UNIVERSIDADE FEDERAL DE SANTA CATARINA
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA
CURSO DE SISTEMAS DE INFORMAÇÃO

Um Estudo sobre Protocolos de Autoconfiguração de Endereços para Redes Móveis Ad-Hoc

Alex Schneider Zis

Florianópolis – SC
2006/2

UNIVERSIDADE FEDERAL DE SANTA CATARINA
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA
CURSO DE SISTEMAS DE INFORMAÇÃO

Um Estudo sobre Protocolos de Autoconfiguração de Endereços para Redes Móveis Ad-Hoc

Alex Schneider Zis

Trabalho de conclusão de curso
apresentado como parte dos
requisitos para obtenção do grau
de Bacharel em Sistemas de Informação

Florianópolis – SC
2006/2

Alex Schneider Zis

Um Estudo sobre Protocolos de Autoconfiguração de Endereços para Redes Móveis Ad-Hoc

Trabalho de conclusão de curso apresentado como parte dos requisitos para obtenção do grau de Bacharel em Sistemas de Informação

Orientador

_____
Prof. Mário Antônio Ribeiro Dantas, Phd
Universidade Federal de Santa Catarina

Banca Examinadora

_____
Prof. João Bosco Mangueira Sobral, Dr.
Universidade Federal de Santa Catarina

_____
Prof. Vitório Bruno Mazzola, Dr.
Universidade Federal de Santa Catarina

Agradecimentos

Agradeço, em primeiro lugar, aos meus familiares, que apesar da distância sempre me deram apoio, incentivo e carinho durante estes longos anos de estudo na Universidade.

Ao meu orientador Prof. Mario Dantas, pelo auxílio, dedicação, motivação e amizade desde a definição do tema do projeto até a conclusão deste trabalho.

Aos amigos, que sempre estiveram ao meu lado, tanto nas horas de estudo bem como nos momentos de diversão, durante todos esses anos de faculdade, desde os tempos da Computação.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ACRÔNIMOS

AC - Autoridade Certificadora

ACD - Autoridade Certificadora Distribuída

AODV - *Ad Hoc On Demand Distance Vector*

ARAN - *Authenticated Routing for Ad hoc Networks*

AREP - *Address Reply*

AREQ - *Address Request*

ARP - *Address Resolution Protocol*

BOOTP - *Bootstrap Protocol*

DAD - *Duplicate Address Detection*

DCDP - *Dynamic Configuration Distribution Protocol*

DHCP - *Dynamic Host Configuration Protocol*

DNS - *Domain Name System*

DoS - *Deny of Service*

DSDV - *Destination Sequenced Distance Vector*

DSR - *Dynamic Source Routing*

GloMo - *Global Mobile Information Systems*

IARP - *Intrazone Routing Protocol*

IERP - *Interzone Routing Protocol*

IETF - *Internet Engineering Task Force*

IP - *Internet Protocol*

IPSec - *Internet Protocol Security*

MAC - *Machine Address Code*

MAE - *Manet Authentication Extension*

Manet - *Mobile Ad-Hoc Network*

MPR - *Multipoint Relay*

OLSR - *Optimized Link State Routing*

OSI - *Open Systems Interconnection*

PACMAN - *Passive Autoconfiguration of Mobile Ad hoc Networks*

PDA - *Personal Digital Assistants*

PDAD - *Passive Duplicate Address Detection*

PKIX - *Public-Key Infrastructure X.509*

PRNET - *Packet Radio Network*

QoS - *Quality of Service*

RARP - *Reverse Address Resolution Protocol*

RREP - *Route Reply*

RREQ - *Route Request*

SAODV - *Secure Ad Hoc On Demand Distance Vector*

SDAD - *Strong Duplicate Address Detection*

SEAD - *Secure Efficient Ad hoc Distance vector*

SRP - *Secure Routing Protocol*

SURAN - *Survivable Adaptive Network*

TBRPF - *Topology Dissemination Based on Reverse-Path Forwarding*

TCP - *Transmission Control Protocol*

UDP - *User Datagram Protocol*

US DARPA - *United States Defense Advanced Research Projects Agency*

WDAD - *Weak Duplicate Address Detection*

ZRP - *Zone Routing Protocol*

RESUMO

Nos dias atuais, com o constante avanço da tecnologia, o uso de dispositivos móveis, como *laptops*, *palmtops* e celulares vem tendo um grande crescimento. Com isto, surge a necessidade de troca de informações entre estes dispositivos.

As redes sem fio permitem a comunicação entre estes dispositivos sem nenhum meio físico. Logo, as informações são transmitidas por ondas de rádio. Essa tecnologia está em amplo desenvolvimento a fim de oferecer melhores serviços, visto que os padrões utilizados atualmente possuem diversas limitações.

As redes móveis *Ad-Hoc* são um modo de operação das redes sem fio. Redes *Ad-Hoc* dispensam qualquer tipo de infra-estrutura para a comunicação, ou seja, a comunicação é realizada diretamente entre os dispositivos. Estas redes são altamente dinâmicas, devido a mobilidade dos equipamentos, o que tornam suas características muito peculiares.

O principal objeto de estudo deste trabalho são os protocolos de autoconfiguração para redes *Ad-Hoc*. Estes protocolos distribuem automaticamente os endereços de rede para os dispositivos a fim de estabelecer comunicação entre os mesmos. Mas muitas propostas não tratam da segurança destes protocolos. Logo, tentarei definir aspectos de segurança necessários aos protocolos que atuem neste tipo de ambiente.

Palavras-chave: Ad-Hoc, autoconfiguração, protocolos, redes, segurança

ABSTRACT

Nowadays with the constant advance of technology, the use of mobile devices such as laptops, palmtops and cellular phones are on the increase. So the necessity of information exchange among these devices arises.

The wireless networks permit the communication among these devices without any physical means. Cosequently the information is transmited by radio waves. This technology is in wide development in order to offer better services because the standards used nowadays have several limitations.

Ad-Hoc mobile networks are an operational way of wireless networks. Ad-Hoc networks manage without any kind of infrastructure for communication, that is, the communication is accomplished directly among the devices. These networks are highly dynamic due to equipment mobility, which become their characteristics very peculiar.

The main study object of this work are the autoconfiguration protocols to Ad-Hoc networks. These protocols distribute automatically the networks addresses to the devices in order to establish a communication among them. But many proposals do not deal with the security of these protocols. So, I will try to define security aspects necessary to the protocols act in this type of environment.

Keywords: Ad-Hoc, autoconfiguration, protocolos, networks, security

1 INTRODUÇÃO

Observando o grande crescimento nas áreas de comunicação celular, redes locais sem-fio e serviços via satélite juntamente com o comércio de dispositivos que utilizam tais serviços, estima-se que em poucos anos, dezenas de milhões de pessoas terão um *laptop*, *palmtop* ou algum tipo de PDA (Personal Digital Assistants). Este crescimento permitirá que em um futuro bem próximo, informações e recursos possam ser acessados a qualquer instante e em qualquer lugar. Independente do tipo de dispositivo portátil, a maior parte desses equipamentos deverá ter capacidade de se comunicar com a parte fixa da rede e, possivelmente, com outros computadores móveis. A esse ambiente de computação dá-se o nome de computação móvel

Este tipo de ambiente, onde os usuários móveis podem realizar comunicações sem nenhum meio físico para acessar recursos distribuídos faz parte da linha de pesquisa de redes móveis sem fio. Basicamente, existem dois tipos de redes móveis sem-fio: as redes *Ad-Hoc* e as redes infra-estruturadas. Será abordado nesta pesquisa o tipo de rede *Ad-Hoc*.

A integração de computadores com comunicações e outras formas de tecnologias de informação está criando novas formas de sistemas e serviços de informação distribuída. É o surgimento dos ambientes de computação ubíquos que deverão ser a nova forma de trabalho do próximo século. Este é o cenário altamente desafiador e excitante que motiva a computação móvel. Nesse cenário as redes móveis *Ad-Hoc* terão uma importância cada vez maior.

Neste contexto tecnológico e móvel, em que a Ciência da Computação e as Telecomunicações se relacionam, as redes *Ad-Hoc* ganham força. Entre as

características destas redes que contribuem para tal, destacam-se: são de fácil instalação; por não serem dependentes de uma ou mais torres fixas, tornam-se independentes de erros ocorridos nas mesmas; apresentam maior conectividade, uma vez que a comunicação pode ser direta, ou seja, não é obrigada a passar pela torre fixa; além de seu fator sucesso, a mobilidade.

1.1 Justificativa

Devido a popularização das redes móveis, em especial as redes *Ad-Hoc*, a necessidade de protocolos de autoconfiguração de endereços para que estas ofereçam segurança e qualidade, é imprescindível. Para oferecer qualidade e segurança aos usuários destas redes, os protocolos necessitam prover, por exemplo, unicidade de endereços IP (*Internet Protocol*), minimizar o tráfego de pacotes e assegurar que somente os nodos autorizados e confiáveis devam ser configurados e tenham acesso aos recursos da rede.

No entanto, nem todos os protocolos oferecem uma gama de serviços que ofereçam qualidade e segurança suficientes aos usuários, principalmente no que se refere à questão da segurança.

Portanto, serão definidas métricas para a avaliação dos protocolos de autoconfiguração de endereços para redes *Ad-Hoc*, a fim de avaliar quais as melhores alternativas a serem utilizadas nesse ambiente, levando em consideração diversos fatores que são relacionados com o desempenho dessas redes.

1.2 Objetivos

Estudar a tecnologia *Ad-Hoc*, em conjunto com os seus respectivos protocolos de autoconfiguração e roteamento, com o objetivo de demonstrar efetivamente quais os benefícios e desvantagens que o uso da tecnologia em questão acarreta, levando em consideração suas características que a tornam mais complexas que redes cabeadas.

Demonstrar que o uso de protocolos de autoconfiguração de endereços para redes móveis *Ad-Hoc* pode oferecer qualidade e segurança aos seus usuários, sem a necessidade de estrutura física.

1.3 Problema

Principais problemas encontrados nos protocolos de autoconfiguração e que devem ser analisados para obter a melhor solução:

- Unicidade dos endereços IP
- Perda de mensagens
- Endereçamento multi-hop
- Minimização do tráfego de pacotes adicionais na rede
- Verificação da ocorrência de solicitações concorrentes de endereço IP
- Flexibilidade ao particionamento e a fusão de redes *Ad-Hoc*
- Sincronização da topologia da rede
- Segurança

Ao contrário das redes de comunicação tradicionais, as redes *Ad-Hoc* demandam mecanismos provedores de segurança que se compatibilizem com as

características deste novo paradigma de redes de comunicação de dispositivos móveis.

A maior parte da pesquisa em redes *Ad-Hoc* destina-se ao desenvolvimento dos mecanismos básicos de operação. Muito ainda deve ser feito no que tange aspectos de segurança, principalmente considerando cenários de operação hostis como em aplicações militares e comerciais. Os requisitos e a complexidade dos mecanismos de segurança devem variar com o tipo de aplicação.

As redes *Ad-Hoc* apresentam vulnerabilidades em diversos níveis nas suas atuais implementações, sendo o objetivo das pesquisas em segurança o de dotar estas implementações de mecanismos capazes de conferir à rede a segurança em seus diversos aspectos, respeitando as limitações do sistema, como a escassez de recursos de rádio, bateria, processamento e memória.

1.4 Organização do trabalho

O trabalho descreve no capítulo 2 o funcionamento das redes móveis *Ad-Hoc*. No capítulo 3 são abordados os protocolos de roteamento para estas redes. O capítulo 4 apresenta um estudo sobre os protocolos de autoconfiguração para as *Manets*. No capítulo 5 são descritas questões de segurança necessárias aos protocolos em redes *Ad-Hoc*. E por fim, no capítulo 6 são apresentadas as considerações finais e propostas para trabalhos futuros.

2 REDES Ad-Hoc E PROTOCOLOS DE ROTEAMENTO

O presente capítulo tem como objetivo realizar um embasamento teórico sobre as tecnologias envolvidas no trabalho. Inicialmente será dada uma visão geral do funcionamento das redes *Ad-Hoc*. Em seguida, será mencionado o funcionamento dos protocolos de roteamento, que para este tipo de rede, apresentam características peculiares.

2.1 Visão geral das redes Ad-Hoc

O conceito de uma rede *Ad-Hoc* data do início da década de 70, quando a *United States Defense Advanced Research Projects Agency* (US DARPA) iniciou um projeto denominado *Packet Radio Network* (PRNET), com o intuito de explorar o uso de redes de pacote de rádio num ambiente tático para comunicação de dados.

Em 1983, a DARPA criou o programa *Survivable Adaptive Network* (SURAN) para ampliar a tecnologia desenvolvida no projeto PRNET para abranger grandes redes e para desenvolver protocolos de rede adaptativos que pudessem se adequar às rápidas mudanças de condições em um ambiente tático.

Por fim, a DARPA lançou em 1994 o programa *Global Mobile Information Systems* (GloMo) para satisfazer os requisitos de defesa para sistemas de informações robustos e rapidamente expansíveis (BELLÉ, 2003).

No ano de 1997, foi criado pela *Internet Engineering Task Force* (IETF), o grupo de trabalho Manet com o objetivo de pesquisar e desenvolver possíveis padrões a fim de oferecer suporte ao roteamento para redes IP móveis sem fio. O principal intuito do grupo é desenvolver especificações para roteamento em redes

Ad-Hoc e introduzi-las como padrões para a Internet, habilitando um roteamento ponto-a-ponto em um ambiente móvel e sem fio (BUIATI, 2004). Os protocolos desenvolvidos devem atender as seguintes características:

- Disponibilizar operações confiáveis sobre uma grande variedade de redes sem fio e seus ambientes;
- Suportar serviços IP não orientados à conexão;
- Reagir eficientemente às mudanças na topologia da rede.

O termo *Ad-Hoc* é geralmente entendido como algo criado ou usado para um problema imediato ou específico. Do Latin, *Ad-Hoc*, tem como significado literal “para isto” ou “para um único propósito”. Mas no âmbito de redes móveis *Ad-Hoc*, o significado é muito mais abrangente.

Uma rede móvel *Ad-Hoc* é composta por nodos móveis conectados por interfaces sem fio, que se comunicam através de ondas de rádio. Esses nodos podem formar dinamicamente uma rede sem a necessidade de qualquer infra-estrutura fixa, ou seja, geralmente não existe uma topologia predeterminada e nem um controle centralizado. A figura 2.1 mostra um exemplo de uma rede com três nodos.

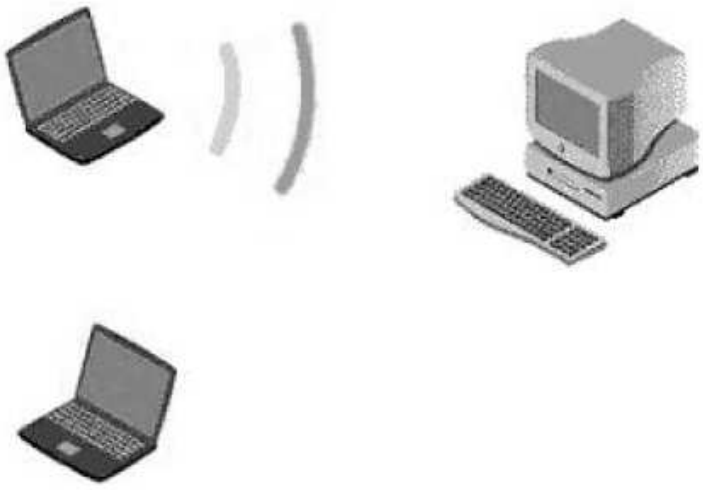

Figura 2.1 – Rede móvel *Ad-Hoc* com três nodos (BUIATI, 2004).

Redes móveis *Ad-Hoc* são também conhecidas como *Mobile Ad-Hoc Network* (*Manet*). Numa *Manet* um nodo só pode se comunicar com os nodos que estão no seu raio de transmissão. Em virtude disto, um pacote destinado a um nodo fora do alcance de transmissão do nodo de origem, deverá passar pelos nodos intermediários, que funcionarão como roteadores até o pacote chegar ao seu nodo de destino.

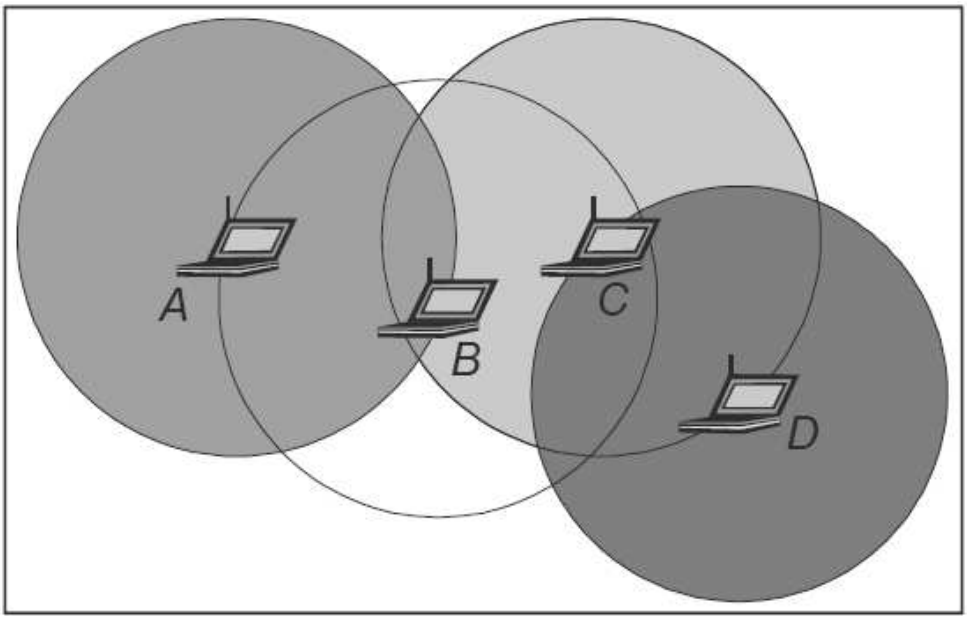

Figura 2.2 – Alcance de comunicação de cada nodo (BELLÉ, 2003).

Na figura 2.2 os círculos representam o alcance de comunicação de cada um dos nodos. Caso o nodo A queira se comunicar com o nodo D a mensagem deverá passar pelos nodos B e C para completar a transmissão dos dados ao nodo D.

Neste tipo de rede, os nodos podem se movimentar livremente e se comunicar diretamente com outro nodo que esteja dentro de sua área de alcance. Deste modo, a topologia da rede muda freqüentemente, de forma imprevisível. Isso significa que um computador intermediário I, que num determinado instante faz parte de uma rota entre os nodos A e B, pode não fazer parte dessa mesma rota mais tarde (BELLÉ, 2003).

2.1.1 Características

As redes *Ad-Hoc* podem operar de forma isolada ou podem atuar em conjunto com uma rede cabeada, sendo que dessa última forma, um roteador é necessário para realizar a transmissão dos pacotes de uma rede para a outra.

Redes *Ad-Hoc* possuem algumas particularidades que as tornam mais complexas que as redes cabeadas e as redes móveis com concentrador de acesso. Essas características são observadas na tabela abaixo (BUIATI, 2004):

Tabela 2.1 – Características das *Manets.*

Características	Descrição
Topologia dinâmica	Os nodos podem se movimentar livremente, logo a topologia da rede muda constantemente e de forma imprevisível.
Largura de banda restrita	Devido a ruídos, interferências, enfraquecimento de sinal, efeitos dos acessos múltiplos e fatores externos, as redes sem fio possuem uma capacidade significativamente menor do que redes cabeadas.
Economia de energia	Dispositivos móveis geralmente utilizam baterias, portanto para esses aparelhos o consumo de energia é um ponto crucial.
Segurança limitada	Redes móveis sem fio são mais vulneráveis a ataques que redes fixas, o que implica numa maior possibilidade de escuta, invasão e ataques. Técnicas de segurança, como IPSec devem ser implementadas para reduzir as chances de ataques. Por outro lado, por possuir um controle descentralizado, possuem maior robustez, já que os serviços operam de forma distribuída.

2.1.2 Classificação

Existem diversas maneiras de classificar as *Manets*. As principais delas são quanto a sua:

- **Comunicação**:
    - Único salto (s*ingle-hop*): os nodos se comunicam diretamente com os outros nodos, pois estão dentro da área de transmissão;
    - Múltiplos saltos (*multi-hop*): alguns nodos não podem se comunicar diretamente com outros nodos, assim é preciso transmitir os dados por nodos intermediários, também chamados de nodos roteadores até que os dados atinjam o nodo destino (BUIATI, 2004).
- **Simetria**:
    - Simétrica: todos os nodos da rede possuem capacidades iguais e dividem responsabilidades similares;
    - Assimétrica: as capacidades como, por exemplo, raio de transmissão, capacidade de processamento e velocidade de movimento; e suas responsabilidades, como habilidade para efetuar roteamento, variam de nó para nó.

Porém, as redes *Ad-Hoc* também podem ser classificadas de acordo com o tipo de tráfego que se espera que os nodos transmitam. Este tráfego pode ser para dados normais ou dados para aplicações em tempo real para aplicações multimídia, como áudio e vídeo. Neste caso, os protocolos utilizados são modelados para se adaptar ao tipo de tráfego a ser transmitido.

Os métodos de roteamento empregados nas várias redes podem ser diferentes. Logo, é possível classificar as redes em relação ao tipo de roteamento:

unicast, *multicast* ou *geocast*. Os métodos de endereçamento também podem servir para a classificação de protocolos. Desta maneira podem ser baseados no *host*, baseados no conteúdo ou até mesmo baseados na capacidade.

Há também outras métricas, como, por exemplo, taxa de transmissão e requisitos de segurança, que podem ser usados como métodos sobre os quais as redes *Ad-Hoc* podem ser classificadas (BELLÉ, 2003).

2.1.3 Aplicações

É vasta a gama de aplicações das redes móveis *Ad-Hoc*, principalmente em situações que requerem a rápida implantação de uma rede de comunicação. O crescimento da computação portátil e da necessidade de mobilidade deve ampliar gradativamente a utilização deste tipo de rede.

As aplicações militares foram as primeiras a utilizar largamente as *Manets*. Nos campos de batalha o terreno era desconhecido, tornando inviável montar e manter uma rede infra-estruturada. Isto fez com que militares investissem em pesquisa e desenvolvimento neste tipo de tecnologia.

Atualmente, as características das redes móveis sem fio permitem taxas de transmissão compatíveis com aplicações multimídia, capacidade de *roaming* e estruturas de rede permitem novas aplicações.

O uso de redes *Ad-Hoc* em operações de resgate, salvamentos e catástrofes naturais em conjunto com comunicação com satélite pode ser extremamente útil. Também podem ser aplicáveis em ambientes de negócios, conferências, feiras onde participantes desejam disseminar ou compartilhar informações rapidamente através de seus *laptops* e PDAs (BUIATI, 2004).

As redes de sensores sem fio constituem outra aplicação recente para as redes *Ad-Hoc*. As redes de sensores são compostas de algumas dezenas até milhares de pequenos dispositivos, de baixa potência, com a capacidade de monitorar um ambiente ou equipamento e comunicar-se com outros elementos da rede. Existem muitos cenários onde as redes de sensores podem ser aplicadas: segurança de instalações, monitoramento das condições climáticas, detecção de falhas em equipamentos, entre outros (NÚCLEO DE COMPUTAÇÃO ELETRÔNICA - NCE/UFRJ, 2006).

2.1.4 Vantagens

A necessidade de instalar redes sem infra-estrutura, a um baixo custo associado com aplicações móveis são as principais vantagens das redes *Ad-Hoc*. Em relação às redes cabeadas, pode-se observar as seguintes vantagens (BUIATI, 2004):

- **Mobilidade:** vantagem primordial;
- **Rápida instalação:** podem sem instaladas em qualquer local sem a necessidade de infra-estrutura física, tornando a rede disponível em pouco tempo e de forma mais rápida;
- **Confiabilidade:** devido a não utilização de infra-estrutura física, torna-se muito mais fácil identificar problemas e reduz-se o tempo de re-configuração de algum nodo caso haja problemas;
- **Conectividade:** dois nós móveis podem se comunicar diretamente, desde que cada nó esteja dentro da área de alcance do outro. Em redes infra-estruturadas, mesmo que dois nós estejam próximos, é necessário que a

comunicação passe pela estação de suporte à mobilidade, no caso de redes fixas pode haver uma ligação por meio de cabos entre os dois nós.

- **Instalação em locais inadequados para redes cabeadas:** locais onde há rios, ruas ou qualquer outro obstáculo entre dois pontos de comunicação, as redes *Ad-Hoc* oferecem um ótimo custo benefício de instalação.

2.1.5 Desvantagens

Apesar das vantagens citadas, alguns problemas e dificuldades podem surgir devido às peculiaridades das redes sem fio. Os maiores problemas relacionados a essa tecnologia são (BUIATI, 2004):

- **Localização:** como os nodos se movem livremente e de forma imprevisível, são necessários mecanismos para conhecer a real localização de cada nodo;
- **Interferências:** como a transmissão e recepção dos dados são feitos utilizando ondas de rádio e freqüências públicas, redes *Ad-Hoc* tornam-se vulneráveis a ruídos e interferência de outros sistemas;
- **Consumo de energia:** dispositivos portáteis geralmente utilizam baterias e estas têm suprimento limitado de energia. Portanto são utilizadas técnicas pelos fabricantes de equipamentos para diminuir o consumo de energia, influenciando diretamente na rede, visto que o nodo não é capaz de receber qualquer informação quando entra em funcionamento visando reduzir o consumo;
- **Inexistência de um ponto central:** a falta de uma entidade centralizadora, com a função de coordenar a rede, é preciso a adoção de algoritmos que gerenciem a rede através dos nodos conectados;

- **Banda passante:** redes sem fio possuem banda passante de no máximo 54 Mbps enquanto em redes cabeadas essa banda pode chegar até 10 Gbps;
- **Interoperabilidade:** redes *Ad-Hoc* ainda possuem diversos produtos proprietários, que podem operar em freqüências diferentes ocasionando um mau funcionamento da rede. Por isso, é aconselhável a implantação de *Manets* com equipamentos de um mesmo fabricante;
- **Segurança:** os dados propagados em uma rede *Ad-Hoc* podem exceder os limites físicos desejados, aumentando a possibilidade de escuta, invasão e ataques;
- **Roteamento:** como a rede possuiu uma topologia dinâmica, é necessário um protocolo de roteamento eficiente para a entrega correta dos pacotes;
- **Taxa de erros:** a taxa de erros associada a enlaces sem fio é mais elevada.

2.2 Protocolos de roteamento

O mecanismo de roteamento em uma rede é responsável pela entrega dos dados entre os diferentes nodos da rede. O nodo responsável por isso recebe a nomenclatura de roteador. Sua principal função é entregar os pacotes de uma máquina de origem para as máquinas de destino. Quando um nodo origem envia pacotes pra um nodo destino, os dados são encaminhados ao roteador local que os encaminha até o destino final. Esse caminho pode conter vários roteadores. Cada roteador seleciona o próximo salto baseado na sua tabela de roteamento, que contem informações sobre todos os roteadores ao longo da rede, até que o pacote chegue ao seu destino. Para atingir esse objetivo, os roteadores trocam informações

entre si, com o intuito de obter um conhecimento parcial ou total da rede, podendo assim selecionar a melhor rota.

Um protocolo robusto e confiável deve gerenciar dinamicamente as informações contidas na tabela de roteamento, visto que a topologia de rede pode mudar freqüentemente (BUIATI, 2004).

Os algoritmos de roteamento nas redes cabeadas podem ser classificados em:

- **Algoritmos estáticos ou não-adaptativos:** são previamente configurados pelo administrador de rede
- **Algoritmos dinâmicos ou adaptativos:** descobrem rotas automaticamente conforme as mudanças na topologia de rede.

Segundo (BUIATI, 2004) as características desejáveis em um algoritmo de roteamento são as descritas na tabela 2.2:

Tabela 2.2 – Características de algoritmos de roteamento.

Características	Descrição
Correto funcionamento	Escolher a melhor rota para o pacote chegar ao seu destino.
Simplicidade	Disponibilizar os serviços com o mínimo de processamento possível.
Robustez	Sempre chegar a uma resposta aceitável e funcionar sem problemas durante anos.
Escalabilidade	Prever o funcionamento da rede e mesmo com o aumento do número de nodos, continue funcionando corretamente.
Convergência	Escolher rapidamente a melhor rota, mesmo com alterações sucessivas das rotas.

Parâmetros de QoS	Suporte a parâmetros de QoS é imprescindível para determinados tipos de tráfego.
Adaptabilidade	Ser capaz de trabalhar com mudanças freqüentes de topologia.
Independência da tecnologia de rede	Funcionamento na maior variedade de computadores e meios físicos.
Justiça	Todos os nodos devem ter acesso a recursos disponíveis na rede a qualquer momento.

A escolha de um protocolo de roteamento varia de acordo com fatores como, por exemplo, complexidade da rede, tamanho, segurança, escalabilidade e estabilidade.

2.2.1 Roteamento em redes Ad-Hoc

Existem diferenças entre os algoritmos de roteamento utilizados em redes cabeadas e redes *Ad-Hoc*. Isso porque, diversos fatores influenciam no desenvolvimento de protocolos para estas redes, como topologia altamente dinâmica, seleção de roteadores e características que podem ser heurísticas na hora de encontrar o melhor caminho para a entrega dos pacotes. Devido à escassez de recursos nas redes *Ad-Hoc,* é necessário otimizar o uso da banda disponível, motivando o desenvolvimento de algoritmos mais eficientes. Logo, em redes móveis *Ad-Hoc* todos os algoritmos de roteamento são dinâmicos devido à mobilidade dos nodos.

Diferentes padrões de mobilidade resultam em dificuldades de desenvolvimento de protocolos de roteamento, visto que, alguns nodos podem se movimentar rapidamente, enquanto outros podem ser fixos ou moverem-se

lentamente, sendo quase impossível prever o padrão de movimentação de nodos, principalmente em redes de larga escala. Isso pode ocasionar uma sobrecarga na troca de mensagem do algoritmo de roteamento, ocasionando a sobrecarga do uso de banda.

O grupo de trabalho *Manet*, com o intuito de observar o mérito e a performance de um protocolo de roteamento, enumera algumas métricas que os protocolos devem seguir. Podem ser tanto qualitativas como quantitativas. Na tabela 2.3 são informadas as métricas qualitativas (CORSON; MACKER, 2006):

Tabela 2.3 – Métricas qualitativas para protocolos de roteamento *Ad-Hoc.*

Métrica	Descrição
Operação distribuída	Característica fundamental a fim de evitar a centralização de informações podendo ocasionar vulnerabilidade.
Livre de *loops*	Para evitar o tráfego de pacotes por muito tempo na rede, pode ser usada uma variável TTL (*time to live*), entretanto uma abordagem mais estruturada é indicada.
Operação baseada na demanda	Algoritmo adaptável às condições de tráfego, utilizando de forma mais eficiente recursos de energia e largura de banda.
Operação pró-ativa	Em certas ocasiões, a latência adicionada pela operação na demanda poderá ser inaceitável. Se os recursos de energia e banda permitirem, operações pró-ativas são desejáveis.
Segurança	Se as camadas de rede e enlace não garantirem segurança, os protocolos de roteamento estarão vulneráveis a ataques. Mecanismos para inibir modificações nas operações do protocolo são desejáveis.

Operação no período de “sonolência”	Durante um período de inatividade, o nodo deve deixar de transmitir e/ou receber pacotes, sem que isso resulte em maiores conseqüências.

Na tabela 2.4 podem-se observar as características quantitativas para avaliação de desempenho dos protocolos de roteamento (CORSON; MACKER, 2006):

Tabela 2.4 – Métricas quantitativas para protocolo de roteamento *Manet.*

Métrica	Descrição
Atraso e desempenho de dados fim a fim	Variância, média e distribuição são dados muito importantes para avaliação de um protocolo de roteamento.
Tempo de descobrimento de rota	Uma forma de medir o atraso do pacote fim a fim de um algoritmo de roteamento é o tempo requerido para estabelecer rotas quando requisitadas.
Porcentagem dos pacotes entregue fora de ordem	Medida para avaliar performance de roteamento de protocolos da camada de transporte como TCP, que entregam pacotes na ordem correta.
Eficiência	Como o tráfego de pacotes de dados e de controle deve compartilhar o mesmo meio e a capacidade dos meios é limitada, o tráfego excessivo de pacotes de controle causará impacto na performance do roteamento.

Devido às peculiaridades características das redes *Ad-Hoc*, obter a eficiência de um protocolo de roteamento não é muito simples. Mas tendo como base os seguintes valores, pode-se medir a eficiência de um protocolo de roteamento para *Manets* (BUIATI, 2004):

- **Bits de dados transmitidos / Bits de dados entregues:** medida que representa a eficiência dos bits de dados entregues dentro da rede. Indiretamente, essa medida fornece também a media de saltos percorridos pelos pacotes de dados.
- **Bits de controle transmitidos / Bits de dados entregues:** medida que representa a eficiência do protocolo no uso entre os pacotes de controle sobre os pacotes de dados entregue.
- **Pacotes de controle e pacotes de dados transmitidos / Pacotes de dados entregues:** medida que tenta capturar a eficiência de acesso ao canal do protocolo.

2.2.1.1 Classificação

Os protocolos de roteamento para redes *Ad-Hoc* podem ser classificados de acordo com o algoritmo de roteamento ou com sua política de descobrimento de rotas.

No que diz respeito ao algoritmo de roteamento, os protocolos podem ser classificados como (PUTTINI, 2004):

- **Algoritmos de vetor de distância:** as rotas são constituídas de acordo com informações de distância entre o nodo de origem e o nodo de destino, mantidas por cada nodo/roteador.
- **Algoritmos de estado de enlace (*link state*):** as rotas consideram todos os enlaces na topologia da rede para se obter rotas ótimas entre origem e destino.

- **Algoritmos de roteamento na origem:** as rotas são estabelecidas para um par origem-destino e estão disponíveis no nodo de origem dos pacotes a serem enviados.

Entretanto, a classificação mais utilizada pelos autores é em relação à política de descobrimento de rotas. Nesta classificação, os protocolos de roteamento são divididos em três grupos: *Global*/Pró-ativos, *On-Demand*/Reativos e Híbridos. A seguir são descritas as características de cada grupo.

Protocolos Pró-Ativos

Os protocolos pró-ativos tentam avaliar continuamente a disposição dos nodos na rede com o intuito de ao ser solicitado um encaminhamento de dados, já se tenha o conhecimento da rota para o destino. Para tanto, cada *host* mantêm uma ou mais tabelas com informações referentes à rede e respondem a mudanças na topologia rede propagando atualizações a fim de manter a sua consistência. Estas atualizações são iniciadas por mecanismos de temporização.

A vantagem deste tipo de abordagem é o atraso mínimo para o envio dos dados, pois a rota pode ser obtida diretamente na tabela de roteamento. Entretanto, a atualização constante destas tabelas, causa uma contínua utilização da rede para troca de pacotes e informações de roteamento.

Estes protocolos são escaláveis em relação à freqüência da conexão fim-a-fim. Protocolos pró-ativos não são escaláveis com relação ao número de nodos, mas podem adquirir essa propriedade se for utilizada uma arquitetura hierárquica (CORRÊA, 2005). O funcionamento de alguns protocolos desta categoria é descrito a seguir.

Destination Sequenced Distance Vector – DSDV

O *Destination Sequenced Distance Vector* (DSDV) é um protocolo pró-ativo baseado em vetor de distâncias, que periodicamente solicita aos seus nodos vizinhos suas tabelas de roteamento, com o intuito de manter suas tabelas atualizadas. Cada nodo possui uma tabela de roteamento com as rotas para todos os demais nodos da rede e o número de saltos para alcançar o destino, mesmo que nunca seja necessário o envio de pacotes a um determinado nodo (PERKINS; BHAGWAT, 2006). Existe apenas uma rota para cada destino.

O DSDV inicia um processo de atualização de rota periodicamente ou ao surgir alguma alteração na topologia da rede (PEREIRA, 2004). Esta atualização pode ser incremental, onde o nodo envia apenas as informações que foram alteradas em sua tabela, ou completa, enviando todas as informações contidas na tabela. Com este procedimento, o protocolo visa evitar congestionamentos na rede.

Optimized Link State Routing – OLSR

O *Optimized Link State Routing* (OLSR) é um protocolo de roteamento pró-ativo que faz uso de *multipoint relays* (MPRs). Os MPRs são nodos selecionados para encaminhar as mensagens de difusão no processo de inundação do protocolo de roteamento. Os MPRs são difundidos na rede para fornecer a cada nodo a informação parcial da topologia da rede para que se possa obter a melhor rota para todos os nodos da rede. O uso de MPRs somado com a eliminação local de duplicidade é usado para reduzir o número de pacotes de controle enviados na rede (PUTTINI, 2004).

O OLSR foi projetado para ser utilizado em redes de larga escala, com tráfego randômico e esporádico. Também apresenta um bom desempenho em redes onde pares de nodos que se comunicam mudam de posição constantemente.

Topology Dissemination Based on Reverse-Path Forwarding – TBRPF

O *Topology Dissemination Based on Reverse-Path Forwarding* (TBRPF) é outro protocolo pró-ativo para *Manets* que fornece roteamento passo a passo ao longo dos caminhos mais curtos para cada destino. Cada nodo gera uma árvore de origem baseado na informação da topologia da rede que é armazenada em uma tabela. Para reduzir o tráfego na rede, cada nodo reporta apenas uma parte de sua árvore de origem para os nodos vizinhos (PUTTINI, 2004).

Utilizando uma combinação de diferentes e periódicas atualizações para manter os vizinhos informados de seu envio de parte da árvore, o TBRPF oferece ainda a possibilidade de enviar informações adicionais da topologia, como por exemplo, a árvore completa, com o objetivo de oferecer uma maior robustez em ambientes altamente móveis.

O TBRPF realiza a descoberta de nodos vizinhos através de mensagens diferenciadas, que contem apenas a mudança do estado dos vizinhos. Isto resulta em mensagens muito menores do que as usadas em outros protocolos de estado de enlace.

Protocolos Reativos

Nos protocolos reativos a descoberta de rota é feita sob demanda, ou seja, somente quando um nodo deseja se comunicar com o seu destino (NIKAEIN; BONNET; NIKAEIN, 2006) Após a rota ser estabelecida, ela é mantida por um mecanismo de manutenção de rotas até que ela seja inacessível ou não ser mais apropriada.

Nesta abordagem o *overhead* de comunicação para determinação de rotas é diminuído, economizando banda e energia. Porém, apresenta um maior atraso no encaminhamento dos pacotes.

Devido a sua natureza de *flooding,* estes protocolos são escaláveis com relação à freqüente mudança na topologia da rede. Mas, não são quanto ao número total de nodos a menos que se utilize uma arquitetura hierárquica. A seguir são descritos alguns destes protocolos.

Dynamic Source Routing – DSR

O *Dynamic Source Routing* (DSR) é um protocolo de roteamento reativo simples e eficiente desenvolvido para ser utilizado em redes *Ad-Hoc multi-hop*. O protocolo permite que a rede se auto-organize e autoconfigure sem necessidade de qualquer administração da infra-estrutura da rede.

O DSR utiliza roteamento na fonte para a entrega de pacotes, ou seja, o nó de origem determina toda a seqüência de nós por onde passará o pacote até chegar ao seu destino (PEREIRA, 2004). Cada nodo possui um *cache* onde são armazenadas todas as rotas conhecidas. O DSR permite múltiplas rotas para um

determinado destino. O protocolo consiste de dois mecanismos: descoberta de rotas e manutenção de rotas.

Ao necessitar encaminhar um pacote a um nodo, o nodo origem verifica se possui rota para o nodo destino em seu *cache*. Caso a rota exista, o nodo origem a utiliza para o encaminhamento do pacote; caso contrário, é iniciado o processo de descoberta de rotas para encontrar dinamicamente um caminho para o destino.

O protocolo DSR oferece um roteamento livre de *loops*, suporte a enlaces unidirecionais e uma rápida convergência quando a topologia de rede é modificada. O protocolo foi desenvolvido para suportar *Manets* com até duzentos nodos e altas taxas de mobilidade (BUIATI, 2004).

Ad Hoc On Demand Distance Vector – AODV

O *Ad Hoc On Demand Distance Vector* (AODV) foi desenvolvido baseado em outros dois protocolos de roteamento para redes *Ad-Hoc*, o DSR e o DSDV. É um protocolo reativo, baseado em vetor de distâncias, que tenta eliminar a necessidade de difusão de mensagens de roteamento. Outra característica importante é sua capacidade de minimizar a latência quando novas rotas são requisitadas.

Seguindo o modelo do DSR, o AODV atua somente sob demanda, descobrindo rotas apenas quando necessário, utilizando os mecanismos de descoberta de rotas e manutenção de rotas. Porém, o protocolo também utiliza características do DSDV, obrigando todos os nodos intermediários a estabelecerem dinamicamente entradas em tabelas locais para cada destino ativo (PEREIRA, 2004). Cada nodo possui conhecimento do próximo salto para atingir o destino e a distância em número de saltos.

Projetado para ser utilizado em *Manets* com dezenas até milhares de nodos móveis, o AODV possui forma de funcionamento semelhante aos algoritmos tradicionais, permitindo uma fácil conexão da rede móvel com uma rede fixa. Além disso, o protocolo oferece suporte ao tráfego *unicast* e *multicast*. Como ponto negativo, apresenta apenas uma única rota para cada destino.

Protocolos Híbridos

Os protocolos de roteamento híbridos combinam características das abordagens pró-ativas e reativas. Segundo (CORRÊA, 2005), são projetados para aumentar a escalabilidade, permitindo que nodos próximos trabalhem em conjunto com o intuito de formar uma espécie de *backbone* tentando reduzir o *overhead* de descoberta de rota.

Esta abordagem pode oferecer o melhor *trade-off* entre *overhead* de comunicação e atraso, mas o *trade-off* pode variar, pois está diretamente ligado ao tamanho e a dinâmica dos grupos formados para o trabalho em conjunto.

Estes protocolos possuem um compromisso com a emissão de escalabilidade com relação ao número total de nodos, à freqüência de conexão fim-a-fim e freqüência de mudança da topologia. O funcionamento de um destes protocolos é descrito na seqüência.

Zone Routing Protocol – ZRP

O *Zone Routing Protocol* (ZRP) é um protocolo híbrido que divide a *Manet* em zonas de roteamento, executando protocolos independentes para comunicação intrazona e entre zonas.

O ZRP utiliza um protocolo pró-ativo para roteamento intrazona, através do módulo *Intrazone Routing Protocol* (IARP). Para que um nodo saiba as rotas para todos os nodos dentro da zona de roteamento, cada nodo possui uma tabela de roteamento que indica qual a rota para cada nodo pertencente a sua zona de roteamento. Estas características fazem com que economize largura de banda e limite o tamanho da tabela de roteamento (FERNANDES, 2006).

O desempenho do ZRP está diretamente ligado ao raio das zonas. Redes densas com nodos em grande movimentação geralmente resultam em zonas de roteamento pequenas. Redes esparsas com pouca movimentação de nodos resultam em zonas de roteamento maiores.

A construção de uma zona de roteamento requer que o nodo inicialmente descubra quem são seus vizinhos. Com base nesses dados e em medidas locais de tráfego um nodo pode estimar a sua zona de roteamento ótima.

O roteamento entre zonas é realizado por um protocolo reativo, denominado *Interzone Routing Protocol* (IERP). Para se alcançar os nodos fora da zona de roteamento, o ZRP faz um pedido de rota para seus nodos periféricos. Caso algum destes nodos possua a rota para o destino solicitado, esta é enviada ao nodo solicitante. Se os seus nodos periféricos não possuírem a rota, estes enviam um pedido para seus respectivos nodos periféricos, e assim sucessivamente até que se

obtenha uma rota para nodo requisitado. Com isto, ocorre um atraso na determinação de rotas para nodos fora da zona de roteamento.

3 PROTOCOLOS DE AUTOCONFIGURAÇÃO

Todo nodo, para se comunicar em uma rede, necessita de um identificador único, que geralmente é o IP (BUIATI, 2004). Diversos protocolos foram criados com o intuito de fornecer automaticamente esse identificador aos equipamentos conectados à rede, tanto para redes infra-estruturadas como para redes *Ad-Hoc*.

3.1 Histórico

No início da década de 80, os administradores de rede precisavam configurar manualmente cada computador. Isto causava muitos problemas, principalmente o de erro na digitação do endereço IP.

Em 1984, o RARP (*Reverse Address Resolution Protocol*) foi padronizado. Este protocolo, que é uma adaptação do protocolo ARP, permitia que os computadores alocassem seus endereços de rede automaticamente. Quando um computador quer realizar um pedido de endereço ao servidor, este envia o endereço físico da sua interface de comunicação, ou seja, o endereço MAC (*Machine Address Code*). O servidor RARP possui uma tabela mapeando os endereços MAC para endereços IP. Se o servidor possuir o endereço físico na tabela, o servidor responde o pedido enviando o endereço de rede para o computador solicitante. Caso o servidor não tenha o endereço físico cadastrado na tabela, o nodo que realizou a solicitação acaba não recebendo o endereço IP. Este protocolo não era muito eficiente, pois era necessário o cadastro de todos os endereços MAC dos equipamentos de rede no servidor. Além disso, a solicitação RARP utiliza *broadcast*

o que impede o encaminhamento a outras redes nos roteadores. Logo, é necessário um servidor RARP para cada rede (JEONG; CHOI; MA, 2005).

No ano de 1985, o BOOTP (*Bootstrap Protocol*) foi criado para solucionar as deficiências apresentadas pelo RARP. Utiliza o protocolo UDP para trafegar suas mensagens, logo, suas mensagens podem ser roteadas para outras redes através de um roteador, não sendo mais necessário a utilização de um servidor para cada rede, como ocorria no RARP. Diferentemente do RARP, o protocolo BOOTP se comunica utilizando a camada de rede. A estação cliente encaminha sua solicitação na rede através de um endereço IP de difusão. Os servidores BOOTP serão os únicos a reconhecer e responder a requisição também por difusão, pois o cliente ainda não possui seu endereço IP para confirmar o recebimento da mensagem. Porém, neste protocolo, ainda é necessária a configuração manual pelo administrador de rede da tabela de endereços.

O DHCP (*Dynamic Host Configuration Protocol*) foi padronizado pela IETF em outubro de 1993, com o intuito de resolver os problemas apresentados pelo BOOTP. A coleção de endereços IP no DHCP é diferente das tabelas de endereços dos protocolos anteriores. Ela também possui informações com máscara de sub-rede, roteador *default*, servidor de nomes (DNS), mas não possui necessariamente o mapeamento de um endereço MAC para um endereço IP. Ao invés disso, o protocolo utiliza uma concessão de endereços IP por um determinado tempo.

3.2 Autoconfiguração em redes móveis Ad-Hoc

Em redes *Ad-Hoc* é difícil garantir acesso a um servidor, devido à mobilidade da rede. É desejável que a configuração dos nodos seja feita de forma dinâmica,

automática e de preferência sem intervenção humana. Portanto, os *hosts* devem cooperar uns com os outros para se configurarem com um endereço único.

3.2.1 Necessidades

Segundo (BUIATI 2004) para se ter um protocolo de autoconfiguração rápido, seguro e confiável, as seguintes características são necessárias:

Tabela 3.1 – Necessidades de um protocolo de autoconfiguração.

Necessidade	Descrição
Unicidade dos endereços IP	Dois ou mais nodos não podem obter o mesmo endereço IP em um determinado instante de tempo.
Correto funcionamento	Um endereço IP é associado a um nodo somente durante o período em que ele estiver na rede. Quando um nodo deixar a rede, o seu endereço IP deve ser disponibilizado a outros nodos que queiram se juntar à rede.
Solucionar problemas relacionados à perda de mensagens	Caso algum nodo falhe ou ocorra perda de mensagens, o protocolo deve agir de forma que não haja dois ou mais nodos com o mesmo endereço IP.
Permitir endereçamento *multi-hop*	Um nodo só não será configurado na rede com um endereço IP somente se não houver nenhum endereço disponível em toda a rede.
Minimizar o tráfego de pacotes adicionais na rede	O protocolo deve minimizar a troca de pacotes entre os nodos durante o processo de autoconfiguração de um nodo a fim de evitar afetar a performance da rede.
Verificar a ocorrência de solicitações concorrentes de endereço IP	Quando dois nodos solicitam um endereço IP no mesmo instante de tempo, deve realizar um tratamento a fim de evitar que os dois nodos obtenham o mesmo endereço.

Ser flexível ao particionamento e à fusão de redes *Ad-Hoc*	O protocolo deve manipular a fusão de duas redes distintas *Ad-Hoc* como também o particionamento em duas ou mais redes.
Realizar o processo de sincronização	O protocolo deve-se adaptar as mudanças da topologia da rede.
Possuir segurança	O protocolo deve se assegurar que somente nodos autorizados e confiáveis tenham permissão para acesso à rede.

3.2.2 Classificação dos protocolos

Os protocolos de autoconfiguração podem ser classificados de diversas formas. Alguns autores classificam os protocolos de autoconfiguração como ativos ou passivos. Os protocolos ativos são aqueles que enviam informações adicionais à rede por *broadcast*, ou seja, enviam pacotes de controle para o correto funcionamento do protocolo. Por outro lado, os protocolos passivos são aqueles que não precisam do envio de pacotes de controle adicionais para a detecção de conflitos. A detecção é realizada através da análise do tráfego do protocolo de roteamento.

No que diz respeito ao processo de detecção de endereços duplicados os protocolos de autoconfiguração de endereços IP podem ser classificados de acordo com o processo de detecção de endereços duplicados (DAD) (PUTTINI, 2004):

- **Alocação para detecção de conflitos**: o nodo escolhe um endereço IP por tentativa e faz a requisição esperando pela aprovação de todos os nodos da rede. Caso algum nodo negar, esse endereço já está em uso e o processo se repete até que se encontre um endereço disponível.

- **Alocação livre de conflitos**: usa o conceito de divisão binária, onde cada nodo possui um conjunto de endereços distintos. Cada nodo pode atribuir um endereço IP sem a necessidade dos demais nodos da rede aprovar. Sendo assim, todos os nodos são responsáveis pelo processo de atribuição de endereços.
- **Alocação por melhor esforço**: os nodos da rede são responsáveis por atribuir um endereço IP para os novos nodos, tentando associar um endereço que não esteja sendo usando na rede. Todos os nodos possuem uma lista de endereços livres ou em uso na rede. Esse tipo de protocolo funciona muito bem em conjunto com protocolos de roteamento pró-ativos, pois os nodos frequentemente realizam difusão com as informações de endereços usados na rede.

Com relação ao processo de autoconfiguração pode-se classificar os protocolos das seguintes maneiras: independente (*Stateless*), dependente (*Stateful*) e híbrido. Na seqüência serão abordadas as características de cada classificação, bem como os protocolos que pertencem a cada uma destas classes.

3.2.2.1 Dependentes (*Stateful*)

Nos protocolos dependentes, cada nodo da rede mantém um conjunto de endereços IP, assim é necessária uma segunda entidade para atribuir um endereço IP a um novo membro da rede. Eles podem ser classificados de acordo com a maneira que mantêm a tabela de alocação de endereços. Dessa maneira, são divididos da seguinte forma:

- Manutenção centralizada da tabela de alocação;

- Manutenção distribuída de uma tabela de alocação comum;
- Manutenção distribuída de uma tabela de alocação individual.

Com uma tabela de alocação centralizada, apenas um nodo na rede, chamado de central, é responsável por distribuir endereços para os novos nodos. Logo, este nodo deve estar sempre acessível na rede para atender as requisições. Caso o nodo central venha a deixar a rede, um novo nodo é escolhido para exercer esse papel dinamicamente. Quando a transferência da tabela de alocação de endereços para o novo nodo central não for possível, é necessário que os nodos na rede sejam notificados para informar seus endereços a fim de serem registrados na tabela ou que realizem uma nova requisição de endereço. Porém, este tipo de abordagem não é adequado a cenários altamente dinâmicos, onde a troca do nodo central é muito freqüente.

Por outro lado, tabelas de alocação distribuídas permitem que todos os nodos na rede possam realizar a concessão de endereços, no entanto é necessário que se mantenha a sincronização das tabelas entre todos os nodos para evitar a duplicidade de endereços, no caso de tabelas comuns. Por outro lado, com o uso de tabelas individuais é necessário garantir que essas tabelas não contenham endereços em comum. A confiança e eficiência da sincronização dessas tabelas são os maiores desafios dessa abordagem, visto que geram consumo de banda considerável. A fusão de redes deve ser tratada especificamente para tratar da sincronização das tabelas de alocação de ambas as partições e identificar conflitos de endereços (WENIGER; ZITTERBART, 2004).

Dynamic Configuration Distribution Protocol – DCDP

O *Dynamic Configuration Distribution Protocol* (DCDP) é um protocolo de autoconfiguração que atua de forma distribuída. Os nodos na rede são responsáveis pela atribuição de endereços. Para isto, utiliza um mecanismo de divisão binária do bloco de endereços, para fornecê-los distintamente.

Um nodo cliente que deseja se associar à rede faz uma requisição em *broadcast* por um endereço IP. Os nodos vizinhos respondem à solicitação, informando o tamanho do seu bloco disponível. O nodo cliente seleciona o vizinho com o maior bloco disponível. Este vizinho (servidor), utilizando o mecanismo de divisão binária (figura 4.1), divide seu conjunto de endereços IP em duas metades e envia uma metade para o nodo cliente e mantêm outra metade para atender futuras requisições. Quando o cliente recebe seu conjunto de endereços, associa o primeiro a si mesmo e mantêm o resto como bloco endereços disponíveis para associação de novos nodos. Após isto, uma mensagem de confirmação é enviada ao nodo servidor (BUIATI, 2004).

O mecanismo de divisão binária implementado no protocolo evita que todos os nodos da rede mantenham conjuntos disjuntos de endereços, evitando o conflito de endereços até mesmo quando ocorre a junção de duas ou mais redes *Ad-Hoc*.

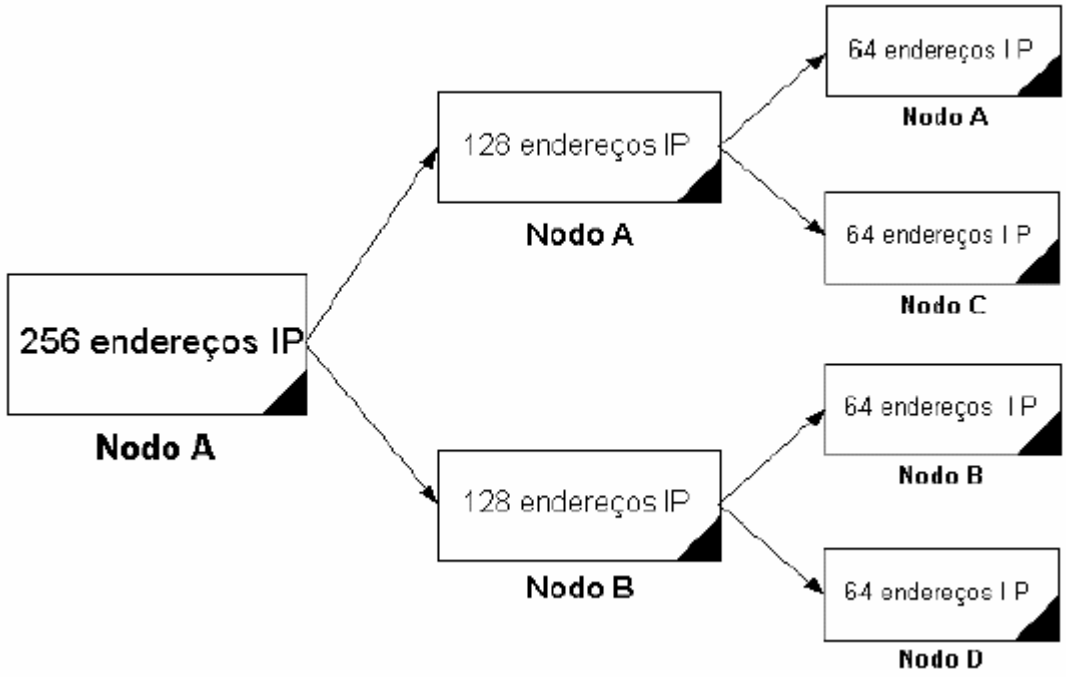

Figura 3.1 – Funcionamento do mecanismo de divisão binária (BUIATI, 2004).

IP Address Assignment in a Mobile Ad Hoc Network

Neste protocolo de autoconfiguração, cada nodo possui um conjunto de endereços IP que são utilizados para configurar novos nodos que desejam ingressar à rede sem a necessidade de consultar os demais nodos na rede, sendo que dentro de uma mesma *Manet* esses conjuntos são distintos.

Um nodo que deseja ingressar à rede, ou seja, o nodo cliente faz uma requisição de endereço a um dos nodos já configurados na rede (nodo servidor). O nodo servidor responde ao nodo cliente e fica responsável pela autoconfiguração de endereço. Em seguida, o nodo servidor divide seu conjunto de endereços em duas metades e envia uma das metades ao nodo cliente, mantendo a outra metade para atender futuras requisições. Quando o nodo cliente recebe o conjunto de endereços, ele associa o primeiro endereço a si próprio e mantêm o resto para disponibilizar

para novos nodos que venham a se juntar à rede. Após isto, o nodo cliente envia uma mensagem confirmando o fim do processo (BUIATI, 2004).

O protocolo trabalha muito bem com fusão e separação de redes por manter conjuntos distintos de endereços IPs nos nodos pertencentes à rede.

MANETconf

O MANETconf é um protocolo de autoconfiguração baseado em uma tabela comum de endereços distribuídos onde cada nodo pode atribuir um endereço IP e manter uma tabela de alocação com os endereços em utilização e disponíveis. A sincronização desta tabela é a tarefa mais crítica e complexa do protocolo.

No MANETconf, um nodo cliente, que deseja se juntar a uma rede móvel *Ad-Hoc* envia uma mensagem em *broadcast* para verificar seus vizinhos. Em seguida, o este nodo seleciona o vizinho que primeiro responder sua mensagem como servidor e faz a ele uma requisição de endereço. O nodo servidor seleciona um endereço de sua tabela e solicita a todos os demais nodos da rede a permissão para atribuí-lo ao novo nodo. Este pedido de permissão se deve a possibilidade de as tabelas de alocação de endereços não estarem sincronizadas ou de dois nodos escolherem o mesmo endereço para atribuição simultaneamente (WEHBI, 2006).

Se todos os nodos responderem positivamente, ele conclui que o endereço está disponível e o envia ao nodo cliente. Ao mesmo tempo, ele envia para todos os nodos através de difusão, uma mensagem informando a alocação do endereço selecionado, para que os demais possam atualizar suas tabelas. Caso o pedido de permissão seja negado, o nodo servidor concluiu que o endereço está em uso e repete o processo algumas vezes. Se o servidor detectar que um ou mais nodos não

respondem, ele entra em contato novamente com estes via *unicast*. Se o nodo contatado ainda está conectado à rede, ele responde ao nodo servidor e o processo de configuração de endereços continua. Caso o nodo contatado não esteja mais presente na rede, a mensagem de resposta não é recebida pelo servidor que trata de difundir para os demais nodos da rede a informação sobre a saída daquele nodo.

A diferenciação entre redes é baseada em um identificador de redes, que é composto pelo menor endereço IP em utilização na rede e um identificador único gerado pelo nodo que utiliza este menor endereço. Quando uma rede sofre um particionamento, uma das partições mantêm o identificador de rede antiga e age como se nada tivesse acontecido, enquanto a outra partição irá detectar o ocorrido assim que ocorrer a primeira alocação de endereço para um novo nodo. Somente após isso, será conhecido o nodo com o menor endereço IP, que será responsável por gerar um novo identificador de rede e o enviará aos demais nodos da rede (NESARGI; PRAKASH, 2006).

Quando dois ou mais nodos se comunicam, eles trocam seus identificadores de rede. Se identificador recebido for diferente do identificador que o nodo possui, uma fusão de redes é detectada. Neste caso, estas redes trocam suas tabelas de alocação para que possa se concluir a fusão. Completada esta troca, caso exista algum conflito de endereços IP, o nodo que possuir o menor número de conexões TCP deverá liberar o endereço IP e iniciar o processo para adquirir um novo.

Portanto, o MANETconf garante a unicidade de endereços e é totalmente distribuído, já que qualquer nodo pode atribuir novos endereços. Além disso, apenas os nodos com endereços duplicados necessitam realizar troca de endereços no caso de fusão de redes. Porém, o protocolo possui uma grande complexidade com relação à comunicação e sincronização da tabela de alocação de endereços. O

mecanismo de atribuição de endereços consome muita banda, visto que consiste de *broadcasts* e um grande número de *unicasts*. Todos os nodos precisam dar permissão para o uso de um novo endereço, o que pode gerar grandes atrasos. E por fim, o protocolo é muito susceptível a falhas de rede devido a sua dependência de comunicações *unicast*.

3.2.2.2 Independentes (*Stateless*)

Nos protocolos com abordagem independente nenhuma tabela de alocação de endereços é mantida. Os nodos constroem seus próprios endereços baseados em um número randômico ou no identificador do hardware. Neste processo é necessário um mecanismo de detecção de endereços duplicados para assegurar a unicidade do endereço, denominado *Duplicate Address Detection* (DAD). Logo, o mecanismo de DAD é a parte mais importante destes protocolos. A configuração dos endereços pode ser realizada antes ou após a execução do mecanismo de detecção de endereços duplicados.

A grande dificuldade nestes protocolos também é a fusão de redes. Para tratar esses eventos o mecanismo de DAD pode ser executado somente após a junção de redes ou estar em execução permanente. No primeiro caso, ao ser detectada a fusão todos os nodos devem ser notificados do ocorrido para repetir o processo de detecção de endereços duplicados. Isto geralmente requer mensagens de difusão, o que pode acarretar em um grande consumo de banda. Já a execução permanente deste mecanismo pode ser obtida através de sua execução periódica ou sua integração com o protocolo de roteamento. Esta última é mais eficiente, pois

causa menos *overhead* na rede, porém é menos eficiente na detecção de endereços duplicados (WENIGER; ZITTERBART, 2004).

IP Address Autoconfiguration for Ad Hoc Networks

O *IP Address Autoconfiguration for Ad Hoc Networks*, é um protocolo de autoconfiguração com similar ao de descoberta de rotas do protocolo de roteamento AODV.

O funcionamento do protocolo utiliza duas fases. Na primeira faze, o nodo que deseja obter um endereço IP, utiliza um endereço randômico e temporário entre 0 e 2047 da rede classe B 169.254/16. Endereços nessa faixa não são utilizados para endereçamento permanente, são apenas utilizados para comunicação com os demais nodos da rede durante o processo de atribuição de um novo endereço. Na segunda fase, o nodo seleciona aleatoriamente um endereço entre 2048 e 65534 para ser utilizado permanentemente por ele na rede. Então ele envia uma mensagem *Address Request* (AREQ) para verificar se o endereço permanente escolhido já está sendo utilizado por algum outro nodo na rede, processo chamado de *Strong Duplicate Address Detection* (SDAD). Caso algum nodo esteja utilizando o endereço solicitado, este nodo envia um *Address Reply* (AREP) notificando a indisponibilidade daquele endereço. Neste caso, o nodo seleciona endereço e repete o procedimento até que não receba nenhuma resposta de outro nodo sobre o endereço escolhido em um determinado espaço de tempo (PERKINS; ROYER; DAS, 2006).

Porém, este protocolo não trata de questões como fusão e separação de redes *Ad-Hoc*, podendo ocasionar endereços IP duplicados. Além disto, o protocolo

permite que dois ou mais nodos utilizem o mesmo endereço IP na faixa de endereços de 0 a 2047, ocasionando um conflito de endereços. O protocolo utiliza tempos constantes para o processo de detecção de endereços duplicados e dependendo do tamanho da *Manet* este tempo pode não ser suficiente para se receber um AREP, podendo causar a alocação de um endereço já utilizado. E ainda, um grande *overhead* é gerado devido à inundação na rede causada pela entrada de cada novo nodo.

Weak Duplicate Address Detection – WDAD

O *Weak Duplicate Address Detection* (WDAD) é um mecanismo de detecção de duplicidade de endereços que tem por idéia tolerar conflito de endereços contanto que as informações enviadas por um nodo remetente alcancem o nodo destino mesmo que o endereço de destino esteja em uso por mais de um nodo na rede (VAIDYA, 2006). É por este motivo que cada nodo seleciona uma chave de identificação para tornar possível a identificação de endereços duplicados através do protocolo de roteamento.

Cada nodo gera uma chave durante a fase de inicialização, e a distribui junto com seu endereço IP em todas as mensagens de roteamento. Esta chave é usada para detectar endereços duplicados. Cada nodo mantêm as chaves junto com os respectivos endereços IP na sua tabela de roteamento. Quando um nodo recebe uma mensagem de roteamento com um endereço IP existente em sua tabela, ele checa se as chaves são diferentes. Caso sejam diferentes, é detectado um conflito de endereços. As informações transmitidas são descartadas e são tomadas ações para informar os demais nodos sobre o conflito de endereços (WEHBI, 2006).

O grande problema do WDAD é sua dependência do protocolo de roteamento. Além de ser necessária a alteração no cabeçalho do protocolo de roteamento para adicionar as informações da chave de identificação, essa alteração gera um aumento no *overhead* do tráfego. Além disso, o protocolo não apresenta um funcionamento adequando com protocolos de roteamento reativos, visto que não são mantidas tabelas de roteamento com rota para todos os nodos da rede.

Passive Duplicate Address Detection – PDAD

O *Passive Duplicate Address Detection* (PDAD) é um mecanismo de detecção de endereços duplicados projetado para protocolos de roteamento *link-state*. O PDAD, ao invés de tentar explicitamente detectar e solucionar problemas de duplicidade enviando informações de controle verifica mensagens de roteamento através de cada nodo e deduz a existência de endereços duplicados por meio de eventos que ocorrem quando este problema ocorre (WENIGER, 2006).

Nos protocolos de roteamento pró-ativos, os nodos periodicamente trocam mensagens com os demais nodos na rede para se conhecer a topologia da rede. Estas mensagens possuem um número de seqüência para se distinguir os pacotes mais novos dos mais antigos. Esta informação é analisada pelo protocolo para a detecção de conflito de endereços. Como o valor do número de seqüência é incrementado a cada pacote, um nodo ao receber um pacote com o número de seqüência maior do que o número que possui em seu próprio contador, a duplicidade de endereços é detectada (WEHBI, 2006).

O protocolo PDAD gera pouco *overhead*, porém exige uma complexa análise do tráfego na rede e um protocolo de roteamento pró-ativo.

Ad Hoc IP Address Autoconfiguration

O *Ad Hoc IP Address Autoconfiguration* é um protocolo de autoconfiguração baseado nos mecanismos do SDAD e WDAD para prover consistência no endereçamento. Logo, o processo de detecção de endereços duplicados não apenas checa por conflito de endereços durante a inicialização, mas também checa e resolve estes problemas detectados por nodos intermediários usando mensagens de roteamento. O uso destes dois mecanismos permite um controle mais fácil do particionamento e fusão de redes (WEHBI, 2006).

Seguindo o modelo do WDAD, cada nodo deve escolher uma chave de 128 bits para o controle dos pacotes do protocolo de roteamento. Os nodos intermediários mantêm esta chave em sua tabela de roteamento ou *cache* para cada endereço. O procedimento de autoconfiguração é o mesmo usado pelo SDAD.

Um nodo, ao receber um pacote de roteamento, verifica todos os endereços IPs e chaves contidas neste pacote e os compara com os endereços e chaves contidos em seu *cache* ou tabela de endereços. Caso encontre para o endereço duas chaves diferentes é detectada uma duplicidade de endereços. Neste caso, o nodo envia uma mensagem de erro via *unicast* para o nodo com a chave de menor valor informando o conflito de endereço.

Por estar integrado ao protocolo de roteamento o *Ad Hoc IP Address Autoconfiguration* existe uma diminuição do número de mensagens trocadas entre os nodos.

3.2.2.3 Híbridos

Protocolos híbridos combinam elementos das abordagens independentes e dependentes. Isto resulta em protocolos mais robustos, mas podem resultar em protocolos com maior complexidade e com maior *overhead*.

Passive Autoconfiguration of Mobile Ad hoc Networks – PACMAN

O protocolo *Passive Autoconfiguration of Mobile Ad hoc Networks* (PACMAN) combina o PDAD com a manutenção de uma tabela alocação comum distribuída. Diferentemente de outros protocolos, as tabelas de alocação atualizadas passivamente, ou seja, os nodos ficam coletando informações sobre os endereços dos novos nodos se integraram à rede através do tráfego gerado pelo protocolo de roteamento (WENIGER, 2006). Portanto, não há consumo extra de largura de banda para executar a tarefa.

Para acelerar o processo de configuração, um nodo que deseja ingressar à rede pode solicitar a tabela de alocação para os nodos vizinhos. Este mecanismo permite uma economia de energia e banda por parte dos nodos, mas permite que exista a possibilidade de atribuir endereços duplicados. Para isto, existe o mecanismo de PDAD, que visa detectar a duplicidade de endereços e tratá-los. O problema da dependência de um protocolo de roteamento é contornado por uma arquitetura modular (WENIGER; ZITTERBART, 2004).

3.2.3 Métricas para avaliação de performance

Existem diversas métricas para se analisar o desempenho de um protocolo de autoconfiguração de endereços (ZHOU; NI; MUTKA, 2006):

- **Operação distribuída**: em uma rede Ad-Hoc um nodo não é tão confiável quanto um servidor DHCP devido aos diversos fatores particulares a esse tipo de rede. A falha de alguns nodos não deve impedir o funcionamento do protocolo, sendo então necessário seu funcionamento de forma distribuída.
- **Exatidão**: dois ou mais nodos não devem possuir o mesmo endereço IP. Portanto, quando acontecer esse fato, o algoritmo de detecção de endereços duplicados deve ser executado o mais rápido possível.
- **Complexidade**: devido à quantidade limitada de memória e processamento de nodos móveis, a solução deve ser o mais simples possível, podendo consistir de módulos como alocação de endereços, detecção de endereços duplicados e manutenção de tabelas de estado do nodo.
- **Comunicação excessiva**: deve-se evitar a difusão em virtude do alto consumo de banda, utilizando-se de alternativas como a comunicação somente com nodos vizinhos. Logo, protocolos onde cada nodo pode atribuir um endereço IP isoladamente são mais eficazes.
- **Igualdade**: distribuição de endereços IP deve ser justa, a fim de evitar a duplicidade de endereços.
- **Latência**: latência é o tempo entre a solicitação e a atribuição de um endereço IP livre a um nodo solicitante. Quanto menor as mensagens de difusão menor a latência.

- **Escalabilidade**: protocolos que utilizam difusão para a autoconfiguração possuem uma baixa escalabilidade em virtude do consumo de banda estar ligado ao número de nodos na rede. Já se a comunicação ocorre entre nodos vizinhos e localmente, o protocolo tem alta escalabilidade.

4 SEGURANÇA DOS PROTOCOLOS

Analisando o funcionamento dos protocolos de autoconfiguração propostos, podemos observar que nenhum tipo de segurança é oferecido, pois todas as abordagens assumem que os nodos são confiáveis. Caso um nodo mal-intencionado venha se juntar à rede, o bom funcionamento da mesma pode ser afetado.

O objetivo deste capítulo é verificar as maneiras de oferecer segurança aos protocolos e analisar as propostas de segurança já desenvolvidas. Para solucionar o problema da segurança em protocolos de roteamento, diversas abordagens já foram feitas. Porém, a segurança dos protocolos de autoconfiguração para redes *Ad-Hoc* ainda é um tema pouco estudado. Logo, a existência de pouco material sobre o assunto restringiu a análise a apenas um protocolo de configuração, proposto por (BUIATI, 2004) que serviu de base para esse estudo. A intenção inicial era realizar uma série de testes para verificar até que ponto o protocolo era realmente seguro. Contudo, dificuldades em relação ao processo de compilação do código fonte do protocolo com a extensão para autenticação em *Manet* (MAE) acabaram impedindo a realização dos testes.

Como veremos em seguida, prover segurança em redes *Ad-Hoc* é algo bastante complexo, já que as essas redes possuem características peculiares, que demandam que as propostas de segurança operem de forma distribuída, auto-organizada e localizada.

4.1 Serviços de segurança

Inicialmente, para fornecer segurança a redes sem fio *Ad-Hoc* devem ser levados em conta os atributos básicos de segurança: autenticidade, confidencialidade, disponibilidade, integridade e não-repúdio. Estas medidas visam evitar o vazamento de informações, fraudes, erros, uso indevido, sabotagens e roubo de informações (BUIATI, 2004).

A autenticidade permite um nodo assegurar a identidade do nodo com o qual está se comunicando. O serviço de autenticação deve assegurar ao destino que a origem da mensagem é aquela informada em seu conteúdo. Este serviço é geralmente disponibilizado através de mecanismos como senha ou assinatura digital. Sem autenticação, um nodo mal-intencionado pode assumir a identidade de um nodo pertencente a *Manet* e ganhar acesso a recursos na rede e interferir na operação de outros nodos pertencentes à rede.

A confidencialidade assegura que as informações não sejam reveladas por nodos não autorizados. Tem por objetivo evitar que alguém que não seja explicitamente autorizado pelo autor da informação possa fazer a leitura e/ou cópia da mesma. Para atender este serviço, utiliza-se principalmente a criptografia.

Disponibilidade consiste na proteção dos serviços prestados pelo sistema de forma que eles não se tornem indisponíveis sem autorização, assegurando aos nodos acessos aos recursos sempre que ele necessitar. Um ataque de negação de serviço (DoS) pode atuar em qualquer camada de uma rede *Ad-Hoc*. Na camada física e de acesso ao meio, pode-se prejudicar a transmissão de dados interferindo o sinal transmitido (*jamming*). Na camada de rede, um nodo inimigo pode derrubar serviços e conexões.

Integridade garante que a mensagem que está sendo transmitida não será modificada sem a permissão do proprietário da informação. A modificação inclui ações como escrita, alteração de conteúdo, alteração de status, remoção e criação de informações. Uma mensagem pode ser corrompida devido a falhas de transmissão na rede ou devido a ataques maliciosos.

O não-repúdio visa impedir que o nodo emissor de uma mensagem negue a sua autoria.

4.2 Ataques à segurança

Os ataques à segurança das *Manets* podem ser classificados de acordo com tipo de ataque ao fluxo das informações. Neste caso, existem quatro classificações (SOUSA JUNIOR; PUTTINI, 2006):

- **Interceptação** - acesso não autorizado a transmissões, possibilitando a cópia das mensagens transmitidas. É o ataque mais comum e de difícil detecção.

- **Modificação** - é um agravante da interceptação, em que o conteúdo da mensagem é alterado.

- **Fabricação** ou **embuste** - simulação para o destino de uma origem legítima. O atacante faz-se passar por uma procedência legítima, inserindo objetos espúrios no sistema atacado.

- **Indisponibilidade** ou **interrupção** - ações não autorizadas ocasionando sobrecarga no processamento de sistemas, tornando-os inacessíveis aos legítimos usuários, por longos períodos ou por sucessões de pequenos intervalos.

Os ataques também podem ser classificados quanto à ação do atacante. Nesta classificação, os ataques a redes móveis *Ad-Hoc* podem ser divididos em passivos ou ativos. Os ataques passivos não afetam a operação da rede, sendo caracterizados pela interceptação dos dados, sem alterá-los. Por outro lado, os ataques ativos são aqueles em que o atacante cria, altera, descarta ou inviabiliza o uso de dados em trânsito. Os ataques ativos são os mais numerosos, podendo atuar em diferentes camadas do modelo OSI.

Os atacantes podem ser classificados como internos ou externos. Atacantes internos são aqueles que conseguem de alguma forma se passar por membros da rede, enquanto que os externos são aqueles que influenciam, mas não participam da rede. De fato, a eficiência e as possibilidades de ataques variam de acordo com o acesso que o atacante tem à rede. Se de alguma forma ele conseguir obter chaves ou for incluído na lista de vizinhos válidos, passando a ser um atacante interno, poderá causar mais problemas (FERNANDES et al., 2006).

4.3 Mecanismos de segurança

Diversos mecanismos podem ser utilizados para fornecer uma maior segurança para a troca de mensagens de um protocolo para redes *Ad-Hoc*. Baseando-se nas propriedades essenciais para a modelagem de um ambiente seguro e nas características peculiares das redes *Ad-Hoc*, temos que a criptografia é o mecanismo básico para se prover segurança. A seguir será abordado o funcionamento das principais técnicas utilizadas atualmente.

4.3.1 Hash – Cadeias de hash

Hash (resumo) é uma função que tem como entrada uma mensagem de tamanho variável e gera na sua saída uma seqüência de tamanho fixo. Esta função é computacionalmente muito difícil de ser invertida, então é impossível de se obter a mensagem original a partir da seqüência gerada pela função. O resultado de uma função *hash* corresponderá a um valor de entrada, e se este valor for alterado, o resultado da função também será diferente, com exceção das colisões, que são possíveis devido ao número de possibilidades na entrada ser muito maior que na saída (AMODEI JUNIOR; DUARTE, 2006). No entanto, utilizando um *hash* de 128 bits, haverá 2^{128} possibilidades na saída, o que torna a probabilidade de colisão desprezível.

Uma cadeia de *hash* é uma seqüência, gerada a partir da aplicação sucessiva da função *hash*, que pode ser um número gerado aleatoriamente. Dado um dos elementos da cadeia de *hash* pode-se garantir que os valores seguintes fazem parte da mesma cadeia, aplicando-se a função *hash* novamente sobre o elemento conhecido um número adequado de vezes. A unidirecionalidade da função *hash* impede que se obtenha os elementos anteriores da cadeia (FERNANDES et al., 2006).

4.3.2 Chaves simétricas

Um dos mecanismos para autenticação de nodos durante a troca de informações são as chaves simétricas. Assim, cada par de nodos que deseja se comunicar deve possuir uma chave secreta, para garantir uma associação com

segurança. Neste mecanismo de segurança existe uma dificuldade na distribuição das chaves secretas, que pode ser feita através de mecanismos de gerenciamento de chaves ou com chaves previamente combinadas. O uso de chaves simétricas tem como vantagem ser mais rápida computacionalmente, não necessitando muito processamento da estação (AMODEI JUNIOR; DUARTE, 2006).

4.3.3 Assinatura digital – Chaves assimétricas

A assinatura digital é outro mecanismo desenvolvido que pode ser utilizado na autenticação de nodos. A assinatura digital consiste resumidamente na obtenção do *hash* de uma mensagem que se deseja transmitir e em seguida, cifrar esse *hash* com a chave privada do nodo emissor da mensagem. Para verificar a autenticidade da mensagem recebida, deve-se gerar um novo *hash* a partir da mesma e comparar com a assinatura digital. Para isso, é necessário decifrar com a chave pública do nodo emissor a assinatura para se obter o *hash* original. Se ele for igual ao *hash* recém gerado, a mensagem está íntegra. Desta maneira, todos os nodos podem verificar que o nodo que enviou a mensagem é realmente quem ele diz ser, já que somente ele pode emitir aquela assinatura digital, pois cada nodo é o detentor da sua própria chave privada.

Esse mecanismo só pode ser usado se cada nodo na rede possuir um par de chaves assimétricas. Deve haver um mecanismo para distribuição de chaves e certificação da associação de uma chave pública a um nodo.

Chaves assimétricas são muito mais seguras que chaves simétricas, pois somente as chaves públicas são divulgadas. Porém, requerem um maior poder de

processamento, o que nem sempre está disponível em dispositivos móveis (AMODEI JUNIOR; DUARTE, 2006).

4.3.4 TESLA

O TESLA é um mecanismo de autenticação baseado em cadeias de *hash* e que necessita uma sincronização fraca entre os relógios dos nodos na rede. O TESLA determina que cada nodo deva gerar uma cadeia de *hash* a partir de uma semente aleatória. Os elementos da cadeia gerada serão utilizados como chaves para a autenticação das mensagens. O nodo emissor deve divulgar o último valor da cadeia de *hash* gerada e, a partir de então, utilizar a cadeia no sentido inverso da geração para autenticar as mensagens. Logo, ao enviar uma mensagem, o nodo emissor deve calcular o tempo médio que a mensagem levará até chegar ao seu destino, divulgando a chave utilizada depois de decorrido esse tempo. Com isto, pode-se garantir que apenas o nodo emissor conhecia a chave TESLA utilizada para autenticar a mensagem recebida. Para verificar se a chave recebida está correta, deve-se aplicar a função *hash* um número adequado de vezes e comparar o resultado com o último elemento da cadeia de *hash* divulgado pelo nodo emissor. Se houver atraso no recebimento da mensagem ou a chave for divulgada antes do recebimento da mensagem, esta é descartada (FERNANDES et al., 2006).

4.3.5 Certificado digital

Certificados digitais são como credenciais, que servem para identificar os nodos na rede. Um certificado digital fornece a garantia de que a chave pública

pertence à entidade identificada no certificado e que esta entidade possui a chave privada correspondente.

Entre os campos obrigatórios do certificado digital, encontra-se a identificação e a assinatura da entidade que o emitiu, as quais permitem verificar a autenticidade e a integridade do certificado. A entidade emissora é chamada de Autoridade Certificadora ou simplesmente AC. A AC é o principal componente de uma Infra-Estrutura de Chaves Públicas e é responsável pela emissão dos certificados digitais. O usuário de um certificado digital precisa confiar na AC (ASSOCIAÇÃO DOS REGISTRADORES IMOBILIÁRIOS DE SÃO PAULO - ARISP, 2006).

4.3.6 Criptografia limiar

O controle das chaves por certificação com assinaturas digitais pode ser acompanhado de um mecanismo de criptografia limiar (*threshold criptography*), que permite a (*t*+1) partes das *n* partes distribuídas nos *n* servidores realizarem o serviço de certificação de forma distribuída, sendo impossível para até *t* partes, inclusive por conspiração, proceder com o serviço. Pode-se dizer então que o esquema é tolerante a *t*, dos *n* servidores estarem comprometidos ou fora de operação naquele instante.

A criptografia por limiar opera numa configuração (*n; t* + 1), onde *n* partes compartilham a operação de criptografia, a assinatura digital, por exemplo, baseada no seu pedaço recebido da chave privada *k* do serviço, sendo suficientes apenas *t* + 1 partes quaisquer para a operação completa e correta do serviço. Há ainda a participação de um dos *n* servidores como uma figura especial, que passa a ser designado combinador, que computa a assinatura final para o certificado com base

nas assinaturas parciais a ele enviadas. Nenhuma informação adicional é visível para o nodo combinador. Esta operação de combinação também pode ser feita em redundância de (*t*+1) servidores a fim de garantir a legitimidade da assinatura e onde qualquer um deles pode verificar a validade da assinatura computada, por meio da chave pública do serviço de certificação (ROCHA; DUARTE, 2006).

4.4 Modelos de confiança e serviços de certificação para Manets

A maior parte das propostas de segurança para protocolos em redes móveis *Ad-Hoc* utiliza uma noção de separação lógica dos nodos da rede em confiáveis e não confiáveis. Desse modo, o uso dos protocolos com segurança geralmente deve ser precedida pelo estabelecimento de uma relação de confiança entre os nodos da rede. Além disso, depois de acordada a confiança entre os nodos, é necessário que esta seja estabelecida formalmente de maneira verificável. Isso pode ser obtido usando, por exemplo, fichas de filiação (*tokens*), compartilhamento de chaves criptográficas ou uso de certificados digitais em esquemas similares ao de infra-estrutura de chave pública.

Mecanismos de certificação geralmente utilizam os padrões Kerberos, X.509 e PKIX. Nestes, duas entidades se autenticam através de uma entidade certificadora. No entanto, este tipo de mecanismo só funciona adequadamente em redes com infra-estrutura definida. Segundo (PUTTINI, 2004) seu funcionamento não é satisfatório nas *Manets* devido aos seguintes aspectos:

- o alto custo para se manter servidores centralizados em grandes redes *Ad-Hoc*;
- servidores AC em *Manets* são vulneráveis a ataques;

- a mobilidade dos nodos demanda a necessidade de constante autenticação, ocasionando problemas de escalabilidade e congestionamento dos servidores AC;
- comunicação *mutli-hop* em meio sem fio propenso a falhas de transmissão ocasionando altas taxas de erro.

Propostas de ACs hierarquizadas e delegações de ACs tentam amenizar, porém não solucionam o problema de robustez do sistema e disponibilidade dos serviços na rede.

Os projetos de serviços de certificação em redes móveis *Ad-Hoc* devem seguir uma abordagem distribuída, auto-organizada e localizada. Duas propostas se destacam como alternativa a esse tipo de serviço, uma com gerenciamento auto-organizado de chaves públicas, proposto por (CAPKUN; BUTTYÁN; HUBAUX, 2007) e outra com autoridade de certificação distribuída (ACD).

A proposta de gerenciamento auto-organizado de chaves públicas consiste em um modelo onde as relações de confiança são estabelecidas entre pares de nodos. Cada nodo gera localmente um par de chaves pública/privada. A chave privada é utilizada para assinar certificados para outros nodos confiáveis, enquanto a chave pública serve para a verificação destes certificados. Um nodo deve possuir diferentes certificados ligando sua chave pública com sua identidade, cada um assinado por outro nodo da rede que o considere confiável. A distribuição do serviço de autenticação é obtida usando repositórios locais de certificados, que armazenam os certificados dos nodos próximos. Esta abordagem apresenta como ponto forte o modelo de confiança ponto a ponto, onde nenhuma entidade externa é necessária, nem mesmo para iniciar o serviço.

A validação dos certificados é realizada estabelecendo-se múltiplas cadeias de certificação a partir da chave pública do nodo que está verificando a validade para a chave pública que está sendo validada. Para avaliar a confiabilidade do processo de validação, são projetadas e utilizadas métricas de autenticação atribuídas a cada cadeia de certificados.

No entanto, esta abordagem, possui vulnerabilidades que impedem sua utilização em ambientes com requisitos de segurança mais restritos. Inicialmente, o uso de métricas de autenticação é útil para detectar nodos mal-comportados que emitem certificados falsos. Porém, esta técnica não é valida para tratar a exposição de certificados válidos de nodos comprometidos, pois as métricas são projetadas para tratar a emissão errônea de certificados e não aqueles que foram gerados corretamente. Outra vulnerabilidade é verificada no que diz respeito a ataques onde um nodo forja diversas identidades para construir uma cadeia de certificação fictícia e distribui estes certificados aos nodos próximos e com isso aumentando os valores aferidos para as métricas de autenticação no processo de avaliação. Com essa técnica, um nodo pode adquirir a confiança de toda a rede, tendo apenas conquistado a confiança de um nodo confiável na rede ou comprometendo um único nodo legítimo na rede (PUTTINI, 2004).

Uma alternativa a este modelo proposto consiste na definição de uma autoridade certificadora distribuída. Nesta abordagem, a chave privada da AC é utilizada para assinar os certificados para todos os nodos da rede. Este certificado pode ser verificado por qualquer nodo com a chave pública da AC. A distribuição das facilidades e serviços providos pela AC é conseguida pelo compartilhamento da chave privada entre os nodos da rede pelo uso de criptografia limiar. Cada nodo da rede mantém uma parte da chave privada da AC. K (uma constante do sistema,

usualmente definida em termos do número médio de vizinhos na rede) portadores das partes da chave privada podem exercer coletivamente a função de AC. Entretanto, a chave privada não pode ser recuperada por nenhum destes nodos. A revogação dos certificados é feita emitindo-se contra-certificados, que também devem ser assinados com a chave privada da AC. Assim, a lista de certificados revogados pode ser mantida localmente por cada nodo pertencente a *Manet*, que fazem parte do *cache* de todos os contra-certificados emitidos. Para que um contra-certificado seja emitido contra um nodo qualquer, os portadores da chave privada devem concordar mutuamente com a decisão.

A auto-organização é obtida definindo-se um protocolo para o estabelecimento dinâmico de coalizões de K portadores da chave privada. Essas coalizões são formadas com intuito de prover três serviços básicos: assinatura de certificados, usada na emissão, renovação e revogação de certificados; emissão de novas partes da chave privada, usadas na iniciação dos nodos que ingressam a rede; e na atualização das partes da chave privada, que deve ocorrer periodicamente a fim de evitar que um adversário possa progressivamente comprometer nodos distintos da *Manet* até quebrar o sistema depois de comprometer todos os nodos do grupo.

Diversas propostas baseadas em ACD foram estabelecidas. Na proposta inicial, os portadores da chave privada eram restritos a um conjunto de nodos “especiais”, que eram previamente iniciados (ZHOU; HAAS, 2007). Logo, o sistema não era completamente organizado, já que era necessário um distribuidor centralizado que entregasse parte da chave privada aos nodos portadores de forma *off-line*. Em uma contribuição posterior, permitiu-se que qualquer nodo detentor de um certificado válido possa participar nos serviços da ACD (KONG et al., 2007).

Neste caso, um nodo que não detenha parte da chave privada pode obtê-la de outros nodos da rede que já possuam partes da chave privada. Este procedimento reduz os requisitos de iniciação da rede, fazendo com que a distribuição centralizada de partes da chave privada seja requerida apenas para a iniciação dos primeiros nodos da *Manet*.

4.5 Segurança dos protocolos de roteamento

A maioria dos protocolos de roteamento atuais para redes móveis *Ad-Hoc* não leva em consideração aspectos de segurança. Nestes protocolos, todos os nodos da rede são considerados confiáveis e não foram levados em conta os tipos de ataques que poderiam afetá-los, especialmente através do uso de nodos maliciosos na rede. Para resolver este problema diversas extensões de autenticação para um determinado protocolo de roteamento foram propostas.

O protocolo AODV possui uma versão modificada, denominada *Authenticated Routing for Ad hoc Networks* (ARAN), que utiliza certificados digitais definidos de maneira particular para autenticar as mensagens do protocolo de roteamento (SANZGIRI et al., 2007). Através da inclusão de assinatura(s) digital(is) em cada mensagem do protocolo é possível verificar a autenticidade da mensagem. Os certificados provêem uma ligação do endereço IP de um nodo e sua chave pública, usada para validar as assinaturas digitais incluídas nas mensagens. Os certificados são fornecidos por um servidor centralizado que possui a confiança de todos os nodos na rede. Como a cada salto as informações nas mensagens do protocolo são alteradas, as mensagens não são assinadas apenas pelo nodo remetente, sendo necessária a assinatura de todo o nodo que estiver na rota para o nodo destino. Isto

causa um grande consumo de recursos computacionais, além de provocar um aumento no tamanho da mensagem a cada salto.

O *Secure AODV* (SAODV) utiliza uma extensão de segurança, que é enviada juntamente com cada mensagem do AODV, portanto a especificação original das mensagens do protocolo é mantida. No SAODV apenas o emitente necessita assinar digitalmente a mensagem. Com relação aos campos mutáveis durante os saltos, são utilizadas cadeias da função *hash* para mantê-los protegidos.

O uso de primitivas de criptografia simétrica é possível ao se estabelecer associações de segurança entre os nodos. Essas associações podem ser derivadas da sincronização dos nodos ou diretamente a partir da mobilidade, possibilitando apenas associações de segurança local. Algumas abordagens também fazem uso de extensões de autenticação de mensagens utilizando criptografia simétrica (PUTTINI, 2004).

O *Secure Routing Protocol* (SRP) foi desenvolvido para dar segurança aos protocolos de roteamento reativos, com enfoque nos protocolos DSR e IERP (PAPADIMITRATOS; HAAS, 2007). No SRP, para cada descoberta de rota, os nodos de origem e destino devem possuir uma associação de segurança entre eles. O protocolo não oferece nenhuma segurança para mensagens de erro de rota, ficando vulnerável a ataques que utilizem este tipo de mensagem.

Nos protocolos *Secure Efficient Ad hoc Distance vector* (SEAD) e Ariadne as chaves de autenticação são extraídas de um protocolo de autenticação por difusão, denominado TESLA. Este protocolo, no entanto, necessita de uma sincronização de relógio entre os nodos na *Manet*, o que nem sempre é possível neste ambiente. No SEAD são propostos mecanismos de segurança com aplicação em protocolos de roteamento do tipo vetor de distância, com análise detalhada do protocolo DSDV,

combinando autenticação por criptografia simétrica e cadeias de *hash* para autenticação de campos mutáveis dos pacotes a cada salto. Já o protocolo Ariadne foi projetado para fornecer segurança em protocolos de roteamento reativos, especialmente o DSR e o IERP (PUTTINI, 2004).

O AODV-S é outra modificação ao protocolo AODV. No AODV-S as mensagens de *Route Request* (RREQ) possuem um campo para identificação do próximo salto e as mensagens de *Route Reply* (RREP) são inundadas na rede, ao contrário do que ocorre no AODV, onde são enviadas por *unicast* (YANG; MENG; LU, 2007). Não existe autenticação para as mensagens do AODV-S, porém uma ficha de filiação é emitida e renovada continuamente para cada nodo, sendo essas fichas usadas para detectar nodos mal-comportados/comprometidos durante a troca de mensagens do protocolo de roteamento. Por trabalhar com *broadcast* todos os nodos que utilizam o AODV-S monitoram promiscuamente as mensagens do protocolo, na tentativa de detectar ataques contra o protocolo de roteamento. Entretanto, o protocolo utiliza o endereço MAC para identificação de cada membro da rede, que pode ser facilmente clonado por algum nodo mal-intencionado.

A tabela 4.1 apresenta um comparativo entre os modelos de segurança para protocolos de roteamento apresentados anteriormente.

Tabela 4.1 – Modelos de segurança para protocolos de roteamento.

Sistema	Protocolo(s) analisado(s)	Alterações no protocolo de roteamento original	Modelo de confiança / gerenciamento de chaves	Sistemas de autenticação	Outras técnicas
ARAN	AODV, DSR	Sim	Distribuição de certificados presumida	Múltiplas assinaturas digitais, com uso de certificação	
SAODV	AODV	Não	Distribuição de certificados presumida	Assinatura digital do emissor, com uso de certificação	Cadeias de *hash* para autenticação dos campos mutáveis
SRP	DSR, IERP	Não	Associação de segurança presumida	Autenticação com criptografia simétrica	
ARIADNE	DSR	Sim	Chaves criptográficas derivadas do TESLA	Autenticação com criptografia simétrica	
SEAD	DSDV	Não	Chaves criptográficas derivadas do TESLA	Autenticação com criptografia simétrica	Cadeias de hash para autenticação dos campos mutáveis
AODV-S	AODV	Sim	Fichas de associação com identificação dos nodos		Monitoração pró-ativa das mensagens e eliminação de nodos mal comportados

4.6 Segurança dos protocolos de autoconfiguração

O projeto e padronização de protocolos de autoconfiguração seguros para redes móveis *Ad-Hoc* ainda estão em fases iniciais. Ao contrário do que ocorre com os protocolos de roteamento seguros que estão em largo desenvolvimento, os projetos de protocolos de autoconfiguração seguros ainda são escassos.

Uma primeira abordagem a respeito do assunto é feita por (BUIATI, 2004). Esta abordagem consiste na adoção de um modelo de confiança desde a entrada de um novo nodo na rede. Os nodos que desejam se juntar à rede necessitam obter a

confiança da rede, através de um certificado, usando os serviços de certificação distribuídos.

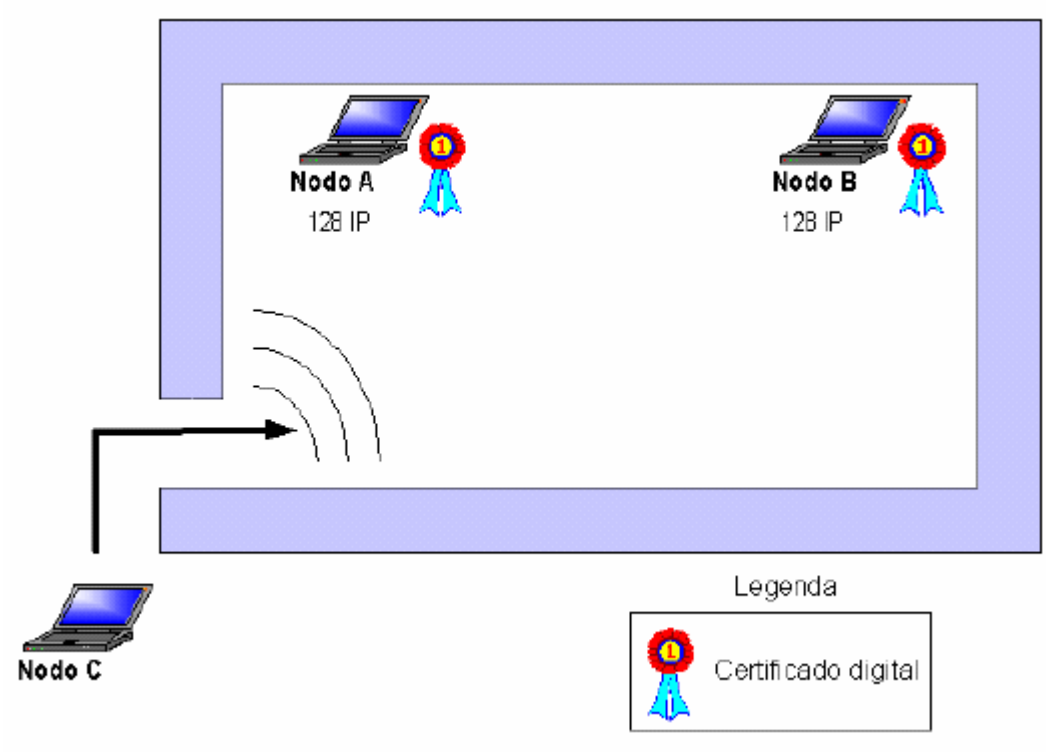

Figura 4.1 – Rede *Ad-Hoc* com dois nodos atendendo requisição de endereço de um nodo sem certificado digital (BUIATI, 2004).

A certificação distribuída é obtida utilizando um modelo baseado na proposta de ACD de (KONG et al., 2007). Porém, no modelo proposto a admissão e renovação de certificados não seguem regras pré-fixadas. Existe um conjunto de políticas configuráveis para emissão, renovação e compartilhamento da chave secreta. Esta política pode ser usada para assegurar que os novos certificados emitidos pelas Autoridades Certificadoras sigam estritamente a mesma verificação de identidade de uma equivalente Autoridade Certificadora centralizada, evitando múltiplas falsas identidades. O modelo proposto ainda possui uma política configurável para a distribuição e manutenção local dos certificados válidos assim

como uma lista dos certificados revogados. Essa política permite que a manutenção dos certificados válidos e da lista de certificados revogados possa ser feita de forma pró-ativa ou reativa, além de um tempo para a manutenção dos certificados válidos. Além disso, o modelo funciona com múltiplas Autoridades Certificadoras Distribuídas com o intuito de suportar perfeitamente a junção de duas partições Manet que utilizam Autoridades Certificadoras diferentes.

Somente após a etapa de obtenção de um certificado ser concluída, o nodo inicia o processo de autoconfiguração de endereço IP. Todas as mensagens do serviço de autoconfiguração devem ser autenticadas utilizando a extensão para autenticação em *Manets* (MAE).

O MAE pode ser utilizado tanto para prover autenticação de mensagens de protocolos de roteamento quanto de autoconfiguração. Na abordagem proposta por (PUTTINI; SOUSA JUNIOR, 2003) são proposto modelos de segurança para os protocolos de roteamento AODV, OLSR, TBRPF e DSR e para o protocolo de autoconfiguração DCDP. O MAE é adicionado a cada mensagem do protocolo e contêm todas as informações de autenticação necessárias para garantir a autenticidade, integridade e não-repúdio para as mensagens que estão sendo protegidas. O MAE é composto de objetos de autenticação. Além de conter o objeto assinatura digital que é obrigatório e autentica todos os campos não mutáveis das mensagens de autoconfiguração, deve conter pelo menos mais um objeto, que pode ser o certificado. O remetente da mensagem deve usar a assinatura digital com a chave privada. A correspondente chave pública está ligada à identidade do remetente no certificado, que está disponível para verificação da assinatura nos nodos que recebem a mensagem. Caso o certificado do nodo não esteja localmente

disponível, o MAE pode conter o objeto CERT, carregando o certificado do assinante do MAE ao longo da mensagem.

Toda a comunicação neste processo, incluindo a autoconfiguração de endereços, ocorre entre vizinhos a um salto de distância e não necessita de um endereço IP previamente configurado. A proposta de autoconfiguração segura tem por base o protocolo DCDP.

Para tratar a fusão e partição de redes, cada partição ou cada rede *Ad-Hoc* possui um identificador único que tem como objetivo detectar a junção de duas ou mais redes. Esse identificador é determinado na inicialização da rede e seu valor é derivado do certificado emitido pelo nodo líder da rede.

A proposta do protocolo é geral e pode facilmente ser utilizada com outros protocolos de autoconfiguração, desde que a certificação dos nodos ocorra antes da execução do processo de autoconfiguração. Para tanto, basta que as mensagens do protocolo de autoconfiguração carreguem em anexo uma MAE com a informação apropriada para autenticá-las (no caso do DCDP, basta uma assinatura digital, já que não há campos mutáveis nas mensagens).

5 CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS

Neste trabalho foi realizado um estudo sobre os protocolos de autoconfiguração de endereços para dispositivos em redes móveis *Ad-Hoc*. Diversos protocolos já foram propostos para a distribuição de endereços aos novos nodos que desejam se juntar a uma rede. Mas devido a alta complexidade de projetar protocolos para operar nestes ambientes, principalmente para tratar questões como o particionamento e fusão de redes, muitos estudos ainda são e serão realizados nessa área.

Outro ponto importante em relação aos protocolos de autoconfiguração para redes *Ad-Hoc* é a segurança. Este assunto é pouco tratado nas abordagens nas que foram tratadas neste trabalho. Isto porque, o projeto e padronização de protocolos de autoconfiguração seguros para redes móveis *Ad-Hoc* ainda estão em fases iniciais.

Este trabalho me proporcionou adquirir um amplo conhecimento sobre redes móveis *Ad-Hoc*, protocolos de roteamento e de autoconfiguração, que certamente poderão ser aplicados no meu futuro profissional ou quem sabe em estudos futuros, visto que essa área está em amplo desenvolvimento devido a sua grande complexidade.

Para trabalhos futuros seria interessante poder contar com uma rede *Ad-Hoc* com um grande números de nodos para testar diversas situações que podem ocorrer na rede para testar o comportamento dos protocolos autoconfiguração principalmente em relação à partição e fusão de redes. Além disso, poder avaliar o desempenho destes protocolos utilizando as métricas mencionadas no decorrer do trabalho.

Outro estudo interessante seria avaliar, conforme a intenção no início do trabalho, a segurança do protocolo de autoconfiguração proposto por (BUIATI, 2004), para verificar o quão o protocolo é realmente seguro.

Por fim, propor e desenvolver um protocolo de autoconfiguração seguro para redes móveis *Ad-Hoc* que cumpra as necessidades levantadas neste trabalho, visto que os trabalhos nesta área ainda são escassos.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO DOS REGISTRADORES IMOBILIÁRIOS DE SÃO PAULO - ARISP. Cartilha de Certificação Digital. Disponível em: <https://www.oficioeletronico.com.br/Downloads/CartilhaCertificacaoDigital.pdf>. Acesso em: 11 dez. 2006.

AMODEI JUNIOR, Aurelio; DUARTE, Otto Carlos M. B.. Segurança no Roteamento em Redes Móveis Ad Hoc. Disponível em: <http://www.gta.ufrj.br/seminarios/CPE825/tutoriais/aurelio/AmDu03.pdf>. Acesso em: 28 dez. 2006.

BELLÉ, Edivane. Avaliação de desempenho em redes móveis sem fio ad hoc. Florianópolis, 2003. 84f. Dissertação (Mestrado) – Universidade Federal de Santa Catarina.

BRIGNONI, Guilherme Venícius. Estudo de Protocolos de Roteamento em Redes Ad Hoc. Florianópolis, 2005. 73 f. Projeto de Conclusão de Curso (Graduação) – Universidade Federal de Santa Catarina.

BUIATI, Fábio Mesquita. Protocolo seguro para autoconfiguração de endereços de redes móveis ad hoc. Brasília, 2004. 117 f. Dissertação (Mestrado) – Universidade de Brasília.

CAPKUN, Srdjan; BUTTYÁN, Levente; HUBAUX, Jean-pierre. Self-Organized Public-Key Management for Mobile Ad Hoc Networks. Disponível em: <http://icwww.epfl.ch/publications/documents/IC_TECH_REPORT_200234.pdf>. Acesso em: 03 jan. 2007.

CORRÊA, Underléa Cabreira. Proposta de um framework de roteamento para redes móveis ad hoc. Florianópolis, 2005. 106 f. Dissertação (Mestrado) - Universidade Federal de Santa Catarina.

CORSON, S.; MACKER, J.. Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations. Disponível em: <http://www.ietf.org/rfc/rfc2501.txt>. Acesso em: 10 set. 2006.

FERNANDES, Natalia C. et al. Ataques e Mecanismos de Segurança em Redes Ad Hoc. Disponível em: <http://www.gta.ufrj.br/ftp/gta/TechReports/FMVC06.pdf>. Acesso em: 28 dez. 2006.

FERNANDES, Rafael de M. S.. Zone Routing Protocol - ZRP. Disponível em: <http://www.gta.ufrj.br/~luish/CPE825/2006/resumos/TrabalhoZRP.pdf>. Acesso em: 19 out. 2006.

JEONG, Insu; CHOI, Hyunjun; MA, Joongsoo. Study on Address Allocation in Ad-Hoc Networks. Fourth Annual Acis International Conference On Computer And Information Science (ICIS'05), Washington, p.604-609, 2005.

JEONG, J. et al. Ad Hoc IP Address Autoconfiguration. Disponível em: <http://tools.ietf.org/wg/autoconf/draft-jeong-adhoc-ip-addr-autoconf-06.txt>. Acesso em: 23 dez. 2006.

KONG, Jiejun et al. Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks. Disponível em: <http://citeseer.ist.psu.edu/kong01providing.html>. Acesso em: 15 jan. 2007.

NESARGI, Sanket; PRAKASH, Ravi. MANETconf: Configuration of Hosts in a Mobile Ad Hoc Network. Disponível em: <http://citeseer.ist.psu.edu/nesargi02manetconf.html>. Acesso em: 15 jul. 2006.

NIKAEIN, Navid; BONNET, Christian; NIKAEIN, Neda. Harp Hybrid Ad Hoc Routing Protocol. Disponível em: <http://citeseer.ist.psu.edu/631906.html>. Acesso em: 11 nov. 2006.

NÚCLEO DE COMPUTAÇÃO ELETRÔNICA - NCE/UFRJ. Redes de Computadores e Sistemas Distribuídos. Disponível em: <http://www.nce.ufrj.br/ensino/posgraduacao/strictosensu/redes.asp>. Acesso em: 15 ago. 2006.

PERKINS, Charles E.; BHAGWAT, Pravin. Highly Dynamic Destination-Sequenced Distance-Vector Routing. Disponível em: <http://www.cs.virginia.edu/%7Ecl7v/cs851-papers/dsdv-sigcomm94.pdf>. Acesso em: 13 nov. 2006.

PERKINS, Charles E.; ROYER, Elizabeth M.; DAS, Samir R.. IP Address Autoconfiguration for Ad Hoc Networks. Disponível em: <http://citeseer.ist.psu.edu/298883.html>. Acesso em: 20 nov. 2006.

PAPADIMITRATOS, Panagiotis; HAAS, Zygmunt. Secure Rotuing for Mobile Ad Hoc Networks. Disponível em: <http://citeseer.ist.psu.edu/papadimitratos02secure.html>. Acesso em: 06 jan. 2007.

PUTTINI, Roberto Staciarini. Um modelo de segurança para redes móveis ad hoc. Brasília, 2004. 191 f. Tese (Doutorado) – Universidade de Brasília.

PUTTINI, Ricardo S.; SOUSA JUNIOR, Rafael T. de. MAE – Manet Authentication Extension for Securing Routing Protocols, 5th IEEE International Conference on Mobile and Wireless Communications Networks (MCWN), 2003.

ROCHA, Luiz Gustavo S.; DUARTE, Otto C. M. B.. Aspectos e Mecanismos de Segurança em Redes Ad Hoc. Disponível em: <http://www.gta.ufrj.br/ftp/gta/TechReports/RoDu02.pdf>. Acesso em: 28 dez. 2006.

SANZGIRI, Kimaya et al. Authenticated Routing for Ad hoc Networks**.** Disponível em: <http://www.cs.ucsb.edu/~kimaya/jsac2005.pdf>. Acesso em: 08 jan. 2007.

SOUSA JUNIOR, Rafael T. de; PUTTINI, Ricardo S.. Principais aspectos na Segurança de Redes de Computadores. Disponível em: <http://www.redes.unb.br/security/lei_info/referencial.html>. Acesso em: 20 dez. 2006.

VAIDYA, Nitin H.. Weak Duplicate Address Detection in Mobile Ad Hoc Networks. Disponível em: <http://www.crhc.uiuc.edu/~nhv/428/weakdad.pdf>. Acesso em: 23 dez. 2006.

YANG, Hao; MENG, Xiaoqiao; LU, Songwu. Self-Organized Network-Layer Security in Mobile Ad Hoc Networks. Disponível em: <http://citeseer.ist.psu.edu/yang02selforganized.html>. Acesso em: 12 jan. 2007.

WEHBI, Bachar. Address Autoconfiguration in Ad Hoc Networks. Disponível em: <http://www.bachwehbi.net/autoconf_report.pdf>. Acesso em: 13 nov. 2006.

WENIGER, Kilian. PACMAN: Passive Autoconfiguration for Mobile Ad hoc Networks. Disponível em: <http://citeseer.ist.psu.edu/weniger04pacman.html>. Acesso em: 23 nov. 2006.

WENIGER, Kilian. Passive Duplicate Address Detection in Mobile Ad Hoc Networks. Disponível em: <http://citeseer.ist.psu.edu/weniger03passive.html>. Acesso em: 18 jul. 2006.

WENIGER, Kilian; ZITTERBART, Martina. Address autoconfiguration in mobile ad hoc networks: current approaches. IEEE Network, Nova Iorque, p.6-11, jul. 2004.

ZHOU, Hongbo; NI, Lionel M.; MUTKA, Matt W.. Prophet Address Allocation for Large Scale MANETs. Disponível em: <http://www.ieee-infocom.org/2003/papers/32_02.PDF>. Acesso em: 08 out. 2006.

ZHOU, Lidong; HAAS, Zygmunt J.. Securing Ad Hoc Networks. Disponível em:

<http://citeseer.ist.psu.edu/zhou99securing.html>. Acesso em: 15 jan. 2007.

ANEXO A: ARTIGO

Um Estudo sobre Protocolos de Autoconfiguração para Redes Móveis Ad-Hoc

Alex Schneider Zis
zis@inf.ufsc.br

Curso de Bacharelado em Sistemas de Informação
Departamento de Informática e Estatística
Universidade Federal de Santa Catarina

Resumo

O principal objeto de estudo deste trabalho são os protocolos de autoconfiguração para redes Ad-Hoc. Estes protocolos distribuem automaticamente os endereços de rede para os dispositivos a fim de estabelecer comunicação entre os mesmos. Mas muitas propostas não tratam da segurança destes protocolos. Logo, tentarei definir aspectos de segurança necessários aos protocolos que atuem neste tipo de ambiente.

Palavras-chave: Ad-Hoc, autoconfiguração, protocolos, redes, segurança

Abstract

The main study object of this work are the autoconfiguration protocols to Ad-Hoc networks. These protocols distribute automaticcally the networks addresses to the devices in order to establish a communication among them. But many proposals do not deal with the security of these protocols. So, I will try to define security aspects necessary to the protocols act in this type of environment.

Keywords: Ad-Hoc, autoconfiguration, protocolos, networks, security

1 Introdução

Observando o grande crescimento nas áreas de comunicação celular, redes locais sem - fio e serviços via satélite juntamente com o comércio de dispositivos que utilizam tais serviços, estima-se que em poucos anos, dezenas de milhões de pessoas terão um laptop, palmtop ou algum tipo de PDA (Personal Digital Assistants). Este crescimento permitirá que em um futuro bem próximo, informações e recursos possam ser acessados a qualquer instante e em qualquer lugar. Independente do tipo de dispositivo portátil, a maior parte desses equipamentos deverá ter capacidade de se comunicar com a parte fixa da rede e, possivelmente, com outros computadores móveis. A esse ambiente de computação dá-se o nome de computação móvel

Este tipo de ambiente, onde os usuários móveis podem realizar comunicações sem nenhum meio físico para acessar recursos distribuídos faz parte da linha de pesquisa de redes móveis sem fio. Basicamente, existem dois tipos de redes móveis sem-fio: as redes Ad-Hoc e as redes infra-estruturadas. Será abordado nesta pesquisa o tipo de rede Ad-Hoc.

A integração de computadores com comunicações e outras formas de tecnologias de informação está criando novas formas de sistemas e serviços de informação distribuída. É o surgimento dos ambientes de computação ubíquos que deverão ser a nova forma de trabalho do próximo século. Este é o cenário altamente desafiador e excitante que motiva a computação móvel. Nesse cenário as redes móveis Ad-Hoc terão uma importância cada vez maior.

Neste contexto tecnológico e móvel, em que a Ciência da Computação e as

Telecomunicações se relacionam, as redes Ad-Hoc ganham força. Entre as características destas redes que contribuem para tal, destacam-se: são de fácil instalação; por não serem dependentes de uma ou mais torres fixas, tornam-se independentes de erros ocorridos nas mesmas; apresentam maior conectividade, uma vez que a comunicação pode ser direta, ou seja, não é obrigada a passar pela torre fixa; além de seu fator sucesso, a mobilidade.

2 Redes Ad-Hoc

Uma rede móvel Ad-Hoc é composta por nodos móveis conectados por interfaces sem fio, que se comunicam através de ondas de rádio. Esses nodos podem formar dinamicamente uma rede sem a necessidade de qualquer infra-estrutura fixa, ou seja, geralmente não existe uma topologia predeterminada e nem um controle centralizado.

Redes móveis Ad-Hoc são também conhecidas como Mobile Ad-Hoc Network (Manet). Numa Manet um nodo só pode se comunicar com os nodos que estão no seu raio de transmissão. Em virtude disto, um pacote destinado a um nodo fora do alcance de transmissão do nodo de origem, deverá passar pelos nodos intermediários, que funcionarão como roteadores até o pacote chegar ao seu nodo de destino.

Neste tipo de rede, os nodos podem se movimentar livremente e se comunicar diretamente com outro nodo que esteja dentro de sua área de alcance. Deste modo, a topologia da rede muda freqüentemente, de forma imprevisível. Isso significa que um computador intermediário I, que num determinado instante faz parte de uma rota entre os nodos A e B, pode não fazer parte dessa mesma rota mais tarde (BELLÉ, 2003).

Características

Redes Ad-Hoc possuem algumas particularidades que as tornam mais complexas que as redes cabeadas e as redes móveis com concentrador de acesso. Essas características são observadas na tabela abaixo (BUIATI, 2004):

Tabela 2.1 – Características das Manets.

Características	Descrição
Topologia dinâmica	Os nodos podem se movimentar livremente, logo a topologia da rede muda constantemente e de forma imprevisível.
Largura de banda restrita	Devido a ruídos, interferências, enfraquecimento de sinal, efeitos dos acessos múltiplos e fatores externos, as redes sem fio possuem uma capacidade significativamente menor do que redes cabeadas.
Economia de energia	Dispositivos móveis geralmente utilizam baterias, portanto para esses aparelhos o consumo de energia é um ponto crucial.
Segurança limitada	Redes móveis sem fio são mais vulneráveis a ataques que redes fixas, o que implica numa maior possibilidade de escuta, invasão e ataques. Por outro lado, por possuir um controle descentralizado, possuem maior robustez, já que os serviços operam de forma distribuída.

Classificação

Existem diversas maneiras de classificar as Manets. As principais delas são quanto a sua comunicação e a sua simetria

Vantagens

A necessidade de instalar redes sem infra-estrutura, a um baixo custo associado com aplicações móveis são as principais vantagens das redes Ad-Hoc. Em relação às redes cabeadas, pode-se observar as seguintes vantagens (BUIATI, 2004): mobilidade, rápida instalação, confiabilidade, conectividade e instalação em locais inadequados para redes cabeadas.

Desvantagens

Apesar das vantagens citadas, alguns problemas e dificuldades podem surgir devido às peculiaridades das redes sem fio. Os maiores problemas relacionados a essa tecnologia são (BUIATI, 2004): localização, interferências, consumo de energia, inexistência de um ponto central, banda passante, interoperabilidade, segurança, roteamento e taxa de erros.

3 Protocolos de roteamento

O mecanismo de roteamento em uma rede é responsável pela entrega dos dados entre os diferentes nodos da rede. O nodo responsável por isso recebe a nomenclatura de roteador. Sua principal função é entregar os pacotes de uma máquina de origem para as máquinas de destino. Quando um nodo origem envia pacotes pra um nodo destino, os dados são encaminhados ao roteador local que os encaminha até o destino final. Esse caminho pode conter vários roteadores. Cada roteador seleciona o próximo salto baseado na sua tabela de roteamento, que contem informações sobre todos os roteadores ao longo da rede, até que o pacote chegue ao seu destino. Para atingir esse objetivo, os roteadores trocam informações entre si, com o intuito de obter um conhecimento parcial ou total da rede, podendo assim selecionar a melhor rota.

Roteamento em redes Ad-Hoc

Existem diferenças entre os algoritmos de roteamento utilizados em redes cabeadas e redes Ad-Hoc. Isso porque, diversos fatores influenciam no desenvolvimento de protocolos para estas redes, como topologia altamente dinâmica, seleção de roteadores e características que podem ser heurísticas na hora de encontrar o melhor caminho para a entrega dos pacotes. Devido à escassez de recursos nas redes Ad-Hoc, é necessário otimizar o uso da banda disponível, motivando o desenvolvimento de algoritmos mais eficientes. Logo, em redes móveis Ad-Hoc todos os algoritmos de roteamento são dinâmicos devido à mobilidade dos nodos.

Diferentes padrões de mobilidade resultam em dificuldades de desenvolvimento de protocolos de roteamento, visto que, alguns nodos podem se movimentar rapidamente, enquanto outros podem ser fixos ou moverem-se lentamente, sendo quase impossível prever o padrão de movimentação de nodos, principalmente em redes de larga escala. Isso pode ocasionar uma sobrecarga na troca de mensagem do algoritmo de roteamento, ocasionando a sobrecarga do uso de banda.

Classificação

A classificação mais utilizada pelos autores é em relação à política de descobrimento de rotas. Nesta classificação, os protocolos de roteamento são divididos em três grupos: Global/Pró-ativos, On-Demand/Reativos e Híbridos. A seguir são descritas as características de cada grupo.

Protocolos Pró-Ativos

Os protocolos pró-ativos tentam avaliar continuamente a disposição dos nodos na rede com o intuito de ao ser solicitado um encaminhamento de dados, já se tenha o conhecimento da rota para o destino. Para tanto, cada host mantêm uma ou mais tabelas com informações referentes à rede e respondem a mudanças na topologia rede propagando atualizações a fim de manter a sua consistência. Estas atualizações são iniciadas por mecanismos de temporização.

A vantagem deste tipo de abordagem é o atraso mínimo para o envio dos dados, pois a rota pode ser obtida diretamente na tabela de roteamento. Entretanto, a atualização constante destas tabelas, causa uma contínua utilização da rede para troca de pacotes e informações de roteamento.

Estes protocolos são escaláveis em relação à freqüência da conexão fim-a-fim. Protocolos pró-ativos não são escaláveis com relação ao número de nodos, mas podem adquirir essa propriedade se for utilizada uma arquitetura hierárquica (CORRÊA, 2005). O funcionamento de alguns protocolos desta categoria é descrito a seguir.

Protocolos Reativos

Nos protocolos reativos a descoberta de rota é feita sob demanda, ou seja, somente quando um nodo deseja se comunicar com o seu destino (NIKAEIN; BONNET; NIKAEIN, 2006) Após a rota ser estabelecida, ela é mantida por um mecanismo de manutenção de rotas até que ela seja inacessível ou não ser mais apropriada.

Nesta abordagem o overhead de comunicação para determinação de rotas é diminuído, economizando banda e energia. Porém, apresenta um maior atraso no encaminhamento dos pacotes.

Devido a sua natureza de flooding, estes protocolos são escaláveis com relação à freqüente mudança na topologia da rede. Mas, não são quanto ao número total de nodos a menos que se utilize uma arquitetura hierárquica. A seguir são descritos alguns destes protocolos.

Protocolos Híbridos

Os protocolos de roteamento híbridos combinam características das abordagens pró-ativas e reativas. Segundo (CORRÊA, 2005), são projetados para aumentar a escalabilidade, permitindo que nodos próximos trabalhem em conjunto com o intuito de formar uma espécie de backbone tentando reduzir o overhead de descoberta de rota.

Esta abordagem pode oferecer o melhor trade-off entre overhead de comunicação e atraso, mas o trade-off pode variar, pois está diretamente ligado ao tamanho e a dinâmica dos grupos formados para o trabalho em conjunto.

Estes protocolos possuem um compromisso com a emissão de escalabilidade com relação ao número total de nodos, à freqüência de conexão fim-a-fim e freqüência de mudança da topologia. O funcionamento de um destes protocolos é descrito na seqüência.

4 Protocolos de autoconfiguração

Todo nodo, para se comunicar em uma rede, necessita de um identificador único, que geralmente é o IP (BUIATI, 2004). Diversos protocolos foram criados com o intuito de fornecer automaticamente esse identificador aos equipamentos conectados à rede, tanto para redes infra-estruturadas como para redes Ad-Hoc.

Autoconfiguração em redes móveis Ad-Hoc

Em redes Ad-Hoc é difícil garantir acesso a um servidor, devido à mobilidade da rede. É desejável que a configuração dos nodos seja feita de forma dinâmica,

automática e de preferência sem intervenção humana. Portanto, os hosts devem cooperar uns com os outros para se configurarem com um endereço único.

Necessidades

Segundo (BUIATI 2004) para se ter um protocolo de autoconfiguração rápido, seguro e confiável, as seguintes características são necessárias:

Tabela 4.1 – Necessidades de um protocolo de autoconfiguração.

Necessidade	Descrição
Unicidade dos endereços IP	Dois ou mais nodos não podem obter o mesmo endereço IP em um determinado instante de tempo.
Correto funcionamento	Um endereço IP é associado a um nodo somente durante o período em que ele estiver na rede. Quando um nodo deixar a rede, o seu endereço IP deve ser disponibilizado a outros nodos que queiram se juntar à rede.
Solucionar problemas relacionados à perda de mensagens	Caso algum nodo falhe ou ocorra perda de mensagens, o protocolo deve agir de forma que não haja dois ou mais nodos com o mesmo endereço IP.
Permitir endereçamento multi-hop	Um nodo só não será configurado na rede com um endereço IP somente se não houver nenhum endereço disponível em toda a rede.
Minimizar o tráfego de pacotes adicionais na rede	O protocolo deve minimizar a troca de pacotes entre os nodos durante o processo de autoconfiguração de um nodo a fim de evitar afetar a performance da rede.
Verificar a ocorrência de solicitações concorrentes de endereço IP	Quando dois nodos solicitam um endereço IP no mesmo instante de tempo, deve realizar um tratamento a fim de evitar que os dois nodos obtenham o mesmo endereço.
Ser flexível ao particionamento e à fusão de redes Ad-Hoc	O protocolo deve manipular a fusão de duas redes distintas Ad-Hoc como também o particionamento em duas ou mais redes.
Realizar o processo de sincronização	O protocolo deve-se adaptar as mudanças da topologia da rede.
Possuir segurança	O protocolo deve se assegurar que somente nodos autorizados e confiáveis tenham permissão para acesso à rede.

Classificação dos protocolos

Os protocolos de autoconfiguração de endereços para redes móveis Ad-Hoc são classificados principalmente em relação ao processo de autoconfiguração. Logo eles podem ser classificados como: independente (Stateless), dependente (Stateful) e híbrido.

Dependentes (Stateful)

Nos protocolos dependentes, cada nodo da rede mantém um conjunto de endereços IP, assim é necessária uma segunda entidade para atribuir um endereço IP a um novo membro da rede.

Independentes (Stateless)

Nos protocolos com abordagem independente nenhuma tabela de alocação de endereços é mantida. Os nodos constroem seus próprios endereços baseados em um número randômico ou no identificador do hardware. Neste processo é necessário um mecanismo de detecção de endereços duplicados para assegurar a unicidade do endereço, denominado Duplicate Address Detection (DAD). Logo, o mecanismo de DAD é a parte mais importante destes protocolos. A configuração dos endereços pode ser realizada antes ou após a execução do mecanismo de detecção de endereços duplicados.

Híbridos

Protocolos híbridos combinam elementos das abordagens independentes e dependentes. Isto resulta em protocolos mais robustos, mas podem resultar em protocolos com maior complexidade e com maior overhead.

5 Segurança dos protocolos

Analisando o funcionamento dos protocolos de autoconfiguração propostos, podemos observar que nenhum tipo de segurança é oferecido, pois todas as abordagens assumem que os nodos são confiáveis. Caso um nodo mal-intencionado venha se juntar à rede, o bom funcionamento da mesma pode ser afetado.

O objetivo deste capítulo é verificar as maneiras de oferecer segurança aos protocolos e analisar as propostas de segurança já desenvolvidas. Para solucionar o problema da segurança em protocolos de roteamento, diversas abordagens já foram feitas. Porém, a segurança dos protocolos de autoconfiguração para redes Ad-Hoc ainda é um tema pouco estudado. Logo, a existência de pouco material sobre o assunto restringiu a análise a apenas um protocolo de configuração, proposto por (BUIATI, 2004) que serviu de base para esse estudo. A intenção inicial era realizar uma série de testes para verificar até que ponto o protocolo era realmente seguro. Contudo, dificuldades em relação ao processo de compilação do código fonte do protocolo com a extensão para autenticação em Manet (MAE) acabaram impedindo a realização dos testes.

Como veremos em seguida, prover segurança em redes Ad-Hoc é algo bastante complexo, já que as essas redes possuem características peculiares, que demandam que as propostas de segurança operem de forma distribuída, auto-organizada e localizada.

Serviços de segurança

Inicialmente, para fornecer segurança a redes sem fio Ad-Hoc devem ser levados em conta os atributos básicos de segurança: autenticidade, confidencialidade, disponibilidade, integridade e não-repúdio. Estas medidas visam evitar o vazamento de informações, fraudes, erros, uso indevido, sabotagens e roubo de informações (BUIATI, 2004).

Ataques à segurança

Os ataques à segurança das Manets podem ser classificados de acordo com tipo de ataque ao fluxo das informações. Neste caso, existem quatro classificações (SOUSA JUNIOR; PUTTINI, 2006): interceptação, modificação, fabricação ou embuste e indisponibilidade ou interrupção.

Mecanismos de segurança

Diversos mecanismos podem ser utilizados para fornecer uma maior segurança para a troca de mensagens de um protocolo para redes Ad-Hoc. Baseando-se nas propriedades essenciais para a modelagem de um ambiente seguro e nas características peculiares das redes Ad-Hoc, temos que a criptografia é o mecanismo básico para se prover

segurança. Além disso, também são utilizados hash, cadeias de hash, assinatura digital, TESLA, certificados digitais e criptografia limiar.

Modelos de confiança e serviços de certificação para Manets

A maior parte das propostas de segurança para protocolos em redes móveis Ad-Hoc utiliza uma noção de separação lógica dos nodos da rede em confiáveis e não confiáveis. Desse modo, o uso dos protocolos com segurança geralmente deve ser precedida pelo estabelecimento de uma relação de confiança entre os nodos da rede. Além disso, depois de acordada a confiança entre os nodos, é necessário que esta seja estabelecida formalmente de maneira verificável. Isso pode ser obtido usando, por exemplo, fichas de filiação (tokens), compartilhamento de chaves criptográficas ou uso de certificados digitais em esquemas similares ao de infra-estrutura de chave pública.

Segurança dos protocolos de roteamento

A maioria dos protocolos de roteamento atuais para redes móveis Ad-Hoc não leva em consideração aspectos de segurança. Nestes protocolos, todos os nodos da rede são considerados confiáveis e não foram levados em conta os tipos de ataques que poderiam afetá-los, especialmente através do uso de nodos maliciosos na rede. Para resolver este problema diversas extensões de autenticação para um determinado protocolo de roteamento foram propostas.

Segurança dos protocolos de autoconfiguração

O projeto e padronização de protocolos de autoconfiguração seguros para redes móveis Ad-Hoc ainda estão em fases iniciais. Ao contrário do que ocorre com os protocolos de roteamento seguros que estão em largo desenvolvimento, os projetos de protocolos de autoconfiguração seguros ainda são escassos.

Uma primeira abordagem a respeito do assunto é feita por (BUIATI, 2004). Esta abordagem consiste na adoção de um modelo de confiança desde a entrada de um novo nodo na rede. Os nodos que desejam se juntar à rede necessitam obter a confiança da rede, através de um certificado, usando os serviços de certificação distribuídos. Somente após a etapa de obtenção de um certificado ser concluída, o nodo inicia o processo de autoconfiguração de endereço IP. Todas as mensagens do serviço de autoconfiguração devem ser autenticadas utilizando a extensão para autenticação em Manets (MAE). A proposta de autoconfiguração segura tem por base o protocolo DCDP. A proposta do protocolo é geral e pode facilmente ser utilizada com outros protocolos de autoconfiguração, desde que a certificação dos nodos ocorra antes da execução do processo de autoconfiguração. Para tanto, basta que as mensagens do protocolo de autoconfiguração carreguem em anexo uma MAE com a informação apropriada para autenticá-las (no caso do DCDP, basta uma assinatura digital, já que não há campos mutáveis nas mensagens).

6 Considerações finais

Neste trabalho foi realizado um estudo sobre os protocolos de autoconfiguração de endereços para dispositivos em redes móveis Ad-Hoc. Diversos protocolos já foram propostos para a distribuição de endereços aos novos nodos que desejam se juntar a uma rede. Mas devido a alta complexidade de projetar protocolos para operar nestes ambientes, principalmente para tratar questões como o particionamento e fusão de redes, muitos estudos ainda são e serão realizados nessa área.

Outro ponto importante em relação aos protocolos de autoconfiguração para redes Ad-Hoc é a segurança. Este assunto é

pouco tratado nas abordagens nas que foram tratadas neste trabalho. Isto porque, o projeto e padronização de protocolos de autoconfiguração seguros para redes móveis Ad-Hoc ainda estão em fases iniciais.

Referências Bibliográficas

BELLÉ, Edivane. Avaliação de desempenho em redes móveis sem fio ad hoc. Florianópolis, 2003. 84f. Dissertação (Mestrado) – Universidade Federal de Santa Catarina.

BUIATI, Fábio Mesquita. Protocolo seguro para autoconfiguração de endereços de redes móveis ad hoc. Brasília, 2004. 117 f. Dissertação (Mestrado) – Universidade de Brasília.

CORRÊA, Underléa Cabreira. Proposta de um framework de roteamento para redes móveis ad hoc. Florianópolis, 2005. 106 f. Dissertação (Mestrado) - Universidade Federal de Santa Catarina.

NIKAEIN, Navid; BONNET, Christian; NIKAEIN, Neda. Harp Hybrid Ad Hoc Routing Protocol. Disponível em: <http://citeseer.ist.psu.edu/631906.html>. Acesso em: 11 nov. 2006.

SOUSA JUNIOR, Rafael T. de; PUTTINI, Ricardo S.. Principais aspectos na Segurança de Redes de Computadores. Disponível em: <http://www.redes.unb.br/security/lei_info/referencial.html>. Acesso em: 20 dez. 2006. 9securing.html>. Acesso em: 15 jan. 2007.