UM PROTOCOLO DE ROTEAMENTO TOLERANTE A INTERRUPÇÕES DE COMUNICAÇÃO PARA REDES SEM FIOS MÓVEIS EM CENÁRIOS DE EMERGÊNCIA

VINÍCIUS FERNANDES SOARES MOTA
ORIENTADOR: JOSÉ MARCOS SILVA NOGUEIRA

UM PROTOCOLO DE ROTEAMENTO TOLERANTE A INTERRUPÇÕES DE COMUNICAÇÃO PARA REDES SEM FIOS MÓVEIS EM CENÁRIOS DE EMERGÊNCIA

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Minas Gerais como requisito parcial para a obtenção do grau de Mestre em Ciência da Computação.

Belo Horizonte
Julho de 2009

Fernandes Soares Mota, Vinícius
D1234p Um Protocolo de Roteamento Tolerante a Interrupções de Comunicação para Redes sem Fios Móveis em Cenários de Emergência / Vinícius Fernandes Soares Mota. — Belo Horizonte, 2009
xviii, 84 f. : il. ; 29cm

Dissertação (mestrado) — Universidade Federal de Minas Gerais
Orientador: José Marcos Silva Nogueira

1. Algoritmo de Roteamento. 2. Redes. 3. DTN. 4. MANET. I. Título.

CDU 519.6*82.10

UNIVERSIDADE FEDERAL DE MINAS GERAIS
INSTITUTO DE CIÊNCIAS EXATAS
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

FOLHA DE APROVAÇÃO

Um Protocolo de Roteamento Tolerante a Interrupções de Comunicação para Redes Sem Fios Móveis em Cenários de Emergência

VINÍCIUS FERNANDES SOARES MOTA

Dissertação defendida e aprovada pela banca examinadora constituída pelos Senhores:

PROF. JOSÉ MARCOS SILVA NOGUEIRA - Orientador
Departamento de Ciência da Computação - UFMG

PROF. CÉLIO VINICIUS NEVES DE ALBUQUERQUE
Departamento de Ciência da Computação - UFF

PROF. ANTONIO ALFREDO FERREIRA LOUREIRO
Departamento de Ciência da Computação - UFMG

Belo Horizonte, 13 de julho de 2009.

Agradecimentos

A Deus. Aos meus pais, principalmente minha mãe pelo apoio incondicional às minhas escolhas.

Ao meu orientador, José Marcos pelo apoio e toda ajuda durante o desenrolar do mestrado. A todos os amigos que fiz no DCC, em especial aos amigos do ATM, os quais ajudaram direta ou indiretamente na construção deste trabalho. Aos grandes amigos de Contagem, companheiros de "confusões" em busca de aventuras.

Não posso deixar de citar meus irmãos quasímodos e a eterna República Notre Dame em Ouro Preto, refúgio para os momentos de *stress* (que não foram poucos). *Ut Incipt Fidelis Sic Permanent.*

Por último e não menos importante, à CAPES, CNPq e FAPEMIG por me permitirem dedicar exclusivamente ao mestrado.

"O pessimista chora,
o otimista sonha,
o realista faz."
(Autor desconhecido)

Resumo

Em cenários críticos e de emergência, tais como em desastres naturais, tecnológicos ou causados pelo homem, equipes de resgate podem formar redes móveis *ad hoc* para suprir a carência de infra-estrutura de comunicação. Em uma rede móvel *ad hoc* os nós se comunicam sem nenhum ponto de acesso fixo, necessitando para isto, que o nó destino esteja ao alcance de transmissão do nó emissor ou que algum outro nó intermediário possa reencaminhar a mensagem. Porém, a comunicação nesses cenários é suscetível a interrupções bem maiores que as redes tradicionais como a Internet.

As redes tolerantes a atrasos e interrupções (*Delay/Disruption Tolerant Network* - DTN) são uma abordagem proposta para situações em que a comunicação é intermitente. Uma DTN suporta interrupções de comunicação armazenando as mensagens e repassando-as quando voltar haver a conexão. Devido à necessidade de retenção temporária das mensagens, os nós devem possuir recursos disponíveis para armazenamento de mensagens. Os protocolos de roteamento Epidêmico e PROPHET têm bom desempenho quando há recurso de armazenamento alto, porém na maioria dos dispositvos móveis os recursos ainda são escassos.

Esta dissertação apresenta um protocolo de roteamento tolerante a interrupções de comunicação, denominado HIGROP (*HIerarquical Group ROuting Protocol*). O HIGROP tem como objetivo aumentar a taxa de entrega de dados em redes intermitentes sem afetar o número de mensagens extras enviadas na rede (*overhead* de comunicação). Pelo nosso conhecimento, o HIGROP é o primeiro protocolo de roteamento em DTNs que utiliza um modelo hierárquico numa rede em que os nós tenham movimentos arbitrários. O HIGROP agrupa os nós vizinhos e elege um líder para cada grupo. As mensagens são transmitidas ao nó líder e este é responsável por entregá-las ao destino ou repassá-las a um outro grupo. Analisamos o HIGROP utilizando um modelo de mobilidade que reflete propriedades de cenários de emergência e verificamos por meio de simulações que o HIGROP teve até 65% de melhoria nas taxas de entrega, comparado aos algoritmos Epidêmico e Prophet, quando o *buffer* de armazenamento de mensagens é limitado e é escalável. O *overhead* de comunicação ficou praticamente constante em todos os cenários analisados.

Abstract

In critical and emergency scenarios, such as natural disasters, technological or man made, first-responders can building mobile ad hoc networks addressing the lack of network communication infrastructure. In a mobile ad hoc network nodes communicate without the need of a fixed access point. Perhaps, communication in such scenarios may become susceptible to long interruptions.

The Delay/Disruption Tolerant Networks are a proposal approach when communication is intermittent. The DTN support communication disruption storing messages and fowarding it when a connection occurs. Due the requirement of storing capability , the nodes must have available resources to store messages. The Epidemic and PROPHET routing protocols have good perfomance when the nodes has a high buffer storage capability, perhaps in the most mobile devices storage resources has tight storage resource.

This dissertation presents a disruptiont tolerant communication routing protocol, called HIGROP (*HIerarquical Group ROuting Protocol*). The HIGROP has as goal increase message delivery rate in a disruption network without having an impact on the communication overhead, optimizing the use of the nodes resource. To our best knowledge, HIGROP is the first protocol that build a hierarquical model to made message routing with in a network wich node has arbitrary movements. The HIGROP cluster neighbors nodes and elect a leader for each clustere. The messages are only forwarding to a leader node and leader become responsible to message delivery to the destination or to a foreign node cluster.

We compare HIGROP to other similar protocols using a group mobility model for such disasters scenarios in a simulation tool. We noticed that HIGROP has up to 65% better message delivery rate than Epidemic and Prophet protocols when message storage buffer is limited and it is scalable. The communication overhead keeps stable in all analyzed scenarios.

Sumário

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

Em cenários de emergência, tais como em desastres naturais, tecnológicos ou causados pelo homem, equipes de busca e resgate da região afetada podem utilizar soluções de redes *ad hoc* móveis (*Mobile Ad Hoc Networks* - MANETs) para suprir eventuais carências de infra-estrutura de rede de comunicação. MANETs são redes autônomas e auto-organizáveis, cujos nós podem se mover aleatoriamente e auto organizarem suas tabelas de roteamento [Manet, 2008].

Nesses cenários de emergência, devido a fatores como mobilidade, obstáculos e interferências, a conectividade fim-a-fim é altamente suscetível a interrupções. Isto faz com que sejam ineficazes os protocolos de roteamento nas MANETs atuais, que necessitam estabelecer um caminho fim-a-fim para comunicação entre os nós, como por exemplo os protocolos AODV e DSR [Jain et al., 2004].

Redes de emergência são aquelas construídas sobre cenários de desastres e têm propriedades tais como comunicação robusta e resiliente, não são necessariamente infra-estruturadas e principalmente oferecem comunicação de dados e não somente voz (como ocorre com rádios atuais) [Rao et al., 2007].

Tais propriedades podem ser satisfeitas usando uma rede de comunicação tolerante a atrasos e interrupções (*Delay/Disruption Tolerant Network* - DTN). Uma DTN é um tipo de rede adequada para suportar longos atrasos, como em redes de satélites, e interrupções de comunicação, como em redes de sensores sem fios. Para atender a esses requisitos, foi proposta uma nova sub-camada na arquitetura, chamada *bundle*, entre as camadas de aplicação e transporte do modelo de camadas OSI [DTNWG, 2008]. Essa camada é responsável por armazenar temporariamente os pacotes (*bundles*) caso não seja possível encaminhá-los ao destino.

Os protocolos de roteamento em DTNs diferem dos protocolos equivalentes de MANETs tradicionais pois suportam que ocorra desconexões entre os nós comunicantes. Dessa maneira, uma DTN pode ter melhor desempenho na taxa de entrega de men-

sagens, especialmente em redes com nós esparsos. Isso ocorrre devido às seguintes propriedades dos nós: comunicação baseada em mensagens assíncronas (*bundles*); não necessidade de caminhos fim-a-fim (os *bundles* podem ficar armazenados nos nós até que seja estabelecida uma conexão e então repassados); possibilidade de atrasos longos e variados; tolerância a altas taxas de erros [DTNWG, 2008].

Os diversos protocolos de roteamento em DTNs diferem no conhecimento que os nós têm sobre a rede. Alguns assumem que os nós não têm conhecimento sobre o estado da rede (conhecidos como protocolos estocásticos). Outros assumem que os nós possuem informações tais como topologia da rede, tempo médio entre encontros sucessivos de dois nós e estimação do congestionamento dos nós (chamados de protocolos determinísticos).

Os algoritmos estocásticos, chamados também de algoritmos epidêmicos, são aplicáveis quando a rede tem um comportamento aleatório e pouco pode ser inferido sobre posições futuras dos nós. Esses protocolos variam desde o simples repasse da mensagem para todos os nós com que se conseguir estabelecer contatos até a decisões baseadas no histórico, padrões de mobilidade ou outras informações [Vahdat e Becker, 2000].

O modelo de mobilidade de nós comumente utilizado nas análises de protocolos de roteamento DTN é o *Random Way Point*, no qual os nós se movimentam aleatoriamente em uma determinada área [Camp et al., 2002]. Este modelo, por ser totalmente aleatório, não representa o comportamento de um usuário real.

Os algoritmos epidêmicos se mostraram eficientes na entrega de mensagens em MANETs, pois através da mobilidade dos nós, uma mensagem pode atingir partes da rede que não estavam acessíveis anteriormente. Porém, o número de mensagens extras enviadas pela rede (*overhead*) para que uma mensagem atinja o destino aumenta proporcionalmente à quantidade de nós.

Espera-se que um protocolo de roteamento em DTNs tenha alta taxa de entrega de mensagens, mas um *overhead* de comunicação pequeno. Controlar o número de mensagens extras sem prejudicar a taxa de entrega das mensagens tem sido o objetivo de trabalhos recentes [Lindgren et al., 2003; Spyropoulos et al., 2005]. Portanto, existe um compromisso entre taxas de entrega e *overhead*, sendo esta decisão baseada no espaço para armazenamento de mensagens disponíveis nos nós.

Dessa forma, faz-se necessário para o desenvolvimento de um protocolo de roteamento em DTNs a avaliação do *overhead* de comunicação gerado pelo protocolo e, em uma análise que pode ser por simulação, utilizar um modelo de mobilidade que se aplica ao problema estudado.

1.1 Objetivos

Neste trabalho é proposto um protocolo de roteamento que busca minimizar o número de mensagens extras geradas pela rede na transmissão de uma mensagem da origem ao destino. Tal protocolo visa introduzir tolerância a interrupções de comunicação em redes móveis *ad hoc* utilizadas por equipes de resgate em cenários de emergência, como em catástrofes e desastres.

Nesses cenários, é comum que haja diversas equipes trabalhando em regiões de interesse e os integrantes de uma determinada equipe se movam unidos. Para validar nosso protocolo, foi proposto um modelo de mobilidade que representa essa forma de movimentação de equipes.

A fim de caracterizar melhor tais cenários, foi estendido o modelo de mobilidade *Reference Point Group Model* (RPGM), que representa o movimento aleatório de grupos de nós [Camp et al., 2002]. No RPGM, os movimentos dos nós de um grupo são baseados no caminho percorrido por um centro lógico do grupo, sendo utilizado para simular cenários de emergência como campos de batalha e catástrofes. Em nosso modelo foi acrescentado ao modelo RPGM, a possibilidade de representação de regiões de interesse e a classificação dos grupos em instituições. Num determinado momento cada grupo de nós tem uma probabilidade de ir para uma determinada região de interesse baseado nas necessidades da região naquele instante. Por exemplo, se uma região necessita de bombeiros essa região será visitada então pelos grupos classificados como bombeiros. Batizamos essa extensão do RPGM de *Mobility Model to Emergency Networks* (MME).

Explorando esse comportamento de mobilidade em grupo propomos um protocolo de roteamento hierárquico baseado em grupos, o qual foi denominado de *Hierarquical Group Routing Protocol* (HIGROP).

O HIGROP possui duas fases. Na primeira fase, em cada nó é construída uma tabela com informações dos nós que têm encontros mais frequentes. Utilizando essa tabela, um nó mantém dinamicamente sua lista de vizinhos utilizando o mecanismo de identificação de vizinhança. Para cada grupo de vizinhos é escolhido um líder a partir da tabela de vizinhos que o nó possui. Na segunda fase, é definida a política de roteamento de mensagens, que dependerá do conhecimento que o nó possui sobre o destino. Se o destino não faz parte dos vizinhos conhecidos do nó origem, então o envio da mensagem segue um princípio básico de hierarquia: mensagem somente é transmitida ao nó líder de um grupo e este é responsável por entregá-la ao destino ou repassá-la a um nó que não seja participante do grupo.

Avaliamos o protocolo proposto por meio de simulações utilizando o modelo de mobilidade MME, medindo sua eficiência em relação às métricas de taxa de entrega,

overhead de comunicação. A escalabilidade também foi mensurada comparando o HIGROP a outros protocolos semelhantes. O desempenho do protocolo foi validado em diferentes cenários de densidades de nós, que foram variados em número de nós e alcance de transmissão de rádio de cada nó. Observamos que o HIGROP é escalável e apresenta melhores taxas de entrega de mensagens quando o *buffer* de armazenamento de mensagens é limitado, sendo praticamente constante o *overhead* de comunicação.

1.2 Contribuições

Este estudo do problema de comunicação em cenários de emergência, o desenvolvimento e a avaliação de um protocolo tolerante a interrupções de comunicação trazem as seguintes contribuições:

- Especificação de uma extensão ao modelo de mobilidade RPGM, acrescentando características que melhor representam cenários de emergência, como regiões de interesse e instituições, nos quais baseados na necessidade de cada região os grupos de nós que atendam essa necessidade têm determinadas probabilidades de visitar.

- Especificação de um protocolo para redes tolerantes a interrupção de comunicação (denominado HIGROP), que utiliza o comportamento de movimentação em grupo dos nós para fazer o roteamento eficiente. Este protocolo utiliza uma política de escolha de líder entre cada grupo e o repasse eficiente de mensagens entre os nós participantes da rede.

- Implementação do protocolo proposto utilizando o simulador *Opportunistic Network Environment* (ONE) que permite simular redes com a conectividade intermitente.

- Avaliação do desempenho de protocolos de roteamento em DTNs, em relação a parâmetros como taxa de entrega, *overhead* de comunicação. Foi analisada a escalabilidade dos protocolos e o impacto da limitação de recursos nos dispositivos que compõem a rede.

Durante o desenvolvimento da dissertação, foram publicados resultados parciais em conferências nacionais. Ainda obtivemos publicações nacionais em temas desenvolvidos paralelos ao mestrado (vide Apêndice A).

1.3 Organização do Texto

Esta dissertação está organizada em sete capítulos. No Capítulo 2, apresentamos as questões inerentes às redes móveis *ad hoc* (MANETs). Identificamos os conceitos e as características básicas de MANETs. Em seguida, são apresentados os principais protocolos de roteamento em MANETs. Por fim, é discutido o problema de particionamento dessas redes relacionado à baixa densidade de nós que as compõem.

No Capítulo 3 são introduzidos os conceitos de redes tolerantes a interrupção de comunicação. É apresentada uma revisão da literatura sobre os protocolos de roteamento em DTNs e suas diferenças com o protocolo proposto.

As redes de emergências e o modelo de mobilidade proposto são discutidos no Capítulo 4. Apresentamos as características de redes de emergência e discutimos como as MANETs e DTNs podem ser aplicadas nessas redes. Discutimos os requisitos necessários em um modelo de mobilidade para que este possa representar cenários de emergência. Consideramos como cenário de emergência situações nas quais a infraestrutura local foi destruída, seja por desastres ecológicos, tecnológicos ou antropogênicos. Apresentamos o modelo comumente usado para representação de movimentação de grupos de nós, chamado *Reference Point Group Model* (RPGM). Apresentamos as extensões feitas ao RPGM para atender aos requisitos inerentes aos cenários estudados. Concluímos o capítulo mostrando as avaliações das características dos encontros dos nós comparando nossa extensão aos modelos de mobilidade *RandomWay-Point* e ao RPGM.

No Capítulo 5 apresentamos o protocolo HIGROP e descrevemos o funcionamento de cada fase do mesmo. Em seguida, apresentamos um algoritmo de identificação de nós vizinhos para formação de grupos (*clustering*), assim como a política de escolha de líder do grupo. Por fim, discutimos o modelo de replicação de mensagem de acordo com o conhecimento que o nó possui sobre o destino de uma mensagem.

No Capítulo 6 fazemos uma avaliação do desempenho e escalabilidade do protocolo proposto. Utilizando o modelo proposto no capítulo 4, avaliamos o HIGROP por meio de simulação comparando-o com protocolos semelhantes descritos no capítulo 3. Analisamos os protocolos em diversos cenários de rede: capacidade de armazenamento de mensagens, densidade de nós por área e modelos de mobilidade. Primeiramente, avaliamos o impacto da conectividade entre os nós participantes da rede variando o raio de transmissão de cada nó. Em seguida, observamos o impacto da capacidade de armazenamento de mensagens (*buffer*) e a escalabilidade do protocolo.

Apresentamos as conclusões da análise do HIGROP no Capítulo 7. Também propomos trabalhos futuros para roteamento em redes tolerantes a interrupção de comunicação.

Capítulo 2

Redes Móveis *Ad Hoc* - Roteamento e Particionamento

Este capítulo apresenta os conceitos e os principais protocolos de roteamento em redes móveis *ad hoc* (MANETs). A Seção 2.1 descreve as características e os conceitos de uma MANET. A seção 2.2 apresenta os protocolos de roteamento em MANETs. A Seção 2.3 discute o problema de particionamento de redes causado pela mobilidade dos nós. Em seguida, mostramos como o problema de particionamento causa interrupções de comunicação e faz com que os protocolos de roteamento atuais sejam ineficazes.

2.1 MANETs

As redes móveis *ad hoc*, do inglês *Mobile ad hoc Networks* - MANETs, surgiram da necessidade de se estabelecer conexões entre dispositivos móveis sem uma infra-estrutura previamente instalada. Inicialmente as redes *ad hoc* consistiram num projeto do departamento de defesa americano no começo dos anos 70, chamado *DARPA packet radio networks* [Jubin e Tornow, 1987], mas se tornaram um interessante objeto de pesquisa pela indústria da computação.

Uma MANET é um sistema autônomo composto por nós móveis que não dependem de nenhuma infra-estrutura para operar. Os nós se comunicam sem nenhum ponto de acesso controlando o acesso ao meio, necessitando para isto, que o nó destino esteja no alcance de transmissão do nó emissor ou que algum outro nó intermediário possa reencaminhar a mensagem. Desta forma, os pacotes são encaminhados de um nó ao outro até que atinjam seu destino. E como os nós podem estar em constante movimento, a topologia da rede está sempre sofrendo alterações.

As MANETs possuem algumas características que devem ser destacadas [Manet, 2008]:

1. **Auto-Organizável**: Podem ser instaladas rapidamente sem a necessidade de planejamento e cabeamento, além de dispensar o uso de dispositivos de interconexão, como comutadores, por exemplo. Consequentemente, uma MANET deve ser autônoma para configuração de seus parâmetros, como atribuição de endereço aos nós participantes da rede, roteamento, identificação de posição, controle de energia, entre outros.

2. **Robustez**: Podem resistir a desastres, como terremotos, pois se os dispositivos permanecerem intactos, pode-se ainda estabelecer a comunicação.

3. **Topologias Dinâmicas**: Como os nós são livres para se movimentar arbitrariamente, a topologia da rede pode mudar rápida e aleatoriamente.

4. **Banda Passante Restrita**: Enlaces de redes locais sem fio possuem, tipicamente, capacidades menores que os enlaces equivalentes em redes cabeadas.

5. **Limitação de Energia**: Os nós de uma MANET dependem, normalmente, de alguma fonte limitada de energia, como baterias. Isto faz com que a economia de energia seja um fator importante nessas redes.

6. **Limitações de Segurança**: Essas redes são mais sujeitas a problemas de segurança que redes cabeadas, pois as informações transmitidas em meios sem fios podem ser capturadas por nós maliciosos.

7. **Problemas de Roteamento**: Apesar da mobilidade dos nós proporcionar uma maior robustez, ela dificulta a localização física dos nós e, consequentemente, o encaminhamento de mensagens, pois seus endereços não estão associados a nenhuma localização geográfica.

A mobilidade é um dos principais atributos de uma MANET e também um dos principais desafios no desenvolvimento de aplicações *ad hoc*.

A análise de aplicações e protocolos de roteamento em MANETs é comumente feita utilizando simulação. Para simular a mobilidade são usados modelos sintéticos, que visam propor modelos de movimentação para os nós. Os modelos de mobilidade podem ter padrões de movimentação individual aleatória, mobilidade em grupo, movimento baseado em rotas pré-planejadas, dentre outros [Camp et al., 2002].

O modelo de mobilidade utilizado pode ter um grande impacto no desempenho do algoritmo de roteamento selecionado [Gerla et al., 2005]. Como a rede está em constante mudança de topologia surgem então as questões: como encontrar um destino e como rotear a mensagem para este destino. Para lidar com esta topologia dinâmica

da rede foram propostos diversos protocolos de roteamento que podem ser classificados em pró-ativos e reativos, os quais são explicados na seção seguinte.

2.2 Roteamento em MANETs

A topologia dinâmica das MANETs faz com que os protocolos de roteamento tenham que se adaptar às mudanças que ocorrem na rede para que as rotas entre pares de nós possam ser estabelecidas corretamente. Devido às características já mencionadas das MANETs, os protocolos de roteamento devem ser distribuídos, já que a rede não depende de nenhuma infra-estrutura, e também ser capazes de lidar com rápidas mudanças na topologia da rede. Com o aumento da densidade da rede, o custo das mensagens de controle dos próprios protocolos de roteamento (para calcular rotas, atualizar topologias, etc) também aumenta drasticamente [Kwon e Gerla, 2002].

[Hong et al., 2002] classificam os protocolos de roteamento em MANETs em três categorias, i) Roteamento plano (Seção 2.2.1), no qual todos os nós possuem as mesmas regras de atuação durante o roteamento, esses protocolos podem ainda ser classificados em pró-ativos e reativos; ii) Roteamento hierárquico (Seção 2.2.2), no qual uma camada virtual é criada para estabelecer uma hierarquia entre os nós, dessa maneira um *backbone* virtual entre nós "líderes" pode ser criado; iii) Roteamento geográfico (Seção 2.2.3), no qual o roteamento é baseado na localização geográfica dos nós. Utilizaremos essa classificação, pois nos permite identificar como os protocolos de roteamento enxergam a camada física da rede.

2.2.1 Roteamento Plano

Essa classificação de roteamento plano é dada aos protocolos que não criam uma camada virtual sobre a infra-estrutura de rede existente, tal que todos os nós participantes do processo de roteamento possuem as mesmas funções. Esses protocolos de roteamento são divididos em duas categorias, pró-ativos e reativos.

Os protocolos pró-ativos tentam avaliar continuamente as rotas, de modo que quando um pacote necessitar de encaminhamento, a rota já seja conhecida e possa ser utilizada imediatamente. Nesse caso, os nós mantêm uma ou mais tabelas com informações referentes à rede e respondem às mudanças na sua topologia propagando atualizações de modo a manter a consistência das informações da rede.

Essas atualizações são iniciadas por mecanismos de temporização, o que faz com que haja sempre um número constante de transmissões em andamento, mesmo quando a rede estiver em equilíbrio. A desvantagem dos algoritmos pró-ativos é a quantidade de atualizações da topologia dentro de um espaço de tempo, feita por meio de mensagens

do tipo *hello* enviadas em *broadcast* periodicamente. Se o número de nós aumentar, a quantidade de mensagens de atualização também aumentará, o que pode tornar tais algoritmos ineficientes visto que cada nó inunda a rede com as informações que possui. De fato, o número de mensagens de controle para manter as rotas é $O(n^2)$, sendo n o número total de nós na rede [Hong et al., 2002]. Os protocolos DSDV e WRP (*Wireless Routing Protocol*) são exemplos de protocolos pró-ativos [Perkins e Bhagwat, 1994; Murthy e Garcia-Luna-Aceves, 1996].

Os protocolos reativos determinam a rota sob demanda, ou seja, quando uma rota é requisitada, ele inicia algum procedimento de descoberta de rotas. Desta forma, o processo é iniciado por um pacote que necessite encaminhamento. Uma vez que a rota é descoberta, utiliza-se algum procedimento de manutenção de rota para que ela continue ativa. Como a chegada de um pacote necessitando encaminhamento é algo aleatório, estes protocolos não trocam mensagens a intervalos regulares, o que economiza banda passante e energia. Porém, estes algoritmos apresentam um maior atraso no encaminhamento das mensagens, justamente devido ao tempo necessário para se descobrir a rota. O AODV (*Ad hoc On demand Distance Vector*) e o DSR são exemplos de protocolos reativos [Perkins e Royer, 1999; Johnson e Maltz, 1996].

Conforme demonstrado em Oliveira et al. [2003], devido ao baixo consumo de energia, rápida adaptação às mudanças da rede e a não existência de laços, os algoritmos reativos, em especial o AODV, apresentam o melhor desempenho em cenários altamente dinâmicos . Já os protocolos pró-ativos são mais eficientes em redes nas quais muitos nós se comunicam entre si, pois o custo da reconstrução periódica de rotas é amortizado pela grande frequência das comunicações [Macedo, 2006].

2.2.2 Roteamento Hierárquico

Diversas abordagens de roteamento hierárquico foram propostas para MANETs [Pei et al., 1999], [Yu e Chong, 2005]. Nesses trabalhos, uma hierarquia (virtual) é construída utilizando a formação de agrupamentos (*clustering*) multi-nível, permitindo uma abstração da topologia da rede para roteamento. Esses algoritmos propõem métodos de agrupamento de nós em MANETs e políticas de repasse de mensagens entre os grupos que compõem a rede. Nos trabalhos apresentados, a formação de *clusters* para roteamento se mostrou eficiente, principalmente na quantidade de mensagens de controle enviadas pela rede. A vantagem da criação e manutenção de grupos é o mapeamento de nós vizinhos fisicamente em grupos lógicos com cada grupo possuindo um líder, dessa forma somente nós líderes são responsáveis pelo repasse de mensagem, aumentando a eficiência de propagação de mensagens pela rede.

As Seções 2.2.2.1 e 2.2.2.2 apresentam os algoritmos para a criação de grupos e os

algoritmos para escolha de nós líderes respectivamente.

2.2.2.1 Criação e Manutenção de Grupos

Os protocolos de roteamento hierárquico podem também ser classificados em pró-ativos ou reativos dependendo da filosofia de criação e manutenção de agrupamento que cada um utiliza. Se a manutenção do grupo é feita enviando mensagens com informações específicas periodicamente, então o protocolo é pró-ativo. O roteamento hierárquico reativo ocorre quando o grupo sofre manutenção somente quando requisitado. A maioria dos procedimentos de criação e manutenção de agrupamento é feita através do envio de pacotes com as informações específicas de cada protocolo, como lista de vizinhos, informações sobre líderes, etc.

Para minimizar o número de mensagens necessárias para a formação e manutenção do *cluster*, Kwon e Gerla [2002] propõem um protocolo de criação de grupos chamado *Passive Clustering* (PC). No PC não há a necessidade de mensagens de controle específicas para a manutenção do *cluster*, a informação sobre o papel do nó no grupo (2 b para quatro possíveis papéis: *initial*, *clusterhead*, *gateway*, *ordinary*) é adicionada em um campo reservado no cabeçalho do pacote MAC [Kwon e Gerla, 2002]. Dessa forma, como os pacotes MAC são transmitidos em difusão, todos os nós vizinhos recuperam a informação do cabeçalho MAC sem sobrecarga. Com isso o PC evita a inundação da rede com mensagens específicas extras; contudo, ele não foi desenvolvido para dar suporte ao roteamento hierárquico e somente cria a estrutura de *clustering* entre nós vizinhos.

Baseado no *Passive Clustering*, Cramer et al. [2004] apresentam um protocolo chamado "*On-Demand Group Mobility-Base Clustering*" (ODGMBC), que estende o PC ao permitir que sejam formados *clusters* com mais de um salto de distância (*multi-hop*). Com isso tem-se o agrupamento entre os nós vizinhos e também com os vizinhos destes nós. O ODGMBC consiste em verificar e contar os quadros recebidos da camada de acesso ao meio (MAC) de um determinado nó, e a partir de um limite pré-estabelecido reconhecer se o nó é vizinho ou não. Quando dois nós se reconhecem como vizinhos, cada um envia uma mensagem para o outro informando sobre esse reconhecimento e então o nó com o menor identificador assume a liderança e envia mensagens periodicamente informando seu estado de liderança. Dessa forma, somente a um subconjunto de nós da rede (líderes) é permitido fazer encaminhamento de mensagens, diminuindo assim o *overhead* de comunicação da rede.

Um algoritmo hierárquico determinístico para redes tolerantes a interrupções é apresentado em [Liu e Wu, 2007], onde é proposta a criação de uma árvore hierárquica para encaminhamento das mensagens. Os autores consideram que os nós são fixos ou que

suas trajetórias são estritamente repetitivas. Dessa forma, um nó sabe quando entrará em contato com outro nó.

Em nosso protocolo (HIGROP) utilizaremos uma política de agrupamento (*clustering*) reativo criando uma hierarquia entre os nós participantes da rede. O ODGMBC será usado como base para criação e manutenção do *clustering*. Porém, no HIGROP não há limitação no padrão de movimentação dos nós que compõem a rede. No Capítulo 5 detalhamos como é feito o agrupamento dos nós vizinhos visando diminuir o *overhead* de comunicação entre os nós.

2.2.2.2 Políticas para Escolha de Nós Líderes

Para atingir o objetivo de disseminação de mensagens de forma eficiente ao utilizar uma hierarquia virtual, uma política para a escolha do nó líder para cada grupo deve ser aplicada após a criação dos grupos de nós.

Diversos algoritmos para escolha de nó líder foram propostos na literatura, como o nó com menor identificador [Ephremides et al., 1987], nó com maior conectividade (grau) [Parekh, 1994], primeiro a se declarar líder [Kwon e Gerla, 2002]. Uma descrição do funcionamento de cada um desses algoritmos é apresentada a seguir.

Menor Identificador No algoritmo de escolha de líder com menor identificador cada nó possui um identificador único. Periodicamente, cada nó envia uma mensagem em difusão informando a lista dos outros nós que ele consegue escutar. Um nó que somente escuta nós com identificadores maior que o seu se declara líder e passa a informar sua liderança. Um nó que escuta a mensagem de dois líderes atua como um gateway entre os dois grupos.

Maior conectividade Cada nó envia uma mensagem por difusão a lista dos nós que consegue escuta (incluindo ele mesmo). Um nó é eleito líder se ele possui o maior conectivade grau) entre os seus vizinhos que ainda não possui um líder. Um nó é dito como "*descoberto*" se ele já conhece seu líder.

Primeiro a se declarar líder Kwon e Gerla [2002] propuseram um novo algoritmo para eleição de líder no qual todos os nós são potenciais líderes. Quando um nó tem uma mensagem para repassar ele se delcara líder e adiciona essa condição no cabeçalho da mensagem. E qualque outro nó que não tenha recebido a mensagem de um nó líder pode se declarar líder e informar os nós que estão na sua área de cobertura (alcance do rádio).

Em nosso trabalho, utilizamos o algoritmo de escolha de líder com menor identificador, essa abordagem apesar de simples, facilita a manutenção e o gerenciamento do agrupamento de nós.

2.2.3 Roteamento Geográfico

Com o advento de dispositivos móveis portando sistemas GPS (*Global Positioning System*) é possível saber com determinada precisão a própria localização de um tal dispostivo. Essa informação sobre a localização de um nó pode ser usada para fazer o roteamento eficiente de mensagens. Contudo, em redes móveis a localização do nó pode ser inexata devido a mobilidade. Por exemplo, um nó A envia a informação com sua localização em um dado instante para um nó B e depois se move. A localização que o nó B tem sobre A neste caso estará inconsistente. Nos protocolos de roteamento geográfico é assumido que os nós da rede conhecem suas coordenadas geográficas [Hong et al., 2002].

2.3 O Problema de Particionamento da Rede

Em todos os protocolos de roteamento *ad hoc* é assumido que a rede é totalmente conectada e há um caminho fim-a-fim entre qualquer par de origem e destino. No entanto, dependendo de como os nós se movem e da densidade da população de nós, o tempo de entrega da mensagem pode variar de segundos a até mesmo dias. Se não há um caminho fim-a-fim em um determinado instante, esses protocolos falham na entrega da mensagem naquele momento.

De fato, Xue e Kumar apresentam um estudo teórico provando que para a rede ser assintoticamente conectada é necessário que cada nó tenha $\Theta(\log n)$ vizinhos, sendo n o número de nós na rede. O teorema 1 formaliza essa prova [Xue e Kumar, 2004].

Teorema 1 *Seja S um quadrado no $\Re^2$, com n nós uniformemente distribuídos em S. Seja $\mathcal{G}(n, \phi_n)$ a rede em S e com cada nó possuindo ϕ_n vizinhos. É suficiente e necessário $\Theta(\log n)$ vizinhos para $\mathcal{G}(n, \phi_n)$ ser assintoticamente conectada. Precisamente, há duas constantes $0 < c_1 < c_2$ tal que:*

$\lim_{n\to\infty} Pr\{\mathcal{G}(n, c_1\phi_n)$ *é desconectada*$\} = 1$ *e*

$\lim_{n\to\infty} Pr\{\mathcal{G}(n, c_2\phi_n)$ *é conectada*$\} = 1$

Contudo, na prática não é possível garantir que em uma MANET cada nó terá $\Theta(logn)$ vizinhos. Além da mobilidade que pode causar a dispersão dos nós, outros fatores como interferência e obstrução de sinal também podem afetar a conectividade da rede.

A Figura 2.1 ilustra dois nós tentando estabelecer comunicação entre si, numa rede particionada e com atraso de comunicação que pode ser de horas ou mesmo dias. Como um caminho fim-a-fim não pôde ser estabelecido, é necessário um mecanismo de roteamento e transmissão de dados que suporte interrupção de comunicação e longos atrasos.

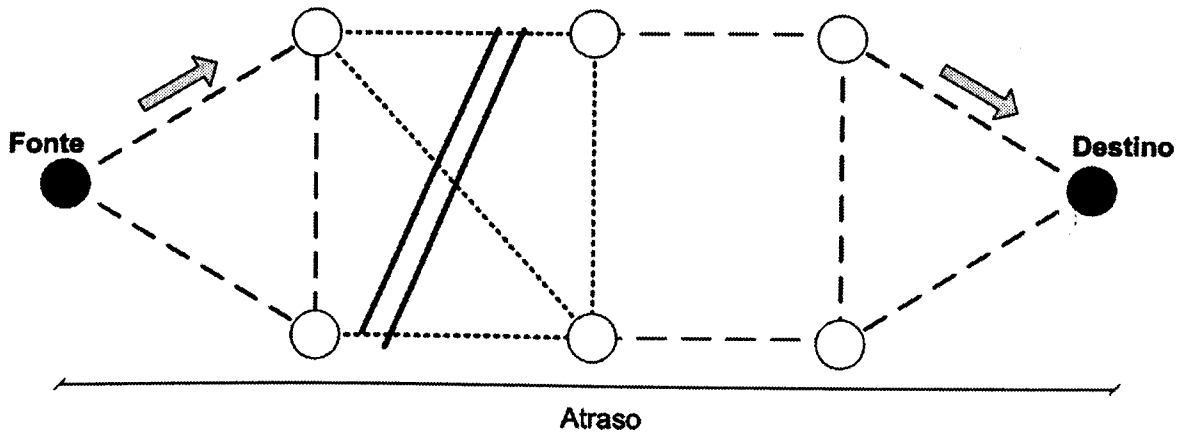

Figura 2.1. Rede *ad hoc* particionada em duas sub redes.

Em alguns casos a quebra do caminho pode ser "evitada" realizando-se previsões de quando uma rota irá falhar e assim computar rotas alternativas antes que a primeira falhe. Esta técnica é conhecida como *Link Prediction* e pode ser aplicada quando os nós apresentam um determinado grau de regularidade em suas movimentações. Por exemplo, em viagens de carro é comum manter a mesma direção e velocidade por um certo período de tempo e, desta forma, pode-se "prever", com certa probabilidade, o estado da rede no futuro. Em [Su et al., 2000], é proposto o protocolo de roteamento *Distance Vector with Mobility Prediction* (DV-MP), que utiliza como métrica o tempo limite do enlace (*Link Expiration Time* - LET), cujo cálculo é baseado no vetor de distância e velocidade entre dois nós. Desta forma, a rota é estabelecida entre os nós com maior LET, por esta ser prevista como estável por um tempo maior, minimizando assim a desconexão causada pela mobilidade.

Quando ocorre o particionamento da rede *ad hoc*, pode-se tentar continuamente restabelecer a conexão ou então adaptar-se a essa desconexão temporária. Uma abordagem que vem sendo investigada é a combinação dos conceitos de redes tolerantes a interrupção juntamente com os conceitos de roteamento em MANETs [Fall e Farrell, 2008]. Em uma rede tolerante a interrupções de comunicação, os dados são encapsulados e armazenados em pacotes chamados *bundles* e transmitidos somente quando a conectividade estiver presente. Essa política de encaminhamento é comumente chamada de transmitir-armazenar-repassar as mensagens. Essa combinação faz com que

os nós possam atuar como roteadores dos pacotes quando há conexão e também como "armazenadores" de dados (*bundles*) quando a rede está particionada. As DTN são discutidas no Capítulo 3.

2.4 Conclusão

Este capítulo apresentou uma revisão da literatura do roteamento em redes móveis *ad hoc* e o problema de particionamento de rede causado principalmente pela mobilidade. As MANETs são redes sem fio criadas onde não há uma infra-estrutura prévia e que em geral cada nó da rede possui os seus interesses, pois a rede pode ser formada por um conjunto heterogêneo de elementos.

Os protocolos de roteamento em MANETs podem ser classificados de acordo com o modo como utilizam a estrutura física da rede. No roteamento plano, os protocolos pró-ativos precisam manter as rotas para o mesmo número de nós que há na rede, mesmo que não precisem das rotas. Essa política diminui o atraso no envio das mensagens, porém caso a rede seja formada por milhares de nós o custo de armazenamento e processamento da tabela de rotas se torna alto demais. Os protocolos reativos descobrem a rota quando necessário. Isso diminui o *overhead* de mensagens de controle mas introduz um atraso no envio das mensagens. No roteamento hierárquico, uma hierarquia virtual é construída utilizando o agrupamento dos nós vizinhos para diminuir o *overhead* de comunicação necessário para se fazer a descoberta e manutenção de rotas.

Todos os protocolos de roteamento em MANETs apresentados no capítulo assumem que o caminho fim-a-fim seja conhecido e esteja estabelecido durante todo o processo de comunicação entre dois nós, caso esse seja interrompido as mensagens que forem enviadas serão descartadas pelos nós. O problema do particionamento de redes é causado nas MANETs principalmente devido a mobilidade. Para manter a conectividade da rede Xue e Kumar provam a necessidade de que cada nó tenha $\Theta(\log n)$ vizinhos, sendo n o número de nós na rede. Entretanto, em uma rede onde os nós podem se mover arbitrariamente não é possível garantir essa vizinhança em cada nó.

Devido à impossibilidade de se evitar o particionamento da rede, alguns protocolos tentam prever o momento em que haverá a conexão (*Link predicition*), contudo essa previsão só é possível se os nós possuem movimentos regulares. Outra forma de se evitar a perda de mensagens em caso de desconexão é utilizar protocolos de roteamento DTN, que suportam interrupções de comunicação: armazenam as mensagens durante a interrupção e as repassam quando a conexão é estabelecida.

Nesta Dissertação, propomos um protocolo de roteamento que combina os conceitos de DTNs e roteamento hierárquico em MANETs. Os nós armazenam as mensagens

quando não há conexão ativa e as repassam para outro nó utilizando um modelo hierárquico e uma métrica probabilística que o novo nó tenha para encontrar o destino.

Capítulo 3

Redes Tolerantes a Interrupções de Comunicação

Este capítulo apresenta e descreve os conceitos, a arquitetura e os principais protocolos de roteamento em redes tolerante a interrupções. Na seção 3.1 apresentamos uma visão geral dos conceitos em redes tolerantes a interrupção, identificamos as necessidades que este tipo de rede possui e as limitações das redes tradicionais. Na seção 3.2 descrevemos a arquitetura de uma rede tolerante a interrupção. Na seção 3.3 discutimos os protocolos de roteamento atuais, as topologias de rede ao qual se aplicam e as métricas utilizadas na avaliação de desempenho desses protocolos.

3.1 Redes Tolerantes a Atraso e Interrupção

Como apresentado no Capítulo 2, os protocolos de roteamento atuais necessitam da existência de um caminho fim-a-fim entre a origem e o destino. Além disto, o desempenho degrada consideravelmente com o aumento do número de saltos em uma comunicação sem fio Ott et al. [2006].

Características como baixa densidade de nós, altas taxas de erros de comunicação, alta latência, limitações de banda e longevidade de nós criam cenários desafiadores de rede, que na literatura são chamados de *Challenged Networks* [Fall, 2003]. Essas características das redes fazem com que as aplicações nesses cenários tenham um comportamento diferente do que teriam em uma rede tradicional.

As redes tolerantes a interrupções ou atrasos (*Disruption-Delay Tolerant Networking* - DTN) surgiram para possibilitar a comunicação em *Challenged Networks* [Fall, 2003]. O conceito de DTN originou-se no projeto *Inter-Planetary Network* (IPN) com o objetivo de dar suporte a comunicações intermitentes e com longos atrasos em redes que interliga pontos a longas distâncias (ex. redes interplanetárias) [Cerf et al., 2001].

Para isso, Cerf et al. propuseram uma arquitetura capaz de suportar interrupções de comunicação utilizando armazenamento temporário de mensagens e reencaminhamento quando do retorno de conectividade. Foi definida uma nova camada (denominada *bundle*) para a arquitetura de rede.

Os conceitos de DTN podem ser aplicados não somente em redes interplanetárias mas também em outros tipos de redes que apresentem intermitência de comunicação, como em redes móveis ou redes de sensores sem fios. Para garantir interoperabilidade o RFC 4838 [Cerf et al., 2007] define a arquitetura DTN de forma independente da tecnologia de rede que estiver dando suporte a comunicação. O documento define a camada *bundle* como uma camada de sobreposição à camada de transporte e as demais camadas inferiores do modelo OSI.

A camada *bundle* visa superar os problemas associados às características relatadas anteriormente ao utilizar a técnica de armazenagem-e-repasse para comutação de mensagens. Mensagens (chamada de *bundles*) recém chegadas em um nó DTN que não tenha conexão são armazenadas e enfileiradas na camada *bundle*. Os *bundles* são repassados para outros nós de acordo com o protocolo de roteamento em uso somente quando a conexão voltar. Segundo Warthman, os nós em uma DTN necessitam de armazenamento persistente para suas filas de mensagens, pelas seguintes razões [Warthman, 2003]:

- Um enlace de comunicação para o próximo nó da rota pode ficar indisponível por um longo período de tempo;
- Um nó de um par de nós comunicantes pode enviar ou receber dados muito mais rápidamente que o outro nó, sendo necessário armazenamento temporário para acomodar diferenças de capacidade.
- Uma mensagem já transmitida a um nó intermediário da rota pode precisar ser retransmitida se um erro ocorrer neste nó intermediário.

Nos atuais protocolos de transporte, se o descarte de pacotes ou o atraso forem muito altos, o TCP pode acabar finalizando a conexão, o que pode levar a falhas as aplicações. Já o UDP não possui garantia de entrega nem mesmo garantia se as mensagens serão recebidas na ordem em que foram enviadas, inexistindo controle para verificar se o destino foi alcançado ou não.

A camada *bundle* suporta tal intermitência na comunicação ao isolar o atraso através da técnica de armazenagem-e-repasse, ou seja, um nó armazena uma mensagem até que seja possível repassá-la a outro nó. Há diferentes tipos de protocolos de roteamento DTN que definem o repasse da mensagem. Esses protocolos variam na política utilizada para fazer repasse de mensagens, que de acordo com a características da aplicação

e o modelo de mobilidade envolvido escolhem para que nós vão repassar a mensagem para que essa chegue ao destino. Por exemplo, movimentos de planetas e satélites são previsíveis, assim os protocolos de roteamento para essas aplicações têm conhecimento sobre quando ocorrerão as conexões entre os nós da rede (roteamento determinístico). Movimentos de soldados em um campo de batalha ou de equipes de resgate em cenários de emergência podem ser arbitrários, os protocolos podem tentar repassar uma mensagem para todos os nós de forma epidêmica na esperança que a mensagem atinja o destino (roteamento estocástico).

3.2 A Arquitetura DTN

A arquitetura DTN acrescenta uma camada na pilha de camadas da Internet (modelo OSI), chamada *bundle* [Fall, 2003] que fica acima da camada de transporte. A rede DTN pode ser formada por diversas sub-redes heterogêneas entre si, ou seja, cada sub-rede pode possuir tecnologia e protocolos de comunicação das camadas inferiores distintos (IP, ATM, etc) tendo em comum somente a camada *bundle*. Portanto, uma DTN é o conjunto de sub-redes que compartilham a camada *bundle*, formando uma rede sobreposta (*overlay*) à essas sub-redes [Warthman, 2003].

A Figura 3.1 apresenta as pilhas de protocolos da Internet e de uma rede DTN. Observe que os protocolos de comunicação da rede são específicos para cada sub-rede, que variam de acordo com o ambiente tecnológico em que estão operando, mas todas as sub-redes precisam possuir a camada *bundle*, que irá fazer a interface entre a aplicação e as diversas tecnologias de comunicação entre as sub-redes.

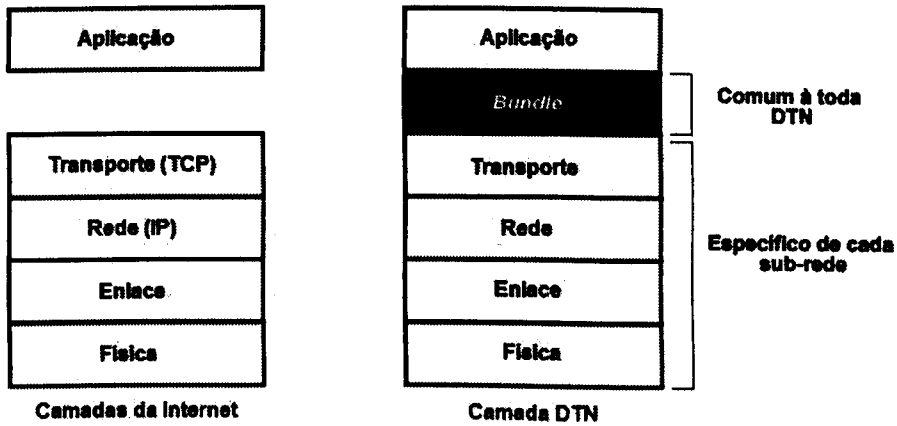

Figura 3.1. Pilha de protocolos da Internet e de uma DTN.

Os *bundles* podem ter tamanhos arbitrários e possuem três componentes: dados

da aplicação origem; controle de informação (provido pela origem descrevendo como processar e armazenar o dado); e o cabeçalho, criado pela camada *bundle*.

Em uma DTN, um nó é uma entidade que possui a camada *bundle*. Os nós podem ser *hosts*, roteadores ou *gateways*. Sendo origem, destino ou repassadores de *bundles*:

- *Host*

  Enviam ou recebem os *bundles*, mas não os repassam.

- Roteador

  Repassam os *bundles* dentro de uma mesma sub-rede DTN, podendo também ser um *host*. Os nós roteadores serão responsáveis por manter o armazemamento da fila de *bundles* até que possa repassá-los.

- *Gateway*

  Repassa os *bundles* entre as sub-redes DTN, podendo também ser um host. Os nós gateways devem saber fazer transferências quando as tecnologias são diferentes, ex.: passar de um nó *wi-fi* (802.11) para um nó *Ethernet* (802.3).

Quando os nós seguem caminhos previsíveis, como na movimentação de satélites, os contatos podem ser agendados já que os nós podem prever quando irão se encontrar e já se prepararem para suas futuras sessões de comunicações. Desta forma, os nós devem armazenar os dados até que sejan encaminhados completamente para o próximo nó da rota.

Uma maneira de se estabelecer a comunicação entre os nós DTN é através de contatos oportunísticos. Tão logo um nó restabeleça comunicação com outro nó é feita a transferência dos *bundles* armazenados, e assim sucessivamente até os *bundles* alcançarem os seus destinos finais. Existem diversas otimizações de como estes *bundles* podem ser encaminhados, discutidas na seção 3.3.

3.3 Roteamento em DTN

O roteamento em DTNs cria novos desafios se comparado ao roteamento em redes tradicionais, visto que há incertezas sobre a duração da conexão entre os nós. Os diversos protocolos de roteamento em DTNs diferem no conhecimento que os nós têm sobre a rede. Alguns assumem que os nós não têm nenhum conhecimento sobre o estado da rede (conhecidos como protocolos estocásticos). Outros assumem que os nós possuem informações tais como topologia da rede, tempo médio entre encontros sucessivos de dois nós e estimação do congestionamento dos nós (chamados de protocolos determinísticos).

Os algoritmos determinísticos baseiam-se nas informações que um nó tem sobre a rede, sendo utilizados quando é possível inferir quando haverá conectividade entre os nós [Handorean et al., 2004; Jain et al., 2004; Liu e Wu, 2007; Merugu et al., 2004]. Em todas essas abordagens determinísticas, o caminho fim-a-fim é estabelecido antes do envio das mensagens, sendo dependente do momento em que foi prevista a possibilidade de conexão. No entanto, na maioria dos casos de redes *ad hoc* móveis não é possível prever a movimentação dos nós da rede.

Os algoritmos estocásticos são aplicáveis quando a rede tem um comportamento aleatório e pouco pode ser inferido sobre posições futuras dos nós. Esses protocolos variam desde o simples repasse da mensagem para todos os nós que se conseguir estabelecer contatos até a decisões baseadas no histórico, padrões de mobilidade ou outras informações [Vahdat e Becker, 2000; Lindgren et al., 2003; Grossglauser e Tse, 2002; Spyropoulos et al., 2005].

Todos os algoritmos de roteamento têm em comum a necessidade de que os nós intermediários tenham a capacidade de armazenamento para os *bundles* (*buffer*) até que possa repassá-los a outros nós. A política de armazenagem e repasse dos *bundles* é definida pelo protocolo de roteamento. A Figura 3.2 ilustra o roteamento de mensagens entre dois nós de sub-redes diferentes. Porém todos os nós devem possuir espaço reservado para armazenamento persistente dos *bundles*.

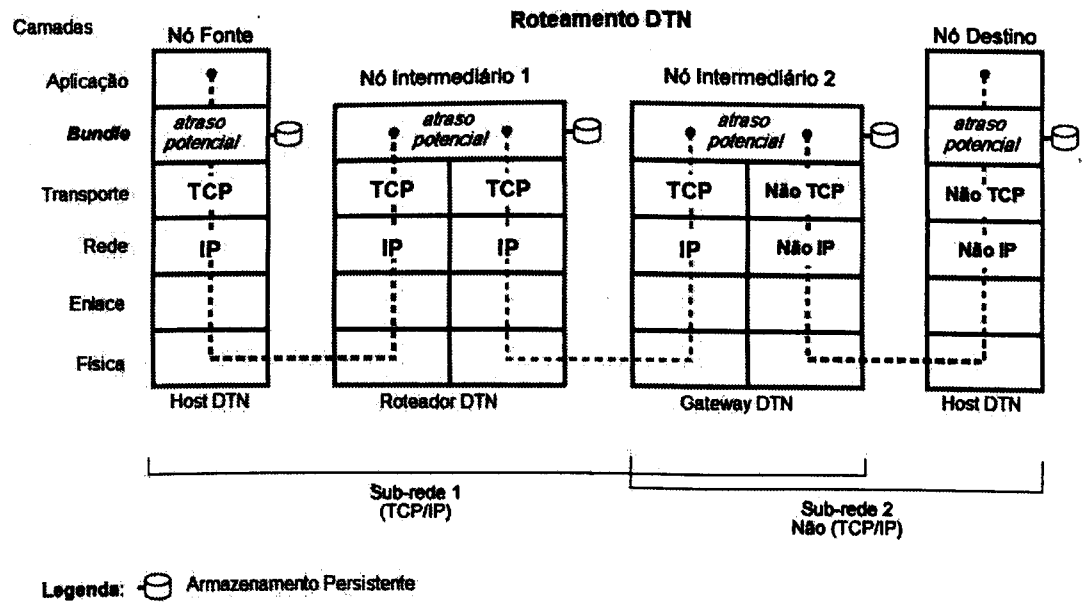

Figura 3.2. Roteamento entre nós com tecnologias de rede diferentes.

As métricas utilizadas para avaliação de desempenhos dos diversos protocolos de roteamento em DTNs são a taxa probabilidade de entrega, que é a taxa de mensagens

que alcançaram o destino; o número de mensagens extras enviadas na rede para que cada mensagem chegue ao destino final e o atraso fim-a-fim de cada mensagem.

Essa dissertação de mestrado tem como resultado a definição de um protocolo de roteamento estocástico que organiza os nós hierarquicamente e as mensagens são encaminhas somente pelos nós líderes até que chegue ao destino final. Portanto, apresentamos nas Seções seguintes uma visão geral dos protocolos de roteamento em DTNs, classificando-os em determinísticos e estocásticos. Uma revisão completa destes protocolos é apresentada em [Jain et al., 2004] e [Zhang, 2006].

3.3.1 Roteamento Determinístico

No roteamento determinístico todos os nós possuem informações sobre a rede, como topologia e previsão do momento em que irá ocorrer conexão entre os nós comunicantes.

O roteamento determinístico pode ser aplicado em situações tais como na troca de mensagens entre satélites orbitais ou mesmo no provimento de acesso à internet e email em regiões remotas usando o horário programado dos ônibus que passam pela região para recolher e entregar as mensagens (os ônibus contêm nós DTN).

O grande problema nesse tipo de algoritmo é que para se conhecer o exato momento em que ocorrerá a conexão é necessário haver sincronização de relógio entre os nós participantes, o que ainda é um problema em aberto. A Figura 3.3 ilustra um esquema no qual dois satélites que precisam trocar informações e devido a distância o atraso de comunicação fim-a-fim pode ser de minutos ou mesmo horas. Como o movimento de ambos os satélites são conhecidos, se o nó fixo estiver com o relógio sincronizado com o satélite, ambos saberão o momento em que a mensagem precisa ser enviada para que ela possa ser recebida corretamente.

Foram propostos na literatura diversos protocolos de roteamento em DTNs que assumen que os nós têm conhecimento sobre a topologia da rede e o momento em que ocorrerão as conexões [Handorean et al., 2004; Jain et al., 2004; Liu e Wu, 2007].

Entretanto, somente em [Liu e Wu, 2007] é apresentado um protocolo de roteamento hierárquico utilizando a formação de agrupamentos e escolha de nós líderes para fazer o roteamento das mensagens. Os autores mostram que através da formação de grupo é possível uma diminuição significativa no número de mensagens que tem que ser enviadas na rede até que a mesma chegue ao destino (*overhead* de comunicação). Porém, o protocolo proposto por Liu e Wu é específico para redes nas quais os nós tem movimento pré-determinado e repetitivos, ou seja, conhece-se o padrão de mobilidade dos nós

Em [Handorean et al., 2004] é apresentado um algoritmo para escolha de um caminho para mensagens que depende da informação que o nó tem sobre a rede. São

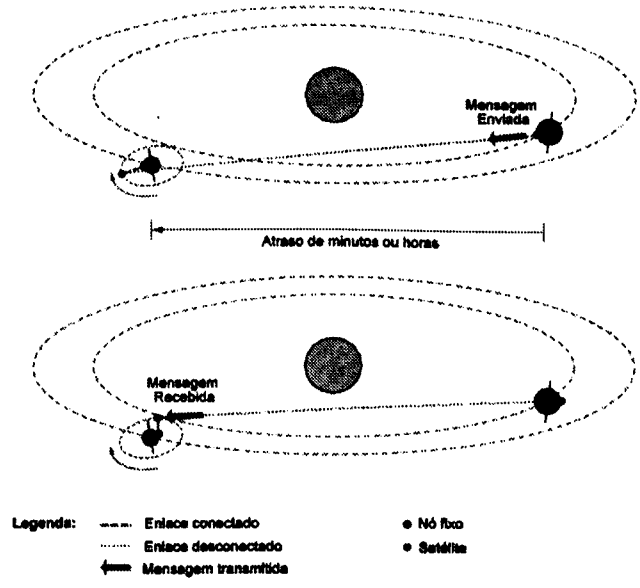

Figura 3.3. Envio de mensagens com o contato agendado.

apresentados três casos:

(i) Quando há conhecimento global das características de movimentação e disponibilidade dos nós em função do tempo. A partir desse conhecimento é construída uma árvore e o caminho final é a sub-árvore com menor número de saltos para alcançar o destino.

(ii) O protocolo assume que inicialmente não há conhecimento nenhum sobre o estado da rede nos nós. Esta informação é aprendida com as trocas de informações (movimentação, velocidade) entre os nós vizinhos de maneira que os caminhos sejam selecionados baseados nesta informação parcial disponível.

(iii) Uma melhora no segundo caso pode ser alcançada armazenando as informações passadas, isto é, armazenando a sequência dos nós pela qual uma mensagem já passou.

Em Jain et al. [Jain et al., 2004] são propostos vários algoritmos baseados em quais informações da rede estão disponíveis, como topologia e demanda de tráfego. Para isto, são definidos quatro "oráculos de conhecimento", cada um representando um tipo específico de conhecimento. Baseado em qual oráculo esteja disponível, os autores apresentam um algoritmo de roteamento correspondente.

Em todas estas abordagens determinísticas o caminho fim-a-fim é estabelecido antes do envio das mensagens, sendo dependente do tempo em que foi prevista a possibilidade de conexão. No entanto, na maioria dos casos de redes *ad hoc* móveis não é possível ter uma previsão sobre a movimentação dos nós da rede.

3.3.2 Roteamento Estocástico

Os algoritmos desta categoria são aplicáveis quando pouco ou nenhum conhecimento sobre posições futuras dos nós pode ser inferido. Esses protocolos variam desde o simples repasse da mensagem para todos os nós que se conseguir estabelecer contatos a decisões baseadas no histórico, padrões de mobilidade e outras informações.

No geral, nas aplicações em MANETs não é possível prever o tempo em que acontecerá uma conexão entre dois nós. Por esse motivo, os trabalhos que focam utilizar os conceitos de roteamento em DTNs para o problema de particionamento de rede em MANETs são epidêmicos em sua essência.

Quando a largura de banda e o espaço de armazenamento persistente das mensagens (*buffer*) são infinitos, o protocolo Epidêmico é ótimo em relação à taxa de entrega e ao atraso. Devido a isso, o protocolo Epidêmico é comumente utilizado como base de comparação com outros protocolos de roteamento. Entretanto, capacidade de armazenamento em *buffer* e largura de banda infinitos não refletem a realidade dos nós.

A mobilidade dos nós participantes de uma MANET nem sempre é totalmente aleatória. Por exemplo, a movimentação de estudantes em um campus; de equipes de resgate em cenários de emergência, tendem a ter um padrão de mobilidade.

Com isso, os protocolos podem, por exemplo, calcular a probabilidade que um determinado nó tem de encontrar o destino baseado no histórico de encontros. Dessa forma é possível diminuir o número de mensagens enviadas pela rede em relação ao protocolo Epidêmico.

Nas seções seguintes destacamos as melhorias do protocolo proposto nessa dissertação em relação aos existentes na literatura. Em especial, em relação ao protocolo Epidêmico [Vahdat e Becker, 2000], por ser uma base de comparação na análise de desempenho de protocolos de roteamento DTN, e ao Prophet [Lindgren et al., 2003], por ser o protocolo de roteamento atualmente utilizado na implementação oficial do protocolo *bundle* pelo grupo de pesquisa DTN [DTNWG, 2008]

3.3.2.1 Epidêmico/Parcialmente Epidêmico

Vahdat e Becker [2000], antes mesmo da consolidação da arquitetura DTN, propuseram um protocolo de roteamento epidêmico para redes *ad hoc* parcialmente conectadas. Nesse protocolo, o nó origem difunde a mensagem para todos os seus vizinhos e cada um destes por sua vez repassa a mensagem para seus vizinhos.

No protocolo Epidêmico, em cada mensagem é incluído um número máximo de saltos (*Limit Hop Count*) e um tempo de vida (*time to live*/TTL) da mesma. A mensagem é difundida na rede até que atinja o número máximo de saltos ou enquanto durar o TTL, quando este for especificado. Dessa forma, a mensagem é distribuída

para todos os nós alcançáveis.

Para evitar redundância de mensagens em um nó, quando um par de nós estabelece contato, primeiramente eles trocam uma lista com o sumário das mensagens que possuem armazenadas. Cada nó determina quais mensagens o outro nó não possui e então as envia. A Figura 3.4 apresenta essa troca de mensagens entre dois nós em função do tempo, em duas fases.

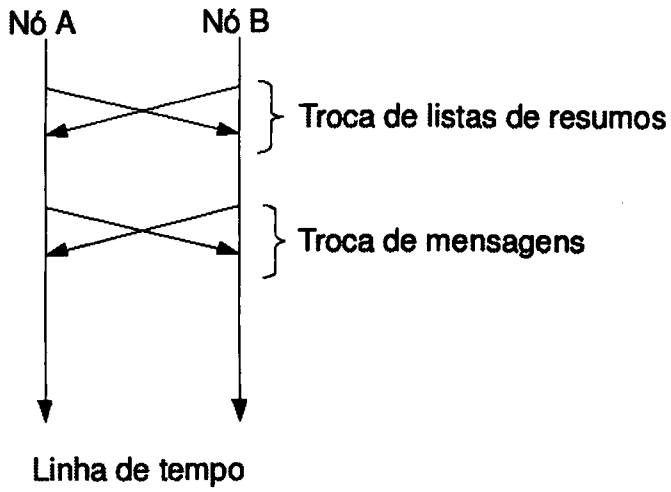

Figura 3.4. Fases de troca de mensagens no protocolo Epidêmico.

Com a mobilidade dos nós e, portanto, com a variação da conectividade da rede, espera-se que as mensagens atinjam partes da rede que não estavam acessíveis (outras sub-redes) no momento do envio.

Algoritmos epidêmicos se mostraram eficientes na entrega da mensagem, porém o número de mensagens extras enviadas pela rede aumenta proporcionalmente à quantidade de nós. Isso implica na necessidade de que os nós tenham uma capacidade de armazenamento de mensagens suficientemente grande para suportar o tráfego da rede.

Em [Grossglauser e Tse, 2002] é utilizada uma política extrema de contenção de replicação de mensagens, na qual a origem retém a mensagem e somente a repassa para o nó destino, caso ocorra uma conexão com o destino. Essa abordagem é conhecida como *two-hop fowarding* e claramente tem *overhead* mínimo mas pode ter alta latência ou caso não ocorra conexão entre a origem e o destino a mensagem não é entregue.

Portanto, existe um compromisso entre o tamanho do *overhead* de comunicação e o tempo de entrega das mensagens. Diminuir o *overhead* implica no aumento do atraso. Por outro lado, algoritmos com *overhead* grande podem causar congestionamento de rede, além de exigirem mais recursos dos nós participantes da rede.

O algoritmo epidêmico mostrou-se eficiente na entrega das mensagens à custa de

grande aumento de *overhead* de comunicação na rede. Visando diminuir esse *overhead*, propomos uma alternativa utilizando o agrupamento de nós para fazer o roteamento eficiente das mensagens. Uma mensagem só é encaminhada a um nó especial de um grupo e este nó é responsável por encaminhar a mensagem ao destino ou a um grupo diferente. Portanto, as mensagens não são replicadas entre nós de um mesmo grupo.

3.3.2.2 Baseados no Histórico e na Probabilidade de Entrega

Ao invés de replicar as mensagens por todos os nós da rede, uma alternativa é estimar a probabilidade que determinado nó tem de entregar a mensagem. Dessa forma, um nó pode decidir se encaminha a mensagem para outro nó ou se aguarda um próximo contato que tenha melhores chances de encontrar o destino da mensagem.

Um protocolo de roteamento probabilístico chamado Prophet (*Probabilist Routing Protocol using History of Encounters and Transitivity*) é proposto em [Lindgren et al., 2003]. O Prophet estima uma métrica probabilística denominada "previsora de entrega" $P_{(A,B)}$ sempre que um nó A estabelece uma conexão com um nó B. Essa métrica indica quais as chances um determinado nó (no caso, A) tem de entregar uma mensagem ao destino (no caso, B). As mensagens são repassadas somente para nós com maior previsibilidade de entrega ao destino. A Figura 3.5 mostra esse repasse de mensagem do Prophet em função do tempo.

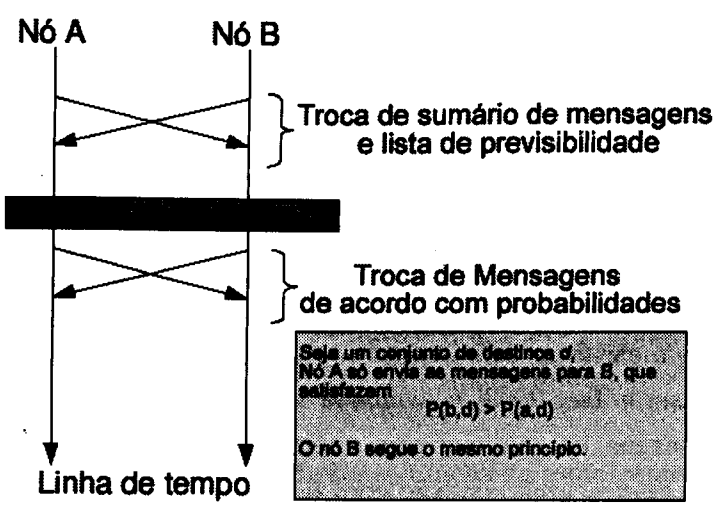

Figura 3.5. Fase de troca de mensagens no protocolo Prophet.

No Prophet, o cálculo da "previsora de entrega" $P_{(A,B)}$ possui três fases e P_{init}, θ e γ são parâmetros configuráveis do algoritmo e $P_{(A,B)old}$ a previsora de entrega antiga entre um par de nóss. Na primeira fase, quando o nó A encontra o nó B, $P_{(A,B)}$ é atualizado como mostrado na Equação 3.1, sendo $P_{init} \in [0,1]$ a probabilidade inicial

no primeiro encontro de um par de nós. Na segunda fase, os nós trocam informações sobre outros nós que já conhecem. Com essa propriedade de transitividade o nó A atualiza a previsibilidade para um nó C que B já conhecia. A Equação 3.2 mostra essa transitividade, sendo $\theta \in [0, 1]$ a constante que indica qual o impacto da transitividade na "previsora de entrega". Na terceira fase, a cada período k a previsora de entrega para os nós conhecidos é atualizada (eq. 3.3), sendo $\gamma \in [0, 1)$ uma constante de envelhecimento e k o tempo que passou desde que ocorreu o último encontro.

$$P_{(A,B)} = P_{(A,B)old} + (1 - P_{(A,B)old}) \times P_{init} \quad (3.1)$$

$$P_{(A,C)} = P_{(A,C)old} + (1 - P_{(A,C)old}) \times P_{A,B} \times P_{B,C} \times \theta \quad (3.2)$$

$$P_{(A,B)} = P_{(A,B)old} \times \gamma^k \quad (3.3)$$

O Prophet possui um compromisso na escolha de um valor inicial (P_{init}) para o cálculo da "previsora de entrega". Se esse for baixo demais, atuam como meros epidêmicos; se for alto demais, o atraso aumentará [Spyropoulos et al., 2005].

Além disso, o Prophet vai tornando epidêmico à medida com que os nós vão adquirindo conhecimento sobre os outros nós e passam a ter altas probabilidades de entrega. A escolha de uma constante k, responsável por atualizar a previsora de entrega, mostrou-se uma tarefa árdua e dependente do modelo de rede.

Lindgren et al. mostraram através de simulações que a taxa de entrega de mensagens do Prophet chega a ser 40% maior do que quando utilizando o roteamento Epidêmico. Obviamente, este resultado é válido na rede considerada na simulação, não existindo (até onde podemos averiguar) uma comparação mais geral.

Em nosso protocolo (o HIGROP) limitamos o repasse de mensagens somente entre grupos de nós diferentes (mais detalhes no Capítulo 5), com este repasse sendo feito pelo nó líder de cada grupo. Dessa forma obtivemos uma diminuição do *overhead* de comunicação em relação ao Prophet.

3.4 Conclusão

Neste capítulo apresentamos os conceitos de redes tolerantes a interrupções de comunicação (DTNs) e fizemos uma revisão da literatura dos principais protocolos de roteamento nessas redes. Focamos nas soluções aplicáveis em MANETs devido a contribuição desta dissertação ser um protocolo de roteamento DTN em MANET.

Os protocolos de roteamento em DTNs podem ser classificados em determinísticos e estocásticos. Os protocolos determinísticos são aplicáveis quando é possível prever o

momento em que irá ocorrer a conexão, ou seja, os nós da rede possuem um padrão de mobilidade pré-determinado. Os protocolos estocásticos não assumem que cada nó tenha informação sobre a rede, sendo aplicáveis em cenários mais gerais em MANETs, nas quais os nós possuem padrão de mobilidade arbitrária.

Nosso protocolo pode ser classificado como estocástico, porém se difere dos demais algoritmos de mesma categoria devido a utilização de agrupamento de nós para fazer um roteamento sem excesso de replicações de mensagens na rede. No Capítulo 6 mostramos que o algoritmo proposto tem melhor desempenho em situações em que recursos como o *buffer* são limitados, que são os casos reais.

Capítulo 4

Redes de Emergência

Neste capítulo definimos os eventos que representam um cenário de emergência e discutimos os conceitos de redes de emergência, suas peculiaridades e seus requisitos. Apresentamos também um modelo de mobilidade para representar o comportamento de equipes no atendimento a situações críticas. Na Seção 4.1 discutimos os cenários de emergência definindo a terminologia usada nesta dissertação. Mostramos como as MANETs podem ser aplicadas para o gerenciamento de emergência nesses cenários, sendo elas uma possível solução para a falta de infra-estrutura de comunicação em casos de desastres e catástrofes. Na Seção 4.2 discutimos o modelo de rede emergência e caracterizamos a mobilidade dos nós que compõem a rede baseando-se no comportamento dos agentes que atuam em cenários de emergência. Finalmente, na Seção 4.3 propomos um modelo de mobilidade sintético para representar o comportamento desses agentes se movimentando em grupos com diversas regiões de interesses a serem visitadas em um cenário de emergência, batizado de Modelo de Mobilidade de Nós em Redes de Emergência (MME). Avaliamos as características dos encontros dos nós no MME e mostramos o comportamento dos nós no MME em relação aos modelos de mobilidade Random-way Point e o RPGM.

4.1 Cenários de Emergência

Cenários de emergência são situações ocasionadas por desastres naturais, tecnológicos ou causados pelo homem no qual é interrompido o funcionamento normal da economia e da sociedade em grande escala. Gerenciamento de emergência é o conjunto de processos que visam minimizar os impactos físicos e sociais desses eventos.

A coordenação e a comunicação entre os agentes humanos que atuam nesses cenários é fundamental para que haja um atendimento eficiente na redução dos impactos ocasionados pelo desastre. Esses agentes podem ser policiais, bombeiros, médicos entre

outros. A utilização de tecnologias para prover comunicação de dados e não somente voz, como ocorre com os dispositivos utilizados atualmente, melhoraria a eficiência no gerenciamento desses agentes.

No começo de 2005, a pedido da Agência Federal de Gerenciamento de Emergências dos Estados Unidos (Federal Emergency Management Agency, FEMA) o Conselho Nacional de Pesquisa americano (National Research Council, NRC) criou o Comitê do Uso de Tecnologia da Informação no Gerenciamento de Desastres. Esse comitê gerou como resultado um relatório com oportunidades do uso de tecnologia da informação no gerenciamento de desastres [Rao et al., 2007].

No Brasil, a Defesa Civil Nacional é o orgão responsável por gerenciar e definir, baseado em diversas métricas, o grau de um desastre ocorrido. A Seção 4.1.1 detalha as métricas utilizadas.

O relatório de Rao et al. [2007] dividiu o gerenciamento de emergência em quatro fases (prevenção, prontidão, resposta e recuperação) e identificou as contribuições e as pesquisas futuras em tecnologia da informação como uma ferramenta de auxílio em cada uma destas fases. Essas fases do gerenciamento de emergência são descritas na Seção 4.1.2.

4.1.1 Caracterizando Cenários de Emergência

Os recentes eventos trágicos como o ataque terrorista de 11 de setembro, o furacão Katrina nos Estados Unidos e o Tsunami na costa asiática demonstraram as limitações dos meios de comunicação das equipes que atuam nesses cenários.

Apesar do Brasil estar em uma região de certa estabilidade climática e geológica e ser um país sem histórico de ataques terroristas, recentes tragédias como o acidente aéreo da Gol na Amazônia e as inúmeras inundações, que segundo dados da Defesa Civil, são responsáveis pelo maior número de vítimas em desastres naturais, também mostraram a necessidade de melhores formas de comunicação por parte das instituições brasileiras.

A Defesa Civil brasileira caracteriza cenários de emergência de acordo com alguns critérios preponderantes que levam em consideração a intensidade dos danos (humanos, materiais e ambientais) e a ponderação dos prejuízos (sociais e econômicos). Com essa forma de avaliação, busca-se valorizar o contexto social no qual o desastre ocorreu para que se possa relacionar os recursos disponíveis com as necessidades desejadas [SNDC, 2009]. Os critérios preponderantes na avaliação de uma situação de emergência são:

1. Intensidade dos Danos

   Danos Humanos

Danos Materiais Destruídos ou Danificados

Danos Ambientais

2. Ponderação dos Prejuízos

   Prejuízos Econômicos

   Prejuízos Sociais

3. Alguns Critérios agravantes

   Ocorrência de desastres secundários

   Despreparo da administração local (geral e defesa civil)

   Grau de vulnerabilidade do cenário e da comunidade

   Padrão evolutivo do desastre

Apesar do termo emergência ser utilizado para acidentes ou desastres causados pela soma de efeitos parciais, os acidentes da construção civil e acidentes de trânsito, por exemplo, mesmo trazendo grandes danos e prejuízos sociais não caracterizam situação de emergência como as tratadas nesta dissertação.

4.1.2 Gerenciamento de Emergência

Todo o trabalho de coordenação e atuação das equipes sobre uma região com o intuito de minimizar os impactos físicos e sociais proporcionados por um desastre é denominado gerenciamento de emergência. Esses esforços são divididos em quatro fases, distintas entre si pelo tempo em relação ao instante em que o fenômeno gerador da crise acontece. Em cada uma dessas fases ferramentas tecnológicas podem auxiliar a coordenação e o gerenciamento de uma emergência. Tais fases são:

Preparação Ocorre semanas ou dias antes da ocorrência do fenômeno. Corresponde aos esforços destinados a minimizar os efeitos de um desastre, como a criação de construções mais resistentes, adequação das construções já existentes e medidas de contenção do fenômeno. O treinamento das equipes e as simulações na tentativa de prever os efeitos do fenômeno causador do desastre também fazem parte dessa fase.

Alguns fenômenos naturais podem ser modelados computacionalmente para se prever sua intensidade e região que será afetada, como por exemplo a previsão metereológica. Dessa forma, podem ser tomadas medidas preventivas nas regiões

mais necessitadas, como retirar as pessoas das áreas a serem atingidas. O treinamento de pessoas e equipes para a utilização dos recursos tecnológicos pode ser realizado nessa fase.

Prontidão Momentos logo antes e durante a ocorrência do fenômeno. São executadas ações destinadas a melhorar a capacidade de resposta, como a criação de planos de ação e o posicionamento das equipes e equipamentos.

Resposta Esforços efetuados imediatamente após o acontecimento do fenômeno, com intuito de conter o evento e minimizar as perdas materiais e humanas. Necessita de coordenação forte e ágil, pois é o momento de atuação mais crítico, no qual o tempo para execução das tarefas relaciona-se com o número de vidas que podem ser salvas.

É nesta fase que está a maior carência de tecnologia atualmente, pois tradicionalmente a comunicação entre as equipes é feita através de rádio. Contudo, este tipo de comunicação é limitado ao uso somente de voz. A integração de voz e dados pode estender a habilidade dos integrantes das equipes de processarem informações, como mapas, localizações entre outros. As redes *ad hoc* podem suprir a falta de infra-estrutura de comunicação provendo-a tanto de voz quanto de dados através de dispositivos portáteis como PDAs e notebooks.

Restabelecimento Ações executadas com o intuito de restaurar o funcionamento normal da região afetada. Podem durar meses, até anos, após a ocorrência do evento.

Após o desastre, a infra-estrutura de comunicação da região afetada pode estar danificada por diversos fatores, como destruição dos equipamentos (torres e cabos), perda de energia e fatores ambientais (ex.: obstáculos para comunicação em redes sem fios).

No gerenciamento de emergência, é crucial que o sistema de comunicação seja robusto e capaz de resistir a possíveis intermitências de comunicação. Adicionar resiliência de comunicação nas redes atuais é um requisito para prover comunicação em um desastre, no qual há prioridade na entrega de mensagem ao destino.

Os protocolos para redes tolerantes a interrupções de comunicação tentam solucionar esse problema de resiliência nas redes tradicionais, adicionando a possibilidade de atrasos variados e particionamento da rede, tais como ocorrem quando há mobilidade e em ambientes que proporcionam contínua quebra de conectividade, como em desastres.

4.2 Modelo de Rede de Emergência

Um dos grandes desafios na comunicação em redes de emergência é falta de conectividade causada pela eventual falta de infra-estrutura e também pela movimentação dos nós comunicantes. Esse particionamento da rede somado a eventuais falhas dos nós e ao comportamento dinâmico destes nós exigem uma maior robustez a este tipo de rede.

Uma rede de emergência pode ser composta por um conjunto de nós heterogêneos. Estes nós podem ser representados pelas equipes de resgate, nós sensores para o monitoramento, pontos de acesso fixos que provêem conexão externa ao local do incidente e computadores gerenciadores. A Figura 4.1 ilustra os componentes da infra-estrutura da rede de emergência. Os nós se comunicam de modo *ad hoc* entre si e podem trocar dados com nós gerenciadores. O acesso externo à Internet pode ser provido por pontos de acesso utilizando tecnologias comerciais como wi-fi ou wimax.

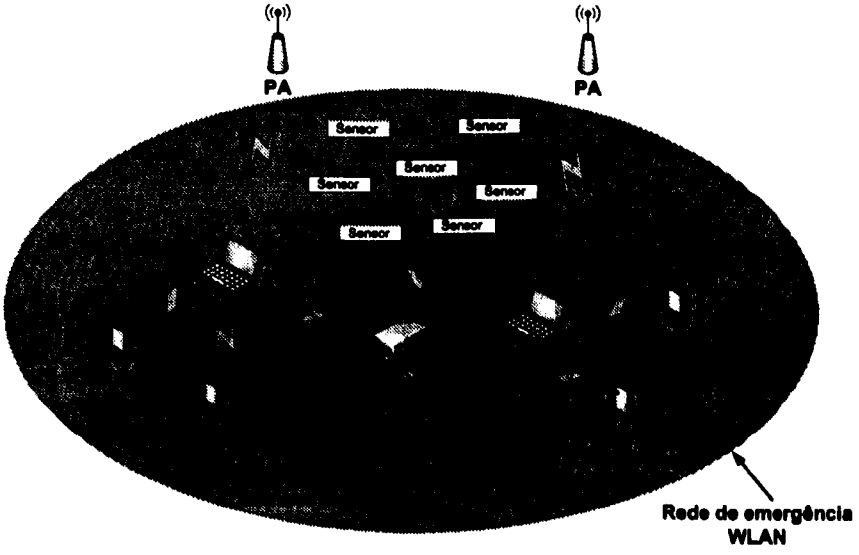

Figura 4.1. Exemplo do Modelo de uma Rede de emergência

As equipes podem ser formadas por participantes de instituições diferentes, governamentais ou não, como bombeiros, policiais, médicos, entre outros. Dessa forma, interoperabilidade é uma das exigências para que a rede funcione corretamente, pois os integrantes das redes podem estar com equipamentos dos mais diversos modelos e tecnologia.

Os nós móveis são os dispositivos portáteis, como PDAs ou notebooks, carregados pelos agentes das equipes de resgate. A vantagem do uso desses dispositivos é permitir que haja comunicação de dados e não somente voz, como ocorre atualmente. Dessa forma, o gerenciamento de emergência torna-se mais eficiente em relação à distribuição de tarefas das diversas equipes que estiverem atuando na região afetada.

Os pontos de acesso são nós fixos com maior alcance de rádio. São responsáveis por aumentar a conectividade da rede, permitindo a comunicação entre nós que estão distantes entre si, porém dentro do raio de alcance dos pontos de acesso e também por prover acesso às fontes externas de dados, como outras redes ou à Internet.

Os nós gerenciadores são nós com maiores capacidades de processamento e memória, responsáveis por receber e processar requisições dos usuários. Essas requisições podem ser imagens de mapas, informações sobre localização de outras equipes e necessidade de recursos para o atendimento da emergência, entre outras.

Os nós sensores podem ser utilizados para o monitoramento e sensoriamento de regiões em risco, por exemplo na monitoração das proximidades de um incêndio e enviando essas informações a um nó gerenciador.

A comunicação entre os nós pode ser estabelecida de modo *ad hoc*, com isso, a rede fica independente da necessidade de uma infra-estrutura de comunicação.

Para validar o protocolo de roteamento proposto nesta dissertação desenvolvemos um modelo de mobilidade que representa o padrão de movimentação de equipes de resgate em um cenário de emergência. Dessa forma, podemos observar como os protocolos de roteamento se comportam no cenário em que estamos analisando. A Seção 4.2.1 apresenta um modelo do comportamento de mobilidade dos agentes em um cenário de emergência. A partir dessa modelagem propomos um modelo de mobilidade em cenários de emergência descrito na seção 4.3.

4.2.1 Mobilidade em Cenários de Emergência

A mobilidade em cenários de emergência é fundamentalmente causada pelos eventos ocorridos e para os locais que os agentes devem se mover em cada atendimento. Por exemplo, no atendimento a uma enchente, diversas equipes atuam no resgate aos atingidos. Essas equipes podem ser formadas por médicos, bombeiros, voluntários, etc. Durante o evento ocorrido, algumas regiões podem necessitar de atendimento prioritário de algum serviço específico, por exemplo bombeiros em uma enxente, e com isso algumas equipes tendem a visitar essas regiões com maiores prioridades. Os locais para os quais as vítimas e/ou desabrigados serão levados (hospitais, abrigos, etc) também são considerados regiões de interesse. A Figura 4.2 ilustra essa tendência de movimentação dos agentes, em uma região alagada há a necessidade de equipes de bombeiros para fazer o resgate e atendimento às vítimas.

Definindo formalmente, seja um evento ocasionado por um desastre em uma determinada área. Há N equipes, sendo que cada equipe pertence a uma determinada instituição (I), como bombeiros, médicos, policiais. Nessa área existem R regiões que são prioritárias, por exemplo regiões de busca por vítimas, hospitais, etc. Cada região

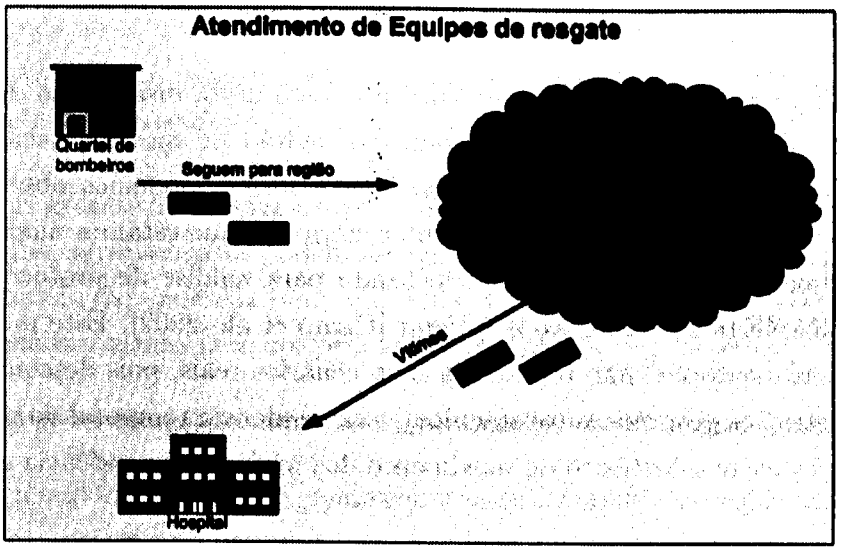

Figura 4.2. Exemplo de movimentação de uma equipe de resgate - As equipes seguem para a região afetada e para locais de interesse como hospitais

pode possuir necessidades de atendimento de um ou mais tipos de instituições e para cada necessidade há uma prioridade R_ϕ associada. Dessa forma, uma região pode ter uma necessidade alta de médicos e baixa de policiais. As equipes de cada instituição então tendem a visitar alguma entre essas R regiões de acordo com a necessidade da mesma.

A mobilidade dos agentes é definida pela instituição a qual ele pertence, o número de regiões e suas respectivas prioridades que compõem o cenário de emergência. Adicionar esse comportamento a um modelo de mobilidade sintético traz características mais realísticas ao analisar esses cenários.

4.3 Modelo de Mobilidade de Nós em Cenários de Emergência

Embora diversos modelos de mobilidade para simulação em redes *ad hoc* tenham sido desenvolvidos e analisados [Camp et al., 2002; Gerla et al., 2005], eles não representam o comportamento de equipes de resgate em um cenário de emergência. A simulação é uma importante ferramenta para ajudar a compreender as características de comunicação em uma rede de emergência. Porém, para isso, é necessário que o modelo de mobilidade utilizado na simulação represente as características dos cenários estudados. O modelo de mobilidade utilizado na análise de protocolos de roteamento impacta diretamente no desempenho destes. A Seção 4.3.1 faz uma análise do comportamento dos nós em relação à duração dos contatos entre os nós e o tempo entre estes contatos,

duas métricas comumente usadas na literatura [Karagiannis et al., 2007; Cai e Eun, 2008].

Para validar o protocolo de roteamento proposto nesta dissertação desenvolvemos um modelo de mobilidade para representar o padrão de movimentação de equipes de resgate em um cenário de emergência. Dessa forma, podemos observar como os protocolos de roteamento se comportam no cenário em que estamos analisando.

O principal modelo de mobilidade utilizado para análise de protocolos de roteamento em MANETs é o *Random-WayPoint* [Camp et al., 2002]. Este modelo, por ter características aleatórias, não representa bem cenários reais, pois desconsidera a existência de restrições geográficas (obstáculos), a dependência temporal do movimento do nó (correlação entre o histórico de movimento dos nós) e a dependência espacial entre os nós.

Visando caracterizar melhor o comportamento humano de mobilidade, Lindgren *et al* criaram um modelo de mobilidade denominado "modelo de comunidade", no qual a área total é dividida em regiões e então cada nó segue para uma região com determinada probabilidade [Lindgren et al., 2003]. Porém, essa abordagem não considera a relação entre os movimentos dos nós.

O modelo de mobilidade *Reference Point Group Model* (RPGM) representa o movimento aleatório de grupos de nós [Camp et al., 2002]. No RPGM, os movimentos dos nós de um grupo são baseados no caminho percorrido por um centro lógico do grupo. Inicialmente cada membro do grupo é distribuído uniformemente próximo ao centro lógico do grupo. A cada instante, velocidades e direções de todos os nós do grupo são baseadas na velocidade e direção do centro lógico, podendo ter um desvio previamente definido. O RPGM é comumente utilizado para simular cenários de emergência como campos de batalha e catástrofes.

Porém, em cenários de emergência diversas instituições com papéis diferentes atuam no sentido de minimizar os danos causados. Essas insituições são formadas por agentes que compõem as equipes de resgate e estes tendem a se mover em grupos. Em geral há regiões de interesse, como o centro de controle e a região de busca e resgate, sendo que cada região pode ter necessidade de atendimento de equipes de instituições diferentes, como quando ocorre um incêndio a uma necessidade pelo atendimento de bombeiros por exemplo.

A fim de caracterizar melhor tais cenários em um modelo de mobilidade, foi introduzida no modelo RPGM a possibilidade de representação de regiões de interesse e a classificação de cada grupo em uma determinada instituição. Num determinado momento, os grupos de nós seguem para uma determinada região de interesse de acordo com a necessidade de cada região.

Utilizaremos neste trabalho um modelo que representa o comportamento dos movimentos de equipes de resgate em cenários de emergência. Para tal consideramos as seguintes premissas baseadas no modelo de rede discutido na seção 4.2:

- Existem grupos de resgate os quais podem ser mapeados em grupos de nós da rede. Tais agrupamentos podem ser representados pelo modelo RPGM, portanto, adicionando dependência temporal entre os nós. Porém, no RPGM os grupos se movimentam aleatoriamente pela área simulada.
- Cada grupo é associado a um tipo de instituição previamente definida.
- Existem regiões de interesse, como centrais de atendimento, região a ser resgatada e pontos críticos a se pesquisar.
- Cada região é associada a uma probabilidade de ser visitada.
- Cada grupo possui um líder, assim como existe uma hierarquia interna nos orgãos institucionais de segurança pública (polícia, bombeiros, etc).

A partir dessas premissas, propomos um modelo de mobilidade em grupo com regiões de interesse denominado *Mobility Model to Emergency Networks* (MME). No MME cada grupo é classificado em uma determinada instituição, o MME estende o RPGM pela adição de regiões de interesse, sendo que cada região possui necessidade de atendimento de instituições específicas. As Definições 1 e 2 formalizam os conceitos de instituições e de região de interesse respectivamente.

Definição 1 ***Instituições*** *são organizações ou mecanismos sociais que controlam o funcionamento da sociedade e dos indivíduos. Todos os grupos que atuam em um cenário de emergência pertencem a uma instituição* ϕ.

Definição 2 ***Região de Interesse*** *é uma área definida pelas coordenadas de um ponto de interesse* $p_{(x,y)}$ *e um raio* d *a partir deste ponto. Essa região pode possuir um ou mais requisitos* $R_\phi \in [0,1]$, *sendo* ϕ *a instituição que atende o requisito com prioridade* $\in [0,1]$, *definindo quais grupos visitarão a região.*

Seja I o conjunto de ϕ instituições definidas previamente, $I = \{\phi_1, \phi_2, ..., \phi_n\}$, que podem representar bombeiros, médicos, policiais, etc. Considere R uma região de interesse formada por um ponto de interesse $p_{(x,y)}$ e um raio d. Essa região possui necessidade de atendimento por k instituições com prioridades independentes entre si, $R^k_\phi = \{R^1_{\phi_1}, R^2_{\phi_2}, .., R^k_{\phi_k}\}$, sendo cada prioridade $R^k_\phi \in [0,1]$. Dessa forma, uma região

com prioridade de atendimento R_ϕ alta, será visitada pelos grupos que pertencem à instituição ϕ.

A Tabela 4.1 sumariza os parâmetros de entrada utilizados no MME.

Tabela 4.1. Parâmetros do MME

Parâmetros de Grupo	
I	Quantidade de instituições.
g	Quantidade de grupos.
n	Número de nós no grupo.
Φ	Instituição que o grupo pertence.
Δd	Desvio de direção de um nó em relação ao centro lógico.
Δs	Desvio de velocidade de um nó em relação ao centro lógico. $\Delta s \in [0,1]$.
Parâmetros de Movimentação	
$s_{(Min,Max)}$	Velocidade mínima e máxima.
$\tau_{(Min,Max)}$	Tempo de pausa mínimo e máximo.
Parâmetros de Regiões de Interesse	
R	Número de Regiões de interesse.
$p_{(x,y)}$	Ponto de interesse (coordenada x,y).
d	Raio de desvio do ponto de interesse.
R_ϕ^k	Conjunto de k prioridades de necessidade de ϕ instituições.

No RPGM, cada grupo de n nós possui um centro lógico representado por um dos nós do grupo, o qual escolhe aleatoriamente uma direção entre 0 e 2π e uma velocidade uniforme entre s_{Min} e s_{Max} . Os $n-1$ nós restantes seguem o movimento do centro lógico mantendo desvios de direção e velocidade aleatórios. As Equações 4.1 e 4.2 caracterizam a velocidade (s) e a direção (Θ) respectivamente de cada membro em relação ao centro lógico do grupo em um instante t. $A \in [0,1]$ é um número aleatório gerado em cada instante t.

$$| s_{(membro)}(t) | = | s_{(centro)}(t) | \pm A * \Delta s * s_{max} \quad (4.1)$$

$$| \Theta_{membro}(t) | = | \Theta_{(centro)}(t) | \pm A * \Delta d \quad (4.2)$$

A diferença entre o RPGM e o MME é que este último pode haver uma ou mais regiões de interesse R. O nó considerado centro lógico de um grupo que pertence a uma instituição ϕ escolhe um p_i de acordo com a necessidade que esta região apresenta (R_ϕ). A Tabela 4.2 exemplifica um cenário do MME no qual há três instituições, $I = \{\phi_1 = A, \phi_2 = B, \phi_3 = C\}$, e duas regiões ($R_1$ e R_2), com prioridade de atendimento diferentes, tal que $\forall$ instituição $\phi \sum_{i=1}^{N} R_\phi^i \leq 1$, sendo N a quantidade de regiões de

interesse, ou seja, cada instituição deve ser distribuída entre as regiões de forma que não ultrapasse sua capacidade de atendimento.

Tabela 4.2. Prioridade de Atendimento em Cada Região de Interesse

	A	B	C
$\mathbf{R_1}$	0.3	0.6	0.1
$\mathbf{R_2}$	0.7	0.0	0.0

No MME, em um determinado instante, de acordo com as prioridades de cada região o centro lógico de um grupo que atenda ao requisito da região escolhe um destino $p_{(x_i,y_i)}$ conforme mostrado nas equações 4.3 e 4.4. O nó seleciona uma velocidade uniforme entre $[s_{min}, s_{max}]$ e os $n-1$ nós participantes do grupo o seguem mantendo uma variação de direção como $\pm\Delta d$. Após alcançado o destino, o centro lógico define uma pausa uniforme entre $[\tau_{Min}, \tau_{Max}]$. Logo após, escolhe um novo destino e uma nova velocidade novamente. A Figura 4.3 ilustra a movimentação de três grupos de nós pertencentes cada um a uma instituição diferente (A,B,C), sendo que os grupos A e B escolheram como destino a região de interesse definida por um ponto p com um raio d e o grupo C escolheu um destino aleatório.

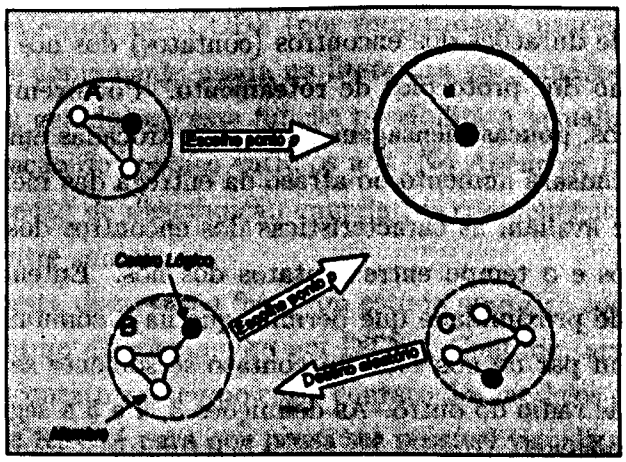

Figura 4.3. Mobilidade em grupo com áreas de interesse: Os diversos grupos de nós escolhem uma determinada região de acordo com os requisitos que possui (R_ϕ).

$$x_i \mid p_x - d \leq x_i \leq p_x + d \tag{4.3}$$

$$y_i \mid p_y - d \leq y_i \leq p_y + d \tag{4.4}$$

A Figura 4.4 mostra uma série de instantâneos representando os posicionamentos dos nós utilizando o MME nos tempos 0s, 100s e 1000s respectivamente. A rede está confinada em uma área de 200m x 200m, com 20 grupos de 5 nós pertecentes a uma única instituição (ϕ), uma região de interesse formada pelo ponto de interesse p(x,y)=(100,150) e com 60% de necessidade de atendimento pela instituição ϕ de ser visitado ($R_\phi = 60\%$). Cada círculo representa o alcance de rádio de cada nó (representado por um quadrado).

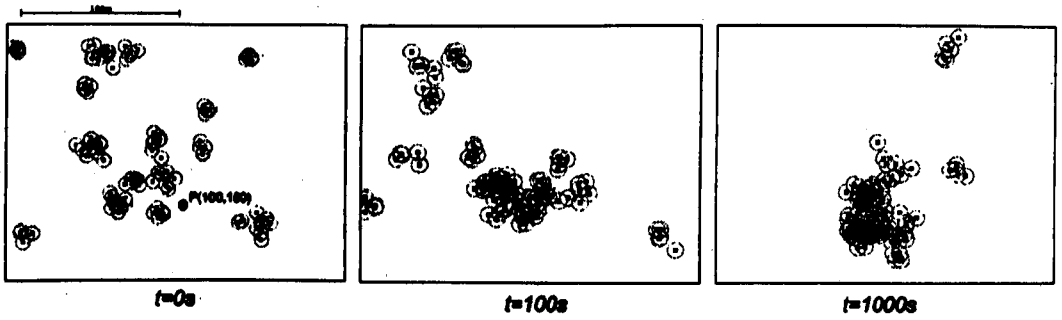

Figura 4.4. Posicionamento dos nós nos tempos 0s, 100s e 1000s em uma área de 200mx200m

4.3.1 Avaliação das Características dos Encontros dos Nós

As características de durações dos encontros (contatos) dos nós em uma rede podem afetar o desempenho dos protocolos de roteamento. Por exemplo, se os tempos de contato são pequenos, poucas mensagens podem ser trocadas em cada encontro o que consequentemente causará aumento no atraso da entrega das mensagens.

As métricas que avaliam as características dos encontros dos nós são o tempo de contato entre os nós e o tempo entre contatos dos nós. Entende-se por contato de dois nós a relação de proximidade que permite que haja comunicação direta entre os mesmos, ou seja, um par de nós está em contato se somente se cada nó está dentro do raio de alcance de rádio do outro. As definições 3, 4 e 5 a seguir [Cai e Eun, 2008] formalizam esse conceito.

Definição 3 ***Contato*** *Seja $\{B_1, B_2, B_3, ..., B_n\}$ um conjunto de nós móveis localizados uma área comum S e $B(t) \in S$ a posição do nó B no instante t. Seja ainda $\mathcal{N}_B(t) \in S$ o conjunto de contatos do nó B. O contato entre um nó X e um nó B no tempo t existe se somente se $X(t) \in \mathcal{N}_B(t)$.*

Definição 4 . ***Tempo de Contato*** *(TC) é a duração de contatos entre um par de nós conectados, ou seja, a diferença entre o instante em que os nós iniciaram o contato*

(t)e o instante em que o contato terminou (t'). Portanto, $TC = t' - t$ é o tempo total em que um nó B_i fez parte do conjunto de contatos do nó B_j ($B_i(t) \in \mathcal{N}_{B_j}(t)$).

Definição 5 ***Tempo entre Contatos** (TEC) é a duração de tempo entre o instante (t_{per}) em que um par de nós (B_i,B_j) perdeu o contato e o instante (t_{res}') em que o contato entre o mesmo par foi restabelecido ($B_i(t_{res}) \in \mathcal{N}_{B_j}(t_{res})$)*
$TEC = t'_{res} - t_{per}$

O problema do efeito dos padrões de mobilidade no desempenho da rede, como no atraso fim-a-fim para caminhamento de mensagens, não é novo, havendo diversos estudos que demonstram uma relação entre a função de distribuição cumulativa complementar[1] do tempo de contato e o tempo entre contato, que se assemelha com uma função cauda longa ou exponencial inversa, e o desempenho de algoritmos de roteamento de mensagens [Grossglauser e Tse, 2002; Karagiannis et al., 2007; Cai e Eun, 2008]. Karagiannis et al. mostram que quando analisado o tempo entre contatos dos modelos de mobilidade sintéticos ou humanos, a função de distribuição cumulativa complemetar destes apresentam um comportamento similar a uma função cauda longa do início até determinado instante e, após esse instante, passam a ter um comportamento de exponencial inversa.

A função de distribuição cumulativa complementar, do inglês *Complementary Cumulative Distribution Function* - CCDF (por simplicidade, usaremos a sigla em inglês ao longo do texto), é comumente usada na literatura para análise de modelos de mobilidade pois a curva gerada por essa função possibilita a visualização do impacto de cada modelo na duração do contato entre os nós. No Apêndice B detalhamos como é feito o cálculo da função de distribuição cumulativa complementar para o tempos de contato e o tempo entre contato.

Não é objetivo desta dissertação fazer um estudo empírico sobre a relação modelo de mobilidade/algoritmo de roteamento em DTNs. Contudo, apresentamos na seção seguinte o tempo de contato e o tempo entre contato dos modelos de mobilidade MME, *Random-way Point* e RPGM para que possa ser possível visualizar as diferenças entre estes.

4.3.1.1 Cenários

Analisamos a conectividade do modelos de mobilidade MME, *Random-way Point* e o RPGM em uma área de 200x200 com 100 nós. A Tabela 4.3 sumariza os parâmetros

[1] A função de distribuição cumulativa complementar é utilizada para visualizar a fração das amostras que são maiores ou menores do que um determinado valor. Em nosso estudo, utilizamos essa função para observar qual os valores dos tempos de contatos e entre contatos em 99% dos contatos estabelecidos na rede, vide Apêndice B.

comuns em todos os modelos e a Tabela 4.4 sumariza os parâmetros específicos do modelo MME.

Para avaliar o encontro dos nós foram gerados 15 arquivos diferentes para cada modelo de mobilidade contendo a movimentação dos nós durante 12000s. Esses arquivos foram utilizados como dados de entrada para o simulador ONE (explicado na Seção 6.1). O simulador ONE possui um módulo de manipulação de mobilidade o qual fornece uma implementação do modelo *Random-way Point*, utilizamos essa implementação para gerar os diversos arquivos com esse padrão de movimentação. Para o RPGM utilizamos a implementação fornecida por [Camp et al., 2002], que gera arquivos com informações sobre os movimentos dos nós formatado como dados de entrada para o simulador NS-2 [ns2, 2008], um simulador extensivamente usado na literatura para a simulação de redes. Modificamos essa implementação para que os arquivos gerados fossem formatados como dados de entrada para o ONE. Para gerar movimentações de nós com o padrão do MME, implementamos um gerador de mobilidade que tivesse como saída um arquivo com as informações de posições dos nós em cada instante simulado, formatado como entrada para o ONE.

Tabela 4.3. Parâmetros comuns em todos os modelos

Duração	12000s
Area	200x200m
$s_{(Min,Max)}$	(0.5, 10.5m/s)
$T_{(Min,Max)}$	(0,120)

Tabela 4.4. Parâmetros específicos MME

I	1
g	20
n	5
Φ	1
Δd	5m
$p_{(x,y)}$	(100,150)
d	20m
R_ϕ^k	R_ϕ^1 =0.6

Variamos o raio de alcance de rádio dos nós em 10, 20 e 30m para verificar a influência do raio de transmissão na conectividade da rede. A área de 200x200m e as velocidades foram definidas baseados em diversos trabalhos sobre análise de mobilidade na literatura [Cai e Eun, 2008; Spyropoulos et al., 2005]. As seções seguintes mostram os resultados obtidos.

4.3.1.2 Distribuição Cumulativa Complementar do Tempo de Contato

O tempo de contato (TC) é a duração de contatos entre cada par de nós conectados. A duração desses contatos influenciar diretamente no desempenho de protocolos de roteamento DTNs pois como nas DTNs, as trocas de mensagens são definidas em cada contato estabelecido; se este for pequeno, o número de mensagens transferidas é reduzido, causando uma queda no número de mensagens que chegam ao destino. A função de distribuição cumulativa complementar nos permite visualizar a probabilidade da duração de contato. Utilizamos a escala log-log para representar os dados.

As Figuras 4.5, 4.6 e 4.7 mostram a função de distribuição cumulativa complementar (CCDF) do tempo de contato para o MME, Randon-Way point (RWP) e RPGM com raios de transmissão de 10, 20 e 30 metros respectivamente. Observamos que em todos os modelos de mobilidade analisados, suas CCDFs apresentem um comportamento cauda-longa até aproximadamente 120s e depois apresentam comportamento de queda exponencial.

De fato, verificamos através da CCDF de tempo de contato quando o raio de transmissão é de 10m (Figura 4.5) que 99% do contatos no MME e no RPGM tem duração inferior à 124s, enquanto no RWP 99% dos contatos a duração é inferior à 94s. O MME se diferencia do RPGM ao manter mais tempo de contato entre os nós. A porcentagem dos contados que duram até 200s é de 0.2% no MME contra 0.006% no RPGM.

Ao duplicar o raio de transmissão (Figura 4.6)observamos comportamento semelhante , mas em 99% dos contatos, a duração é inferior à 225s, 240s e 141s para o MME, RPGM e RWP respectivamente. Isto mostra que o tempo de contato é dobrado com o raio de transmissão em todos os modelos de mobilidade. Novamente, o MME se diferencia dos demais em manter contatos mais duradouros nesses 1% restante de contatos.

Na Figura 4.7 é mostrada a CCDF do tempo de contato com raio de transmissão igual a 30m, em 99% dos contatos, a duração é inferior à 285s, 275s e 221s para o MME, RPGM e RWP respectivamente.

Concluímos que o comportamento de tempo de contato para o RPGM e o MME são semelhantes independentemente do raio de transmissão dos nós, contudo o MME é capaz de gerar contatos mais duradouros.

4.3.1.3 Distribuição Cumulativa Complementar do Tempo entre Contato

O tempo entre contato (TEC) nos mostra durante quanto tempo um par de nós ficaram sem se encontrar desde o momento do último encontro. O tempo entre contato baixo indica que os nós tendem a se encontrar mais frequentemente. No roteamento em DTNs essa característica pode definir o desempenho de um protocolo. Os protocolos

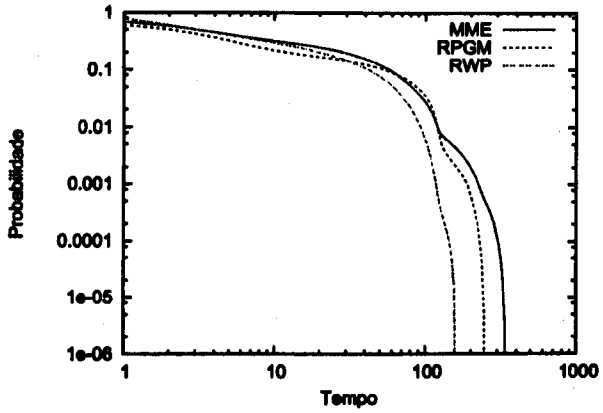

Figura 4.5. CCDF Tempo de Contato com raio de alcance de 10m

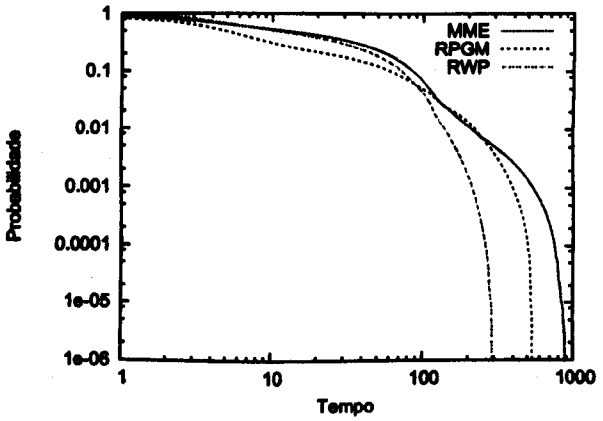

Figura 4.6. CCDF Tempo de Contato com raio de alcance de 20m

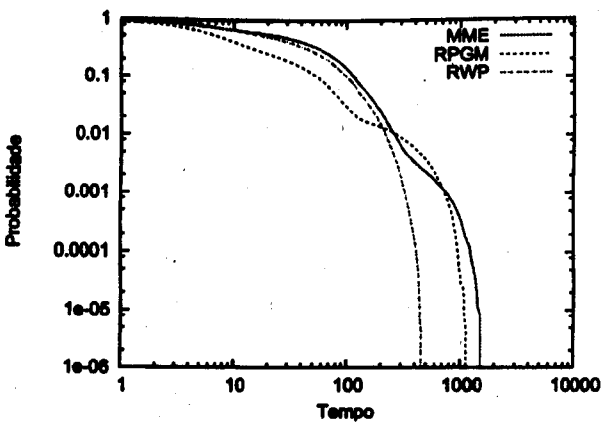

Figura 4.7. CCDF Tempo de Contato com raio de alcance de 30m

que utilizam como métrica probabilística de entrega a frequência de encontro (como o Prophet) não são tão eficientes visto que eles se tornam muito semelhantes ao Epidêmico, pois com a alta frequência de encontros os nós tendem a ter alta probabilidade de entrega também. De fato, esse comportamento é observado e detalhado no Capítulo 6 quando comparamos os protocolos de roteamento em DTN.

As Figuras 4.8, 4.9 e 4.10 mostram a função de de distribuição cumulativa complementar do tempo entre contato para o MME, Randon-Way point (RWP) e RPGM com raios de transmissão de 10, 20 e 30 metros respectivamente.

Na Figura 4.8 é mostrado a ccdf do TEC quando o raio de transmissão é de 10m. Observamos que em 99% a duração dos TECs no MME (< 1150s) chega a ser menos da metade do que exibido pelo RPGM (< 2647s) e RWP (< 2148). O fato da duração do TEC do RPGM ser superior ao RWP indica que os nós mesmo se movendo em grupos saem com frequência do raio de alcance do mesmo.

Observamos que aumentar o raio implica na diminuição da duração do tempo entre o contato dos nós. Para raio de transmissão de 20m (Figura 4.9), a duração do TEC do MME foi inferior a 629s em 99% dos casos, ou seja, menos da metade.

Ao aumentar o raio de alcance para 30m, em 99% dos casos o TEC foi inferior à 477s, 1036s, 958s para o MME, RPGM e RWP.

No tempo entre contatos, o MME apresentou características que indicam que os nós se encontram com uma frequência maior. Essa característica é importante em cenários onde a rede é intermitente, pois quanto maior a frequência de encontro dos nós maior a possibilidade de repasse de mensagens entre estes.

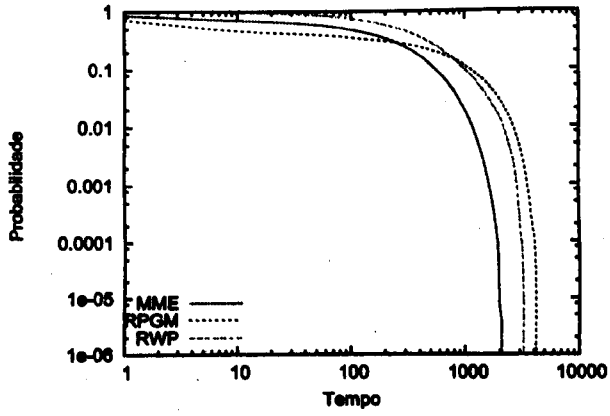

Figura 4.8. CCDF Tempo Entre Contato com raio de alcance de 10m

4.4 Conclusão

Este Capítulo apresentou os eventos que caracterizam um cenário de emergência e como estes são classificados pela agências governamentais. Mostramos também as fases no gerenciamento de emergência e a importância da cada uma na prevenção, na atuação e na recuperação de um desastre. Em seguida, discutimos os conceitos de redes de emergência, suas características e seus requisitos. Por fim, analisamos o comportamento de mobilidade das equipes de resgate e propomos um modelo de mobilidade sintético,

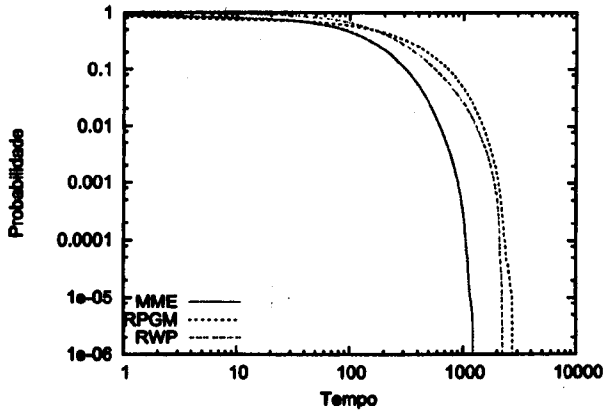

Figura 4.9. CCDF Tempo Entre Contato com raio de alcance de 20m

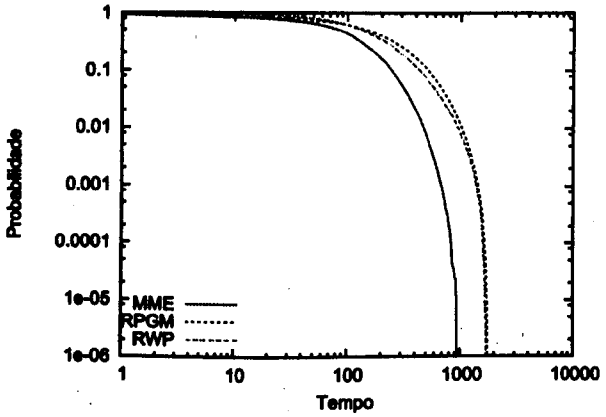

Figura 4.10. CCDF Tempo Entre Contato com raio de alcance de 30m

batizado de MME, que introduz características mais similares a movimentação destas equipes. Observamos que o MME traz um maior tempo de contato entre os nós em relação a outros modelos de mobilidade sintéticos comumente utilizados.

Apresentamos a terminologia usada nesta dissertação para definir cenários de emergência, que são caracterizados por situações nas quais o funcionamento normal da sociedade e da economia foi interrompido em larga escala. No Brasil, a Secretaria Nacional de Defesa Civil é a responsável pelas ações de prevenção, coordenação de resposta e recuperação em casos de desastres, sendo enchentes um dos desastres mais comuns no território brasileiro.

Atualmente, a comunicação entre as equipes de resgate é feita somente através de rádio (voz), como em desastres a infra-estrutura de comunicação (como antenas, postes, etc) podem ser afetadas, as MANETs podem prover uma solução para comunicação de dados/voz, aumentando assim a eficiência no gerenciamento de emergência nesses cenários.

Em seguida discutimos um modelo de rede emergência e caracterizamos a mobi-

lidade dos agentes que atuam em cenários de emergência. Por meio desse estudo, definimos as premissas que caracterizam o movimento das equipes em um cenário de emergência: os agentes se movimentam em grupos e existe uma ou mais regiões onde haverá atendimento prioritário. Essas premissas foram utilizadas no desenvolvimento de um modelo de mobilidade sintético que representa a movimentação dos agentes em cenários de emergência para então analisarmos o comportamento dos protocolos de roteamento nesses cenários.

A seguir apresentamos os modelos de mobilidade sintéticos comumente usados na literatura, observamos que o *Random-Way point* produz movimentos aleatórios e sem nenhuma correlação entre os nós participantes da rede, já o RPGM introduz uma correlação entre os movimentos dos nós, porém com direção e sentidos ainda aleatórios. Baseado nisso, propusemos um modelo de mobilidade sintético para representar o comportamento desses agentes se movimentando em grupos e com diversas regiões de interesses a serem visitadas em um cenário de emergência, batizado de Modelo de Mobilidade de Nós em Redes de Emergência (MME). Avaliamos as características dos tempos de contato e os tempos entre contatos dos nós utilizando o MME, *Random-way Point* e o RPGM e verificamos que o MME produz um cenário onde a rede possui contatos mais duradouros.

Capítulo 5

Protocolo HIGROP

Neste capítulo descrevemos o protocolo proposto, denominado HIGROP (*HIerarquical Group ROuting Protocol*). A Seção 5.1 apresenta os conceitos, as premissas e os requisitos utilizados para a especificação do protocolo e suas aplicações alvo. Em seguida, a Seção 5.2 apresenta o funcionamento detalhado do protocolo e os algoritmos que o compõem. Por fim, na Seção 5.3 é feita uma análise do custo assintótico do protocolo proposto.

5.1 Premissas e Requisitos do Protocolo

O HIGROP é um protocolo de roteamento hierárquico baseado em grupos para redes móveis *ad hoc* que tem como objetivo fazer a entrega de mensagens sem aumentar número de mensagens extras enviadas pela rede para que a mensagem atinja o destino.

Consideramos como nó de rede um dispositivo com (i) um identificador único, (ii) um módulo implementando o protocolo de roteamento e (iii) uma interface de comunicação sem fios. As seguintes primitivas serão utilizadas ao longo do texto para se referir a comunicação de dados entre dois nós com raio de alcance R:

1. *envia*$_A$*(B,m)*: nó A transmite uma mensagem m para o nó B.

2. *recebe*$_A$*(B,m)*: nó A recebe uma mensagem m do nó B.

3. *difusao*$_A$*(m)*: nó A transmite uma mensagem m para todos os nós no alcance de R.

4. Um *enlace(A,B)* existe quando dois nós A e B podem se comunicar diretamente, por exemplo *A(B)* pode receber transmissões de *B(A)*.

5. *vizinho(A,B)*: A é vizinho de B se mantiverem um enlace(A,B) por um determinado tempo mínimo. Chamamos de relação de vizinhança o relacionamento entre dois nós A e B tal que *vizinho(A,B)*.

A partir dos conceitos acima, definimos um conjunto de premissas e requisitos sobre as características da rede. Esses requisitos, que são apresentados a seguir, foram definidos com o objetivo de tornar o HIGROP um protocolo eficiente em nosso modelo de rede de emergência.

Mobilidade de nós em grupo: Como definido no Capítulo 4, em um cenário de emergência os agentes que compõem as equipes de resgate se movem em grupos. Desse modo, assumimos que os nós da rede se movam em grupos. Se a movimentação dos nós for totalmente aleatória, o protocolo fica impossibilitado de criar grupos estáveis.

Criação de grupos de nós vizinhos: O protocolo deve utilizar uma métrica que indica se o encontro de um par de nós caracteriza uma relação de vizinhança entre os nós ou não. Em uma rede móvel nem todo contato entre os nós é uma relação de vizinhança. Devido à mobilidade, o tempo de contato entre dois nós pode ser de curta duração, o que indica que estes nós tiveram um contato mas não possuem relação de vizinhança. Portanto, o protocolo deve estimar o tempo mínimo da duração do contato entre dois nós para que estes sejam considerados vizinhos.

Manutenção de alta estabilidade dos grupos de nós: A partir do momento em que dois nós se reconhecem como vizinhos é importante evitar que pequenas desconexões descaracterizem essa relação de vizinhança. Ou seja, se o tempo entre contatos de um par de nós for pequeno, estes devem continuar sendo caracterizados como vizinhos para manter o agrupamento estável.

Baixo *overhead* de manutenção dos grupos: Como o objetivo do protocolo é minimizar o número de mensagens extras na rede (*overhead* de comunicação) para que a mensagem atinja o destino, o controle e reconhecimento de vizinhos deve ser feito de forma passiva e não por meio de envio explícito de mensagens informando o papel do nó, o que causaria um *overhead* de mensagens de controle. Em uma rede em que contatos são estabelecidos com frequência, o overhead de controle poderia ser maior que o overhead de comunicação, descaracterizando o objetivo do protocolo.

Baixo *overhead* na disseminação de mensagens: Somente um subconjunto de nós faz replicação de mensagens. A construção de uma hierarquia virtual visa diminuir o número de nós que podem fazer replicação de mensagens na rede.

Desempenho: O protocolo objetiva prover comunicação de dados eficientes em dispositivos *ad hoc* em redes de emergência. Portanto, espera-se que o mesmo tenha um bom desempenho em métricas como taxa de entrega e *overhead* de comunicação.

Tendo definido os requisitos e premissas sobre as quais o protocolo proposto se baseia, iremos agora descrever o seu funcionamento.

5.2 Funcionamento do Protocolo

O HIGROP é um protocolo de roteamento distribuído tolerante a interrupções de comunicação para redes *ad hoc*. Utilizando o paradigma de armazenar-repassar o protocolo é responsável por escolher qual o próximo nó que a mensagem deve ser encaminhada na rede. Mensagens que não possam ser encaminhadas em um instante (devido a desconexão dos nós, por exemplo) aguardam no buffer de armazenamento até que ocorra uma nova conexão.

O HIGROP constrói uma hierarquia virtual para definir as políticas de encaminhamento de mensagens e evitar assim a disseminação da mensagem por todos os nós da rede. Para isso, cada nó mantém uma tabela com informações sobre os contatos que estabelece com os demais nós na rede. Em cada conexão entre um par de nós, *enlace(A,B)*, é atualizado o tempo de contato cumulativo (TCC), que indica o tempo que dois nós estão mantendo contato, e o tempo em que ocorreu essa última conexão (UC). Utilizando essas informações, um nó constrói dinamicamente sua tabela de vizinhos. Cada nó HIGROP possui um identificador único (ID) e o papel (P) que ele possui em relação aos demais participantes do grupo.

O HIGROP é composto por dois módulos: Identificação de vizinhança e o encaminhamento e recebimento de mensagens. A Figura 5.1 apresenta a arquitetura do HIGROP.

No módulo de identificação de vizinhança, o serviço de identificação de vizinhança (SIV) é o responsável por fazer a comunicação entre o protocolo e a interface de comunicação. A cada *enlace(A,B)* estabelecido cada nó informa para o outro seu papel (P) em relação ao grupo e enquanto existir esse enlace essa informação é re-enviada periodicamente, sendo este período ω uma constante do algoritmo.

Ao receber essa informação o SIV de cada nó verifica se a tabela de vizinhos já contém o outro nó; caso não contenha, adiciona na tabela o ID e o papel do nó, marca o tempo em que ocorreu essa conexão (UC) e inicializa o tempo de contato cumulativo (TCC = 0). Em uma nova conexão com um nó que a tabela já contém o ID recebido, o SIV atualiza o tempo da UC e calcula o TCC conforme mostrado na Eq. 5.1, que mostra há quanto tempo existe o *enlace(A,B)*, sendo T_{atual} o instante em que ocorreu a conexão. Enquanto a conexão está ativa, a cada período ω o valor de TCC é atualizado.

$$TCC = TCC + T_{atual} - UC \tag{5.1}$$

As constantes α e β representam respectivamente o tempo máximo que um nó pode ficar desconectado sem ser desconsiderado como vizinho (isso evita que pequenas desconexões descaracterizem o nó como um vizinho) e o tempo mínimo acumulativo que dois nós devem manter conexão para serem considerados vizinhos.

O algoritmo de escolha do líder de um grupo de vizinhos é feita a favor do vizinho com menor identificador no grupo na tabela de vizinhos, após a escolha é informado ao SIV essa decisão. É importante ressaltar que o modelo de mobilidade descrito no Capítulo 4, o MME, somente gera padrões de movimentação em grupo, não interferindo em nenhuma informação que um nó tenha sobre seus vizinhos.

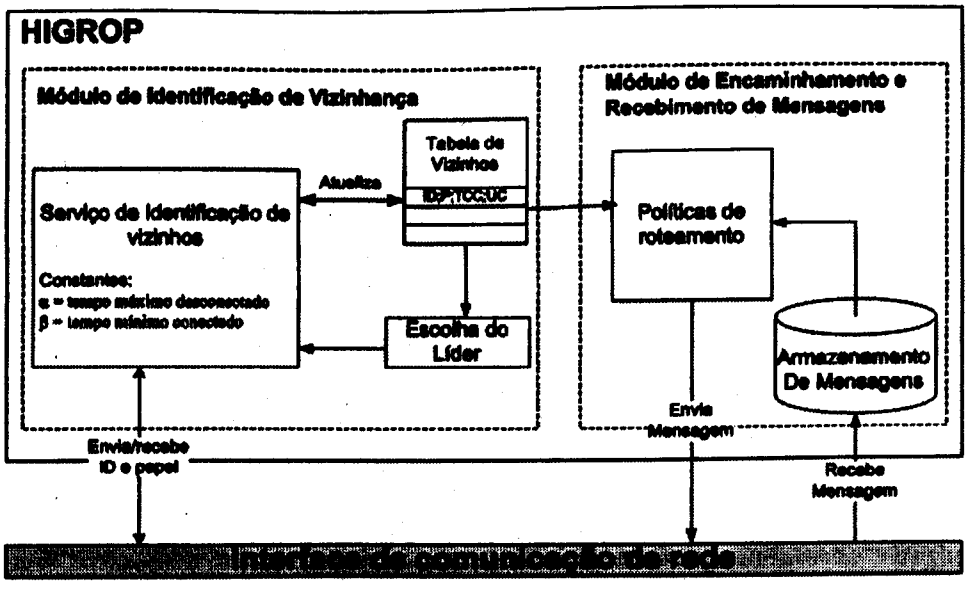

Figura 5.1. Arquitetura do HIGROP

O módulo de encaminhamento e recebimento de mensagens possui uma política de roteamento de mensagens que segue um princípio básico de hierarquia: As mensagens

somente são transmitidas ao nó líder de um grupo e este é responsável por entregá-las ao destino ou repassá-las a um nó que não seja participante do grupo. Dessa forma, somente os nós líderes fazem replicações das mensagens; os demais nós somente encaminham as mensagens para seus líderes.

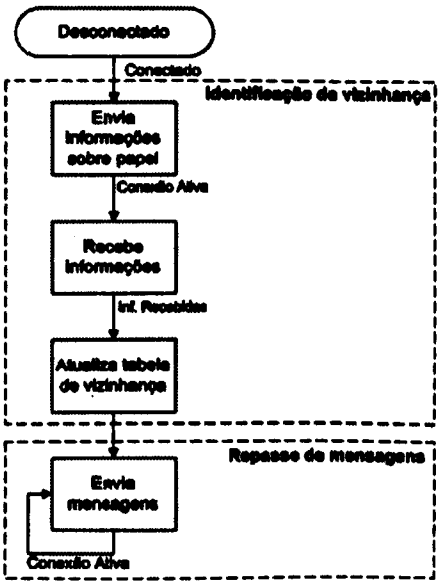

Figura 5.2. Máquina de estados do HIGROP

A Figura 5.2 mostra a máquina de estados do HIGROP para cada vez que é estabelecido um enlace entre dois nós. Primeiramente, ao estabelecer um contato é sempre feita a atualização da tabela de vizinhança pelo SIV e depois é feito o envio das mensagens.

Um nó HIGROP recebe as mensagens e as armazena em um *buffer* caso tenha espaço disponível. Se o espaço disponível no *buffer* é pequeno ele tenderá a estar sempre cheio caso a rede possua tráfego intenso.

As Seções 5.2.1 e 5.2.2 detalham os módulos de Identificação de Vizinhança e o Repasse e recebimento de mensagens respectivamente. A Seção 5.2.3 detalha como o HIGROP trata o descarte de mensagens quando o buffer de armazenamento está cheio.

5.2.1 Identificação de Vizinhança

Para fazer a criação e manutenção de grupos na rede, cada nó HIGROP possui um papel em relação a um grupo, podendo ser:

ISOLADO O nó não faz parte de nenhum grupo (não membro).

MEMBRO Membro comum de um grupo.

LIDER Líder do grupo.

Utilizamos como base para o nosso trabalho o ODGMBC [Cramer et al., 2004], pois no ODGMBC a manutenção do agrupamento não impacta no desempenho o algoritmo. Isso é feito utilizando um campo reservado de 2 bytes no cabeçalho do pacotes MAC, como o protocolo MAC envia pacotes periodicamente (*BEACONS*) em difusão na rede, todos os nós no raio de alcance do nó emissor podem "escutar" o *BEACON* e saber então qual o papel do nó emissor. O HIGROP envia esses *BEACONS* a cada tempo ω.

O HIGROP possui um "Serviço de Identificação de vizinhança" (SIV) que mantém uma tabela com as informações dos nós conhecidos. Essas informações são uma quádrupla composta por:

- Identificador do nó (ID), por exemplo o endereço MAC.
- Papel do nó, indica qual o papel do nó em relação ao grupo.
- Última conexão (UC), indica o instante em que recebeu o último *BEACON* do nó.
- Tempo de conexão cumulativo (TCC), tempo total que o nó está na tabela de vizinhos.

O papel inicial de cada nó é *ISOLADO* e dessa forma todos são potenciais líderes. Em um primeiro contato, cada nó adiciona o endereço do outro em sua a tabela e marca o tempo (t) em que ocorreu a conexão ($UC = t$). A cada nova conexão ou a cada *BEACON* recebido de uma conexão ativa com o mesmo nó é executado o cálculo da diferença entre o novo tempo (T_{atual}) e o tempo marcado anteriormente. Dessa forma é possível verificar quanto tempo o contato está ativo, um nó é considerado vizinho se somente se satisfazer as Equações 5.2 e 5.3.

$$TCC_{enlace(A,B)} \geq \beta \tag{5.2}$$

$$(T_{atual} - UC)_{enlace(A,B)} \leq \alpha \tag{5.3}$$

As constantes α e β são parâmetros configuráveis do HIGROP. Sendo α o tempo máximo que define um nó como vizinho mesmo sem que estejam conectados (isso evita que pequenas desconexões descaracterizem o nó como um vizinho). Se não há um *enlace(A,B)* e nas informações sobre B em A $(T_{atual} - UC_B) > \alpha$, o nó B é removido da tabela de vizinhos de A, ou seja, toda conexão é inserida na tabela porém são

mantidos somente os nós que satisfaçam a Eq. 5.3. A constante β indica o tempo mínimo que um nó tem que manter conexão para ser considerado um vizinho.

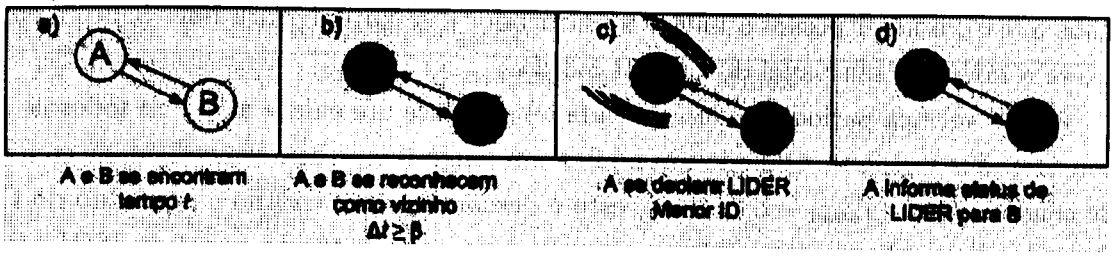

Figura 5.3. Reconhecimento de nós vizinhos

Os nós aguardam um período de *warm up* para que todos os vizinhos possam ser reconhecidos. O *warm up* é somente o período inicial ao início da rede. Após esse período, a partir da lista de vizinhos construída, o nó com o menor identificador assume a liderança e altera seu papel para *LIDER*.

Diversas políticas de escolha de líder em MANETs vêm sendo propostas Yu e Chong [2005]. Optamos por utilizar o algoritmo de líder com menor identificador devido à simplicidade deste método.

O nó líder envia uma mensagem aos seus vizinhos informando sobre sua liderança. Cada nó informado sobre o líder passa para o papel *MEMBRO* e informa aos seus vizinhos (que estão no papel *ISOLADO*) sobre o líder; os nós informados também passam para o papel de *MEMBRO*. Periodicamente então é enviado um *BEACON* com a operação *difusao(LIDER,m)*, sendo LIDER o nó declarado líder e m a informação sobre seu papel de LIDER. A Figura 5.4 mostra o diagrama de estados de um nó em relação a partir do momento que é estabelecido um enlace.

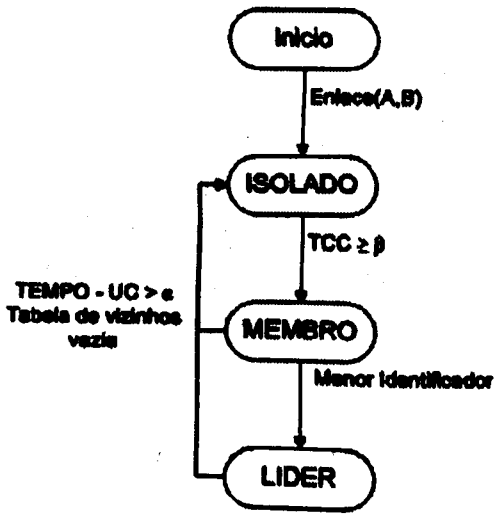

Figura 5.4. Diagrama de estados do papel desempenhado pelo nó

A Figura 5.3 mostra dois nós em processo de reconhecimento de vizinhança, em 5.3(a) dois nós com papel ISOLADO se encontram e informam seus papéis, após permanecerem conectados por tempo maior que β ($TCC \geq \beta$) se reconhecem como vizinhos 5.3(b), o nó A possui o menor identificador e se auto-declara líder 5.3(c) e então passa a informar seu papel de LIDER 5.3(d).

O SIV verifica periodicamente (a cada ω) se existe um enlace ativo em todos os nós considerados vizinhos. Quando um nó fica um longo tempo sem conectividade com um de seus vizinhos ($T_{atual} - UC > \alpha$), este é desconsiderado vizinho e removido do CV. Se o vizinho analisado for o líder conhecido, o nó volta então ao papel de *ISOLADO*.

5.2.2 Política de Roteamento em Grupo Hierárquico

Utilizando a hierarquia criada pelo Serviço de Identificação de Vizinhança, buscamos então minimizar o número de mensagens extras enviadas pela rede para que algoritmos de roteamento em DTN se tornem escaláveis, mas que não seja imposto um número máximo de replicações de mensagens.

A política de envio e repasse do HIGROP é baseada no conhecimento que o nó possui sobre o destino. O HIGROP age diferentemente se o destino da mensagem for um nó do mesmo grupo da origem ou se for para um grupo diferente.

O papel do nó determina a política de repasse de mensagens. Um nó MEMBRO somente repassa a mensagem ao destino ou ao LIDER, enquanto o nó LIDER é responsável por distribuir as mensagens entre grupos diferentes. A definição 6 abaixo formaliza da participação de um nó N em um grupo G:

Definição 6 *Seja* $N_{a..z}(G) \mid N[a...z] \in G$, *um* N_k *nó pertencente ao grupo* G.

O algoritmo 1 descreve o princípio básico do nosso protocolo. Ao longo do texto utilizaremos l.# para comentar as linhas do algoritmo, sendo # o número da linha citada. O algoritmo tem como entrada M mensagens para N destinos.

Para cada mensagem M_j para um destino N_k (l. 1-2) verifica se o destino pertence ao grupo usando a tabela de vizinhança mantida pelo SIV, na qual cada nó pode saber quem são seus vizinhos e quem é o LIDER do grupo. Se a mensagem deve ser enviada para um nó que faz parte do mesmo grupo (l. 3) então o repasse de mensagem é feito diretamente para o destino (l.4). Como dois nós podem ser considerados vizinhos mesmo não havendo uma conexão por um tempo limite (β), se no momento do envio não houver conexão, a mensagem é repassada para o nó LIDER (l.5-7).

Se a mensagem é para ser enviada a outro grupo, se o nó que possui a mensagem é o o líder, ele se responsabiliza por enviar a mensagem para um nó que não faça parte do grupo (l.9-12). Senão, o né então repassa a mensagem para o nó líder (l.13). O

nó do grupo que recebeu a mensagem repete essas operações até que a mensagem seja entregue.

Algoritmo 1: Repasse de Mensagens

Entrada: Nó $N_i(G)$ com M Mensagens para N destinos

```
1  for M_0 to M_max do
2      N_k Destino de M_j;
3      if N_k ∈ G then
4          envia(N_k,M_j) ;
5          if N_i não está conectado com N_k then
6              envia(LIDER,M_j);
7          end
8      end
9      if N_k ∉ G then
10         if N_i(G) é LIDER then
11             Envio M_j para nós que não pertencem a G;
12         end
13         else envia(LIDER,M_j);
14     end
15 end
```

5.2.3 Descartes de Mensagem do *Buffer* de Armazenamento

Em todos os protocolos de roteamento em uma DTN é assumido que os nós participantes da rede possuem recursos para armazenamento temporário de mensagens, se a capacidade de armazenamento de mensagens (*Buffer*) é ilimitado, o protocolo Epidêmico é ótimo em relação a entrega de mensagens e atraso fim-a-fim [Vahdat e Becker, 2000]. Contudo esse cenário é irreal, ainda atualmente dispositivos portáteis como PDA e celulares possuem recursos de processamento e memória limitados.

As mensagens ficam armazenadas no *buffer* para serem encaminhadas para outros nós. Se houver congestionamento e o *buffer* de armazenamento ficar cheio, ao receber uma nova mensagem o nó então deve possuir uma política para descarte de mensagem. Utilizamos uma política de fila "primeiro-entrar primeiro-sair" (*First-in First-out* FIFO) no HIGROP, dessa forma as mensagens mais antigas são descartadas para que possa ser possível receber uma nova mensagem.

5.3 Análise do Protocolo

Nesta seção fazemos uma análise do custo assintótico do HIGROP em relação ao consumo de memória, utilização de processador e quantidade de mensagens enviadas,

utilizando a notação "Big-Oh". Para esta análise, iremos considerar uma rede com N nós formada por n grupos com uma densidade média de v vizinhos por grupo, ou seja, em média um nó consegue se comunicar diretamente com v vizinhos.

O primeiro aspecto analisado é o consumo de memória do protocolo. A título de ilustração, comparamos o consumo de memória do HIGROP com o do Prophet. O HIGROP necessita armazenar uma tabela com uma quádrupla com as informações dos nós com que manteve conexão. Como todos os contatos que ocorrem são adicionados a tabela de vizinhança, o custo de memória para armazenamento dessa tabela é $O(N)$. Entretanto, como os nós que não são considerados vizinhos pelo controle de vizinhança são removidos da tabela, o consumo de memória do HIGROP é de $\Theta(v)$ bytes. O Prophet mantém uma tabela com a probabilidade para cada nó com que teve contato, logo manter essa lista de probabilidade tem consumo de memória de $O(N)$ bytes.

Seja uma rede formada por 100 nós e com média de 10 vizinhos. Cada quádrupla do HIGROP consome 68 bits(16 bits para o identificador, 16 bits para o tempo acumulado de conexão, 32 bits para tempo da última conexão e 2 bits para o papel do nó) de memória e cada tupla de probabilidade do Prophet consome 48 bits (16 bits para o identificador e 32 bits para probabilidade), como está implementado em nosso simulador. Nesse cenário o HIGROP consumiria 680 bits de memória contra 4800 bits do Prophet.

No aspecto de quantidade de mensagens enviadas na rede para que a mensagem atinja o destino (*overhead* de comunicação), no HIGROP se uma mensagem é destinada para um nó do mesmo grupo do nó origem, no máximo a mensagem é repassada ao líder, que a repassa ao destino, havendo duas replicações da mensagem. Se a mensagem é destinada a um nó que não pertence ao grupo, no pior caso a mensagem será replicada para um nó de cada grupo e seus líderes, ou $2n$ replicações. No Epidêmico e no Prophet o número de replicações pode chegar a N. Portanto, o HIGROP replica $O(n)$ mensagens enquanto o Epidêmico e o Prophet replicam $O(N)$ mensagens.

Tal análise demonstra que em redes nas quais o número de nós é pequeno a diferença do *overhead* de comunicação entre o HIGROP e o Epidêmico pode ser insignificante. Porém, ao aumentar o tamanho da rede, a diminuição do *overhead* é conseguida de forma satisfatória.

5.4 Conclusão

Neste Capítulo apresentamos os requisitos e premissas para o funcionamento do nosso protocolo, detalhamos seu funcionamento e fazemos uma análise do custo assintótico do HIGROP em relação ao consumo de memória, processamento e quantidade de men-

sagens enviadas.

O HIGROP é um protocolo de roteamento para redes tolerantes a interrupções de comunicação que cria uma hierarquia virtual na rede, armazenando as mensagens em um *buffer* e repassando-as quando ocorre uma conexão. A hierarquia é feita pelo serviço de identificação de vizinhança, que gerencia os nós vizinhos em cada nó e as mensagens são repassadas pelos nós líderes.

O objetivo do HIGROP é minimizar o *overhead* de comunicação da rede. Isso é obtido ao realizar o agrupamento dos nós e escolhendo nós líderes para serem replicadores de mensagem. Com isso, mostramos que o número de mensagens extras enviadas pelo HIGROP é $O(n)$, sendo n a quantidade de grupos formados na rede.

Capítulo 6

Avaliação de Desempenho

Neste capítulo avaliamos o HIGROP utilizando o simulador ONE (*Opportunistic Network Environment*) [Keränen et al., 2009]. Como DTNs e roteamento oportunístico são tópicos relativamente novos, até onde sabemos o ONE é o único simulador específico para DTNs que dá suporte a contatos oportunísticos e ao paradigma de armazenamento-e-repasse de mensagens. A Seção 6.1 descreve as características da aplicação utilizada na simulação e as métricas avaliadas. O protocolo foi avaliado em cenários diferentes para o estudo detalhado de cada requisito. Comparamos o HIGROP com o protocolo Epidêmico e o Prophet. A Seção 6.2 avalia como a conectividade da redeA Seção 6.3 analisa a influência do tamanho da capacidade do *buffer* de armazenamento no desempenho do protocolo. A Seção 6.4 analisa a escalabilidade do protocolo.

6.1 Caracterização da Simulação

Executamos as simulações em dois cenários: O desempenho em uma área com alta densidade de nós e uma aplicação com características mais realísticas. No primeiro cenário, executamos as simulações em uma área confinada de 200x200m com 100 nós para verificarmos a influência do raio de transmissão no desempenho dos protocolos. Pois, ao aumentar o raio de transmissão dos nós observamos que o tempo de contato entre os nós também aumentavam (Seção 4.3.1). Os parâmetros de mobilidade utilizados nesse cenário são idênticos aos usados na Seção 4.3.1.

No segundo cenário, a aplicação simulada consiste em um cenário de emergência, no qual consideramos uma área de 3000x3000m, com um ponto de interesse com raio de 300m. Esta área equivale a região central da cidade de Belo Horizonte. Como discutido no Capítulo 4, uma rede de emergência é formada por equipes de resgate utilizando dispositivos portáteis, podendo haver nós fixos ou não. Como o objetivo dessa avaliação é observar o comportamento do protocolo em nós móveis não utilizamos nós fixos em

nossos cenários. A rede é formada por nós móveis que podem se mover com velocidade entre 0 e 10.5m/s. Utilizamos os valores padrões do IEEE 802.11 para alcance de rádio e largura de banda dos nós, com 250m e 1Mbps respectivamente.

Avaliamos e comparamos o desempenho do HIGROP com diferentes protocolos de roteamento, utilizando o simulador "*Opportunistic Networking Environment*" (ONE) [Keränen et al., 2009]. O ONE é um simulador de eventos discretos que tem como principais funções modelar a mobilidade dos nós, contato entre os nós de acordo com o raio de alcance de cada nó, roteamento e tratar as mensagens com um modelo de comunicação tolerante a interrupções. Os nós seguem o paradigma *armazenar-transportar-repassar* mensagens (*store-carry and foward*), mantendo-as em um *buffer* caso o nó não tenha conexão direta com o destino.

No ONE um par de nós está em contato se um está dentro do raio de alcance de transmissão do outro, não é implementado interferências por ruído ou degradação de sinal.

Nossa avaliação se concentrou em comparar o HIGROP com o protocolo Epidêmico [Vahdat e Becker, 2000] e com o Prophet [Lindgren et al., 2003], utilizando duas métricas:

- Entrega de mensagens, que consiste ma quantidade de mensagens enviadas que atingiram o destino; e
- *Overhead* relativo, calculado por $(\frac{\text{mensagens transmitidas}-\text{mensagens entregues}}{\text{mensagens entregues}})$. Ou seja, quantas mensagens tiveram que ser transmitidas na rede para cada mensagem entregue corretamente ao destino.

Neste tabalho não focamos em um estudo sistemático sobre a latência fim-a-fim pois o objetivo do protocolo é diminuir o consumo de recursos de armazenamento na rede. Porém, observamos que existe um compromisso entre o *overhead* de comunicação e a latência. Pois é esperado que ao replicar uma mensagem para o maior número de nós possíveis na rede a mensagem tende a atingir o destino com menor tempo. Apresentamos a latência para o cenário discutido na Seção 6.2 e para os outros cenários o comportamento da latência é semelhante.

As mensagens foram geradas com distribuição uniforme entre 20 e 35s e com tamanho entre 50kb e 500kb, que pode representar troca de arquivos de texto e imagens de pequena resolução. O tempo simulado foi de 6000s.

Antes de receber uma mensagem, um nó verifica se existe espaço de armazenamento em seu *buffer*. Caso esse esteja cheio, as mensagens mais antigas são descartadas até que haja espaço para a nova mensagem. Esta política de fila "primeiro a entrar - primeiro a sair" para descarte de mensagens foi utilizada em todos os algoritmos de

roteamento analisados. Um nó somente aceita uma mensagem caso ela já não esteja armazenadas em seu *buffer*.

Analisamos a influência do tamanho do *buffer* disponível para armazenamento de mensagens e em seguida fizemos uma análise da escalabilidade do HIGROP com diversos tamanhos de *buffers*.

No Prophet, em todos os cenários foram utilizados os parâmetros $P_{init} = 0.75$, $\theta = 0.25$, $\gamma = 0.98$ e $k = 30$s como em [Lindgren et al., 2003] e Seção 3.3.2.2.

Para a mobilidade dos nós em um cenário de emergência implementamos um gerador de *traces* utilizando o MME, discutido na Seção 4.3. Foi fixada somente uma instituição e uma região de interesse com 60% de necessidade por essa instituição ($R_\phi = 60\%$). Todos os resultados apresentados possuem 95% de intervalo de confiança. Cada protocolo foi analisado com 15 sementes geradoras para o modelo de mobilidade.

A escolha dos parâmetros do Serviço de Identificação de Vizinhança (SIV) do HIGROP foi feita de acordo com a característica de cada constante. Se o valor de α (o tempo em que o nó pode ficar desconectado sem ser desconsiderado vizinho) fosse muito baixo, não haveria estabilização dos grupos, ou seja, os nós seriam desconsiderados vizinhos em pequenas desconexões. Já um valor alto de α faz com que os grupos se tornem grandes demais, não ocorrendo renovação da lista de vizinhos no SIV. O valor de β (o tempo acumulado que dois nós devem permanecer conectados) foi escolhido de forma a evitar que contatos esporádicos identificarem vizinhança. Se β também for muito alto, os grupos tendem a ser pequenos demais. Portanto, os valores foram fixados em $\alpha = 500s$ e $\beta = 60s$ para todas as simulações realizadas. A cada 30s ($\omega = 30$) cada nó envia um *BEACON* para descobrir os nós que estão em seu raio de alcance. No MME, foram formados grupos de 5 nós e variada a quantidade de grupos de nós na rede.

6.2 Impacto do Raio de Transmissão

Neste cenário variamos o raio de transmissão dos nós em 5m, 10m, 20m e 30m. Como a topologia da rede é densa, ao aumentar o raio de transmissão da rede a conectividade total da rede também é aumentada, ou seja, o raio de transmissão aumenta o número de enlaces ativo a cada instante. A rede é composta por 100 nós em uma área 200x200, todos os nós possuem capacidade de *buffer* de armazenamento infinito. O objetivo deste estudo é verificar o desempenho do protocolo em relação à conectividade da rede.

As Figuras 6.1 e 6.2 mostram a taxa de entrega e o *overhead* relativo ao aumentar o raio de alcance dos nós. Observamos que o Epidêmico e o Prophet possuem desempenho muito semelhante, como os encontros entre os pares de nós são muito frequentes

todos os nós tem alta probabilidade de encontrar o destino, o que distorce a métrica de previsora de entrega do Prophet. O HIGROP apresentou taxa de entrega muito próxima aos outros protocolos, 4% inferior quando o nós possuem um raio de alcance de 5m e 1% quando o raio é de 30m. Contudo, o *overhead* relativo do HIGROP foi significantemente inferior, enquanto o Epidêmico e o Prophet replicaram aproximadamente 100 mensagens para cada mensagem entregue, o HIGROP teve que replicar a mensagem aproximadamente 2 vezes para que esta fosse entregue.

A Figura 6.3 mostra a latência fim-a-fim dos protocolos analisados. Como esperado, o HIGROP apresenta uma latência superior ao Epidêmico e ao Prophet. Ao aumentar o raio de transmissão de cada nó e assim a conectividade da rede, a latência do HIGROP apresenta uma queda, porém ainda é 2 vezes superior ao outros protocolos (com raio de transmissão de 30m). Esse resultado já era esperado, pois como um nó HIGROP só replica uma mensagem para nós específicos (líder ou não participante do grupo) ao invés de replicá-la por todos os nós, o tempo gasto até que a mensagem seja repassada a esses nós específicos impacta na latência fim-a-fim. Com o aumento da conectividade de rede os grupos são formados por mais nós, fazendo com que as mensagens sejam encaminhadas para os nós líderes que a encaminhará para outros grupos ou o destino mais rapidamente.

Observamos um compromisso entre o *overhead* relativo e a latência fim-a-fim. Protocolos epidêmicos em um cenário ideal, com *buffer* de armazenamento infinito, rede densa e com alta conectividade são ótimos em relação a taxa de entrega de mensagens e latência. Contudo, esses cenários não são realistas. Na próxima seção analisamos a influência da capacidade do *buffer* de armazenamento no desempenho dos protocolos.

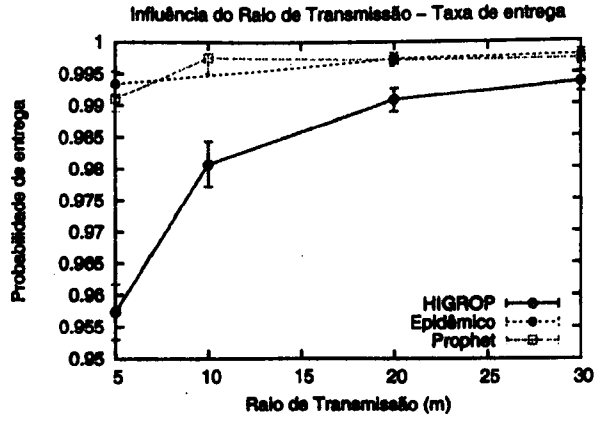

Figura 6.1. Taxa de entrega variando o raio de alcance dos nós

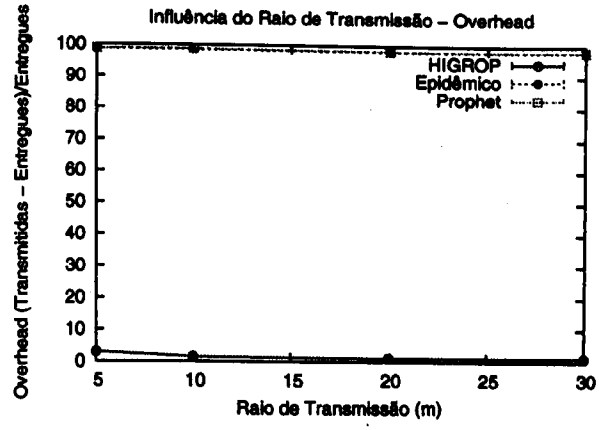

Figura 6.2. Overhead relativo variando o raio de alcance dos nós

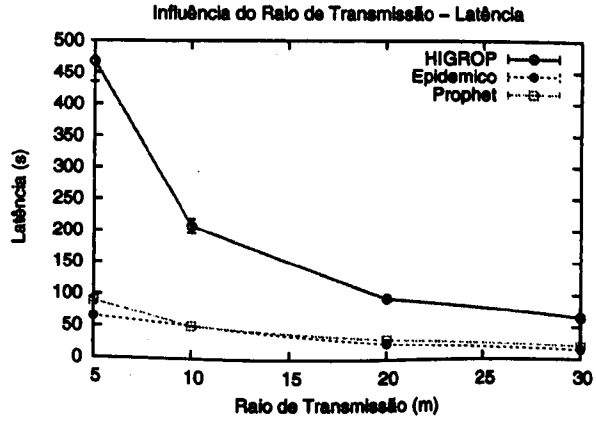

Figura 6.3. Latência variando o raio de alcance dos nós

6.3 Impacto da Capacidade de Armazenamento do *Buffer* de Mensagens

Nesta seção, avaliamos a influência do tamanho da capacidade de armazenamento do *buffer* de mensagens. O objetivo deste estudo foi observar o comportamento de cada protocolo para capacidade de *buffer* pequeno até *buffers* de maiores capacidades. Variamos a capacidade de armazenamento de mensagens entre 5MB e 100MB em cada nó. Executamos os testes com 50 e 100 nós.

Os gráficos das Figuras 6.4 e 6.3 mostram o desempenho dos protocolos em relação à capacidade do *buffer* em uma rede com 50 nós. O algoritmo Epidêmico e o Prophet, por causarem inundação na rede, têm um baixo desempenho com capacidade de *buffers* pequenos. Contudo, o *overhead* relativo teve valores extremamente altos para os dois algoritmos. Com 5MB de capacidade de *buffer*, o Epidêmico enviou em média 1200 mensagens para cada uma que entregou. Tal fato ocorre devido à política de descarte de mensagens do *buffer*. Quando um nó recebe uma mensagem e está com a capacidade

do *buffer* completamente utilizada, o nó exclui a mais antiga do *buffer*. Dessa forma, quando a capacidade de armazenamento é baixa, o nó está excluindo e recebendo uma mesma mensagem várias vezes.

O HIGROP manteve o melhor desempenho de taxa de entrega de mensagens nas situações em que as capacidades de armazenamento dos *buffers* eram pequenas (até 60MB). Contudo, manteve sua taxa de *overhead* praticamente constante. Com 5MB de capacidade de *buffer*, o HIGROP foi superior ao Epidêmico e ao Prophet em média de 65% na taxa de entrega e teve um *overhead* 1400% inferior. No outro extremo, com 100MB de capacidade de *buffer*, o HIGROP teve um desempenho na taxa de entrega de aproximadamente 17% inferior em relação aos outros analisados, mas manteve um *overhead* de 58% abaixo dos apresentados pelos demais algoritmos.

Os gráficos das Figuras 6.6 e 6.7 mostram o mesmo experimento, porém com 100 nós participando da rede. Percebemos um comportamento bastante similar entre os cenários com 50 e 100 nós para taxa de entrega e *overhead* dos algoritmos Epidêmico e Prophet. Em ambos os cenários, o *overhead* relativo manteve um comportamento de distribuição exponencial inversa e o HIGROP uma constante aproximada. Ressaltamos que com 100 nós o número de mensagens extras transmitidas na rede praticamente triplicou no protocolo Epidêmico e no Prophet.

Para *buffer* de armazenamento de mensagens com capacidade maiores que 100MB, os resultados mantêm-se constantes. Os mesmos testes foram refeitos utilizando *buffer* com capacidade de 500MB. Os resultados mostraram que, com o padrão de carga de tráfego de mensagens utilizado, o aumento de capacidade de *buffer* para mais que 100MB não causa diferença nos resultados das métricas utilizadas.

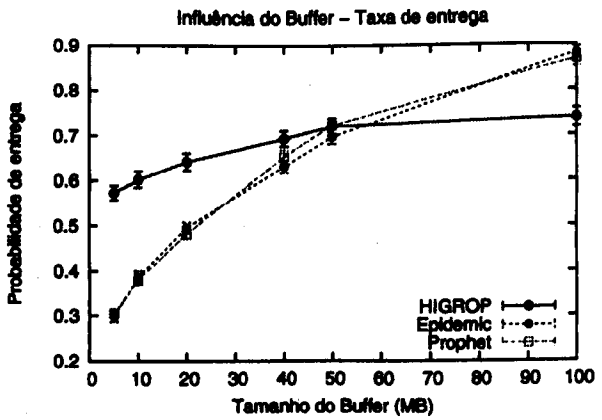

Figura 6.4. Taxa de entrega variando a capacidade do *buffer* de armazenamento com 50 nós na rede

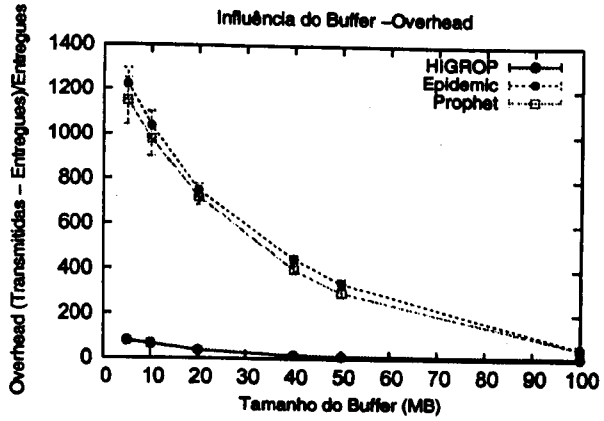

Figura 6.5. Overhead relativo variando a capacidade do *buffer* de armazenamento com 50 nós na rede

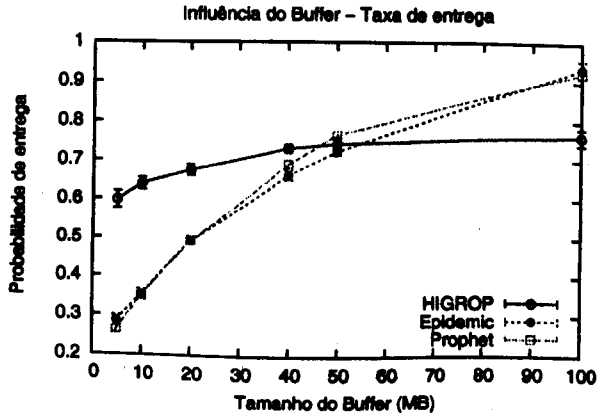

Figura 6.6. Taxa de entrega variando a capacidade do *buffer* de armazenamento com 100 nós na rede

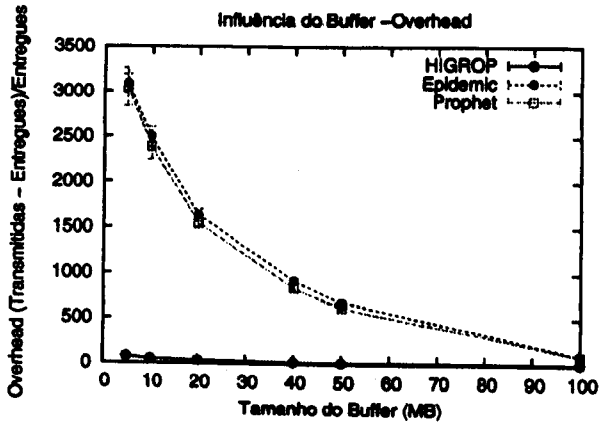

Figura 6.7. Overhead relativo variando a capacidade do *buffer* de armazenamento com 100 nós na rede

6.4 Escalabilidade

Nessa seção analisamos a escalabilidade dos algoritmos em dois cenários. Primeiramente, observamos o comportamento dos algoritmos quando o *buffer* de mensagens tem

capacidade limitada (10MB). Em seguida fizemos a mesma análise utilizando *buffers* com capacidade de 50MB de armazenamento, pois a partir da análise da deção anterior percebemos que as diferenças entre os protocolos com essa capacidade de buffer os protocolos possuem comportamento semelhante. Por fim, verificamos a escalabilidade dos protocolos com um buffer de 100MB. Em todos os testes, variamos a quantidade de nós participantes da rede de 20 a 200 nós. O motivo para o limite de nós se deve aos limites computacionais do ambiente de simulação empregado. O tempo requerido para simulações para redes acima de 200 nós, feitas em um computador QuadCore 2.6GHz, ultrapassa uma semana.

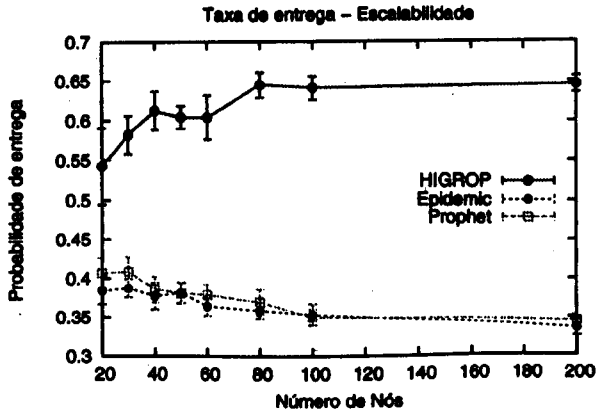

Figura 6.8. Escalabilidade da Taxa de Entrega dos protocolos com *Buffer* de 10MB

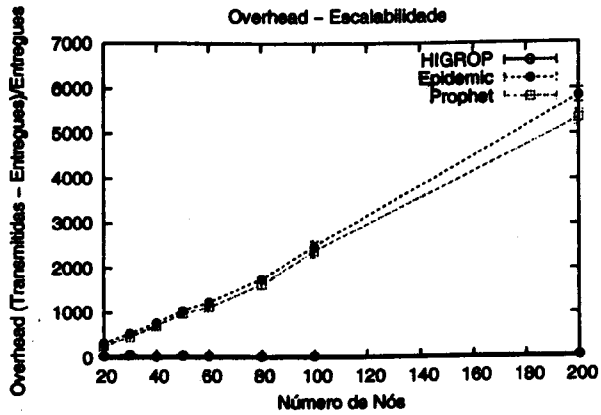

Figura 6.9. Escalabilidade do Overhead dos protocolos com *Buffer* de 10MB

Com a capacidade de *buffer* de 10MB, o HIGROP mostrou-se eficiente na entrega dos dados, mantendo a taxa de entrega crescente em relação à quantidade de nós na rede, enquanto o *overhead* relativo manteve-se praticamente constante. Como esperado, em situações com *buffer* limitado, o algoritmo Epidêmico tem o pior desempenho de taxa de entrega e de *overhead* relativo entre os algoritmos analisados. Os gráficos das Figuras 6.8 e 6.9 mostram os resultados nesse cenário.

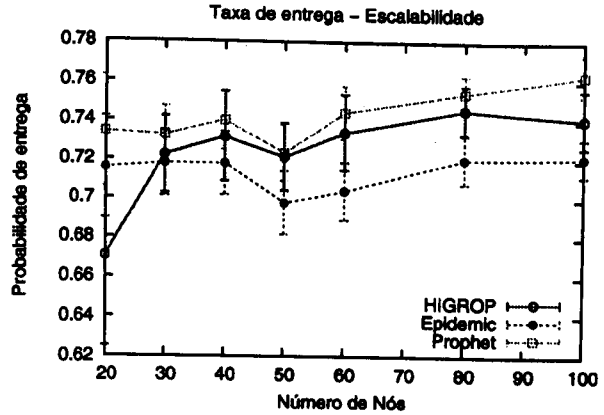

Figura 6.10. Escalabilidade da Taxa de Entrega dos protocolos com *Buffer* de 50MB

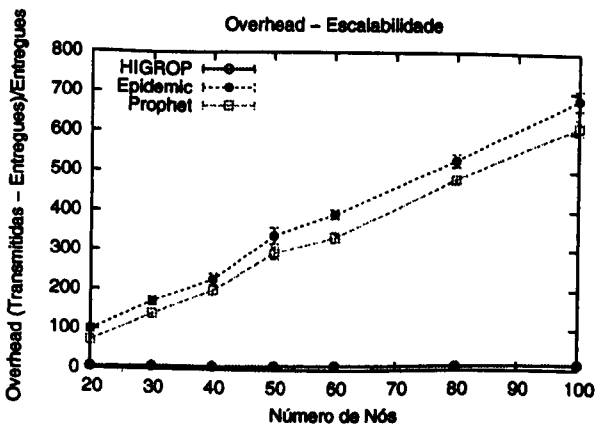

Figura 6.11. Escalabilidade do Overhead dos protocolos com *Buffer* de 50MB

O algoritmo Epidêmico e o Prophet apresentaram taxas de entrega decrescentes em relação ao número de nós. Isso ocorre pois o aumento do número de nós causa o aumento de mensagens transmitidas na rede. Porém, com a capacidade de *buffer* limitada, o *buffer* de mensagens estará constantemente cheio, o que causará descarte das mensagens na fila de entrega.

Observamos na Figura 6.10 que para *buffers* de armazenamento com capacidade de 50MB, os protocolos possuem taxas de entregas bastante semelhantes. De fato, dentro de um intervalo de confiança de 95% não se pode inferir que um protocolo tenha melhor taxa de entrega que outro. Porém o *overhead* de comunicação, mostrado na Figura 6.11 manteve-se estável para o HIGROP e ainda muito alto para o Epidêmico e para o Prophet, chegando a ser 8 vezes o número de nós na rede.

Os gráficos das Figuras 6.12 e 6.13 mostram a escalabilidade dos algoritmos analisados utilizando um *buffer* de mensagens com capacidade de 100MB. O Epidêmico e o Prophet mantêm uma taxa de entrega superior ao HIGROP. Entretanto, o *overhead* de transmissão de dados para o Epidêmico e o Prophet é crescente (linearmente) em

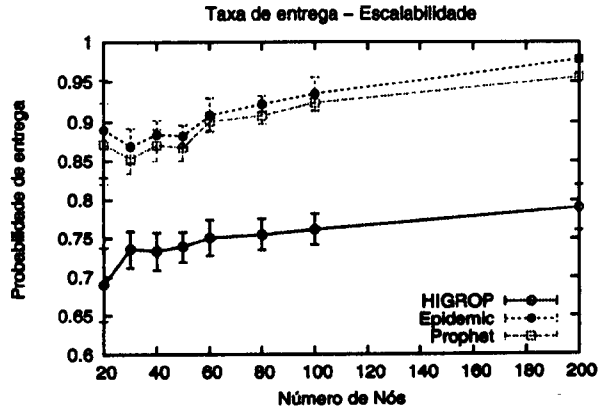

Figura 6.12. Escalabilidade da Taxa de Entrega dos protocolos com *Buffer* de 100MB

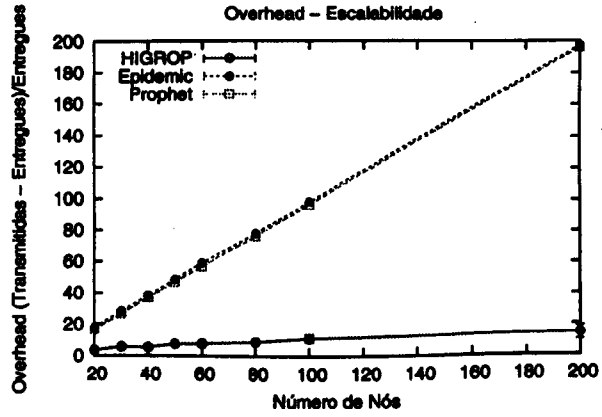

Figura 6.13. Escalabilidade do Overhead dos protocolos com *Buffer* de 100MB

relação ao número de nós. Isso significa que nesses algoritmos, quando há espaço suficiente de armazenamento no *buffer* de mensagens, uma mensagem é replicada até N vezes para cada mensagem entregue, sendo N o número de nós na rede. Já o HIGROP manteve-se praticamente constante no *overhead* de comunicação. A pequena variação é causada pela quantidade de grupos existentes em cada quantidade de nós.

Apesar do HIGROP ter um desempenho inferior quando a capacidade do *buffer* de mensagens é alto, ele se mostrou um algoritmo escalável em todos os cenários analisados. Um compromisso entre memória disponível para armazenamento de mensagens e taxa de entrega fazem do HIGROP uma solução atraente quando os dispositivos que compõem a rede possuem recursos limitados.

6.5 Conclusão

Este capítulo apresentou uma avaliação por simulação do protocolo HIGROP. As simulações procuraram se aproximar de um cenário de emergência em uma grande cidade.

Para isso, utilizamos o modelo de mobilidade proposto no Capítulo 4.

Apresentamos as premissas e os requisitos para o funcionamento do protocolo. Como o HIGROP é um protocolo de roteamento que agrupa os nós considerados vizinhos e elege um líder para cada grupo, é necessário que os nós participantes da rede se movam em grupos como ocorre em situações de emergência.

Analisamos e comparamos o HIGROP em relação ao Epidêmico e o Prophet quanto a taxa de entrega de mensagens e o *overhead* de comunicação. Avaliamos a influência da capacidade do *buffer* de armazenamento e a escalabilidade dos protocolos.

Mostramos que quando o *buffer* de armazenamento é de até 50MB, o HIGROP teve um desempenho superior na taxa de entrega, mantendo o *overhead* de comunicação praticamente constante. Para *buffers* superiores a 50MB o HIGROP teve o desempenho de aproximadamente 17% inferior aos outros protocolos. Tal resultado já era o esperado visto que os outros protocolo replicam as mensagens em mais nós da rede, se não ocorre descarte de mensagens devido ao estouro de capacidade do *buffer* a mensagem é propagada pela rede até que atinja o destino. Os resultados mostraram curvas semelhantes quando duplicado o número de nós da rede, a grande diferença está no *overhead* de comunicação que em uma rede com 100 nós é quase o triplo do *overhead* quando com 50 nós para o Epidêmico e o Prophet, enquanto no HIGROP se manteve constante. Acreditamos que o comportamento do Prophet foi muito semelhante ao do Epidêmico devido as características de contatos na rede. Os encontros entre os nós eram tão frequentes que eles destorcem a métrica de previsora de entrega no Prophet, fazendo com que todos os nós tenham alta probabilidade de entrega para outros nós. Com isso, o Prophet apresenta um comportamento epidêmico.

Analisamos a escalabilidade dos protocolos com duas configurações de tamanho de *buffer*, 10 e 100Mb. Observamos que com o *buffer* de armazenamento pequeno o HIGROP é aproximadamente 33% superior ao Epidêmico e o Prophet. Contudo, com *buffer* maior o HIGROP chega a ser 22% inferior ao Epidêmico. Mas para isso o *overhead* relativo do Epidêmico e do Prophet cresce linearmente, chegando a 200 mensagens enviadas para cada mensagem entregue (com 200 nós), enquanto o HIGROP enviou 15 mensagens extras para entregar cada uma na rede com 200 nós.

Concluímos que existe um compromisso entre o tamanho do *buffer* disponível para armazenamento de mensagens e a taxa de entrega em algoritmos epidêmicos. Em cenários que estes recursos são limitados, esses algoritmos podem não ser aplicáveis. O HIGROP apresentou uma boa relação taxa de entrega por consumo de recursos, porém em alguns cenários, precisa alcançar uma melhor taxa de entrega para prover confiabilidade na rede.

Capítulo 7

Conclusões

Prover comunicação de dados para equipes de resgate que atuam em cenários de emergência é um grande desafio, haja vista que nesses cenários existe a possibilidade de que toda a infra-estrutura de comunicação possa ter sido parcialmente ou totalmente destruída.

Este trabalho apresentou um estudo sobre redes em cenários de emergência, quando não existe infra-estrutura de comunicação disponível, chamadas de redes de emergência. A partir deste estudo desenvolvemos um modelo de mobilidade que representa a movimentação das equipes de resgate em direção às áreas de interesse, que pode ser um hospital, quartel, a área afetada, etc. Esse modelo, chamado de Modelo de Mobilidade de Nós em Cenários de Emergência (MME), estende o modelo de mobilidade RPGM introduzindo o conceito de áreas de interesse, sendo que pode haver uma ou mais regiões de interesse com necessidade R_ϕ de ser visitada por grupos de nós que pertencem a instituição ϕ. Avaliamos as características dos tempos de contato e os tempos entre contatos dos nós utilizando os modelos MME, *Random-way Point* e o RPGM e verificamos que o MME produz um cenário onde a rede possui contatos mais duradouros.

Nessas redes, devido à mobilidade e outras interferências, os algoritmos de roteamento ad hoc móveis tradicionais podem não ser eficientes, pois estes assumem que há um caminho fim-a-fim entre a origem e o destino. Propomos nesta dissertação um novo algoritmo de roteamento para redes tolerantes a interrupções, batizado de HIGROP, que tem como objetivo aumentar a taxa de entrega de dados em redes intermitentes sem afetar o *overhead* de comunicação de rede. Esta diminuição no *overhead* de transmissão é essencial quando os dispositivos que formam a rede *ad hoc* possuem recursos limitados, como por exemplo em redes de sensores sem fios.

Analisamos nosso algoritmo utilizando um modelo de mobilidade que reflete propriedades de cenários de emergência. O HIGROP se mostrou escalável em todos os

cenários analisados, visto que o aumento do número de nós não afeta o *overhead* de transmissão de dados, como ocorre com os algoritmos Epidêmico e Prophet. O Epidêmico e o Prophet exigem que se tenha capacidade de armazenamento de mensagens proporcional ao número de nós e ao padrão de tamanho e frequência de mensagens na rede. Em dispositivos de rede com recursos limitados o HIGROP se mostrou eficiente na taxa de entrega sem afetar o *overhead* de comunicação da rede. Percebemos um compromisso entre taxa de entrega e *overhead* de comunicação.

7.1 Contribuições

A principal contribuição desta dissertação é o desenvolvimento de um protocolo de roteamento tolerante a interrupções para redes móveis *ad hoc*. O HIGROP cria uma hierarquia virtual na rede agrupando os nós considerados vizinhos e elegendo um líder para cada grupo, sendo os nós líderes responsáveis pela replicação de mensagem. Desse modo, o HIGROP produz um baixo *overhead* de comunicação. Utilizando o paradigma de armazenar-repassar, cada nó armazena as mensagens em um *buffer* caso não haja conexão com outros nós e então as repassam quando ocorre uma conexão.

Desenvolvemos um modelo de mobilidade sintético que possui características de movimentação de equipes de resgate em cenários de emergência, batizado de MME. No MME são definidas R regiões de interesse e I instituições, cada grupo é classificado em uma instituição ϕ, os grupos visitam as regiões de acordo com a necessidade de uma região por uma determinada instituição R_ϕ. Utilizamos esse modelo para analisar o HIGROP comparando-o com os protocols Epidêmico e o Prophet.

Os resultados parciais foram publicados em um artigo completo em conferência nacional e obtivemos ainda outras duas publicações de artigos completos em tema paralelo ao desta dissertação (vide Apêndice A). Estamos elaborando um artigo para ser submetido a conferência internacional.

7.2 Trabalhos Futuros

Como trabalhos futuros, pretendemos continuar o desenvolvimento do HIGROP adicionando características probabilísticas, de forma que os nós líderes repassem uma determinada mensagem para nós de outros grupos que tenham maiores probabilidades de entregá-la ao destino.

Atualmente, escolha do líder é baseada na política de nó vizinho com menor identificador. Acreditamos que a utilização de um método mais eficiente, como nó com

maior quantidade de vizinhos conectados, também poderia trazer melhorias na taxa de entrega.

Além disso, pretendemos fazer uma análise sobre o impacto de políticas de descarte de mensagens que sigam outros modelos de filas além do modelo "Primeiro-entrar, Primeiro-Sair" utilizado neste trabalho.

Apêndice A

Publicações

Durante o mestrado, foram publicados artigos em conferências e periódicos nacionais relatando resultados parciais dos estudos realizados. A lista abaixo contém publicações resultantes de trabalhos diretamente relacionados e paralelos ao tema da dissertação, que foram desenvolvidos durante o mestrado.

1. Vinícius F. S. Mota, Thiago H. Silva, José Marcos S. Nogueira. Introduzindo Tolerância a Interrupções em Redes Ad Hoc Móveis para Cenários de Emergência.*In 27º Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos, 2009.*

2. Thiago H. Silva, Vinícius F. S. Mota, Everthon Valadão, Jussara Almeida, Dorgival Guedes. Caracterização do Comportamento dos Espectadores em Transmissões de Vídeo ao Vivo Geradas por Usuários. *In 27º Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos, 2009.*

3. Thiago H. Silva, Vinícius F. S. Mota, Roteamento de Fluxos de Vídeo ao Vivo em Redes Par-a-Par Heterogêneas. *In Workshop Peer-to-Peer (WP2P), 26º Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos, 2008.*

Apêndice B

Função de Distribuição Cumulativa Complementar

A função de distribuição cumulativa complementar (do inglês *Complementary Cumulative Distribution Function* CCDF) é utilizada para visualizar a fração das amostras que são maiores do um determinado valor. Formalmente:

$P[X > x] = 1 - P[X \leq x] = 1 - FX(x)$

As CCDFs dos tempos de contatos (TC) e os tempos entre contatos (TEC) foram calculadas a partir dos arquivos com a movimentação dos nós para cada modelo de mobilidade. A partir da análise desses arquivos foram gerados para o TC e para o TEC novo arquivos com tuplas de tempo (t_i) (de contato ou entre contatos) e quantidade (q_i) de conexões duraram este tempo. O arquivo possui a seguinte formatação:

$$t_i \; q_i$$
$$\vdots$$
$$t_n \; q_n$$

O cálculo da ccdf é feito então em dois passos. No primeiro, calcula-se a soma de todas as quantidades de conexões (Eq. B.1). No segundo passo, para cada tempo de duração (de contato ou entre contatos) é calculada a quantidade de conexões acumuladas, a CCDF para cada tempo (t_i) é feita com o complemento da média do tempo acumulado (Eq. B.2).

$$\epsilon = \sum_{i=0}^{n} q_i \tag{B.1}$$

$$ccdf(t_i, q_i) = (t_i, 1 - \frac{\sum_{i=0}^{n}\sum_{j=i}^{n} q_j}{\epsilon}) \tag{B.2}$$

Referências Bibliográficas

Cai, H. e Eun, D. Y. (2008). Toward stochastic anatomy of inter-meeting time distribution under general mobility models. In *MobiHoc '08: Proceedings of the 9th ACM international Symposium on Mobile Ad Hoc Networking and Computing*, pp. 273–282. ACM.

Camp, T.; Boleng, J. e Davies, V. (2002). A survey of mobility models for ad hoc network research. *Wireless Communications and Mobile Computing*, 2(5):483–502.

Cerf, V.; Burleigh, S.; Hooke, A.; Torgerson, L.; Durst, R.; Scott, K.; Fall, K. e Weiss, H. (2007). Delay-Tolerant Networking Architecture. Technical report, Internet RFC 4838.

Cerf, V.; Burleigh, S.; Hooke, A.; Torgerson, L.; Durst, R.; Scott, K.; Travis, E. e Weiss, H. (2001). Interplanetary Internet (IPN): Architectural Definition. *Relatório técnico, IPN Research Group.*

Cramer, C.; Stanze, O.; Weniger, K. e Zitterbart, M. (2004). Demand-driven clustering in manets. In *International Conference on Wireless Networks*, pp. 81–87. CSREA Press.

DTNWG (2008). Delay-tolerant network work group. http://www.dtnwg.org/.

Ephremides, A.; Wieselthier, J. e Baker, D. (1987). A design concept for reliable mobile radio networks with frequency hopping signaling. *Proceedings of the IEEE*, 75(1):56–73.

Fall, K. (2003). A delay-tolerant network architecture for challenged internets. *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*, pp. 27–34.

Fall, K. e Farrell, S. (2008). DTN: an architectural retrospective. *IEEE Journal on Selected Areas in Communications*, 26(5):828–836.

Gerla, M.; Chen, L.; Lee, Y.; Zhou, B.; Chen, J.; Yang, G. e Das, S. (2005). Dealing with node mobility in ad hoc wireless network. *Formal Methods for Mobile Computing*, 3465:69–106.

Grossglauser, M. e Tse, D. (2002). Mobility increases the capacity of ad hoc wireless networks. *IEEE/ACM Transactions on Networking (TON)*, 10(4):477–486.

Handorean, R.; Gill, C. e Roman, G. (2004). Accommodating Transient Connectivity in Ad Hoc and Mobile Settings. *Proceedings Pervasive Computing: Sec. International Conference*, pp. 18–23.

Hong, X.; Xu, K. e Gerla, M. (2002). Scalable routing protocols for mobile ad hoc networks. *IEEE Network*, 16:11–21.

Jain, S.; Fall, K. R. e Patra, R. K. (2004). Routing in a delay tolerant network. *ACM SIGCOMM Computer Communication Review*, pp. 145–158.

Johnson, D. e Maltz, D. (1996). Dynamic source routing in ad hoc wireless networks. *Kluwer International Series in Engineering and Computer Science*, pp. 153–179.

Jubin, J. e Tornow, J. (1987). The DARPA packet radio network protocols. *Proceedings of the IEEE*, 75(1):21–32.

Karagiannis, T.; Boudec, J.-Y. L. e Vojnovic, M. (2007). Power law and exponential decay of inter contact times between mobile devices. In Kranakis, E.; Hou, J. C. e Ramanathan, R., editores, *MOBICOM*, pp. 183–194. ACM.

Keränen, A.; Ott, J. e Kärkkäinen, T. (2009). The one simulator for dtn protocol evaluation. In *SIMUTools '09: Proceeding of the 2nd International Conference on Simulation Tools and Techniques*, New York, NY, USA. ACM.

Kwon, T. e Gerla, M. (2002). Efficient flooding with Passive Clustering (PC) in ad hoc networks. *ACM SIGCOMM Computer Communication Review*, 32(1):44–56.

Lindgren, A.; Doria, A. e Schelen, O. (2003). Probabilistic routing in intermittently connected networks. *Mobile Computing and Communications Review*, 7(3):19–20.

Liu, C. e Wu, J. (2007). Scalable routing in delay tolerant networks. In *Proceedings of the 8th ACM international symposium on Mobile ad hoc networking and computing*, pp. 51–60. ACM Press New York, NY, USA.

Macedo, F. D. (2006). Um protocolo de roteamento para redes de sensores sem fio adaptável por regras de aplicação. Master's thesis, Universidade Federal de Minas Gerais.

Manet (2008). Ietf working group on mobile ad-hoc networks. http://www.ietf.org/html.charters/manet-charter.html.

Merugu, S.; Ammar, M. e Zegura, E. (2004). Routing in space and time in networks with predictable mobility. Technical report, Georgia Institute of Technology.Technical Report GIT-CC-04-7.

Murthy, S. e Garcia-Luna-Aceves, J. (1996). An efficient routing protocol for wireless networks. *Mobile Networks and Applications*, 1(2):183–197.

ns2 (2008). *NS-2 Simulator*. Information Science Institute. http://www.isi.edu/nsnam/ns/.

Oliveira, L.; Siqueira, I. e Loureiro, A. (2003). Evaluation of Ad-Hoc Routing Protocols under a Peer-to-Peer Application. *Proc. IEEE WCNC 2003*, pp. 1143–1148.

Ott, J.; Kutscher, D. e Dwertmann, C. (2006). Integrating dtn and manet routing. In *CHANTS '06: Proceedings of the 2006 SIGCOMM workshop on Challenged networks*, pp. 221–228, New York, NY, USA. ACM Press.

Parekh, A. (1994). Selecting routers in ad-hoc wireless networks. In *Proceedings SBT/IEEE Intl Telecommunications Symposium*, pp. 420–424.

Pei, G.; Gerla, M.; Hong, X. e Chiang, C. (1999). A wireless hierarchical routing protocol with group mobility. In *Wireless Communications and Networking Conference, 1999. WCNC. 1999 IEEE*, pp. 1538–1542.

Perkins, C. e Bhagwat, P. (1994). Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers. *Proceedings of the conference on Communications architectures, protocols and applications*, pp. 234–244.

Perkins, C. E. e Royer, E. M. (1999). Ad-hoc on-demand distance vector routing. *proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, 2:90–100.

Rao, R.; Eisenberg, J. e Schmitt, T. (2007). Improving Disaster Management: The Role of IT in Mitigation, Preparedness, Response, and Recovery. *National Research Council, National Academy of Sciences Washington DC, ISBN: 0-309-66744-5.*

SNDC (2009). *Defesa Civil*. Secretaria Nacional de Defesa Civil. http://www.defesacivil.gov.br.

Spyropoulos, T.; Psounis, K. e Raghavendra, C. (2005). Spray and wait: an efficient routing scheme for intermittently connected mobile networks. In *ACM SIGCOMM workshop on Delay-tolerant networking*, pp. 252–259. ACM.

Su, W.; Lee, S. e Gerla, M. (2000). Mobility prediction in wireless networks. *IEEE MILCOM 2000: 21st Century Military Communications Conference Proceedings*, 1:491–495.

Vahdat, A. e Becker, D. (2000). Epidemic routing for partially connected ad hoc networks. *Tec. Report, Duke University.*

Warthman, F. (2003). Delay-tolerant networks. *A Tutorial. DTN Research Group Internet Draft.*

Xue, F. e Kumar, P. R. (2004). The number of neighbors needed for connectivity of wireless networks. *Wireless Network*, 10(2):169–181.

Yu, J. e Chong, P. (2005). A survey of clustering schemes for mobile ad hoc networks. *Communications Surveys & Tutorials, IEEE*, 7(1):32–48.

Zhang, Z. (2006). Routing in intermittently connected mobile ad hoc networks and delay tolerant networks: overview and challenges. *Communications Surveys & Tutorials, IEEE*, 8(1):24–37.