ANÁLISE DO ROTEAMENTO EM REDES MÓVEIS AD HOC EM CENÁRIOS DE OPERAÇÕES MILITARES

Ivana Cardial de Miranda Pereira

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

Aprovada por:

_____

Prof. Aloysio de Castro Pinto Pedroza, Dr.

_____

Prof. Luci Pirmez, D.Sc.

_____

Dr. Gustavo Henrique Alves Martins, Ph.D.

_____

Prof. Luís Henrique Maciel Kosmalski Costa, Dr.

RIO DE JANEIRO, RJ - BRASIL

JUNHO DE 2004

PEREIRA, IVANA CARDIAL DE MIRANDA

Análise do Roteamento em Redes Móveis Ad Hoc em Cenários de Operações Militares [Rio de Janeiro] 2004

XV, 92 p. 29,7 cm (COPPE/UFRJ, M.Sc., Engenharia Elétrica, 2004)

Tese - Universidade Federal do Rio de Janeiro, COPPE

1. Redes ad hoc
2. Aplicações militares
3. Modelos de mobilidade
4. Protocolos de roteamento

I. COPPE/UFRJ II. Título (série)

A Juarez Cardial de Miranda.

Agradecimentos

À minha mãe e aos meus irmãos, pelo amor, confiança, incentivo e apoio ao longo da minha vida.

Ao meu pai, que me ensinou a importância do conhecimento.

Ao meu marido Rogério, não só pelo companheirismo, confiança e incentivo, mas como pelas valiosas contribuições dadas neste trabalho.

Ao meu filho Pedro pelo carinho e paciência durante este período.

Ao meu orientador Prof. Aloysio, pelo estímulo, confiança e orientação para a realização deste trabalho.

Ao Capitão David Fernandes e ao Capitão-de-Fragata Jorge Armando, pela colaboração na especificação dos cenários militares, e ao Capitão-de-Corveta Vasconcellos pelo incentivo ao meu ingresso no programa de mestrado.

Aos professores e a toda a equipe do GTA, em particular aos amigos, Bagatelli, Bernardo, Daniel, Eric, Gardel, Ingrid, Kleber, Luis Gustavo, Paulo Stein, Pedro, Renata, Saulo, pela amizade e pela boa convivência durante a tese e, especialmente, à minha amiga Andréa pela amizade, parceria e confiança durante todo o curso.

À professora Luci Pirmez, ao Capitão-de-Mar-e-Guerra Gustavo e ao professor Luís Henrique pela presença na banca examinadora.

Ao Centro de Análises de Sistemas Navais e à Marinha do Brasil, pela oportunidade e confiança.

Às funcionárias do Programa de Engenharia Elétrica da COPPE/UFRJ, pela presteza no atendimento na secretaria do Programa.

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

ANÁLISE DO ROTEAMENTO EM REDES MÓVEIS AD HOC EM CENÁRIOS DE OPERAÇÕES MILITARES

Ivana Cardial de Miranda Pereira

Junho/2004

Orientador: Aloysio de Castro Pinto Pedroza

Programa: Engenharia Elétrica

As redes móveis sem fio têm despertado particular interesse nas comunidades militares. Para que uma tropa possa cumprir sua tarefa de uma forma adequada em um campo de batalha, ela depende, em grande parte, da eficácia do seu sistema de comunicações. É primordial que este sistema funcione perfeitamente, para que o comandante de um grupo possa controlar seus subordinados, obter e difundir informações e ordens, e coordenar as ações de sua unidade. O objetivo deste trabalho é analisar, por meio de simulações de cenários realistas, o problema de roteamento em redes móveis *ad hoc* quando aplicadas a uma operação militar. A partir desta análise, desenvolvemos e implementamos modelos de mobilidade em grupo e buscamos as condições que melhor se adéqüem a este tipo de cenário ou a outros com características similares. Além disto, espera-se que os modelos desenvolvidos neste trabalho possam ser utilizados como ferramenta para auxiliar no planejamento das comunicações em ações militares táticas de infantaria, ou como parte de sistemas de Jogo de Guerra, possibilitando que, a partir da área de operação, se estime com uma maior precisão a quantidade de elementos de combate que devem estar dotados de dispositivos de comunicação *ad hoc*, de forma a garantir a conectividade e a eficácia da rede.

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

ROUTING ANALYSIS IN MOBILE AD HOC NETWORKS FOR MILITARY OPERATIONS

Ivana Cardial de Miranda Pereira

June/2004

Advisor: Aloysio de Castro Pinto Pedroza

Department: Electrical Engineering

The military have been particularly interested in applications of mobile ad hoc wireless networks. In the battlefield, soldiers depend greatly on reliable and effective communications in order to accomplish their mission. It is of utmost importance that the communication system works perfectly to support a well-defined chain of command, allowing the commanding officer to control and coordinate the forces under his command, and to obtain and deliver information and orders. In this work we analyze, employing simulation models of realistic scenarios, the problems concerning routing in mobile ad hoc networks when applied to military operations. From this analysis we develop a group mobility model and we seek the best routing alternatives for this kind of scenario. Furthermore, we hope that the modeling tools developed in this work may help the planning process of military tactical land communication operations, with more accurate estimates of the size of combatant groups carrying digital communication devices in an ad hoc network, guaranteeing the connectivity and the effectiveness of the network.

Sumário

Resumo **v**

Abstract **vi**

Lista de figuras **x**

Lista de tabelas **xii**

Lista de acrônimos **xiv**

1 Introdução **1**

1.1 Motivação 2

1.2 Redes Móveis *Ad Hoc* 4

1.3 Objetivo 6

2 Roteamento em Redes *Ad Hoc* **8**

2.1 Protocolos de Roteamento para Redes *Ad Hoc* 9

2.1.1 *Dynamic Source Routing* - DSR 10

2.1.2 *Destination Sequenced Distance Vector* - DSDV 13

2.1.3 *Ad Hoc On Demand Distance Vector* - AODV 15

2.2 Considerações sobre os protocolos 17

2.3 Comentários 19

3 Um Novo Modelo de Mobilidade 20

3.1 O Gerador de Cenários - ScenGen 21

3.2 Modelos de Mobilidade para Redes *Ad Hoc* 22

3.2.1 Modelos de Mobilidade Individual 23

3.2.2 Modelos de Mobilidade em Grupo 24

3.3 Cenário Militar 28

3.3.1 Requisitos Básicos 28

3.3.2 Movimentação 29

3.3.3 Descrição 30

3.4 Modelo Proposto - *Mixed Waypoint* 31

3.4.1 Desenvolvimento 32

3.4.2 Descrição do Modelo 33

3.5 Comentários 35

4 Simulações 36

4.1 O padrão IEEE 802.11 37

4.1.1 *Point Coordination Function* - PCF 37

4.1.2 *Distributed Coordination Function* - DCF 38

4.2 Ambiente de simulação 41

4.3 Métricas de Desempenho 43

4.4 Padrão de Movimentação 45

4.5 Padrão de Tráfego 47

5 Análise dos Resultados 49

5.1 Simulação 01 - utilizando taxa de transmissão de dados de 2Mbps 51

5.2 Simulação 02 - utilizando taxa de transmissão de dados de 11Mbps 58

5.3 Simulação 03 - variando o alcance máximo dos transmissores 62

5.4 Simulação 04 - incluindo um grupo no cenário 66

5.5 Simulação 05 - excluindo um grupo no decorrer da simulação 69

5.6 Simulação 06 - variando o tráfego 72

5.7 Resumo dos principais resultados das simulações 75

5.8 Resultados Complementares 76

5.9 Comentários 77

6 Conclusões e Trabalhos Futuros 79

Referências Bibliográficas 84

A O Modelo Mixed Waypoint 88

Lista de Figuras

1.1 Modelo de comunicação em redes móveis *ad hoc* 5

2.1 Descoberta de rotas usando o protocolo DSR 11

2.2 Propagação do *Route Reply* (RREP) no protocolo DSR 11

2.3 Descoberta de rotas usando o protocolo AODV 16

2.4 Propagação do *Route Reply* (RREP) no protocolo AODV 16

3.1 Mobilidade usando o modelo *Random Waypoint*. 25

3.2 Movimento Aleatório x Movimento Militar. 25

3.3 Mobilidade segundo o modelo Perseguição. 26

3.4 Mobilidade em Grupo usando o modelo RPGM. 28

3.5 Uso de comunicação sem-fio em aplicações militares. 29

3.6 Cenário militar. 31

3.7 Modelo de Mobilidade *Mixed Waypoint*. 33

4.1 Mecanismo de acesso básico do DCF. 39

4.2 Mecanismo de acesso opcional do DCF usando RTS/CTS. 39

4.3 O problema do terminal escondido. 40

5.1 Simulação 01 - Comparação dos protocolos para as diferentes métricas usando largura de banda de 2Mbps. 56

5.2 Simulação 02 - Comparação dos protocolos para as diferentes métricas usando largura de banda de 11Mbps. 61

5.3 Simulação 03 - Comparação dos protocolos para as diferentes métricas variando o alcance dos transmissores. 64

5.4 Comparação dos protocolos com a métrica número de saltos. 65

5.5 Simulação 04 - Comparação dos protocolos para as diferentes métricas usando largura de banda de 11Mbps, incluindo um grupo. 68

5.6 Comparação entre os cenários utilizando diferentes números de grupos de combate. 69

5.7 Comparação entre os cenários utilizados na Simulação 02 e Simulação 05. 70

5.8 Simulação 05 - Comparação dos protocolos para as diferentes métricas usando largura de banda de 11Mbps, excluindo um grupo. 71

5.9 Simulação 06 - Comparação dos protocolos para as diferentes métricas variando a taxa de envio de pacotes. 74

Lista de Tabelas

4.1 Resumo dos parâmetros utilizados nas simulações. 46

5.1 Valores dos parâmetros da simulação 01. 51

5.2 Resultados das simulações com taxa de transmissão de dados de 2Mbps. . 52

5.3 Principais motivos de descartes de pacotes de dados. 52

5.4 Valores dos parâmetros da simulação 02. 59

5.5 Resultados das simulações empregando taxa de transmissão de dados de 11Mbps. 59

5.6 Principais motivos dos descartes com taxa de transmissão de 11Mbps. . . 60

5.7 Valores dos parâmetros da simulação 03. 62

5.8 Resultados das simulações variando o alcance dos transmissores usando o AODV. 63

5.9 Resultados das simulações variando o alcance dos transmissores usando o DSR. 63

5.10 Resultados das simulações variando o alcance dos transmissores usando o DSDV. 63

5.11 Número de pacotes RREQ que foram enviados ou encaminhados no AODV. 65

5.12 Valores dos parâmetros da simulação 04. 67

5.13 Resultados com a inclusão de um novo grupo no cenário proposto. 67

5.14 Valores dos parâmetros da simulação 05. 70

5.15 Impacto da exclusão de um grupo. 70

5.16 Impacto da variação do tráfego nas métricas avaliadas utilizando o DSDV. 72

5.17 Impacto da variação do tráfego nas métricas avaliadas utilizando o AODV. 73

5.18 Impacto da variação do tráfego nas métricas avaliadas utilizando o DSR. . 73

5.19 Número de pacotes RREQ que foram enviados ou encaminhados no AODV. 75

5.20 Resumo do resultado dos experimentos usando o protocolo DSDV. 75

5.21 Resumo do resultado dos experimentos usando o protocolo AODV. 76

5.22 Resumo do resultado dos experimentos usando o protocolo DSR. 76

5.23 Resultados das simulações usando o modelo *Random Waypoint*. 77

5.24 DSR sem o uso do mecanismo de escuta promíscua. 77

Lista de acrônimos

AODV :	*Ad hoc On-demand Distance Vector*;
ACK :	*Acknowledgement*;
CBR :	*Constant Bit Rate*;
CRC :	*Check Redundancy Cyclic*;
CSMA/CA :	*Carrier-Sense Multiple Access with Collision Avoidance*;
CTS :	*Clear To Send*;
DCF :	*Distributed Coordination Function*;
DIFS :	*Distributed Inter-Frame Space*;
DSDV :	*Destination Sequenced Distance Vector*;
DSR :	*Dynamic Source Routing*;
FIFO :	*First-In-First-Out*;
IEEE :	*Internet Engineering Task Force*;
IFQ :	*Interface Queue*;
LL :	*Link Layer*;
LLC :	*Logic Link Control*;
MAC :	*Medium Access Control*;
MONARCH :	*Mobile Networking Architectures*;
NAV :	*Network Allocation Vector*;
ns :	*Network Simulator*;
PCF :	*Point Coordination Function*;
RERR :	*Route Error*;
RPGM :	*Reference Point Group Mobility*;

RREP : *Route Reply*;

RREQ : *Route Request*;

RTS : *Request To Send*;

SIFS : *Short Inter-Frame Space*;

TCP : *Transport Control Protocol*;

VINT : *Virtual Internet Testbed*.

Capítulo 1

Introdução

O CONJUNTO de aplicações das redes móveis sem fio é bastante abrangente, variando desde pequenas redes com pouca mobilidade, restritas, normalmente, pelo consumo de energia, até grandes redes, com alto grau de mobilidade de seus nós e com uma topologia bastante dinâmica. O projeto de protocolos de roteamento para essas redes é uma tarefa de elevado grau de complexidade. A determinação de rotas viáveis e a entrega de mensagens em ambientes descentralizados e de topologia altamente dinâmica é um problema normalmente mal definido. Fatores como a qualidade variável das ligações sem fio, perdas por propagação, interferência mútua, consumo de energia e alterações topológicas se tornam aspectos relevantes. Em função disso, a rede deve ser capaz de alterar suas rotas de forma adaptativa e, em ambientes como os que existem nas operações militares, outros fatores, como segurança, latência, confiabilidade, bloqueio e interferência intencionais por parte do inimigo e recuperação de falhas adquirem evidente relevância. Este trabalho se destina a analisar o problema do roteamento em redes móveis *ad hoc* quando aplicadas a uma operação militar em um campo de batalha. A partir desta análise, busca-se as condições que melhor se adéqüem a este tipo de cenário ou a outros com características similares.

1.1 Motivação

As redes móveis sem fio têm despertado particular interesse nas comunidades militares. Em aplicações militares, a confiabilidade do meio de transmissão é um requisito indispensável, de modo que a utilização de cabos pode causar transtornos, uma vez que o rompimento de um destes cabos pode comprometer todo o sistema de defesa. Por outro lado, não é possível estabelecer a conexão por fio a partir de carros de combate, aeronaves, navios, etc. A mobilidade da rede, por sua vez, também apresenta papel relevante nas operações militares, pois equipamentos portáteis, como *palmtops* e *laptops*, podem ser utilizados por soldados para enviar mensagens, gravar registros, receber instruções de seus superiores, mesmo em situações de crise.

A segurança das operações é aumentada quando se reduz significativamente o tempo necessário à transmissão dessas mensagens, substituindo o emprego do canal de voz pela transmissão exclusiva de dados em forma digital. Além disto, desta forma pode ser preservado o silêncio imprescindível para o sucesso deste tipo de operação.

Atualmente, as forças militares mais avançadas tecnicamente estão desenvolvendo redes móveis sem fio de larga escala para apoiar uma variedade de tipos de tráfego de comunicações táticas. As novas redes buscam transportar informações por voz, vídeo e dados, onde a conectividade entre os roteadores sem fio deve considerar com muita atenção os critérios de robustez e segurança. As redes são muito dinâmicas; os enlaces entre os nós podem surgir e desaparecer em questão de segundos. Desse modo, uma configuração de rede descentralizada e independente de estruturas fixas é uma importante vantagem ou, até mesmo, uma necessidade operacional. Para que uma tropa possa cumprir sua tarefa de forma adequada em um campo de batalha, ela depende, em grande parte, da eficácia do seu sistema de comunicações. É primordial que este sistema funcione perfeitamente, para que o comandante de um grupo possa controlar seus subordinados, obter e difundir informações e coordenar as ações de sua unidade. Soluções que atendem de forma satisfatória às redes comerciais podem deixar de atender a tais exigências.

Além disso, aplicações militares típicas se caracterizam pelos fatos descritos a seguir:

- as forças militares têm uma estrutura bem definida de comando. Embora não se

sugira aqui que as comunicações devam seguir estritamente essa estrutura, a cadeia de comando sempre existirá e, em geral, os nós da rede estarão fisicamente localizados de acordo com este modelo, o que produz um efeito evidente na topologia da rede móvel;

- nas forças militares, os nós móveis são organizados em grupos e estes grupos obedecem a um padrão de movimentação pré-determinado, uma vez que buscam, de forma cooperativa, alcançar um determinado objetivo comum, segundo doutrinas de operação pré-estabelecidas. Essa característica leva, em geral, a padrões de mobilidade mais previsíveis, com um grau de aleatoriedade controlado;

- os movimentos são restritos, uma vez que as forças operam em áreas limitadas e por um período de tempo predeterminado; e

- o padrão de conexão obedece às regras impostas pela hierarquia militar.

A mobilização real de efetivos para treinamento tático costuma ser demorada, desgastante para os militares e com alto custo. Com isso, várias soluções baseadas em ambientes virtuais têm sido adotadas para que algumas etapas do treinamento possam ser exaustivamente realizadas em simulações por computador, antes que os efetivos sejam levados a campo. As simulações de confronto têm desempenhado um papel relevante no moderno treinamento militar, principalmente para os oficiais que precisam aprender a tomar decisões sob diversas circunstâncias e, ainda, trabalhar com novas tecnologias. Em geral, as simulações são usadas para avaliar a evolução das ações, o impacto de novas estratégias e o planejamento de contingências [1, 2]. É importante mencionar que as simulações, tradicionalmente, são utilizadas de duas maneiras principais: diretamente como ferramenta de análise para comparação da eficácia de alternativas táticas, possivelmente em um ambiente de meta-simulação em experimentos planejados; ou de modo conjunto com outras ferramentas de análise, como, por exemplo, modelos de otimização, compondo complexos sistemas denominados Jogos de Guerra, onde se busca estudar possibilidades e opções estratégicas.

1.2 Redes Móveis *Ad Hoc*

Nos últimos anos, o crescente consumo de produtos como *laptops*, *palmtops*, telefones celulares, PCs e seus periféricos é resultado da contínua redução de custo e tamanho destes dispositivos. Estima-se que em poucos anos será comum que as pessoas possuam algum tipo de dispositivo portátil para se comunicar com a parte fixa da rede, e com outros computadores móveis.

As redes sem fio surgiram da necessidade de eliminação dos cabos de conexão entre os equipamentos, uma vez que, muitas vezes, estes cabos são oriundos de diferentes fabricantes, dificultando a interligação dos equipamentos devido às diferenças em sua tecnologia.

Nas redes sem fio, os pacotes são transmitidos através do ar em canais de freqüência de rádio (radio difusão) ou infravermelho. As redes sem fio podem ser classificadas de duas formas: redes infra-estruturadas e redes *ad hoc*. Nas redes infra-estruturadas, toda a comunicação entre os nós é feita por meio de estações de suporte à mobilidade na rede fixa. Neste tipo de rede, os nós, mesmo dentro do alcance uns dos outros, estão impossibilitados de estabelecer comunicação direta entre si.

Uma rede *ad hoc* (Figura 1.1) é um conjunto de nós sem fio, que são capazes de se comunicar diretamente entre si, formando dinamicamente uma rede temporária, sem o uso de qualquer ponto de acesso centralizado ou estação de suporte. Nesse tipo de rede, os nós funcionam como roteadores, sendo capazes de descobrir e manter rotas para outros nós da rede; e como estações, executando aplicações dos usuários.

As redes *ad hoc* podem ser divididas em redes de comunicação direta e em redes de comunicação por múltiplos saltos. Na comunicação direta, as estações se comunicam apenas com aquelas que estiverem dentro dos seus raios de alcance, denominadas vizinhas. Nas redes de múltiplos saltos, todas as estações possuem, também, a propriedade de rotear/encaminhar mensagens. Assim, estações que estejam mutuamente fora de alcance podem se comunicar, se as mensagens puderem ser encaminhadas por meio de outras estações que estejam dispostas a cooperar na comunicação.

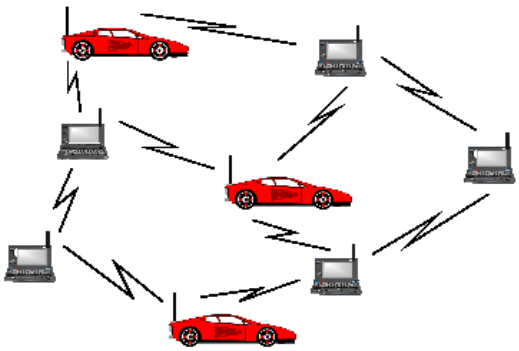


Figura 1.1: Modelo de comunicação em redes móveis *ad hoc*

As redes móveis *ad hoc* possuem suas raízes no ambiente de pesquisa e desenvolvimento militar. A formação de uma rede *ad hoc* é indicada em áreas onde há pouca ou nenhuma infraestrutura de comunicação (fixa ou celular), ou onde a infraestrutura existente é cara ou inconveniente para uso, e está associada a cenários em que há a necessidade de se instalar rapidamente uma rede. Uma rede sem fio, dinâmica, temporária, de topologia imprevisível e carente de suporte ou infraestrutura, unindo nós com uma complexa mobilidade, parece descrever com perfeição o ambiente encontrado no campo de batalha. Como outros exemplos de aplicações *ad hoc*, podemos citar: operações de busca e resgate de emergência em lugares de difícil acesso, em situações de desastre, como terremotos, furacões ou inundações; e conferências, onde os participantes desejam disseminar ou compartilhar informações rapidamente, por meio de seus *laptops* ou *palmtops*.

Devido à mobilidade dos nós, as redes *ad hoc* apresentam uma topologia dinâmica, isto é, mudam freqüentemente e de forma imprevisível, tornando, assim, o roteamento em redes *ad hoc* um grande desafio. A pesquisa acadêmica relacionada a estes tipos de redes tem focado, principalmente, o estudo dos aspectos relativos aos protocolos de roteamento, responsáveis em última instância por manter a conectividade dad rede.

Desde o surgimento destas redes, diversos protocolos foram propostos para resolver o problema de roteamento em redes *ad hoc* para encontrar eficientemente rotas entre dois nós de comunicação. Tais protocolos devem ser projetados de forma a lidar com as limitações típicas deste tipo de rede, como o consumo de energia dos nós móveis, a

banda passante limitada e a alta taxa de erros devido a conexões sem fio; assim como, deve ser capaz de resolver os problemas decorrentes do alto grau de mobilidade dos nós, que, freqüentemente, alteram drasticamente e de forma imprevisível a topologia da rede.

1.3 Objetivo

O principal objetivo deste trabalho é avaliar o problema do roteamento em redes móveis *ad hoc* em um contexto mais específico, representado por um cenário realístico que retrata uma operação militar típica, diferenciando-se de comparações anteriores [3, 4, 5], onde os movimentos dos nós são puramente aleatórios. Para isto, foi desenvolvido e simulado um cenário que representa a movimentação dos nós em uma ação de oportunidade constituída de assalto e tomada de posição inimiga. Foi revelado os problemas decorrentes da utilização deste tipo de rede em um cenário com estas características, ou a outros com características similares, buscando as melhores condições para contornar estes problemas. Além disso, por meio das simulações realizadas podemos avaliar o impacto que a mobilidade em grupo, a configuração de rede hierárquica e o movimento dos nós em uma direção predeterminada podem causar no roteamento dos dados.

A análise do comportamento dos protocolos no cenário proposto foi realizada por meio de simulações [6, 7], variando diversos tipos de parâmetros relativos ao alcance da comunicação, a quantidade de grupos da rede, a taxa de transmissão dos dados e a taxa de envio de pacotes. Foram realizadas variações do cenário, com a finalidade de submeter os protocolos ao maior conjunto possível de situações. O intuito desse conjunto de variações é testar a eficiência dos protocolos nas mais diversas situações, típicas do contexto da aplicação militar analisado. Inicialmente, simulações são conduzidas buscando-se obter o melhor dimensionamento da rede para este cenário, ressaltando a influência provocada nos resultados pela escolha de diferentes parâmetros. Posteriormente, pretende-se avaliar essa rede em condições de crise. O que se está observando nas análises é o atraso, a taxa de entrega de pacotes e a sobrecarga de roteamento. Além disso, são também identificadas as causas que levam à perda de pacotes.

Os protocolos de roteamento AODV e DSR foram selecionados neste trabalho pela

sua importância nas redes *ad hoc* e porque eles mostraram os melhores resultados em trabalhos anteriores [3, 4, 8]. Porém, estes protocolos não haviam sido comparados em cenários com as características abordadas neste trabalho, onde os nós são dispostos em grupo, inicialmente posicionados de acordo com uma necessidade tática, apresentando movimentos com a finalidade de alcançar um determinado objetivo, e obedecendo a condições de tráfego definidas de acordo com uma cadeia hierárquica. Já o DSDV é um protocolo proativo e foi incluído para ilustrar a diferença de comportamento entre protocolos por demanda e protocolos proativos. A motivação principal desse trabalho é extrair as qualidades relativas dos tipos de protocolo analisados, de modo a se adquirir conhecimento para futuras propostas que melhor atendam às necessidades características de redes *ad hoc* com configuração claramente hierárquica.

Este trabalho está organizado em seis capítulos. O capítulo 2 apresenta o roteamento em redes *ad hoc*, onde são descritos os protocolos selecionados para análise. No capítulo 3, são discutidos os modelos de mobilidade utilizados em redes *ad hoc*, alguns aspectos relativos à representação do movimento dos nós em redes *ad hoc*, bem como o cenário desenvolvido para este trabalho. Detalhes referentes às simulações são apresentados no capítulo 4 e à análise dos resultados são apresentados no capítulo 5. Finalmente, no capítulo 6 é apresentada a conclusão do trabalho e são propostos trabalhos futuros.

Capítulo 2

Roteamento em Redes *Ad Hoc*

EM redes móveis *ad hoc*, uma rota entre dois nós pode ser formada por vários saltos através de um ou mais nós na rede. O roteamento consiste, basicamente, na determinação de uma rota entre dois nós e o transporte dos pacotes. Para que estes objetivos sejam alcançados de forma satisfatória, o algoritmo de roteamento deve atender, principalmente, aos seguintes requisitos: ter habilidade de escolher a melhor rota para o pacote, sendo que esta rota pode variar de acordo com a métrica utilizada (menor caminho, maior banda passante, menor atraso, etc.); oferecer seus serviços com a menor sobrecarga possível; ser independente da tecnologia da rede; e ter a capacidade de lidar de forma robusta e consistente com as mudanças de topologia, falhas de equipamento e diferentes cargas de tráfego.

Os roteadores em uma rede *ad hoc* trocam informações de roteamento uns com os outros com a finalidade de tomar conhecimento das disponibilidades de rotas e da topologia da rede. Em princípio, os roteadores conhecem apenas os seus próprios endereços e as conexões a que estão interligados. Com a troca de mensagens de roteamento, cada roteador constrói o conhecimento da rede. O roteamento é feito por um *software* que é executado no roteador. Este *software* implementa um dos protocolos de roteamento, que são baseados em algum algoritmo ou mecanismo de roteamento.

A seção 2.1 apresenta os protocolos de roteamento selecionados para análise neste trabalho; na seção 2.2 é realizada uma comparação entre os protocolos, destacando as

suas principais vantagens e desvantagens; e por fim é ressaltado aspectos importantes deste capítulo na seção 2.3.

2.1 Protocolos de Roteamento para Redes *Ad Hoc*

Os protocolos de roteamento podem ser classificados em proativos e reativos (sob demanda) [9]. Os protocolos proativos mantêm rotas para todos os nós da rede, independentemente do uso ou necessidade destas rotas. Eles reagem à troca de topologia, mesmo que nenhum tráfego seja afetado por esta troca. Para que isso seja possível, são trocadas mensagens periódicas para manter rotas para todos os nós e, desta forma, quando uma das rotas for requisitada, ela pode ser usada imediatamente.

Os protocolos reativos iniciam as atividades de roteamento de acordo com a demanda, de maneira a minimizar a sobrecarga de roteamento, permitindo que rotas sejam descobertas com reações rápidas a possíveis mudanças na topologia da rede. Neste caso, somente se estabelecem rotas entre os nós na presença de pacotes de dados.

Operar sob demanda, ou de forma proativa, é uma escolha que depende do resultado que se deseja obter com o uso do algoritmo. Nos casos onde o principal interesse é a utilização eficiente dos recursos da rede e da carga da bateria, e quando o tempo não é uma restrição crítica, a operação sob demanda pode ser a mais indicada. Em outros casos, a latência gerada para que o protocolo opere de acordo com a demanda pode vir a ser inaceitável. Nestes casos, é desejável que o protocolo trabalhe de maneira proativa, buscando descobrir as informações antes que estas se tornem necessárias. Para ilustrar, podemos citar como exemplo as redes militares. Estes tipos de rede possuem expectativas diferentes das redes comerciais: espera-se que existam poucos nós, que trocam pequenas mensagens utilizadas para manipular e controlar sistemas aplicativos altamente distribuídos, como, por exemplo, sistemas de comunicação, de controle tático e sistemas de armas. Possivelmente, o mais importante nesses casos é encontrar os nós de modo eficiente, e no menor espaço de tempo possível. Sob esta visão, a economia de energia e banda passante torna-se um problema secundário.

A seguir é apresentado uma breve descrição dos protocolos de roteamento que serão avaliados neste trabalho.

2.1.1 *Dynamic Source Routing* - DSR

O protocolo *Dynamic Source Routing* (DSR) foi desenvolvido pelo Departamento de Ciência da Computação da *Rice University*, por meio do projeto MONARCH (*MObile Networking ARCHitectures*) [10].

O DSR [5, 11] é um protocolo de roteamento sob demanda que usa roteamento pela fonte para entregar pacotes de dados, isto é, a fonte descobre e armazena, no cabeçalho de cada pacote que envia, o caminho completo e ordenado que o pacote deve percorrer até alcançar o destino, isto é, o cabeçalho de cada pacote de dados carrega esta seqüência de nós. Cada nó mantém um *cache*, onde todas as suas rotas conhecidas são armazenadas.

O DSR possui dois mecanismos principais: **descoberta de rotas** e **manutenção de rotas**. Quando um nó fonte ou origem deseja enviar pacotes para um nó destino, o nó de origem verifica se possui uma rota para o destino desejado em seu *cache*. Caso a rota exista, a origem usa esta rota para enviar o pacote; em caso contrário inicia um processo de descoberta de rotas para buscar dinamicamente uma rota para o destino.

O mecanismo de **descoberta de rotas**, que pode ser visto na Figura 2.1, é iniciado quando o nó origem transmite em *broadcast* um pacote de requisição de rota *Route Request* (RREQ), que é recebido por todos os nós que estão na área de alcance de transmissão do nó de origem. Cada pacote *Route Request* identifica a origem e o destino da rota que está sendo buscada e contém uma identificação da requisição determinada pelo iniciador do processo de descoberta de rotas. Cada nó intermediário, ao receber este pacote, verifica no seu *cache* se possui uma rota para o destino requisitado. Se o nó intermediário conhecer uma rota válida para este destino, envia para a origem um pacote de resposta *Route Reply* (RREP), como pode ser visto na Figura 2.2, que contém uma lista com a seqüência de todos os nós até o destino. Caso o nó desconheça uma rota para o destino, ele reenvia o pacote RREQ para os seus vizinhos, após ter inserido seu próprio endereço no registro de rotas armazenado no pacote. O pacote RREQ propaga-se através da rede

até alcançar o nó de destino, ou um nó que possua uma rota para este destino. Quando a rota é encontrada, um pacote RREP, contendo a seqüência de nós para alcançar o destino, será enviado ao nó de origem.

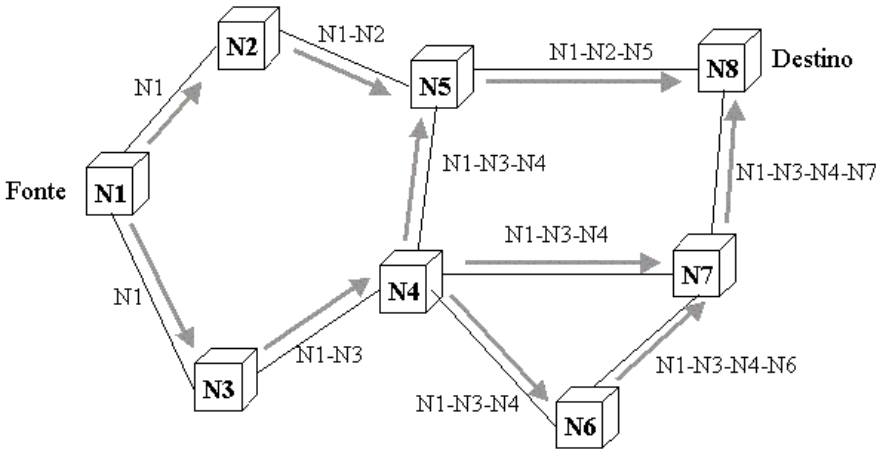


Figura 2.1: Descoberta de rotas usando o protocolo DSR

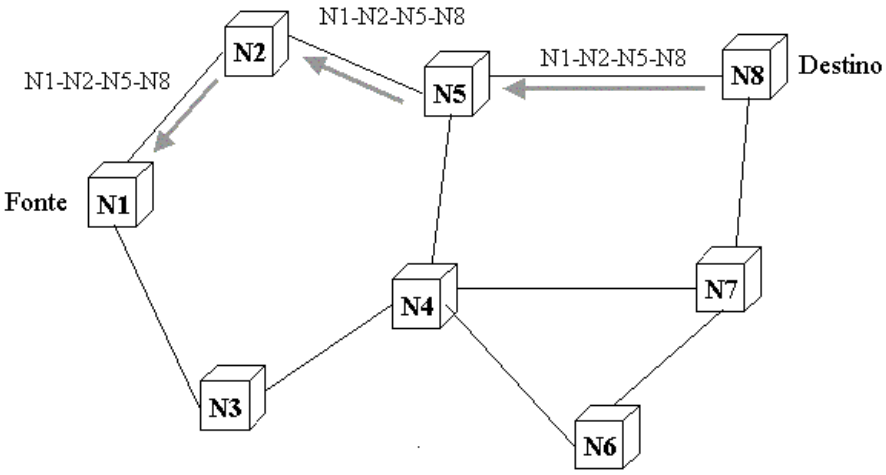


Figura 2.2: Propagação do *Route Reply* (RREP) no protocolo DSR

Para que o DSR funcione em conexões unidirecionais, é necessário que o nó que responderá à requisição de rotas verifique em seu *cache* se possui uma rota para o nó de origem. Caso não possua, um mecanismo de descoberta de rotas é acionado para encontrar um caminho para este nó. Para evitar infinitas recursões de descoberta de rotas, o nó destino deve incluir (*piggyback*) a reposta à requisição de rota no pacote contendo

seu próprio *Route Request* para a origem. Embora o DSR suporte rotas unidirecionais, o IEEE 802.11 exige uma troca de RTS/CTS/Dados/ACK para todos os pacotes *unicast*, implicando na necessidade de usar conexões bidirecionais para enviar pacotes de dados. Portanto, um pacote *Route Reply* pode ser encaminhado de volta a origem revertendo a seqüência de saltos contidas no pacote RREQ que chegou ao nó destino.

O DSR permite que cada nó mantenha múltiplas rotas para o mesmo destino. Desta forma, em caso de falha em algum nó na rota para o destino pode-se evitar uma nova inundação na rede, caso a fonte possua um caminho alternativo em sua tabela. Por outro lado, em cenários de alta mobilidade, as mudanças de topologia da rede podem causar freqüentes quebras de enlace, que aumentam consideravelmente a sobrecarga de roteamento e diminuem a taxa de entrega de pacotes [5].

Para evitar a inundação da rede com pacotes RREQ´s, utiliza-se o processo de questionar primeiramente aos nós vizinhos, para verificar se alguma rota está disponível para o destino desejado. Esse processo é feito por meio do envio de um primeiro pacote RREQ com um limite de salto igual a zero, significando que o pacote não deve ser encaminhado para os outros vizinhos. Se nenhuma resposta é obtida, um novo pacote RREQ é propagado através da rede.

O protocolo DSR possui a vantagem de ser capaz de "aprender" rotas. Quando um nó **A** encontra uma rota para um nó **C** passando pelo nó **B**, **A** aprenderá uma rota para **B**, e **C** aprenderá uma rota para **A**. Quando os dados começarem a fluir de **A** para **C**, **B** aprenderá uma rota para **C** e **B** aprenderá uma rota para **A** quando o pacote RREP passar por **B**. Cada rota aprendida possui um tempo de vida associado e, quando este tempo expira, a rota se torna inválida e deve ser descartada.

No mecanismo de manutenção de rotas, o nó detecta alterações na topologia da rede, devido à movimentação dos nós, que podem comprometer o uso das rotas. Desta forma, se um nó percebe a queda de um enlace em uso, envia um pacote *Route Error* (RERR) para a fonte, pelo caminho reverso. A fonte remove qualquer rota contendo a conexão falha de seu *cache* e inicia um novo procedimento de descoberta de rotas, caso não possua em seu *cache* uma rota alternativa para este destino. Os nós intermediários, que encaminham o pacote RERR, também atualizam seu *cache* de forma similar.

O protocolo DSR apresenta algumas otimizações adicionais [4] descritas a seguir.

- **escuta promíscua** - os nós também podem aprender rotas em modo promíscuo, "ouvindo" pacotes que não são endereçados a eles. O nó verifica se estes pacotes podem ser encaminhados por ele, para obter uma rota mais curta para o destino. Caso isto seja possível, o nó envia um pacote "RREP gratuito" para a fonte da rota com a informação de uma nova e melhor rota. A escuta promíscua permite que um nó aprenda diferentes rotas sem participar diretamente do processo de descoberta de rotas. Entretanto, esta característica exige um receptor ativo nos nós, acarretando em um maior consumo de energia, o que não é desejável em redes sem-fio.

- **salvamento** - este processo consiste em um nó intermediário poder usar uma rota alternativa do seu *cache* quando um pacote de dados encontra uma conexão quebrada em sua rota da fonte. Caso não haja uma rota alternativa no seu *cache*, o pacote é descartado.

- **reparo de rotas gratuito** - um nó fonte, quando recebe um pacote RERR, inclui este pacote no RREQ seguinte, auxiliando assim a limpeza dos *caches* dos outros nós.

2.1.2 *Destination Sequenced Distance Vector* - DSDV

O protocolo DSDV [12] é um protocolo de roteamento proativo, baseado no algoritmo de vetor de distâncias, que trabalha requisitando periodicamente, de cada um dos nós vizinhos, suas tabelas de roteamento, com a finalidade de mantê-las atualizadas. Cada nó da rede mantém uma tabela de roteamento contendo o próximo salto e o número de saltos para cada destino alcançável. As tabelas incluem rotas para todos os nós da rede, mesmo que nunca seja necessário enviar pacote para este nó. Cada nó mantém apenas uma rota para cada destino.

Os *loops* de rotas podem ocorrer quando informações de roteamento incorretas são mantidas na rede após uma troca de topologia. Geralmente ocorre quando um nó detecta uma queda no enlace com o nó vizinho e, antes que consiga propagar sua nova tabela,

recebe de outro nó informação desatualizada referente à conexão interrompida. A vantagem principal do DSDV sobre os protocolos baseados em vetor de distâncias tradicionais é que ele garante ausência de *loops*, usando o conceito de número de seqüência mantido em cada rota. O número de seqüência é estabelecido pelo nó destino e é incrementado a cada novo aviso de rota. As rotas mais recentes possuem um número de seqüência maior e são as mais favoráveis. Caso os números de seqüência sejam iguais, a rota que tiver o menor número de saltos será a mais favorável. Neste contexto, o uso de números de seqüência faz com que o DSDV se adapte melhor para redes de topologia dinâmica como redes *ad hoc*.

O DSDV inicia um processo de atualização de rotas periodicamente, ou quando a topologia da rede se altera, para manter as tabelas de roteamento consistentes. Na implementação do DSDV é estabelecido um intervalo mínimo entre atualizações por troca de topologia. Portanto, a transmissão desta atualização é atrasada, quando necessário, de forma a cumprir o intervalo mínimo estabelecido entre duas atualizações. Este procedimento visa a evitar que haja sobrecarga na rede, quando a troca de topologia está ocorrendo muito rapidamente. Quando um nó **B** percebe que sua conexão para **C** foi interrompida, marca sua rota para **C** com um contador de saltos infinito, incrementa o numero de seqüência da rota que foi "quebrada" e propaga esta nova tabela na rede. Com este procedimento, qualquer nó **A** que esteja roteando pacotes através de **B** incorpora esta métrica de rota infinita em sua tabela de roteamento até que o nó **A** "ouça" uma rota para **C** com um número de seqüência maior.

O DSDV possui dois tipos de atualizações que podem ser enviadas por um nó: incremental e completa. Na atualização incremental, o nó envia apenas as informações que foram alteradas em sua tabela, desde o seu último envio, e na atualização completa o nó envia todas as informações contidas em sua tabela. Com este procedimento, evita-se possíveis congestionamentos na rede.

2.1.3 *Ad Hoc On Demand Distance Vector* - AODV

O protocolo AODV [5, 13] é um protocolo reativo, baseado em vetor de distâncias, e pode ser considerado como uma combinação do DSR e do DSDV. Assim como o DSR, o AODV é baseado em demanda, ou seja, descobre rotas somente quando necessário, e utiliza os mecanismos de **descoberta de rotas** e **manutenção de rotas**. Entretanto, o AODV utiliza a característica do DSDV de obrigar todos os nós intermediários a estabelecerem dinamicamente entradas em tabelas de roteamento locais para cada destino ativo. Cada nó tem conhecimento do próximo salto para alcançar o destino e a distância em número de saltos. Pode ser considerado como uma versão melhorada do DSDV, uma vez que seu funcionamento baseado em demanda minimiza o número de inundações na rede exigido pelo DSDV para criação de rotas.

Quando um nó necessita encontrar uma rota para outro nó, e esta rota não está presente na sua tabela de rotas, inicia um procedimento de descoberta de rotas (Figura 2.3), enviando pacotes *Route Request* (RREQ) para todos os nós vizinhos, incluindo o último número de seqüência para aquele destino. Os pacotes RREQ são propagados pela rede até alcançar o nó destino ou um nó intermediário com uma rota recente para o destino. Durante o processo de encaminhamento do pacote RREQ, os nós intermediários gravam em suas tabelas de rotas o endereço do vizinho que encaminhou o pacote. Desta forma, estabelece um caminho reverso que será utilizado pelo pacote *Route Reply* (RREP) para alcançar o nó de origem (Figura 2.4), quando a rota para o destino for encontrada.

Uma importante característica do AODV é manter um estado relacionado ao tempo em cada nó, com referência às entradas da tabela de roteamento. Isto significa que uma entrada é expirada caso não seja utilizada em um espaço de tempo pré-determinado. O AODV utiliza números de seqüência para cada destino, para evitar *loops* de roteamento causados pela utilização de rotas que não são mais válidas.

Em cada entrada na tabela de roteamento é mantido o conjunto de nós antecessores que utilizam esta entrada para rotear pacotes de dados. Então, quando uma conexão é interrompida, estes nós antecessores são notificados com pacotes *Route Error* (RERR). Cada nó antecessor encaminha este pacote para sua lista de nós antecessores, permitindo

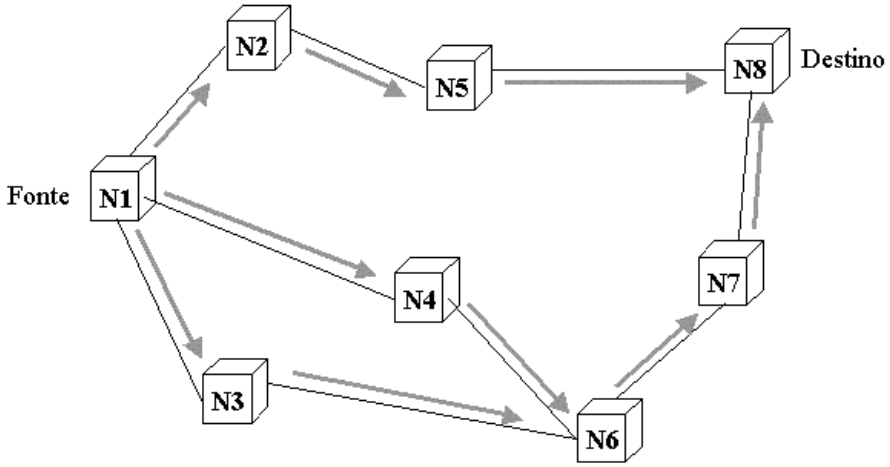


Figura 2.3: Descoberta de rotas usando o protocolo AODV

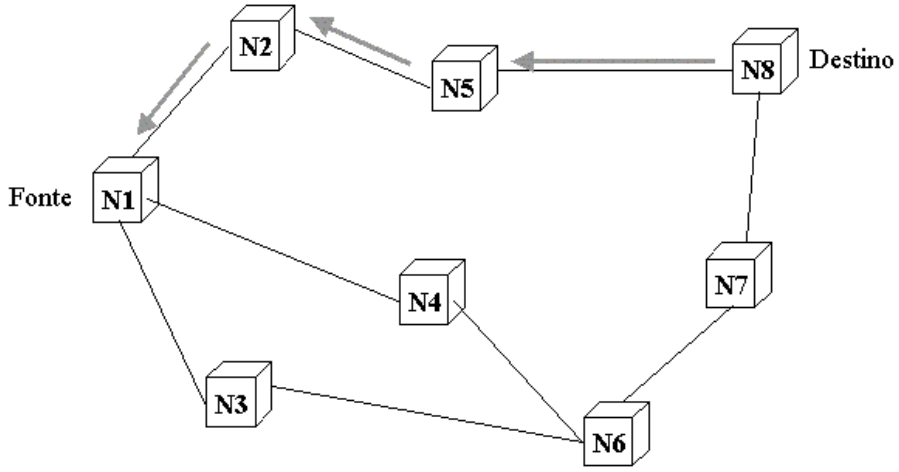


Figura 2.4: Propagação do *Route Reply* (RREP) no protocolo AODV

assim que efetivamente seja propagada a informação de conexão falha.

Para a manter a conectividade com os nós vizinhos, o AODV normalmente exige que cada nó periodicamente transmita uma mensagem *HELLO*. Estas mensagens são enviadas com a finalidade de detectar se os nós vizinhos estão ativos. Se um nó não recebe mensagens *HELLO* de um vizinho para qual foi enviado tráfego durante um determinado período de tempo, assume-se que o nó se moveu e esta conexão foi interrompida. Neste caso, o nó avisa a todos os nós que dependiam desta conexão, por meio de um RREP “não

solicitado" de rotas, contendo uma métrica infinita para aquele destino, que o mesmo não está mais disponível. Se a rota ainda estiver sendo usada, o nó pode realizar uma nova busca de rota. Dependendo do protocolo de acesso ao meio utilizado, a especificação do AODV sugere uma outra forma alternativa de verificar a conectividade com os nós vizinhos. O nó pode fazer uso dos métodos da camada de enlace para detectar uma eventual queda na conexão, de forma a consumir menos energia e banda.

Para as simulações realizadas neste trabalho foi utilizada a implementação do protocolo AODV que elimina o mecanismo padrão de mensagens *HELLO*, utilizando, para a manutenção de rotas, somente as informações da camada de enlace do 802.11. A utilização deste procedimento melhora bastante o desempenho do AODV [3], resultando em uma significativa economia na sobrecarga de roteamento, ocasionada pela transmissão das mensagens *HELLO*. Por outro lado, todas as detecções de quebra de enlace ocorrem por demanda. A perda da conectividade não é percebida até que haja necessidade de enviar um pacote por este enlace, enquanto que o uso de mensagens *HELLO* permite que se detecte a queda do enlace antes que um pacote necessite ser encaminhado por esta conexão.

2.2 Considerações sobre os protocolos

As técnicas de roteamento proativo buscam determinar a localização dos nós na rede durante todo o tempo, de modo que o tráfego possa ser encaminhado prontamente, assim que surgir a necessidade. Além disso, os esquemas de roteamento proativo continuamente fazem novas avaliações dos caminhos por onde o tráfego flui, ajustando-os às mudanças de circunstâncias. O roteamento reativo, por outro lado, procura a localização de um nó apenas quando algum tráfego necessita ser enviado para este nó, normalmente utilizando alguma forma de inundação da rede nessa busca. Os protocolos reativos geralmente mantêm os caminhos encontrados até que não sejam mais válidos, mesmo quando se tornam incovenientes devido aos movimentos dos nós.

Em redes com uma topologia dinâmica, o DSDV apresenta sérias dificuldades para manter rotas válidas e, por este motivo, muitos pacotes são perdidos. Com o aumento da

mobilidade, seu esforço para manter rotas para todos os nós aumenta o tráfego de controle da rede. O DSDV transmite atualizações periódicas, independente da troca de topologia, o que o torna ineficiente. O DSDV também apresenta um valor alto na sobrecarga de roteamento em *bytes*, conseqüência da necessidade de atualizar freqüentemente suas tabelas de roteamento, e estas atualizações contêm as entradas das tabelas de roteamento.

Embora o DSR e o AODV compartilhem a mesma característica de buscar rotas somente na necessidade de enviar um pacote de dados, eles apresentam algumas diferenças. A primeira delas é que o DSR obtém um maior conhecimento da rede por meio de escuta promíscua e aprendizagem das rotas dos pacotes que encaminha. O AODV, como tem um conhecimento da rede mais limitado, é obrigado a iniciar procedimentos de descoberta de rotas mais freqüentemente, o que acarreta em uma sobrecarga maior na rede. Em um único ciclo de descoberta de rotas, o DSR responde a todos os RREQ's que alcançam o destino e o AODV responde apenas ao primeiro que recebe, ignorando o resto. Com isto, no DSR, a fonte aprende várias rotas alternativas para o mesmo destino, enquanto que o AODV mantém em sua tabela apenas uma entrada para cada destino. Quando as rotas têm muitos saltos, o roteamento na fonte usado pelo DSR acarreta em um considerável aumento na sobrecarga de roteamento em *bytes*. Já o protocolo AODV apresenta uma baixa sobrecarga de roteamento em *bytes*, devido aos pacotes de dados carregarem somente o endereço de destino e não as rotas para alcançar este destino. Entretanto, apresenta uma alta sobrecarga de roteamento em pacotes devido às mensagens *HELLO* que envia periodicamente para os seus vizinhos.

O AODV apresenta-se melhor que o DSR, com o aumento do tráfego, o aumento da mobilidade, e/ou o aumento do número de nós. A razão para isto é o uso de roteamento na fonte usado pelo DSR, que fornece benefícios até um certo ponto. Entretanto, o DSR tem um melhor desempenho em situações mais amenas, com redes com pequeno número de nós, baixa mobilidade e poucas fontes.

O DSDV apresenta taxa de entrega de pacotes mais baixa em relação aos outros protocolos avaliados, devido aos descartes de pacotes antes que as rotas tenham sido estabelecidas na rede. O DSR freqüentemente se utiliza de rotas antigas, já que não possui nenhum mecanismo para eliminar rotas inválidas do seu *cache* e o tamanho da rota é

o parâmetro para escolha quando depara-se com múltiplas rotas para o mesmo destino, causando assim o alto consumo de largura de banda e poluição dos *caches* em outros nós.

2.3 Comentários

Neste capítulo foram apresentados as características gerais dos protocolos AODV, DSR e DSDV. Entretanto, o comportamento de cada um dos protocolos pode sofrer alterações de acordo com o cenário que está sendo utilizado, e/ou os parâmetros selecionados para realizar as simulações. Cada protocolo apresenta vantagens e desvantagens, dependendo das condições que lhe são impostas. O que veremos no capítulo 5 é que alguns resultados não condizem com as expectativas. No início deste trabalho, acreditávamos que um protocolo com características proativas, como o DSDV, seria o mais adequado para o cenário proposto, devido ao fato de que os grupos de nós apresentam baixas velocidades e as condições de tráfego são amenas. Imaginávamos, ainda, poder extrair o benefício característico dos protocolos proativos em apresentar pequenos atrasos para entrega de pacotes. Entretanto, o DSDV apresentou baixo desempenho na taxa de entrega dos pacotes, quando comparado aos protocolos que funcionam por demanda. Nos cenários com propósitos militares, a entrega dos pacotes de forma eficiente e rápida é de extrema relevância. O protocolo “ideal” deve atender a todas as restrições impostas pelas necessidades de comunicação.

No próximo capítulo, será descrito sucintamente alguns modelos de mobilidade individuais e em grupos utilizados para representar os padrões de movimento dos usuários em uma rede móvel. Nesse capítulo também será detalhado o cenário militar utilizado no nosso trabalho, assim como a proposta de um modelo para retratar com mais realismo os movimentos dos grupos que compõem este cenário.

Capítulo 3

Um Novo Modelo de Mobilidade

A TOPOLOGIA e o movimento dos nós são fatores cruciais no desempenho dos protocolos. Uma vez que os nós tenham sido inicialmente distribuídos na área de simulação, o modelo de mobilidade impõe o movimento dos nós na rede. Como a mobilidade dos nós impacta diretamente no desempenho dos protocolos [14], os resultados das simulações obtidos com modelos de movimento não realísticos podem não refletir corretamente o verdadeiro desempenho dos protocolos. A maioria dos modelos de mobilidade existentes para redes *ad hoc* não provê cenários de movimentos realísticos; são limitados ao modelo *Random Waypoint*, descrito a seguir. O modelo de movimentação *Random Waypoint* é considerado muito genérico e distante de uma aplicação real. Isto se deve, em parte, ao modo como ocorrem as movimentações, pois cada dispositivo se move de forma completamente independente dos demais.

Atualmente, existem duas formas principais de representar os padrões de movimentos dos nós de uma rede móvel [15]: os registros de movimentação (*traces*) e os modelos de mobilidade. O uso de registros de movimentos permite a captura de informações do comportamento real de movimentação dos nós móveis. Fornecem informações precisas, principalmente quando envolve um grande número de nós durante um longo período de observação. Entretanto, em ambientes muito dinâmicos, como em redes *ad hoc*, a captura destes registros torna-se uma tarefa difícil. Neste tipo de redes é necessário a utilização de modelos de mobilidade, que se propõem a representar o comportamento dos nós móveis sem o uso de *traces*. Além disso, o uso de *traces* reais impede o emprego de técnicas

baseadas em amostragem estatística para a obtenção de medidas de eficácia, visando à generalização dos resultados.

A ferramenta ScenGen foi utilizada para modelar o movimento dos nós móveis, baseada nas características táticas e na previsão de movimentos dos integrantes da operação militar. Na tentativa de modelar o cenário utilizado neste estudo da forma mais realista possível, se fez necessário propor um novo modelo de mobilidade, uma vez que os modelos disponíveis no ScenGen não foram suficientes para alcançar este objetivo. Dessa forma, o Modelo *Mixed Waypoint* foi adicionado ao conjunto de modelos disponíveis na ferramenta ScenGen.

Na seção 3.1 é apresentada a ferramenta ScenGen; na seção 3.2 são mostrados os principais modelos de mobilidade utilizados para a avaliação de desempenho em redes *ad hoc*; na seção 3.3 é detalhado o cenário militar que foi utilizado neste trabalho; um novo modelo de mobilidade é disponibilizado no ScenGen e é apresentado na seção 3.4; e por fim, é descrito alguns comentários sobre o conteúdo deste capítulo na seção 3.5.

3.1 O Gerador de Cenários - ScenGen

O ScenGen [16] é uma ferramenta desenvolvida por Li Qiming, que permite a geração de cenários de mobilidade que possibilitam o desenvolvimento de simulações em redes móveis *ad hoc*. Esta ferramenta gera uma saída configurada para o uso no simulador de rede *ns-2*, que será descrito no capítulo 4, a partir de *traces* da movimentação dos nós da rede ou por meio de modelos de mobilidade. O ScenGen foi desenvolvido na linguagem C++ e implementa os seguintes modelos de mobilidade: *Random Waypoint, Perseguição, Browniano, Coluna* e *Gauss-Markov*.

O ScenGen gera padrões de movimentação em grupos e permite que se especifique, dentro da área de simulação, áreas menores que são capazes de se mover segundo algum dos modelos implementados. Os dispositivos contidos nesta área também se movimentam, dentro da sua área, de acordo com um modelo de mobilidade especificado, permitindo assim que os grupos de dispositivos se movam de forma aleatória. Este modelo de

grupos é mais apropriado para representar determinadas aplicações como, por exemplo, uma operação militar onde os grupos constituem os pelotões de infantes.

O programa admite duas entradas: o arquivo **model-spec**, que apresenta todos os parâmetros de cada modelo com os respectivos valores *default* para cada um destes parâmetros; e o arquivo **scen-spec**, que descreve o cenário que se deseja simular.

O arquivo **scen-spec** apresenta uma seção denominada "*global*", que deve conter informações globais sobre o cenário a ser especificado, tais como tamanho da área de simulação, tempo de início da simulação e tempo de término da simulação.

Para cada grupo de nós presente no cenário, existe uma seção, no arquivo **scen-spec**, identificada pelo nome do grupo, descrevendo as especificações desse grupo. Esta especificação deve conter, no mínimo, dois parâmetros: número de nós e modelo de mobilidade utilizado para modelar o movimento destes nós. Os outros parâmetros do modelo que não são referenciados no arquivo são inicializados com o valor padrão definido no arquivo **model-spec**.

A ferramenta *Ad-Hockey* [17], que está integrada ao simulador *ns*, pode ser utilizada para visualização da movimentação dos nós do cenário gerado, antes de executar a simulação, permitindo uma avaliação prévia do comportamento dos nós.

O ScenGen permite a inclusão de novos modelos ou alteração de modelos já existentes. Para adicionar um modelo à ferramenta, deve-se desenvolver um arquivo com o código do novo modelo na linguagem C++.

3.2 Modelos de Mobilidade para Redes *Ad Hoc*

Os modelos de mobilidade para redes *ad hoc* buscam representar o comportamento da movimentação dos dispositivos móveis na rede. Esses modelos são utilizados na avaliação do desempenho de aplicações e sistemas de comunicação, permitindo analisar o impacto causado pela mobilidade no funcionamento dos mesmos [18].

Segundo Camp [15], existem no mínimo sete modelos de mobilidade individual e

cinco modelos de mobilidade em grupo que podem ser utilizados para representar o movimento dos nós em uma diversidade de cenários, e que são usados para avaliar o comportamento de algoritmos de roteamento em redes *ad hoc*. Entretanto, os padrões de movimentos gerados por esses modelos não reproduzem fielmente cenários realistas. Por exemplo, as pessoas em um campus de uma universidade, em conferências ou em *shoppings* normalmente não se movem em direções aleatórias. Elas selecionam um destino específico (não aleatório) e seguem um caminho bem definido para alcançar este destino. Pesquisas anteriores [14, 15, 18, 19] mostram que o desempenho de um protocolo em redes *ad hoc* pode variar significativamente de acordo com a utilização de diferentes modelos de mobilidade. Portanto, é de extrema importância que o modelo de mobilidade escolhido represente, da melhor forma possível, o movimento dos nós no cenário que se pretende simular na rede, podendo-se, assim, conduzir um estudo para determinar qual o protocolo mais apropriado para ser usado. O modelo de mobilidade selecionado deve, portanto, buscar representar os movimentos dos nós móveis em cenários reais.

Os modelos de mobilidade podem ser classificados de duas formas: os modelos de mobilidade individual (entidade) e os modelos de mobilidade em grupo, e serão descritos a seguir.

3.2.1 Modelos de Mobilidade Individual

Os modelos de mobilidade individual são modelos de mobilidade que representam o comportamento de movimentação de um nó móvel, cujas ações de cada nó são completamente independentes dos demais nós móveis da rede. Esses modelos são os mais utilizados na literatura para avaliação da eficiência dos algoritmos de roteamento em redes *ad hoc* [20], devido à sua modelagem mais simples e fácil implementação. Porém, estes modelos restringem-se a comportamentos de movimentação específicos, que, em alguns casos, se afastam demais da realidade [18]. A seguir, apresentaremos os dois modelos de mobilidade individual mais comumente utilizados pelos pesquisadores para avaliar o desempenho dos protocolos de redes *ad hoc*.

Modelos de Mobilidade de Percurso Aleatório

No modelo de mobilidade de percurso aleatório (*Random Walk*) [20, 21] ou *Browniano*, um nó move-se de sua posição atual para uma nova posição selecionando aleatoriamente uma direção e uma velocidade. A nova velocidade e direção são ambas selecionadas aleatoriamente dentro de um intervalo [velocmin,velocmax] e [0,2π] respectivamente. É um modelo de mobilidade sem memória, isto é, a direção e velocidade do movimento em um novo espaço de tempo não têm relação nenhuma com os valores dos instantes anteriores. Com isto, este modelo pode gerar um comportamento não realístico, com mudanças súbitas de direção, paradas abruptas e acelerações bruscas no movimento do nó móvel.

Modelos de Mobilidade *Random Waypoint*

O modelo de mobilidade *Random Waypoint* (RWP) [22], divide o percurso de um nó móvel em períodos de movimentação e de pausa. Inicialmente, o nó móvel permanece em um local por um certo período de tempo (tempo de pausa) e depois se move para um novo destino, selecionado aleatoriamente na área de simulação e com uma velocidade que segue uma distribuição uniforme entre [velocmin, velocmax], conforme pode ser visto na Figura 3.1. Quando o nó alcança o destino, pára por um determinado tempo de pausa, e então repete o processo selecionando um novo destino e velocidade.

Muitos pesquisadores utilizam este modelo, onde a velocidade e direção do movimento no novo intervalo de tempo não têm nenhum relacionamento com os valores utilizados no intervalo anterior. Este modelo se comporta de forma semelhante ao modelo *Random Walk* se o tempo de pausa for configurado em zero.

3.2.2 Modelos de Mobilidade em Grupo

Esses modelos de mobilidade buscam representar o comportamento da movimentação de um grupo de nós móveis, cujo movimento de cada nó é dependente do movimento dos outros nós. Em redes de telefonia celular, o foco dos modelos de mobilidade é em movimentos individuais, uma vez que as comunicações, em geral, são realizadas ponto a ponto; já em redes *ad hoc* existem várias situações em que é necessário modelar o comportamento dos nós móveis quando eles se movem de forma cooperativa [19], como por

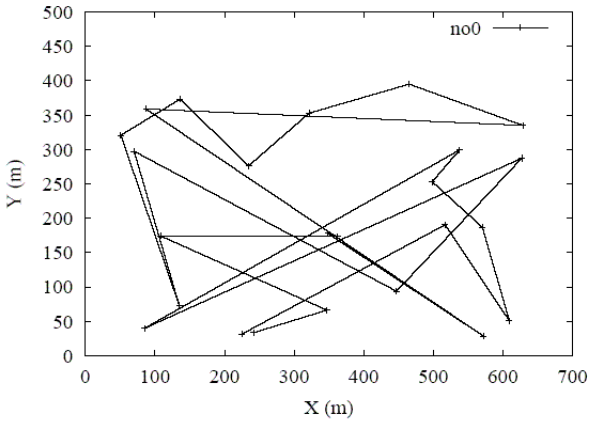


Figura 3.1: Mobilidade usando o modelo *Random Waypoint*.

exemplo, os cenários militares terrestres. Nesses cenários, os grupos de soldados se movem de forma cooperativa para cumprir uma determinada tarefa. A Figura 3.2 exibe à esquerda a representação de uma rede *ad hoc* típica que segue o modelo de mobilidade *Random Waypoint*, estando os nós livres para moverem-se em qualquer direção e inicialmente posicionados em qualquer ponto dentro da área especificada. No lado direito representa-se uma rede *ad hoc* militar, onde os grupos de nós se movem juntos com a finalidade de cumprir uma missão. É uma representação gráfica de um *trace* real de um exercício em um campo de batalha, ocorrido em 2000 na Austrália [23]. A seguir é apresentado alguns modelos de mobilidade em grupo que podem ser aplicados em operações com fins militares.

Figura 3.2: Movimento Aleatório x Movimento Militar.

Modelos de Mobilidade em Coluna

Este modelo [24] representa um conjunto de nós móveis que se movem ao redor de uma linha ou coluna que está se movendo em uma determinada direção, como por exemplo, uma fila de soldados avançando juntos de encontro ao inimigo.

Para a implementação deste modelo, define-se uma grade de referência inicial formando uma coluna de nós móveis. Cada nó móvel é então posicionado em relação ao seu ponto de referência na grade. O movimento aleatório dos nós móveis ao redor do seu ponto de referência é baseado em um modelo de mobilidade individual. O movimento da grade de referência é baseado em uma distância e um ângulo aleatório e os nós seguem a grade e continuam a mover-se ao redor do seu ponto de referência. Este ângulo está incluído no intervalo de 0 a π, uma vez que os movimentos são direcionados somente para frente.

Modelos de Mobilidade de Perseguição

Este modelo [24] representa nós móveis acompanhando um alvo particular. Pode representar, por exemplo, policiais tentando capturar um criminoso.

A figura 3.3 mostra nós móveis movendo-se de acordo com o modelo de mobilidade de perseguição. O nó branco representa o nó que está sendo perseguido e os nós pretos representam os nós perseguidores.

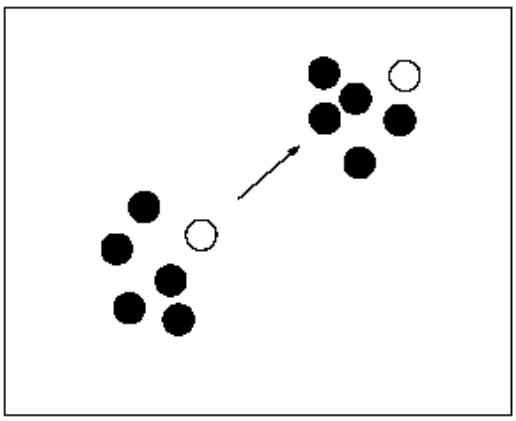


Figura 3.3: Mobilidade segundo o modelo Perseguição.

Modelos de Mobilidade de Grupo com Ponto de Referência - RPGM

Este modelo foi desenvolvido por Gerla [19] e representa o movimento aleatório de um grupo de nós móveis, bem como o movimento aleatório de cada nó individualmente com o grupo.

Neste modelo, cada grupo tem um centro lógico. O movimento do centro define o comportamento de movimentação de todo o grupo, incluindo localização, velocidade, direção, aceleração, etc. Desta forma, a trajetória do grupo é determinada por um caminho realizado pelo centro do grupo. Geralmente, os nós são distribuídos uniformemente dentro da área geográfica do grupo e cada nó é associado a um ponto de referência, que segue o movimento do grupo. Um nó é aleatoriamente posicionado na vizinhança de seu ponto de referência. O esquema de ponto de referência permite a modelagem de um comportamento de movimentação aleatório independente para cada nó, além do movimento do grupo.

A figura 3.4 exemplifica este modelo com dois grupos. Cada grupo tem um vetor de movimentação de grupo $\overrightarrow{V_{gi}}$. Na movimentação do nó, o ponto de referência move-se de RP(*t*) para RP(*t*+1), com o vetor de movimentação do grupo $\overrightarrow{GM}$=$\overrightarrow{V_{gi}}$. Então, a nova posição do nó é gerada adicionando-se o vetor de movimento aleatório $\overrightarrow{RM}$ ao novo ponto de referência RP(*t*+1). O vetor $\overrightarrow{RM}$ tem seu comprimento uniformemente distribuído dentro de um certo raio centralizado no ponto de referência e sua direção uniformemente distribuída entre 0 e 2π. Este vetor aleatório $\overrightarrow{RM}$ é independente da localização anterior do nó.

O modelo RPGM (*Reference Point Group Mobility*) define o movimento do grupo explicitamente, fornecendo um caminho para cada grupo. O caminho que um grupo segue é definido por uma seqüência de *check points* (pontos de verificação) ao longo da trajetória correspondendo a um intervalo de tempo de *t*.

Por meio da seleção de *check points*, pode-se modelar muitas situações realistas, onde um grupo deve alcançar destinos pré-definidos com um dado intervalo de tempo para completar uma determinada tarefa. O uso de arquivos de cenário contendo *check points* tem a vantagem de desassociar o padrão de movimentação do modelo em si. Muitos métodos podem ser usados para gerar arquivos de cenário: manualmente, digitalizando uma rota de um mapa, usando saídas de um programa ou por meio de um perfil realista.

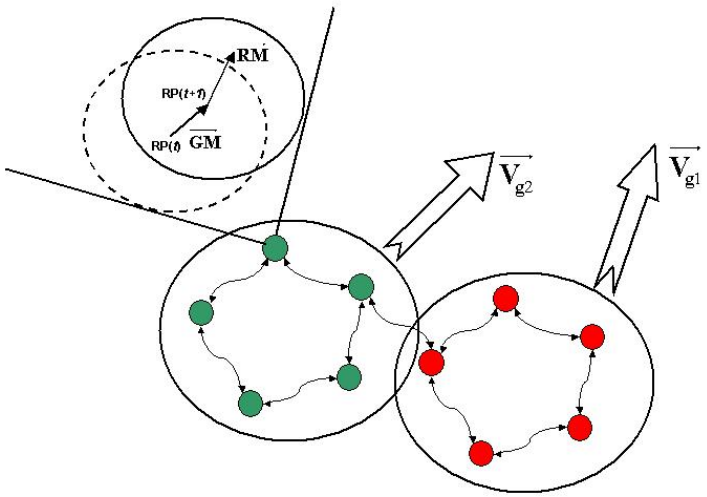


Figura 3.4: Mobilidade em Grupo usando o modelo RPGM.

Um exemplo [15] da utilização deste modelo é um resgate numa avalanche, onde a equipe de resgate é formada por cães e pessoas trabalhando cooperativamente. O caminho que os cães devem seguir é definido pelas pessoas, já que elas conhecem a localização aproximada das vítimas. Os cães criam seus próprios caminhos aleatórios em torno da área predeterminada.

3.3 Cenário Militar

3.3.1 Requisitos Básicos

No campo de batalha do futuro provavelmente se fará uso extensivo de comunicação sem fio (Figura 3.5). As unidades móveis poderão ser usadas nos centros de comando e controle, nos veículos (como carros de combate, helicópteros, navios ou aeronaves), assim como os próprios soldados poderão carregar seus terminais de comunicação pessoal. Portanto, para que o cenário descrito seja implementado de forma confiável, vários requisitos básicos devem ser atendidos para o uso de comunicação sem-fio em aplicações militares. Inicialmente, e como fator primordial, a segurança - as mensagens devem ser criptografadas de forma rápida e segura quando necessário. Em ambientes hostis, as comunicações

não devem sequer ser percebidas, uma vez que o inimigo deve estar tentando constantemente bloquear e interferir na comunicação, ou até mesmo destruir o transmissor. Além disso, deve-se privilegiar as necessidades de roteamento em condições de mobilidade diversas, uma vez que os nós da rede podem estar localizados em aeronaves sobrevoando a área a ser controlada; em veículos leves ou pesados, com velocidade moderada; ou em baixa velocidade, quando se considera combatentes a pé. Complementarmente, o sistema de comunicações deve lidar adequadamente com as diferentes prioridades advindas do nível de urgência das mensagens. Finalmente, o próprio ambiente onde as ações são conduzidas pode apresentar dificuldades de ordem física às transmissões eletromagnéticas (reflexão, difração, *scattering*, etc), devido a acidentes geográficos, como por exemplo, montanhas e florestas [25].

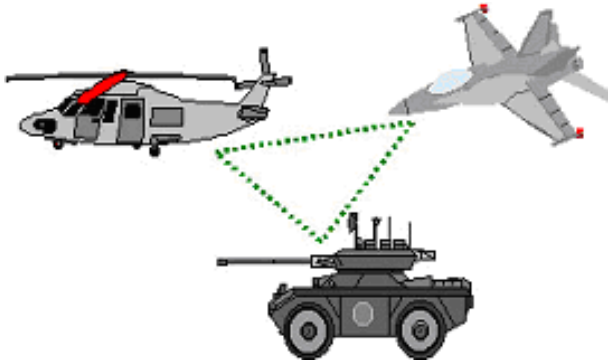


Figura 3.5: Uso de comunicação sem-fio em aplicações militares.

3.3.2 Movimentação

As utilizações militares de redes *ad hoc* possuem algumas características próprias que podem ser assim resumidas [23]: uma cadeia de comando bem definida, que pode impactar na topologia da rede; as unidades (grupos de nós) devem cooperar umas com as outras, uma vez que, normalmente, compartilham uma missão; e as operações militares, que tipicamente, são conduzidas dentro de limites espaço-temporais bem definidos. Esses fatores implicam em restrições à mobilidade dos nós da rede, em especial no controle da aleatoriedade dos movimentos [26].

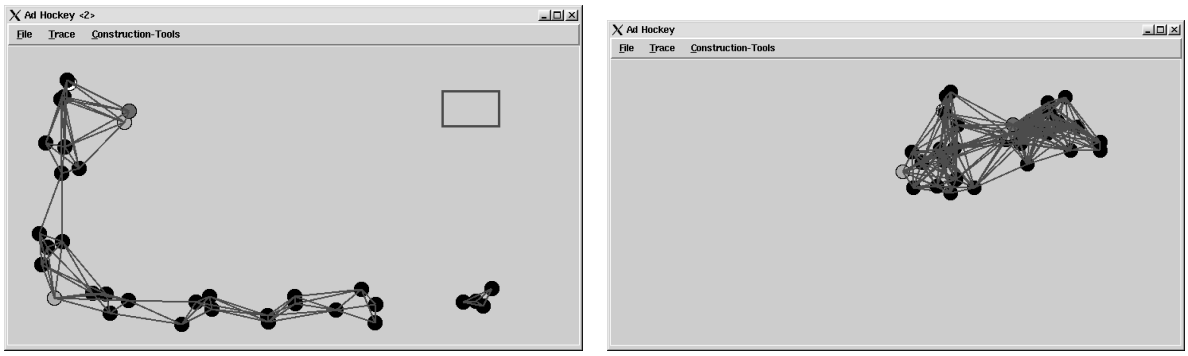
3.3.3 Descrição

Neste trabalho é apresentado um padrão de comunicação em uma ação de oportunidade, constituída de assalto e tomada de posição inimiga. Este tipo de ação caracteriza-se pela necessidade de um alto nível de coordenação entre os grupos e por não se esperar forte reação por parte do inimigo, devido ao efeito do elemento surpresa.

O cenário proposto na Figura 3.6 representa um típico pelotão de infantaria em operação militar, composto de 35 participantes, cada qual com seu comunicador pessoal, dotado da capacidade de formação de uma rede *ad hoc*. Este pelotão está dividido em oito grupos de combate, cada um com quatro elementos; um grupo adicional, formado por dois observadores, ocupa uma posição avançada em relação aos outros grupos, e tem como tarefa mantê-los informados da situação e das posições ocupadas pela força inimiga, quando houver; e uma Central de Comando, CC (representada pelo nó cinza na figura), operando no interior de um veículo (carro de combate, caminhão, etc).

Os grupos ocupam posições estratégicas para que possam alcançar, de forma cooperativa, um determinado ponto-objetivo neste cenário, com a finalidade de cumprir uma determinada tarefa, normalmente o domínio físico do objetivo. O padrão de tráfego empregado neste cenário consiste no envio de ordens e missões pela central de comando, seguido da mensagem de reconhecimento do grupo de combate que recebe a missão. Outro tipo usual de comunicação é o envio de informações por parte dos grupos de combate à CC, trazendo informes acerca do campo de batalha.

As características deste cenário incluem diversos particionamentos na rede causados pelo próprio comportamento da movimentação em grupo dos nós móveis, acarretando, a cada momento, diferentes situações de conectividade dos nós. A seleção de todos os parâmetros de mobilidade e tráfego para este cenário tem como objetivo uma maior aproximação da aplicação real.



(a) Posição inicial dos grupos de combate (b) Posição final dos grupos de combate

Figura 3.6: Cenário militar.

3.4 Modelo Proposto - *Mixed Waypoint*

Para atender às restrições de mobilidade do cenário utilizado, com um comportamento mais realístico, surgiu a necessidade de criar e implementar no ScenGen um novo modelo, que foi chamado de *Mixed Waypoint*.

Para adicionar um novo modelo à ferramenta deve-se implementar a modelagem proposta na linguagem de programação C++. Este código deve ser estruturado em uma classe com herança da classe **model**, que é implementada pelo ScenGen. Dentro desta classe todo o código que representa o movimento dos nós deve estar no método **makemove**. Este método é chamado sempre que a ferramenta necessite calcular a próxima posição de um nó.

Todo nó da simulação é um objeto da classe **node**. Esta classe possui algumas propriedades relativas à movimentação do nó. Estas propriedades são:

- node->dest: representa a posição de destino que o nó possuirá após a execução do movimento atual;
- node->pos: representa a posição atual do nó;
- node->startTime: representa o tempo em que o nó iniciará o movimento atual;
- node->arrivalTime: representa o tempo em que o nó irá atingir a posição node-

>dest;

- node->nextStartTime: representa o tempo em que o nó irá iniciar o próximo movimento;
- node->speed: representa a velocidade do nó no movimento atual.

Assim, as variáveis descritas acima devem ter os respectivos valores atribuídos no método **makeMove** para que a movimentação ocorra corretamente.

Após criar o código para o modelo proposto, este deve ser incorporado ao conjunto de modelos de mobilidade do ScenGen. O programa em C++ que caracteriza este modelo é apresentado em anexo no final deste trabalho.

3.4.1 Desenvolvimento

Este novo modelo busca representar o movimento de um nó, que parte de um ponto de origem prefixado e se move para um ponto de destino selecionado aleatoriamente dentro de uma sub-área definida na área de simulação, como mostra a Figura 3.7. Desta forma, todos os grupos partirão para o mesmo objetivo, mas alcançarão pontos distintos, restritos ao limite de uma pequena área.

A dimensão desta sub-área representa uma fração da área total da simulação, e sua localização é definida a partir de um ponto especificado pelo usuário no arquivo **scenspec** (especificação do cenário), que, para efeito de simplicidade do modelo, refere-se à localização do ponto do canto superior direito desta área. Note-se que esse esquema não compromete a generalidade do modelo.

Como não faz sentido dois nós moverem-se exatamente da mesma forma, o *Mixed Waypoint* modela o movimento de apenas um nó. O emprego principal deste modelo é modelar o movimento do centro do grupo, inspirado no modelo(RPGM) que foi descrito por Gerla [19].

O modelo utilizado para o cenário militar é uma especialização do RPGM, utilizando-se de características próprias do modelo de mobilidade individual *Random Waypoint* em

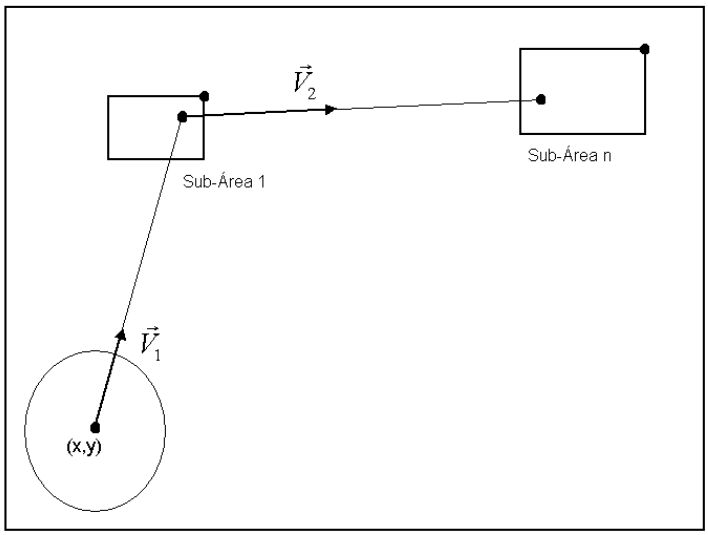


Figura 3.7: Modelo de Mobilidade *Mixed Waypoint*.

conjunto com as de grupo, permitindo um maior grau de controle e realismo. O modelo *Random Waypoint* apresenta algumas dificuldades inerentes ao processo de geração aleatória do posicionamento inicial e das subseqüentes movimentações dos nós, o que provoca uma considerável falta de aderência com o realismo dos movimentos. Embora muitos pesquisadores utilizem diretamente o modelo *Random Waypoint* em suas simulações, muitas vezes essas dificuldades deixam de ser endereçadas apropriadamente, no que diz respeito à preservação do efeito que se deseja simular.

O presente modelo pode ser considerado como uma classe de modelos, e apresenta a vantagem de prover uma espécie de *template* geral e flexível para descrever um conjunto de padrões de mobilidade.

3.4.2 Descrição do Modelo

O código abaixo é parte de um arquivo de especificação **scen-spec**, onde o centro do grupo foi modelado de acordo com o modelo *Mixed Waypoint*. O arquivo **scen-spec** deve conter configurações referentes a cada um destes parâmetros.

- posição inicial do nó (x_0, y_0);

- tamanho relativo da sub-área *i* de destino - percentual da área total de simulação - $perc_i$, i = 1, ..., número de sub-áreas;
- tempo de pausa inicial - antes do primeiro movimento - t_0;
- posição relativa de cada sub-área *i* de destino, em relação à área de simulação (canto superior direito) - (x_i, y_i);
- velocidade de deslocamento do nó até o próximo ponto (*i*) - gerado aleatoriamente no interior da sub-área *i* de destino - $\overrightarrow{V_i}$; e
- tempo de pausa no destino *i* - t_i.

```
[grupo1]
num_nodes = 4
member_area = rect (150,150)
member_model = Waypoint
member_model.T_min = 0
member_model.T_max = 5
member_model.V_min = 0
member_model.V_max = 2
# centro do grupo modelado com o modelo Mixed Waypoint
center_model = MixWP
# ponto inicial do centro do grupo está
# posicionado na coordenada (60,50)
# área de destino corresponde a 20% da área total da simulação; e
# tempo de pausa inicial é igual a 0
center_model.wp1 = (60,50,20,0)
# coordenada (1200,200) corresponde
# à posição do canto superior direito da próxima área de destino
# velocidade até o próximo ponto é igual a 13
# tempo de pausa quando alcançar o próximo destino é igual a 30
center_model.wp2 = (1200,200,13,30)
center_model.wp3 = (1500,200,14,200)
```

```
center_model.wp4 = (1700,200,15,200)
```

3.5 Comentários

Neste capítulo, foi mostrada a importância da escolha de um modelo de mobilidade adequado para representar o movimento real dos nós em um determinado cenário, uma vez que o desempenho dos protocolos de roteamento em uma rede *ad hoc* pode variar significativamente dependendo do modelo empregado. Este fato deve ser levado em consideração, principalmente, quando se está buscando encontrar o protocolo mais apropriado para ser utilizado em um cenário com características definidas. Dando continuidade a esta busca, foi proposto um novo modelo que foi implementado na ferramenta ScenGen, com o objetivo de retratar o cenário militar, em análise, de forma mais realista.

No capítulo seguinte serão apresentadas as principais características da modelagem e os detalhes referentes às simulações.

Capítulo 4

Simulações

UM dos métodos mais importantes para se avaliar o desempenho dos protocolos de roteamento em redes *ad hoc* é o uso de modelos de simulação. As simulações fornecem aos pesquisadores uma quantidade de benefícios significativos, incluindo a possibilidade de variações de cenários, isolamento de parâmetros e a exploração de uma variedade de métricas.

Neste trabalho, o objetivo das simulações é permitir uma análise do comportamento de três protocolos de roteamento em redes *ad hoc* (AODV, DSR e DSDV), sob a influência de um cenário que retrata uma aplicação militar, revelando os problemas decorrentes da utilização deste tipo de rede em um cenário com estas características, e buscando as melhores condições para contornar estes problemas. Além disso, por meio das simulações realizadas podemos avaliar o impacto que a mobilidade em grupo, a configuração de rede hierárquica e o movimento dos nós em uma direção pré-determinada podem causar no roteamento dos dados.

Por meio dos resultados obtidos neste trabalho foi possível verificar que a competição pelo acesso ao meio é uma grande limitação para este cenário. Portanto, de forma a melhorar o entendimento destes resultados, iniciaremos o capítulo com uma breve explicação dos métodos de acesso da subcamada MAC (*Medium Access Control*) do IEEE 802.11 na seção 4.1; na seção 4.2 é apresentado o simulador de redes ns-2, utilizado nas simulações realizadas; na seção 4.3 definimos as métricas que foram utilizadas para com-

parar o desempenho dos protocolos nesta análise; na seção 4.4 foi definido o padrão de movimentação e os respectivos parâmetros que foram utilizados nas simulações; na seção 4.5 foi definido o padrão de tráfego utilizado nas simulações.

4.1 O padrão IEEE 802.11

Em redes sem fio, várias estações compartilham o mesmo meio de transmissão. Portanto, controlar eficientemente o compartilhamento deste meio torna-se uma tarefa complexa. Muitos protocolos para a camada MAC foram propostos. O padrão IEEE 802.11 [27] é um padrão para redes locais sem fio que define tanto a camada física quanto a subcamada de controle de acesso ao meio (MAC) da camada de enlace, e é largamente utilizado em quase todas as simulações realizadas em pesquisas relacionadas a redes *ad hoc*.

A subcamada MAC define dois diferentes métodos de acesso: a função de coordenação centralizada (PCF - *Point Coordination Function*) e a função de coordenação distribuída (DCF - *Distributed Coordination Function*). Uma função de coordenação é um mecanismo que determina quando uma determinada estação tem permissão para transmitir.

4.1.1 *Point Coordination Function* - PCF

O PCF é um mecanismo centralizado onde o ponto de acesso controla o acesso ao meio. A decisão de quando uma estação pode transmitir é centralizada em um ponto, que determina qual estação deve transmitir e em que momento, evitando colisões. Embora o mecanismo centralizado tenha sido especificado para permitir a transmissão de tráfego de tempo-real, ele se baseia em enquetes (*polling*) do ponto de acesso, isto é, cada estação deve transmitir apenas quando receber uma enquete do ponto de acesso. Como o foco deste trabalho são as redes *ad hoc*, não existe o ponto de acesso e, conseqüentemente, o método de acesso centralizado não se mostra adequado [28].

4.1.2 *Distributed Coordination Function* - DCF

A função de coordenação distribuída (DCF) utiliza o protocolo CSMA/CA (*Carrier-Sense Multiple Access with Collision Avoidance*), com reconhecimento (ACK), para controlar o acesso ao meio. A utilização deste método é obrigatório para todas as estações e pontos de acesso nas configurações *ad hoc* e com infra-estrutura. O DCF é um mecanismo distribuído, onde a decisão de quando a estação deve transmitir é tomada individualmente pelos nós, o que pode resultar em transmissões simultâneas.

Existem duas técnicas que são usadas para transmissão de pacotes de dados em DCF: o método de acesso básico e um método de acesso opcional que usa troca de quadros RTS/CTS. No método de acesso básico, a estação que deseja transmitir deve ouvir o meio para certificar-se que nenhuma outra estação está transmitindo, antes de iniciar a transmissão. Se o meio estiver ocupado, isto é, outra estação estiver transmitindo, a estação aguarda o final da transmissão. Se o meio estiver livre a estação aguarda um certo intervalo de tempo (*Inter-Frame Space* - IFS). Se depois de decorrido este intervalo de tempo (ver Figura 4.1), o meio ainda estiver livre, a estação pode iniciar a transmissão. O valor deste intervalo de tempo é determinado de acordo com o tipo de quadro que deve ser transmitido. Os quadros ACK utilizam um intervalo de tempo chamado de SIFS (*Short Inter-Frame Space*) e têm prioridade sobre os pacotes de dados, que usam o intervalo DIFS (*Distributed Inter-Frame Space*). Além disto, para evitar colisão, uma estação deve esperar, além do tempo DIFS, um tempo aleatório (*backoff*). No caso de várias estações tentarem transmitir ao mesmo tempo, aquela que tiver o menor tempo de *backoff* irá transmitir primeiro. Este tempo é calculado a partir de um fator que depende do número de vezes consecutivas de geração do *backoff* multiplicado por um número aleatório. Quando o meio está livre, o nó transmissor decrementa o tempo de *backoff*. Se o meio está ocupado o tempo de *backoff* permanece inalterado. Quando o *backoff* chegar a zero, o nó transmite o pacote. As colisões entre os pacotes são minimizadas, uma vez que a probabilidade de dois nós selecionarem o mesmo tempo de *backoff* é pequena. A razão pela qual a detecção de colisão não pode ser utilizada nas transmissões do IEEE 802.11 é que quando um nó está transmitindo, não pode ouvir qualquer outro nó que esteja transmitindo, já que seu próprio sinal “sufocaria” qualquer outro que estivesse chegando ao nó.

A estação receptora confere o CRC (*check redundancy cyclic*) do pacote recebido e transmite um pacote de reconhecimento (ACK), acusando o recebimento correto do pacote, o que indica que não ocorreu nenhuma colisão. Se o aviso de recebimento não chegar, até um tempo determinado, a estação de origem retransmite o pacote. Após sete tentativas (de acordo com o padrão) de retransmitir o pacote, este será descartado.

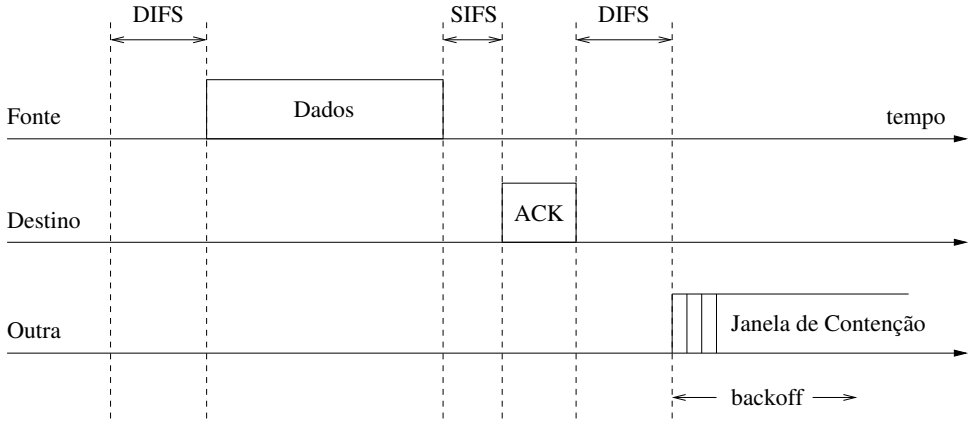


Figura 4.1: Mecanismo de acesso básico do DCF.

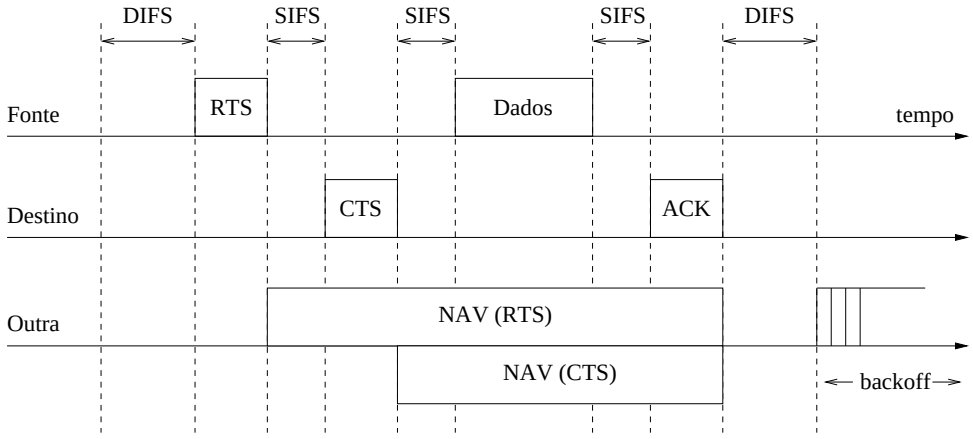


Figura 4.2: Mecanismo de acesso opcional do DCF usando RTS/CTS.

O problema do terminal escondido é um problema clássico de redes sem fio *ad hoc*, onde os nós podem causar interferência na transmissão dos dados. A Figura 4.3 ilustra um cenário onde pode ocorrer este problema. As estações **A** e **C** estão fora do raio de alcance mútuo e alcançam apenas a estação **B**, enquanto que **B** alcança **A** e **C**. Considere que **A** comece a transmitir para **B**. Em seguida, **C** também começa a transmitir para **B**, tendo em vista que **C** não é capaz de perceber que **B** já está recebendo informações de **A**.

Neste caso, haverá colisão em **B** e apenas esta estação perceberá. As estações **A** e **C** só perceberam o problema após a expiração do tempo de espera pelo reconhecimento (ACK) de **B**.

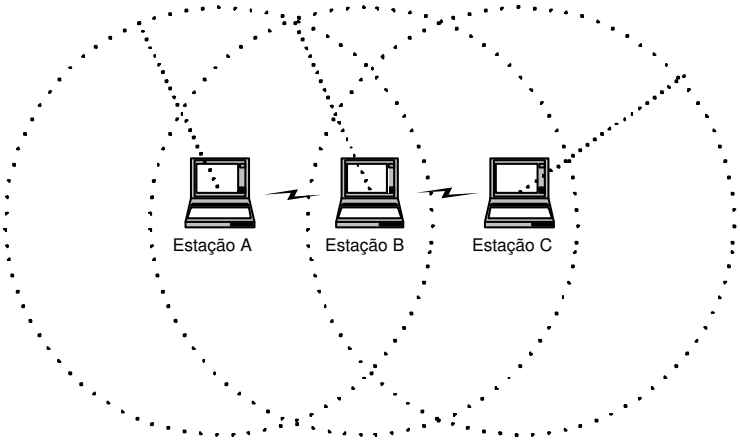


Figura 4.3: O problema do terminal escondido.

Para evitar o problema do terminal escondido, o padrão define um mecanismo opcional que envolve a troca de pacotes de controle RTS (*Request to Send*) / CTS (*Clear to Send*) antes da transmissão dos pacotes de dados. Desta maneira, as estações devem enviar, antes de cada transmissão de pacote de dados, um quadro chamado RTS, que inclui a fonte, o destino e a estimativa da duração da transmissão do pacote de dados. A estação receptora responde, caso o meio esteja livre, com um quadro CTS, que inclui as mesmas informações de duração. Após receber o quadro CTS, o transmissor envia o pacote de dados. O quadro RTS possui duas funções: reservar o meio para transmissão do pacote de dados e verificar se a estação de destino está pronta para recebê-lo.

Todas as estações que receberem o pacote RTS e/ou o CTS devem atualizar o valor do seu vetor de alocação de rede NAV (*Network Allocation Vector*), com a duração da transmissão (Figura 4.2), e adiar suas tentativas de transmissões para depois de passado o intervalo de tempo reservado. Este mecanismo reduz a probabilidade de colisões na recepção porque a estação ouve o CTS e reserva o meio até o final da transmissão, garantindo que as colisões só ocorram entre quadros de RTS, que são menores e não transportam dados.

Além do problema de terminais escondidos, as estações enfrentam o problema de terminal exposto. Um nó é considerado exposto quando está no raio de alcance do transmissor, mas está fora do raio de alcance de interferência do receptor. O problema do nó exposto resulta na sub-utilização da banda disponível, causando sérios problemas em redes sem-fio com múltiplos saltos.

O padrão IEEE 802.11 original permite a transmissão de dados a 1 e 2 Mbps na banda de 2,4GHz. Em seguida foi normalizada uma extensão conhecida como IEEE 802.11b [29]. Nesta norma é permitido a transmissão de dados em taxas de 5,5 Mbps e 11 Mbps. Também é prevista a existência de mecanismos para a mudança dinâmica de taxa de transmissão. No entanto, o cabeçalho de cada quadro deve ser transmitido a 1Mbps para manter a compatibilidade de todos os produtos. Assim, as taxas de transmissão foram categorizadas como taxas básicas (1 e 2 Mbps) e taxas de dados (5,5 e 11 Mbps). Um detalhe importante a ser ressaltado é o fato de que todos os quadros de controle (RTS, CTS e ACK), bem como os quadros transmitidos em difusão (*broadcast*) ou difusão seletiva (*multicast*) devem ser enviados em uma das taxas básicas da estação base, no caso de redes infra-estruturadas, ou a 1 Mbps no caso de redes *ad hoc*.

Posteriormente, foi definido o padrão IEEE 802.11a [30] que utiliza a faixa de freqüências de 5 GHz e a taxa de transmissão pode alcançar 54 Mbps. No entanto, este padrão é incompatível com os anteriores, tornando-o pouco utilizado.

Recentemente foi definido um novo padrão, o IEEE 802.11g, que também possui uma taxa de transmissão de 54 Mbps, mas usa a faixa de freqüências de 2,4 GHz, mantendo a compatibilidade com o padrão IEEE 802.11b.

4.2 Ambiente de simulação

O ambiente de simulação utilizado é composto do ns-2 (*Network Simulator*) [31], um simulador dirigido a eventos discretos para a modelagem de serviços e de protocolos de rede, e da ferramenta *ScenGen* para desenvolver os modelos de mobilidade. O ns-2 encontra-se em desenvolvimento dentro do projeto *Virtual InterNet Testbed* (VINT),

uma colaboração entre a Universidade da Califórnia em Berkeley, o *Lawrence Berkeley National Laboratory* (LBNL), o *Information Sciences Institute* (ISI) da Universidade da Califórnia do Sul (USC) e o laboratório Xerox PARC. O ns-2 utiliza as linguagens C++ e OTcl (*Object Tool Command Language*), sendo o seu núcleo implementado em C++, para permitir um melhor desempenho. As simulações executadas são configuradas através de *scripts* OTcl, que descrevem a topologia, o cenário de mobilidade, os protocolos e as aplicações a serem simuladas.

Os nós móveis consistem de componentes de rede, tais como *Link Layer* (LL), *Interface Queue* (IFQ), interface de rede, camada MAC, conectados ao canal nos quais os nós transmitem e recebem sinais. No início de uma simulação em redes sem fio, é necessário que se defina cada um destes componentes de rede dentre outros parâmetros, como tipo de antena, modelo de propagação de rádio, etc.

A estrutura de um nó da rede no ns-2 é composta de agentes, um ponto de entrada no nó, um classificador de endereços e um classificador de portas. Os agentes são entidades produtoras ou consumidoras de pacotes e implementam determinados tipos de protocolos. Um pacote gerado por um agente é entregue ao nó ao qual o agente está conectado, através do ponto de entrada, que também recebe pacotes cujo destino é o próprio nó. Após passar pelo ponto de entrada, o pacote é recebido pelo classificador de endereços, que verifica se o pacote deve ser entregue a um agente pertencente ao nó ou deve ser transmitido para um enlace de saída. Caso o pacote seja destinado a um agente do próprio nó, o pacote é então repassado ao classificador de porta que, de acordo com o endereço de destino, entrega o pacote ao respectivo agente.

O ns-2 possui módulos para simular as camadas física e de enlace do padrão IEEE 802.11. O modelo da camada física utilizado leva em consideração a interferência devido à reflexão do sinal (*TwoRayGround*). Na subcamada de controle de acesso ao meio (MAC) foi utilizado um módulo que implementa o mecanismo de controle de acesso distribuído (DCF) segundo as especificações da norma.

O modelo do protocolo de roteamento recebe todos os pacotes de dados que serão transmitidos ou encaminhados e solicita, quando necessário, atividades de roteamento. O tamanho da fila de interface (IFQ - *Interface Queue*) da subcamada MAC com a subca-

mada de enlace lógico (*Logic Link Control* - LLC) foi configurada para armazenar até 50 pacotes. Este parâmetro é importante, como será visto mais adiante, porque o descarte de pacotes pela subcamada MAC, devido ao transbordo da fila IFQ, é um dos motivos de perdas de pacotes que pode influir ,significativamente no desempenho dos protocolos. Esta fila prioriza os pacotes de roteamento, inserindo-os no início da fila.

O ns-2 também disponibiliza implementações de alguns dos principais protocolos de roteamento para redes *ad hoc* propostos na literatura. Dentre os protocolos disponíveis, escolheu-se utilizar o DSR, o DSDV e o AODV para análise neste trabalho. O AODV e o DSR foram escolhidos por serem os protocolos mais estudados na literatura técnica e, por conseqüência, possuirem uma boa documentação. Além disso, o DSR e o AODV possuem uma implementação para o ns-2 mais estável e confiável, e já foram testados em diversos trabalhos [3,8]. O DSDV é um protocolo proativo e foi incluído para ilustrar a diferença de comportamento entre protocolos por demanda e protocolos proativos.

Uma decisão importante a ser tomada em relação à configuração dos cenários de simulação é o padrão de mobilidade a ser utilizado. O pacote do simulador ns-2 disponibiliza o gerador de cenários *setdest*, que gera padrões de movimento utilizando o modelo de mobilidade *Random Waypoint*. Ferramentas adicionais, como o ScenGen e o *BonnMotion*, geram cenários de mobilidade compatíveis com o ns-2. Todas essas ferramentas, quando executadas, geram um arquivo de *trace* contendo cada movimento feito pelos nós. Este arquivo é a entrada utilizada pelo ns-2 para simular a movimentação dos nós, e pode ser visualizado graficamente antes da simulação ser realizada por meio da ferramenta *Ad-Hockey*, como já mencionado. Esta ferramenta é bastante útil, tendo em vista que a movimentação desejada pode ser extensivamente analisada antes mesmo de realizar-se a simulação.

4.3 Métricas de Desempenho

Como a proposta deste trabalho é avaliar os protocolos de roteamento utilizando um cenário de uma aplicação real, as variações dos parâmetros precisam obedecer às restrições impostas por este cenário. De forma geral, os principais parâmetros selecionados

como variáveis independentes nas simulações são o alcance dos transmissores, o tráfego e a quantidade de nós que consegue alcançar o destino. As variações dos parâmetros têm a finalidade de propiciar a avaliação do desempenho dos protocolos quando impostos a condições críticas ou buscar os melhores parâmetros para este tipo de rede. As métricas utilizadas para comparar o desempenho dos protocolos são as seguintes:

- **taxa de entrega de pacotes** - razão entre o número de pacotes entregues para o destino final e o número de pacotes gerados pela aplicação na fonte;
- **atraso médio fim a fim dos pacotes de dados** - inclui todos os possíveis atrasos causados pela latência da descoberta de rotas, propagação, atrasos devido a retransmissões da camada MAC e tempos de transferência;
- **número de pacotes de roteamento** - são medidos a quantidade total de pacotes de roteamento, representada pelos pacotes de descoberta e manutenção das rotas enviados pela origem ou encaminhados pelos nós intermediários. Nos protocolos por demanda (AODV e DSR) estes pacotes são representados pelos pacotes RREQ, RREP e RERR. No DSDV são representados pelas tabelas de roteamento que são trocadas periodicamente;
- **número de *bytes* de roteamento** - são medidos a quantidade total de *bytes* em cada pacote de roteamento, incluindo a quantidade de *bytes* de cabeçalho em pacotes de dados, que corresponde, normalmente, ao roteamento na fonte;
- **sobrecarga de roteamento normalizada pelo número de pacotes** - razão entre a quantidade de pacotes de roteamento transmitidos na rede durante a simulação e a quantidade de pacotes de dados recebidos; e
- **sobrecarga de roteamento normalizada pelo número de *bytes*** - razão entre a quantidade de *bytes* de roteamento transmitidos na rede durante a simulação e a quantidade de *bytes* recebidos.

A taxa de entrega é uma medida essencial para a aplicação e permite avaliar o funcionamento correto e completo do protocolo. A sobrecarga de roteamento é importante, pois determina a escalabilidade do protocolo. O tráfego referente ao roteamento deve

ser o menor possível quando comparado ao tráfego de dados, pois para se enviar pacotes de roteamento gasta-se energia dos nós e consome-se banda, que são recursos escassos em redes sem fio. Contabiliza-se a sobrecarga de roteamento, também por meio do número de *bytes*, para que se possa avaliar o impacto causado pelo roteamento por fonte do DSR. Para as redes militares, a taxa de entrega e o atraso são as métricas mais importantes, mas vale ressaltar que estas métricas não são completamente independentes. Por exemplo, uma taxa de entrega mais baixa significa que a métrica de atraso foi calculada com um número menor de amostras; se a sobrecarga de roteamento se torna muito alta, pode-se congestionar a rede causando atrasos relevantes, e se as rotas são mais longas, a probabilidade de descartar pacotes é maior [4].

4.4 Padrão de Movimentação

Com a proposta de avaliar o impacto da mobilidade no funcionamento dos protocolos de roteamento para redes *ad hoc*, foi desenvolvido neste trabalho um padrão de movimentação que busca se aproximar das características de um cenário militar real. Por meio desse padrão evita-se mudanças bruscas de direção, permitindo-se que os movimentos sejam feitos na mesma direção com velocidades distribuídas uniformemente e com intervalos de pausa no movimento também distribuídos uniformemente. Desta forma, tenta-se retratar com uma maior aproximação o movimento real dos usuários no cenário proposto.

Como mencionado anteriormente, para a especificação do padrão de mobilidade deste cenário foi usado o gerador de cenários *ScenGen*.

Foram considerados dois tipos de movimento para este cenário: o movimento individual dos membros de cada grupo relativo ao centro do grupo e o movimento do grupo como um todo, aplicando-se o modelo de movimentação ao centro do grupo. Foram utilizados como base os modelos *Random Waypoint* [15] e *Mixed Waypoint*, respectivamente, para modelar os dois movimentos citados acima.

O resumo dos parâmetros que foram utilizados nas simulações é apresentado na Tabela 4.1. Os nós móveis que formam os grupos movem-se com uma velocidade que segue

uma distribuição uniforme entre o intervalo de 0 a 2m/s e um tempo de pausa distribuído uniformemente entre o intervalo de 0 a 5 segundos. O nó que está operando no veículo move-se com velocidade média de 3m/s. Os grupos se movimentam com velocidade média de 2m/s em direção a um determinado objetivo militar (Figura 3.6). Para a área total da simulação utilizou-se um campo retangular de 2000 x 1000m com a seguinte distribuição dos nós: 8 grupos formados por 4 nós cada grupo, 1 grupo formado por 2 nós que representam os observadores-avançados e um nó montado em um veículo representando a central de comando. A área de simulação ocupada por cada grupo é de 150 x 150m, de modo que todos os nós que participam do mesmo grupo são mutuamente alcançáveis. O raio de alcance eficaz do transmissor de cada nó é configurado inicialmente em 250 metros. O tempo de simulação é de 500 segundos, que é o tempo médio que os grupos levariam para alcançar o objetivo neste cenário.

Velocidade do veículo (nó do comando)	3m/s
Velocidade dos nós	0 a 2m/s
Tempo de pausa	0 a 5s
Tempo de simulação	500s
Número total de nós	35
Número de grupos de combate	8 (4 nós cada)
Número de observadores	2
Número de veículos	1
Área total da simulação	2000x1000m
Área individual dos grupos	150x150m
Área individual dos observadores	80x80m
Área individual do comando	50x50m
Tamanho dos pacotes	512*bytes*
Taxa dos pacotes	4pac/s
Tipo de tráfego	*Constant Bit Rate*
Número de conexões	20

Tabela 4.1: Resumo dos parâmetros utilizados nas simulações.

Cada ponto dos gráficos mostrados neste trabalho é o valor médio de 30 rodadas de simulação com cada um dos protocolos, utilizando cenários variados. As variações dos cenários obedeceram às restrições impostas pelo objetivo da aplicação, e são conduzidas da seguinte forma: inicialmente, na área de simulação são criadas 8 sub-áreas com dimensões de 150m x 150m para serem ocupadas por cada grupo de combate, uma sub-área com dimensões de 50m x 50m para o nó que representa o comando e uma sub-área de dimensões de 80m x 80m para os observadores-avançados. Os nós que formam cada um destes grupos são distribuídos aleatoriamente dentro da sub-área correspondente ao seu grupo. Os nós se movimentam em uma determinada direção, com velocidades aleatoriamente distribuídas dentro de um intervalo, sendo que estas velocidades variam no decorrer da simulação. Os destinos destes nós são pontos escolhidos aleatoriamente dentro de uma sub-área da área de simulação. Com isto, conseguimos gerar cenários com uma suficiente abrangência.

4.5 Padrão de Tráfego

O ns-2 disponibiliza o gerador de tráfego *cbrgen*, que cria conexões aleatórias de tráfego TCP (*Transport Control Protocol*) ou CBR (*Constant Bit Rate*) entre dois nós móveis. Entretanto, como as conexões no cenário que está sendo estudado obedecem a um padrão de tráfego com fortes características hierárquicas, foi implementado um novo gerador de tráfego, de forma a cumprir as exigências impostas por este padrão.

O gerador de tráfego implementado seleciona aleatoriamente um nó-líder entre os participantes de cada grupo, que representa o comandante do grupo de combate. Cada um destes nós-líderes é o responsável pela comunicação de seu grupo com a central de comando. Para estas simulações, o tráfego foi gerado por 10 fontes do tipo CBR (*Constant Bit Rate*), posicionadas na central de comando, uma fonte em cada um dos nós-líderes e nos nós que representam os observadores-avançados, totalizando 20 fontes CBR gerando pacotes com tamanho de 512 *bytes* cada. Todas as conexões são iniciadas em tempos aleatórios, uniformemente distribuídos no intervalo de 0 a 180 segundos, evitando-se, assim, que todas as fontes comecem a transmitir simultaneamente.

Para obter uma comparação justa entre os protocolos, preferiu-se utilizar um tráfego a taxa constante (CBR), ao invés de se empregar o TCP, uma vez que o TCP possui um mecanismo de controle de congestionamento, o que acarretaria em condições de desigualdade para a avaliação destes protocolos. Além disso, os pacotes de reconhecimento (ACK) do TCP disputam o canal, podendo causar colisões e degradar o desempenho.

No capítulo seguinte serão apresentados os resultados obtidos a partir das simulações realizadas.

Capítulo 5

Análise dos Resultados

NESTA seção serão apresentadas todas as simulações realizadas neste trabalho com seus respectivos resultados. As simulações foram conduzidas com a finalidade de avaliar o comportamento dos protocolos de roteamento para redes *ad hoc* em um cenário que representa uma operação militar, buscando as condições que melhor se adéqüem a este cenário ou a outros que apresentem características similares.

Conforme descrito na seção 2.1, as simulações realizadas neste trabalho utilizam a implementação do protocolo AODV que elimina o mecanismo padrão de mensagens *HELLO*, utilizando, para a manutenção de rotas, somente as informações da camada de enlace do 802.11. Um aviso é enviado para a camada de roteamento quando a camada MAC falha ao enviar um pacote *unicast* para o próximo salto. Esta indicação pode acontecer, por exemplo, pelo não recebimento de um quadro CTS depois de ser enviado um quadro RTS, ou a ausência de um ACK após a transmissão de um pacote de dados.

Nas simulações são levadas em consideração somente as comunicações entre os grupos, não se considerando as comunicações entre os membros de cada grupo, uma vez que estes são alcançáveis entre si.

Para que os algoritmos possam ser submetidos ao maior conjunto de situações possíveis, foram utilizados diferentes modelos de simulações. O intuito desse conjunto de variações é testar a eficiência dos protocolos nas mais diversas situações, típicas no contexto da aplicação militar que estamos analisando. De uma forma geral, os parâmetros

variados ao longo das simulações são o alcance da comunicação, a quantidade de grupos da rede, a taxa de transmissão dos dados e a taxa de envio de pacotes. O que se está observando nas análises é o atraso, a taxa de entrega de pacotes, a quantidade de pacotes de roteamento gerados por período do tempo de simulação, a quantidade de *bytes* de roteamento gerados por períodos do tempo de simulação e a sobrecarga de roteamento medida em pacotes e em *bytes*. Além disso, são também identificadas as causas que levam à perda de pacotes.

Para todas as medidas, foram calculados intervalos de confiança de 95% relativos à média das amostras, representadas como barras de erro verticais nos gráficos. Na maioria dos gráficos mostrados neste trabalho foram apresentados apenas os valores médios, a fim de tornar mais clara a visualização dos resultados comparativos. Os intervalos de confiança calculados, em cada instante, apresentam valores relativos muito pequenos, quando comparados ao valor médio da métrica considerada.

As simulações 01, 02, 03 e 04 buscam obter o melhor dimensionamento da rede para este cenário, ressaltando a influência provocada nos resultados pela escolha de diferentes parâmetros. As simulações 05 e 06 pretendem avaliar esta rede em condições de crise:

- Simulação 01: a situação em que todos os grupos alcançam os seus objetivos com sucesso, utilizando capacidade da rede de 2Mbps;
- Simulação 02: a situação em que todos os grupos alcançam os seus objetivos com sucesso, utilizando capacidade da rede de 11Mbps;
- Simulação 03: a situação em que todos os grupos alcançam os seus objetivos com sucesso, utilizando capacidade da rede de 11Mbps, variando o alcance dos transmissores;
- Simulação 04: a situação em que todos os grupos alcançam os seus objetivos com sucesso, utilizando capacidade da rede de 11Mbps, incluindo um novo grupo neste cenário;
- Simulação 05: buscando avaliar o impacto nas métricas apresentadas, simulamos a situação em que um dos grupos deste pelotão não consegue completar a missão,

deixando de cooperar na comunicação de forma repentina, a partir de um determinado tempo de simulação. Nosso objetivo é avaliar a capacidade dos protocolos se recuperarem de forma satisfatória em situações de particionamento inesperado da rede; e

- Simulação 06: conduzimos simulações variando as condições de tráfego na rede, de forma a retratar uma situação de crise.

As seções a seguir são organizadas de acordo com a variação de objetivos que motivaram aquele determinado conjunto de experimentos.

5.1 Simulação 01 - utilizando taxa de transmissão de dados de 2Mbps

Ao dimensionarmos a rede para ser usada neste cenário, testou-se, inicialmente, a taxa de transmissão de dados de 2Mbps, uma vez que se trata de um cenário com poucos nós (35 nós), movimentando-se com baixa velocidade e com carga de tráfego baixa (4pac/s), taxa esta utilizada em vários trabalhos anteriores [3, 4, 8].

Largura de banda	2Mbps
Alcance de transmissão	250m
Tempo de simulação	500s
Número de nós	35
Tempo de pausa(max)	5s
Tamanho dos pacotes	512*bytes*
Taxa dos pacotes	4pac/s
Área de simulação	2000x1000m
Tipo de tráfego	*Constant Bit Rate*
Número de conexões	20

Tabela 5.1: Valores dos parâmetros da simulação 01.

Os parâmetros utilizados para esta simulação são os apresentados na Tabela 5.1 e o resumo dos resultados obtidos nas simulações, para cada protocolo, é apresentado na Tabela 5.2. A Tabela 5.3 apresenta um resumo dos principais motivos de descarte de pacotes de dados observados nos protocolos analisados.

MÉTRICAS AVALIADAS	**DSDV**	**AODV**	**DSR**
Taxa de Entrega	77,34%	77,80%	85,87%
Atraso médio (s)	0,4160	1,0610	1,0005
Sobrecarga de Pacotes	0,101	1,189	0,167
Sobrecarga de *Bytes*	0,131	0,217	0,167

Tabela 5.2: Resultados das simulações com taxa de transmissão de dados de 2Mbps.

Motivo dos Descartes	**DSDV**	**AODV**	**DSR**
Quebra de Enlace	2865 (35%)	3225 (41%)	-
Fila de Roteamento	1812 (22%)	330 (4%)	-
Fila IFQ	3067 (38%)	3628 (46%)	4084 (84%)
Falta de Rota	-	590 (7%)	571 (12%)
Outros (arp,ttl,etc)	303 (5%)	110 (2%)	183 (4%)
Descarte Total	**8047 (100%)**	**7883 (100%)**	**4838 (100%)**

Tabela 5.3: Principais motivos de descartes de pacotes de dados.

O AODV e o DSDV apresentam taxa de entrega de pacotes similares e 41% e 35%, respectivamente dos descartes apresentados ocorreram por queda no enlace. Analisando-se os arquivos de saída das simulações realizadas com o protocolo AODV, observa-se que a maioria dos descartes que foram reportados como quebra de enlace pela camada MAC são, na realidade, motivados pela dificuldade de um nó alcançar o nó vizinho, em decorrência das diversas colisões ocorridas com os pacotes RTS, devido ao congestionamento do meio de transmissão. Após sete tentativas sem sucesso de receber o CTS, o nó que está tentando reservar o meio entende que ocorreu um evento de falha de rota, e informa à sua camada superior que houve uma quebra no enlace. Em redes sem fio CS (*carrier*

sense) o alcance de interferência do transmissor é maior que o alcance em que os receptores estão aptos a receber um pacote oriundo desta transmissão. Por esta razão podem ocorrer colisões entre nós que não podem se comunicar diretamente, mas estão no alcance de interferência um do outro [32]. O principal motivo da dificuldade de capturar o meio para a transmissão dos pacotes de dados ocorre em decorrência desse cenário restringir a concentração do tráfego em direção a um único destino, uma vez que só é possível o envio de pacotes dos nós líderes para o nó de comando ou vice-versa. Esta característica é típica de redes que apresentam configuração hierárquica.

O DSR entrega, em média, 10% mais pacotes que os outros dois protocolos, e praticamente não apresenta descarte por quebra de enlace, pois utiliza a política de "salvar pacotes", que significa que um nó, ao encontrar o próximo salto da sua rota pela fonte inalcançável, busca em seu *cache* uma rota alternativa para este destino, evitando, assim, que o pacote seja descartado. O DSR também apresenta inúmeras colisões dos pacotes RTS e, com isto, tem dificuldade de capturar o meio para enviar pacotes de dados. Diferentemente do AODV, ao invés de descartar o pacote por quebra de enlace, faz novas tentativas por meio de outras rotas. Como o DSR utiliza roteamento na fonte e escuta promíscua, aprende muito mais rotas que o AODV. A aprendizagem do AODV limita-se ao conhecimento da fonte quando encaminha os pacotes.

Os pacotes de dados e os pacotes de roteamento que são enviados pela camada de roteamento são enfileirados na fila de interface (IFQ) até que a camada MAC possa transmitílos. A fila de interface é FIFO (*First-in-First-out*), e esta fila está configurada com a capacidade de armazenamento máxima de 50 pacotes. Uma vez que, no cenário apresentado, os líderes de cada grupo só recebem pacotes do nó que representa a central de comando, em determinados momentos as filas de interface relativas a este nó tendem a ficar congestionadas com pacotes aguardando para serem enviados, ultrapassando a quantidade máxima de pacotes permitida para armazenamento. Com isto, observa-se uma grande quantidade de pacotes de dados descartados neste nó. Este é o principal motivo para o descarte de pacotes de dados nos três protocolos, sendo que, no DSR, representa 84% dos descartes medidos. Como o DSR possui um melhor conhecimento da rede por meio de suas rotas alternativas, consegue acumular mais pacotes enfileirados na fila de interface.

A medida de atraso de entrega de pacotes foi significativamente menor para o DSDV e foi similar para o AODV e DSR. Isto se deve ao fato dos protocolos com modo de operação proativo, como o DSDV, possuirem rotas para todos os destinos armazenados em tabelas, enquanto que o AODV e o DSR operam por demanda, somente buscando as rotas no instante que necessitam enviar um pacote para um destino com rota desconhecida.

Embora o DSR e o AODV possuam mecanismos de construir rotas por demanda muito similares, a sobrecarga de roteamento exigida por ambos apresenta-se bem distinta. Analisando os resultados obtidos, verifica-se que o AODV gera, em média, seis vezes mais pacotes de roteamento do que o DSR por causa da inundação da rede com pacotes de descoberta de rotas (RREQ). O AODV interpreta como quebra de enlace quando o nó não consegue reservar o meio para enviar pacotes de dados, devido ao congestionamento na rede. Com isto, propaga a falsa informação de rota inválida através de pacotes de RERR, estimulando que se inicie processos de descoberta de rotas desnecessariamente, aumentado o número de pacotes de roteamento que trafegam nesta rede. O AODV inicia uma média de 1350 descobertas de rotas em 500 segundos de simulação, o que resulta na transmissão em média de 22.000 pacotes de RREQ.

O DSR limita a propagação de pacotes RREQ na rede por meio de sua política de aprendizado de rotas, que inclui escuta promíscua, armazenamento de rotas dos pacotes que são encaminhados pelo nó e o procedimento de questionar primeiramente os nós vizinhos para obter uma rota desejada. A inundação da rede só acontece com o não recebimento de uma resposta destes vizinhos. Em um único ciclo de busca de rota, o DSR responde a todos os questionamentos que alcança o destino, portanto a fonte aprende várias rotas alternativas para o mesmo destino, o que é útil quando ocorre falha na conexão. Com isto tudo, o DSR envia em média 830 pacotes de *Route Request* em 500 segundos de simulação, sendo que 230 destes pacotes são não propagáveis, isto é, obteve-se as rotas questionando apenas os vizinhos e cerca de metade dos pacotes de roteamento que circulam na rede são pacotes RREP, uma vez que o DSR responde a todas as requisições de rota que alcançam o destino, diferentemente do AODV, que responde apenas à primeira requisição de rota recebida.

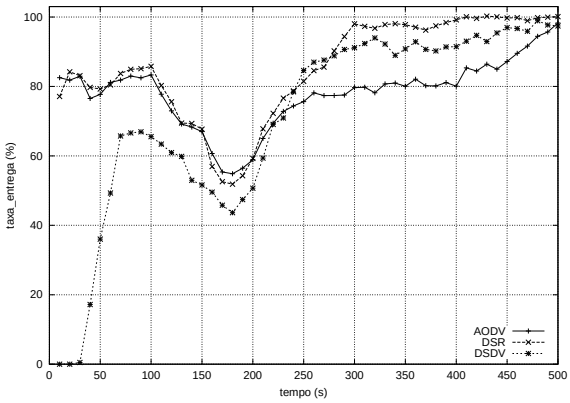
Embora o DSDV exija trocas periódicas de tabelas de roteamento, com a finalidade de manter suas tabelas atualizadas, esse protocolo apresenta o melhor resultado com relação ao número de pacotes de roteamento gerados, uma vez que não utiliza pacotes de requisição de rotas, que são específicos dos protocolos que operam por demanda. Como as rotas neste cenário são relativamente curtas, o roteamento na fonte utilizado pelo DSR não causa grandes impactos na medida realizada em *bytes* da sobrecarga de roteamento, em relação aos outros dois protocolos.

Como mencionado anteriormente, este trabalho busca enfocar o estudo do comportamento dos protocolos em um cenário correspondente a um campo de batalha, onde o movimento dos nós apresenta uma aleatoriedade controlada. Por isto, ao longo deste trabalho, os resultados das diferentes métricas para cada protocolo são apresentados dinamicamente, no decorrer do tempo de simulação, por meio de gráficos, uma vez que o padrão de mobilidade desenvolvido para este cenário apresenta características diferentes ao longo do tempo.

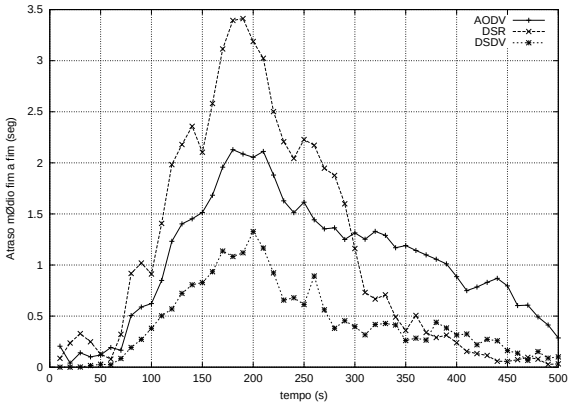
A taxa média de entrega de pacotes para os diferentes protocolos é mostrada na Figura 5.1(a). Aos 34 segundos, observa-se que a taxa de entrega decresce suavemente no caso dos protocolos DSR e AODV. Esta queda é decorrente do início da transmissão de pacotes para um grupo que encontra-se neste momento particionado do restante da rede, como pode ser observado na Figura 3.6, ocorrendo, então, o descarte destes pacotes.

O DSDV demora cerca de 35 segundos até que esteja pronto para enviar o primeiro pacote de dados, uma vez que opera de forma proativa, montando suas tabelas de entradas, independentemente da necessidade de utilização de uma rota. Isto faz com que este protocolo apresente um alto índice de descarte nos primeiros segundos de simulação, devido aos pacotes que são enviados e perdidos antes que as rotas tenham sido estabelecidas. Estes descartes ocorrem porque se ultrapassa a quantidade máxima de 5 pacotes que podem aguardar na camada de roteamento por uma rota para serem encaminhados.

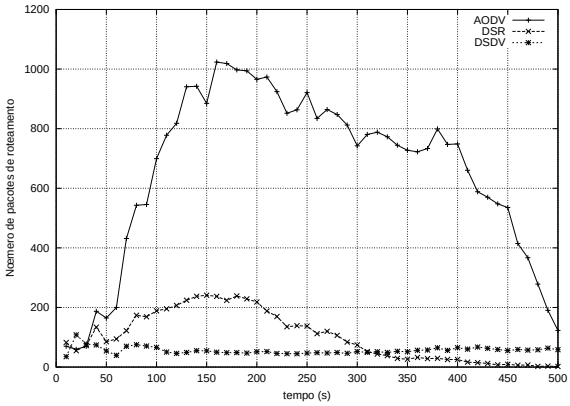
Como pode ser observado nos gráficos da Figura 5.1, a simulação apresenta condições críticas durante o intervalo de 100 a 180 segundos. Nota-se que, neste período, ocorre um efeito de “afunilamento”, uma vez que todas as fontes associadas ao nó de comando já iniciaram a geração de pacotes para os nós líderes da rede. Estes pacotes ficam enfileirados



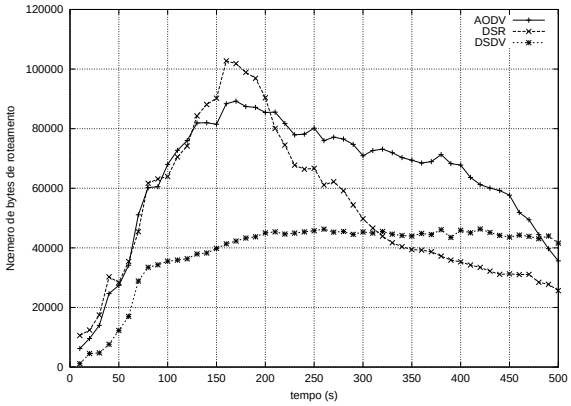
(a) Taxa de Entrega dos Pacotes



(b) Média de Atraso dos Pacotes



(c) Número de Pacotes de Roteamento



(d) Número de *Bytes* de Roteamento

Figura 5.1: Simulação 01 - Comparação dos protocolos para as diferentes métricas usando largura de banda de 2Mbps.

na fila de interface (IFQ) aguardando o meio estar livre para que possam ser enviados pela camada MAC. Isto resulta em atrasos maiores, neste intervalo, para o envio dos pacotes (Figura 5.1(b)) e aumento da sobrecarga de roteamento (Figura 5.1(c) e Figura 5.1(d)) para manter rotas para todos os destinos (no caso dos protocolos por demanda). Neste momento, observa-se uma acentuada queda na taxa de entrega para os três protocolos (Figura 5.1(a)), devido ao congestionamento na fila de interface associada ao nó de comando, motivada pela dificuldade de capturar o meio para enviar estes pacotes, sendo que o DSR, que até então estava se mostrando ligeiramente melhor que o AODV, atinge valores mais baixos.

A partir de 250 segundos de simulação, os nós deste cenário tendem a ficar mais próximos uns dos outros, eliminando, assim, o problema de partições ocasionais na rede. Com isto, as rotas ficam mais estáveis, uma vez que todos os grupos partem de pontos diferentes, mas com o propósito de alcançar o mesmo destino. A taxa de entrega tende a atingir 100%, sendo que o DSR é o primeiro a se aproximar deste valor.

O DSDV apresenta o pior desempenho quando as condições da rede são críticas, mas recupera-se rapidamente quando estas condições se mostram mais amenas. Quando as rotas sofrem menos alterações, o DSDV se prevalece de sua propriedade de manter rotas em tabelas e se mostra superior ao AODV, que para manter suas rotas exige uma alta sobrecarga na rede com pacotes de roteamento, como já foi mostrado anteriormente.

A Figura 5.1(b) mostra a métrica de atraso médio de pacotes para os três protocolos. O DSDV apresenta o menor atraso, pois suas rotas estão armazenadas em tabelas de roteamento, fazendo com que a latência seja mínima. No início da simulação, o atraso é zero porque todos os seus pacotes foram descartados. O DSR apresenta o maior atraso quando as condições da rede são críticas, decrescendo acentuadamente quando estas condições melhoram. Em condições críticas as rotas alternativas presentes no *cache* do DSR desatualizam-se mais rapidamente, resultando em perda de tempo com a utilização destas rotas. O uso de rotas alternativas não é eficaz quando ocorrem muitas quebras de enlace. Observa-se que os três protocolos apresentam um atraso maior no trecho crítico da rede. Isso ocorre porque as filas de interface ficam muito cheias.

A quantidade de pacotes de roteamento apresentado na Figura 5.1(c) mostra que o DSDV não reage às diferentes condições da rede, uma vez que os seus intervalos de atualizações de rotas permanecem inalterados. O AODV gera a maior quantidade de pacotes de roteamento, devido às constantes inundações da rede em busca de rotas para diferentes destinos. O DSR limita a quantidade de busca de rotas devido ao seu processo de aprendizado de rotas. A quantidade de *bytes* de roteamento apresentada na Figura 5.1(d) mostra-se aproximadamente constante para o DSDV, devido às trocas periódicas das tabelas de roteamento. O roteamento na fonte usado pelo DSR faz com que ele apresente uma quantidade de *bytes* de roteamento elevada. Os principais responsáveis pelos *bytes* de roteamento apresentados pelo AODV são os pacotes de controle decorrentes das inun-

dações da rede, uma vez que o AODV não se utiliza do roteamento pela fonte e os seus pacotes de dados carregam somente o endereço de destino e o próximo salto para alcançar o destino desejado.

Com o objetivo de obter uma comparação justa entre os protocolos executou-se uma simulação com o DSDV, modificando o tráfego CBR para que as fontes só começassem a enviar pacotes de dados após o protocolo montar sua tabela de roteamento (a partir de 35 segundos). A partir dessa alteração, observa-se que o protocolo passa a apresentar um nível de descarte inferior em 15%.

5.2 Simulação 02 - utilizando taxa de transmissão de dados de 11Mbps

Com o objetivo de alcançar um melhor resultado para as métricas apresentadas neste trabalho, tentamos solucionar os problemas que foram apresentados na simulação anterior. Para isto, repetimos as simulações fazendo diversas alterações nos parâmetros e condições deste cenário, como inserção de um outro nó na central de comando, de forma a dividir a concentração do tráfego, aumento do tamanho de fila de interface, alteração do intervalo das atualizações periódicas do DSDV e aumento do tamanho da fila de roteamento. Os resultados destas simulações foram suprimidos deste trabalho por não apresentarem melhoras significativas. Os melhores resultados obtidos ocorreram quando aumentamos a largura de banda para 11Mbps. Os parâmetros utilizados para esta simulação são apresentados na Tabela 5.4 e o resumo dos resultados obtidos nas simulações, para cada protocolo, é apresentado na Tabela 5.5.

Como pode ser observado na Tabela 5.5, como a rede não está mais congestionada, todos os protocolos aumentam sua taxa de entrega de pacotes. Porém, o AODV apresenta um índice de melhora significativo nos seus resultados, apresentando valores de taxa média de entrega de pacotes equivalentes ao DSR. Os protocolos reativos (AODV e DSR) entregam, em média, 11% mais pacotes que o protocolo proativo DSDV. Praticamente

Largura de banda	11Mbps
Alcance de transmissão	250m
Tempo de simulação	500s
Número de nós	35
Tempo de pausa(max)	5s
Tamanho dos pacotes	512*bytes*
Taxa dos pacotes	4pac/s
Área de simulação	2000x1000m
Tipo de tráfego	*Constant Bit Rate*
Número de conexões	20

Tabela 5.4: Valores dos parâmetros da simulação 02.

não ocorrem mais descartes ocasionados pelo transbordo das filas de interface. Observa-se, por meio da Tabela 5.6, que os poucos descartes que ainda ocorrem nesta rede são motivados por falta momentânea de rotas para alguns destinos, ocasionada pelos particionamentos ocasionais desta rede, uma vez que a movimentação em grupo restringe os movimentos dos nós, facilitando, assim, este tipo de ocorrência. O DSDV, entretanto, apresenta dificuldades em encontrar rotas e ainda apresenta muitos descartes por quebra de enlace.

MÉTRICAS AVALIADAS	**DSDV**	**AODV**	**DSR**
Taxa de Entrega	86,05%	96,35%	96,60%
Atraso médio (s)	0,0308	0,0379	0,0567
Sobrecarga de Pacotes	0,084	0,094	0,053
Sobrecarga de *Bytes*	0,136	0,123	0,125

Tabela 5.5: Resultados das simulações empregando taxa de transmissão de dados de 11Mbps.

Os três protocolos apresentam atrasos muito menores para entregar pacotes, uma vez que foi reduzida a latência representada pelas retransmissões da camada MAC, a descoberta de rotas e o tempo de transferência dos pacotes. O DSR apresenta métrica de atraso

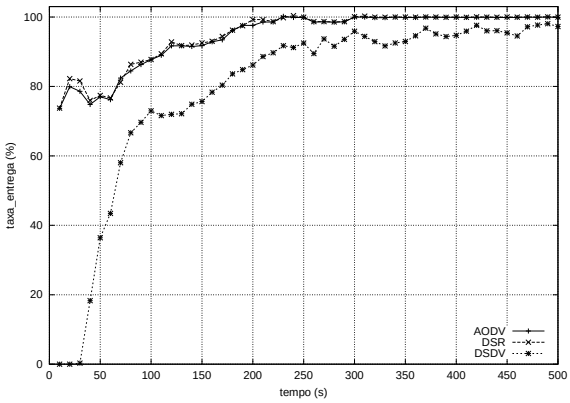
Motivo dos Descartes	DSDV	AODV	DSR
Quebra de Enlace	2135 (44%)	67 (7%)	-
Fila de Roteamento	2432 (51%)	338 (33%)	-
Fila IFQ	136 (3%)	-	133 (16%)
Falta de rota	-	575 (57%)	564 (67%)
Outros (arp,ttl,etc)	91 (2%)	30 (3%)	141 (17%)
Descarte Total	**4794 (100%)**	**1010 (100%)**	**838 (100%)**

Tabela 5.6: Principais motivos dos descartes com taxa de transmissão de 11Mbps.

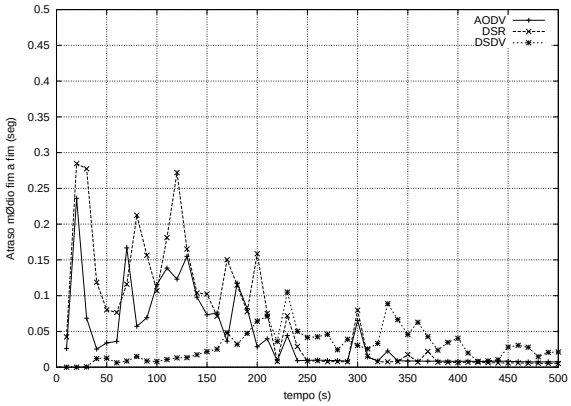
médio maior que os outros protocolos devido às inúmeras tentativas que este protocolo faz de enviar o pacote por rotas alternativas incorrendo, às vezes, em aumento no tempo de entrega. Conseqüentemente, inicia menos processos de descobertas de rotas, apresentando a menor sobrecarga de roteamento. Observamos para o AODV uma drástica melhora em relação à quantidade de pacotes de roteamento que trafegam na rede. O aumento da capacidade da rede minimiza a dificuldade de conseguir a reserva do meio para transmissão dos pacotes de dados e, conseqüentemente, reduz as colisões observadas nos pacotes RTS, restringindo, assim, o número de inundações da rede, resultante das repetidas descobertas de rotas iniciadas. Mesmo assim, o AODV foi o protocolo que apresentou a maior medida de sobrecarga de roteamento.

Podemos verificar, por meio da Figura 5.2, que até 200 segundos de simulação, esta rede apresenta condições críticas. Todas as conexões se iniciam durante o intervalo de 0 a 180 segundos, gerando, com isto, um tráfego bastante intenso, principalmente com os protocolos por demanda que começam a buscar rotas para prover estas conexões. Percebemos, com isto, que neste período ocorrem muitos descartes e os atrasos são significativamente maiores.

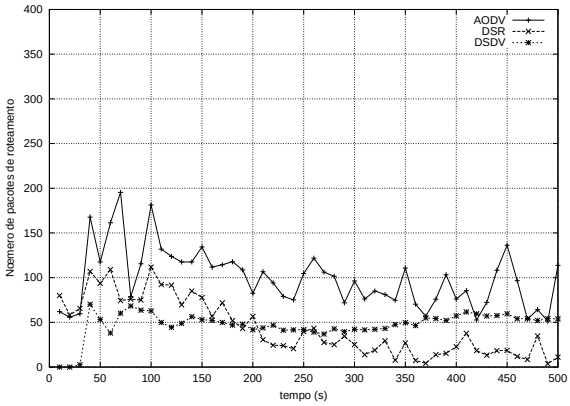
Uma observação interessante é que o DSR, durante o intervalo crítico da rede, apresenta atrasos e *bytes* de roteamento superiores aos outros protocolos, sendo o DSDV o que apresenta o menor atraso. A partir de 200 segundos de simulação, esta situação se inverte. O DSR diminui consideravelmente sua atividade de roteamento, apresentando um desempenho melhor que o DSDV e o AODV até o final da simulação. Observa-se,



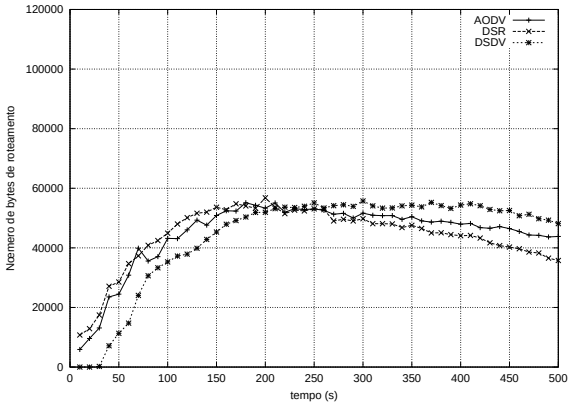
(a) Taxa de Entrega dos Pacotes



(b) Média de Atraso dos Pacotes



(c) Número de Pacotes de Roteamento



(d) Número de *Bytes* de Roteamento

Figura 5.2: Simulação 02 - Comparação dos protocolos para as diferentes métricas usando largura de banda de 11Mbps.

neste período, que pelas próprias características dos cenários, as rotas se apresentam mais estáveis, e conseqüentemente as condições da rede se mostram mais amenas. Portanto, os protocolos sob demanda, que já estão com suas rotas estabelecidas, apresentam atrasos próximos de zero, e suas taxas de entrega atingem 100%, sendo que o DSDV não consegue alcançar este valor. O AODV sofre a maior sobrecarga na rede com pacotes de roteamento, durante todo o tempo de simulação.

Estes resultados concordam com comparações de trabalhos anteriores [3, 4, 8], onde o DSR apresenta um desempenho melhor que o AODV quando as condições da rede

são mais amenas (a partir de 200 segundos), e se mostra pior quando as condições se apresentam críticas (de 0 a 200 segundos).

As próximas simulações que serão apresentadas, até o fim do nosso trabalho, empregam uma taxa de transmissão de dados de 11Mbps.

5.3 Simulação 03 - variando o alcance máximo dos transmissores

Na tentativa de solucionar os problemas decorrentes dos diversos particionamentos na rede que ainda se apresentavam, repetimos a simulação anterior variando o alcance dos transmissores e, com isto, tentamos obter um resultado mais próximo à eficácia exigida para este tipo de aplicação. Ressaltamos, também, o impacto que o alcance dos transmissores causa nas diferentes métricas observadas. Foram realizadas simulações usando o alcance dos transmissores de 250, 300, 350, 400, 450 e 500 metros. Os resultados estão apresentados na Figura 5.3.

Largura de banda	11Mbps
Alcance de transmissão	250,300,350,400,450,500m
Tempo de simulação	500s
Número de nós	35
Tempo de pausa(max)	5s
Tamanho dos pacotes	512*bytes*
Taxa dos pacotes	4pac/s
Área de simulação	2000x1000m
Tipo de tráfego	*Constant Bit Rate*
Número de conexões	20

Tabela 5.7: Valores dos parâmetros da simulação 03.

Os parâmetros utilizados para esta simulação são apresentados na Tabela 5.7 e o resumo dos resultados obtidos nas simulações, para cada protocolo, é apresentado nas Ta-

belas 5.8, 5.9 e 5.10.

MÉTRICAS AVALIADAS	300m	350m	400m	450m	500m
Taxa de Entrega	99,36%	99,88%	99,94%	99,95%	99,88%
Atraso Médio (s)	0,015	0,011	0,007	0,008	0,010
Sobrecarga de Pacotes	0,042	0,027	0,023	0,029	0,027
Sobrecarga de *Bytes*	0,106	0,102	0,093	0,082	0,071

Tabela 5.8: Resultados das simulações variando o alcance dos transmissores usando o AODV.

MÉTRICAS AVALIADAS	300m	350m	400m	450m	500m
Taxa de Entrega	99,47%	99,94%	99,99%	99,99%	99,99%
Atraso Médio (s)	0,023	0,013	0,004	0,004	0,003
Sobrecarga de Pacotes	0,020	0,011	0,009	0,008	0,008
Sobrecarga de *Bytes*	0,103	0,096	0,085	0,072	0,063

Tabela 5.9: Resultados das simulações variando o alcance dos transmissores usando o DSR.

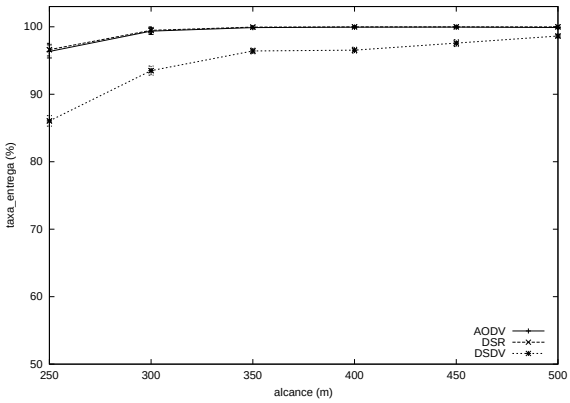
MÉTRICAS AVALIADAS	300m	350m	400m	450m	500m
Taxa de Entrega	93,50%	96,41%	96,53%	97,58%	98,62%
Atraso Médio (s)	0,012	0,007	0,008	0,008	0,004
Sobrecarga de Pacotes	0,077	0,071	0,069	0,065	0,059
Sobrecarga de *Bytes*	0,124	0,116	0,107	0,096	0,088

Tabela 5.10: Resultados das simulações variando o alcance dos transmissores usando o DSDV.

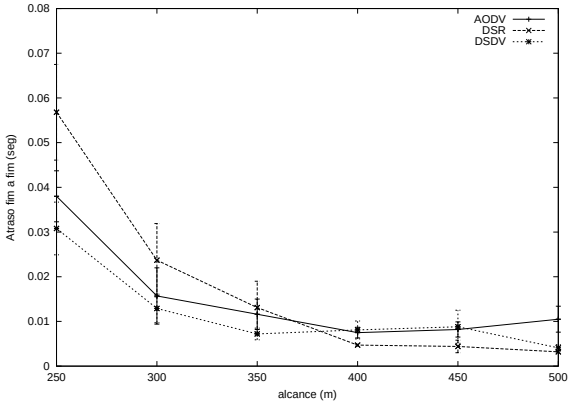
As curvas da Figura 5.3(a) apresentam um comportamento previsível, pois podemos verificar que a taxa de entrega de pacotes cresce com o aumento do alcance dos transmissores, sendo que os protocolos por demanda (AODV e DSR) estabilizam seus valores a partir do alcance de 300 metros. No caso do DSDV, a taxa sofre um aumento significativo no intervalo de 250 a 350 metros, porém atinge valores máximos inferiores aos

outros protocolos. Há uma clara diminuição no número de pacotes de dados perdidos com aumento do alcance.

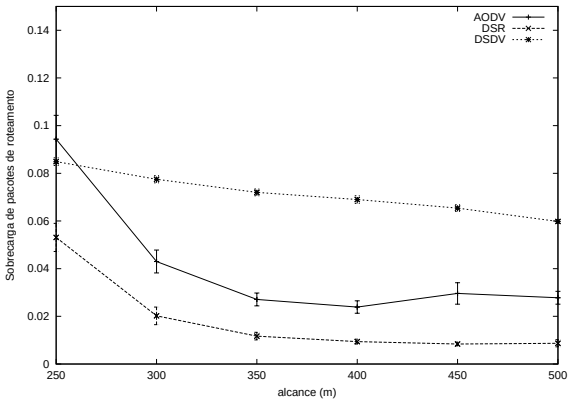
No gráfico da Figura 5.3(b) percebemos que, com alcances de 250 a 300 metros, o DSR apresenta um atraso bem maior que o AODV para entregar a mesma quantidade de pacotes de dados. Estas diferenças de atrasos vão diminuindo e, a partir de 400 metros, o DSR começa a apresentar atrasos menores que o AODV.



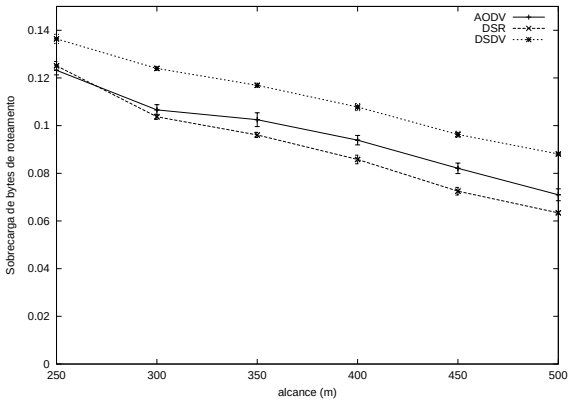
(a) Taxa de Entrega dos Pacotes



(b) Média de Atraso dos Pacotes



(c) Número de Pacotes de Roteamento



(d) Número de *Bytes* de Roteamento

Figura 5.3: Simulação 03 - Comparação dos protocolos para as diferentes métricas variando o alcance dos transmissores.

Os gráficos das Figuras 5.3(b) e 5.3(c) apresentam um conjunto de observações muito interessantes. O atraso e a sobrecarga de roteamento em pacotes, que vinham diminuindo

com o aumento do alcance, começam a sofrer acréscimos com alcances a partir de 450 metros, usando o protocolo AODV. A explicação para este fato é que o número médio de saltos das rotas diminui sensivelmente com o aumento do alcance dos nós. No gráfico apresentado na Figura 5.4, observa-se que, quando se tem um alcance de 250 metros, o tamanho médio das rotas do AODV é de 3 saltos. O número médio de saltos diminui gradualmente com o aumento do alcance, até atingir um valor médio inferior a 2 saltos com alcance de 500 metros. Ao se aumentar o alcance, os nós que estão mais distantes começam a entrar na área de alcance do transmissor, dispensando de suas novas rotas os nós intermediários. Com a mobilidade, esses nós saem facilmente da área de alcance, invalidando estas rotas e obrigando o AODV a iniciar novas descobertas de rotas, uma vez que, diferentemente do DSR, o AODV não possui outros caminhos alternativos para o mesmo destino. Com isto, o AODV apresenta um maior atraso dos pacotes e um aumento da quantidade de pacotes de roteamento que trafegam na rede com alcances a partir de 450 metros, como pode ser verificado na Tabela 5.11. Este problema também afeta o DSDV, que apresenta maiores atrasos neste intervalo. O DSR consegue contornar o problema utilizando suas rotas alternativas.

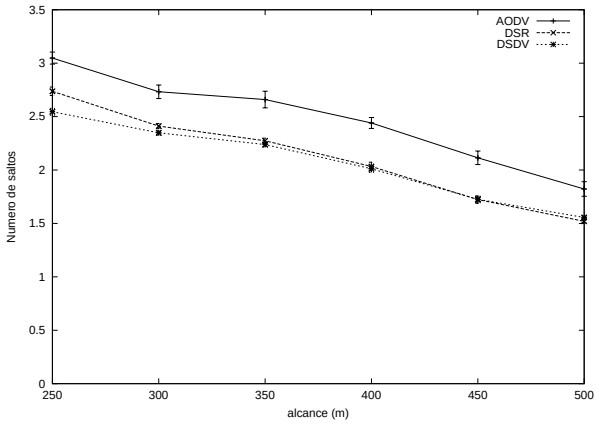


Figura 5.4: Comparação dos protocolos com a métrica número de saltos.

AODV	250m	300m	350m	400m	450m	500m
Descoberta de Rotas	2782	1284	831	758	940	911

Tabela 5.11: Número de pacotes RREQ que foram enviados ou encaminhados no AODV.

O número de pacotes de roteamento gerados pelos protocolos que operam por demanda diminui consideravelmente com o aumento do alcance dos transmissores, até o alcance de 400 metros, como mostra Figura 5.3(c), sendo que o DSDV sofre leves alterações com a variação do alcance, uma vez que não altera suas atividades de roteamento com as alterações sofridas pela rede.

A quantidade de *bytes* de roteamento diminui com o aumento do alcance dos transmissores (Figura 5.3(d)) e o DSR, embora utilize roteamento na fonte, é o protocolo que melhor se apresenta em relação a esta métrica, uma vez que compensa o problema com o seu resultado de baixas atividades de roteamento.

Analisando os resultados obtidos, podemos concluir que, com o alcance de 300 metros, conseguimos uma melhora significativa nas métricas avaliadas, atenuando o problema dos diversos particionamentos na rede e quebras de enlace, causados pelo próprio comportamento da movimentação em grupo dos nós móveis.

Alcances maiores que este não são aconselháveis, por não acarretarem em aumentos significativos nos resultados que justifiquem a possibilidade de comprometer a segurança da operação.

5.4 Simulação 04 - incluindo um grupo no cenário

Uma outra possível solução para o problema de partições freqüentes nesta rede é a inclusão de um novo grupo de combate neste cenário. Baseado nas simulações anteriores, observa-se que oito grupos inicialmente dispostos ao longo de uma área com as dimensões apresentadas não se mostram suficientes para garantir a conectividade contínua desta rede, quando utilizamos o alcance dos transmissores de 250 metros.

Os parâmetros utilizados para esta simulação são apresentados na Tabela 5.12 e o resumo dos resultados obtidos nas simulações, para cada protocolo, é apresentado na Tabela 5.13. Observa-se, pela Tabela 5.13, que com a inserção de um novo grupo, todos os protocolos entregam mais pacotes e apresentam um atraso menor. Porém, o DSDV continua descartando bem mais que o AODV e o DSR, uma vez que a maior parte dos descartes

apresentados por este protocolo é motivada pelas quedas de enlace provocadas pelo movimento dos nós. A inclusão de um novo grupo resolve, principalmente, o problema da falta de conectividade, criando um novo caminho para alguns grupos da rede.

Largura de banda	11Mbps
Alcance de transmissão	250m
Tempo de simulação	500s
Número de nós	39
Tempo de pausa(max)	5s
Tamanho dos pacotes	512*bytes*
Taxa dos pacotes	4pac/s
Área de simulação	2000x1000m
Tipo de tráfego	*Constant Bit Rate*
Número de conexões	20

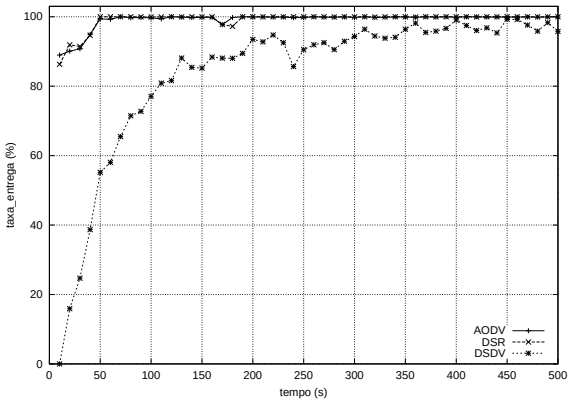
Tabela 5.12: Valores dos parâmetros da simulação 04.

MÉTRICAS AVALIADAS	**DSDV**	**AODV**	**DSR**
Taxa de Entrega	89,58%	99,70%	99,79%
Atraso Médio (s)	0,0263	0,0138	0,0183
Sobrecarga de Pacotes	0,101	0,071	0,032
Sobrecarga de *Bytes*	0,142	0,116	0,116

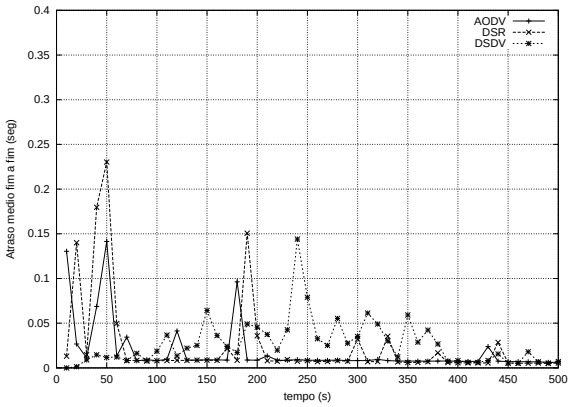
Tabela 5.13: Resultados com a inclusão de um novo grupo no cenário proposto.

Os protocolos sob demanda apresentam a sobrecarga em pacotes e em *bytes* menores, com o aumento do número de nós. A inclusão de mais nós na rede apresenta o custo de aumentar a sobrecarga de roteamento que é gerada quando ocorrem as inundações, mas, por outro lado, há uma menor necessidade de se iniciar processos de descoberta de rotas. O DSDV sofre a influência do acréscimo de nós, apresentando um aumento de 23% nos pacotes de roteamento e, conseqüentemente, um aumento nos *bytes* de roteamento. Os gráficos da Figura 5.5 apresentam as métricas no decorrer do tempo de simulação. A Figura 5.5(a) mostra que os protocolos por demanda demoram cerca de 50 segundos para

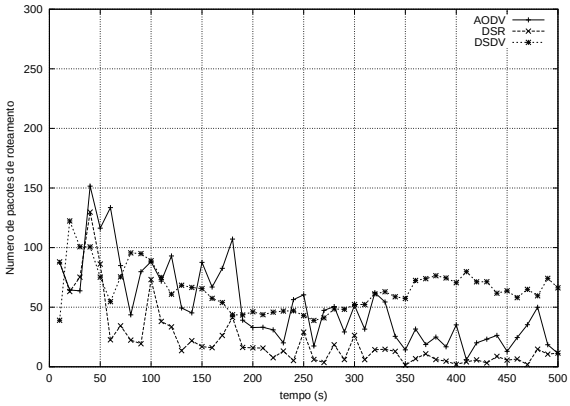
atingir taxas próximas de 100%, estabilizando-se neste valor. Pode-se notar que, para os protocolos AODV e DSR, o número de pacotes de dados perdidos diminui significativamente com o aumento do número de grupos. A razão para isto é o aumento de alternativas de rotas até o destino, que são fundamentais no re-roteamento de pacotes a partir dos nós intermediários. O DSDV demora cerca de 200 segundos para alcançar suas maiores taxas.



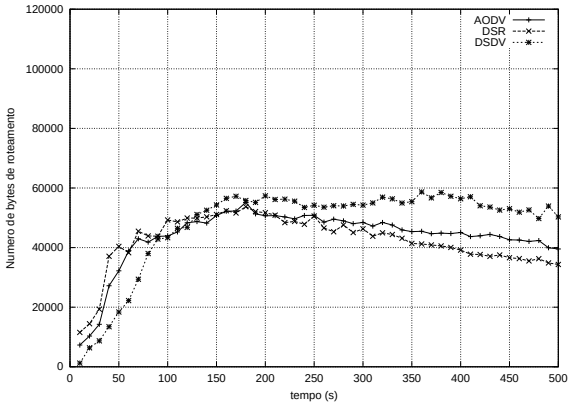
(a) Taxa de Entrega dos Pacotes



(b) Média de Atraso dos Pacotes



(c) Número de Pacotes de Roteamento

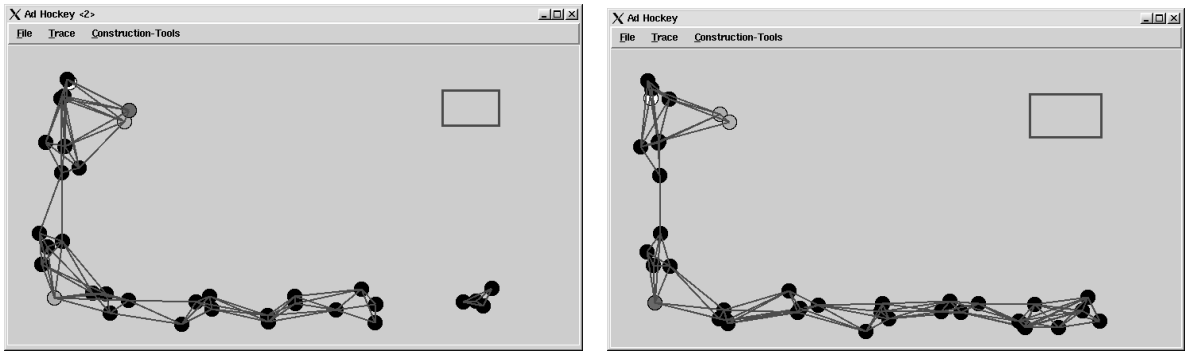


(d) Número de *Bytes* de Roteamento

Figura 5.5: Simulação 04 - Comparação dos protocolos para as diferentes métricas usando largura de banda de 11Mbps, incluindo um grupo.

Considera-se que a inclusão de um grupo nesta rede é favorável, e que os protocolos por demanda melhoram consideravelmente o seu desempenho, uma vez que solucionam os problemas de partições na rede apresentados na simulação 02. Portanto, a quantidade mínima necessária de grupos para que não ocorram partições nesta rede é de nove grupos,

cobrindo as extremidades da área, como mostra a Figura 5.6(b).



(a) Cenário militar utilizando 8 grupos de combate (b) Cenário militar utilizando 9 grupos de combate

Figura 5.6: Comparação entre os cenários utilizando diferentes números de grupos de combate.

5.5 Simulação 05 - excluindo um grupo no decorrer da simulação

Tratando-se de um cenário militar, é perfeitamente possível que, por motivos diversos, ocorra a exclusão de um ou mais grupos no decorrer da operação. Por isto, julgamos necessário conduzir simulações nestas condições, para avaliar o impacto causado nesta rede quando um grupo pára de cooperar na comunicação de forma repentina. Nosso objetivo é avaliar a capacidade dos protocolos se recuperarem de forma satisfatória em situações de particionamento inesperado da rede. Os parâmetros utilizados para esta simulação são apresentados na Tabela 5.14 e o resumo dos resultados obtidos nas simulações, para cada protocolo, é apresentado na Tabela 5.15.

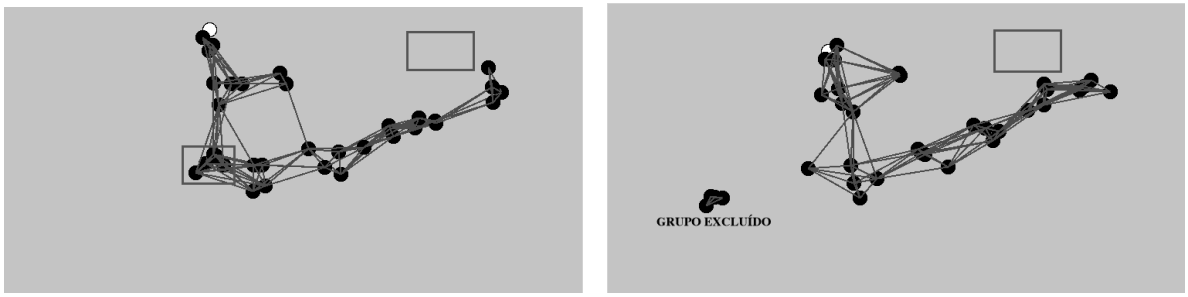
Para simular a exclusão de um grupo nesta rede, interrompe-se, a partir de um determinado instante, a movimentação deste grupo e a transmissão de pacotes pela fonte CBR associada ao seu líder.

Largura de banda	11Mbps
Alcance de transmissão	250m
Tempo de simulação	500s
Número de nós	35 e 31
Tempo de pausa(max)	5s
Tamanho dos pacotes	512*bytes*
Taxa dos pacotes	4pac/s
Área de simulação	2000x1000m
Tipo de tráfego	*Constant Bit Rate*
Número de conexões	20

Tabela 5.14: Valores dos parâmetros da simulação 05.

	DSDV		**AODV**		**DSR**	
MÉTRICAS AVALIADAS	**Sim 2**	**Sim 5**	**Sim 2**	**Sim 5**	**Sim 2**	**Sim 5**
Taxa de Entrega	86,05%	66,80%	96,35%	78,67%	96,60%	78,96%
Atraso Médio (s)	0,0308	0,0384	0,0379	0,0709	0,0567	0,1330
Sobrecarga de Pacotes	0,084	0,101	0,094	0,354	0,053	0,179
Sobrecarga de *Bytes*	0,136	0,150	0,123	0,148	0,125	0,152

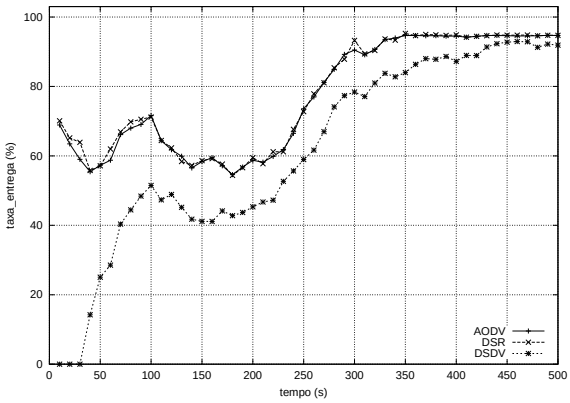
Tabela 5.15: Impacto da exclusão de um grupo.



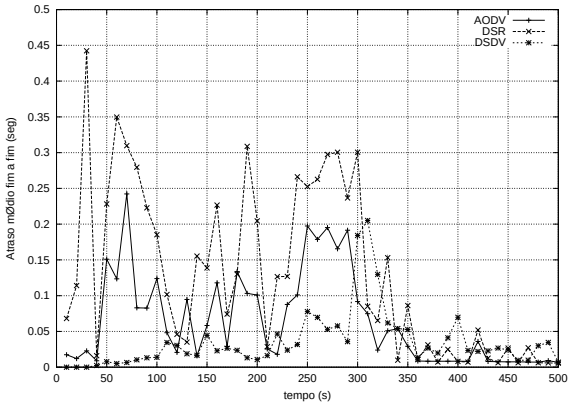
(a) Cenário militar utilizando 8 grupos de combate

(b) Cenário militar com exclusão de um grupo de combate

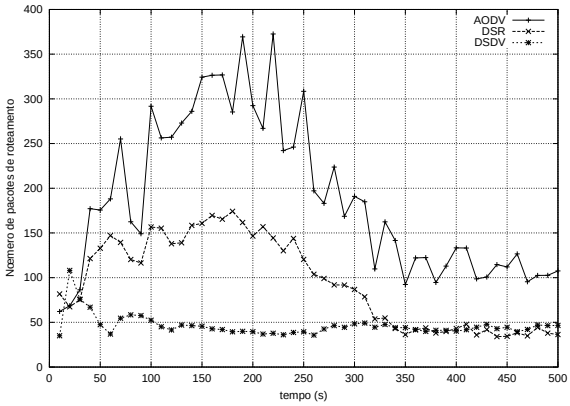
Figura 5.7: Comparação entre os cenários utilizados na Simulação 02 e Simulação 05.



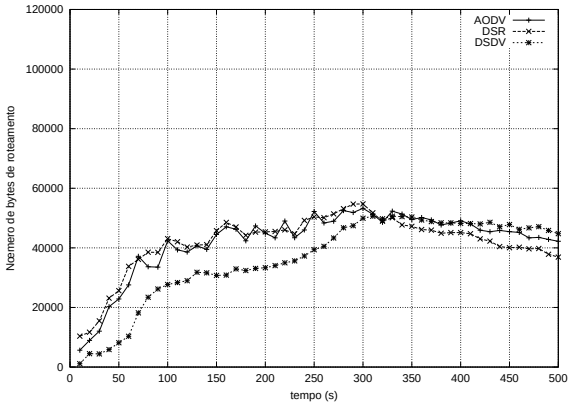
(a) Taxa de Entrega dos Pacotes



(b) Média de Atraso dos Pacotes



(c) Número de Pacotes de Roteamento



(d) Número de *Bytes* de Roteamento

Figura 5.8: Simulação 05 - Comparação dos protocolos para as diferentes métricas usando largura de banda de 11Mbps, excluindo um grupo.

Observa-se que há uma queda, em média, de 25% na taxa de entrega para os protocolos sob demanda e 30% para os protocolos proativos, relativa aos freqüentes descartes decorrentes da falta de rota para alguns destinos, ocasionadas pela saída de um grupo desta rede. O AODV e o DSR geram três vezes mais pacotes de roteamento do que na simulação 02, devido à necessidade de buscar novas rotas válidas para substituir as rotas que utilizam os nós que pertencem ao grupo excluído. O DSDV apresenta uma queda no número de pacotes e *bytes* de roteamento, motivados pela redução do número de nós que necessitam trocar tabelas de roteamento.

Como pode ser observado nos gráficos da Figura 5.8(a), a simulação apresenta condições críticas durante o intervalo de 100 a 180 segundos. Este período corresponde à eliminação de um grupo que compunha esta rede (Figura 5.7(b)), resultando, com isto, em medidas maiores de sobrecarga de roteamento (Figura 5.8(c) e 5.8(d)) e uma acentuada queda na taxa de entrega para os três protocolos (Figura 5.8(a)). Os protocolos por demanda demoram cerca de 60 segundos para se recuperar da quebra repentina de rota. Os protocolos só começam a se estabilizar a partir de 230 segundos, mas não conseguem atingir taxas equivalentes aos 100%, devido aos descartes dos pacotes que são destinados ao grupo excluído. O DSDV apresenta o pior desempenho quando as condições da rede são críticas, mas se recupera rapidamente quando estas condições melhoram, embora apresente resultados inferiores aos protocolos por demanda.

5.6 Simulação 06 - variando o tráfego

Como já citado anteriormente, a aplicação, que o cenário representa, está passível de sofrer alterações decorrentes de situações críticas apresentadas. Uma conseqüência desta crise é a necessidade dos nós trocarem mais mensagens, que pode ser representado com um aumento do número de fontes geradoras do tráfego ou com o aumento da taxa de envio dos pacotes. Com isto, conduzimos novas simulações, variando a taxa de envio de pacotes, com a finalidade de avaliar o impacto causado pelo aumento do tráfego para esta aplicação. As Tabelas 5.16, 5.17 e 5.18 mostram a variação das métricas para cada protocolo utilizando diferentes taxas de envio de pacotes.

	DSDV			
MÉTRICAS AVALIADAS	**4pac/s**	**6pac/s**	**8pac/s**	**10pac/s**
Taxa de Entrega	86,05%	83,17%	78,43%	74,77%
Atraso Médio (s)	0,030	0,075	0,143	0,250
Sobrecarga de Pacotes	0,084	0,057	0,046	0,040
Sobrecarga em *Bytes*	0,136	0,126	0,126	0,128

Tabela 5.16: Impacto da variação do tráfego nas métricas avaliadas utilizando o DSDV.

	AODV			
MÉTRICAS AVALIADAS	**4pac/s**	**6pac/s**	**8pac/s**	**10pac/s**
Taxa de Entrega	96,35%	95,83%	94,83%	85,82%
Atraso Médio (s)	0,037	0,036	0,046	0,265
Sobrecarga de Pacotes	0,094	0,086	0,137	0,280
Sobrecarga em *Bytes*	0,123	0,122	0,126	0,143

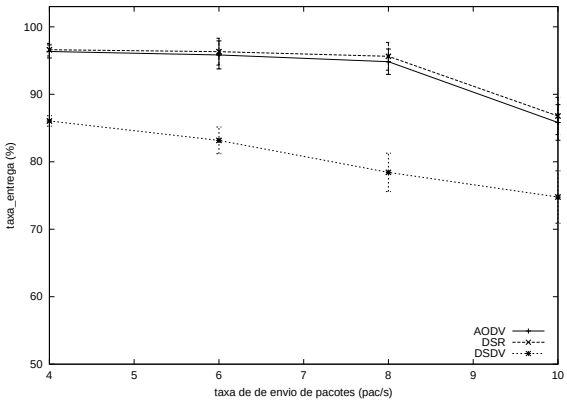
Tabela 5.17: Impacto da variação do tráfego nas métricas avaliadas utilizando o AODV.

	DSR			
MÉTRICAS AVALIADAS	**4pac/s**	**6pac/s**	**8pac/s**	**10pac/s**
Taxa de Entrega	96,60%	96,32%	95,63%	86,78%
Atraso Médio (s)	0,056	0,040	0,047	0,251
Sobrecarga de Pacotes	0,053	0,036	0,032	0,046
Sobrecarga em *Bytes*	0,125	0,119	0,118	0,134

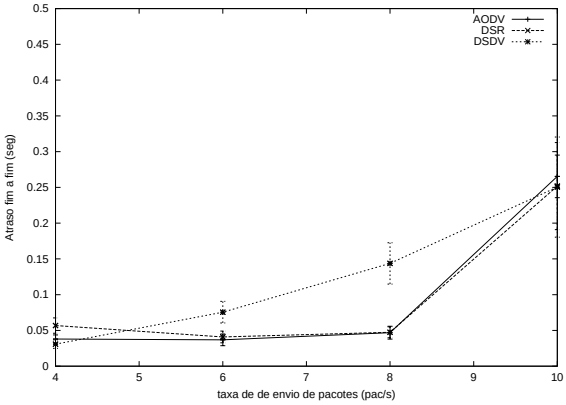
Tabela 5.18: Impacto da variação do tráfego nas métricas avaliadas utilizando o DSR.

Podemos observar, por meio da Figura 5.9(a), que os protocolos por demanda apresentam comportamentos similares, e conseguem manter seus índices de perda de pacotes com baixas variações até a taxa de 8 pac/s, sofrendo uma acentuada queda quando a taxa utilizada é de 10 pac/s. O DSDV perde mais pacotes à medida que as taxas de envio de pacotes aumentam, mostrando que é fortemente influenciado pelo aumento do tráfego. O que se percebe é que, com aumento da carga, as filas da subcamada MAC se enchem e são esvaziadas lentamente pela dificuldade de acesso ao meio, ocorrendo um elevada perda de pacotes por falta de *buffers*. O DSR e o AODV só começam a sofrer as conseqüências deste congestionamento na rede com a taxa de 10 pac/s, enquanto que o DSDV tem o seu desempenho influenciado progressivamente com o aumento da carga.

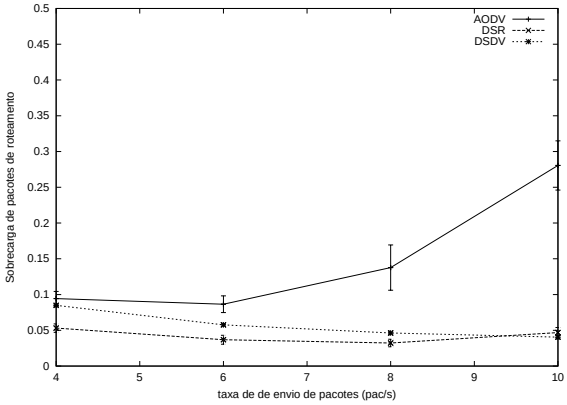
Nas curvas da Figura 5.9(b) verificamos que, com a taxa de 4pac/s, o DSDV apresenta menor atraso do que os outros protocolos. Com taxas superiores a esta, o atraso aumenta quase que linearmente com o aumento do tráfego, alcançando, em todos os casos, valores superiores aos outros protocolos. O AODV e o DSR apresentam poucas variações de atraso até 8 pac/s, sendo que o AODV apresenta atrasos menores que o DSR nas taxas



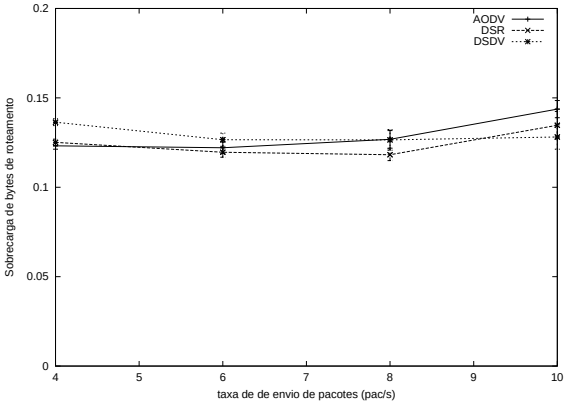
(a) Taxa de Entrega dos Pacotes



(b) Média de Atraso dos Pacotes



(c) Sobrecarga de Roteamento em Pacotes



(d) Sobrecarga de Roteamento em *Bytes*

Figura 5.9: Simulação 06 - Comparação dos protocolos para as diferentes métricas variando a taxa de envio de pacotes.

mais baixas. A partir daí os dois protocolos sofrem um aumento considerável na métrica de atraso de pacotes.

O AODV sofre um considerável acréscimo na sobrecarga de roteamento com o aumento do tráfego, como mostra a Figura 5.9(c). O atraso para acessar o meio faz com que a subcamada MAC interprete que ocorreu queda no enlace, avisando a camada superior. Com isto, são disparadas diversas descobertas de rotas desnecessárias, aumentando a sobrecarga de roteamento. Na Tabela 5.19 mostramos o número de pacotes RREQ's enviados pelo AODV durante o tempo de simulação, com diferentes taxas. O DSR apre-

senta este problema de forma mais suave, porque tenta acessar o meio por outro caminho alternativo, antes de iniciar novos procedimentos de descoberta de rotas. O DSDV não sofre alterações com o aumento do tráfego, uma vez que os seus intervalos de atualizações de rotas são constantes.

AODV	4pac/s	6pac/s	8pac/s	10pac/s
Descoberta de Rotas	2782	3648	7224	16031

Tabela 5.19: Número de pacotes RREQ que foram enviados ou encaminhados no AODV.

A sobrecarga de roteamento em *bytes* cresce (Figura 5.9(d)) quando são utilizadas taxas de 10pac/s, para o AODV e o DSR, motivado pelo aumento da quantidade de pacotes de roteamento.

5.7 Resumo dos principais resultados das simulações

As Tabelas 5.20, 5.21 e 5.22 apresentam o resumo dos experimentos realizados, a fim de alcançar uma melhor visualização dos resultados obtidos, apresentando o comportamento de cada protocolo em função dos parâmetros que compõem este cenário.

MÉTRICAS AVALIADAS	Sim 1	Sim 2	Sim 3	Sim 4	Sim 5
Taxa de Entrega	77,34%	86,05%	93,50%	89,58%	66,80%
Atraso Médio (s)	0,4160	0,0308	0,0129	0,0263	0,0384
Sobrecarga de Pacotes	0,101	0,084	0,077	0,101	0,101
Sobrecarga de *Bytes*	0,131	0,136	0,124	0,142	0,150

Tabela 5.20: Resumo do resultado dos experimentos usando o protocolo DSDV.

MÉTRICAS AVALIADAS	Sim 1	Sim 2	Sim 3	Sim 4	Sim 5
Taxa de Entrega	77,80%	96,35%	99,36%	99,70%	78,67%
Atraso Médio (s)	1,0610	0,0379	0,0157	0,0138	0,0709
Sobrecarga de Pacotes	1,189	0,094	0,042	0,071	0,354
Sobrecarga de *Bytes*	0,217	0,123	0,106	0,116	0,148

Tabela 5.21: Resumo do resultado dos experimentos usando o protocolo AODV.

MÉTRICAS AVALIADAS	Sim 1	Sim 2	Sim 3	Sim 4	Sim 5
Taxa de Entrega	85,87%	96,60%	99,47%	99,79%	78,96%
Atraso Médio (s)	1,005	0,0567	0,0236	0,0183	0,133
Sobrecarga de Pacotes	0,167	0,053	0,020	0,032	0,179
Sobrecarga de *Bytes*	0,167	0,125	0,103	0,116	0,152

Tabela 5.22: Resumo do resultado dos experimentos usando o protocolo DSR.

5.8 Resultados Complementares

Com o intuito de efetuar comparações, conduzimos um conjunto de simulações nas quais preservamos a área de operação, padrão de tráfego e os parâmetros (número de nós, velocidade, etc.) utilizados na simulação 02. Entretanto, desta vez, os nós foram distribuídos aleatoriamente na área de simulação e seus movimentos foram baseados exclusivamente no modelo *Random Waypoint*. Nosso objetivo é analisar o impacto causado no desempenho dos protocolos, caso os nós se movimentassem de modo completamente aleatório, ao invés de seguir os movimentos ditados pela missão militar. Verifica-se, na Tabela 5.23, uma queda acentuada no desempenho dos três protocolos, uma vez que a dimensão da área não garante uma densidade razoável para a rede em questão. Todos os nós movimentado-se em direção ao mesmo objetivo, como no cenário militar proposto, favorecem a conectividade desta rede.

Trabalhar com as interfaces em modo promíscuo, como o DSR, pode causar sérios problemas de segurança. Desta forma, todas as informações são compartilhadas, mesmo as que não estão sendo dirigidas para o nó. Assim, algum intruso pode facilmente ter

MÉTRICAS AVALIADAS	DSDV	AODV	DSR
Taxa de Entrega	53,42%	52,71%	53,87%
Atraso médio (s)	0,0444	0,2370	0,3203
Sobrecarga de Pacotes	0,145	0,748	0,455
Sobrecarga de *Bytes*	0,199	0,219	0,254

Tabela 5.23: Resultados das simulações usando o modelo *Random Waypoint*.

acesso a informações da rede que não estejam criptografadas. Com isto, realizamos diversas simulações alterando a implementação do DSR, de forma a não operar no modo promíscuo. Nosso objetivo é fazer comparações neste trabalho, com o DSR funcionando com e sem utilização de modo promíscuo. Verifica-se que o uso do modo promíscuo não promove melhoras significativas no desempenho da rede, vindo a confirmar resultados apresentados em [8]. Os resultados deste conjunto de simulações são apresentados na Tabela 5.24.

	8 grupos		excl. 1 grupo	
MÉTRICAS AVALIADAS	s/ e. prom.	c/ e. prom.	s/ e. prom.	c/ e. prom.
Taxa de Entrega	96,57%	96,60%	76,61%	77,91%
Atraso Médio (s)	0,0611	0,0567	0,215	0,146
Sobrecarga de Pacotes	0,061	0,053	0,206	0,186
Sobrecarga de *Bytes*	0,146	0,125	0,185	0,164

Tabela 5.24: DSR sem o uso do mecanismo de escuta promíscua.

5.9 Comentários

Baseados nas simulações que foram apresentadas neste capítulo, podemos observar que redes que apresentam a característica de concentrar o tráfego em determinadas rotas, como as redes militares, ao invés de distribuir o tráfego por toda a rede, tendem a sofrer congestionamentos. Com isto, apresentam problemas referentes à dificuldade de acessar o meio para enviar pacotes, ocorrendo uma grande quantidade de descartes devido ao trans-

bordamento nas filas de interface. Uma outra limitação apresentada por redes militares é o particionamento da rede decorrente da movimentação em grupo dos seus nós. Algumas soluções foram apresentadas com a finalidade de contornar os problemas apresentados, como a inclusão de um novo grupo de combate ou o aumento do alcance dos transmissores. Porém, convém ressaltar que o desempenho desta rede não cresce linearmente com o acréscimo de grupos ou com o aumento do alcance. As análises realizadas com valores de alcance e número de grupos superiores aos indicados já não acarretavam benefícios, devido ao custo do aumento das atividades de roteamento pela inclusão de mais nós nesta rede ou por mais nós estarem alcançáveis.

Capítulo 6

Conclusões e Trabalhos Futuros

AS operações militares são exemplos clássicos de aplicações de redes *ad hoc*. O objetivo principal deste trabalho é analisar o problema do roteamento, quando associados a cenários que retratam esses tipos de operações, onde os movimentos dos nós não são tratados de forma puramente aleatória. Para isto, foi projetado e simulado um cenário que busca retratar uma situação real de uma operação militar em um campo de batalha. As características deste cenário foram estabelecidas por meio do estudo em manuais operacionais e por intermédio de entrevistas com militares experimentados no assunto, de forma que sua representação se tornasse a mais fiel possível. Diferentemente das experimentações freqüentemente conduzidas para se avaliar a eficiência destes algoritmos utilizando simulações, o cenário proposto tem, como principais características, a mobilidade em grupo dos seus nós, que visam alcançar, de forma cooperativa, um determinado objetivo; o padrão de tráfego e a disposição física dos nós obedecem às exigências impostas pelo modelo hierárquico militar. Os protocolos de roteamento AODV, DSR e DSDV foram selecionados para análise.

É importante mencionar que modelos de simulação são amplamente empregados no processo de planejamento militar nas Forças Armadas mais desenvolvidas, inclusive no caso brasileiro. Esses modelos são tradicionalmente utilizados de duas maneiras principais: diretamente como ferramenta de análise para comparação da eficácia de alternativas táticas, possivelmente em um ambiente de meta-simulação em experimentos planejados; ou de modo conjunto com outras ferramentas de análise, compondo complexos sistemas

denominados Jogos de Guerra, onde se busca estudar possibilidades e opções estratégicas e testar planejamentos antes do início das missões.

Para o desenvolvimento do padrão de movimentação deste cenário, foi utilizada a ferramenta *Scengen*. Para melhor representar os movimentos reais dos nós, tornou-se necessário desenvolver e implementar um novo modelo, denominado *Mixed Waypoint*, que representa o movimento do grupo como um todo, utilizando-se o modelo tradicional *Random Waypoint* para os movimentos individuais dos nós que compõem o grupo. A nova modelagem proposta foi desenvolvida em C++ e incorporada ao conjunto de modelos de mobilidade disponíveis no *Scengen*. O gerador de tráfego também foi implementado de modo que as conexões dos nós sigam os padrões hierárquicos exigidos para esses tipos de operação. Desta forma, pôde-se obter resultados e medidas que caracterizam o desempenho dos protocolos selecionados de forma dinâmica, no decorrer do tempo da operação, tornando possível uma avaliação dos problemas apresentados por redes *ad hoc* em que os nós se movem em grupo, para uma determinada direção e que apresentam uma configuração hierárquica, isto é, onde as conexões não são feitas aleatoriamente, mas cumprem as exigências impostas por este tipo de cenário. Além disto, este trabalho contribui buscando, com as diversas simulações realizadas, as condições da rede e os protocolos que melhor se adéquam a este tipo de cenário. Foram utilizados diversos modelos de simulações, com o intuito de avaliar a eficácia e a eficiência dos protocolos, no maior conjunto de situações possível.

Os resultados indicam que, quando se utiliza uma taxa de transmissão da rede de 2Mbps, ocorre uma sobrecarga do tráfego no nó que representa a central de comando, e surgem sérias dificuldades no acesso ao meio, o que resulta em problemas de atraso, descarte de pacotes e, conseqüentemente, aumento da sobrecarga de roteamento. Estes acontecimentos são decorrências do fato de que este cenário implica na concentração do tráfego em direção a um único destino, um vez que só é possível o envio de pacotes dos nós líderes para o nó de comando ou vice-versa. No cenário proposto, os nós apresentam baixa velocidade, portanto as rotas permanecem, em geral, mais estáveis, e o que se observa é que, tipicamente, existem um ou mais períodos críticos onde as condições de tráfego podem sobrecarregar o nó que exerce o controle dos outros nós do grupo. Este fato deve ser considerado como relevante quando se busca estabelecer uma rede *ad hoc*

com finalidade de emprego militar com as características apresentadas neste trabalho, uma vez que a competição pelo acesso ao meio é uma grande limitação deste cenário. O congestionamento na rede causa sérios prejuízos ao desempenho do AODV, uma vez que a dificuldade de acessar o meio para transmitir os pacotes de dados o obriga a iniciar inúmeros procedimentos de descoberta de rota desnecessários, sobrecarregando ainda mais o tráfego na rede. Este problema é amenizado redimensionado-se a capacidade da rede para 11 Mbps, em que o AODV exibe uma melhora significativa nos seus resultados, e apresenta valores de taxa média de entrega de pacotes equivalentes ao DSR.

O DSR é o protocolo que apresenta o melhor desempenho nas diversas simulações realizadas e, praticamente, não descarta pacotes por quebra de enlace, uma vez que possui em seu *cache* várias rotas para o mesmo destino. Como neste cenário os nós dentro de um grupo estão próximos uns dos outros, as rotas são facilmente restabelecidas em caso de queda no enlace, uma vez que, em geral, qualquer nó dentro de um grupo pode servir para encaminhar pacotes. Portanto, protocolos que operam sob demanda e têm a característica de múltiplas rotas, como o DSR, são indicados para este tipo de cenário, embora tenham o custo de um atraso ligeiramente maior. O DSDV apresenta o menor atraso médio de pacotes, e o atraso é uma métrica importante quando se trata de redes militares. Porém, seu uso não é indicado para este tipo de rede. As características proativas do DSDV o tornam inflexível na busca de novas rotas quando ocorre queda de enlace, ocorrência extremamente comum quando há mobilidade em grupo, comprometendo, assim, a entrega dos pacotes.

Foram realizadas diversas simulações buscando amenizar o problema decorrente da falta de conectividade que ocorre quando não existe um caminho para se chegar ao destino. A análise dos resultados mostra que, para redes com características semelhantes às apresentadas pelo cenário, oito grupos inicialmente dispostos ao longo de uma área de simulação com as dimensões apresentadas não se mostram suficientes para garantir a conectividade desta rede, quando utilizamos o alcance dos transmissores de 250 metros. Considera-se que a inclusão de um grupo nesta rede é favorável, e que os protocolos sob demanda melhoram consideravelmente o seu desempenho, uma vez que solucionam os problemas de partição de rede. Portanto, recomenda-se que sejam usados no mínimo nove grupos de combate (ou uma proporção equivalente entre número de grupos e tamanho da

área de operações) para garantir a conectividade dos nós. Uma outra possível solução é aumentar o alcance dos transmissores para 300 metros de modo a atenuar o problema de diversos particionamentos na rede, causados pelo próprio comportamento da movimentação em grupo dos nós móveis. Alcances maiores que este não são aconselháveis, por comprometerem desnecessariamente a segurança da operação.

Embora a rede analisada apresente um número limitado de nós, com reduzida velocidade e uma limitada taxa de envio de pacotes, observa-se que ela difere das redes *ad hoc* típicas, nas quais os nós possuem livre movimento para qualquer direção, e podem estabelecer comunicação indiscriminadamente com qualquer outro nó dentro de seu alcance. As forças militares possuem uma cadeia hierárquica de comando bem definida e, em geral, a localização dos elementos de combate (nós), sua mobilidade e a comunicação entre eles seguem este preceito, ocasionando um considerável efeito restritivo na topologia da rede ad hoc.

Buscando avaliar o impacto causado nas métricas avaliadas, simulamos a situação em que um dos grupos deste pelotão não consegue completar a missão, deixando de cooperar na comunicação de forma repentina, a partir de um determinado tempo de simulação. Nosso objetivo é avaliar a capacidade dos protocolos de se recuperarem de forma satisfatória em situações de particionamento inesperado da rede. De acordo com os resultados, a exclusão de um grupo acarreta em uma queda, em média, de 25% na taxa de entrega para os protocolos sob demanda e de 30% para os protocolos proativos, relativa aos freqüentes descartes decorrentes por falta de rota para alguns destinos, ocasionadas pela saída de um grupo desta rede. Esta situação é perfeitamente possível quando se trata de um cenário militar.

Uma outra possível condição para este cenário é a necessidade dos nós trocarem mais mensagens, buscando o controle de uma situação crítica apresentada. Realizamos medições, com o objetivo de avaliar o impacto causado pelo aumento do tráfego nesta rede. Percebe-se que, com o aumento da carga, as filas da subcamada MAC, quando cheias, são esvaziadas lentamente pela dificuldade de acesso ao meio, ocorrendo um elevada perda de pacotes por falta de *buffers*. O DSR e o AODV só começam a sofrer as conseqüências deste congestionamento na rede com a taxa de 10 pac/s, enquanto que o DSDV tem o seu

desempenho influenciado progressivamente com o aumento da carga. O AODV sofre um considerável acréscimo na sobrecarga de roteamento com o aumento do tráfego, devido a dificuldade de acesso ao meio. O aumento da carga da rede afeta diretamente o tempo de acesso ao meio, aumentando, por conseqüência, o descarte de pacotes devido ao transbordo das filas da subcamada MAC, enquanto a variação da mobilidade provoca perdas de pacotes devido a falta de rota.

Para fins comparativos realizaram-se simulações onde os nós foram posicionados aleatoriamente na área de simulação, e seus movimentos foram baseados exclusivamente no modelo *Random Waypoint*. Verificou-se uma queda acentuada no desempenho dos três protocolos, uma vez que a dimensão da área não garante uma densidade razoável para a rede em questão. Quando os nós se movimentam todos em direção ao mesmo destino, como no cenário proposto, a conectividade desta rede torna-se possível, isto é, pode-se estabelecer uma rede conectada com um número muito menor de estações.

Para futuras pesquisas é sugerido que, baseado nas simulações apresentadas, seja proposto um protocolo extraindo as características dos protocolos avaliados que melhor se adaptem ao cenário proposto. Além disso, deve-se avaliar o impacto de implementações que contemplem aspectos relativos à segurança nesse tipo de rede [33]. Deve ser conduzido um estudo sobre o consumo de energia para a rede proposta, levando em consideração o tempo de duração da missão. Os modelos desenvolvidos neste trabalho podem ser prontamente incorporados a Sistemas de Apoio à Decisão (SAD) militares voltados para ações táticas de infantaria, ou ser aplicados a módulos de simulação de movimentação de tropas, principalmente nos aspectos correspondentes à comunicação operacional, em grandes Jogos de Guerra. Por fim, conduzir novas simulações com outros protocolos existentes, a fim de dar continuidade à busca de um protocolo que melhor atenda às exigências impostas por este tipo de cenário realista.

Referências Bibliográficas

[1] SILVA, C. A., E SEIXAS, R. B. Integração de agentes autônomos e sig em uma arquitetura para simulação de confrontos. In *Simpósio de Desenvolvimento e Manutenção de Software da Marinha - SDMS 2003* (2003).

[2] SANTOS, F. M. A., CASANOVA, M. A., E SEIXAS, R. B. Alternativas do emprego de computação móvel nos exercícios do cfn. In *Revista Marítima* (2003).

[3] BROCH, J., MALTZ, D. A., JOHNSON, D. B., HU, Y.-C., E JETCHEVA, J. A performance comparison of multi-hop wireless for ad hoc network routing protocols. In *in Proceedings of the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking* (outubro de 1998), pp. 85–97.

[4] PERKINS, C. E., ROYER, E. M., DAS, S. R., E MARINA, M. K. Performance comparison of two on-demand routing protocols for ad hoc networks. *Proceedings of the IEEE Conference on Computer Communications (INFOCOM)* (março de 2000), 3–12.

[5] VILLELA, B. A. M., E DUARTE, O. C. M. B. Uma análise de protocolos de roteamento sob demanda de redes ad hoc. In *(SBT'2003) Simpósio Brasileiro de Telecomunicações* (outubro de 2003).

[6] PEREIRA, I. C. M., E PEDROZA, A. C. P. Aplicações militares empregando redes móveis ad-hoc. In *VI Simpósio de Pesquisa Operacional da Marinha VII Simpósio de Logística da Marinha, Escola de Guerra Naval - Praia Vermelha - Rio de Janeiro , SPOLM 2003* (dezembro de 2003).

[7] PEREIRA, I. C. M., E PEDROZA, A. C. P. Análise de redes móveis ad hoc para cenários de operações militares. In *I Workshop de Ciências da Computação e Sistemas da Informação da Região Sul, WorkComp SUL* (maio de 2004).

[8] JOHANSSON, P., LARSSON, T., HEDMAN, N., MIELCZAREK, B., E DEGERMARK, M. Scenario-based performance analysis of routing protocols for mobile ad-hoc networks. In *In Proceedings of ACM/IEEE MOBICOM'99* (1999), pp. 195–206.

[9] ROYER, E. M., E TOH, C. A review of current routing protocols for ad hoc mobile wireless networks. *IEEE Personal Communications 6*, 2 (abril de 1999), 46–55.

[10] MONARCH PROJECT. *The Rice Monarch Project – Wireless and Mobility Extensions to ns-2*, novembro de 2000. http://www.monarch.cs.rice.edu/cmu-ns.html.

[11] JOHNSON, D. B., E MALTZ, D. A. The dynamic source routing protocol for mobile ad hoc networks. In *Internet Draft, draft-ietf-manet-dsr-06.txt* (fevereiro de 2002).

[12] PERKINS, C., E BHAGWAT, P. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. In *ACM SIGCOMM Conference on Communications Architectures, Protocols and Applications* (agosto de 1994), pp. 234–244.

[13] PERKINS, C. E., BELDING-ROYER, E. M., E DAS, S. R. *Ad Hoc On-Demand Distance Vector (AODV) Routing*, novembro de 2002. http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv-12.txt.

[14] JARDOSH, A., BELDING-ROYER, E. M., ALMEROTH, K. C., E SURI, S. Towards realistic mobility models for mobile ad hoc networks. *MobiCom'03* (setembro de 2003), 217–229.

[15] T. CAMP, J. BOLENG, V. D. A survey of mobility models for ad hoc network research. In *Wireless Communications and Mobile Computing (WCMC)* (2002), pp. 483–502.

[16] QUIMING, L. *The Scenario Generator: a tool to generate MANET mobility scenarios for NS-2*. UC Berkeley, LBL, USC/ISI, and Xerox PARC (The VINT Project), abril de 2002. http://www.comp.nus.edu.sg/liqm/scengen.

[17] *NS-2 and Adhockey*. http://www.monarch.cs.rice.edu/ns-faq/faq.html.

[18] CAMPOS, C. A. V., E MORAES, L. F. M. Modelos markovianos de mobilidade individual para redes móveis ad hoc. In *SBRC Simpósio Brasileiro de Redes de Computadores* (maio de 2003).

[19] HONG, X., GERLA, M., PEI, G., E CHIANG, C. A group mobility model for ad hoc wireless networks. In *MSWiM Proceedings of the ACM International Workshop on Modeling and Simulation of Wireless and Mobile Systems* (agosto de 1999).

[20] DAVIES, V. Evaluating mobility models within ad hoc network. Relatório técnico, Colorado School of Mines Los Angeles, 2000.

[21] KARLIN, S., E TAYLOR, H. M. A first course in stochastic processes - second edition.

[22] JOHNSON, D. B., E MALTZ, D. A. Dynamic source routing in ad hoc wireless networks. Relatório técnico, Kluwer Academic Publishers, 1996.

[23] CISCO SYSTEMS, I. Mobile ad hoc networks for the military. In *MSWiM Proceedings of the ACM International Workshop on Modeling and Simulation of Wireless and Mobile Systems* (janeiro de 2003).

[24] SANCHEZ, M. *Mobility models*. http://www.disca.upv.es/misan/mobmodel.htm. Acessado em 10 de abril de 2004.

[25] MÄÄTTÄ, R. Wireless ad hoc routing protocols, a taxonomy. *Defence Forces Research Institute* (maio de 2000).

[26] HAAS, Z. J., E TABRIZI, S. On some challenges and design choices in ad hoc communications. In *In IEEE MILCOM'98, Bedford, MA* (oct de 1998).

[27] IEEE. *Wireless LAN medium access control (MAC) and physical layer (PHY) specificationsns Notes and Documentation - Part 11*. Standard 802.11, 1999.

[28] VELLOSO, P. B. *Transmissão de Voz em Redes Ad Hoc*. Tese de Mestrado, Universidade federal do Rio de Janeiro, 2003.

[29] IEEE. *Supplement to part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications*. Standard 802.11b, 1999.

[30] IEEE. *Supplement to part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specificationsns Notes and Documentation - Part 11*. Standard 802.11a, 1999.

[31] FALL, K., E VARADHAN, K. *ns Notes and Documentation*. UC Berkeley, LBL, USC/ISI, and Xerox PARC (The VINT Project), abril de 2002. http://www.isi.edu/nsnam/ns/ns-documentation.html.

[32] XU, S., E SAADAWI, T. Does the IEEE 802.11 MAC protocol work well in multihop wireless ad hoc networks. *IEEE Comunications Magazine* (junho de 2001), 130–137.

[33] HU, Y.-C., PERRIG, A., E JOHNSON, D. B. Ariadne: a secure on-demand routing protocol for ad hoc networks. In *ACM International Conference on Mobile Computing and Networking - MobiCom* (setembro de 2002), pp. 12–23.

Apêndice A

O Modelo Mixed Waypoint

O MODELO desenvolvido neste trabalho, implementado na linguagem C++ e incorporado à ferramenta ScenGen, tem seu código apresentado na listagem que se segue, relativa ao arquivo mixwp.cc.

```
//###########################################################################
//     Arquivo   : mixwp.cc
//     Autor     : Ivana Cardial de Miranda Pereira
//     Data      : 16/09/2003
//     Descricao : Este programa  descreve o modelo Mixed Waypoint criado para
//                 ser utilizado pelo ScenGen. Este  modelo tem como função
//                 modelar o movimento de um nó, partindo de  um   ponto pré-
//                 fixado com destino a uma área definida  dentro da área de
//                 simulação. Esta área corresponde a uma fração da área total
//                 da simulação e é definida a partir de um  ponto
//                 correspondente ao canto superior direito passado como
//                 parâmetro pelo usuário na especificação do cenário (scen-
//                 spec)
//###########################################################################

// mixwp.cc
//
// Modelo Mixed Waypoint
#include "defs.h"
#include "util.h"
```

```
#include "model.h"
#include "mixwp.h"

MixWP::MixWP() : Model()
{
    type_ = MODEL_MIXWP;
    moveList_ = new List();
    assert(moveList_);
    primMovim_ = true;
    primPonto_ = true;
    proxMovim_ = NULL;
}

MixWP::~MixWP()
{
    assert(moveList_);
    delete moveList_;
}

void MixWP::init(model_time_t startTime, model_time_t stopTime,
                  node_id_t startID, int num_nodes, Area *area, bool cp)
{
// modela apenas um nó.
    assert(num_nodes == 1);

// inicializa os parâmetros do modelo
    Model::init(startTime, stopTime, startID, num_nodes, area, cp);

    assert(paramList_->getCount() > 0); //obtém o numero de elementos da lista

    long i = 0;
    char key[100];   // usado para construir a chave da lista

    char *move_s = NULL;
    Move *move = NULL;
    double ptoX, ptoY, veloc, pausa, area_destX, area_destY, fracao;

    paramList_->reset();
```

```
  while ( (move_s = (char *)paramList_->nextValue()) != NULL) {
      int result = sscanf(move_s, "(%lf,%lf,%lf,%lf)",
                          &ptoX, &ptoY, &veloc, &pausa);
      if (result == 0) continue;
      move = new Move();
      assert(move != NULL);

      if (primPonto_) {
     move->dest_.x_ = ptoX;
         move->dest_.y_ = ptoY;
     // o primeiro ponto define o tamanho da área de destino como uma
         // fração em relação à área total de simulação
         fracao = veloc/100; // transforma a entrada (%) em fração
         area_destX = area_->maxX()*(fracao);
         area_destY = area_->maxY()*(fracao);
      } else {
         // o ponto de chegada é escolhido aleatoriamente dentro da área de
         // destino, definida dentro da área de simulação
     move->dest_.x_ = getRandomDouble(DIST_UNIFORM,
                                      ptoX - area_destX, ptoX);
         move->dest_.y_ = getRandomDouble(DIST_UNIFORM,
                                      ptoY, ptoY + area_destY);
         move->speed_ = veloc;

    }// fim if

    // define o tempo do movimento como o tempo de pausa
    // o tempo correto deve ser calculado em proxMovim()
    move->time_ = pausa;

    // insere o movimento na moveList_
    i++;
    sprintf(key, "wp%ld", i);
    moveList_->set(key, move);
primPonto_ = false;

  } // fim while
```

```
    // deve ter no mínimo um movimento
    assert(moveList_->getCount() > 0);

    // recupera o primeiro movimento do proxMovim_
    moveList_->reset();
    proxMovim_ = (Move *) (moveList_->nextValue());
    assert(proxMovim_);
    primMovim_ = true;
    initialized_ = true;
}

// cria o movimento
void MixWP::makeMove(Node *node)
{
    assert(node);

    if (primMovim_) {   // cria o primeiro movimento
        node->pos_ = proxMovim_->dest_;
        node->dest_ = proxMovim_->dest_;
        node->nextStartTime_ = startTime_ + proxMovim_->time_;
        node->speed_ = 0;
        primMovim_ = false;
    } else { // cria os próximos movimentos
        node->pos_ = node->dest_;
        node->dest_ = proxMovim_->dest_;
        node->speed_ = proxMovim_->speed_;
        node->startTime_ = node->nextStartTime_;
        // tempo gasto para alcançar o destino
        model_time_t t = (node->dest_ - node->pos_).length()/node->speed_;
      // calcula o instante de chegada no ponto de destino
        node->arrivalTime_ = node->startTime_ + t;
      // calcula o instante da próxima partida adicionando
      // o tempo de pausa do nó
        node->nextStartTime_ = node->arrivalTime_ + proxMovim_->time_;
    }

    // avança para o próximo movimento proxMovim_
    proxMovim_ = (Move *) (moveList_->nextValue());
```

```
    if (proxMovim_ == NULL) {
        moveList_->reset();
        proxMovim_ = (Move *) (moveList_->nextValue());
    }
    assert(proxMovim_);

}
```