *Makefile* para compilar também o AODV_D.

```
OBJ_CC =
...
aodvd/aodvd_logs.o aodvd/aodvd.o \
...
```

9.2 IMPLEMENTAÇÃO DE PRIORIDADES NA CAMADA MAC

Para criação das prioridades foram criados outros tipos de pacotes, então o cabeçalho de cada um deles foram definidos no arquivo *common/packet.h*.

```
#define HDR_MAC802_11(p) ((hdr_mac802_11 *)hdr_mac::access(p))
#define HDR_MAC802_11x(p) ((hdr_mac802_11x *)hdr_mac::access(p))
#define HDR_MAC802_11y(p) ((hdr_mac802_11y *)hdr_mac::access(p))
#define HDR_MAC802_11z(p) ((hdr_mac802_11z *)hdr_mac::access(p))
```

No arquivo *lib/ns-mobilenode.tcl* são definidos os métodos da biblioteca TCL de maneira similar ao existente para o protocolo 802_11.

```
if {$mactype == "Mac/802_11x"} {
```

```
    $mac nodes [$god_ num_nodes]
}
if{$mactype == "Mac/802_11y"} {
    $mac nodes [$god_ num_nodes]
}
if{$mactype == "Mac/802_11z"} {
    $mac nodes [$god_ num_nodes]
}
if {$mactype == "Mac/802_11x"} {
    $self instvar mac_
    set ns_ [Simulator instance]
    set beacon_period [$ns_ delay_parse $beacon_period]
    set cfp_duration [$ns_ delay_parse $cfp_duration]
    $mac_(0) cfp $beacon_period $cfp_duration
}
if {$mactype == "Mac/802_11y"} {
    $self instvar mac_
    set ns_ [Simulator instance]
    set beacon_period [$ns_ delay_parse $beacon_period]
    set cfp_duration [$ns_ delay_parse $cfp_duration]
    $mac_(0) cfp $beacon_period $cfp_duration
}
if {$mactype == "Mac/802_11z"} {
    $self instvar mac_
    set ns_ [Simulator instance]
    set beacon_period [$ns_ delay_parse $beacon_period]
    set cfp_duration [$ns_ delay_parse $cfp_duration]
    $mac_(0) cfp $beacon_period $cfp_duration
}
```

No arquivo *tcl/lib/ns-default.tcl* são definidos os valores padrão para as variáveis de cada protocolo. O valor inicial usado pelo algoritmo de *backoff* (CWMin_) e o valor máximo do mesmo algoritmo (CWMax_) são alterados para uma distinção entre os protocolos 802_11x, 802_11y e 802_11z.

```
Mac/802_11x set CWMin_                  15
Mac/802_11x set CWMax_                  301
Mac/802_11x set SlotTime_               0.000020
Mac/802_11x set SIFS_                   0.000010
Mac/802_11x set PreambleLength_         144
Mac/802_11x set PLCPHeaderLength_       48
Mac/802_11x set PLCPDataRate_           1.0e6
Mac/802_11x set RTSThreshold_           0
Mac/802_11x set ShortRetryLimit_        7
Mac/802_11x set LongRetryLimit_         4
Mac/802_11x set bugFix_timer_ true;

Mac/802_11y set CWMin_                  31
Mac/802_11y set CWMax_                  501
Mac/802_11y set SlotTime_               0.000020
Mac/802_11y set SIFS_                   0.000010
Mac/802_11y set PreambleLength_         144
Mac/802_11y set PLCPHeaderLength_       48
Mac/802_11y set PLCPDataRate_           1.0e6
Mac/802_11y set RTSThreshold_           0
Mac/802_11y set ShortRetryLimit_        7
Mac/802_11y set LongRetryLimit_         4
Mac/802_11y set bugFix_timer_ true;

Mac/802_11z set CWMin_                  257
Mac/802_11z set CWMax_                  4097
Mac/802_11z set SlotTime_               0.000020
```

```
Mac/802_11z set SIFS_                   0.000010
Mac/802_11z set PreambleLength_         144
Mac/802_11z set PLCPHeaderLength_       48
Mac/802_11z set PLCPDataRate_           1.0e6
Mac/802_11z set RTSThreshold_           0
Mac/802_11z set ShortRetryLimit_        7
Mac/802_11z set LongRetryLimit_         4
Mac/802_11z set bugFix_timer_ true;
```

O arquivo *lan/ns-mac.tcl* também foi alterado com os parâmetros de cada novo protocolo.

```
if [TclObject is-class Mac/802_11x] {
   Mac/802_11x set delay_ 64us
   Mac/802_11x set ifs_ 16us
   Mac/802_11x set slotTime_ 16us
   Mac/802_11x set cwmin_ 16
   Mac/802_11x set cwmax_ 1023
   Mac/802_11x set rtxLimit_ 16
   Mac/802_11x set bssId_ -1
   Mac/802_11x set sifs_ 8us
   Mac/802_11x set pifs_ 12us
   Mac/802_11x set difs_ 16us
   Mac/802_11x set rtxAckLimit_ 1
   Mac/802_11x set rtxRtsLimit_ 3
   Mac/802_11x set basicRate_ 1Mb
   Mac/802_11x set dataRate_ 1Mb
}

if [TclObject is-class Mac/802_11y] {
   Mac/802_11y set delay_ 64us
   Mac/802_11y set ifs_ 16us
```

```
    Mac/802_11y set slotTime_ 16us
    Mac/802_11y set cwmin_ 16
    Mac/802_11y set cwmax_ 1023
    Mac/802_11y set rtxLimit_ 16
    Mac/802_11y set bssId_ -1
    Mac/802_11y set sifs_ 8us
    Mac/802_11y set pifs_ 12us
    Mac/802_11y set difs_ 16us
    Mac/802_11y set rtxAckLimit_ 1
    Mac/802_11y set rtxRtsLimit_ 3
    Mac/802_11y set basicRate_ 1Mb
    Mac/802_11y set dataRate_ 1Mb
}

if [TclObject is-class Mac/802_11z] {
    Mac/802_11z set delay_ 64us
    Mac/802_11z set ifs_ 16us
    Mac/802_11z set slotTime_ 16us
    Mac/802_11z set cwmin_ 16
    Mac/802_11z set cwmax_ 1023
    Mac/802_11z set rtxLimit_ 16
    Mac/802_11z set bssId_ -1
    Mac/802_11z set sifs_ 8us
    Mac/802_11z set pifs_ 12us
    Mac/802_11z set difs_ 16us
    Mac/802_11z set rtxAckLimit_ 1
    Mac/802_11z set rtxRtsLimit_ 3
    Mac/802_11z set basicRate_ 1Mb
    Mac/802_11z set dataRate_ 1Mb
}
```

No diretório *tcl/lan*, são gerados os arquivos ns-mac-802_11x.tcl, ns-mac-802_11x.tcl e ns-mac-802_11x.tcl e em cada um deles as ocorrências de 802_11 são alteradas para 802_11x, 802_11y ou 802_11z. O arquivo *lib/ns-lib.tcl* foi modificado para a inclusão dos arquivos criados.

```
source ../lan/ns-mac-802_11.tcl
source ../lan/ns-mac-802_11x.tcl
source ../lan/ns-mac-802_11y.tcl
source ../lan/ns-mac-802_11z.tcl
```

Da mesma forma, no diretório mac, foram criados os arquivos referentes a cada protocolo. Foram geradas cópias dos arquivos mac-802_11.h, mac-802_11.cc, *mac-timers.h* e *mac-timers.cc* e em cada um deles todas as ocorrências de 802_11 foram alteradas para 802_11x, 802_11y e 802.11z.

```
mac-802_11x.h / mac-802_11x.cc
mac-802_11y.h / mac-802_11y.cc
mac-802_11z.h / mac-802_11z.cc
mac-timersx.h / mac-timersx.cc
mac-timersy.h / mac-timersy.cc
mac-timersz.h / mac-timersz.cc
```

Nos arquivos mac-802_11x.h, mac-802_11y.h e mac-802_11z.h é alterado a função de incremento do valor máximo para o algoritmo de *backoff* da forma mostrada a seguir. O valor inicial de cw_ é o valor CWMin_ definido em tcl/lib/ns-default.tcl e o valor máximo de cw_ é CWMax_.

```
mac-802_11.h: cw_ = (cw_ << 1) + 1;
mac-802_11x.h: cw_ = cw_ + 50;
mac-802_11y.h: cw_ = cw_ + 100;
mac-802_11z.h: cw_ = (cw_ << 2) + 1;
```

Por fim, o arquivo *Makefile* é modificado para a inclusão dos novos arquivos.

```
mac/channel.o mac/mac.o mac/ll.o mac/mac-802\_11.o \
mac/mac-802\_11x.o mac/mac-802\_11y.o mac/mac-802\_11z.o \

mac/mac-timers.o trace/cmu-trace.o mac/varp.o \
mac/mac-timersx.o mac/mac-timersy.o mac/mac-timersz.o \
```

Livros Grátis

(http://www.livrosgratis.com.br)

Milhares de Livros para Download:

Baixar livros de Literatura
Baixar livros de Literatura de Cordel
Baixar livros de Literatura Infantil
Baixar livros de Matemática
Baixar livros de Medicina
Baixar livros de Medicina Veterinária
Baixar livros de Meio Ambiente
Baixar livros de Meteorologia
Baixar Monografias e TCC
Baixar livros Multidisciplinar
Baixar livros de Música
Baixar livros de Psicologia
Baixar livros de Química
Baixar livros de Saúde Coletiva
Baixar livros de Serviço Social
Baixar livros de Sociologia
Baixar livros de Teologia
Baixar livros de Trabalho
Baixar livros de Turismo