UNIPAC
UNIVERSIDADE PRESIDENTE ANTÔNIO CARLOS
FACULDADE DE CIÊNCIA DA COMPUTAÇÃO

CURSO DE CIENCIA DA COMPUTAÇÃO

Márcio Lopes Silvério

REDES AD HOC: PROTOCOLO DE ROTEAMENTO E SEGURANÇA

BARBACENA
JULHO DE 2005

MÁRCIO LOPES SILVÉRIO

REDES AD HOC: PROTOCOLO DE ROTEAMENTO E SEGURANÇA

Monografia apresentada à
Universidade Presidente Antonio Carlos,
como requisito parcial para
a obtenção do título de
Bacharel em Ciência da Computação

ORIENTADOR: Luís Augusto Mattos Mendes

Barbacena
Julho de 2005

MÁRCIO LOPES SILVÉRIO

REDES AD HOC: PROTOCOLO DE ROTEAMENTO E SEGURANÇA

Monografia apresentada à
Universidade Presidente Antonio Carlos,
como requisito parcial para
a obtenção do título de
Bacharel em Ciência da Computação

Aprovada em _____/_____/_____

BANCA EXAMINADORA

.....
Prof. Luis Augusto Mattos Mendes (Orientador)
Universidade Presidente Antônio Carlos

.....
Prof. Msc. Gustavo Campos Menezes (Membro da Banca Examinadora)
Universidade Presidente Antônio Carlos

.....
Prof. Msc. Elio Lovisi Filho (Membro da Banca Examinadora)
Universidade Presidente Antônio Carlos

Barbacena
Julho de 2005

Agradecimentos

Quero primeiramente agradecer aos meus pais, por acreditarem em mim e me ajudarem, mais uma vez, a dar o primeiro passo rumo a essa grande vitória.

Aos meus irmãos por serem fonte inspiradora desta conquista.

Aos meus amigos, por serem meus professores e me ensinarem a nunca desistir diante das adversidades que apareceram durante esta grande jornada, e muitas outras que aparecerão durante toda a minha vida, compreendo agora que aprendi esta lição, já que estou colhendo o fruto desta persistência.

A minha namorada, pela paciência e amor dedicados a minha pessoa, outra não os teria tanto, por ter me ajudado e me mostrado o que a dor fez esquecer, o amor.

Aos meus parentes por estarem sempre presentes durante esta jornada.

Um agradecimento especial aos meus avós, principalmente ao Sr. Francisco Severino Lopes (*in memoriam*), por me darem um grande exemplo de vida.

Aos meus professores pelos anos de dedicação ao ensino e a formação de novos profissionais.

Depois destes agradecimentos quero finalizar agradecendo a quem tornou tudo isso possível, Deus. Foi Ele que colocou todas essas pessoas para caminharem lado a lado comigo e nunca deixou que eu caminhasse sozinho. Foi Ele que me disse para sempre acreditar em meus sonhos, se eu desejar do fundo do meu coração e ter fé eles se transformarão em realidade.

Obrigado!

Márcio Lopes Silvério

Barbacena

Julho de 2005

SUMÁRIO

Barbacena

Julho de 2005

LISTA DE FIGURAS

Barbacena

Julho 2005

1-INTRODUÇÂO

Com o avanço dos diversos tipos de tecnologias, principalmente na área de comunicação, e o surgimento de inúmeras outras tecnologias na área de informática, as redes sem-fio se tornaram um grande marco na história da comunicação da humanidade. Por conseqüência, estas tecnologias transformaram a forma de se comunicar das pessoas e impuseram um novo significado a forma de comunicação da humanidade.

O objetivo deste trabalho é tratar como esta comunicação é feita e se desenvolveu ao longo de anos de pesquisa, é o objetivo deste trabalho, focando mais especificamente redes *ad hoc*, uma tecnologia recente e ainda em desenvolvimento.

O capitulo 2 diferencia uma rede *ad hoc* de uma rede sem-fio convencional. Este capítulo é fundamental para estabelecer conceitos básicos que possibilitem uma visão geral de uma rede *ad* hoc, suas vantagens e desvantagens perante uma rede sem-fio convencional, além de considerar a sua capacidade de transmissão de dados, sua utilidade e como esta se comunica dentro da sua própria estrutura.

O capitulo 3 é um ponto importante deste projeto, pois trata de como as redes *ad hoc* se comunicam entre si. Para que seja possível a comunicação entre as redes *ad hoc* são utilizados protocolos de roteamento que são responsáveis pela comunicação entre os nós que compõem a rede.

O capítulo 4 apresenta os fatores de segurança que compõem este tipo de rede, que mostrando as vulnerabilidades e as falhas da rede *ad hoc* bem e como estes algorítmos reagem a ataques do meio externo e/ou até mesmo de “nós maliciosos” e como solucionar alguns destes problemas.

2-REDES SEM FIO

Com o crescente volume de informações circulando a todo o momento pelos diversos meios de comunicação existentes , principalmente pela *Internet*, e o mundo globalizado impulsionando as pessoas a se manterem sempre informadas torna-se mais necessário à mobilidade. Sendo assim, nos dias atuais as redes sem-fio nos permitem comunicar com outras pessoas, e até mesmo computadores remotos, mesmo estando em constante movimento.

As redes sem-fio tiveram sua primeira aplicação e desenvolvimento no período entre guerras, mais especificamente 1ª e 2ª Grande Guerras, onde seu uso foi largamente difundido. Alguns especialistas já afirmam que no futuro só haverá dois tipos de comunicação uma através de fibra ótica e outro através de redes *wireless* ou sem-fio [1].

As redes *wireless* constituem o principal meio de comunicação existente e em grande expansão e podendo ser divididas em dois tipos:

Redes sem-fio com infra-estrutura montada ou centralizada e Redes *ad hoc*[1] ou sem infra-estrutura.

2.1-Redes sem fio com infra-estrutura montada

As redes sem fio com infra-estrutura montada são assim definidas, porque utilizam pontos de acesso *(Acess Point*) para estabelecer a comunicação entre dois pontos. A Figura 1 além de ilustrar esse modo de transmissão, ainda demonstra que

[1] Ad hoc- Do latim " ad hoc" que significa literalmente para isto ou apenas para este propósito

ondas de radio são o tipo de tecnologia utilizada para se estabelecer à comunicação entre os diversos pontos da rede. A tecnologia utilizada na Figura 1é uma transmissão por ondas de rádio onde cada *ERB* (Estação de Rádio Base) corresponde a uma área específica e sua área de abrangência.

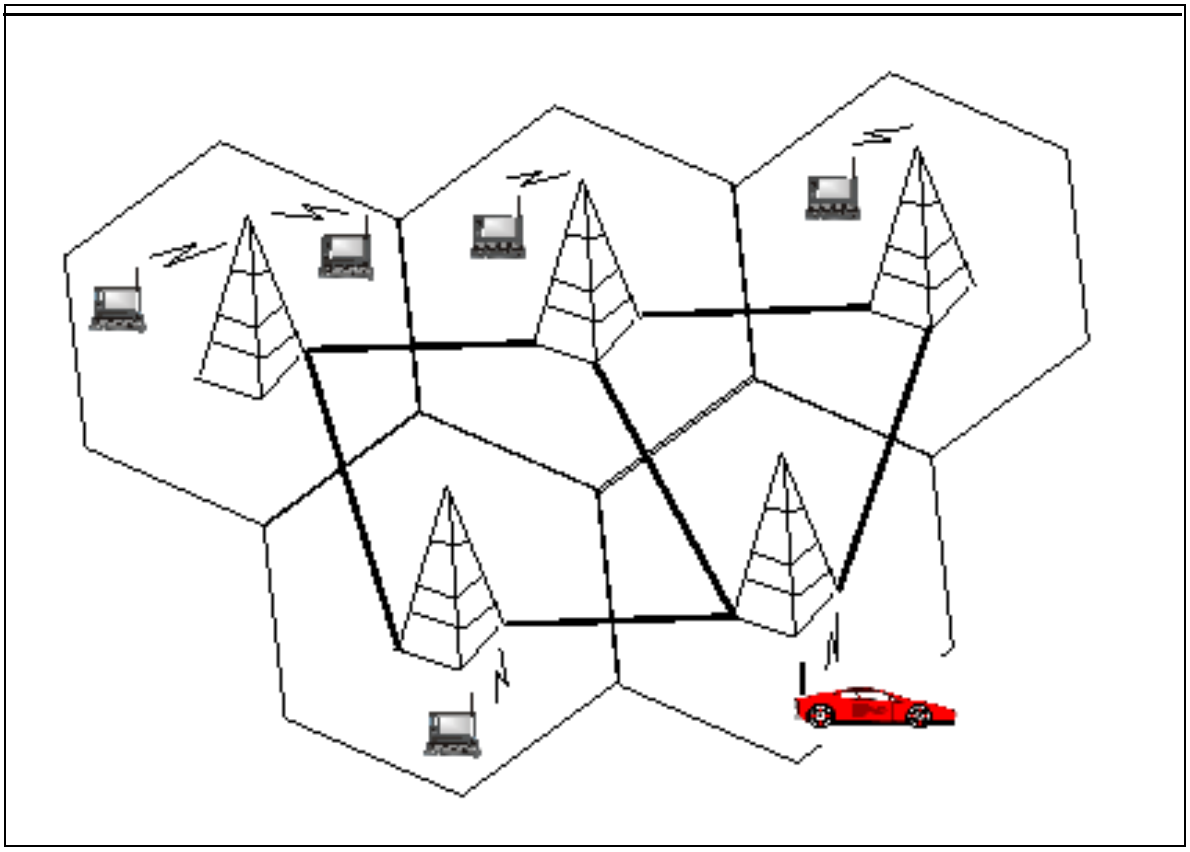

Figura 1- Redes sem fio com ponto de acesso (*Acess Point*)

Uma rede *wireless* pode ser implantada em qualquer tipo de terreno ou área, visto que é possível analisar a viabilidade de sua implantação e adequando assim os diversos tipos de comunicação de uma rede sem fio. Adequar a implantação de uma rede sem fio a topologia de uma determinada área pode trazer inúmeros benefícios, não só econômicos, como também no que se refere à forma de transmissão, evitando assim perda de informações decorrentes de interferências eletromagnéticas ou mesmo obstáculos naturais que o próprio meio poderá impor a transmissão da informação.

Através da implantação de antenas, podem ser transmitidas e recebidas informações a uma distância consideravelmente grande, o que depende do tipo de

transmissão utilizado. A seguir serão apresentados os tipos de transmissão mais utilizados.

2.1.1-Transmissão via ondas de rádio

Atualmente são as mais utilizadas, pois são omnidirecionais, ou seja, se propagam em diversas direções a partir do ponto de origem. Isso significa que nem sempre o receptor precisa estar na mesma direção do ponto que transmite a informação [1].

As ondas transmitidas por este tipo de transmissão podem percorrer grandes distâncias, dependendo do tipo de freqüência com que a transmissão é feita, ondas de baixa freqüência percorrem distâncias menores, atravessam qualquer obstáculo e se propagam em qualquer direção, já as ondas de alta freqüência conseguem percorrer maiores distâncias pois, se propagam em linha reta mas tendem a sofrer a interferência da chuva e não atravessam barreiras naturais [1].

A capacidade das ondas de percorrerem grandes distâncias, pode se tornar um grande problema para os usuários desse tipo de transmissão, já que uma freqüência pode chegar a interferir sobre a outra. Nesse caso os governos chegam a desempenhar o papel de controladores de freqüências. No Brasil o órgão responsável por esta fiscalização é a Anatel (Agência Nacional de Telecomunicação). A Anatel permite a exploração das diversas freqüências distribuídas conforme a classificação abaixo [7], [8] e [9]:

-Ondas Médias: Opera na faixa de 525 KHz a 1.605 KHz e 1.605 Khz a 1.705 KHz, com modulação em amplitude;

-Ondas Tropicais: Opera nas faixas de 2.300 KHz a 2.495 KHz, 3.200 KHz a 3.400KHz, 4.750 KHz a 4.995 KHz e 5.005 KHz a 5.060 KHz, com modulação em amplitude;

-Ondas Curtas: Opera nas faixas de 5.950 kHz a 6.200 kHz, 9.500 kHz a 9.775 kHz, 11.700 kHz a 11.975 kHz, 15.100 kHz a 15.450 kHz, 17.700 kHz a 17.900 kHz, 21.450 kHz a 21.750 kHz e 25.600 kHz a 26.100 kHz, com modulação em amplitude.

2.1.2-Transmissão através de microondas

A transmissão de microondas é um meio muito utilizado em comunicação de longa distância, telefonia celular e transmissão de televisão.

As microondas trafegam em linha reta, tornando assim à distância entre as torres de transmissão e os pontos de recepção ou de retransmissão da informação muito distantes entre si.

As freqüências mais baixas de microondas, ao contrário das de rádio não atravessam obstáculos, não sendo assim as mais viáveis para serem utilizadas nas transmissões. Um outro problema das transmissões por microondas é que algumas dessas ondas podem ser refratadas nas camadas atmosféricas mais baixas, retardando a chegada das informações ao seu destino. Esse processo é chamado de *fading* por múltiplos caminhos (*multipath fading*), para se evitar esse problema os operadores costumam manter dez por cento de seus canais ociosos como sobressalentes para se evitar o *fading*.

As freqüências em que são transmitidas as informações por microondas são cada vez mais altas, devido a um grande avanço tecnológico, mas isso gera um grande problema, visto que a partir de 8GHz as ondas são absorvidas pela água, gerando assim, “um grande aparelho de microondas a céu aberto”.

As transmissões através de microondas tem inúmeras vantagens em relação à telefonia fixa, já que dependendo da banda a ser utilizada por esse tipo de transmissão não é necessária uma licença de operação.

2.1.3-Ondas milimétricas e infravermelho

São usadas em larga escala nas comunicações sem fio de curto alcance, dentro de pequenas empresas e escritórios, são ondas relativamente direcionais, baratas e de fácil instalação, daí serem as preferidas de empresas para instalação já que não atravessam obstáculos. Talvez esse seja o único inconveniente deste tipo de rede, mas isso vem favorecer as empresas no que se diz respeito à espionagem industrial.

2.2-Padrões *IEEE* 802.11

Para se fazer à comunicação entre pontos de uma rede *wireless,* criou-se normas internacionais que regem a interconexão entre os mais diversos tipos de equipamentos. O IEEE *(Institute of Electrical and Eletronics Engineers)* é o órgão que regulamenta e estabelece os padrões e normas técnicas para esse tipo de transmissão.

Entre os diversos padrões existentes, que regularizam a interconexão de equipamentos sem fio, a família mais utilizada é a do padrão IEEE 802.11. Esse padrão é o responsável por estabelecer o enlace entre redes locais sem fio, também denominados de padrão *WLAN'S* (*Wireless Local Networks)* ou *Wi-Fi* (*Wireless Fidelity*) ou fidelidade sem fio [10].

Segundo o IEEE, existem na família 802.11 subdivisões porém, todas elas utilizam o mesmo padrão de protocolo para transmissão na Internet. Elas foram classificadas, pelo IEEE, da seguinte maneira [12]:

802.11- Aplicado em LAN's*, em* 1ou 2 Mbps em uma freqüência de 2,4 GHz.

802.11a- Uma extensão do 802.11 e atua na faixa de 54 Mbps e numa freqüência que pode variar de 5 GHz a 6 GHz.

802.11b- O mais utilizado para transmissões de dados devido as suas características que evidenciam maior segurança na transmissão dos dados, mais rapidez na transmissão dos mesmos e são menos susceptíveis a interferências de programação *multipath*.

802.11e- É o primeiro padrão que atravessa ambientes fechados. Soma qualidade de serviço (*QoS*) a características de multimídia. Auxilia outros padrões existentes da família 802.11 e mantém a compatibilidade com os outros padrões anteriores. Além da *QoS* a característica de oferecer transmissões de áudio e vídeo a clientes residenciais e alta velocidade nas transmissões de acesso a Internet uma de suas principais vantagens.

802.11g-Também aplicado em LAN's e provê mais de 20 Mbps de transmissão, nos seus 2,4 GHz de freqüência. É o mais recente padrão aprovado pelo IEEE oferecendo 54 Mbps em transmissões de curta distância, também operam na mesma faixa de freqüência dos padrões 802.11 e 802.11b e é compatível com seus antecessores

802.11i- Soma as características dos seus padrões anteriores à característica AES (*Advanced Encription Standard*), ou seja, a característica de criptografia avançada, que é o protocolo de segurança para os padrões 802.11

2.3-Redes *ad hoc*

Redes *Ad Hoc* ou *MANET (Mobile Ad Hoc Network)* são redes *wireless* que não dependem de uma infra-estrutura montada para se comunicar, ou seja, não precisam de uma central responsável para se estabelecer à comunicação entre dois pontos da

rede, os próprios nós ou pontos da rede são as “centrais” de transmissão de informações. A *Figura 2* demonstra como é feito este tipo de transmissão.

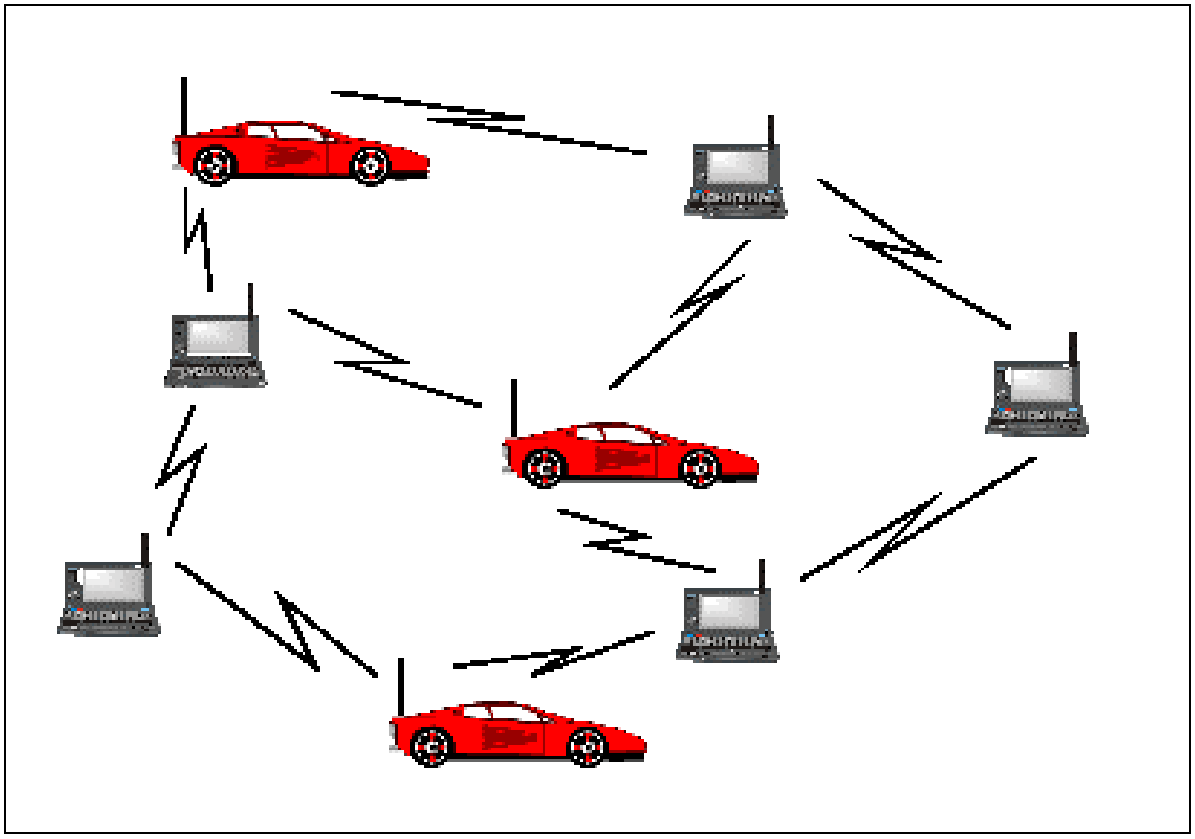

Figura 2- Transmissão em uma rede *Ad Hoc*

Uma das principais características de uma rede *Manet é* se adaptar a qualquer tipo de terreno (topologia), já que cada nó da rede é o responsável, não só em enviar uma informação ou pacote de dados a outro nó, como também por encontrar um caminho que leve a informação ao ponto desejado. Mas o ponto desejado (destinatário) que pode estar em qualquer lugar dentro de uma área especifica.

Os nós de uma rede *ad hoc* podem mudar constantemente a sua posição dentro da rede, o que depende da mobilidade dos nós propriamente dita, assim conectividade entre os nós pode mudar constantemente, requerendo uma permanente adaptação e reconfiguração das rotas de transmissão.

Uma outra característica de uma rede *ad hoc* é a de que um nó passa a fazer parte da rede quando envia, recebe ou retransmite a mensagem de um ponto a outro dentro da rede.

A utilização de uma rede *ad hoc*, esta inicialmente associada a cenários de difícil acesso e onde é complicado instalar uma rede de infra-estrutura em um curto espaço de tempo.

Quando foi criado e aplicado o conceito de redes *ad hoc* seu principal uso era o militar, e foi neste cenário em que se desenvolveu mais a tecnologia *ad hoc*.

Hoje em dia, devido ao avanço tecnológico, uma rede *ad hoc*, pode ser utilizada em diversos tipos de aplicações , tais como:

Coordenação de resgates em situações de desastre e compartilhamento de informação em reuniões e conferências.

Devido ao constante desenvolvimento de tecnologias em redes *wireless,* que possibilitam o melhor aproveitamento dos recursos disponíveis buscando sempre uma logística que defina melhor o termo eficiência no que se refere à utilização de uma rede *ad hoc*, a sua utilização está se tornando muito mais abrangente.

2.3.1-Vantagens e Desvantagens

Ao se comparar uma rede *ad hoc* a uma rede de infra-estrutura, podemos citar algumas vantagens e desvantagens de uma rede *ad hoc* em relação a todo o processo que as envolve, conforme apontado por Pinheiro [6]:

Vantagens	Desvantagens
Instalação rápida, já que redes *ad hoc* são estabelecidas dinamicamente em qualquer local	Roteamento, talvez a principal desvantagem de uma rede *ad hoc,* pois, em uma topologia de rede dinâmica torna a construção de algorítmos uma tarefa difícil
Tolerância a falhas, adapta-se as constantes mudanças da rede permitindo que perdas de conectividade sejam facilmente resolvidas	Localização, o endereço de uma máquina não tem relação com sua posição atual
Mobilidade, a principal característica de uma rede *ad hoc*	Banda passante, em redes cabeadas pode chegar a 1Gbps, já em redes *wireless ad hoc* chega a atingir até 54Mbps
Conectividade, desde que dois ou mais nós estejam no raio de alcance do outro	Taxa de erros, se comparada a enlaces de infra-estrutura a taxa é bem mais elevada

Tabela 1-Vantagens e Desvantagens de uma rede *ad hoc*

2.3.2-Transmissão de Dados em uma rede *ad hoc*

Em uma rede *wireless* com uma infra-estrutura montada, quando um nó deseja transmitir uma informação, o ponto de acesso é quem faz a verificação se o nó de destino está dentro da área de abrangência do seu sinal e só retransmite a mensagem até o seu destino.

Já em uma rede *ad hoc*, cada ponto pode, por si só, transmitir ou retransmitir a mensagem, até o seu destino, essa talvez seja a principal característica que diferencia uma rede *ad hoc* de uma rede de infra-estrutura montada.

Quando um nó deseja transmitir uma informação, a primeira coisa a verificar é se o nó de destino está no raio de alcance do nó que deseja transmití-la, caso este nó não esteja no raio de alcance deve-se formar uma cadeia de nós até que a informação possa chegar ao nó de destino, esse processo é denominado de *multi-hop* (múltiplos saltos) . Deste modo o alcance de cada nó não fica limitado ao seu raio de atuação.

A F*igura 3* ilustra um processo *multi-hop* entre *A* e *D. D* encontra-se fora do raio de atuação de A, mas a transmissão é possível graças a capacidade que os nós de uma rede *ad hoc* possuem, a de poder rastrear e transmitir pacotes de dados de um nó fonte até o nó de destino.

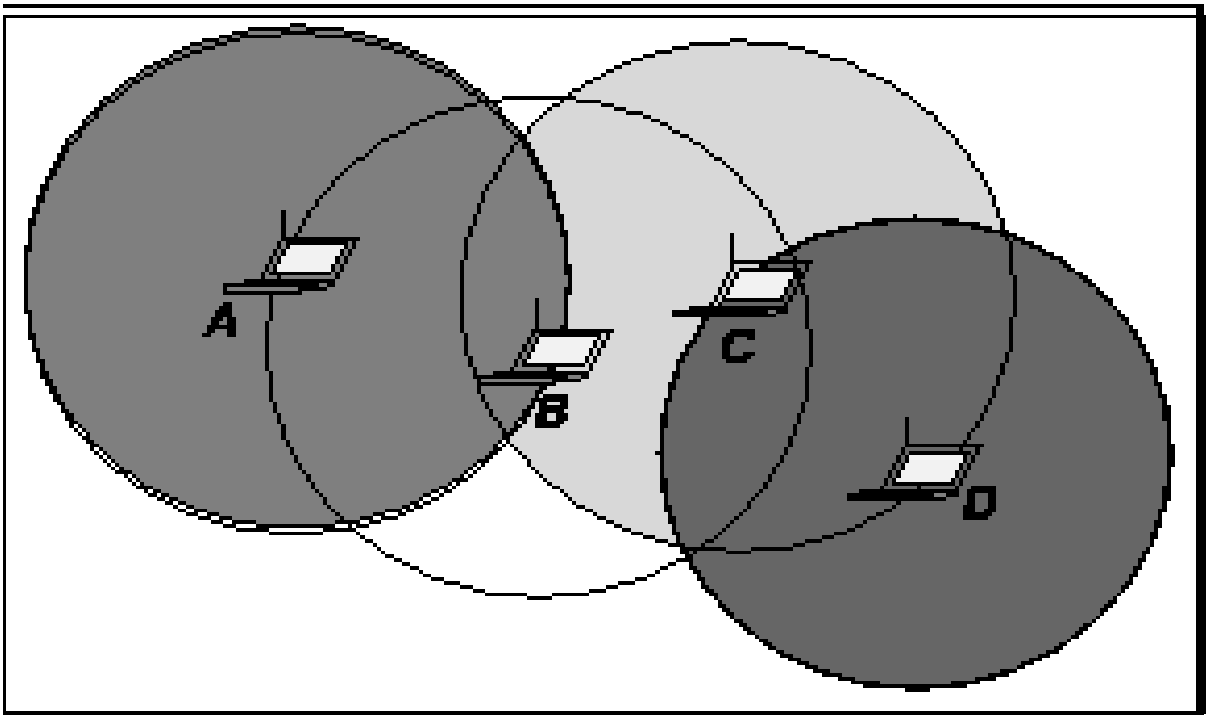

Figura* 3- Processo *multi-hop

Este processo aparentemente simples é na verdade muito mais complexo do que imaginamos visto que inúmeras considerações são feitas e tratadas de acordo com o tipo de algoritmo de roteamento usados pelos nós para transmitir a mensagem da sua fonte ao seu destino e serão abordadas no capítulo 3 sobre cada tipo de protocolo de roteamento.

Todo o processo descrito até então, é feito através de algoritmos de roteamento que tem como principal função determinar qual caminho o pacote de dados vai percorrer até chegar ao seu destino, bem como o envio da confirmação de recebimento do pacote pelo nó de destino.

Podemos classificar uma rede *ad hoc* de várias maneiras, no entanto, a forma mais usual é classificá-la quanto ao tipo de roteamento que ela utiliza. Quanto a este quesito, podemos classificar uma rede *ad hoc* de duas maneiras, que serão melhor detalhadas nos capítulos 2.3.3 e 2.3.4:

- Pró-ativos ou *Table-driven*;
- Reativos ou *On-Demand* (sobdemanda).

2.3.3- Protocolos de Roteamento Pró-Ativos

Os primeiros protocolos de roteamento *ad hoc* que surgiram eram pró-ativos. Tais protocolos têm como característica principal utilizarem-se de uma memória *"cache"*[2] , para armazenar rotas que são mantidas e utilizadas temporariamente, já que os nós da rede se movem aleatoriamente. Tudo isso é com o intuito de já se ter traçado um caminho que liga o nó fonte ao nó de destino já armazenado na memória, evitando assim o tempo de latência para o estabelecimento da conexão entre dois ou mais nós da rede.

Este tipo de protocolo é bastante utilizado em redes cabeadas, e podemos utilizar vários tipos de algoritmos, tais como os baseados em estado de enlace e vetor de distância [3], [5].

O uso desses algorítmos visa manter as rotas sempre atualizadas, evitando assim, que uma rota não esteja correta e gere indefinidas mensagens de erros já que a cada instante os nós não estão na mesma posição em que iniciaram a transmissão do pacote e os custos acabam sendo muito altos.

[2] *Cache*- Armazena rotas que são mantidas e usadas temporariamente

Um destes custos é o chamado *"overhead"*[3]*",* acarretando um maior consumo de bateria, talvez esse seja um dos principais problemas de uma rede *ad hoc*.

Outro grande problema causado por este tipo de roteamento, é a chamada técnica de inundação, que consiste em mandar informações de roteamento para todos os nós de uma rede, podendo gerar assim, ciclos (*loops)* indesejáveis e rotas erradas [3].

O desperdício de banda, juntamente com o desperdício de processamento sobre estas rotas, que constantemente mudam de posição e algumas dessas rotas nem sempre chegam a ser usadas, fecha o quadro das desvantagens causadas por este tipo de algoritmo.

2.3.4- Protocolados de Roteamento Reativos

Com os inúmeros problemas causados pelos algoritmos de roteamento pró-ativos, teve-se a necessidade de criar os protocolos reativos que conseguem, na maioria dos casos, sanar as deficiências causadas pelos algoritmos pró-ativos.

A transmissão de dados em um algoritmo reativo ocorre de acordo com critérios estabelecidos em ordem cronologicamente disposta da seguinte forma.

Em primeira instância, o nó que deseja transmitir o pacote de dados envia mensagens a vários outros nós da rede perguntando se estes são nós de destino do pacote, caso este nó não seja o nó de destino, o nó em questão anexa o seu endereço ao cabeçalho da mensagem e este retransmite a mensagem até que ela chegue ao destino, quando a mensagem chega ao nó de destino este envia uma mensagem ao nó que enviou o pacote confirmando a entrega do mesmo e o caminho é percorrido pelo pacote em sentido contrário.

Mesmo conseguindo sanar algumas deficiências dos protocolos pró-ativos, os protocolos do tipo reativo causam o aumento no tempo de latência[4] no estabelecimento

[3] Overhead- cada nó deve ficar mais tempo ligado a rede
[4] Latência- Tempo que se dá entre o envio e resposta de uma requisição de transmissão

das comunicações. Mas na maioria dos casos a troca de um algoritmo pró-ativo por um reativo acaba sendo mais vantajosa [3].

2.3.5- Características Essenciais a um Protocolo de Roteamento

Diante dos vários tipos de protocolos existentes, não só reativos como também pró-ativos, cada qual com características diferentes e adaptados a diversos tipos de cenários diferentes, é impossível estabelecer qual é o mais adequado a um cenário específico.

No entanto, o grupo de trabalho MANET, estabeleceu um determinado número de requisitos que um protocolo de roteamento *ad hoc* deve satisfazer, são eles [6]:

- Operação distribuída;
- o algoritmo de roteamento deve evitar a formação de *loops* de roteamento. Soluções do tipo *TTL (time-to-live)* devem ser evitadas, pois abordagens mais estruturadas podem levar a um desempenho melhor;
- uma rota deve ser criada somente quando um nó fonte deseja transmitir uma mensagem. Economiza-se em banda passante e energia, porém,o tempo gasto de latência é maior;
- operações com algorítmos pró-ativos, em algumas ocasiões, são aceitáveis se comparadas ao tempo de latência dos algorítmos sob demanda ;
- é necessária a existência de técnicas de segurança, não só na camada de rede como também na de enlace, proporcionando assim, algum tipo de segurança já que os algorítmos de roteamento são vulneráveis a diversos tipos de ataque;
- o protocolo deve se adaptar a longos períodos de inatividade , mesmo que estes não sejam anunciados e;

- suporte a enlaces unidirecionais: Normalmente assume-se que um enlace é bidirecional, e vários algorítmos não funcionam quando geram enlaces unidirecionais.

3-Protocolos de Roteamento

Em uma rede *ad hoc* todo o processo de transmissão de dados é feito em cima dos protocolos de roteamento, como visto no capítulo anterior, são eles os responsáveis por transmitir, rotear e responder caso afirmativamente ou não a chegada do pacote de dados ao seu destino. Se estes algorítmos são os responsáveis por todas essas tarefas, é sobre eles que se concentram o ataque de intrusos.

A maioria destes algorítmos utiliza o roteamento pela fonte dinâmico (*Source Routing*), e entender como ocorre este processo é o primeiro passo para desvendar como funciona a maioria dos algorítmos utilizados em uma rede *ad hoc.*

3.1-Roteamento pela Fonte Dinâmico

Este conceito de roteamento não é só utilizado em redes sem fio, mas também em redes com fio, mais especificamente em transmissões *multicast* [5].

O protocolo de roteamento pela fonte dinâmico tem como principal característica o pré- estabelecimento de uma rota por onde o pacote de dados deve passar para chegar ao seu destino, contrariando uma forma usual que é à medida que um pacote de dados trafega na rede é que se determina o caminho a se seguir até chegar ao seu destino.

[5] Multicast- *Multicast,é* uma tecnologia que permite enviar pacotes (pequenas unidades de informação em rede) para um determinado grupo de máquinas simultaneamente, de forma eficiente. A informação é enviada de forma semelhante ao broadcast, mas somente os computadores que realmente desejam receber a informação, irão recebê-la. Para isso eles se "inscrevem" em grupos, e a informação somente será passada de roteador (máquinas que conectam as várias redes formando a Internet global).

Neste tipo de roteamento as rotas são descobertas dinamicamente, ou seja, é armazenado em uma memória chamada *cache* de rotas, rotas aprendidas recentemente são mantidas na memória por algum tempo, o que depende muito da mobilidade da rede.

Em um algoritmo de descoberta dinâmica quando a descoberta de uma rota se faz necessária, devido ao constante movimento da rede e, a rota contida em *cache* não é mais válida ou a rota não existe armazenada na memória, significa que existe um meio de descobrir. Este processo de descobrimento de rotas será detalhado na seção 3.3.

Um protocolo de roteamento pela fonte dinâmico tem como principal característica à economia de bateria dos nós móveis, já que este constitui um fator fundamental para o funcionamento de uma rede *ad hoc.* Também podemos citar a economia de banda passante, que é de primordial importância a este tipo de processo, já que não se faz necessário à atualização constante da memória *cache*.

Já que neste tipo de protocolo não existe atualização constante da memória *cache,* um processo de verificação de rotas se faz necessário, este processo é denominado de procedimento de manutenção de rotas e é descrito na seção 3.2.

3.2- Processo de Manutenção de Rotas

Em um protocolo de roteamento pela fonte dinâmico, para se transmitir uma mensagem, primeiramente será consultado a memória *cache* para verificar se há uma rota disponível para o nó de destino e se está rota é válida ou ainda está disponível no instante da requisição. Caso a rota exista, o nó envia uma requisição de reconhecimento para o próximo nó da lista e fica aguardando um reconhecimento do registro da rota por parte dos nós que a compõem.

Se num enlace qualquer da rota a requisição de reconhecimento é impossibilitada de prosseguir até o nó de destino, o nó onde ocorreu à falha, então, envia um pacote de

erro de rota de volta ao nó fonte. Visto que a conexão com o nó de destino falhou, com a rota pré-estabelecida pela memória *cache*, o emissor atualiza o seu *cache* de rotas descartando, parcialmente, a rota utilizada até então. Este descarte é feito a partir do nó que foi identificado o erro ou não conseguiu fazer a conexão com o próximo nó. As *Figuras 4, Figura 5 e Figura 6* ilustram este processo.

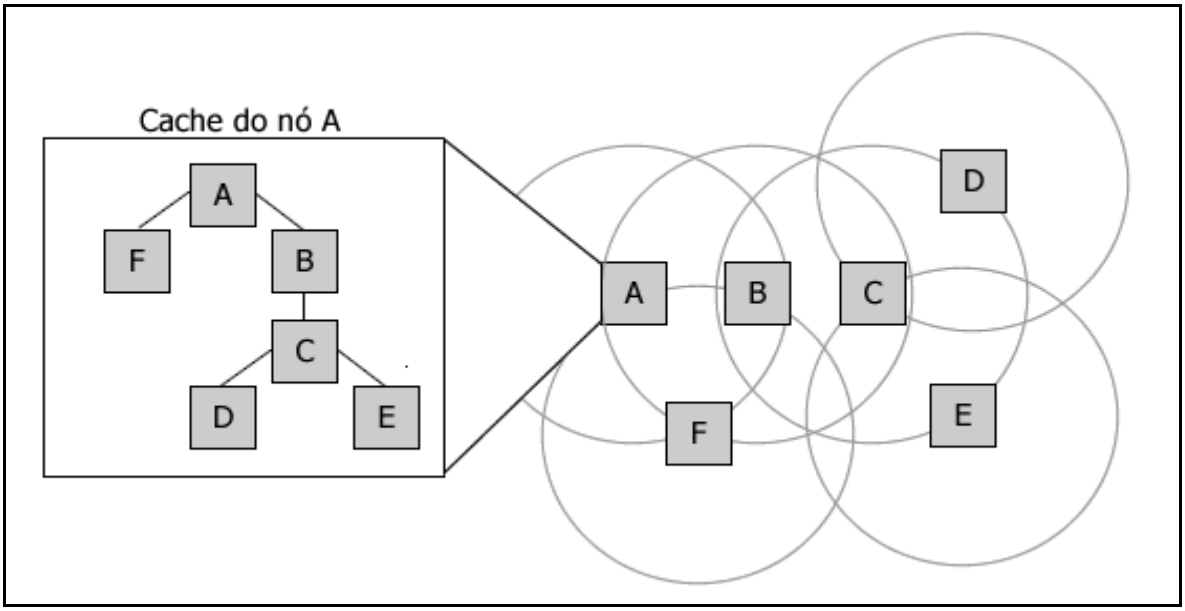

Figura 4- Cache* de memória de *A

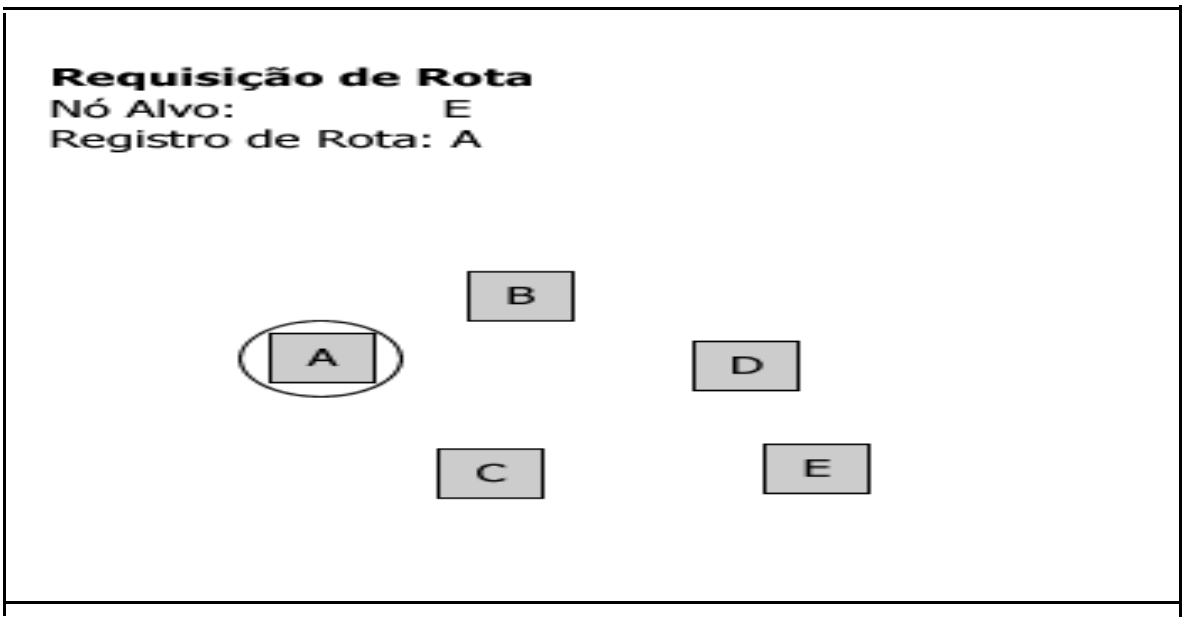

Figura 5*- Nó alvo *E

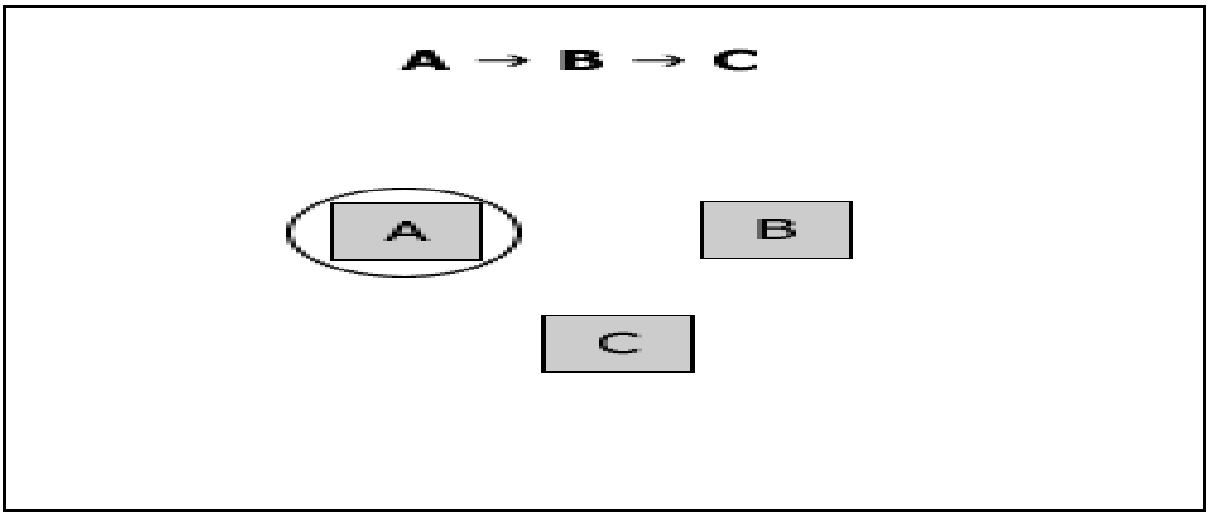

***Figura 6*- Erro de transmissão (redução de rota em *C*)**

Quando um erro, como o descrito anteriormente, ocorre à primeira coisa que o nó que detectou o erro faz é verificar se existe alguma rota para o emissor guardada em *cache*. Segundo Laufer [2], existindo essa rota, ela é preferida e é usada, caso contrário podem ser tomadas as medidas a seguir:

O nó que detectou o erro utiliza a própria rota que o pacote usou para alcançá-lo, porém invertida.

O pacote de erro é armazenado em *buffer* e é iniciado um processo de descobrimento de rota para o emissor, descrito na seção 3.3, e assim que ele é completado, o pacote é enviado.

Quando um nó transmite um pacote de dados, em alguns casos, todo o processo de reconhecimento é feito através da camada de enlace, diz-se então que o reconhecimento do pacote é dependente do enlace, pois é ela a responsável pelo reconhecimento nó a nó do pacote de dados. Quando há um erro no reconhecimento do pacote, o enlace é desfeito, e então uma mensagem é enviada como descrito anteriormente.

3.3- Descobrimento de Rotas

Quando um caminho não está contido na memória *cache* ou a rota se tornou inválida por um motivo qualquer, um novo processo é ativado para se descobrir um caminho que leve a mensagem do nó fonte até o nó de destino, este processo é denominado de descobrimento de rotas. Este processo permite que se descubra um caminho para outro nó qualquer de uma rede *ad hoc*.

O princípio de funcionamento deste tipo de processo é simples e será descrito a seguir.

Para se estabelecer à comunicação com um outro nó, o nó fonte, envia através de difusão um pacote de requisição de rota. Neste pacote está contido o endereço do nó que se deseja enviar o pacote, ou seja, o nó alvo. Neste pacote existe um campo denominado registro de rota, e é nele que se grava toda a rota a ser percorrida pelo pacote de dados até chegar ao nó alvo. Como o envio da mensagem é feito em difusão, os vizinhos que estão ao alcance do nó fonte recebem o pacote de requisição de rota e

anexam o seu endereços a requisição que é retransmitida da mesma forma. A Figura 7 ilustra este processo.

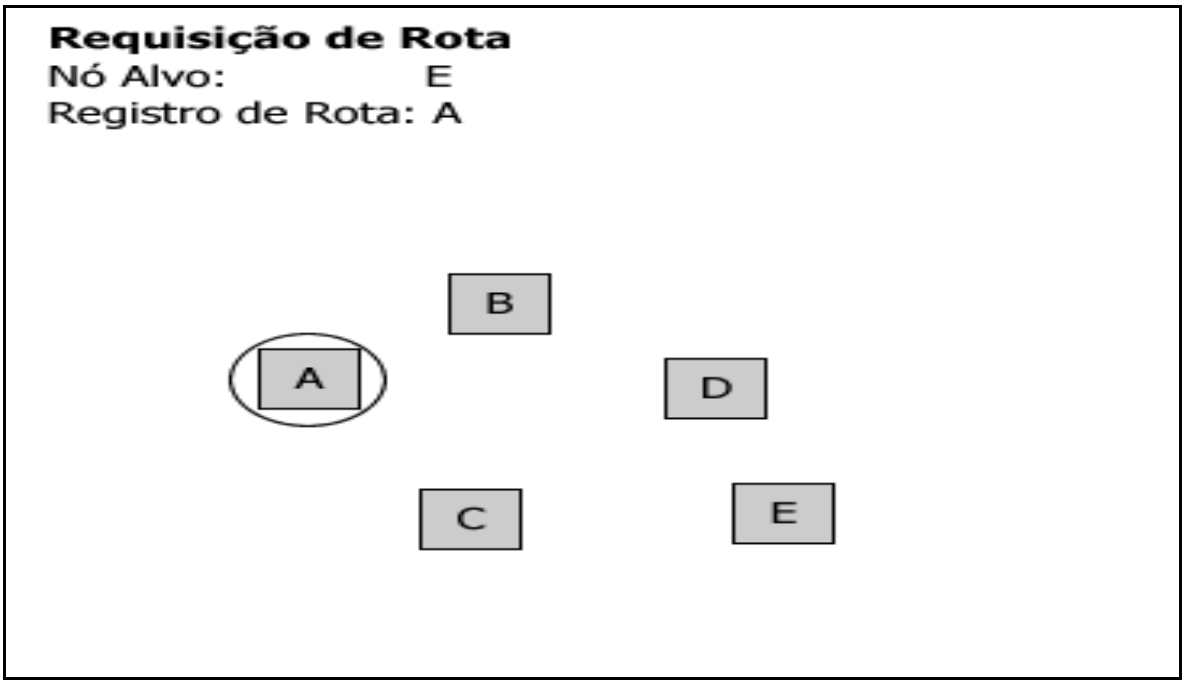

***Figura7*-Envio por difusão de uma requisição de rotas**

Quando um mesmo nó recebe um pacote que já foi processado por ele, e o nó verifica isso através de um campo denominado identificador de rotas, ele é descartado, terminando assim, o seu papel no processo.

Para se evitar que um nó não processe o mesmo pacote repetidas vezes, gerando assim *loops* que prejudicam o desempenho da rede, a requisição de rotas contém um campo chamado de identificador de rota. A função deste campo é detectar pacotes duplicados ou que seguiram rotas diferentes na mesma rede. Sua função é usada junto com o endereço do inicializador do processo.

Quando o nó alvo é atingido, ele mesmo tem a obrigação de enviar a resposta de rota e consiste em fazer caminho para o nó fonte, agora contida no registro de rotas.

Este processo recebe o nome de caminho inverso, visto que o caminho percorrido é o inverso daquele contido na requisição de rotas.

Pode parecer simples o processo de recebimento de pacotes de requisição, mas na verdade é muito mais complexo que imaginamos. A seguir, é apresentado o funcionamento deste algorítmo, mostrando a sua complexidade porém tentando minimizar o esforço para seu entendimento.

Quando um pacote de requisição é recebido por um nó, primeiramente ele verifica o par, o endereço e identificador. Em um processo análogo ao do *cache* de memória de rotas, o pacote de requisição de rotas é comparado com uma lista de rotas contidas em memória. Se um par, idêntico ao contido na requisição de rotas até então, for detectado o pacote é descartado, prevenindo assim a ocorrência de *loops* intermináveis na rede, caso contrário o próximo passo é seguido.

Se o nó atual for o alvo da mensagem então, faz-se necessário enviar uma mensagem de resposta para o nó fonte. Para isso, primeiramente é verificado, na memória *cache*,se há uma rota para atingir o alvo. Caso está rota esteja na memória ela então é utilizada, se não é invertida a rota descrita no registro de rotas. Fica claro observarmos aqui que para isso funcionar é necessário que o enlace entre essas rotas funcione bem nos dois sentidos da transmissão.

Em último caso o nó retransmite a requisição de rota anexando o seu endereço ao identificador de rotas.

3.4-Roteamento por Vetor de Distância

O termo roteamento por vetor de distância (*Distance Vector Routing)* é também encontrado como roteamento por distância vetorial ou *Bellman-Ford algorithm*, este último devido ao algorítmo de *Bellman-Ford* ser usado para calcular os caminhos mínimos para o roteamento [11].

O funcionamento de um algorítmo de vetor de distância é bastante simples, ele mantém um vetor responsável em informar a menor distância conhecida entre um nó fonte e um nó de destino, bem como o próximo roteador na rota mínima para o nó de destino. Este caminho pode estar relacionado com diversas medidas, a mais utilizada é a *hop count*, que utiliza como base o número de roteadores na rota mais utilizada.

Neste tipo de medida, inicialmente, os valores de cada tabela são calculados por cada um dos vetores, sem levar em consideração a existência de outras rotas. Em um segundo passo, os roteadores levam em conta, as informações trocadas entre si a fim de se atualizar os caminhos mínimos.

Apesar da simplicidade de um algorítmo de *Bellman-Ford*, sua principal desvantagem é que ele pode se tornar lento em redes de grande porte.

3.5-Roteamento por Estado de Enlace

Algorítmos de estado de enlace (*link-state algorithm)* usam base de informações (*link-state database)* replicado em cada nó de uma rede *ad hoc* [11].

Para que esse procedimento funcione, cada roteador cria uma tabela contendo informações de sua conexão com toda a rede, tais como, arcos adjacentes, pesos de cada arco, e roteadores vizinhos. De posse destas informações da rede, é então replicada um quadro para cada nó da rede, possibilitando assim, o cálculo do menor caminho entre um nó fonte e um nó de destino.

Para se determinar o custo de cada rota é feito à soma dos custos de cada arco em seu caminho, deste modo pode-se determinar o caminho mínimo entre um nó e outro. Os algorítmos mais utilizados para se calcular o menor caminho são os algorítmos de *Dijkstra* e o algorítmo de *Bellman-Ford* [11].

O que acontece, na realidade, para calcular o caminho mínimo entre cada nó da rede, é calcular para cada destino a árvore de caminhos mínimos de cada roteador. Todo esse processo funciona da seguinte maneira, segundo Luciana Buriol [11]:

Para cada rede composta por $|V|$ roteadores e $|E|$ arcos, supondo que cada roteador seja destino de fluxo, são calculados $|V|$ grafos de caminho mínimos. Os grafos de caminhos mínimos usados para o roteamento são caracterizados por possuírem arcos direcionados e por terem como raiz não o nó fonte e sim o nó de destino.

Uma das principais características deste tipo de algorítmo é que uma arvore não é exclusiva, ela pode possuir múltiplos caminhos.

Existem vários tipos de algorítmos de vetores de estado de enlace, no entanto, a maioria se diferencia na forma de como constrói e usa seu vetor de caminhos mínimos. O custo de cada arco depende de que protocolo está sendo utilizado, em geral, atribui-se um valor para cada arco, seguindo uma métrica que pode ser através da distância, custo da comunicação, tráfego médio do nó na rede, largura da banda, comprimento médio da fila e retardo detectado. O valor de cada arco pode ser agregado a mais de um valor de medida.

Não se pode precisar qual dos dois algorítmos, por vetor de distância ou estado de enlace é o mais eficiente, pois o desempenho dos dois pode variar de acordo com a topologia e as condições de tráfego de cada rede, no entanto, os algorítmos de vetores de estado de enlace tem um melhor desempenho devido às atualizações mais rápidas dos caminhos mínimos quando a topologia da rede muda, e o conhecimento da rede em geral, por cada um dos nós, possibilitam maior flexibilidade no uso desta informação.

4-Segurança em Redes Ad Hoc

Como visto na seção 3, são os protocolos de roteamento os principais responsáveis por estabelecer a comunicação entre dois ou mais nós de uma rede *ad hoc*, e os principais tipos de ataques e falhas de segurança concentram-se sobre eles.

Em uma rede *ad hoc,* devido a sua própria natureza já faz dela uma rede insegura e diferente de qualquer outro tipo de rede conhecida. Cada nó de uma rede *ad hoc* contribui, em sua plena capacidade e independência, para o bom funcionamento da rede, a qual este faz parte. É de vital importância para toda a rede que não haja "agentes maliciosos" implantados na rede ou até mesmo de nós que estejam contaminados [13].

Em sua grande maioria, os protocolos de roteamento foram idealizados em cenários onde não havia a necessidade da utilização de mecanismos que implementassem métodos para impedir a ação de "agentes maliciosos", no entanto, com o crescente aumento das diversas formas de aplicação deste tipo de tecnologia, faz-se necessário à inclusão de medidas que empeçam a ação de agentes mal intencionados.

Ao ser analisado como são feitos estes ataques, deve-se primeiramente ser estabelecidos os objetivos de segurança que uma rede, principalmente a rede *ad hoc,* deve atender, analisados na seção 4.1.

Na seção 4.2 será descrito de que forma e como são feitos estes ataques a uma rede deste porte e o que podemos fazer para que se possa, não evitar, como também minimizar os prejuízos causados pela ação de nós maliciosos.

4.1- Objetivos de Segurança

Na maioria das redes, seja ela uma rede cabeada ou uma rede *wireless*, são considerados alguns critérios para que se possa avaliar com exatidão a segurança da comunicação, mesmo não levando em conta o tipo de serviço prestado por esta rede. Tais serviços se fazem necessários, pois os protocolos não ficam apenas capacitados em estabelecer a comunicação entre dois ou mais nós. Podem-se enumerar estes critérios e discuti-los da seguinte maneira, como visto em ROCHA E DUARTE [14]

1. **Disponibilidade:** Podemos descrever este meio como a sobrevivência de uma rede sobre o ataque de um nó malicioso, seja ela de qualquer natureza ou a qualquer parte da camada de transmissão de pacotes de dados;

2. **Confidêncialidade:** Todo tipo de rede deve assegurar que uma determinada informação não venha a cair em mãos erradas, ou seja, que uma mensagem não seja violada pela ação de terceiros;

3. **Integridade:** Todo o sistema de comunicação deve garantir que nenhum pacote ou parte da informação, seja perdida na transferência dos dados a não ser por falhas na transmissão de rádio, nunca pela ação de nós maliciosos na rede;

4. **Autenticação:** Este requisito é de vital importância em uma rede *ad hoc,* pois, deve possibilitar a identificação por parte de cada nó, de seus pares de comunicação, evitando assim, o mascaramento e a personificação por parte de nós com outros intuitos;

5. **Não-repúdio:** No caso específico, o de uma rede *ad hoc*, confere a cada nó, identificar a origem de uma mensagem, o que pode a vir a ser muito útil, pois podemos através deste dispositivo detectar nós maliciosos na rede.

Como visto anteriormente todo o sistema de segurança, em qualquer tipo de rede, deve atender a estes requisitos de forma eficiente e eficaz. Já em redes *ad hoc* a

implantação deste tipo de mecanismo, não só é dispendiosa como também de difícil, devido a fatores que restringem componentes de *hardware* e de *software* fica inviável atender a todos estes requisitos ao mesmo tempo, ou que eles cumpram o seu papel com a mesma eficiência com que é feito nos demais tipos de rede, já que nestes outros tipos o que as tornam tão eficientes é a junção de dispositivos de segurança nas áreas de *software* e *hardware*.

4.2- Tipos de Ataque

Como visto na seção 4.1, para se proteger uma rede, não basta usarmos só dispositivos de *hardware* ou de *software* separadamente, por isso uma rede *ad hoc* pode ser tão vulnerável perante ataques externos.

Há várias formas de ataques em uma rede *ad hoc,* na sua grande maioria eles visam impedir que informações cheguem ao seu destino, ou obter informações sigilosas na rede. Pode-se classificá-los da seguinte forma: de acordo com a região e como atacam, ativos e passivos ou internos e externos.

Na sua grande maioria o objetivo principal de um ataque há uma rede é a obtenção de informações sigilosas, mas em uma rede *ad hoc* estes ataques podem também impossibilitar a ação de um nó, incapacitando-o de transmitir ou retransmitir informações dentro da rede, gerando assim, falhas de transmissão ou até mesmo fazendo com que este nó se torne um “espião” dentro da própria rede a que ele faz parte, comprometendo a eficiência de toda a rede.

Podemos destacar, que para uma rede *ad hoc*, o principal tipo de ataque seja o ativo interno, já que neste tipo de ataque o nó, que faz parte da rede, se beneficia disto e ataca os outros nós, por isso este tipo de ataque recebe também o nome de protegido. Podendo vários nós como estes atuar em grupos. O menos importante, mas

também perigoso, é a interceptação das ondas de rádio por onde são enviadas as mensagens, mas mesmo assim não podem ser deixados de lado [13].

4.2.1- Ataques de alteração em campo de tabela

Neste tipo de ataque o nó malicioso altera a composição de campos na tabela de transmissão de dados, mais precisamente no campo D*estinaition Sequence Numbers*, impossibilitando assim que informações cheguem ao seu destino, ou até mesmo se fazendo passar pelo destinatário da mensagem.

Estes ataques são feitos principalmente em protocolos de roteamento em que se faz uso da descoberta de rotas *RREQ (Request Routing)*, onde os nós que desejam transmitir uma mensagem são obrigados a encontrar uma rota através de uma *RREQ.*

A Figura 8 demonstra como é feita uma *RREQ (Request Routing)* e como um nó I pode se apoderar deste tipo de requisição e replicar a mensagem, fazendo com que ele passe a ser o destinatário da mensagem que A vai enviar para D, ou que toda a informação da rede passe por ele antes de chegar ao seu destino.

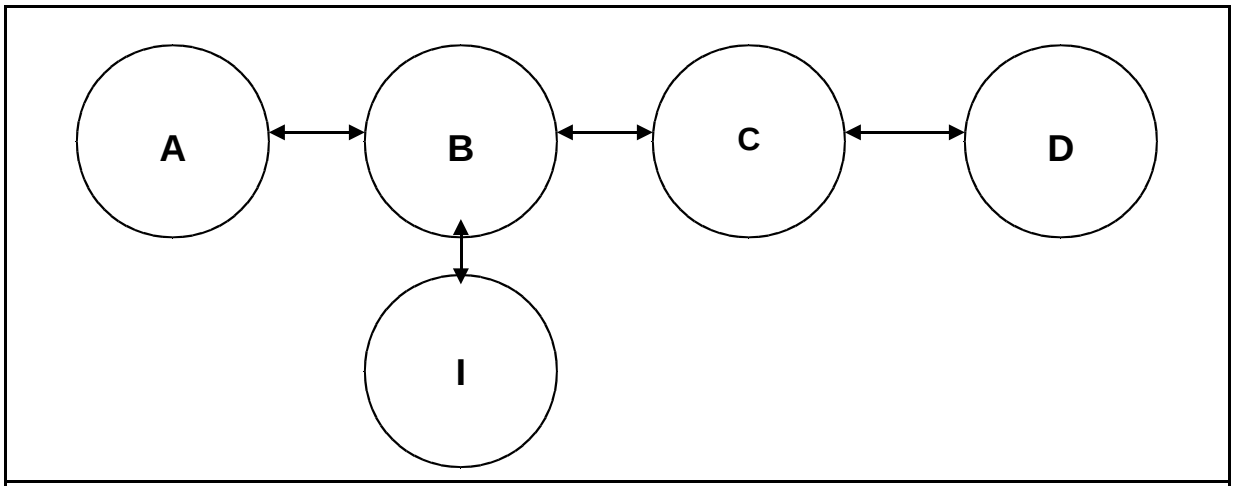

***Figura 8*- Exemplo de alteração em campo de tabela**

4.2.2-Ataques multihop

Vimos no capitulo 2 que alguns algorítmos utilizam-se do processo de *multihop* para se comunicarem com outros nós da rede, no entanto, este mesmo processo é utilizado para se alterar o numero de saltos dados por um pacote de dados dentro da rede, este processo denomina-se *spoofing*[6].

Agindo desta maneira o nó malicioso pode colocar-se na lista por onde a mensagem vai passar, obrigando que todo o tráfego passe por ele.

Na Figura 9, podemos ver como este processo funciona, *A* tenta enviar uma mensagem para *D*, *I* desenvolve um processo de *spoofing* na rede e passa a receber as mensagens destinadas a D.

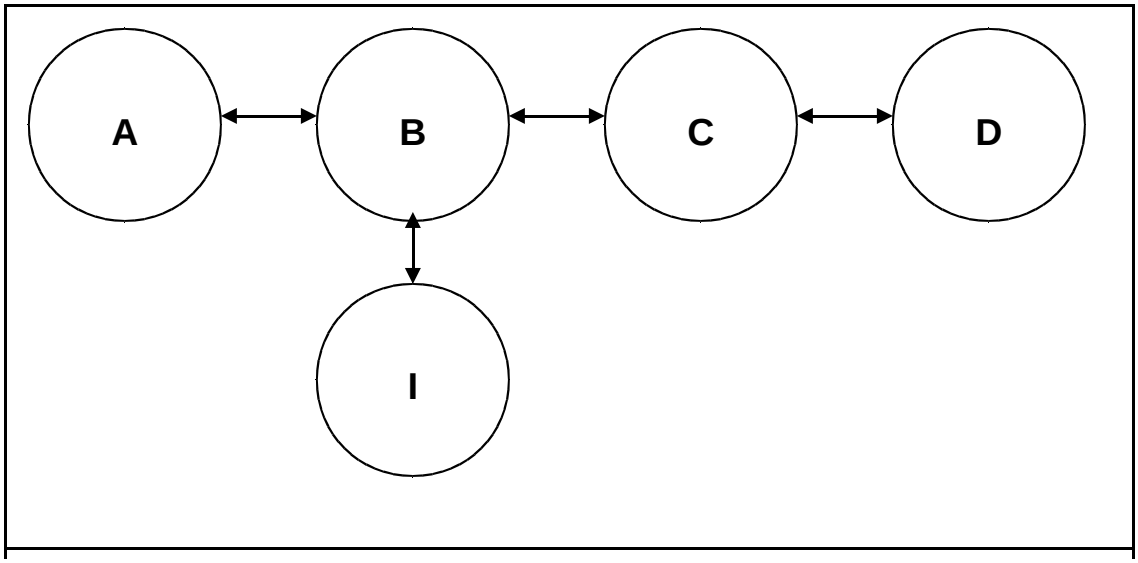

Figura 9* – Exemplo de ataque *multihop.

[6] Spoofing- Diminuição no numero de saltos de um processo *multihop*

4.2.3- Ataques de Negação de Serviço(DoS- Denial of Service)

Como visto no capítulo 3, alguns algorítmos implementam mecanismos para manter suas tabelas de rotas atualizadas [13].

A maioria dos ataques de negação de serviço ocorre quando o mecanismo de atualização de tabelas é acionado, ou quando algum nó da rede deseja transmitir uma mensagem.

Este tipo de ataque ocorre quando um nó malicioso impede que uma mensagem chegue ao seu nó de destino, mesmo sendo possível o enlace entre eles, ignorando a presença do próximo nó da rede, gerando assim, uma mensagem de erro que retorna ao nó de origem por uma rota estabelecida até então.

A “quebra“ do link, efetuada pelo nó malicioso, pode causar inúmeras lacunas nas tabelas de atualização de rotas ou fazendo com que o tempo de envio de uma mensagem seja muito grande, prejudicando o desempenho da rede.

4.2.4- Envenenamento de Tabelas de Rotas

Alguns protocolos, como o *Dynamic Source Routing*, tentam aprender novas rotas observando os pacotes que trafegam na rede [13].

Geralmente este aprendizado é feito de forma promiscua, e quando uma destas rotas contém um nó inexistente na rede, o nó é acrescentado a rotas já existentes na memória de rotas, causando um envenenamento das rotas já existentes em *cache* [15].

Quando uma mensagem esta para ser enviada, o primeiro lugar que um algorítmo, do tipo *DSR* (*Dynamic Source Routing*) procura uma rota que leve ao nó de destino é em seu *cache* de rotas. Caso encontre, uma rota em uma de suas tabelas e esta esteja

envenenada a mensagem não chegará ao nó de destino, ou dependendo do caso demorará a chegar ao se destino.

4.3- Medidas de Segurança

Para que possamos estabelecer níveis de segurança mais confiáveis aos protocolos de roteamento de uma rede *ad hoc,* algumas medidas devem ser tomadas no sentido de impedir que nós maliciosos sejam impossibilitados de acessar e/ou interromper o envio de pacotes na rede.

Tais medidas devem ser cuidadosamente implantadas, para não prejudicarem o desempenho da rede. A seguir descreveremos algumas medidas já utilizadas hoje, que não prejudicam o desempenho de uma rede *ad hoc.*

4.3.1-Proteção Física

Quando pensamos em proteger uma rede convencional, logo pensamos em aliar um *software* e um dispositivo de *hardware*. Em redes *ad hoc* esta implantação, principalmente de um dispositivo de *hardware* é muito mais dispendiosa, já que podemos imaginar a captura destes dispositivos de acordo com o fim estabelecido pelo tipo de rede.

Uma solução paliativa, mas não totalmente segura, é a implantação de *smart cards*, como cartões *SIM* [7]de *cards GSM*[8], Seja uma forma de utilizar o dispositivo móvel apenas como interface e centralizar as informações em si.

4.3.2- Proteção de Enlace

Como toda a comunicação é feita pelo ar, uma estratégia de transação de informações adequada deve ser empregada para evitar que um *jamming* ou *eavesdropping* [9] seja feito [14].

Dar uma solução que seja viável para estes problemas, é indiscutivelmente difícil, já que isso dependerá, não só do tipo de dispositivo a ser usado como também em que área ele será implementado. No entanto, a solução mais freqüentemente usada é o espalhamento por salto de freqüência (FHSS) , já que esta técnica permite dividir a banda disponível em vários subcanais, que são selecionados para utilização de forma aleatória.

---

[7] SIM- O SIM é o cartão que controla a interface do dispositivo GSM, realizando um intercâmbio interativo entre uma aplicação de conexão e o usuário final e atenda ao controle de acesso da conexão. Graças a ele, por primeira vez o cartão SIM tem um papel eminentemente ativo no dispositivo, já que o SIM inicia os comandos independentemente do dispositivo e da conexão.

[8] GSM- A sigla GSM vem do inglês Global System for Mobile Communications (ou Global Standard Mobile), que quer dizer "Sistema Global para Comunicações Móveis". O GSM é um sistema de celular digital baseado em divisão de tempo, como o TDMA, e é considerado a evolução deste sistema, pois permite, entre outras coisas, a troca dos dados do usuário entre telefones através do Sim-Card e acesso mais rápido a seviços WAP e Internet, através do sistema GPRS.

[9] "jamming ou eavesdropping" - um ruído igual a uma buzina intermitente destinada a deliberadamente interferir em transmissões "indesejadas"

4.3.3-Criptografia

O meio mais comum utilizado, hoje em dia, para se proteger os dados que trafegam por uma rede, seja de qual tipo for, é a criptografia. No entanto, a sua implantação em redes *ad hoc* deve seguir parâmetros próprios que caracterizam este tipo de ambiente. Vale lembrar dos objetivos de segurança das redes *ad hoc,* tratados anteriormente, na seção 4.1.

Um esquema de segurança baseia-se em chaves assimétricas para se desenvolver uma comunicação segura entre os nós de uma rede *ad hoc*. Entretanto, este esquema de chaves assimétricas, ao ser implantado em uma rede *ad hoc*, deve levar em conta características essenciais, tais como as apresentadas a seguir, e também discutidas por Rocha e Duarte [14]:

- As propriedades de autoridade de uma rede *ad hoc*;
- Acessibilidade de um nó em relação à rede;
- Comportamento da fase de inicialização do esquema;
- O tipo de relação entre os nós;
- E entre os nós e a autoridade da rede;
- A distribuição de confiança na rede.

À parte do problema que abrange a inicialização do sistema de segurança (*boolstrap*), fica difícil de ser explicada tal a sua complexidade, com relação às outras características, as propostas mais recentes baseiam-se em dois princípios que tendem a cobri-las bem, sendo eles: redundância na topologia da rede e distribuição de confiança [14].

Para tais cenários são empregados esquemas de criptografia tais como, assinaturas digitais com infra-estrutura de chave pública e uma estrutura denominada

de autoridade de certificação. Tal entidade responde pela associação entre os nós da rede e suas chaves públicas. Enquanto um nó detém sua chave privada, a sua chave pública é anunciada para toda a rede. O que difere este método em uma rede *ad hoc* é a responsabilidade de cada nó diante da distribuição do gerenciamento desta chave perante toda a rede [14].

A forma mais usual de se proteger uma rede *ad hoc,* utilizando criptografia, é utilizando o protocolo *WEP (Wired Equivalent Privacy),* que é um padrão desenvolvido juntamente com o padrão IEEE 802.11, que utiliza uma chave baseada no algorítmo RC4 para criptografia dos pacotes que trafegam no ar, além do CRC32, que possibilita ao receptor detectar se a mensagem esta corrompida.

5- Considerações Finais

Estabelecer parâmetros que possam nos dar uma visão de como é o funcionamento de uma rede *ad hoc,* procurando estabelecer diferenças básicas entre uma rede *ad hoc* e uma rede sem fio convencional e como esta se porta em aspectos tão importantes como a transmissão e retransmissão de pacotes de dados, é um passo primordial para o entendimento e aplicação dos fundamentos de uma rede *ad hoc,* nos possibilitando, não só entendermos como um pacote de dados é transmitido através da rede, como também nos abrir caminhos, até então , inexplorados e que se diversificam de acordo com os rumos deliberados pelo autor.

O principal desafio de um protocolo de roteamento não é enviar um pacote de dados do emissor ao destinatário da mensagem dentro da rede, e sim, gerenciar recursos escassos como energia, banda passante, além de estabelecer parâmetros de segurança para a transmissão de dados dentro da rede e localizar o nó de destino na rede.

Este último talvez seja o requisito mais importante, já que como visto anteriormente, é fácil induzirmos alguns nós da rede ao erro, mesmo diante há novas técnicas de segurança.

Diante dos argumentos apresentados neste trabalho, fica em aberto diversas questões que podem ser exploradas em trabalhos futuros,tais como: na área de segurança dos protocolos de roteamento, aplicações avançadas sobre os protocolos, principalmente o mais usado o roteamento pela fonte dinâmico, tais como simulações entre este e outros tipos de protocolos.

Podemos, enfim, concluir que a implantação de uma rede *ad hoc* em grande escala, principalmente depois de solucionados problemas descritos durante todo este trabalho, nos trará inúmeros benefícios, principalmente na área de comércio e prestação de serviço.

Bibliografia

[1] TANEMBAUM, Andrew S. Redes de Computadores. Tradução da terceira edição. 8° tiragem Editora Campus.

[2] LAUFER, Rafael P. Roteamento pela Fonte em Redes *Ad Hoc.* Departamento de Eletrônica /EE Universidade Federal do Rio de Janeiro- UFRJ .Disponível em: < **www.gta.ufrj.br** >
Acesso em: 19/04/2004
[3] JUNIOR,Aurélio Amodei; DUARTE, Otto Carlos M. B. . COOPPE/EE – Programa de Engenharia Elétrica Universidade Federal do Rio de Janeiro. Disponível em: < **www.gta.ufrj.br/seminarios/CPE825/tutorial** >
Acesso em: 19/04/2004

[4] JÚNUOR, Smith Tupinambá D'Oliveira. Análise de Tráfego de Dados em Redes Bluetooth. Universidade Federal de Pernambuco. Disponível em: **<www.cin.ufpe.br/~tg/2001-1/stj.doc> .** Acesso em:19/09/2004

[5] CARVALHO,Teresa Cristina Carvalho. Diretora do Laboratório de Arquitetura e Redes de Computadores da USP- Universidade do Estado de São Paulo. Disponível em: **<www.itweb.com.br/colunistas/artigo.asp> .** Acesso em:19/09/2004.

[6] PINHEIRO, **José Maurício Santos. Disponível em: <**http://www.projetoderedes.com.br/artigos/artigo_redes_moveis_ad_hoc.php**>** Acesso em: 13/04/2005.

[7] Anatel. Disponível em: **<www.anatel.gov.br/difusao/OM>** . Acesso em: 13/04/05.

[8] Anatel. Disponível em: **<www.anatel.gov.br/difusao/OT>** . Acesso em: 13/04/05.

[9] Anatel. Disponível em: **www.anatel.gov.br/ difusao/ OC >.** Acesso em: 13/04/05.

[10]Pinheiro, José Mauricio dos Santos**.** Disponível em: **<http://www.projetoderedes.com.br/artigos/artigo_vulnerabilidades_em_redes_wireless.php>.** Acesso em 27/03/2005

[11] Buriol, Luciana Salete. Tese apresenta a Faculdade Engenharia Elétrica e de Computação da Universidade Estadual de Campinas. Disponível em: **<www.densis.fee.unicamp.br/~buriol/tese/tese-buriol.pdf>** . Acesso em: 08/05/2005

[12] IEEE. Disponível em: **<www.iee.com>** . Acesso em 04/05/2005

[13] Albuquerque, Luciano Renovato de. Tese apresentada ao Instituto Alberto Luiz Coimbra de Pós-Graduação e Pesquisa de Engenharia da Universidade Federal do Rio de Janeiro. Disponível em: **<www.lockabit.coppe.ufrj.br/downloads/ academicos/seguranca_redes_adhoc.pdf>** -Acesso em: 05/06/2005

[14] Rocha, Luiz Gustavo S; Duarte, Otto C. M. B. .Grupo de Teleinformática e Automação COPPE/ POL –PEE/ DEL., Universidade Federal do Rio de Janeiro- UFRJ. Disponível em**: <www.gta.ufrj.br/r> .** Acesso em: 05/06/05

[15] Praticas de Segurança para Administradores de Redes de Internet. NIC BR Segurit Office Versão 1.1.1 Copyright 24 setembro de 2002 NBSO. Disponível em: **<www.nic.br/docs/seg_adm_redes/old/seg_adm_redes_1.1.1.pdf> .** Acesso em: 08/07/2005