

APLICAÇÕES MILITARES EMPREGANDO REDES MÓVEIS AD HOC

Ivana Cardial de Miranda Pereira

CASNAV – Centro de Análises de Sistemas Navais

<http://www.casnav.mar.mil.br/>

Grupo de Teleinformática e Automação (GTA)

COPPE/EE - Programa de Engenharia Elétrica

Universidade Federal do Rio de Janeiro

<http://www.gta.ufrj.br/>

ivana@gta.ufrj.br

Aloysio de Castro P. Pedrosa

Grupo de Teleinformática e Automação (GTA)

COPPE/EE - Programa de Engenharia Elétrica

Universidade Federal do Rio de Janeiro

<http://www.gta.ufrj.br/>

alloysio@gta.ufrj.br

Resumo

O objetivo deste artigo é avaliar o problema de roteamento em redes móveis *ad hoc* sob o ponto de vista de aplicações militares. Para esta finalidade, comparamos o comportamento de três protocolos de roteamento propostos para redes *ad hoc*, DSR, AODV e DSDV, utilizando um cenário que representa uma aproximação de uma operação militar específica em um campo de batalha – uma ação de assalto e tomada de posição inimiga.

Palavras-Chaves: Redes móveis sem-fio *ad hoc*; Protocolo de roteamento; Aplicações militares;

Abstract

The purpose of this work is to evaluate the performance of three routing protocols in military applications of hierarchical-type mobile *ad hoc* networks, namely DSR, AODV and DSDV. We develop a scenario that approximates a real battlefield military operation – an assault and take-over of an enemy position.

Keywords: Military applications; Ad hoc mobile networks; Routing protocols.

1. INTRODUÇÃO

Devido ao atual crescimento do segmento de computadores pessoais portáteis, estima-se que em poucos anos será comum que as pessoas possuam um *laptop*, *palmtop* ou algum tipo de dispositivo portátil com capacidade para se comunicar com a parte fixa da rede, e com outros computadores móveis. Este ambiente de computação é chamado de computação móvel.

As redes móveis 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 móveis é feita por meio de estações de suporte à mobilidade na rede fixa. Neste tipo de rede, os nós móveis, mesmo próximos um do outro, estão impossibilitados de estabelecer comunicação direta entre si.

Uma rede *ad hoc* (Figura 1) é um conjunto de nós móveis 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 à mobilidade. Neste tipo de rede, os nós funcionam como roteadores, que são capazes de descobrir e manter rotas para outros nós da rede; e como *hosts*, executando aplicações dos usuários.

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.

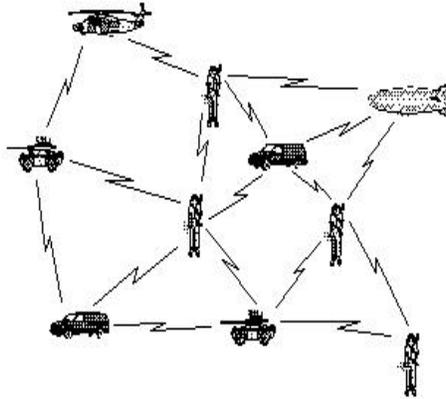


Figura 1 - uma rede *ad hoc*

Em razão da mobilidade dos nós, as redes *ad hoc* apresentam uma topologia dinâmica, isto é, mudam frequentemente e de forma imprevisível, influenciando fortemente as características da rede, tornando, assim, o roteamento em redes *ad hoc* um grande desafio. Desde o surgimento destas redes, diversos protocolos foram propostos para resolver o problema de roteamento. Tais protocolos devem ser projetados de tal forma que possam lidar com as limitações típicas deste tipo de rede, que incluem alto consumo de energia dos nós móveis, banda passante limitada e alta taxa de erros devido a conexões sem fio.

Os protocolos de roteamento DSDV, AODV e DSR foram selecionados para análise neste trabalho. O AODV e o DSR foram escolhidos pela sua importância e porque apresentaram os melhores resultados [3,8], mas não foram comparados em cenários com fins militares. O DSDV é um protocolo pró-ativo e foi incluído para ilustrar a diferença de comportamento entre protocolos por demanda e protocolos pró-ativos. A motivação principal é se 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.

Como exemplo 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; conferências, onde os participantes desejam disseminar ou compartilhar informações rapidamente, por meio de seus laptops ou *palmtops*; e aplicações militares.

Neste artigo nós nos concentramos em avaliar o problema de roteamento em rede *ad hoc* sob o ponto de vista de operações militares. Devido às características de mobilidade de suas operações, a comunidade militar tem demonstrado grande interesse nas comunicações móveis. Especificamente, as redes *ad hoc* são de extrema importância para as suas aplicações, uma vez que em uma situação de conflito as comunicações no campo de batalha não podem depender de infra-estruturas fixas, tornando-se as redes *ad hoc* a única estrutura de rede viável para este tipo de aplicação, onde informações táticas são trocadas e uma configuração de rede descentralizada é uma vantagem operativa ou até mesmo uma necessidade.

Este trabalho foi dividido da seguinte forma: na seção 2 é apresentada uma breve introdução sobre protocolos de roteamento em redes ad hoc, onde são descritos de forma sucinta os protocolos selecionados para análise; na seção 3 são discutidos alguns aspectos relativos à representação do movimento dos nós em redes ad hoc; a seção 4 apresenta a descrição do cenário desenvolvido para este trabalho; as características da simulação são descritas na seção 5; os resultados são apresentados na seção 6; finalmente, a seção 7 conclui o trabalho.

2. PROTOCOLOS DE ROTEAMENTO EM REDES AD HOC

Em redes móveis *ad hoc*, uma rota entre dois computadores pode ser formada por vários saltos através de um ou mais computadores 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: 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, diferentes cargas de tráfego e rede.

Roteadores 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.

Os protocolos de roteamento podem ser classificados em pró-ativos e reativos. Os protocolos pró-ativos 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 pela 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. Já os protocolos reativos iniciam as atividades de roteamento de acordo com a demanda. Neste caso, somente se estabelecem rotas entre os nós na presença de pacotes de dados.

Operar sob demanda, ou de forma pró-ativa, 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 alguns casos, a latência gerada para que o protocolo opere de acordo com a demanda pode vir a ser inaceitável. Neste caso, é desejável que o protocolo trabalhe de maneira pró-ativa, tentando descobrir as informações antes que estas se tornem necessárias.

Nesta seção apresentaremos uma breve descrição dos protocolos de roteamento que serão avaliados neste trabalho.

2.1. DYNAMIC SOURCE ROUTING - DSR

O DSR [7] é um protocolo de roteamento reativo que usa roteamento na fonte para entregar pacotes de dados, ou seja, o nó origem determina toda a seqüência de nós por onde passará o pacote até chegar ao seu destino e os cabeçalhos dos pacotes de dados carregam esta seqüência de nós. Cada nó mantém um *cache*, onde todas as suas rotas conhecidas são armazenadas. O DSR consiste de dois mecanismos: descoberta de rotas e manutenção de rotas.

Quando um nó precisa enviar um pacote para outro nó, o nó de origem verifica se possui uma rota para o nó de destino 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 encontrar dinamicamente uma rota para o destino. O DSR permite que cada nó mantenha múltiplas rotas para o mesmo destino.

O mecanismo de descoberta de rotas do DSR consiste em enviar por *broadcasting* um pacote *Route Request* (RREQ) (Figura 2.a). Quando um nó recebe este pacote, verifica no seu *cache* se tem uma rota para o destino requisitado. Se o nó conhecer uma rota, envia para a origem um pacote *Route Reply* (RREP) (Figura 2.b), que contém uma lista com a seqüência de todos os nós até o destino. Caso o nó não tenha uma rota para o destino, encaminha um pacote RREQ por *broadcast* 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 destino, ou um nó com uma rota para o destino. Quando uma rota é encontrada, um pacote RREP, contendo a seqüência de nós para alcançar o destino, retorna pelo caminho reverso para a fonte, o que implica na necessidade de conexões bidirecionais.

Para que o DSR funcione também em conexões unidirecionais, é necessário que o nó verifique em seu *cache* se possui uma rota para a origem, caso não tenha, um mecanismo de descoberta de rotas é acionado para encontrar um caminho para o nó de origem.

O protocolo DSR possui a vantagem de ser capaz de "aprender" rotas. Quando um nó A encontra uma rota para um nó C através do 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.

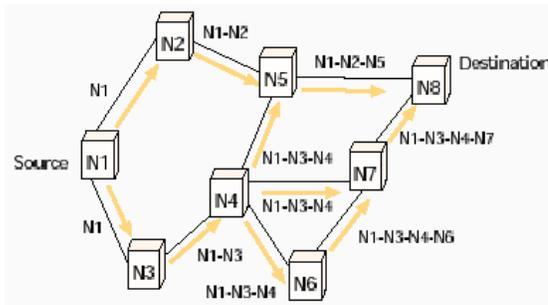


Figura 2.a - Descoberta de rotas

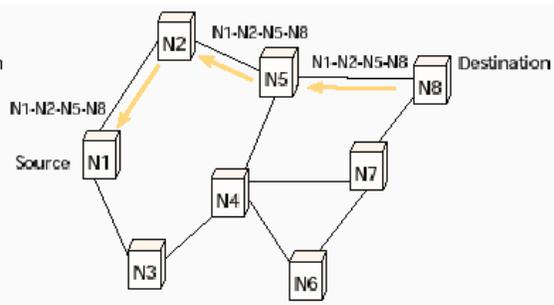


Figura 2.b - Propagação do *Route Reply*

Para evitar a inundação da rede com pacotes RREQ's, utiliza-se o procedimento de se perguntar primeiramente aos nós vizinhos, para verificar se alguma rota está disponível para o destino desejado. Isto é feito enviando um primeiro pacote RREQ com um limite de salto de zero, significando que não deve ser encaminhado para os outros vizinhos. Se nenhuma resposta é obtida, um novo pacote RREQ é propagado através da rede.

No mecanismo de manutenção de rotas, o nó origem detecta se ocorreram alterações na topologia da rede que poderão comprometer o uso das rotas. Desta forma, se um nó percebe algum problema de comunicação com o nó vizinho, envia um pacote *Route Error* (RERR) de volta para o nó de origem. A origem remove qualquer rota usando a conexão falha de seu *cache* e inicia um novo procedimento de descoberta de rotas, caso não tenha uma rota alternativa para este destino.

2.2. DESTINATION SEQUENCED DISTANCE VECTOR - DSDV

O DSDV [6] é um protocolo de roteamento pró-ativo, baseado em vetor de distâncias, que trabalha requisitando periodicamente de cada um dos nós vizinhos suas tabelas de roteamento com a finalidade de manter suas tabelas atualizadas. Cada nó da rede mantém uma tabela de roteamento que contém o próximo salto e o número de saltos para alcançar o

destino. As tabelas mantêm 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.

A vantagem principal do DSDV sobre os protocolos baseados em vetor de distâncias tradicionais é que eles garantem ausência de *loops*, usando o conceito de número de seqüência mantidos em cada destino, para indicar qual a rota mais recente. As rotas mais recentes possuem um número de seqüência maior e são as mais favoráveis. Caso os números de seqüências sejam iguais, a rota que tiver a menor distância será a mais favorável. Os *loops* de rotas podem ocorrer quando informações de roteamento incorretas são mantidas na rede após uma troca de topologia. O DSDV inicia um processo de atualização de rota periodicamente ou quando a topologia da rede muda.

Quando um nó percebe que uma conexão para B foi interrompida, notifica sua rota para B com um contador de saltos infinito e incrementa o número de seqüência. 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 B com um número de seqüência maior.

2.3. AD HOC ON DEMAND DISTANCE VECTOR - AODV

O AODV [1] é um protocolo reativo, e é uma combinação do DSR e o 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 manter tabelas de roteamento tradicionais de uma entrada para cada destino, diferentemente do DSR que permite múltiplas rotas para cada destino. Pode ser considerado como uma versão melhorada do DSDV, já que seu funcionamento baseado em demanda minimiza o número de *broadcasts* exigidos para criação de rotas.

Quando um nó necessita encontrar uma rota para outro nó, e esta rota não existe na sua tabela de rotas, inicia um procedimento de descoberta de rotas, inundando a rede com mensagens *Route Request* (RREQ) para todos os nós vizinhos (Figura 3). Quando as requisições de rotas são propagadas pela rede, todos os nós atualizam suas tabelas com relação ao nó origem. Os pacotes RREQ vão trafegar na rede até alcançar o destino ou um nó com uma rota recente para o destino. Durante o processo de encaminhamento do RREQ, os nós intermediários gravam em suas tabelas de rotas o endereço do vizinho que encaminhou o pacote, estabelecendo assim um caminho reverso que será utilizado pelo pacote *Route Reply* (RREP) para alcançar o nó de origem, quando o destino, ou uma rota para o destino é encontrado.

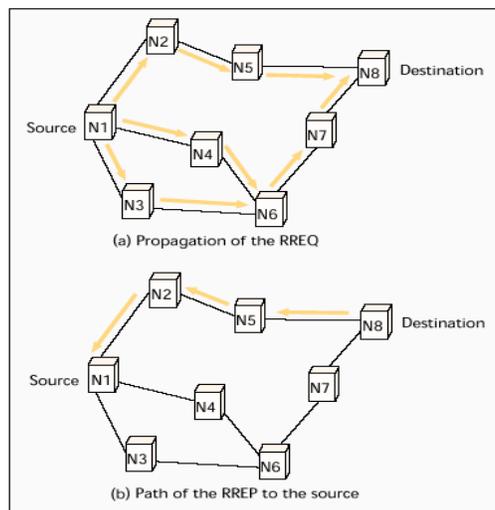


Figura 3 – Descoberta de rotas

Uma importante característica do AODV é manter um estado relacionado ao tempo em cada nó, isto significa que uma entrada é expirada se não é utilizada em espaço de tempo determinado.

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 assim que efetivamente seja propagada a informação de conexão falha.

O AODV utiliza mensagens *hello* para manter a conectividade de um nó. Para detectar se os nós vizinhos estão ativos, estas mensagens são enviadas periodicamente, com uma taxa *default* de um por segundo. Se um nó não recebe mensagens *hello* de um vizinho para qual envia tráfego, é considerado que o nó se moveu e esta conexão é considerada interrompida. Neste caso o nó avisa a todos os nós que dependiam desta conexão, através de uma requisição não solicitada de rotas contendo uma métrica infinita para aquele destino, que o mesmo não está mais disponível.

3. MODELOS DE MOBILIDADE PARA REDES AD HOC

Existem duas maneiras de representar padrões de movimentos de usuários de uma rede móvel [11]: através da captura de informações do comportamento real de movimentação do nó móvel, ou seja, com o uso de registros de movimentação, ou por meio de modelos de mobilidade. Como a captura dos registros torna-se uma tarefa difícil em ambientes dinâmicos, como em redes *ad hoc*, utiliza-se, na maioria dos casos, os modelos de mobilidade.

Os modelos de mobilidade buscam representar o comportamento da movimentação dos dispositivos móveis em uma rede *ad hoc*. Esses modelos, quando utilizados nesse tipo de rede, podem ser classificados de duas formas: os modelos de mobilidade individual (entidade), que servem para representar o comportamento da movimentação dos nós móveis de forma independente dos demais na rede; e os modelos de mobilidade em grupo, que representam o movimento de um grupo de nós móveis cujo movimento de cada nó é dependente do movimento dos outros nós. Os modelos de mobilidade em grupo são utilizados em situações em que é necessário se modelar o comportamento dos nós móveis quando eles se movem juntos. Como exemplo, podemos citar os cenários militares, em que grupos de soldados se movem de forma cooperativa com o objetivo de cumprir uma determinada tarefa.

Existem diversos modelos de mobilidade utilizados para representar o movimento dos usuários em uma diversidade de cenários, que são usados para avaliar o comportamento de algoritmos de roteamento em redes *ad hoc*. Os modelos de mobilidade individual são os mais utilizados na literatura para avaliação da eficiência dos algoritmos de roteamento nessas redes, devido às suas características de modelagem mais simples e fácil implementação. Porém, estes modelos restringem-se a comportamentos de movimentação específicos, que, muitas vezes, se afastam demais da realidade [11].

O desempenho de um protocolo em redes *ad hoc* pode variar significativamente de acordo com a utilização de diferentes modelos de mobilidade [9]. Portanto, é de extrema importância que o modelo de mobilidade escolhido represente da melhor forma possível o movimento dos nós no cenário real que se deseja simular em uma rede *ad hoc*, podendo-se, assim, iniciar um estudo para se determinar qual o protocolo mais apropriado para ser utilizado naquele cenário específico. O modelo de mobilidade deve buscar reproduzir os movimentos dos nós móveis em cenários realistas.

4. REDES AD HOC PARA APLICAÇÕES MILITARES

No campo de batalha do futuro provavelmente se fará uso excessivo de comunicação sem fio. As unidades móveis poderão ser usadas nos centros de comando e controle, nos próprios

veículos (como carros de combate, helicópteros, navios ou aeronaves), assim como os próprios soldados poderão carregar seus próprios terminais de comunicação pessoal.

Entretanto, 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, já 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 [5].

As redes militares possuem características diferentes das redes comerciais. Possuem um pequeno número de nós, mas com a necessidade de se comunicar com uma estrutura global bem maior. Suas mensagens geralmente são pequenas e são usadas para manipular e controlar sistemas distribuídos. Para as aplicações militares, o tempo para entregar uma mensagem é uma restrição crítica. 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.

As utilizações militares de redes *ad hoc* possuem algumas características próprias que podem ser assim resumidas [13]: uma cadeia de comando bem definida que pode impactar na topologia da rede; as unidades (grupos de nós) devem cooperar uns com os outros, uma vez que, normalmente, compartilham uma missão; e as operações militares, 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.

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 representa um pelotão de infantaria em operação militar composto de 35 participantes, cada qual com seus comunicadores pessoais dotados 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 formado por dois observadores que ocupam uma posição avançada em relação aos outros grupos, e que têm como missão mantê-los informados da situação e das posições ocupadas pela força inimiga, quando houver; e uma central de comando, operando no interior de um veículo (carro de combate, caminhão, etc).

Os grupos ocupam posições no terreno para que possam alcançar, de forma cooperativa, um determinado ponto-objetivo neste cenário, com a finalidade de cumprir uma determinada tarefa. 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 central de comando, 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 escolha de todos os parâmetros de

mobilidade e tráfego para este cenário teve como objetivo uma maior aproximação da aplicação real.

5. SIMULAÇÕES

Para as simulações foi utilizado o simulador de rede ns-2 [10]. Este simulador foi desenvolvido pela Universidade da Califórnia em Berkeley e pelo projeto VINT. Posteriormente, o grupo de pesquisa MONARCH da CMU (*Carnegie Mellon University*) desenvolveu extensões para fornecer suporte a simulações para redes sem-fio completas que modela o padrão IEEE 802.11 na camada física, camada de enlace e camada MAC usando o modo DCF (*Distributed Coordination Function*). Antes de transmitir pacotes de dados *unicast*, o DCF do 802.11 reserva o meio através de pacotes de controle *Request-to-send* (RTS) e *Clear-to-send* (CTS) para reduzir a probabilidade de colisões decorrentes do problema de “terminais escondidos”. A transmissão dos pacotes de dados é seguida de uma confirmação (ACK) enviada pelo receptor para o emissor.

O modelo do protocolo de roteamento recebe todos os pacotes de dados que são transmitidos ou encaminhados e solicita, quando necessário, atividades de roteamento.

Foram realizados dois tipos de simulação: na primeira simulação, os grupos alcançam seu ponto-objetivo sem baixas; e na segunda simulação, um dos grupos deste pelotão não consegue completar a missão, deixando de cooperar na comunicação de forma repentina. Nosso objetivo é avaliar a capacidade dos protocolos de se recuperarem de forma satisfatória em situações de particionamento inesperado da rede.

As métricas utilizadas para comparar o desempenho dos protocolos foram:

- Fração de entrega de pacotes - razão do número de pacotes entregues para o destino para aqueles gerados pela fonte;
- Média de atraso de pacotes de dados - inclui todos os possíveis atrasos causados pela latência da descoberta de rotas, propagação, atrasos devido a retransmissões do MAC e tempos de transferência;
- *Overhead* - foram medidos o número de pacotes de controle e o *byte overhead*, que inclui o *overhead* em pacotes de dados. Esta métrica mede a escalabilidade do protocolo, isto é, como ele funcionaria em ambientes congestionados ou com baixa largura de banda, e sua eficiência em termos de consumo de energia no nó.

5.1. MODELO DE MOBILIDADE



Figura 4 – Posição dos grupos no início da simulação

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 possível cenário militar real. Por meio desse padrão evitou-se mudanças bruscas de direção, permitindo-se que os movimentos sejam feitos na mesma direção, com velocidades distribuídas uniformemente entre uma velocidade mínima e uma velocidade máxima e com intervalos de pausa no movimento também distribuídos uniformemente entre um tempo de pausa mínimo e um tempo de pausa máximo. Desta forma, tenta-se retratar com uma maior aproximação o movimento real dos usuários no cenário proposto.

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* e *Fixed Waypoint* [9], respectivamente, para modelar os dois movimentos citados acima.

O modelo *Random Waypoint* divide o percurso de um nó móvel (NM) em períodos de movimentação e estabelece uma pausa. Inicialmente, o nó móvel fica parado por determinado intervalo de tempo e, então, move-se para uma posição escolhida aleatoriamente com uma velocidade que segue uma distribuição uniforme entre a velocidade mínima e a velocidade máxima. O modelo *Fixed Waypoint* é uma adaptação do modelo *Reference Point Group Mobility* (RPGM) [12], que representa o movimento aleatório de um grupo de NM, bem como o movimento dos próprios NM dentro do grupo. O movimento dos grupos é baseado no trajeto de um ponto de referência lógico (centro) do grupo. Este ponto de referência é utilizado para se calcular o movimento aleatório de cada NM. Neste trabalho, todos os NM de um grupo possuem apenas um ponto de referência, de maneira a se preservar a integridade do movimento em grupo na direção geral do objetivo militar conjunto.

Os NM que formam os grupos movem-se com uma velocidade que segue uma distribuição uniforme entre 0 e 2 m/s e um tempo de pausa distribuído uniformemente entre 0 e 5 segundos. O nó que está montado no veículo move-se com velocidade média de 3 m/s.

Os grupos se movimentam com velocidade média de 2m/s em direção a um determinado ponto (objetivo militar).

Para especificação deste cenário foi usado o gerador de cenários de mobilidade ScenGen [14], que gera uma saída configurada para o uso do simulador de rede ns-2.

Para a área de simulação utilizou-se um campo retangular de 2000×1000m (Figura 4) com a seguinte distribuição dos nós: 8 grupos formados por 4 nós cada grupo, 1 grupo formado por 2 nós e um nó montado em um veículo. Cada nó tem um raio de alcance de 250 metros. O tempo de simulação foi de 500 segundos, que é o tempo médio que os grupos levam para alcançar o ponto-objetivo.

5.2. MODELO DE TRÁFEGO

Para esta simulação, o tráfego foi gerado por 10 fontes *continuous bit-rate* (CBR) – posicionadas na central de comando. Além disso, cada um dos 10 grupos móveis possui uma fonte adicional. O tamanho dos pacotes é de 512 bytes, a taxa de envio de pacotes de 4 pacotes/segundo. O gerador de tráfego foi implementado de forma a selecionar aleatoriamente um líder entre os participantes de cada grupo, representando o comandante do grupo de combate. Cada um destes comandantes será o responsável pela comunicação de seu grupo com a central de comando.

6. RESULTADOS

6.1. MÉTRICAS

O resumo dos resultados obtidos nas simulações para cada protocolo no cenário proposto são apresentados na Tabela 1 (valores médios).

	DSDV		AODV		DSR	
	Sim 1	Sim 2	Sim 1	Sim 2	Sim 1	Sim 2
Taxa de Entrega	86,15%	73,08%	97,10%	84,85%	97,69%	85,23%
Atraso Médio (seg)	0,0437	0,0360	0,0143	0,0491	0,0566	0,0960
Overhead de Pacotes	2646	2416	2994	7507	1466	3890
Byte Overhead (MB)	1,93	1,67	1,99	1,81	1,82	1,72

Tabela 1: Resultados das simulações com largura de banda de 11Mbps.

Na primeira simulação (Sim 1) observamos que os protocolos reativos AODV e DSR apresentaram taxa de entrega de pacotes similares e entregaram em média 11% mais pacotes que o protocolo pró-ativo DSDV. Na segunda simulação (Sim 2) observamos que houve uma queda em média de 12% nesta taxa de entrega, relativa aos freqüentes descartes decorrentes da falta de rota para alguns destinos, ocasionadas pela saída de um grupo desta rede.

O AODV apresentou o melhor desempenho em relação à métrica de atraso nas duas simulações. O DSDV exibiu um atraso médio na entrega dos pacotes menor na segunda simulação porque muitos pacotes foram descartados, e no cálculo do atraso só são considerados os pacotes que alcançaram o destino com sucesso. Vale ressaltar que as métricas não são completamente independentes, portanto uma taxa de entrega mais baixa significa que a métrica de atraso foi calculada com um número menor de amostras, e caso as rotas sejam mais longas, a probabilidade de descartar pacotes é maior [4].

Embora o DSR e o AODV possuam mecanismos de gerar pacotes por demanda muito similares, o *overhead* exigido por ambos apresenta-se bem distinto. Analisando os resultados obtidos, verificou-se que o AODV gerou, em média, um *overhead* de pacotes duas vezes superior ao DSR nas duas simulações apresentadas, por causa das inundações da rede com pacotes de descoberta de rota. O DSR limita a propagação de pacotes RREQ's 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.

6.2. ANÁLISE COMPARATIVA DOS PROTOCOLOS

Uma vez que este trabalho busca focar o estudo do comportamento dos protocolos em um cenário similar ao campo de batalha, faz-se necessário apresentarmos dinamicamente os resultados das diferentes métricas para cada protocolo no decorrer do tempo de simulação, uma vez que o padrão de mobilidade desenvolvido para este cenário apresenta características diferentes ao longo do tempo (Figuras 5, 6, 7, 8).

Como pode ser observado nos gráficos abaixo¹, o cenário apresentou condições críticas durante o intervalo de 120 a 180 segundos na segunda simulação, devido às suas características dinâmicas. Este período corresponde à eliminação de um grupo que compunha esta rede, resultando, com isto, em medidas maiores de *overhead* (Figura 7) e uma acentuada queda na taxa de entrega para os três protocolos (Figura 5).

O DSDV demorou cerca de 35 segundos até que estivesse pronto para enviar o primeiro pacote de dados, já que opera de forma pró-ativa, 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, pois ultrapassam a

¹ Estão apresentados apenas os valores médios, a fim de tornar mais clara a visualização dos resultados comparativos. Os intervalos de confiança calculados, em cada instante, apresentaram pequenos valores quando comparados à média da métrica.

quantidade máxima permitida de pacotes, aguardando na camada de roteamento uma rota para serem encaminhados (Figura 5).

A partir de 150 segundos de simulação, os nós deste cenário tendem a ficar mais próximos uns dos outros, e com isto as rotas ficam mais estáveis, já que todos os grupos partiram de pontos diferentes, mas com o objetivo de alcançar o mesmo ponto. Com isso, a taxa de entrega tende a atingir 100%, sendo que o DSDV é o último a se aproximar deste valor, demorando cerca de 100 segundos a mais que os outros protocolos (Figura 5(a)). Na segunda simulação, os protocolos só se estabilizam a partir de 250 segundos, e não conseguem atingir os 100%. O DSDV apresenta o pior desempenho quando as condições da rede são críticas, mas se recupera rapidamente quando estas condições melhoram (Figura 5(b)).

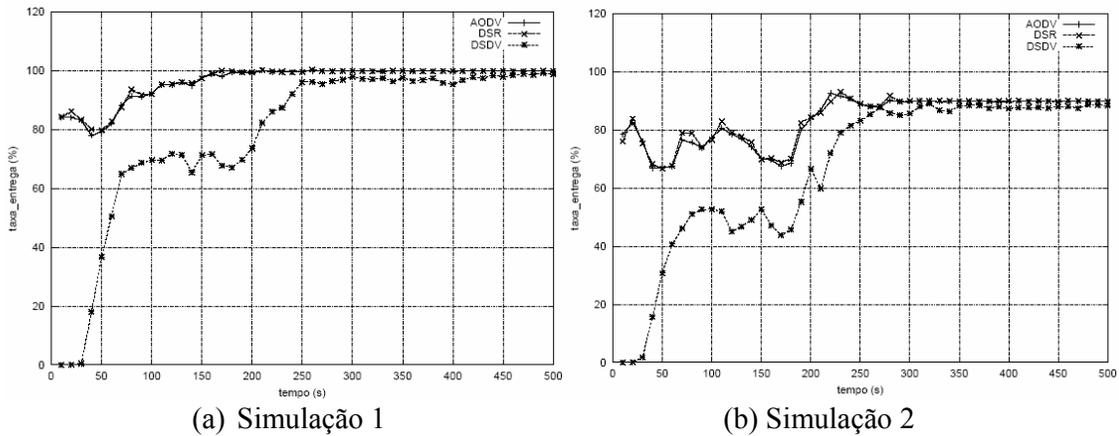


Figura 5 – Taxa de Entrega dos pacotes para as duas simulações realizadas

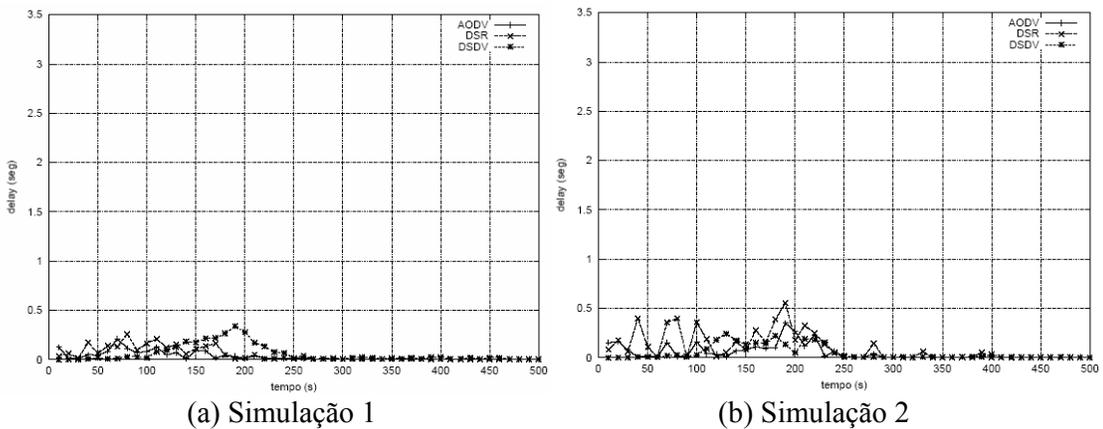


Figura 6 – Atraso médio dos pacotes para as duas simulações realizadas

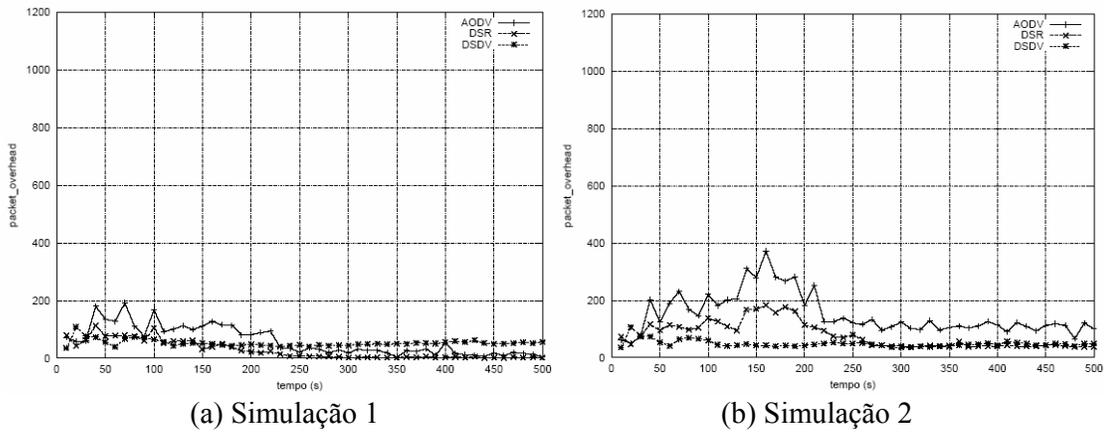


Figura 7 – *Overhead* de pacotes para as duas simulações realizadas

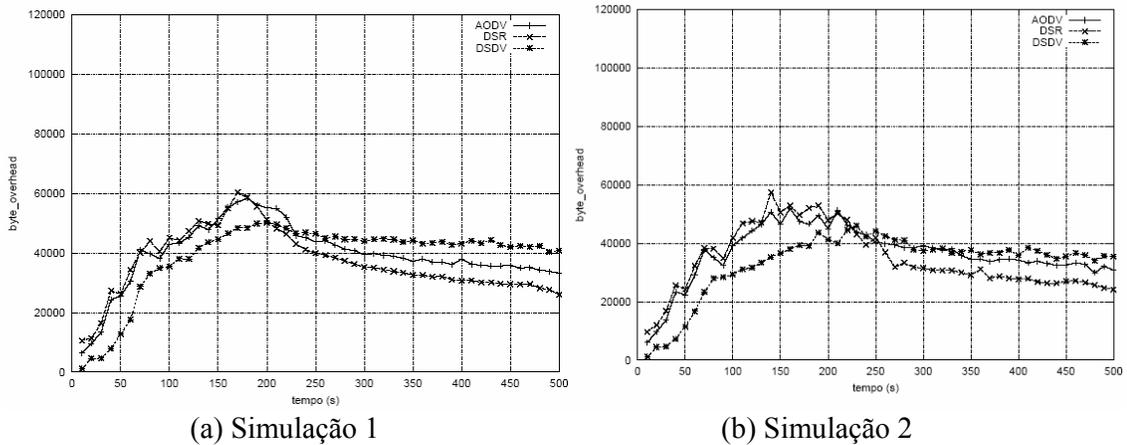


Figura 8 – *Byte overhead* para as duas simulações realizadas

7. CONCLUSÃO E TRABALHOS FUTUROS

As simulações apresentadas neste trabalho confirmam o fato de que cada protocolo apresenta vantagens e desvantagens, dependendo das condições que lhe são impostas. Nos cenários com propósitos militares, que utilizam redes *ad hoc* com configuração hierárquica, a entrega dos pacotes de forma eficiente e rápida é de extrema relevância. O protocolo “ideal” atenderia a todas as restrições impostas pelas necessidades de comunicação em cenário tipicamente militares, mas o que se pôde concluir a partir dos resultados alcançados é que cada um dos protocolos avaliados mostrou-se melhor em determinada métrica ou condição.

No cenário proposto, os nós apresentam baixa velocidade, portanto as rotas permanecem, em geral, mais estáveis, e o que se observa é que, tipicamente, pode existir um ou mais períodos críticos onde as condições de tráfego podem sobrecarregar o nó que exerce o controle dos outros nós do grupo. As redes *ad hoc* militares caracterizam-se por apresentar uma configuração hierárquica, acarretando na sobrecarga de tráfego em determinados nós da rede, e em sérias dificuldades na disputa do meio, o que resulta em problemas de atraso, descarte de pacotes e, conseqüentemente, aumento de *overhead*. Este problema foi amenizado redimensionando-se a capacidade da rede para 11Mbps. 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.

Como os nós dentro de um grupo estão próximos um do outro, as rotas deste cenário são facilmente restabelecidas em caso de quebra de enlace, uma vez que, em geral, qualquer nó

dentro de um grupo pode encaminhar pacotes, em caso de algum nó, que esteja servindo de rota, sair momentaneamente do alcance. Portanto, protocolos que tenham a característica de múltiplas rotas, como o DSR, se adaptam bem para este tipo de cenário.

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 (planas), nas quais os nós possuem livre movimento, para qualquer direção, e podem estabelecer comunicação 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*.

Para futuras pesquisas sugerimos combinar alguns protocolos para trabalharem juntos na rede, prevalecendo-se das situações em que eles apresentam maiores vantagens, ou ainda, baseado nas simulações apresentadas, propor um protocolo extraindo as características dos protocolos avaliados que melhor se adaptem ao cenário proposto. Além disso, deve-se avaliar o impacto de implementações relativas à segurança nesse tipo de rede, tais como [2]. Por fim, conduzir novas simulações com outros protocolos propostos e com cenários correspondentes a outras missões militares, a fim de dar continuidade à busca de um protocolo que melhor atenda às exigências impostas por essas aplicações.

8. REFERÊNCIAS BIBLIOGRÁFICAS

- [1] Perkins, C. E., Belding-Royer, E. M., and Das, S. R. (2002). Ad Hoc On-Demand Distance Vector (AODV) Routing. <http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv-12.txt>.
- [2] Hu, Y.C., Perrig, A., and Johnson, D. B. (2002). Ariadne: a secure on-demand routing protocol for ad hoc networks. In *ACM International Conference on Mobile Computing and Networking – MobiCom*, pages 12-23.
- [3] Per Johansson, Tony Larsson, Nicklas Hedman, Bartosz Mielczarek, Mikael Degermark "Scenario-based Performance Analysis of Routing Protocols for Mobile Ad-hoc Networks "
- [4] Samir R. Das, Charles E. Perkins, Elizabeth M. Royer, "Performance Comparison of Two On-demand Routing Protocols for Ad Hoc Networks "
- [5] Määttä, R. (2000). Wireless ad hoc routing protocols, a taxonomy. Defence Forces Research Institute.
- [6] Charles E. Perkins, Pravin Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers"
- [7] David B. Johnson, David A. Maltz , "Dynamic Source Routing in Ad Hoc Wireless Network"
- [8] Broch, J., Maltz, D. A., Johnson, D.B., Hu,Y.C., and Jetcheva, J. (1998) "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*, pages 85-97
- [9] T. Camp, J. Boleng, V. Davies. "A Survey of Mobility Models for Ad Hoc Network Research". Departamento de Matemática e Ciência da Computação, Colorado School of Mines, Golden, CO, EUA, April 12, 2002
- [10] Fall, K. and Varadhan, K. (2002). ns Notes and Documentation. UC Berkeley, LBL, USC/ISI, and Xerox PARC (the VINT Project). <http://www.isi.edu/nsnam/ns/ns-documentation.html>.

- [11] Campos, C. ^a V. and Moraes, L. F. M. (2003). Modelos Markovianos de Mobilidade Individual para Redes Móveis Ad Hoc. In *SBRC Simpósio Brasileiro de Redes de Computadores*.
- [12] X. Hong, M. Gerla, G. Pei, and C. Chiang. “A group mobility model for ad hoc wireless networks” *Proceedings of the ACM International Workshop on Modeling and Simulation of Wireless and Mobile Systems (MSWiM)*, Agosto 1999.
- [13] Cisco Systems, Inc. “Mobile Ad hoc Networks for the Military” White paper, 2003
- [14] Qiming, L. (2002). The Scenario Generator: a tool to generate MANET mobility scenarios for NS-2. UC Berkeley, LBL, USC/ISI, and Xerox PARC (The VINT Project). <http://www.comp.nus.edu.sg/liqm/scengen>.