FACULDADE FARIAS BRITO
CIÊNCIA DA COMPUTAÇÃO

THALES JONES ROSA RIBEIRO

Estudo Comparativo de Protocolos de Roteamento para Redes Sem Fio *Ad Hoc* Móveis e Suas Aplicações em Atividades Emergenciais.

Fortaleza, 2010

THALES JONES ROSA RIBEIRO

Estudo Comparativo de Protocolos de Roteamento para Redes Sem Fio *Ad Hoc* Móveis e Suas Aplicações em Atividades Emergenciais.

Monografia apresentada para obtenção dos créditos da disciplina Trabalho de Conclusão do Curso da Faculdade Farias Brito, como parte das exigências para graduação no Curso de Ciência da Computação.

Orientador: José Helano Matos Nogueira, Msc.

Fortaleza, 2010

ESTUDO COMPARATIVO DE PROTOCOLOS DE ROTEAMENTO PARA REDES SEM FIO *AD HOC* MÓVEIS E SUAS APLICAÇÕES EM ATIVIDADES EMERGENCIAIS.

Thales Jones Rosa Ribeiro

PARECER _____

NOTA: FINAL (0 – 10): _____

Data: _/_____/_____

BANCA EXAMINADORA:

_____
MSc. José Helano Matos Nogueira
Orientador

_____
MSc. Murilo Eduardo Ybanez Nascimento
Examinador

_____
MSc. Sérgio Araújo Yunes
Examinador

Dedico este trabalho à minha família, em especial a Elidiane, pois representaram a motivação central para a conclusão do mesmo.

AGRADECIMENTOS

Ao Orientador Msc José Helano, pela coordenação, disponibilidade, ajuda, e por acreditar neste trabalho o que permitiu que o projeto fosse concluído com qualidade.

Ao Vinícius Lima por criticar, alertar, relembrar e revisar, tarefas que exigiram esforço e muita paciência. Agradecê-lo principalmente por alertar pontos de divergência e estratégias a se tomar para uma melhor conclusão do trabalho.

À Elidiane Martins por acreditar, incentivar integralmente e principalmente não deixar esmorecer em nenhum momento depositando todas as fichas em meu esforço e dedicação.

Aos professores e colegas da faculdade que ajudaram de maneira direta ou indireta para a minha formação.

Aos amigos e profissionais de trabalho por se colocarem a disposição.

E a todos que puderam contribuir de alguma forma.

RESUMO

Os constantes avanços tecnológicos vêm proporcionando um cenário cada vez mais voltado para a mobilidade e integração de dispositivos. A comunicação sem fio vem evoluindo bastante se aliando à grande variedade de dispositivos portáteis. Isso vem contribuindo para que as redes móveis sejam cada vez mais utilizadas, rompendo as barreiras de conectividade limitada em tempo e localidade. Nesse contexto, inseriram-se as redes *ad hoc* móveis, que são formadas por um conjunto de dispositivos móveis conectados sem nenhuma ligação física. Essas redes não possuem infraestrutura e os próprios dispositivos são responsáveis por controlar e manter a conectividade entre eles. As redes *ad hoc* são temporárias e arbitrárias, portanto sua utilização é geralmente emergencial. Na tentativa de maximizar o tempo de conectividade e minimizar diversas restrições de ambiente foram criados os protocolos de roteamento. Embora exista uma grande diversidade de protocolos de roteamento para os mais variados tipos de restrições, a escolha de um protocolo para implantação ainda é um trabalho de muita complexidade. É necessário saber que fatores são mais relevantes para o ambiente de aplicação. Neste contexto inseri-se esta monografia que apresenta uma análise comparativa entre os principais protocolos de roteamento de redes *ad hoc* e suas aplicações em atividades emergenciais. Este trabalho tem sua contribuição no fornecimento de uma análise entre os principais protocolos de roteamento de redes *ad hoc*, ressaltando quais são os mais apropriados para determinadas situações emergenciais.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

AP	Acess Point
AES	Advanced Encription Standard
AODV	Ad hoc On-demand Distance Vector routing
DFS	Dynamic Frequency Selection
DSDV	Destination Sequenced Distance Vector
DSR	Dynamic Source Routing
DSSS	Direct Sequence Spread Spectrum
DV	Distance Vector
ENIAC	Electronic Numerical Integrator And Calculator
FHSS	Frequency Hopping Spread Spectrum
FSR	Fisheye State Routing
GPS	Global Processing System
GSR	Global State Routing
IEEE	Institute of Electrical and Electronic Engineers
IP	Internet Protocol
LS	Link State
MAC	Medium Access Control
MANET	Mobile Ad Hoc Network
MIMO	Multiple Input Multiple Output
OFDM	Orthogonal Frequency Division Multiplexing
PDA	Personal Digital Assistants
RREP	Route Replay
RREQ	Route Request
RRER	Route Error
SAFER	Secure And Fast Encryption Routine
TFC	Transmit Power Control
TTL	Time To Life
WI-FI	Wireless Fidelity
WBAN	Wireless Body Area Network
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network

WPAN Wireless Personal Area Network

WRP Wireless Routing Protocol

WWAN Wireless Wide Area Network

VOIP Voz sobre IP

ZHLS Zone-based Hierarquical Link State

ZRP Zone Routing Protocol

INTRODUÇÃO

As redes sem fio têm vivenciado constantes avanços tecnológicos nos últimos anos, tais como facilidade de instalação e manuseio; melhorias na transmissão, desempenho, conectividade, mobilidade, segurança e privacidade na rede (NOGUEIRA, 2009, p. 15). O aumento de sua popularização se dá, principalmente, pela facilidade de instalação, onde para montar-se uma rede sem fio infraestruturada são necessários apenas dispositivos que possuam placa de rede sem fio e pontos de acessos, enquanto nas redes com fio é preciso instalar cabos, pontos de rede em diversos locais, utilizar ferramentas para testes e medições, bem como muitas vezes quebrar paredes e pisos para se ter uma rede local. Além da dificuldade na instalação, outro aspecto que merece um destaque maior para o aumento da popularização das redes sem fio é a mobilidade, que proporciona maior praticidade e flexibilidade, possibilitando acesso nos mais variados ambientes, como em faculdades, shoppings, aeroportos, restaurantes, além de proporcionar um acesso a partir de dispositivos que não sejam necessariamente um computador, como aparelhos telefônicos e *palms*.

Com a utilização cada vez maior das redes sem fio, foi possível perceber que os principais motivos para esse crescimento são a rapidez na instalação e manutenção, e a praticidade. Contudo, junto a esse crescimento, foram criados também novos desafios e paradigmas, como realizar a comunicação entre dispositivos sem a necessidade de muitos equipamentos e investimentos. Nesse contexto inserem-se as redes sem fio sem infraestrutura ou redes *ad hoc*. Essas redes oferecem maior praticidade, maior largura de banda e baixo custo quando comparada às redes com infraestrutura, pois nelas não há necessidade de utilização de estações base e pontos de acesso. Sua utilização está geralmente associada a atividades temporárias de poucos dias ou até mesmo por poucas horas. No entanto sua

característica mais marcante é a mobilidade, pois fornece um ganho expressivo em tarefas que envolvem deslocamentos, alta flexibilidade e comunicação a distâncias curtas.

As redes *ad hoc* também podem ser chamadas de redes sem fio *ad hoc* móveis ou MANETs (*Mobile Ad Hoc Networks*). Um exemplo de MANET amplamente utilizada na atualidade é o *Bluetooth*. Essa tecnologia já é bastante difundida no mercado mundial em diversos equipamentos, como em fones de ouvido, celulares, *laptops* e até mesmo em aparelhos de sons e TVs. A tecnologia *Bluetooth* proporciona comunicação sem fio e sem infraestrutura para transferência de arquivos, músicas, fotos, vídeos e até mesmo compartilhamento de conexão.

No entanto, como toda e qualquer rede, as redes *ad hoc* também apresentam algumas limitações, como restrição de energia de bateria, altas taxas de erros, limitação de largura de banda, dentre outros. Para o controle dessas limitações é necessário a utilização de protocolos de roteamento eficiente e eficazes, que promovam a redução da quantidade de mensagens enviadas, quantidade de processamento e dados transmitidos, e que sejam capazes de recuperar a conexão entre fonte emissora e fonte receptora mesmo quando haja mudança na topologia da rede.

Portanto, esse trabalho insere-se no contexto de tecnologias da computação aplicadas na área de redes de computadores sem fio e tem como objetivo principal apresentar os principais protocolos de roteamento de redes *ad hoc* móveis, bem como realizar uma análise comparativa entre suas principais características. Além disso, serão propostos a partir da análise comparativa quais protocolos se adéquam melhor a determinadas situações emergenciais.

Este trabalho será organizado em seis capítulos que englobam desde o referencial teórico até a comparação entre os protocolos de roteamento de redes *ad hoc* e definições de quais protocolos melhor se adaptam aos cenários de aplicação emergenciais. No primeiro capítulo será descrito um breve histórico das redes sem fio e seus principais conceitos, contemplando sua composição, categorias e padrões que norteiam essas redes. No capítulo 2 serão discutidos os principais conceitos de redes *ad hoc* que fornecerão as bases do conhecimento necessário sobre a tecnologia. No capítulo terceiro serão apresentados alguns dos principais protocolos de roteamento de redes *ad hoc* de acordo com suas classificações.

No capítulo subsequente será realizado um estudo comparativo das principais características dos protocolos de roteamento discutidos no capítulo anterior. No capítulo 5 serão abordados cenários de aplicação de redes *ad hoc*, bem como que tipos de protocolos melhor se adéquam para cada cenário citado. Por fim, o capítulo 6 que exibe as conclusões finais do trabalho.

1. REDES SEM FIO

Com a popularização do uso dos computadores e da Internet nos últimos anos, o mundo vem sofrendo constantes revoluções tecnológicas. As redes de computadores que antes eram conhecidas apenas nos meios militares e acadêmicos, tornaram-se parte do cotidiano de empresas, instituições de ensino e lares. “O aumento da necessidade do uso constante de computadores em todas as esferas sociais e acesso fácil e rápido a Internet fez com que “culminasse” no que se chama hoje de redes sem fio.” Essas redes têm sido cada vez mais utilizadas para comunicação entre dispositivos de diversos tipos, tais como *notebooks*, *PDAs* (Personal Digital Assistants), telefones celulares, dentre outros (NOGUEIRA, 2009).

O objetivo deste capítulo é contextualizar fundamentos de redes sem fio, iniciando com um breve histórico dessa tecnologia, em seguida será abordada a tecnologia sem fio bem como suas vantagens e desvantagens, serão descritas também as categorias de redes sem fio e finalizando com os tipos de padrões de redes sem fio existentes.

1.1 Histórico

Dentre as esferas sociais, a área de tecnologia da informação é quem vivencia maior influência dos avanços tecnológicos nas últimas décadas. Embora sua ascensão tenha ocorrido recentemente, quando comparada a setores industriais (por exemplo, o de automóveis, transporte aéreo, telefônico, etc.), foi espetacular o avanço tecnológico que os computadores sofreram em um curto período de tempo. É importante citar que o primeiro computador existente veio a ser lançado somente no ano de 1945, o chamado ENIAC (*Electronic Numerical Integrator And Calculator*) (TANENBAUM, 2003). De acordo com

Nogueira (2009, p.13), durante as duas primeiras décadas de existência dos computadores, havia somente grandes computadores conhecidos como *Mainframes*. Esses computadores se caracterizavam por possuírem sistemas e arquitetura altamente acoplados e centralizados. Eles ficavam em salões com paredes de vidros e deixavam pessoas que não trabalhavam com eles admiradas com tamanha invenção eletrônica. De acordo com Tanenbaum (2003), dentre as diversas inovações tecnológicas, foi possível seguir o avanço da telefonia em escala mundial, a invenção dos rádios e televisão, a criação e crescimento acentuado da indústria computacional, dentre outros.

Como consequência do acelerado crescimento tecnológico, é cada vez menor as diferenças entre coleta, transporte, armazenamento e tratamento de informações. Hoje é possível coordenar diversas filiais de empresas em locais dispersos com poucos cliques em botões (COMER, 2007). Com o constante crescimento da capacidade de colher e tratar a informação torna-se cada vez maior a busca por formas mais eficientes e modernas de gerir a informação (TANENBAUM, 2003). Com isso, a idéia de se ter um "CPD – Centro de Processamento de Dados", contendo um único computador em um salão atendendo a todas as necessidades computacionais de uma empresa se tornou ultrapassado. As redes de computadores vieram para quebrar esse paradigma centralizado (NOGUEIRA, 2009).

Existem várias definições de redes de computadores, dentre elas foram escolhidas as de dois autores renomados que foram utilizadas como base para este trabalho. De acordo com Tanenbaum (2003) e Comer (2007), as redes de computadores nada mais são que diversos computadores interconectados por um meio físico. Ou seja, dois ou mais computadores estão em rede ou formam uma rede de computadores quando estão interconectados por algum meio físico e tem a capacidade de trocarem informações uns com os outros. Existem diversos meios físicos de interconexão, como os de fios de cobre, fibras óticas, microondas, ondas de infravermelho e até mesmo satélites de comunicações (KUROSE; ROSS, 2006).

1.2 Tecnologia Sem Fio

De acordo com Tanenbaum (2003), em 1901 um físico italiano chamado Guglielmo Marconi conseguiu demonstrar como funcionava um telégrafo sem fio que

realizava transmissão de um navio ao continente através de código Morse. Os sistemas digitais sem fio mais modernos possuem a mesma idéia de codificação, porém com desempenho bem melhor. Um sistema de comunicação é constituído de um emissor e um receptor que estão conectados por algum meio físico de comunicação (KWOK; LAU, 2007 apud NOGUEIRA, 2009, p. 14). As redes sem fio operam basicamente por ondas de radiofrequência como meio de transmissão. Seu desenvolvimento durou vários anos e seu primeiro padrão foi aprovado em 1997, o IEEE 802.11 (NOGUEIRA, 2009).

É evidente a ascensão que as redes sem fio e seus serviços móveis vem obtendo. Com os avanços tecnológicos, em especial das tecnologias de comunicação sem fio, tornou-se comum a conexão de diversos tipos de dispositivos para as mais variadas aplicações. Isso acarreta maior controle de acesso, acesso difundido e compartilhamento de informação entre os dispositivos, aumentando assim a familiarização e, consequentemente, a experiência dos usuários com essa nova tecnologia (COMER, 2007). O crescente aumento do uso das redes sem fio e dos seus meios de acesso estão permitindo que haja comunicação entre os mais variados tipos de equipamentos, portáteis ou não. A tendência é que todos os dispositivos venham num futuro bem próximo com algum tipo de interface sem fio embutida (DIXIT; PRASAD, 2005). Para que isso ocorra, serão necessárias muitas pesquisas na área de redes de computadores sem fio, envolvendo transmissão, desempenho, conectividade, mobilidade, segurança e privacidade na rede. Atualmente há vários tipos de equipamentos portáteis como *notebooks, PDAs* e *smartphones*. Em um futuro próximo, será possível montar uma rede sem fio sem complicações, a qual permitirá que uma ou mais pessoas ou até mesmo uma organização possua conectividade, controle e acesso sem fio a um ou vários dispositivos eletrônicos. Esse é o ponto chave que motiva o uso das redes sem fio (NOGUEIRA, 2009, p. 15).

Para propor aplicações e investimentos em tecnologias novas é necessário, antes de tudo, realizar uma análise de possíveis custos e benefícios que poderão ser gerados com a implantação dessa tecnologia. Não fugindo a essa linha, Webb (2007), em seus relatos, diz que, basicamente, quase todas as atividades realizadas envolvendo comunicações sem fio requerem maior atenção, detalhismo e visão mais apurada. Os usuários compradores desses equipamentos sem fio precisam avaliar que tipos de serviços eles oferecem e se é viável investir nessa tecnologia. Os fabricantes, por sua vez, precisam saber que investimentos priorizar, quais atividades de pesquisas irão incentivar e quais tecnologias e equipamentos

deverão desenvolver para construir um produto final atraente para o consumidor. É necessário que o produto final seja atraente o suficiente para despertar o interesse e curiosidade do comprador, bem como aliar isso à necessidade do uso daquele dispositivo para a vida do consumidor. Não obstante aos consumidores e fabricantes, estão os meios acadêmicos que são responsáveis por enxergarem as áreas que necessitam de maiores avanços e pesquisas mais detalhadas. É preciso realizar projeções e previsões, pois existem muitos casos de fracasso devido a erros de avaliações. Um exemplo disso foi o caso do Irídium (telefone via satélite). Foram feitas previsões de que muitos usuários iriam adquirir este equipamento de telefonia internacional de custo elevado, mas com grandes vantagens. Porém isso não ocorreu, o prejuízo foi enorme e o projeto fracassou (KEEGAN, 2000, p. 206).

As redes sem fio de um modo geral possuem muitas utilidades como já descrito nas sessões anteriores, seu uso se estende desde um simples escritório até mesmo uso militares e policiais. Qualquer pessoa possuidora de um *notebook* ou *PDA* e um modem sem fio pode se conectar a uma rede sem fio, como se esta fosse cabeada (NIEBERT et al, 2007 apud NOGUEIRA, 2009, p. 16). De acordo com Kurose e Ross (2006), é possível identificar os seguintes elementos em uma rede sem fio:

- Nós sem fio: Assim como em redes cabeadas ou com fio, os nós são equipamentos de sistemas finais que executam aplicações. Os nós também podem ser chamados de hospedeiros. Um hospedeiro pode ser um computador, *notebook*, um *palmtop*, um *PDA*, ou até mesmo um celular. Eles podem ser fixos ou móveis.
- Estação base: A estação base é parte essencial das redes sem fio com infraestrutura (*access point*, fios). Ela é responsável por todo o controle de envio e recebimento de dados (pacotes) de um hospedeiro sem fio para outro que esteja associado à mesma estação. O termo “associado” significa, para este contexto, que o nó está dentro do alcance de comunicação da estação base e se utiliza dela para retransmitir dados entre ele e a rede. São exemplos de estações base de uma rede sem fio (padrão IEEE 802.11) os pontos de acesso também conhecidos como *Access Point* ou simplesmente AP e torres de celulares. Uma estação base é encarregada de coordenar a transmissão de vários dispositivos a ela associados. Na

figura 1, a estação base está conectada através de uma infraestrutura cabeada à rede maior (e. g. Internet, rede coorporativa local, rede telefônica) e, portanto, funciona como retransmissora da camada de enlace entre o hospedeiro sem fio e o restante do mundo ao qual esse nó pode se comunicar.

- Enlace sem fio: Para um nó se conectar a outro nó sem fio ou a uma estação base é necessário que esse nó possua um enlace sem fio. As tecnologias desses enlaces de comunicação podem possuir diferentes taxas de transmissão e podem transmitir dados e informações a distâncias diferentes. Esses enlaces sem fio "podem se conectar a roteadores", pontes, comutadores e outros equipamentos de rede. A figura 1 representa uma rede sem fio onde os enlaces se conectam aos nós nas bordas da rede de maior alcance.

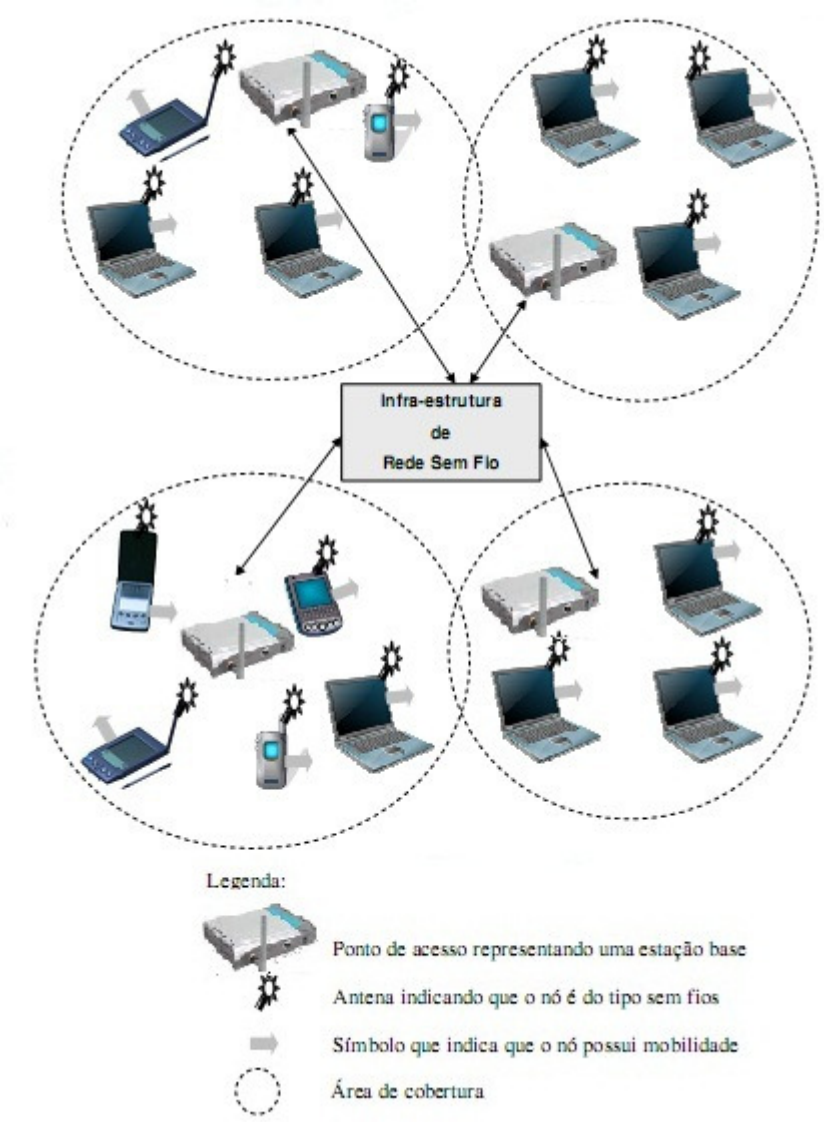


Figura 1 – Elementos de uma infraestrutura de rede sem fio (NOGUEIRA, 2009).

De acordo com Nogueira (2009) infere-se da figura 1 que a infraestrutura de rede é a rede de maior alcance com a qual um dispositivo sem fio pode se comunicar. Nesse mesmo contexto, quando vários hospedeiros estão associados a uma estação base, pode-se dizer que estão operando em modo de infraestrutura, já que todos os serviços que a rede provê como, por exemplo, atribuição de endereçamento e roteamento, são fornecidas pela rede através da estação base. Contudo, quando os nós sem fio não possuem nenhuma infraestrutura com a qual se conectar, pode-se dizer que a rede é do tipo *ad hoc* ou ponto-a-ponto. Nesse tipo de rede a ausência de infraestrutura faz com que os próprios hospedeiros venham a prover serviços de roteamento, endereçamento e outros que seriam fornecidos pela infraestrutura (NOGUEIRA, 2009, p. 18). Mais detalhes desse tipo de rede serão discutidos no capítulo 2.

De acordo com Gast (2002) e Walke (2003), comparando-se as redes cabeadas com as redes sem fio no padrão 802.11, uma simples placa de rede sem fio substitui uma placa de rede cabeada sem grandes complicações, já que na camada de rede ou acima dela, não há praticamente nenhuma mudança. Portanto, julga-se que na camada de enlace é que devem se concentrar as maiores pesquisas, pois é nela que há grandes diferenças entre as redes sem fio e as cabeadas, devendo ser tratada e melhor estudada (FLICKENGER, 2003 apud NOGUEIRA, 2009).

Para uso das redes sem fio em qualquer tipo de tarefa, devem-se levar em consideração alguns fatores relevantes para que seu uso seja eficiente e eficaz. Esse trabalho não tem como principal objetivo levantar maiores discussões de vantagens e desvantagens do uso da tecnologia sem fio. Porém, julga-se necessário abordar alguns pontos "alarmantes" citados por alguns autores, como os trabalhos realizados por Nogueira (2004), Kurose e Ross (2006) que apresentam algumas dessas realidades:

Vantagens das redes sem fio:

- Mobilidade: Os equipamentos de redes locais sem fio podem ser deslocados de um local a outro fornecendo ao usuário acesso à informação em qualquer lugar em tempo real.
- Instalação rápida e simples: A instalação de uma rede sem fio é feita rapidamente e de forma simples e fácil, eliminando a necessidade de atravessar cabos pelas paredes e evitando possíveis danos e acidentes.
- Flexibilidade: Com essa tecnologia é possível se alcançar locais em que a rede cabeada não é capaz de chegar.
- Custo reduzido: Embora as redes sem fio inicialmente tivessem um custo mais elevado, hoje em dia isso não faz parte da realidade. A instalação mais rápida e o ciclo de vida das redes sem fio são muito maiores do que as redes cabeadas, reduzindo drasticamente os custos com manutenção e se tornando cada vez mais atrativas.

- Escalonamento: As redes sem fio podem ser montadas seguindo diversas topologias de configuração de rede, podendo ser escolhida aquela que melhor se adéqua às necessidades e aplicações do usuário. Essas configurações podem ser modificadas de forma fácil e as distâncias entre as estações podem ser adaptadas para poucos ou muitos usuários.

Desvantagens das redes sem fio:

- Redução da força do sinal: As radiações eletromagnéticas são atenuadas (diminuídas) quando atravessam alguns tipos de materiais, como por exemplo, a parede, ou seja, as ondas transmitidas ao encontrarem obstáculos pelo caminho vão sendo enfraquecidas. Há outro problema chamado de nó oculto, onde os obstáculos físicos presentes no ambiente (por exemplo, outro nó, edifício, montanha) criam um anteparo impedindo a comunicação entre os nós.
- Interferência de outras fontes: As redes sem fio têm a característica de transmitir na mesma banda de frequência de outras fontes de rádio, isso acarreta em interferência entre as fontes. Como exemplo tem-se os telefones sem fio que utilizam a frequência 2.4 GHz, frequência essa utilizada também pelas redes sem fio, causando interferência entre as fontes transmissoras. O ruído eletromagnético é outro fator que pode causar interferência, por exemplo, um microondas ligado.
- Propagação multivias: Ocorre quando as ondas eletromagnéticas se refletem em objetos (metais brilhosos, espelhos naturais e artificiais, água) e também no solo tomando caminhos com comprimentos de onda diferentes entre emissor e receptor. Isso resulta em embaralhamento do sinal recebido no hospedeiro fim. Objetos que se movimentam entre o emissor e receptor também podem fazer com que a propagação multivias mude com o tempo.
- Fragilidade da segurança: Nas redes cabeadas a infraestrutura fica dentro das corporações, já nas redes sem fio a transmissão de dados ocorre através das ondas eletromagnéticas transmitidas no ar, o que aumenta a

chance de acesso não autorizado, sendo assim mais suscetíveis a ataques de hackers e pessoas mal intencionadas, quando sua segurança não está configurada adequadamente.

1.3 Categorias de Redes Sem Fio

As redes sem fio podem ser classificadas em categorias dependendo do alcance dos seus sinais de radiofrequência. Tomando como referência os estudos realizados por Tanenbaum (2003), as redes sem fio podem ser decompostas em três categorias:

1.3.1 Wireless Personal Area Networks(WPAN)

De acordo com Tanenbaum (2003), as redes de alcance pessoal (WPAN), ou simplesmente, redes de interconexão de sistemas, consistem em interconexões de componentes de computador através do uso de ondas com frequência de alcance limitada. Todo computador que possui gabinete, teclado, mouse e periféricos como impressora, estão conectados via cabo à unidade central de processamento. Isso ocasiona transtornos como falta de organização, limitação de espaço e alcance, risco de acidentes e até mesmo dificuldade na montagem da infraestrutura. Segundo Tanenbaum (2003), algumas empresas se uniram para projetar uma rede sem fio cujo principal objetivo era evitar esses tipos de transtornos. Dessa união surgiu o que chamamos hoje de rede *Bluetooth*, uma rede de alcance limitado sem necessidade do uso de infraestrutura.

As redes *Bluetooth* permitem conexões dos mais variados tipos de equipamentos, como computadores, *notebooks*, *PDAs*, celulares, câmeras digitais, fones de ouvido, dentre outros. Não há necessidade de instalação de programas, nem de *drivers*, basta que os equipamentos possuam a tecnologia, estejam ativos e ao alcance da rede, para que possam estabelecer conexão e trocar dados. Isso tem trazido grandes facilidades e vantagens no uso cotidiano, já que não há necessidade da montagem de toda uma infraestrutura para troca de dados e informações de forma rápida e momentânea (NOGUEIRA, 2009).

As redes de alcance pessoal, conforme visto na figura 2, em sua forma mais básica, utiliza-se do modelo mestre-escravo. Normalmente, a unidade central normalmente é o mestre, no qual estabelece comunicação com os dispositivos secundários como mouse, teclado e impressora, que por sua vez atuam como escravos. O mestre é o responsável por enviar aos escravos informações do tipo de protocolo, que frequência estará utilizando, quais os endereços que serão utilizados, quando os escravos poderão iniciar transmissão de informações e por quanto tempo será possível realizar essa transferência (TANENBAUM, 2003, p.23).

Figura 2 – Redes Sem Fio de Alcance Pessoal (WPAN)

1.3.2 Wireless Local Area Networks (WLAN)

As redes sem fio locais (WLAN), por sua vez, de acordo com Brignoni (2005, p.16) possuem dois modos de operação, são eles o modo infraestruturado e o modo *ad hoc*. O primeiro possui obrigatoriamente uma estação base que permite a comunicação entre os equipamentos, como mostra a figura 3. As estações base são tipicamente conectadas a uma rede infraestruturada e elas são responsáveis por realizar a comunicação entre os dispositivos móveis da sua área e os *hosts* das redes com fio. São exemplos de estações base as torres de celulares e *Access Points*. Além das estações base, as redes sem fio locais possuem *hosts* sem

fio e enlaces sem fio. Os *hosts* sem fio nada mais são que dispositivos que possuem uma placa de rede sem fio, como *notebooks, PDAs*, celulares, dentre outros. Já os enlaces sem fio têm a função de conectar os dispositivos móveis às estações base. O modo *ad hoc*, no entanto, não se utiliza de estações base e será discutido em detalhes no próximo capítulo (KUROSE, 2006).

Figura 3 – Modelo de Redes Sem Fio Local (WLAN)

De acordo com Nogueira (2004), as WLAN estão se alastrando rapidamente, seu uso tem se intensificado principalmente em escritórios e lares, onde a instalação de fiação torna-se mais trabalhoso. Elas possuem um padrão definido pelo IEEE 802.11, cujo âmbito já está globalmente difundido. As WLAN são também conhecidas como *wi-fi*(*Wireless Fidelit*), *wireless* ou padrão IEEE 802.11 (TANENBAUM, 2003). Elas funcionam como sistema de transmissão de dados flexíveis que permite a comunicação entre equipamentos sem a necessidade de uma conexão física direta (NOGUEIRA, 2004). Podem servir de alternativa às redes com fio. O seu princípio de funcionamento está diretamente associado à transmissão de dados no ar através de ondas eletromagnéticas. Nogueira (2004) em seus relatos alerta sobre a preocupação do uso de faixas de frequências comuns em redes sem fio, já que são poucas as faixas que não necessitam da autorização do órgão de controle (Anatel – Agência Nacional de Telecomunicações) para uso do espectro de frequências.

1.3.3 Wireless Wide Area Networks (WWAN)

A terceira e última categoria relatada por Tanenbaum (2004) são as redes sem fio geograficamente distribuídas (WWAN), que possuem certa semelhança com as WLAN quanto ao seu funcionamento, porém diferem no que se refere ao alcance do sinal. As WWAN tem um alcance bem maior do que as WLAN. Para atingir um alcance maior, as redes geograficamente distribuídas necessitam de tecnologias e equipamentos diferenciados para gerenciar o sinal a receber e transmitir. Ela se utiliza de satélites de comunicação compartilhados com as redes de telefonia móvel, porém essas redes possuem taxas de bits muito mais baixas do que as LAN. Atualmente o enfoque das WWAN está no acesso à internet com alta largura de banda e de maneira independente da telefonia (TANENBAUM, 2003). No entanto as WWAN não são de grande serventia às redes sem fio *ad hoc* devido ao alto custo de infraestrutura, grandes distâncias entre emissor e receptor e problemas de transmissão (NOGUEIRA, 2009).

1.4 Padrões Sem Fio da Indústria

De acordo com Brignoni (2005) existem vários padrões de redes sem fio na indústria, contudo os mais utilizados até o momento são: o padrão IEEE 802.11, HiperLAN e *Bluetooth*. Com esses padrões pode-se garantir que todo tipo de equipamento possa realizar comunicação utilizando os mesmos protocolos e interfaces de comunicação.

1.4.1 IEEE 802.11

O padrão 802.11 é responsável por definir as redes locais sem fio (WLAN). Mesclando os conhecimentos de Tanenbaum (2003), Brignoni (2005) e Sacramento (2007), esse padrão até 1997 especificava três técnicas de transmissão na camada física, das quais duas são especificações com opção para rádio (FHSS e DSSS), operando na faixa de 2.400 a 2.483 MHz (variando de acordo com regulamentação de cada país) e a outra opção de especificação para infravermelho. Porém em 1999 foi apresentada uma nova técnica de transmissão chamada OFDM. Os autores detalham-nas da seguinte maneira:

- *Frequency Hopping Spread Spectrum* (FHSS): consiste em uma técnica de espalhamento de espectro, cuja largura de banda total de 2.4GHz é dividida em canais de frequências, no qual o emissor e o receptor transmitem utilizando um desses canais durante determinado tempo e logo após saltam para outro canal, daí o nome de espalhamento de espectro por salto em frequências.
- *Direct Sequence Spread Spectrum* (DSSS): é um método de espalhamento de espectro no qual diferentes transmissões simultâneas são separadas por códigos. Nessa técnica também é utilizada a banda total de 2.4GHz que é fracionada em 14 canais de 22 MHz que são responsáveis por enviar dados sem saltos para outras frequências.
- Infravermelho: essa técnica utiliza como meio de transmissão feixes de luz infravermelho difusos fornecendo operação a 1 Mbps com opção de até 2 Mbps. Porém essa não é a técnica mais popular devido problemas como o sinal não atravessar paredes deixando células isoladas.
- *Orthogonal Frequency Division Multiplexing* (OFDM): essa técnica é utilizada em WLANs de velocidades mais altas, como o padrão 802.11a que será detalhado em breve. Ela tem capacidade de transmitir até 54 Mbps em banda larga de 5 GHz e usa diferentes frequências. É considerada uma forma de espectro de dispersão e sua principal vantagem é a divisão do sinal em bandas estreitas que imunizam a interferência e a possibilidade de usar bandas não-contíguas.

Atualmente existem diversas variantes do padrão 802.11, como: IEEE 802.11a,b,c,d,e,f,g,h,i,n. Para maiores detalhes sobre essas variantes, verificar trabalho de Brignoni (2005).

1.4.2 HiperLAN

Esta especificação WLAN foi desenvolvida pelo Instituto Europeu de Padrões de Telecomunicações (ETSI – *European Telecommunications Standards Institute*) em 1996.

Esse padrão tem por característica suporte a redes baseadas em infraestrutura e redes *ad hoc* de alto desempenho. A primeira das quatro especificações desenvolvidas pelo ETSI foi a HiperLAN/1 e ela opera a uma taxa de dados de 23.5 Mbps. Seu alcance médio chega a aproximadamente 50 metros, operando a uma frequência de 5 GHz.

O segundo tipo de rede criado pelo ETSI foi o HiperLAN/2 que opera em até 54 Mbps de taxa de dados e pode ser utilizada em diversos tipos de redes como ATM, 3G e redes em geral baseadas em IP (*Internet Protocol*). Sua especificação prevê o uso de dados, voz e vídeo, incluindo QoS. A HiperLAN/2 tem um alcance maior, podendo variar de 50 a 100 metros sua área de cobertura. (BRIGNONI, 2005).

Existem ainda outros dois tipos de redes criados pelo ETSI são o HiperLAN/3 e HiperLAN/4. O tipo 3 também opera na frequência 5 GHz, e possui um alcance ainda maior, chegando aos 5000 metros. Já o tipo 4 opera numa frequência de 17 GHz, com alcance médio de 150 metros e taxa de dados de 150 Mbps.

Dos quatro tipos de redes criados pelo ETSI o mais utilizado pelos europeus é o HiperLAN/2, pois abrange todas as características e modelos de operação dos outros tipos. Suas principais características são:

- Altas taxas de transmissão;
- Provê qualidade de serviço;
- Possui suporte a segurança e mobilidade;
- Orientado a conexão.

O padrão IEEE 802.11a é um padrão puramente americano, já o padrão HiperLAN/2 foi criado pelos europeus. O HiperLAN/2 é semelhante ao 802.11a operando a 5 GHz e utilizando modulação do tipo OFDM, diferindo apenas na subcamada MAC. De acordo com Schiller (2003), as principais características entre os dois padrões podem ser representadas na tabela 1.

Tabela 1 - Características entre o padrão 802.11a e HiperLAN/2

Característica	IEEE 802.11a	HiperLAN/2
Espectro	5 GHz	5 GHz
Max. Taxa na camada física	54 Mbps	54 Mbps
Max. Taxa na camada 3	32 Mbps	32 Mbps
Protocolo MAC	CSMA/CA	TDMA/TDD
Suporte a QoS	Não	Sim
Seleção de frequência	Portadora	Seleção dinâmica de frequência (DFS)
Codificação de dados	RC4 (chave de 40 bits)	DES (chave de 56 bits)
Autenticação	Não	Sim
Controle de qualidade do sinal	Não	Adaptação do Link
Suporte a redes fixas	Ethernet	Ethernet, IP, ATM, UMTS, FireWire, PPP

1.4.3 Bluetooth

De acordo com Tanenbaum (2003), em 1994 a empresa L. M. Ericsson se interessou em utilizar conexão entre telefones móveis e outros dispositivos sem cabos. Com essa idéia ela se uniu a mais quatro empresas (IBM, Intel, Nokia e Toshiba) para formar um grupo chamado SIG (*Special Interest Group*), cujo objetivo era desenvolver uma especificação para interconectar dispositivos de comunicação móveis com dispositivos computacionais utilizando rádios sem fio de curto alcance, baixo custo e potência. Essa especificação recebeu o nome de *Bluetooth*.

Inicialmente a idéia do *Bluetooth* era se livrar dos cabos conectados entre os dispositivos, porém logo tomou outro rumo chegando à invasão da área das WLANs. Atualmente o *Bluetooth* provê funcionalidades como pontos de acesso para tráfego de dados e voz, redes pessoais e substituição de cabos entre periféricos e estações de trabalho. Sua unidade básica é denominada *piconet,* que suporta em torno de sete conexões em paralelo com uma taxa de transmissão de 1 Mbps. Sua potência de transmissão chega a atingir até 0,1 Watts a uma distância de até 10 metros e opera a uma banda de frequência de 2,4 GHz, mesma banda utilizada pelos padrões 802.11b/g. Por operarem na mesma banda um sofre interferência com o outro, porém o padrão 802.11 sofre maiores ruínas nas transmissões, pois o *Bluetooth* salta com maior rapidez (TANENBAUM, 2003). A modulação utilizada por esse padrão é do tipo FHSS (BRIGNONI, 2005).

Esta especificação possui dois níveis de potência, uma alta para cobrir áreas maiores como uma casa e uma menor de alcance pessoal como dentro de uma sala, por exemplo. De acordo com Tanenbaum (2003), as redes *Bluetooth* trabalham com o paradigma mestre-escravo, no qual é definido na criação da rede um responsável por atuar como mestre, que tem a responsabilidade de controlar a comunicação entre os dispositivos escravos ao seu alcance. Toda comunicação é feita entre mestre e escravo, jamais um escravo se comunica com outro escravo sem passar pelo mestre. Quanto à segurança, o *Bluetooth* se utiliza de um tipo de criptografia que se baseia no algoritmo chamado SAFER (*Secure And Fast Encryption Routine*). Esse tipo de segurança é utilizado no software do *Bluetooth* e apresenta baixo esforço computacional. Contudo os aspectos de segurança no *Bluetooth* ainda deixam muito a desejar quanto a sua robustez nas transmissões de dados e devem ser melhorados (BRIGNONI,2005).

2. REDES SEM FIO *AD HOC*

Neste capítulo serão abordados aspectos importantes referentes às redes *ad hoc* com o intuito de fornecer as bases do conhecimento necessário sobre essa tecnologia.

Os tópicos tratam de uma breve introdução sobre a tecnologia, mobilidade em uma rede sem fio e características e tecnologias de alcance das redes do tipo *ad hoc*. Para se realizar o comparativo entre os diferentes tipos de protocolos de roteamento, é necessário, antes de tudo, entender o que é uma rede *ad hoc,* para que elas servem, como elas se classificam e em que situações pode-se aplicá-las. Portanto, julga-se necessário solidificar esses conceitos.

2.1 Introdução

As redes *ad hoc* tiveram seu início há pelo menos duas décadas e sua existência é proveniente da evolução das redes móveis de pacotes via rádio e das redes de malha móvel. Essas redes eram basicamente utilizadas por aplicações da área militar em campos de guerra, como por exemplo, na comunicação de tanques em ambientes hostis. Contudo, com os constantes avanços tecnológicos foi possível ampliar a sua utilidade introduzindo novas tecnologias como o *Bluetooth* e os diversos tipos de padrões IEEE 802.11, possibilitando assim a criação de novas aplicações para este tipo de rede comumente chamada de MANET, não se limitando mais somente a aplicações de cunho militar (REZENDE, 2004). Devido esses avanços, é cada vez mais comum a utilização das redes *ad hoc* nos mais variados tipos de aplicações (WU; TSENG, 2007).

Segundo Cordeiro (2002), uma rede *ad hoc* é definida como um sistema autônomo de equipamentos móveis conectados por enlaces sem fio. A união destes forma uma rede de comunicação modelada na forma de um grafo arbitrário. Já Rodrigues (2004) define o termo *ad hoc* como algo que é criado ou usado para um fim específico, porém a rede *ad hoc* não se limita somente a isso. Elas geralmente não possuem topologia predefinida, e nem um controle centralizado como nas redes infraestruturadas. Os nós nessas redes não possuem conexões predeterminadas para se comunicarem criando assim uma rede do tipo *on the fly*. Esses nós podem fazer parte da rede durante o tempo de uma sessão de comunicação ou enquanto estão ao alcance do restante da rede.

Os dispositivos de uma rede *ad hoc*, podem se mover arbitrariamente fazendo com que haja mudanças frequentes na topologia da rede. Essas mudanças afetam a conectividade entre os nós, e o tratamento de roteamento entre eles, o que acaba por requerer adaptações constantes e reconfigurações de rotas (BRIGNONI, 2005). Além disso, essas redes são compostas por dispositivos portáteis que possuem limitações de banda passante e de energia das baterias dos nós (FERNANDES, 2008).

À medida que os nós se movem, a mudança na topologia deve ser informada aos outros nós participantes da rede para que todos possuam essa informação. Essas redes são tolerantes a falhas e à saída de nós, pois sua organização e controle são feitas por todos os nós, já que todos possuem a função de traçar rotas e retransmitir pacotes (REZENDE, 2004).

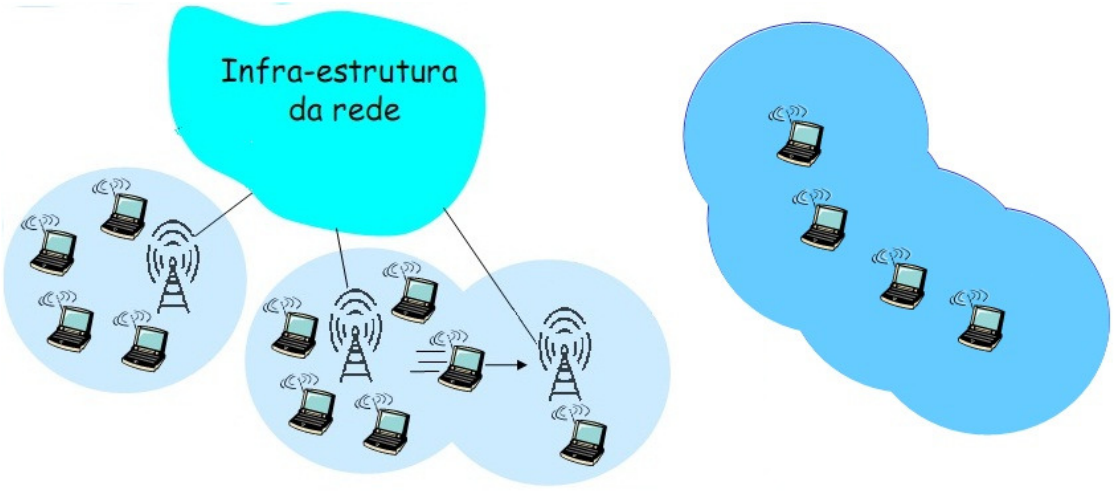
Em contraste a esse conceito têm-se as redes de celulares, que se utilizam do modelo de rede de salto simples, no qual entre dois dispositivos que se comunicam há somente a estação base que opera como ponto de acesso fixo. Por outro lado em uma rede *ad hoc* não existe nenhuma infraestrutura entre os dispositivos comunicantes e sua topologia pode ser modificada dinamicamente, através da mobilidade dos nós (REZENDE, 2004)

2.2 Mobilidade

O aumento demasiado do uso de dispositivos computacionais portáteis, bem como equipamentos automatizados industriais e comerciais, aliados à capacidade de se

comunicarem com outras redes e equipamentos móveis, introduziu um novo conceito, a computação móvel, que tem despertado interesse de uso nos mais variados tipos de cenários (BASAGNI et *al,* 2004).

De acordo com Tanenbaum (2003) e Kurose e Ross (2006), as redes sem fio móveis podem ser classificadas de duas maneiras: redes com infraestrutura ou infraestruturada e redes sem infraestrutura ou *ad hoc*. Nas redes infraestruturadas os nós não se comunicam com os seus vizinhos diretamente, mesmo que estejam bem próximos uns aos outros, toda comunicação passa pela estação base como se pode identificar na figura 4 (a). Já nas redes do tipo *ad hoc*, os nós sem fio móveis podem se comunicar diretamente entre si, formando uma rede temporária dinâmica sem uso de estação base como podemos visualizar na figura 4 (b). É por causa dessa dinamicidade e capacidade de adaptação rápida que o mercado atual vem realizando grandes investimentos e pesquisas científicas nessa tecnologia.



(a) Rede infraestruturada (b) Rede *ad hoc*

Figura 4 - Tipos de redes sem fio (TANENBAUM, 2003).

A mobilidade apresenta papel fundamental em cenários que há maior necessidade de locomoção e que não haja viabilidade de montagem de infraestrutura de rede, como em cenários de guerras e incidentes, facilitando o envio de mensagens, transferência de arquivos, sons e imagens, recebimento de ordens, dentre outras vantagens, porém essa mobilidade pode vir a trazer problemas referentes à segurança. Ela por si só introduz obstáculos para aplicação de mecanismos de segurança, devido suas constantes alterações de topologia e por seu meio de transmissão ter maior vulnerabilidade. Sendo assim, os mecanismos de segurança a serem

implantados devem se adaptar à dinamicidade da rede e às mudanças da topologia (FERNANDES, 2008).

As forças militares investem muito em redes sem fio móveis devido sua larga atuação em ambientes táticos que não possuem infraestrutura (HAAS; TABRIZI, 1998). Contudo, a maior preocupação do uso dessas redes está nos critérios de segurança, pois o uso militar requer exaustiva robustez, segurança na comunicação e transporte de dados e informações sigilosas. Uma vantagem desse tipo de rede para esse cenário é a configuração de rede descentralizada e independente de infraestrutura fixa, o que pode ocasionar em sucesso operacional numa missão já que geraria dificuldade para os inimigos localizarem as redes, por serem montadas dinamicamente, e os dispositivos serem móveis e por terem um processo de associação e desassociação rápidos. Contudo, para que uma equipe realize suas tarefas e atinja suas metas, é necessário possuir um sistema de comunicação confiável, bem configurado, eficiente e eficaz, onde seja possível trocar informações importantes (PEREIRA, 2004).

Todavia, quando se trabalha usando a mobilidade em redes sem fio, é importante destacar que o deslocamento do dispositivo móvel para fora do campo de alcance de uma estação, e possível associação do equipamento no campo de outra estação, fará com que o dispositivo mude seu ponto de conexão para aquela rede maior em um processo chamado de *handoff* (transferência) (KUROSE; ROSS, 2006).

2.3 Redes *Ad Hoc*

As redes *ad hoc* são capazes de estabelecer comunicação diretamente entre si formando redes dinâmicas temporárias sem o uso de pontos de acessos ou estações base. Nesse tipo de rede, os nós podem operar tanto como roteadores, descobrindo e estabelecendo rotas, como servidores, rodando aplicações para os clientes. As redes *ad hoc* utilizam roteamento colaborativo, permitindo que nós que não estejam ao alcance de transmissão possam se comunicar através de múltiplos saltos com a colaboração de nós intermediários (FERNANDES, 2008).

De acordo com Rodrigues (2004), as redes *ad hoc,* se dividem em: redes *ad hoc* de comunicação direta como ilustrado na figura 5 (a); e redes *ad hoc* de comunicação por múltiplos saltos, figura 5 (b). Na rede *ad hoc* de comunicação direta, os nós se comunicam apenas com aqueles que estiverem ao alcance do sinal transmitido, ou seja, nesse tipo de rede o alcance é bem mais limitado. Já nas redes *ad hoc* de comunicação por múltiplos saltos, os dispositivos operam como encaminhadores de pacotes e todos possuem a propriedade de traçar rotas. Com isso, os dispositivos que não estiverem ao alcance de transmissão de um dado nó poderão se comunicar utilizando-se do envio de pacotes pelos encaminhadores que estão ao seu alcance, formando uma rede de cooperação de comunicação (RODRIGUES, 2004).

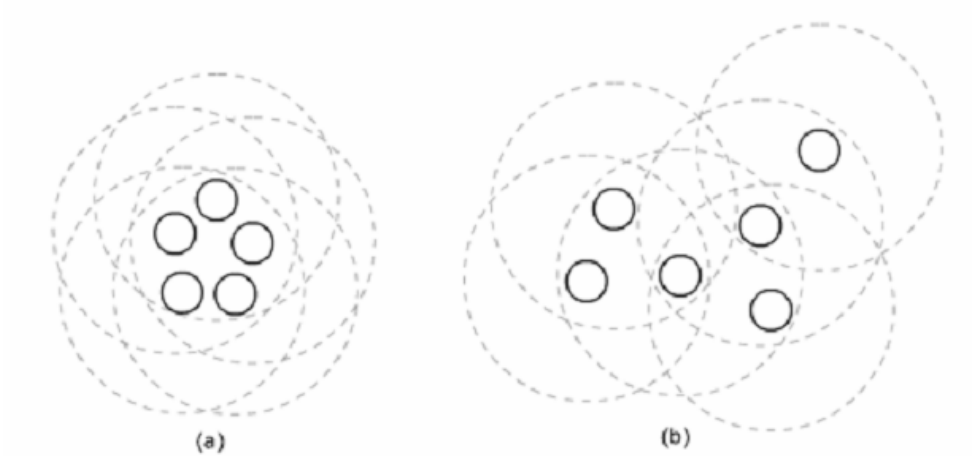


Figura 5 - Tipos de redes ad hoc. (a) Comunicação direta (b) Múltiplos saltos (RODRIGUES 2004).

De acordo com Rodrigues (2004), as redes *ad hoc* possuem diversas vantagens como oferecer alta flexibilidade sem uso de infraestrutura de comunicação e ser bastante robusta. Já Rezende (2004) relata como principais características dessas redes sem fio:

- Topologia dinâmica: os nós podem se mover arbitrariamente mudando rapidamente de posição em momentos imprevisíveis e aleatórios;
- Enlaces com capacidade variável e largura de banda limitada: os enlaces sem fio continuam com capacidade muito menor do que os enlaces de redes com fio. Adiciona-se a isso problemas como desvanecimento, ruído e interferências;
- Operação de conservação de energia: dispositivos móveis possuem limitações, pois dependem de baterias e meios que esgotam energia;

- Segurança física limitada: as redes sem fio por si só são mais propícias a ataques do que as cabeadas, devido ao sinal passar pelo ar e ser passível de sofrer ataques de escuta (*sniffing*), de logro (*spoofing*), de negação de serviço, dentre outros. A vantagem dessas redes é a natureza descentralizada e são robustas contra falhas simples.

Fernandes (2008) conceitua redes sem fio *ad hoc* como sendo um conjunto de nós móveis que formam uma rede temporária dinâmica sem uso de infraestrutura, podendo os nós se movimentarem aleatoriamente ou de forma organizada. O autor comenta também que o caminho entre os nós pode possuir múltiplas ou uma única ligação e a rede pode estar associada à outra rede, como a internet, ou não. Além disso, existem problemas como mobilidade, consumo de energia de bateria, largura de banda limitada, diversidade de dispositivos, configurações diversas, dentre outros, que tornam as redes sem fio *ad hoc* repletas de desafios e incentivam novas pesquisas.

As redes sem fio *ad hoc* possuem características interessantes em cenários temporários, como facilidade de conexão, configuração rápida e dinâmica, flexibilidade e robustez (NOGUEIRA, 2009). A rapidez de configuração e instalação é primordial para se alcançar metas e objetivos.

Contudo, nessas redes é fundamental a cooperação e esforço dos nós, com o intuito de colaborar com o restante da rede para o sucesso da comunicação. Sua principal desvantagem é a complexidade exigida de cada nó, pois cada um é responsável por manter e rastrear rotas, atuar como servidor e receptor, evitar problemas característicos das redes sem fio como terminal oculto, dentre outras (RODRIGUES, 2004).

2.4 Tecnologias de Alcance das Redes *Ad Hoc*

As redes *ad hoc*, assim como as redes sem fio de um modo geral, possuem classificação quanto ao alcance dos seus sinais, sendo esta mais específica ainda. A

classificação das redes *ad hoc* exibida na figura 6 está baseada na união dos conhecimentos dos trabalhos de Tanenbaum (2003), Rodrigues (2004) e Kurose e Ross (2006):

I. Redes sem fio corporais (*Wireless Body Area Network* - WBAN): Seu alcance é de aproximadamente 1 metro;
II. Redes sem fio de alcance pessoal (*Wireless Personal Area Network* - WPAN): Seu alcance é entre 1 metro a aproximadamente 10 metros;
III. Redes sem fio locais (*Wireless Local Area Network* - WLAN): Seu alcance é entre 10 metros a 500 metros;
IV. Redes sem fio metropolitanas (*Wireless Metropolitan Area Network* - WMAN): Seu alcance pode variar entre 10 quilômetros a 50 quilômetros;
V. Redes sem fio geograficamente distribuídas (*Wireless Wide Area Network* - WWAN): Seu alcance pode chegar a mais de 50 quilômetros de área.

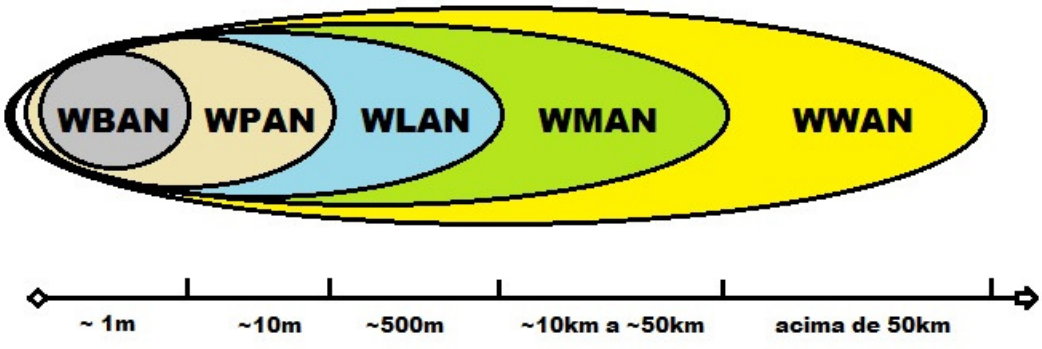


Figura 6 – Taxonomia das redes *ad hoc*.

As WBAN ou redes sem fio corporais são redes de alcance de até um metro de distância e se referem a dispositivos sem fio que podem ser utilizados junto ao corpo humano, como por exemplo, fones de ouvido, relógios, microfones, dentre outros. Contudo, ela não se resume a dispositivos corporais, são também utilizadas em computadores com o intuito de evitar a utilização de cabos entre seus periféricos. Esse tipo de classificação tem por característica a interconexão de aplicações e equipamentos sem fio em uma única relação. Já as WPAN se caracterizam por ter um alcance de até 10 metros e sua frequência de sinais usa banda de 2,4 GHz, porém sua principal diferença para as WBAN é a conectividade de dispositivos sem fio a outros equipamentos, ou seja, sua relação é de um para vários

dispositivos em uma rede, o que permite conexão com pessoas ou equipamentos próximos ou ao redor de um ambiente (RODRIGUES, 2004).

As WLAN ou redes sem fio locais têm um alcance médio de até 500 metros, cobrindo regiões maiores como edifícios e conjuntos habitacionais. Ela possui as mesmas características das LANs, porém enfrentam problemas típicos das redes sem fio como redução da força do sinal, propagação multivias, interferência, ruído e falhas de segurança. As redes *ad hoc* do tipo WLAN são redes ponto-a-ponto que se configuram dinamicamente formando redes temporárias com seus nós dentro dos limites de alcance (RODRIGUES, 2004).

As redes sem fio *ad hoc* metropolitanas (WMAN) e as de área geograficamente distribuídas (WWAN) são redes que implementam o uso de múltiplos saltos (*multihop*), cuja complexidade é elevada e possui muitos desafios a serem descobertos e tratados, como qual melhor tipo de roteamento, descoberta de localização, tratamento de segurança em cada salto, dentre outros. Atualmente essas classificações não possuem tecnologia necessária para resolver os desafios citados e não se enquadram nos cenários de testes deste trabalho. Portanto, não serão detalhadas e nem abordadas mais neste trabalho (NOGUEIRA, 2009).

Atualmente as classificações mais utilizadas são as WBAN, WPAN e WLAN, que são redes de menor alcance de sinal e de comunicação direta. Elas estão cada vez mais presentes no cotidiano devido seus constantes casos de sucesso. Assim sendo são essas tecnologias que serão utilizadas e estudadas durante este trabalho (NOGUEIRA, 2009).

3. ROTEAMENTO EM REDES *AD HOC*

Neste capítulo serão documentados os tipos de protocolos de roteamento para redes *ad hoc*. Ele será dividido em introdução, classificação dos protocolos de roteamento e contextualização dos principais algoritmos de roteamento.

3.1 Introdução

Em redes *ad hoc* para se encaminhar um pacote a um determinado nó, muitas vezes são necessários vários saltos envolvendo nós intermediários. Para que isso ocorra da melhor forma possível, é necessária a definição de rotas. Essas rotas são definidas a partir de algoritmos de roteamento que, por sua vez, devem atender alguns requisitos, como escolher a melhor rota para encaminhamento do pacote, fornecer serviço com menor sobrecarga possível, manter rotas ótimas mesmo em situações de tráfego intenso, poder se adaptar facilmente e rapidamente à robustez e as mudanças da topologia da rede sabendo lidar com falhas (REZENDE, 2003). O roteamento é feito por um programa que é executado pelo roteador. Esse programa implementa um dos protocolos de roteamento que se baseiam em algum algoritmo (PEREIRA, 2004).

Ao contrário das redes infraestruturadas que utilizam técnicas de roteamento no seu núcleo de rede (*backbone*) como técnica principal, as redes *ad hoc* móveis provêem roteamento autônomo em cada nó como sua técnica principal. Para isso, é necessário o desenvolvimento de protocolos de roteamento que sejam capazes de viabilizar operações robustas, eficientes e eficazes para que sejam incorporadas funcionalidades de roteamento a cada um dos nós. No entanto, o roteamento em redes *ad hoc* é um dos grandes desafios a serem solucionados, já que cada nó da rede possui limitações de recursos, largura de banda,

durabilidade de bateria e necessita assumir características de roteador e estação (FERNANDES, 2003).

De acordo com Rezende (2003) e Brignoni (2004), outros fatores que também devem ser considerados nas redes *ad hoc,* são as mudanças constantes de topologia da rede e de localização dos nós, o processo de inicialização de requisições, a escolha de nós intermediários a serem utilizados e a escalabilidade. Levando-se em consideração esses fatores, é possível definir qual "caminho poderá ser mais eficiente e eficaz" para se encaminhar pacotes ao nó destino.

Para se encaminhar um pacote entre dois nós pertencentes a uma rede *ad hoc* que não possui nenhuma ligação direta entre si, é necessário o uso de nós de salto, que são nós responsáveis por realizarem o encaminhamento dos pacotes entre a origem e o destino. Contudo, esses nós também possuem a capacidade de se locomover livremente e pode ocorrer dos nós de salto não pertencerem mais a rota ótima utilizada no momento do encaminhamento de um pacote ou até mesmo não possuir mais o caminho de roteamento entre os dois nós. São através dessas características e limitações que o roteamento em redes *ad hoc* se torna complexo e diferente do roteamento em redes infraestruturadas (PEREIRA, 2004).

3.2 Classificação dos Protocolos de Roteamento

De acordo com Sarkar, Basavaraju e Puttamadappa (2008), os protocolos de roteamento se classificam em três esquemas, conforme Figura 7.

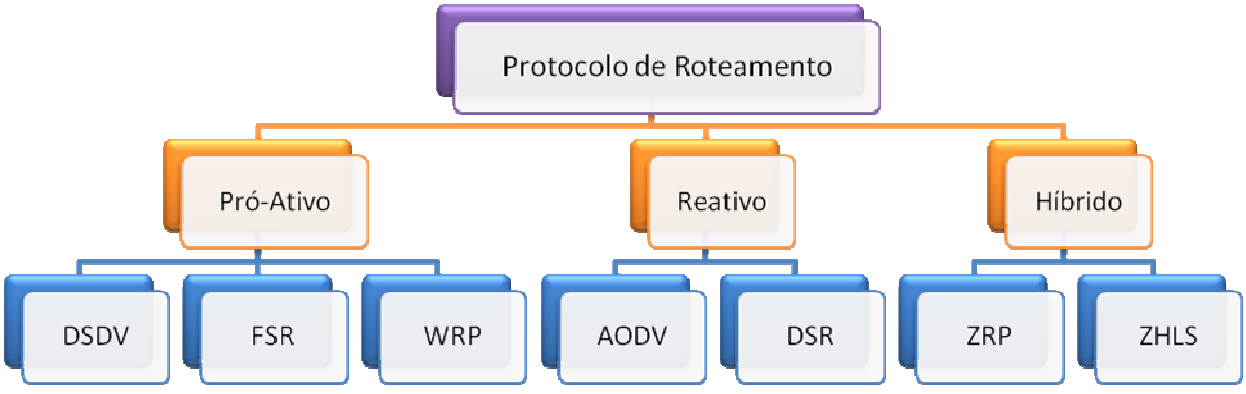


Figura 7 – Classificação dos protocolos de roteamento de redes *ad hoc*.

Os protocolos pró-ativos que também são chamados de esquemas orientados por tabela, possuem a característica de trocarem informações de rotas constantemente entre os nós, não dependendo da ocorrência de requisições. Eles mantêm rotas para todos os nós da rede atualizando suas tabelas de roteamento. Essas atualizações ocorrem através de mensagens periódicas e reagindo a cada mudança de topologia de rede, mesmo que essas rotas não sejam utilizadas ou que nenhum tráfego seja alterado (FERNANDES, 2003). Esses protocolos mantêm sempre uma quantidade estável de transmissões em andamento, não sendo gerado assim atraso de transmissão para busca de rotas. No entanto, esse esquema não é aconselhável para topologias com alta dinamicidade, pois consome muitos recursos de dispositivos móveis que possuem muitas limitações (REZENDE, 2004).

De acordo com Fernandes (2003), Rezende (2004) e Brignoni (2005), os protocolos reativos ou esquemas baseados em demandas, possuem a característica de iniciar suas atividades somente quando surgem demandas, ou seja, quando o nó fonte necessitar enviar um pacote, iniciando assim o procedimento de busca de rotas. Esse procedimento só é concluído quando for descoberta a rota até o destino do pacote ou todas as rotas alternativas forem examinadas. Como o evento disparador de busca de rotas é o envio de um pacote de dados, esse protocolo não envia mensagens regularmente, o que economiza energia de bateria, banda e sobrecarga de roteamento. Ao contrário do pró-ativo, esse protocolo não mantém informações de roteamento nos nós, o que faz dele uma solução para redes *ad hoc* com alta escalabilidade, apesar do atraso inicial para busca de rotas até o destino. Esse protocolo não mantém rotas para nós que não estiverem ativos.

Os protocolos híbridos ou hierárquicos têm como característica principal a combinação dos principais valores dos protocolos reativos e pró-ativos, com o intuito de superar as deficiências de ambas as partes (SARKAR, BASAVARAJU e PUTTAMADAPPA, 2008). Eles exploram arquiteturas de rede hierarquicamente, utilizando-se de regras diferenciadas para cada nó. Seu princípio é abordar a organização dos nós em grupos (*clusters*), estabelecendo funcionalidades diferenciadas de acordo com as características e demandas dos nós de dentro e de fora dos grupos. Com esse tipo de estratégia diminui-se o tamanho das tabelas de roteamento e o tamanho dos pacotes para atualização de

rotas, contendo agora somente informações de parte da rede e não do todo, o que reduz o tráfego de pacotes de controle (REZENDE, 2004).

3.3 Protocolos de Roteamento em Redes *Ad Hoc*

Nesta seção serão abordados os principais protocolos de roteamento de redes *ad hoc* conforme Sarkar, Basavaraju e Puttamadappa (2008). São eles: vetor de distâncias de destino em saltos (DSDV), protocolo olho de peixe (FSR), protocolo de roteamento sem fio (WRP), vetor de distâncias por demanda para redes *ad hoc* (AODV), Roteamento de origem dinâmica (DSR), protocolo de roteamento por zona (ZRP) e protocolo hierárquico de estado de enlace baseado em zonas (ZHLS).

3.3.1 Protocolo Vetor de Distâncias de Destino em Saltos (DSDV)

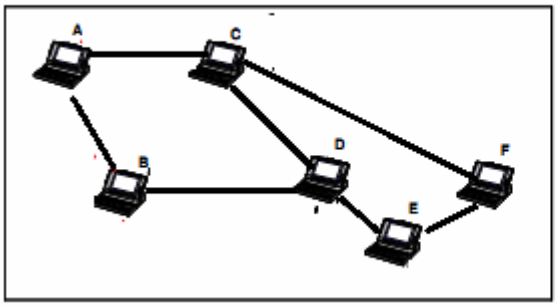
O DSDV (*Destination Sequenced Distance Vector*) é um protocolo de roteamento pró-ativo que se baseia no algoritmo de vetor de distâncias (*Bellman-Ford*). Ele trabalha com requisição periódica de tabelas de roteamento dos nós vizinhos com a finalidade de mantê-las atualizadas. Cada nó possui uma tabela de roteamento contendo as entradas da tabela, que são compostas por: nós de destino, o próximo dispositivo para se chegar ao destino (próximo salto), quantidade de saltos e o número de sequência estabelecido pelo destino. As tabelas possuem rotas para cada dispositivo da rede e cada nó possui apenas uma rota para cada destino. A vantagem desse protocolo sobre outros que trabalham também com vetor de distâncias é que ele garante ausência de *loops* usando uma técnica de número de sequência mantido em cada rota, no qual é estabelecido pelo destino um número de sequência e é incrementado a cada aviso de rota. O número mais alto será a rota mais recente e favorável (REZENDE, 2004).

Esse protocolo atualiza as tabelas de roteamento periodicamente ou quando a topologia é alterada, de modo a garantir a consistência dessas tabelas quando qualquer tipo de alteração na rede for detectado. Ao receber uma requisição de atualização de tabela, os dispositivos comparam-na com as informações contidas em sua tabela. Rotas com número de sequência menores são descartadas, pois são consideradas desatualizadas. Rotas com número de sequência igual considera-se aquela com menor número de saltos. A quantidade de saltos e

o número de sequência são sempre incrementados, pois há necessidade de mais um salto para se chegar ao destino e precisa-se acrescer o número de sequência para que seja detectado que essa é a última atualização realizada. Após a atualização da tabela, é disparada a propagação das mensagens de atualização para que outros dispositivos atualizem suas tabelas de roteamento também (CAMPOS, 2005).

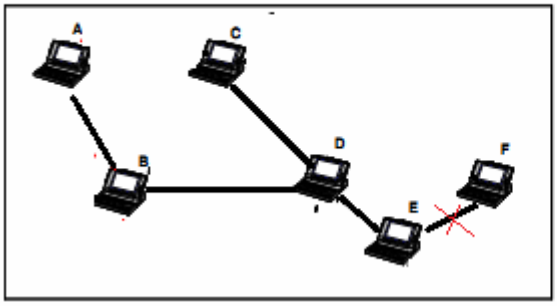
A ruptura de enlaces é um dos grandes problemas de redes *ad hoc*. Ela pode ser detectada por um hardware de comunicação ou ser inferida caso nenhuma mensagem de atualização tenha sido recebida do vizinho. O dispositivo detector da ruptura atualiza sua tabela inserindo na quantidade de saltos valor infinito para aquele nó e também para todos os caminhos que possuem o dado nó como intermediário. Com isso o número de sequência é acrescido em um para cada destino não alcançável e um novo envio de atualização de tabelas é feito. Para melhor visualizar o comportamento do protocolo DSDV, será exibida na figura 8 uma movimentação na rede, bem como a ocorrência de uma ruptura de enlace. Nesta figura também será possível verificar as mudanças na tabela de roteamento de um nó ao ocorrer essas alterações (CAMPOS, 2005).

Cenário de roteamento e tabela de roteamento do dispositivo C.



Destino	Próximo Salto	Qtd Saltos	Número de Seqüência
A	A	1	S316•A
B	A	2	S551•B
C	C	0	S212•C
D	D	1	S428•D
E	D	2	S420•E
F	F	1	S542•F

Cenário de roteamento e tabela de roteamento do dispositivo C, após mudança na topologia da rede.



Destino	Próximo Salto	Qtd Saltos	Número de Seqüência
A	D	3	S420•A
B	D	2	S690•B
C	C	0	S550•C
D	D	1	S550•D
E	D	2	S690•E
F	D	∞	S842•F

Figura 8 – Comportamento do protocolo DSDV.

De acordo com Campos (2005), as mensagens de atualização de rotas provocam um aumento do tráfego da rede. Como o DSDV é um protocolo pró-ativo o tráfego de mensagens de atualização é muito grande ocasionando em um aumento ainda mais expressivo do tráfego de rede. Para minimizar essa problemática o DSDV possui dois tipos de atualizações, a incremental e a completa. Na incremental cada nó envia apenas as informações que sofreram alterações nas suas tabelas desde o último envio. Já na atualização completa, cada dispositivo envia toda a tabela de roteamento (PEREIRA, 2004).

O DSDV adota o critério de seleção de rotas através do número de sequência e quantidade de saltos. Contudo, isso pode provocar problemas de flutuações nas rotas, já que um dispositivo pode vir a receber uma atualização com uma quantidade de saltos e número de sequência e, logo após, receber outra atualização com o mesmo número de sequência, porém com número de saltos menor, gerando assim uma rajada de novas atualizações de rotas. Para resolver esse tipo de problema o DSDV adota o procedimento de atraso de divulgação de rotas, no qual só é enviada a mensagem de atualização de rota quando receber a melhor rota. Para que não haja uma grande espera da melhor rota, os dispositivos são responsáveis por determinar a probabilidade de chegada das melhores rotas através da manutenção do histórico dos tempos médios para um dado destino. Esse tempo é obtido através da diferença entre chegada da melhor rota e a chegada da primeira atualização (CAMPOS, 2005).

O protocolo DSDV, apesar de prover rotas livres de *loops*, apresenta várias desvantagens por ser um protocolo de abordagem pró-ativa e, portanto, não escalável. Podemos citar algumas dessas desvantagens, de acordo com Campos (2005):

- Por adotar o envio de informações de roteamento periódicas, o DSDV precisa de um tempo para convergir antes que a rota possa vir a ser utilizada. Contudo, esse tempo causa perda na taxa de entrega dos pacotes até que seja encontrada uma nova rota;
- Em um cenário de grande mobilidade e escalável, há necessidade de aumento de largura de banda e tamanho das tabelas. Isso faz com que aumente demasiadamente a quantidade de pacotes de atualização de rotas e, consequentemente, cause perda do desempenho da rede.

3.3.2 Protocolo Olho de Peixe (FSR)

O FSR (*Fisheye State Routing*) é um protocolo simples e eficiente desenvolvido pela *Adaptative Wireless Mobility* (WAM) no laboratório da Universidade da Califórnia. Nesse protocolo cada dispositivo contém um mapa da topologia da rede e por ser baseado na estratégia de roteamento LS (*Link State* - Estado de enlace), cada nó envia o estado dos seus enlaces para todos os nós da rede. Nele é possível atribuir valores ou custos aos caminhos, que podem ser calculados a partir de atributos como capacidade do enlace, congestionamento, dentre outros fatores (IETF, 2002).

De acordo com Farias (2006), o FSR é um melhoramento do protocolo GSR (*Global State Routing*), contudo o GSR se utiliza de um número elevado de mensagens de atualização, o que acarreta em elevado consumo de largura de banda. Nas mensagens de atualização do FSR não estão contidas informações referentes a todos os dispositivos da rede, apenas dos seus vizinhos. A informação é trocada com maior frequência entre os dispositivos que possuem número de salto igual a um (*hop* = 1). O nó mais ao centro possui informações precisas de todos os nós vizinhos, porém quanto maior a distância do nó central, menor será a precisão da informação obtida.

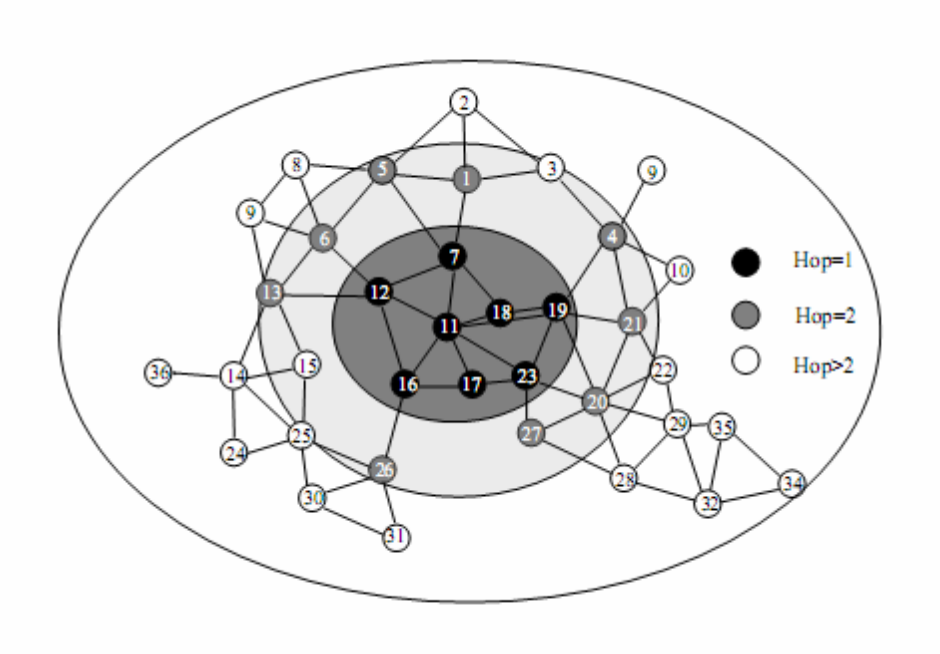


Figura 9 – Comportamento do protocolo FSR (PEI, GERLA e CHEN, 2000).

De acordo com Rezende (2004) e Farias (2006), esse protocolo é similar ao LS, por manter um mapa de topologia de rede em cada dispositivo. Porém, de acordo com Rezende (2004), o FSR se difere nos seguintes aspectos:

- Otimização de troca de informações de estado de enlace: O FSR não faz inundações de mensagens de controle de estado de enlace, a troca de informações de estado de enlace é feita somente entre vizinhos e a tabela de estado de enlace é mantida através das atualizações das informações recebidas pelos vizinhos;

- Inundações de informações de estado de enlace são disparadas por tempo e não por evento: De tempos em tempos é disparada a inundação de informações de estado de enlace, como por exemplo, na ocorrência de queda de enlace, o que diminui a frequência de atualizações em um ambiente instável, onde os enlaces são pouco confiáveis;

- O tempo de disparo é incerto: Para cada tipo de entrada na tabela pode-se usar intervalos diferentes, considera-se também o número de saltos para o disparo e os nós distantes do dispositivo possuem intervalos de tempos maiores.

Portanto esse protocolo possui algumas vantagens importantes quando comparado ao protocolo LS, como não fazer inundações em toda a rede, redução dos pacotes de controle e frequência de propagação e a troca de informações de estado de enlace é pequena para redes de proporções maiores. O FSR é indicado para ser utilizado em redes com um número elevado de nós e de alta mobilidade devido às informações de controle serem restritas ao número de saltos entre os dispositivos (FARIAS, 2006).

3.3.3 Protocolo de Roteamento Sem fio (WRP)

O *Wireless Routing Protocol* (WRP) é um protocolo de classificação pró-ativa no qual os dispositivos de roteamento contêm a informação do predecessor e a distância até cada destino da rede. Caracteriza-se como nó predecessor o último nó antes de se chegar ao destino desejado. Todos os nós vizinhos ao predecessor remetem informações sobre ele e cada nó verifica a consistência dessas informações a fim de evitar *loops* e prover convergências de rotas mais eficiente e eficaz (FERNANDES, 2003).

De acordo com Cunha (2002) e Fernandes (2003), esse protocolo tem uma característica bem diferenciada dos demais protocolos, por possuir e manter quatro tabelas, são elas:

- Tabela de distância: contêm uma matriz das distâncias de nós considerando os parâmetros de destinos e predecessores.
- Tabela de roteamento: é um vetor que contêm uma entrada para cada destino. Está contido nessa tabela um identificador de destino, a distância para o destino, o predecessor e o sucessor do menor caminho e um marcador *tag* para atualizar a tabela.
- Tabela de custo de conexão: contêm uma lista de custos de transmissão para cada vizinho do nó e o número de atualizações desde que o nó recebeu uma mensagem de erro.
- Tabela de mensagens para transmissão: permite que um nó saiba que atualizações deverão ser retransmitidas e quais vizinhos são elegíveis para reconhecer essas transmissões.

No protocolo WRP são enviadas mensagens de atualização periodicamente aos vizinhos a fim de manter as informações de roteamento precisas. Com essas mensagens um nó pode escolher se irá atualizar sua tabela de roteamento com as informações fornecidas ou pode detectar que há uma mudança na conexão com o vizinho. O nó destino ao receber uma mensagem livre de erros envia uma mensagem de aceite (ACK) a fim de informar que a conexão está adequada e a mensagem foi processada. As mensagens de atualização possuem alguns parâmetros em seu cabeçalho, são eles o identificador do nó emissor, uma lista de

atualizações (contêm a identificação do nó destino, o predecessor do nó destino e a distância até o destino) e outra lista de resposta que contêm os nós que devem enviar uma mensagem ACK. Logo, esse protocolo requer que o dispositivo mantenha uma grande quantidade de informações armazenadas e o tráfego da rede é maior devido à periodicidade das trocas de informações de roteamento (FERNANDES, 2003).

A conectividade dos nós também é averiguada com o recebimento de mensagens de reconhecimento do tipo *hello messages* que são transmitidas periodicamente. Quando um nó recebe essa mensagem de um nó novo na rede, as informações contidas nesse nó serão adicionadas na tabela de roteamento de quem recebeu. Caso o dispositivo não receba mensagens por um tempo quatro vezes maior ao do tempo de recebimento dessas mensagens, o dispositivo assume que a conexão com aquele nó vizinho foi perdida (FERNANDES, 2003).

Na figura 8 é ilustrada uma rede sem fio *ad hoc* com uso do protocolo WRP. Os custos estão ilustrados através dos valores ponderados acima das linhas de conexão. As setas indicam e limitam a direção das mensagens de atualização, já os valores contidos nos parênteses indicam a distância e o predecessor ao destino **D**. O nó **A** é a origem, o nó **D** é o destino e os dispositivos **B** e **C** são vizinhos do nó **A**. Para melhores esclarecimentos do funcionamento desse protocolo verificar o trabalho de Fernandes (2003).

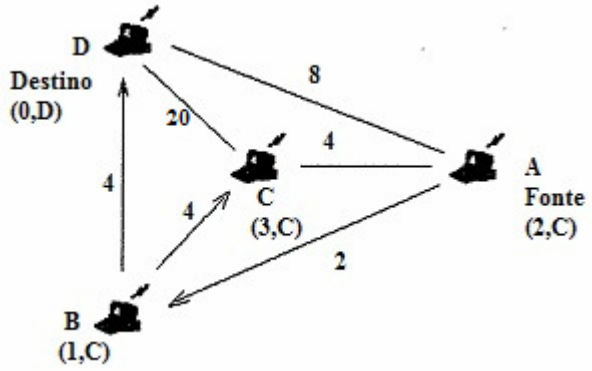


Figura 10 – Exemplo cenário WRP (FERNANDES, 2003).

3.3.4 Protocolo de Roteamento de Origem Dinâmica (DSR)

Este protocolo foi desenvolvido pelo Departamento de Ciência da Computação da *Rice University*, através do projeto MONARCH (*MObile Networking ARCHitectures*). O *Dynamic Source Routing* (DSR) é um protocolo reativo que utiliza roteamento na fonte para enviar dados, ou seja, no seu cabeçalho é carregado o caminho completo e ordenado que o pacote deverá percorrer até alcançar o seu destino. Ele possui duas características que são a descoberta e manutenção de rotas. Quando um determinado nó deseja enviar um pacote a um destino usando esse protocolo, é feita uma verificação se já existe uma rota até o destino em seu *cache*, caso exista é enviado o pacote de dados por essa rota, senão será iniciado o processo de busca dinâmica de rotas (PEREIRA, 2004).

O DSR tem como característica a não propagação de mensagens periódicas para detecção de conectividade com dispositivos vizinhos, o que reduz a utilização de energia de bateria e largura de banda. Esses fatores são ainda mais importantes quando não há mudança de topologia de rede ou quando todas as rotas já foram descobertas (CAMPOS, 2005).

Esse protocolo permite que sejam mantidas várias rotas para o mesmo destino. Desta forma é garantido que não ocorrerão inundações na rede, pois caso haja falha nos nós intermediários pertencentes à rota até o destino, haverá outra rota para que seja encaminhado o pacote. O processo de descoberta de rotas é disparado toda vez que algum dispositivo desejar enviar um pacote de dados e a fonte não possua nenhuma rota cadastrada no *cache*. Nesse caso é disparado um pacote de requisição de rotas por difusão para todos os vizinhos do dispositivo de origem. Nesta requisição são enviados os endereços da fonte e do destino, um identificador de requisição e um registro de rotas para armazenamento do endereço dos nós intermediários visitados até a chegada do nó destino. Na figura 11 tem-se um exemplo de descoberta de rota para o protocolo DSR, no qual o nó origem “A” quer se comunicar com o nó destino “G” (FERNANDES, 2003).

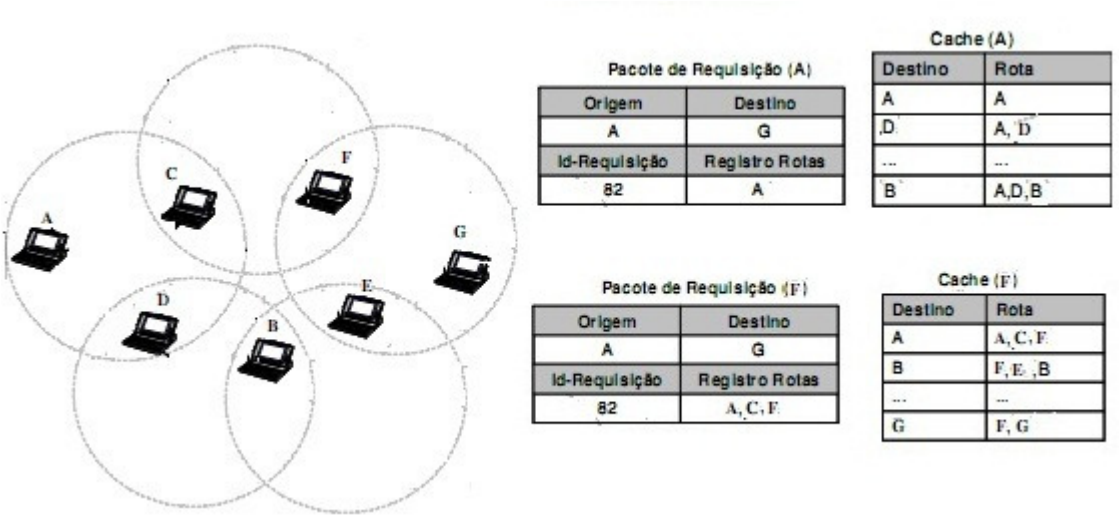


Figura 11 – Procedimento de requisição de rotas para o protocolo DSR.

De acordo com Campos (2005), com o recebimento do pacote de requisição, o nó receptor realiza a leitura do pacote seguindo algumas condições de prioridade:

- O pacote será descartado caso o endereço da origem e identificador de requisição já estejam armazenados na lista de requisições recebidas, ou seja, o pacote já foi processado e outra requisição do mesmo tipo foi enviada, havendo repetição de pacote de requisição;

- O pacote também será descartado caso o endereço do dispositivo já exista no registro de rotas da requisição;

- O pacote será processado caso o dispositivo seja o destino do pacote. Será emitido então para a origem, um pacote do tipo resposta de rota. A rota do destino à origem é identificada através dos registros de rotas contidos no pacote de requisição de rotas.

- Caso nenhuma das condições acima seja satisfeita, será armazenado no registro de rota o endereço do dispositivo e será retransmitido o pacote de requisição para todos os seus vizinhos, ou seja, a cada processamento realizado pelos nós intermediários registra-se o endereço do dispositivo no registro de rotas.

- As rotinas anteriores serão repetidas até que seja achado o dispositivo destino ou que seja localizada uma rota válida em algum nó visitado.

No DSR a quantidade de mensagens de requisição de rotas retransmitidas é limitada pelo parâmetro TTL (*Time To Life*) do pacote IP. Este parâmetro é decrementado a cada visita a algum dispositivo até que atinja o valor zero. Quando esse parâmetro atinge o valor zero não são permitidas mais retransmissões, portanto a origem deverá definir que critério utilizar: retransmitir a requisição ou concluir que não há condições de localizar o destino (CAMPOS, 2005).

O reconhecimento passivo é um mecanismo de manutenção de rotas presente no DSR. Sua existência justifica-se devido ao dinamismo da topologia de redes *ad hoc*. Nesse protocolo, ao invés de utilizarem-se mensagens de sinalização periódicas para manter a conectividade com seus vizinhos, usa-se o monitoramento dos pacotes de confirmação dos outros dispositivos ou usa-se o modo de trabalho promíscuo, no qual é possível ouvir todas as comunicações que passam pelo dispositivo. Agindo assim, quando um dispositivo detecta falhas na comunicação com algum vizinho, remove-se aquele dispositivo de sua *cache* e é enviada uma mensagem de erro para cada dispositivo que tenha enviado algum pacote por aquela rota, utilizando-o como nó intermediário (FERNANDES, 2003).

Segundo Campos (2005), umas das principais vantagens desse protocolo é a abordagem reativa com uso de roteamento na origem, devido à maneira como as rotas são obtidas e ausência de sinalizações periódicas. Outra grande vantagem é a economia de bateria e largura de banda, fatores essenciais para redes *ad hoc* móveis. Apesar disso em cenários de alta mobilidade e mudanças constantes de topologia, poderão ocorrer quebras de enlaces, aumento da sobrecarga de roteamento e diminuição da taxa de entrega. Outro ponto negativo do DSR refere-se à utilização do modo promíscuo, no qual pode gerar problemas de segurança devido à escuta de comunicações.

3.3.5 Protocolo Vetor de Distâncias Por Demanda para Redes Ad hoc (AODV)

O AODV (*Ad hoc On-demand Distance Vector routing*) é um protocolo do tipo reativo que também se baseia em vetor de distâncias. Ele é um dos protocolos mais discutidos em publicações sobre redes *ad hoc* devido alguns problemas que foram detectados na sua criação. Esse protocolo é padronizado pelo IETF (RFC 3561) e é considerado a mesclagem do protocolo DSDV e DSR. Sua semelhança com o DSR é por ser baseado em demandas, descobrir rotas somente quando há necessidade e utilizar técnicas de descoberta e manutenção de rotas. No entanto o AODV utiliza algumas características do DSDV como conhecimento do próximo salto para alcançar o destino e a distância em números de saltos. Ele é considerado uma versão melhorada do DSDV, pois, seu funcionamento baseado em demandas, minimiza as inundações na rede (PEREIRA, 2004).

Nesse protocolo cada dispositivo possui uma tabela de roteamento similar a do protocolo DSDV. Segundo Campos (2005), por ser um protocolo reativo, as informações armazenadas em suas tabelas de roteamento são temporárias e necessita-se de alguns campos adicionais para manter o controle desta característica. São eles: tempo de vida da rota e lista de vizinhos que se utilizam de alguma rota da tabela de roteamento do dispositivo.

O AODV se utiliza de mensagens diferenciadas para manter e descobrir rotas. As mensagens de requisição de rotas são comumente chamadas de RREQ (*Route Request*) e se propagam pela rede à procura do destino ou alguma rota que seja possível alcançar o destino. Esta mensagem é retornada ao dispositivo de origem através de uma mensagem do tipo *route replay* (resposta de rota - RREP) assim que o destino for localizado, seja através da localização direta do dispositivo destino ou por alguma rota localizada em outro dispositivo. Neste mesmo protocolo ainda são enviadas dois tipos de mensagens, a mensagem do tipo *hello* (RREP especial) que fornece dados de conectividade das rotas ativas e a mensagem do tipo *Route Error* (RERR) que indica a indisponibilidade de uma rota (REZENDE, 2004).

De acordo com Campos (2005), o processo de busca de rotas é iniciado quando um nó deseja enviar um pacote a um destino para o qual o dispositivo não conhece sua rota ou sua rota não é mais válida, ou seja, o tempo da rota se encontra expirado. Imediatamente é

disparada uma mensagem de requisição de rota por difusão para todos os vizinhos, contendo os seguintes campos:

- O último número de sequência do destino (caso não exista será enviado zero) e o endereço ip da origem;
- O número de sequência da origem incrementado de um, a fim de evitar conflitos com outras rotas;
- Um contador de saltos inicializado com zero;
- Um identificador de requisições que identifica a quantidade de requisições enviadas.

Ao receber uma mensagem do tipo RREQ, o nó verifica a identificação da requisição e o endereço IP da origem, fatores esses que juntos identificam unicamente a requisição. Após realizar a identificação da requisição é verificado se ela já foi processada antes, caso tenha sido processada anteriormente o pacote será descartado. Caso não tenha sido processada, o dispositivo processará a requisição e verificará se ele é o destino desejado. Caso seja o destino, é enviada uma mensagem do tipo RREP para a origem, como mostra a figura 12. Caso o dispositivo não seja o destino, será verificado em sua tabela de roteamento se há uma rota para o destino desejado, como mostra a figura 13. Caso não haja rota nenhuma para o destino, o dispositivo enviará via *broadcast* (difusão) para seus vizinhos uma mensagem de requisição com a quantidade de saltos acrescida de um e armazenará sua própria identificação para encaminhamento reverso. Cada nó intermediário atualizará as informações referentes ao tempo de duração da rota e gravará o número de sequência com valor mais alto. O número de retransmissões das mensagens RREQ é limitado por um campo chamado TTL (*time to life*) do cabeçalho IP (FERNANDES, 2003).

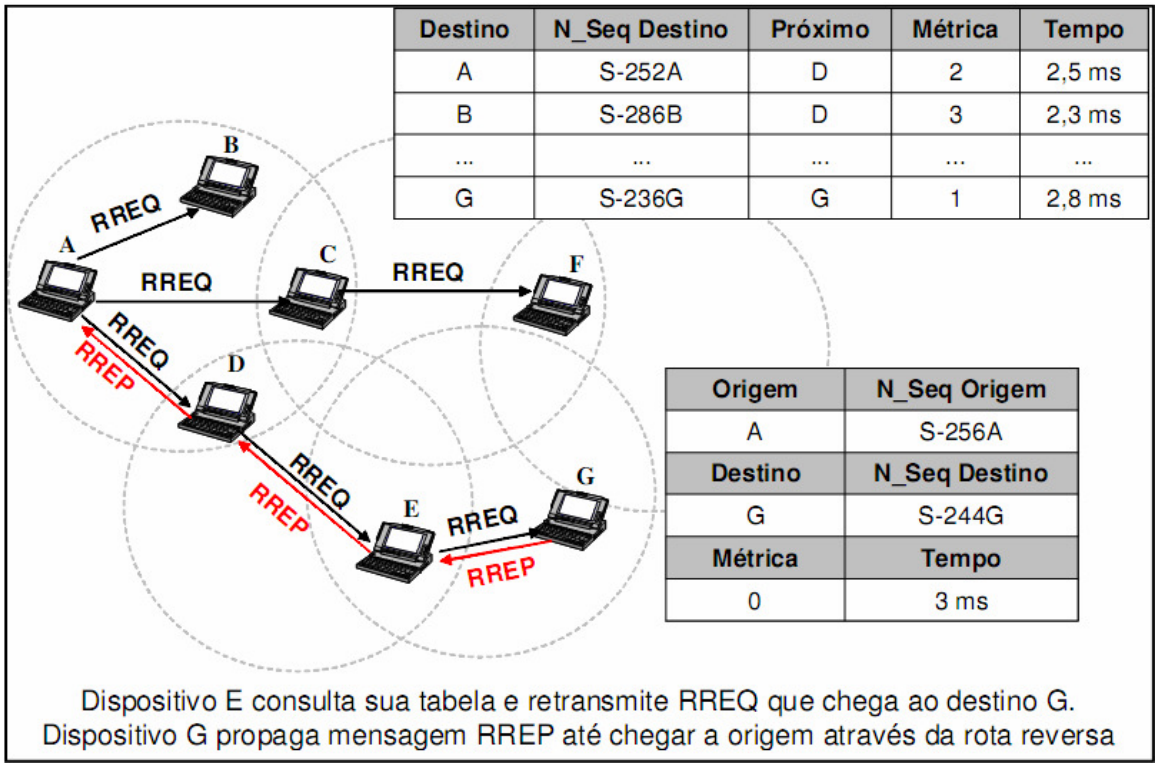


Figura 12 – Procedimento de resposta de rotas iniciado pelo destino (CAMPOS, 2005).

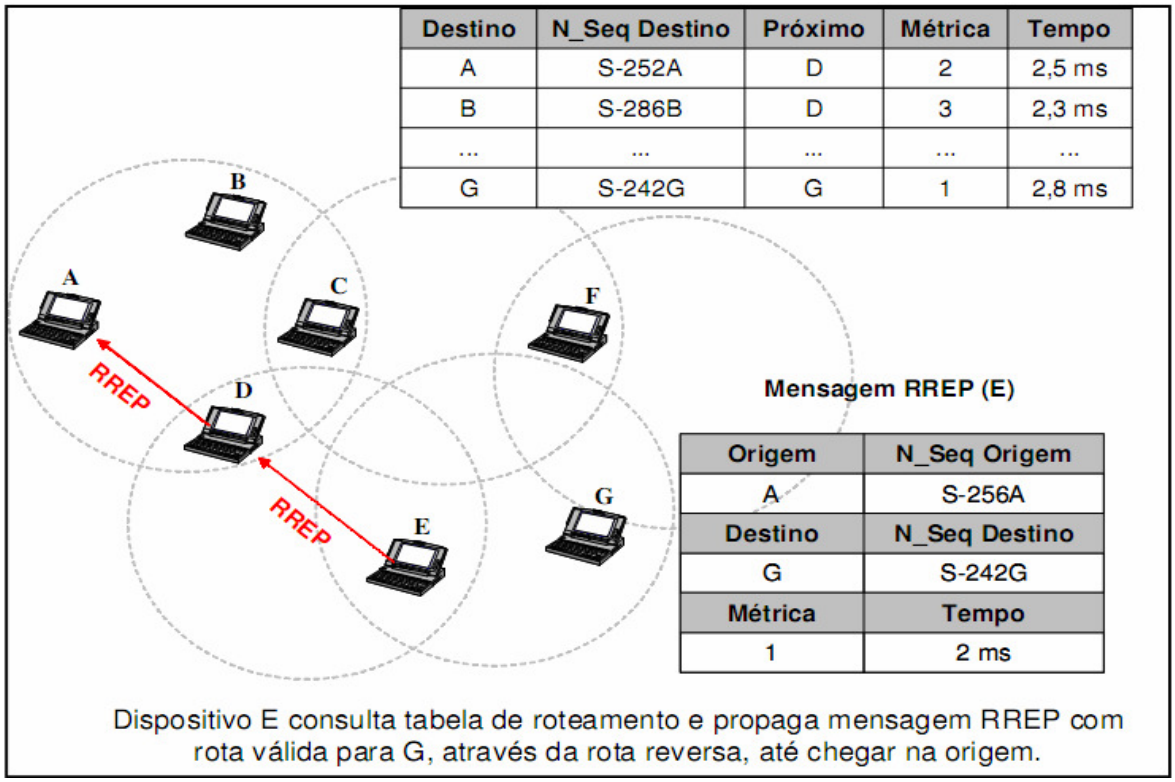


Figura 13 – Procedimento de resposta de rotas iniciado por um dispositivo intermediário (CAMPOS, 2005).

Com o intuito de manter as rotas ativas, o AODV implementa o envio de mensagens periódicas para sua lista de vizinhos. Essas mensagens são do tipo *route replay* com TTL igual a um. Caso o dispositivo não receba mensagens de conectividade dos seus vizinhos, será inferido que a rota está indisponível (CAMPOS, 2005).

Devido à grande mobilidade dos nós em redes *ad hoc,* é necessário constantes manutenções de rotas. Quando a origem é o dispositivo a se movimentar, é necessário reiniciar o processo de descoberta de rotas. Quando um dispositivo intermediário detecta alguma falha ou rota inválida, uma mensagem do tipo *route error* - RERR é processada e enviada para todos os vizinhos que utilizam essa rota até chegar à origem. Para que isso aconteça é feito um incremento no número de sequência do destino e a quantidade de saltos é alterada para infinito. No interior da mensagem RERR tem um campo que identifica a quantidade de destinos não alcançáveis (FERNANDES, 2003).

Esse protocolo, quando comparado com protocolos de classificação pró-ativa, apresenta uma redução no número de mensagens enviadas de roteamento, o que aumenta o desempenho da rede. Ele possui uma única rota por destino, o que reduz a quantidade de mensagens trafegadas na rede. Contudo, a ausência de rotas impacta no retardo do envio de pacotes de dados. Quando comparado com protocolos de classificação reativa com roteamento na origem, o AODV deixa a desejar no quesito carga de roteamento, pois com um ciclo simples de requisição, os protocolos de roteamento na origem obtêm diversas rotas, enquanto o AODV só aprende rotas com seus vizinhos imediatos e origem. Outra desvantagem desse protocolo é que ele não trabalha com nós unidirecionais (CAMPOS, 2005).

3.3.6 Protocolo de Roteamento por Zona (ZRP)

De acordo com Brignoni (2005), Fernandes (2006) e IETF (2002), o protocolo ZRP é classificado como híbrido, pois se utiliza de duas classificações dentro de seu protocolo, a reativa e a pró-ativa. Sua característica principal é a divisão dos nós em zonas de roteamento. Essa divisão é definida por nó da rede e inclui na sua zona aqueles nós com

distância mínima em saltos. Dentro de cada zona é obrigatório que o nó tenha as informações de roteamento do outro nó da zona e isso acontece utilizando algoritmos pró-ativos, ou seja, o algoritmo utilizado na intrazona é do tipo pró-ativo e, consequentemente, o algoritmo da interzona é do tipo reativo.

Para inclusão de nós na intrazona é necessário uma distância mínima em saltos do nó considerado, essa distância mínima é denominada raio da zona. O raio da zona pode ser escolhido pelo gerenciador da rede ou dinamicamente pelos nós. De acordo com Fernandes (2006), o parâmetro considerado para essa escolha é sempre o deslocamento dos nós na rede. Caso haja muito deslocamento de nós na rede, o raio da zona deve ser pequeno, caso os nós da rede não modifiquem constantemente de posição, deve-se utilizar um raio de zona maior.

De acordo com Brignoni (2005), se o destino de um pacote de dados é um nó dentro da intrazona do nó origem, o pacote será enviado diretamente ao nó destino, pois o nó origem já conhece suas informações através do uso do algoritmo pró-ativo. Caso o destino não esteja na intrazona, o pacote é enviado por difusão para todos os dispositivos que estão na borda da zona de roteamento, questionando se possuem alguma rota para o destino solicitado. Caso algum dos nós possua essa informação, é enviado um ack e a conexão é fechada. Contudo, caso os dispositivos da borda não possuam nenhuma rota que se possa chegar ao destino, o procedimento de envio de mensagem por difusão aos dispositivos de suas bordas é feito por cada dispositivo da borda do nó origem e assim sucessivamente até que seja localizado o nó destino e seja enviada a mensagem de aceite ack ou o número de saltos chegue ao máximo e não seja possível localizar o destino na rede.

Por possuir característica híbrida, esse protocolo se beneficia por utilizar as melhores características de cada abordagem. Ele possui a característica de o roteamento ocorrer rapidamente na intrazona, pois as rotas já estão previamente definidas através da classificação pró-ativa e possuem as principais características da classificação reativa, como por exemplo, ser escalável, as mudanças na topologia serem detectadas rapidamente e possuem tabelas pequenas (FERNANDES, 2006).

Contudo, esse protocolo possui algumas desvantagens provindas das duas classificações utilizadas. De acordo com Brignoni (2005) e Fernandes (2006), na intrazona a

desvantagem é devido ao protocolo de roteamento não ser especificado, com isso intrazonas diferentes podem utilizar protocolos diferentes. Já na interzona a desvantagem acontece quando há troca de informações entre as interzonas, devido a utilização de protocolos por demanda ou reativos e o principal problema desses tipos de protocolos é o atraso decorrente da espera de resposta de uma requisição.

3.3.7 Protocolo Hierárquico de Estado de Enlace Baseado em Zonas (ZHLS)

O protocolo de roteamento ZHLS possui estrutura hierárquica e se baseia no protocolo de estados de enlace (LS). Nesse algoritmo também há divisão em zonas, porém com uma diferença do protocolo ZRP, suas zonas são do tipo não-sobrepostas. Cada nó é identificado através de um identificador de nó e outro identificador de zona que é calculado através do uso de GPS (*Global Processing System*) (REDIN, 2004).

De acordo com Redin (2004) e Brignoni (2005), a topologia hierárquica desse protocolo possui dois níveis: a topologia de nível do nó e a topologia de nível de zona. No ZHLS o sistema que gerencia a localização é bem simplificado, pois não há nenhum agrupamento por cabeça (*cluster-head*) e nem gerenciamento de localização (*location manager*) com o intuito de coordenar a transmissão dos dados, evitando assim *overhead* de processamento para essas funções. Com essa característica simples evitam-se pontos de falhas únicos e picos de excesso de tráfego. Outra vantagem desse protocolo é que quando comparado com protocolos reativos como o AODV e o DSR, ele consegue reduzir bastante o *overhead* da comunicação.

De acordo com Redin (2004), Brignoni (2005) e Corrêa (2005), nesse protocolo quando ocorre do destino estar em outra zona, o dispositivo de origem envia um pedido de requisição de localização do nível da zona para todas outras zonas, o que gera um *overhead* bem menor do que as abordagens que se utilizam de inundações (*flooding*) dos protocolos reativos. Nesse protocolo, a necessidade de manutenção das rotas ou novas buscas é bem menor, mesmo que a topologia da rede varie bastante, pois como são considerados apenas o identificador do nó e da zona do destino para a realização do roteamento, nenhuma busca de

localização adicional será necessária, a menos que haja mudança na zona do destino. Isso minimiza bastante o tráfego da rede de troca de informações de manutenção e busca de nós, o que diferencia esse dos protocolos reativos, onde qualquer mudança na topologia poderia ocasionar na quebra de enlaces e invalidação de rotas, podendo desencadear em um novo processo de descoberta de rotas.

De acordo com Brignoni (2005), a desvantagem desse protocolo, no entanto, é a necessidade de que cada dispositivo possua um mapa de zona estático pré-programado. No entanto, em situações em que as limitantes geográficas são muito dinâmicas, isso não é possível. Esse protocolo se apresenta bem adaptável a mudanças topológicas, gerando menor *overhead* quando comparado a protocolos reativos e com isso tem a capacidade de ser escalável em grandes redes.

4. ESTUDO COMPARATIVO DOS PROTOCOLOS DE ROTEAMENTO

Neste capítulo serão conceituadas as características mais relevantes para a análise comparativa dos protocolos de roteamento. Para a escolha das características, será levada em consideração a real necessidade delas para os cenários emergenciais propostos no próximo capítulo.

4.1 Estratégia de Roteamento

Foi visto no capítulo anterior que os protocolos de roteamento de redes *ad hoc* se baseiam de alguma forma em adaptações dos algoritmos utilizados nas redes tradicionais como estratégia de roteamento, são eles o algoritmo de vetor de distâncias e o algoritmo de estado de enlace.

O algoritmo de vetor de distâncias (DV) é responsável por enviar atualizações de roteamento de tempos em tempos a outros roteadores vizinhos, de maneira a atualizar as tabelas de roteamento desses roteadores (nós) com novas rotas. Os protocolos de roteamento de redes *ad hoc* que se utilizam desse tipo de algoritmo possuem melhor desempenho em redes estáticas, pois seus nós mantém uma visão de toda a topologia da rede. Esses protocolos são indicados para aplicações em tempo real, ou seja, aplicações que necessitem de tráfego pesado de informações. Uma vantagem associada à utilização desse algoritmo é quanto à diminuição da utilização de recursos de memória e processamento quando comparado ao algoritmo de estado de enlace. Porém esses protocolos não são indicados para redes com alta dinamicidade, pois apresentam convergência lenta e tráfego de controle excessivo (REZENDE, 2004).

O algoritmo de estado de enlace (LS) é responsável por descobrir quem são os vizinhos de um dado nó e qual o estado do enlace desses vizinhos. Ele mede os custos associados aos enlaces que possui em seu mapa de rede e transmite essas informações para todos os nós da rede. Ele também é responsável por construir o melhor caminho para cada nó da rede. Os protocolos de roteamento de redes *ad hoc* que se utilizam desse tipo de algoritmo se adéquam melhor em redes que necessitam de QoS, pois permitem que se associe custos às capacidades de enlace. Contudo seu tráfego de controle é ainda maior, já que todos os nós necessitam conhecer a topologia completa da rede. Nos casos de redes dinâmicas, a sobrecarga de informações de controle é ainda mais crítica quando comparado ao tipo DV (REZENDE, 2004).

4.2 Estrutura de armazenamento

As tabelas de roteamento são composição essencial para as redes *ad hoc*, elas fazem parte da estrutura de armazenamento dos protocolos de roteamento, sendo responsáveis por armazenar as rotas para diversos nós pertencentes à rede. Nas redes *ad hoc* essas tabelas sofrem constantes alterações devido às mudanças topológicas da rede, como por exemplo, a simples mudança de localidade de um dado nó se utilizando da característica de mobilidade nessas redes. Muitas vezes essa simples mudança acarreta em um processo de atualização de rotas na rede, mudando completamente rotas para se chegar a um nó destino.

Cada tipo de protocolo pode implementar processos de armazenamento distintos, como pôde ser visto no capítulo anterior. Alguns protocolos optam por possuir toda a topologia da rede em cada nó, outros optam por possuir apenas parte da topologia da rede em cada nó se utilizando de técnicas para detectar as mudanças topológicas. Essas escolhas acontecem, principalmente, a fim de melhorar o desempenho da rede diminuindo o tráfego de informações de manutenção de rotas para todos os nós e se utilizando de nós vizinhos para descoberta de rotas. Outro processo de armazenamento utilizado por alguns protocolos é o da utilização de *cache*, no qual o protocolo guarda as rotas mais utilizadas nesse tipo de memória, minimizando o processo de manutenção e descobertas de rotas (BRIGNONI, 2005).

Outra característica muito importante na estrutura de armazenamento dos protocolos é se o protocolo é capaz de armazenar várias rotas para um mesmo destino. Essa característica minimiza bastante a utilização de mensagens periódicas para manutenção de rotas, pois caso uma rota se torne indisponível na rede será possível utilizar rotas auxiliares para se chegar ao destino, evitando assim uma nova busca por rotas (BRIGNONI, 2005).

4.3 Processo de descoberta de rotas

O processo de descoberta de rotas nada mais é do que um mecanismo que um nó fonte utiliza para obter uma rota até um dado nó destino. Para se obter essa rota há duas maneiras de localizá-la, a primeira maneira é quando o nó destino está ao alcance do nó fonte, desta forma o nó fonte envia o pacote de dados diretamente para o nó destino, pois está ao seu alcance. A segunda maneira é quando o nó destino não está ao alcance direto do nó fonte, então deverá ser utilizado rotas que levem a nós intermediários para se chegar ao nó destino. O processo de descoberta de rotas se inicia quando o nó fonte transmite um pacote de solicitação de rota chamado RREQ. Essa transmissão pode variar de acordo com cada protocolo (FERNANDES, 2003).

Alguns protocolos implementam tipos diferentes de inundação de mensagens na rede, como por exemplo o envio de mensagens de requisição para todos os nós da rede que estão ao alcance do nó fonte de uma única vez ou até mesmo o envio de mensagens apenas para os vizinhos do nó fonte, caracterizando respectivamente duas classes de descoberta de rotas: inundação de toda a rede e inundação controlada (REZENDE, 2004).

4.4 Processamento de atualização de rotas

Cada protocolo de roteamento possui sua particularidade quando se trata de processamento de atualização de rotas. Como pode ser visto no capítulo anterior, alguns protocolos optam por atualizarem suas rotas a partir da troca de informações de roteamento com seus vizinhos, outros a cada atualização de rotas enviam sinalizações via *broadcasting* para todos os nós da rede, outros se utilizam de técnicas como a de número de sequência que detecta qual a rota mais recente para atualização das tabelas, dentre outras abordagens já relatadas no capítulo anterior. No entanto existem algumas características que são comuns a

essas abordagens e que são de suma importância para o desempenho positivo dos protocolos. Características essas que serão abordadas logo abaixo.

4.4.1 Métrica para seleção de rotas

Os protocolos de roteamento se utilizam de métricas para selecionar as melhores rotas para se enviar um pacote de dados de um nó fonte a um nó destino. São elas:

- ✓ Menor caminho: Nessa métrica cada nó possui em sua tabela de roteamento a distância física que se encontra o nó fonte do nó destino ou a quantidade de saltos entre eles. Quanto menor for a distância do nó fonte ao nó destino ou quanto menor for a quantidade de saltos que o pacote percorrerá, melhor será a métrica e, portanto, será essa rota a escolhida para enviar o pacote de dados (FERNANDES, 2003).
- ✓ Número de sequência: Nessa métrica as rotas da tabela de roteamento possuem números identificadores que são chamados de número de sequência. Esses números servem para identificar qual rota é a mais atualizada para um nó origem enviar um pacote (REZENDE, 2004).

Alguns protocolos se utilizam de ambas as características para obter sempre a melhor rota possível de um nó fonte a um nó destino e ter um ganho ainda maior na qualidade de serviço. Vale destacar que estes protocolos de roteamento podem utilizar técnicas de Inteligência Artificial para melhor os seus desempenhos (CAMPOS, 2005).

4.4.2 Existência de Loops

No processamento de atualização de rotas é extremamente importante que o protocolo seja livre de *loops*, pois pode evitar que os pacotes trafeguem pela rede por muito tempo à procura de um destino e esse destino não seja alcançável. Os protocolos que utilizam a métrica de número de sequência são livres de *loops.* Outros protocolos se utilizam de técnicas como a utilização do TTL para minimizar ao máximo a ocorrência de *loops* (REZENDE, 2004).

4.4.3 Convergência das rotas

No processamento de atualização de rotas outra característica bastante relevante é o tempo de convergência das rotas ótimas. Rotas ótimas são rotas que possuem maior probabilidade de serem utilizadas e, portanto, devem possuir o menor caminho possível entre origem e destino. Como as rotas se modificam rapidamente nas redes *ad hoc,* devido à mobilidade dos nós, o algoritmo deve selecionar o mais rápido possível a rota mais eficiente e eficaz para enviar o pacote de dados. Portanto, aqueles protocolos que se utilizam de algoritmos que conseguem acelerar esse processo, serão mais eficazes no envio de informações (AMORIM, 2002).

4.5 Envio de atualizações de rotas

O envio de atualizações de rotas está relacionado diretamente ao envio de mensagens periódicas aos nós da rede, a fim de sinalizar que uma nova rota ou uma atualização de rota foi detectada ou até mesmo uma quebra de enlace e deverá ocorrer uma atualização em massa. Contudo essas mensagens podem ser disparadas de diversas formas e cada protocolo possui e adota uma forma para si. No entanto o envio de mensagens periódicas é comum à grande maioria dos protocolos e, portanto, será descrito abaixo como funciona essa característica (REZENDE, 2004).

4.5.1 Envio de mensagens periódicas

O envio de mensagens periódicas pode ocorrer de duas formas nos protocolos discutidos neste trabalho, de acordo com Rezende (2004), são eles:

- ✓ Por tempo: Nessa categoria o envio de mensagens de atualização só ocorre quando decorrido um período de tempo definido pelo protocolo. Alguns protocolos definem como parâmetro um *timeout,* ou seja, uma mensagem de atualização só será reenviada até o momento em que o tempo definido

pelo protocolo acabar, outros realizam cálculos para medir a probabilidade de chegada de atualização de rotas e a partir dessa probabilidade definem um valor médio em tempo para se realizarem as atualizações.

- ✓ Por evento: Nessa categoria o envio de mensagens de atualização ocorre toda vez que houver alguma mudança topológica na rede, ou seja, qualquer movimentação na rede pode impactar em mensagens de atualização de rotas. Essa categoria acarreta certa perda no desempenho devido à grande quantidade de inundações de mensagens na rede.

4.6 Comparativo entre os protocolos de roteamento

Com o intuito de consolidar as características e informações de cada protocolo de roteamento descrito nesse trabalho, será apresentada a seguir uma tabela comparativa contendo as características mais relevantes, por protocolo estudado, para os cenários de aplicação que serão apresentados nesse trabalho.

Em cada combinação de característica x protocolo será inserido um valor, que pode variar da seguinte forma:

- O termo “T”, contido nas células informa que o protocolo de roteamento é totalmente compatível com aquela característica, ou seja, o protocolo possui a característica integralmente, sem adaptações;
- O termo “P”, contido em algumas células informa que o protocolo de roteamento é parcialmente compatível com aquela característica, ou seja, o protocolo possui a característica, porém com algumas adaptações para utilização;
- O termo “N/A” significa que o protocolo não possui a característica citada;
- Já o termo “N/I”, significa que a característica citada não foi localizada em nenhuma das pesquisas realizadas.

Tabela 2 – Associação de Características x Protocolo de roteamento

Características	**DSDV**	**FSR**	**WRP**	**AODV**	**DSR**	**ZRP**	**ZHLS**
1) Estratégia de roteamento:							
Vetor de distância (DV)	T	N/A	T	T	T	P	N/A
Estado de enlace (LS)	N/A	T	N/A	N/A	N/A	P	T
2)Estrutura de armazenamento:							
Topologia completa da rede em todos os nós	T	T	T	N/A	N/A	N/A	T
Topologia parcial da rede em todos os nós	N/A	N/A	N/A	T	T	T	N/A
Utiliza cache de rotas	N/A	N/A	N/A	T	T	N/A	N/A
Múltiplos caminhos	N/A	T	T	N/A	T	N/A	T
3) Processo de descoberta de rotas:							
Inundação de toda a rede	T	N/A	N/A	N/A	N/A	N/A	N/A
Inundação controlada	N/A	T	T	T	T	T	T
4) Processamento de atualização de rotas:							
4.1) Métrica para seleção de rotas:							
Menor caminho	T	T	T	T	T	N/I	N/I
Número de sequência	T	N/A	N/A	T	T	T	N/A
4.2) Existência de loops:							

Características	DSDV	FSR	WRP	AODV	DSR	ZRP	ZHLS
Elimina a ocorrência de loops	T	N/A	N/A	T	T	N/A	N/I
Minimiza as situações de loops	N/A	T	T	N/A	N/A	T	N/I
4.3) Convergência de rotas:							
Acelera a convergência	T	T	T	T	T	T	T
Rápida	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5) Envio de atualização de rotas:							
5.1) Envio de mensagens periódicas:							
Por tempo	T	T	T	N/A	N/A	P	N/I
Por evento	T	N/A	T	T	T	P	T

Legenda:

T – Totalmente compatível;

P – Parcialmente compatível;

N/I – Não Informado;

N/A – Não se Aplica.

5. CENÁRIOS DE APLICAÇÃO DE REDES *AD HOC*

Neste capítulo serão apresentados alguns dos principais cenários emergenciais que são passíveis da aplicação de redes *ad hoc*. Neles serão propostos quais protocolos de roteamento melhor se adéquam para cada situação, vislumbrando associar as características dos protocolos estudados com a real necessidade de cada cenário. Os resultados obtidos a partir desse estudo são meramente hipotéticos, se baseando apenas na fundamentação lógica estudada nos protocolos e classificações.

5.1 Cenários de Aplicação

O uso da tecnologia sem fio das redes *ad hoc* é favorável em vários fatores para diversas áreas, tais como: negócio, indústria, defesa, segurança, dentre outras. É através da Internet que a comunicação sem fio móvel vem vivenciando avanços de tecnologia e aumento de utilização. É possível vislumbrar em um futuro bem próximo que as redes sem fio sejam ampliadas em termos de suas funções e capacidades de transmissão de dados de alcance limitado, sendo complementares à comunicação tradicional. As tecnologias que se utilizam de radiofrequência, como as MANETs e o *Bluetooth*, possibilitam transferência de dados e comunicação de forma bem simplificada e com custos bem mais reduzidos quando comparado às tecnologias tradicionais. Características como flexibilidade, portabilidade, mobilidade, custos e aplicabilidade entre diversos tipos de dispositivos, fazem com que as redes *ad hoc* tenham um desempenho bem promissor em um futuro próximo (NOGUEIRA, 2009).

O mercado atual tem sido bastante movimentado quando se trata de tecnologias móveis. A aceitação e a formação de massa crítica a respeito dessa tecnologia têm ocorrido de

forma bastante positiva, como podemos comprovar através da utilização de dispositivos que possuem a tecnologia *Bluetooth*. Vale lembrar que uma rede sem fio *ad hoc* é uma rede em que os dispositivos são móveis e não possuem uma infraestrutura fixa de topologia de rede. Esses dispositivos realizam papéis de fontes emissoras e receptoras de informações, podendo se utilizar também de outros dispositivos intermediários para transmitirem informações a terceiros. Essas redes possuem a particularidade de serem bastante utilizadas em locais onde não é possível ou viável a montagem de uma rede com infraestrutura física, justificando assim o seu uso em cenários de cunho emergencial (NOGUEIRA, 2009).

5.2 Tipos de Cenários Emergenciais

Alguns serviços públicos e privados necessitam de avanços tecnológicos a fim de se comunicarem de forma rápida, eficiente e eficaz para a realização com sucesso de suas missões. Contudo a maior parte dos serviços prestados por esses órgãos ainda não contam com inovações tecnológicas, prejudicando muitas vezes o cumprimento de tarefas exercidas por esses servidores. Essa deficiência tem prejudicado e dificultado bastante os trabalhos realizados, principalmente, por aqueles órgãos que trabalham na segurança pública, no socorro às vítimas de incidentes e na realização de eventos de grandes proporções. Portanto, a seguir serão apresentados alguns cenários emergenciais nos quais o uso das redes *ad hoc* é fundamental para o sucesso dessas missões, além de serem propostos o uso de alguns protocolos de roteamento a fim de tornar o uso das redes *ad hoc* nesses cenários ainda mais eficiente e eficaz.

5.2.1 Levantamento de local de crime

De acordo com Nogueira (2009), local de crime é caracterizado como qualquer área pela qual tenha ocorrido um fato que assuma algum tipo de infração penal, exigindo assim a presença de peritos policiais para as devidas providências. Uma vez localizada a área de abrangência do crime, devidamente isolada e preservada as provas, é chegado o momento de fazer o levantamento do crime. O levantamento do crime é feito pelos peritos criminais e

consiste nos atos praticados por esses peritos no local do fato ocorrido. De acordo com Nogueira (2009), esses atos são geralmente caracterizados como busca, identificação, posicionamento e coleta de vestígios que deverão ser utilizados para constatar a materialidade da prática delituosa pelo infrator.

No momento da busca e coleta de informações, esses peritos enfrentam grandes dificuldades, pois necessitam de equipamentos eletrônicos de última geração para realizar o armazenamento e transferência de informações do local do crime o mais rápido possível, pois o tempo nesses cenários é fator determinante. Durante toda a análise da perícia são coletadas imagens, são feitas descrições narrativas da cena do crime, a área é filmada, são realizadas verificações através de programas especializados, dentre outras análises. Daí a necessidade do uso de dispositivos portáteis nesses locais conectados em uma rede. Outro fator importante é a duração dessas operações que costumam durar no máximo um dia para se avaliar todo o local do crime. Normalmente, nessas operações a quantidade de peritos envolvidos varia entre dois a dez, dependendo do tamanho do perímetro. Dessa forma, montar uma infraestrutura de rede pode vir a atrapalhar toda a operação. Com esses dispositivos portáteis conectados entre si através de uma rede *ad hoc*, é possível armazenar, transferir e compartilhar todas as provas coletadas entre os peritos, dando maior agilidade, eficiência e eficácia ao resultado pericial. Outra vantagem do uso desse tipo de rede nessa situação emergencial é a possibilidade dos peritos obterem uma análise prévia e checagem no próprio local do crime dando maior agilidade às tomadas de decisão (NOGUEIRA, 2009).

Contudo, para montar uma rede *ad hoc* que possa ser o mais eficiente e adaptável às características desse cenário é necessário avaliar primeiramente que classificação se adapta melhor a esse tipo de situação de acordo com suas características. Com a tabela a seguir é possível se ter uma noção do grau de importância de cada característica para cada classificação, facilitando assim a tomada de decisão de qual classificação utilizar no cenário.

Tabela 3 – Características x Classificações.

Características	Pró-ativo	Reativo	Híbrido
Escalabilidade	B	A	A
Dinamicidade	B	A	A
Energia de Bateria	B	A	B
Eficiência	A	B	A

Legenda:

A – Alta importância;

B – Baixa importância;

Nesse cenário a classificação que mais se adéqua é a **pró-ativa** devido à quantidade de nós envolvidos serem pequena, não havendo necessidade de serem utilizados protocolos com maior escalabilidade. Outra característica que culminou na escolha dessa classificação foi a duração do evento, já que essa operação dura algumas poucas horas ou no máximo um dia e a energia de bateria não será um fator determinante, pois haverá maior facilidade de carregamento desses dispositivos nesses locais de crimes. Outro ponto importante que ajudou na escolha da classificação para esse cenário foi a eficiência, já que o tempo é fator determinante e uma das principais características da classificação pró-ativa é a eficiência obtida através da sua previsão antecipada de rotas.

A partir da escolha da classificação a ser utilizada, foi levado em consideração as características fundamentais que os protocolos precisam possuir para esse cenário, como pode ser visto na tabela 4, tais como: estratégia de roteamento baseada em vetor de distâncias, característica essa muito utilizada nesse cenário para o tráfego pesado de informações (imagens, vídeos e áudios); a convergência de rotas acelerada é outra característica importante para esse cenário, pois minimiza o tempo de convergência e aumenta a utilização de rotas ótimas, melhorando assim o desempenho e eficácia; o envio de mensagens periódicas de atualização para esse cenário deve ser por evento, pois garante que os nós sempre estarão com suas rotas atualizadas.

Tabela 4 – Protocolos que se adéquam ao cenário de levantamento de local de crime.

Características	**DSDV**	**WRP**
1) Estratégia de roteamento:		
Vetor de distância (DV)	T	T
Estado de enlace (LS)	N/A	N/A
2) Processamento de atualização de rotas:		
2.1) Convergência de rotas:		
Acelera a convergência	T	T
Rápida	N/A	N/A
3) Envio de atualização de rotas:		
3.1) Envio de mensagens periódicas:		
Por tempo	T	T
Por evento	T	T

Legenda:

T – Totalmente compatível;

P – Parcialmente compatível;

N/I – Não Informado;

N/A – Não se Aplica.

5.2.2 Busca, identificação e salvamento de vítimas em incidentes

Incidentes de grandes proporções como terremotos, grandes incêndios, maremotos, *tsunamis,* explosões e até mesmo quedas de aviões são exemplos de incidentes de destruição em massa que causam grande impacto social na população em busca de resultados rápidos dos órgãos públicos. Órgãos como polícia federal, bombeiros, defesa civil, hospitais, clínicas e institutos médico-legais são os mais procurados nesses incidentes. Geralmente nessas catástrofes ou eventos repentinos há mais mortos e feridos do que os recursos da localidade podem suportar. Eventos esses que podem ocorrer a qualquer momento e local, como os ocorridos recentemente na queda do avião da TAM no aeroporto de Congonhas em

São Paulo com quase 200 mortos, na queda do avião da *Air France* próximo da ilha de Fernando de Noronha com mais de 200 mortos ou até mesmo na enchente ocorrida em Santa Catarina em novembro de 2009, quando morreram 99 pessoas, mais de 50 mil ficaram sem abrigos e quase um milhão e meio de pessoas foram atingidas. Todos esses incidentes esgotaram os recursos de infraestrutura disponíveis para o atendimento imediato das vítimas. De acordo com opiniões e relatos feitos pelos órgãos participantes desses resgates, as maiores dificuldades enfrentadas foram a falta de equipamentos e infraestrutura de comunicação, já que os incidentes deixaram boa parte da população sem esses recursos. Toda a infraestrutura deve ser montada rapidamente nesses locais, pois alguns minutos podem ser determinantes para o salvamento de várias vidas. O seu uso permite compartilhar informações de busca de vítimas, identificação de pontos de risco, salvamento de vítimas, troca de informações e laudos médicos, podem ser enviados imagens e vídeos do próprio local do incidente. A solução que dará o melhor custo-benefício nessas situações são as redes *ad hoc*, pois sua montagem é rápida, barata, flexível e portátil, fatores primordiais para eficácia e eficiência da missão (NOGUEIRA, 2009).

No entanto, para se montar uma rede *ad hoc* em cenários como esses são necessários estudos técnicos, a fim de analisar a viabilidade do seu uso na situação, bem como avaliar que classificação e que protocolos poderão ser utilizados para que a rede *ad hoc* possua um resultado real favorável e não venha a ser só mais um equipamento de ajuda, e sim um equipamento primordial para o envio e recebimento de informações para o salvamento de vítimas.

Nesse cenário de aplicação, os nós tendem a se movimentar com maior frequência devido à área de alcance ser grande, havendo assim a necessidade de percorrer toda a área na busca de vítimas, portanto os protocolos para esse cenário devem se adaptar bem à grande dinamicidade dos nós. A quantidade de nós utilizados nesses cenários é geralmente grande, o que faz com que o fator escalabilidade seja outro fator relevante. Nesse cenário, apesar de envolver o salvamento de vítimas, o desempenho não se torna um fator primordial, já que o equipamento portátil servirá apenas para enviar informações. A energia de bateria é outro fator primordial, já que a durabilidade dessas operações costuma ser bem prolongada e os recursos disponíveis no local, como ausência de energia, pode ter sido afetada. A partir das

características de cada classificação de protocolos, como visto na tabela 3, é possível definir que a classificação **reativa** possui melhor adaptabilidade a esses fatores. Isso acontece devido à classificação possuir como principais características a dinamicidade, escalabilidade e economia de energia de bateria, contemplando assim todos os fatores primordiais desse cenário.

A partir da escolha da classificação a ser utilizada, foi levado em consideração as características fundamentais que os protocolos precisam possuir para esse cenário, como pode ser visto na tabela 5, tais como: a estrutura de armazenamento ser do tipo topologia parcial da rede e os nós guardarem suas rotas em cache, o que proporciona maior economia de energia de bateria, pois diminui a quantidade de sinalizações na rede e as rotas sendo guardadas em cache melhora o desempenho da rede; outra característica importante é a descoberta de rotas através de inundação controlada, pois também diminui a quantidade de sinalizações na rede e a sobrecarga de roteamento, fatores esses que consomem bastante energia de bateria; o envio de atualizações de rotas é outra característica importante nesse cenário, pois os dispositivos devem se manter sempre atualizados devido à grande dinamicidade dos nós, o envio de atualizações por evento garante que a partir de qualquer evento ocorrido nesse cenário se gere uma rajada de atualizações para os nós.

Tabela 5 – Protocolos que se adéquam ao cenário de busca, identificação e salvamento de vítimas.

Características	**AODV**	**DSR**
1)Estrutura de armazenamento:		
Topologia completa da rede em todos os nós	N/A	N/A
Topologia parcial da rede em todos os nós	T	T
Utiliza cache de rotas	T	T
Múltiplos caminhos	N/A	T
2) Processo de descoberta de rotas:		
Inundação de toda a rede	N/A	N/A
Inundação controlada	T	T
3) Envio de atualização de rotas:		
3.1) Envio de mensagens periódicas:		

Características	AODV	DSR
Por tempo	N/A	N/A
Por evento	T	T

Legenda:

T – Totalmente compatível;

P – Parcialmente compatível;

N/I – Não Informado;

N/A – Não se Aplica.

5.2.3 Segurança em eventos de grandes proporções

A segurança em eventos de grandes proporções é um fator extremamente relevante e requer total envolvimento de policiais, guardas armadas e seguranças para proteção dos envolvidos. Um evento é considerado de grande proporção quando é demandada a utilização de recursos além do que as forças policiais da localidade possam tomar de conta, tais como: Jogos Panamericanos, Copa do Mundo de Futebol, Olimpíadas, Cúpula e Reuniões de órgãos mundiais (ONU, UNESCO, OIT, etc). Nesses casos, existe a necessidade de um auxílio de outras unidades, como as forças de segurança nacional, policias federais ou até mesmo militares. Geralmente, eventos que necessitam desse tipo de segurança envolvem a presença de autoridades nacionais e internacionais. Todavia, um dos grandes problemas enfrentados por esses profissionais que fazem a segurança desses eventos é a ausência de tecnologia de comunicação de última geração, a fim de enviar, receber, coletar e transmitir informações do próprio local do evento (NOGUEIRA, 2009).

Os responsáveis pela organização e coordenação da segurança desses eventos convivem com a necessidade constante de informações sobre os locais que irão atuar. Contudo, as equipes subordinadas a esses coordenadores muitas vezes desconhecem em que locais deverão atuar, onde ficará localizada cada unidade ou equipe, quem será o responsável imediato pela organização do evento ou setores. Muitas vezes, o local do evento não possui planta ou mapa, não são conhecidas as autoridades participantes e sua importância ou até

mesmo possíveis alvos. Essas situações são reais e enfrentadas por parte de quem promove a segurança desses eventos. Além disso, outros fatores como grandes áreas dispersas, quantidade de empresas e pessoas envolvidas agravam ainda mais a complexidade da segurança. Outros fatores comuns a esses eventos são as mudanças de última hora na programação, devido a atrasos de vôos, acréscimos de pessoas a serem protegidas, monitoramento do local do evento, mudança de localidade dos eventos e até mesmo possíveis mudanças das rotas de fuga em caso de incidente. Portanto, fica mais do que comprovado que há necessidade de que todos os membros envolvidos na segurança possuam um meio de comunicação para transferência de dados e informações atualizadas e em tempo real. É nesse contexto que se inserem as redes *ad hoc* como tecnologia mais viável para esses tipos de situações, onde o tempo, a flexibilidade e agilidade são fatores primordiais e decisivos para o sucesso da operação. Essas redes irão fornecer a todos os envolvidos na segurança a possibilidade de enviar mensagens instantâneas, comandos, fotos, vídeos e até mesmo acesso à internet. A dinamicidade, rapidez na configuração, mobilidade, portabilidade e pronto atendimento fornecido nessas redes são fatores ímpares para o sucesso total dessas atividades (NOGUEIRA, 2009).

Portanto, para montar uma rede *ad hoc* nesse tipo de cenário é necessário avaliar que classificação e quais protocolos se adequarão melhor às circunstâncias e características da operação.

Nesse cenário de aplicação, a quantidade de envolvidos na segurança desses eventos costuma ser grande, portanto o protocolo a ser utilizado nesse cenário deve possuir boa escalabilidade. A movimentação nesse cenário é outro fator relevante, pois alguns nós necessitam estar transitando constantemente a fim de garantir a segurança dos convidados e autoridades, analisando diversos locais em áreas grandes, portanto os protocolos para esse cenário devem se adaptar bem à grande dinamicidade dos nós. Devido o cenário envolver a segurança de autoridades importantes, a rapidez é outro ponto bastante importante para esse cenário. Analisando as características de cada classificação de protocolos vista na tabela 3 é possível definir que a classificação **híbrida** possui melhor adaptabilidade a esses fatores. Com a utilização dessa classificação nesse cenário, é possível se obter a rapidez do envio de

informações dos protocolos pró-ativos, e a dinamicidade e escalabilidade dos protocolos reativos, contemplando assim todos os fatores primordiais desse cenário.

A partir da escolha da classificação a ser utilizada, foi levado em consideração as características fundamentais que os protocolos precisam possuir para esse cenário, como pode ser visto na tabela 6, tais como: estratégia de roteamento baseada em estado de enlace, característica esta importante devido a dinamicidade exigida pelo cenário; outra característica importante é a descoberta de rotas através de inundação controlada, pois diminui a quantidade de sinalizações na rede e a sobrecarga de roteamento e assim fornece melhor desempenho e economia de energia de bateria; a convergência de rotas acelerada é outra característica importante para esse cenário, pois minimiza o tempo de convergência e aumenta a utilização de rotas ótimas, melhorando assim o desempenho e eficácia; o envio de atualizações de rotas é outra característica importante nesse cenário, pois os dispositivos devem se manter sempre atualizados devido à grande dinamicidade dos nós, o envio de atualizações por evento garante que a partir de qualquer evento ocorrido nesse cenário se gere uma rajada de atualizações para os nós.

.

Tabela 6 – Protocolos que se adéquam ao cenário de Segurança em eventos de grandes proporções.

Características	**ZRP**	**ZHLS**
1) Estratégia de roteamento:		
Vetor de distância (DV)	P	N/A
Estado de enlace (LS)	P	T
2) Processo de descoberta de rotas:		
Inundação de toda a rede	N/A	N/A
Inundação controlada	T	T
3) Processamento de atualização de rotas:		
3.1) Convergência de rotas:		
Acelera a convergência	T	T
Rápida	N/A	N/A
4) Envio de atualização de rotas:		
4.1) Envio de mensagens periódicas:		

Características	ZRP	ZHLS
Por tempo	P	N/I
Por evento	P	T

Legenda:

T – Totalmente compatível;

P – Parcialmente compatível;

N/I – Não Informado;

N/A – Não se Aplica.

6. CONCLUSÕES

Com o passar do tempo houve a popularização das redes de computadores e, principalmente da Internet, o que acelerou o crescimento tecnológico e o surgimento das redes sem fio. Com esses avanços é cada vez maior o uso de recursos computacionais no mundo globalizado com a finalidade de aplicá-los em várias áreas de atuação. A comunicação sem fio cresceu bastante, principalmente devido à variedade de dispositivos móveis. Isso vem contribuindo para que as redes móveis sejam cada vez mais utilizadas, rompendo as barreiras entre mobilidade e integração de dispositivos. Nesse contexto, são inseridas as redes *ad hoc* móveis, que são formadas por um conjunto de dispositivos móveis conectados sem nenhuma ligação física. As redes *ad hoc* são temporárias e arbitrárias, portanto sua utilização é geralmente emergencial. Essas redes se tornaram uma tendência mundial e atualmente foram expandidas suas áreas de atuação. Em vários países globalmente desenvolvidos essas tecnologias já são utilizadas para segmentos como operações táticas; busca, identificação e salvamento de vítimas; e até mesmo para segurança de eventos.

Visto a novidade tecnológica, seu crescimento, seus desafios e suas áreas de atuação, a matéria despertou interesse de estudos e pesquisas. No decorrer dos estudos realizados foi possível perceber a ausência de pesquisas e resultados relacionados à melhor adequação de protocolos de roteamento em redes *ad hoc* para cenários emergenciais. Com isso esse trabalho se insere nesse contexto, o que caracteriza o ineditismo deste estudo. No entanto, para fornecer esses resultados foram necessários estudos relacionados às redes sem fio, como sua história, seus principais conceitos, sua composição e categorias, e os padrões existentes na atualidade. Também foi necessário pesquisar sobre as redes *ad hoc*, estudo esse que forneceu as bases do conhecimento necessário sobre essa tecnologia. Para se chegar aos objetivos delimitados pelo escopo do trabalho foi discutido aprofundadamente os principais

protocolos de roteamento de redes *ad hoc,* suas classificações e, principalmente, suas características. Logo após o estudo dos protocolos de roteamento das redes *ad hoc*, foi montada uma tabela comparativa de protocolos por características, e essas características foram escolhidas se baseando na necessidade dos cenários de aplicação. Por fim foram abordados cenários emergenciais e suas peculiaridades, e foram propostos para cada cenário os protocolos de roteamento de redes *ad hoc* que melhor se adequaram às peculiaridades do cenário.

Como contribuições acadêmicas e científicas, este trabalho abordou um referencial teórico que contempla os principais conceitos de redes sem fio e redes *ad hoc*, analisou vantagens e desvantagens das redes sem fio *ad hoc* móveis, caracterizou os principais protocolos de roteamento de redes *ad hoc*, elaborou cenários de aplicações de utilização de redes *ad hoc* e por fim, mostrou os protocolos de roteamento que melhor se adéquam a cada cenário abordado.

É válido destacar que como toda nova tecnologia, essa também possui a necessidade de se realizarem pesquisas constantes e superar diversos desafios e limitações. Papel este que rende estudos aprofundados em várias universidades e centros de pesquisas do mundo inteiro. É esperado que este trabalho possa auxiliar também esses estudantes e pesquisadores.

Por fim a grande questão tratada nesse trabalho foi o estudo comparativo entre os protocolos de roteamento, com o intuito de saber diferir o que cada protocolo se propõe a fazer, para a partir de suas características poder identificar quais deles se adéquam melhor a cenários reais emergenciais. O intuito dessa abordagem foi facilitar a decisão da escolha do protocolo a ser utilizado numa abordagem emergencial.

Como trabalhos futuros sugerem-se:

- Testar a aplicabilidade desses protocolos de roteamento propostos em cada cenário por meio de simulações utilizando ferramentas como o NS2;
- Estudar, comparar e analisar a aplicabilidade de outros protocolos de roteamento não estudados nesse trabalho para os cenários citados;

- Propor novos cenários de aplicação e testar a aplicabilidade dos protocolos citados neste trabalho.

REFERÊNCIAS BIBLIOGRÁFICAS

AMORIM, Glauco F. **Análise de Desempenho de Protocolos de Roteamento com Diferenciação de Serviços em Redes de Comunicação Móvel *Ad Hoc.*** 2002. 127 f. Dissertação de Mestrado (Sistema e Computação) Instituto Militar de Engenharia, RJ, Rio de Janeiro, 2002.

BASAGNI, Stefano; et al. **Mobile Ad hoc Networking.** Hoboken: Wiley-IEEE Press, 2004.

BRIGNONI, Guilherme V. **Estudo de Protocolos de Roteamento em Redes *Ad Hoc.*** 2005. 73 f. Trabalho de Conclusão de Curso (Ciências da Computação) Universidade Federal de Santa Catarina, SC, Florianópolis, 2005. Disponível em <http://projetos.inf.ufsc.br/arquivos_projetos/projeto_208/TCC%20-%20Estudo%20de%20protocolos%20de%20roteamento%20em%20redes%20Ad%20hoc.pdf >

CAMPOS, Gláucia M. M. **Avaliação de Desempenho de Protocolos de Roteamento para Redes Móveis *Ad Hoc* sob Condições de Tráfego de Aplicações de Videofone.** 2005. 110 f. Dissertação de Mestrado (Departamento de informática e Matemática aplicada) Universidade Federal do Rio Grande do Norte, RN, Rio Grande do Norte, 2005. Disponível em: < http://www.ppgsc.ufrn.br/html/Producao/Dissertacoes/GlauciaMelissaMedeirosCampos.pdf>. Acesso em 15 de maio de 2010.

COMER, Douglas E. **Redes de computadores e Internet.** 4. Ed. São Paulo: Editora Bookman, 2007.

CORDEIRO, Carlos M.; AGRAWAL, Dharma P. **Ad hoc & Sensor Networks: Theory and**

Applications. Hackensack: World Scientific Publishing, 2006.

CORRÊA, Underléa C. **Proposta de um *Framework* de Roteamento para Redes Móveis *Ad Hoc*.** 2005. 106 f. Dissertação de Mestrado (Programa de Pós-Graduação em Ciência da Computação) Universidade Federal de Santa Catarina, SC, Rio Grande do Sul, 2005. Disponível em: <http://www.lisha.ufsc.br/~guto/teaching/theses/underlea.pdf>. Acesso em 15 de maio de 2010.

CUNHA, Daniel O. **Roteamento em MANETs.** In: Seminário de Redes de Computadores, 1. 2002. Rio de Janeiro. Disponível em < http://www.gta.ufrj.br/seminarios/semin2002_1/Daniel/>. Acesso em: 23 de maio de 2010.

DIXIT, Sudhir; PRASAD, Ramjee. **Technologies for Home Networking**. Hoboken: John Wiley & Sons, 2005.

FARIAS, Márcio M. **Estudo Comparativo em Algoritmos de Roteamento para Redes *Wireless Ad Hoc*.** 53 f. 2006. Curso de Pós-Graduação (Ciência da Computação) Pontífica Universidade Católica do Rio Grande do Sul, RS, Rio Grande do Sul, 2006. Disponível em < http://www.inf.pucrs.br/~eduardob/pucrs/research/students/MarcioFarias/TI1/ti_12_07.pdf> Acesso em 15 de maio de 2010.

FERNANDES, Natalia C. **Controle de Acesso Distribuído para Redes Ad hoc**. 2008. 132 f. Dissertação de Mestrado (Engenharia Elétrica) Universidade Federal do Rio de Janeiro, RJ, Rio de Janeiro, 2008. Disponível em <*www.gta.ufrj.br/ftp/gta/TechReports/natalia08.pdf*>. Acesso em 02 março de 2010.

FERNANDES, Bruno V. **Protocolos de Roteamento em Redes *Ad Hoc***. 2003. 90 f. Dissertação de Mestrado (Instituto de Computação) Universidade Estadual de Campinas, SP,

São Paulo, 2003. Disponível em < *http://libdigi.unicamp.br/document/?down=vtls000342497*>. Acesso em 10 maio de 2010.

FERNANDES, Rafael M. S. **Zone Routing Protocol - ZRP**. Programa de Engenharia de Sistema e Computação – Coppe/UFRJ. Rio de Janeiro. RJ. 2006. Disponível em < *http://www.gta.ufrj.br/ensino/CPE825/2006/resumos/TrabalhoZRP.pdf*>. Acesso em 15 maio de 2010.

FLICKENGER, Rob. **Building *Wireless* Community Networks**. Cambridge: O'Reilly, 2001.

GAST, Mattew. **802.11 *Wireless* Networks: The Definitive Guide**. Cambridge: O'Reilly, 2002.

HAAS, Zygmunt J.; TABRIZI, Siamak. **On Some Challenges and Design Choices in Ad hoc Communications**. Bedford: International Conference for Military Communications, Proceedings IEEE MILCOM , 1998.

IETF. **Fisheye State Routing Protocol (FSR) for *Ad Hoc* Networks.** 2002. Disponível em < http://tools.ietf.org/html/draft-ietf-manet-fsr-03>. Acesso em 13 de maio de 2010.

KEEGAN, Warren J. **Marketing Global.** 7ª ed. São Paulo: Pearson, 2006.

KUROSE, James F.; ROSS, Keith W. **Redes de Computadores e a Internet: Uma Nova Abordagem**. 3. ed. São Paulo: Addison Wesley; 2006.

KWOK, Yu Kong R.; LAU, Vincent K. N. ***Wireless*** **Internet and Mobile Computing**: Interoperability and Performance. Hoboken: John Wiley & Sons, 2007.

MACCABE, Karen. **Ieee ratifies 802.11n, *Wireless* LAN specification to provide significantly improved data throughput and range.** Piscataway – New Jersey, 2009. Disponível em <http*://standards.ieee.org/announcements/ieee802.11n_2009amendment_ratified.html*>. Acesso em 15 abril 2010.

NIEBERT, Norbert; et al; **Ambient Networks Co-Operative Mobile Networking for *Wireless* World**. West Sussex: John Wiley & Sons, 2007.

NOGUEIRA, José Helano M. **Alerta**: **As Redes Sem Fios Chegaram**. Brasília-DF: I Conferência Internacional de Perícias em Crimes Cibernéticos, 2004.

NOGUEIRA, José Helano M. **Aplicações de Redes sem Fio *AD HOC* Móveis em Operações Policiais**. 2009. 71 f. Trabalho de Conclusão de Curso (Gestão de Políticas de Segurança Pública) Academia Nacional de Polícia, DF, Brasília, 2009.

PEI, Guangyu; GERLA, Mario; CHEN, Tsu-Wei. **Fisheye State Routing in Mobile *Ad Hoc* Networks.** *Proceedings of workshop on Wireless Network and Mobile Computing,* Taipei, Taiwan, Abril. 2000.

PEREIRA, Ivana C. M. **Análise do Roteamento em Redes Móveis Ad hoc em Cenários de Operações Militares**. 2004. 107 f. Dissertação de Mestrado (Engenharia Elétrica) Universidade Federal do Rio de Janeiro, RJ, Rio de janeiro, 2004. Disponível em < http://www.pee.ufrj.br/teses/textocompleto/2004064002.pdf > Acesso em 02 de abril 2010.

REDIN, João C. **Segurança de Dados no Contexto de Redes *Ad Hoc***. 2004. 98 f. Dissertação de Mestrado (Programa de Pós-Graduação em Ciência da Computação) Universidade Federal de Santa Catarina, SC, Rio Grande do Sul, 2004. Disponível em: < http://www.inf.ufsc.br/~rsvargas/disser.pdf>. Acesso em 17 de maio de 2010.

REZENDE, Nelson S. **Redes Móveis sem fio *ad hoc*.** 2004. 87 f. Trabalho de Conclusão de Curso de Pós-Graduação (Gerência de Redes de Computadores) Universidade Federal do Rio de Janeiro, RJ, Rio de Janeiro, 2004. Disponível em <http://www.nce.ufrj.br/labnet/Teses_Artigos_Finais/Nelson_Soares/Monografia_MOT.pdf> Acesso em 18 de Abril 2010.

RODRIGUES, Miguel. **Redes Móveis Ad hoc**: **Necessidades e Desafios**. 2004. 129 f. Trabalho de Conclusão de Curso (Lic. Engenharia de Informática) Instituto Superior de Engenharia do Porto. PT, Porto, 2004. Disponível em: < *www.dei.isep.ipp.pt/~paf/.../Redes%20Moveis%20Ad%20Hoc.pd* > Acesso em 22 de março 2010.

SARKAR, Subir K.; BASARAVAJU, T. G.; PUTTAMADAPPA, C. **Ad hoc Mobile *Wireless* Networks**: **principles, protocols, and applications**. Boca Raton: Auerbach Publications, 2008.

SACRAMENTO, Vágner. **Redes Locais Sem Fio – Wireless LAN**. 2007. Notas de aula. Disponível em <http://www-di.inf.puc-rio.br/~endler/courses/Mobile/transp/WLAN-80211.pdf>. Acesso em 20 de abril de 2010.

STALLINGS, William. **Criptografia e Segurança de Redes**: **Princípios e Práticas**. 4. ed. São Paulo: Editora Prentice Hall, 2006.

TANENBAUM, Andrew. S. **Redes de Computadores**. 4. ed. São Paulo: Editora Campus, 2003.

WALKE, Bernhard H.; MANGOLD, Stefan; BELERMANN, Lars. **IEEE 802 *Wireless* Systems Protocols, Multi-hop Mesh/Relaying, Performance and Spectrum Coexistence**. West Sussex: John Wiley & Sons, 2006.

WEBB, William. ***Wireless* Communications**: **The Future**. Hoboken: John Wiley & Sons, 2007.

WU, Shih Lin; TSENG, Yu Chee. ***Wireless* Ad hoc Networking**: **Personal-Area, Local-Area, and The Sensory-Area Networks**. Boca Raton: Auerbach Publications, 2007.

MATERIAL DE ESTUDO

JENSEN, Robert A. **Mass Fatality and Casualty Incidents: A Field Guide**. Washington, DC: CRC Press, 1999.

KAVEH, Pahlavan. ***Wireless*** **Information Networks**. Hoboken: John Wiley & Sons, 2005.

NOGUEIRA, José Helano M; JÚNIOR, Joaquim C. **Computação Autonômica Aplicada à Criminalística Computacional**. Gramado-RS: VIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, Anais do SBSEG, 2008.

SARANGAPANI, Jagannathan. ***Wireless*** **Ad hoc and Sensor**: Networks, Protocols, Performance, and Control. Boca Raton: CRC Press, 2007.