Capítulo

2

Segurança em Redes *Mesh*: Tendências, Desafios e Aplicações

Elisangela Santana Aguiar[1], Antônio Jorge Gomes Abelém[2], Douglas Brito Damalio[2], Rafael Lopes Gomes[2] e Billy Anderson Pinheiro[3].

[1] Programa de Pós-Graduação em Engenharia Elétrica, Universidade Federal do Pará (PPGEE/UFPA)
[2] Faculdade de Computação, Universidade Federal do Pará (FC/UFPA)
[3] Programa de Pós-Graduação em Ciência da Computação, Universidade Federal do Pará (PPGCC/UFPA)

Abstract

Mesh networks are multi-hop wireless networks emerging as a low cost infrastructure for community access networks and digital cities. In this context, support for killer applications such as cooperative services and mobile multimedia applications are the in great demand. This mini-course aims at presenting, in a theoretical way, main problems, solutions and challenges for providing security in wireless mesh networks. The course has three main focuses: the mesh networks contextualization; Security issues in wireless mesh networks, with your challenges and deficiency and; the main proposals found in the literature.

Resumo

Redes mesh são redes em malha sem fio auto-configuráveis e de crescimento orgânico. Recentemente vêm sendo consideradas como infra-estrutura de baixo custo para a construção de redes de acesso comunitárias e de cidades digitais. Neste contexto, é grande o interesse em suportar aplicações multimídia como telefonia IP móvel, e aplicações cooperativas. Este mini-curso tem como objetivo apresentar, de maneira teórica, os principais problemas de segurança em redes mesh e a discussão de soluções propostas para solucioná-los. O curso tem três focos principais: a contextualização das redes mesh; o estado da arte e as questões de segurança em redes em malha sem fio, com seus desafios e deficiência e; as principais propostas encontradas na literatura.

2.1. Introdução

Desde a apresentação, em 1997, do padrão IEEE (*Institute of Electrical and Electronic Engineers*) 802.11, muitas aplicações vêm sendo criadas para esta tecnologia. Seu principal uso é em redes locais e públicas, através de pontos de acesso interligados diretamente a uma rede fixa cabeada tradicional (*wired*), utilizando redes 802.11 infra-estruturadas [GT-Mesh 2006].

Com o avanço das tecnologias sem fio (*wireless*) e o baixo custo destes produtos, o uso de dispositivos móveis que se comunicam através de ondas de rádio está se tornando cada vez maior. Por esta razão, mais estabelecimentos comerciais como *shoppings* e aeroportos estão procurando meios, através da tecnologia sem fio, para oferecer aos seus clientes acesso à Internet banda larga.

Uma dessas novas aplicações são as redes em malha sem fio, mais conhecidas como redes *mesh* (*WMN - Wireless Mesh Networks*). Este novo tipo de rede dispensa o uso da rede fixa entre os pontos de acesso utilizados para realizar o roteamento do tráfego entre si dinamicamente.

As redes em malha sem fio, também conhecidas como redes comunitárias de acesso sem fio, surgiram da constatação de que as redes sem fio poderiam ser aproveitadas para reduzir o custo da "última milha" no acesso à Internet. Através da colaboração entre os nós, um enlace com a rede fixa poderia ser compartilhado, permitindo um uso mais eficiente da banda, evitando o custo da passagem de fios até os usuários finais [Breuel 2004].

Uma rede *mesh* possibilita a comunicação entre diferentes dispositivos. Alguns participantes comporão a estrutura principal da rede, ou seja, formarão o *backbone*, trabalhando apenas como roteadores, e comunicando-se via interface sem fio. Outros nós podem se conectar a estes roteadores por cabos e trabalharem apenas como clientes [GT-Mesh 2006].

As redes m*esh* assemelham-se em muito às redes móveis *Ad-hoc* (*Mobile Ad-hoc networks*, ou MANETs), já que ambas utilizam transmissão sem fio e têm topologia dinâmica variável e de crescimento orgânico. A principal diferença entre as duas tecnologias, no entanto, reside no fato de que nas redes *mesh* os nós clientes não precisam obrigatoriamente ser roteador, possuindo, portanto, menor complexidade nas pontas da rede.

O conceito de redes *mesh* traz consigo uma serie de vantagens que tornam cada vez mais interessantes a sua implantação, como por exemplo:

- Redes de baixo custo: O compartilhamento de recursos faz com que o custo total da rede caia, viabilizando a criação de redes comunitárias [Luiz e Júnior 2005].
- Fácil implantação: Como as redes *mesh* possuem a característica de serem autoconfiguráveis, a sua implantação se torna fácil, pois não são necessárias configurações complexas, nem necessidade de mudança caso algum nó venha a entrar na rede.
- Tolerante a falhas: A capacidade de roteamento dinâmico aliado à existência de múltiplas rotas de acesso a um nó faz com que a rede consiga se recuperar de falhas como a perda de um enlace de comunicação.

- Escalável: Uma das melhores características das redes *mesh* é que sua capacidade de roteamento cresce conforme os nós são adicionados, logo o crescimento das redes, diferente da arquitetura tradicional não é um problema [Harada 2006].

Entretanto, existem algumas desvantagens, a maioria presente ainda pela recente atenção dada as redes *mesh* por parte tanto do mercado quanto da academia, como por exemplo:

- Falta de padronização: Este problema impossibilita até então a adoção da tecnologia em larga escala, espera-se que em 2009 tal problema já esteja solucionado [802.11s 2008].
- Alto preço dos dispositivos: Atualmente o preço dos dispositivos torna o acesso a estes muito restritivos, espera-se que com a padronização da tecnologia os preços tornem-se mais acessíveis.
- Interferência: O uso da faixa, não regulamentada de 2.4 GHz, possibilita a interferência de equipamentos externos à rede que degradam a qualidade desta como um todo [802.11s 2008].
- Baixo *throughput*: Os valores atuais ainda devem ser aprimorados, tendo em mente a possibilidade de crescimento de uma rede *mesh*. Uma alternativa para maximizar o *throughput* é utilizar um canal exclusivo para o tráfego de *backbone*, o que gera um desempenho bastante superior [Kyasanur 2007].
- Falta de segurança: A segurança ainda é um campo aberto no que diz respeito às redes *mesh*, além dos problemas normais de segurança em redes sem fio tradicionais, ainda existe o problema de garantir a privacidade dos dados que estão trafegando entre os nós [Breuel 2004].
- Ausência de qualidade de serviço: Assim como os problemas de segurança, a falta de qualidade de serviço em redes *mesh* é uma linha de pesquisa pouco explorada, tendo algumas propostas para estes problemas, como o algoritmo de roteamento denominado WMR (*Wireless Mesh Routing*) [Xue e Ganz 2005].

Dois tipos de nós podem ser encontrados nas redes *mesh*, no entanto elas aceitam a comunicação com outros tipos de redes e seus respectivos equipamentos [Akyildiz et al. 2005]:

a)Roteadores *mesh* (*MR - Mesh Routers*)

Possuem as mesmas funcionalidades de roteadores convencionais, como *gateway* e *bridge*, porém com o suporte a *mesh*, que provê maior flexibilidade a rede, pois permite a comunicação com outros tipos de redes, como a cabeada, através do uso de múltiplas interfaces. Para que todos estes recursos possam ser executados de maneira satisfatória é necessário um maior poder computacional, necessitando normalmente de um computador para realizar o papel de nó central ou simplesmente fazer uso de um sistema embarcado.

b)Clientes *mesh* (MC - *Mesh Clients*)

Podem realizar o processo de encaminhamento de pacotes entre os demais elementos *mesh* da rede, no entanto não podem exercer as funções de *bridge* ou *gateway*. Em

contrapartida, este tipo de nó apresenta apenas uma interface de rede e um *hardware* bem mais simples, podendo variar desde um *laptop* até um telefone IP (*Internet Protocol*).

Através da combinação desses dois tipos de nós *mesh* juntamente com a utilização de interfaces de redes não *mesh*, podem ser formadas três tipos de arquiteturas [Akyildiz et al. 2005]:

a)Arquitetura Cliente

Apenas nós clientes (*Mesh Clients*) são usados nesta arquitetura. Cada nó faz tanto o papel de cliente como o de roteador, como mostra a Figura 2.1. Eles se comunicam como em uma rede *peer-to-peer* formando uma estrutura muito próxima a de uma rede *ad hoc*, diferindo apenas na utilização de uma única tecnologia de transmissão.

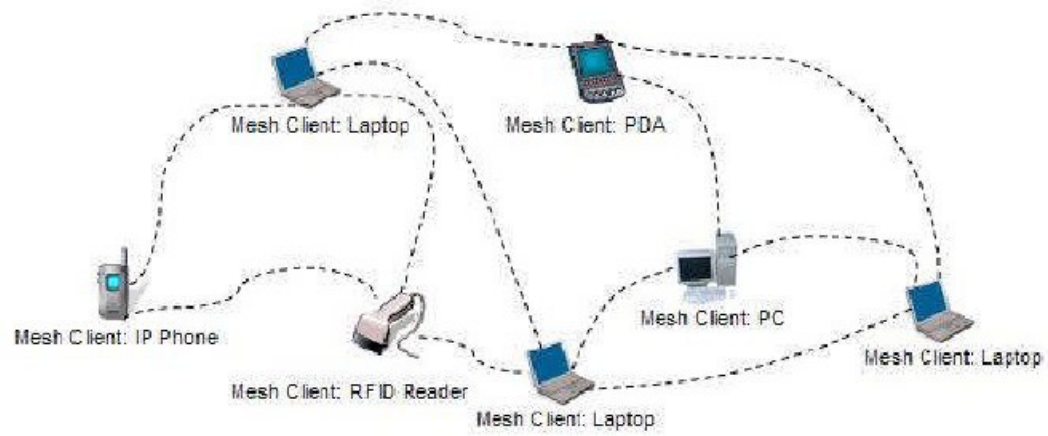

Figura 2.1. Arquitetura cliente (Fonte [Akyildiz et al. 2005])

b)Arquitetura Infra-Estruturada

O *backbone* da rede é composto de roteadores *mesh* que fornecem a infra-estrutura básica para a conexão de clientes não *mesh*, vista na Figura 2.2. Através deste *backbone* formado é possível interligar diferentes redes com diferentes tecnologias de transmissão. Esse é o tipo de rede *mesh* mais usada, pois necessita de modificações apenas nos seus roteadores que normalmente utilizam duas antenas com canais distintos, uma para o *backbone* e outra para atender os clientes.

c)Arquitetura Híbrida

Esta arquitetura faz o uso tanto dos roteadores como dos clientes *mesh*. Ela é a configuração mais completa, fazendo o uso de todas as possibilidades de comunicações que as redes *mesh* oferecem, possibilitando que clientes *mesh* e convencionais tenham acesso ao *backbone mesh* que oferece uma série de interligações com outras redes. A Figura 2.3 apresenta este tipo de arquitetura.

Das arquiteturas expostas cada uma tem seu grau de utilização e aplicação, cabe lembrar que as redes *mesh*, não estão restritas a tecnologia *Wi-Fi (Wireless Fidelity)*, sendo possível a utilização, por exemplo, de dispositivos *Bluetooth* em uma arquitetura cliente *mesh*, assim como vários outros tipos de configurações.

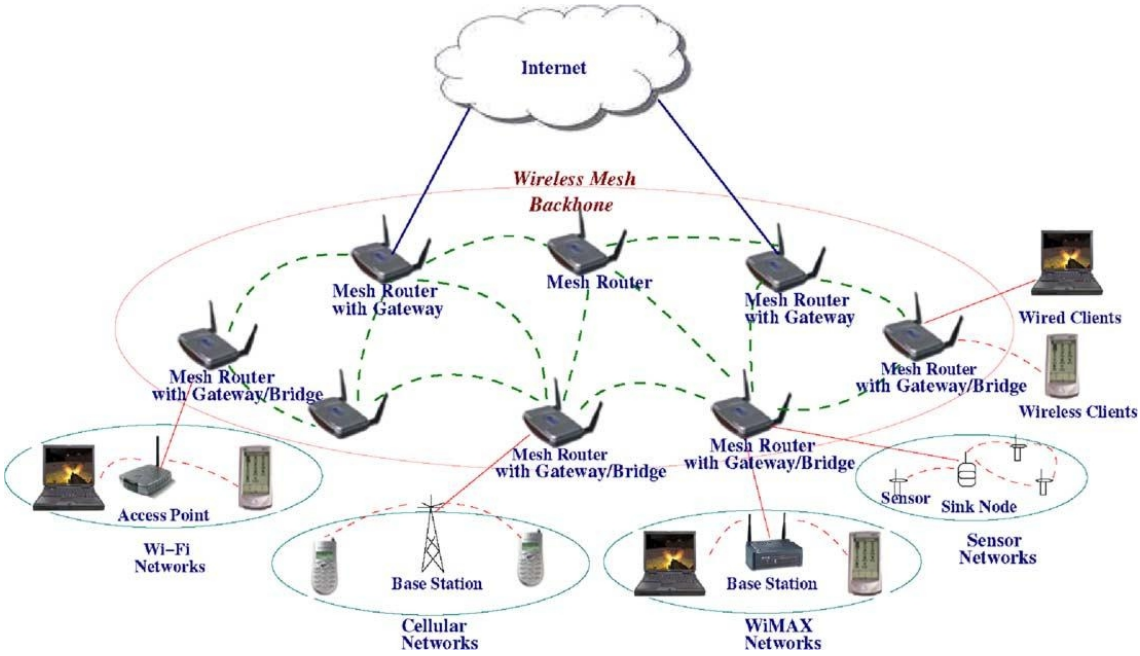

Figura 2.2. Arquitetura Infra-estruturada (Fonte [Akyildiz et al. 2005])

Figura 2.3. Arquitetura Híbrida (Fonte [Akyildiz et al. 2005])

As principais linhas de pesquisas em redes *mesh* estão diretamente ligadas aos principais desafios da tecnologia, sendo eles: a busca pelo melhor roteamento na rede, garantir a segurança e integridade da rede e garantir a qualidade de serviço perante uma topologia dinâmica. Essas abordagens podem ser encontradas em [Faccin et al. 2006].

Considerando a existência de mobilidade em maior ou menor grau e a configuração dinâmica da rede, mecanismos de autenticação serão necessários para garantir o acesso à rede de forma segura e íntegra. Recomenda-se que o mínimo possível seja alterado nas especificações do padrão IEEE 802.11i.

Os mesmos tópicos de segurança identificados nas redes sem fio tradicionais valem para as redes *mesh*, entretanto ganham um nível de dificuldade a mais pela necessidade de serem obtidos salto-a-salto. São três os pontos fundamentais a serem alcançados [Salem e Hubaux 2006]:

- A descoberta de pontos *mesh* corrompidos. Como exemplo dessas corrupções tem-se a possibilidade dos pontos serem removidos, acessados para roubo de informações, acessados com alterações de informações e por último, clonados.
- A definição e o uso de um protocolo de roteamento seguro.
- A definição e a utilização de uma métrica apropriada e justa para redes *mesh*.

Considerando vantagens como baixo custo, fácil implantação e tolerância à falhas, a tecnologia de redes *mesh* é extremamente promissora para implementação de acesso de última milha e capilarização de *backbones*. Entretanto, todo esse potencial não deve ser estudado sem a consideração dos aspectos de segurança envolvidos.

Uma rede *mesh* em seu escopo é semelhante a uma WLAN (*Wireless Local Area Network*), onde a transmissão via rádio pode ser interceptada. Desta forma, as mensagens podem ser interceptadas e alteradas, ou seja, a rede pode ser acessada indevidamente ou sofrer ataques de negação de serviços, DoS (*Denial of Service*).

Em virtude da sua descentralização através de múltiplos saltos, pode-se levar um maior tempo para detectar e tratar um ataque indevido em uma rede *mesh*, permitindo assim ao atacante uma vantagem indesejada para a administração da rede. Conseqüentemente o roteamento efetuado em uma rede *mesh* deve ser seguro.

Os serviços visualizados em redes *mesh* envolvem a privacidade do usuário e a confiabilidade dos fluxos da comunicação. De forma generalizada, assim como nos demais tipos de redes, é importante garantir confidencialidade, integridade, autenticação, controle de acesso e disponibilidade.

O tráfego de qualquer rede pode ser protegido em diferentes camadas (física, rede, transporte e aplicação), entretanto especificamente no caso das redes *mesh*, significa proteger o emlace sem fio, através do uso de diferentes esquemas de encapsulamento de *frames*, diferentes protocolos de autenticação e algoritmos de criptografia.

Os requisitos de segurança a serem atendidos em uma rede *mesh* estão diretamente associados ao seu cenário de utilização, como por exemplo: Domínios administrativos; Tipos de nós envolvidos na rede; Classes dos usuários; Integração a outras redes; etc.

Este capítulo tem como principal objetivo apresentar, de maneira teórica, os principais problemas de segurança em redes *mesh* e a discussão de soluções propostas para solucioná-los, bem como as suas tendências e aplicações.

O restante do texto está estruturado da seguinte maneira. A Seção 2.2 aborda o estado da arte e as questões de segurança em redes em malha sem fio, com seus desafios e metas. A Seção 2.3 aborda os aspectos de roteamento. A Seção 2.4 aborda os aspectos de gerenciamento, apresentando a sua realcção com segurança. A Seção 2.5 versa sobre as principais propostas encontradas na literatura. Para finalizar, a Seção 2.6 apresenta as conclusões, apontando os principais desafios atuais que demandam novas pesquisas na área, bem como suas tendências futuras.

2.2. Segurança em Redes *Mesh*

Para contextualizar o cenário das redes *mesh*, usaremos como base a Figura 2.4 abaixo, representando uma comunicação simples e típica, envolvendo um cliente *mesh* (MC - *Mesh Client*) associado ao ponto de acesso 3 (AP_3 – *Access Point* 3) com saída Internet através do WHS (*Wireless Hot Spot*), passando pelos pontos de acesso intermediários AP_2 e AP_1. Ou seja, as informações de/para o cliente passam por 4 saltos até a Internet.

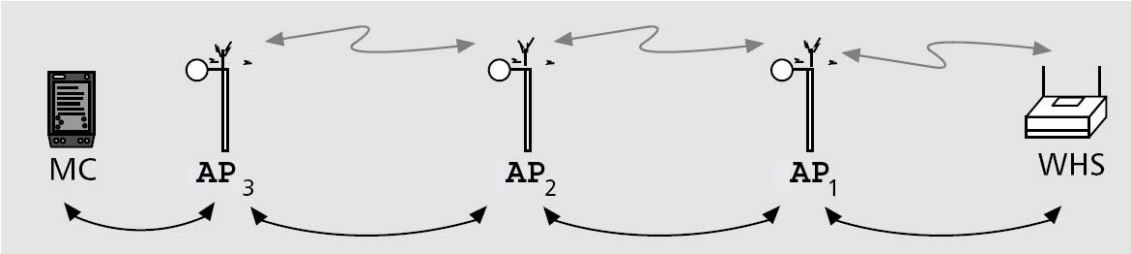

Figura 2.4. Exemplo de comunicação em redes *mesh* (Fonte [Salem e Hubaux 2006])

Baseado nisso, algumas análises podem ser realizadas antes de uma mensagem chegar à rede infra-estruturada:

a)Autenticação

Geralmente acesso à Internet é um serviço pago pelo cliente, conseqüentemente o AP_3 precisa autenticar o MC para executar o faturamento corretamente. Esta autenticação pode ser realizada de modos diferentes, como por exemplo:

- Usando uma conta de bilhetagem temporária (cartão de crédito).
- Através do uso de uma senha pré-definida e compartilhada (se o MC for um cliente da rede associada ao AP_3).
- Usando um serviço similar ao *roaming* da rede celular (se o MC não for um cliente da rede associada ao AP_3).

A autenticação deverá evitar o uso da troca de chaves de criptografia assimétricas pelo MC, uma vez que este faz uso de bateria e necessitaria de um consumo maior para o processamento computational, sendo propenso a ataques de DoS. Isso porque se o protocolo de autenticação necessitar do processamento ou validação de uma chave, poderá ser usado por um invasor que continuamente poderá fazer solicitações de serviços ao MC, levando ao consumo total da sua bateria.

b)Autenticação mútua entre os nós da rede (APs e WHS)

Existe diferença entre a autenticação necessária durante a inicialização ou re-inicialização dos nós e a durante uma sessão estabelecida pelo MC.

A fase de inicialização ou re-inicialização ocorre quando a rede é descoberta pela primeira vez ou quando a rede necessita de uma reconfiguração (por exemplo, um AP foi desligado). No geral, os APs e o WHS são energizados de forma cabeada, sem a restrição do uso de baterias, podendo desta forma, processar autenticação através de chaves criptográficas para autenticação mútua.

A autenticação mútua dos nós durante uma sessão é diferente, pois as mensagens geradas de/para o MC são enviadas através de múltiplos saltos e o uso de chaves

criptográficas para autenticar o receptor/emissor de cada e todo pacote é um processo pesado que introduz atrasos e pode ocasionar alta utilização de recursos de rede. Nesse caso a auetnticação ocorreria a cada AP ou no WHS, dependendo do sentido da comunicação.

c)Integridade das mensagens trocadas

Uma vez que o MC e os nós de rede tenham sido autenticados, é necessário verificar a integridade das mensagens trocadas. Esta análise pode ser feita fim-a-fim, a cada AP ou de ambas as formas.

A partir disso, pode-se dizer que os desafios de segurança em redes *mesh* além de estarem associados ao seu cenário de utilização, referem-se ainda às suas características de topologia/arquitetura de rede, como por exemplo:

- O dinamismo da rede pode provocar alterações na topologia, desta forma qualquer esquema de segurança estático não será suficiente.
- A diferença entre os componentes da rede (clientes e roteadores/APs) representa característica e funcionamento diferente relacionada à mobilidade e consumo de energia, portanto a solução de segurança pode não ser aplicável a ambos.

2.2.1. Tipos de Ataques

Quanto aos possíveis ataques em uma rede *mesh*, pode-se caracterizá-los em dois tipos:

- Ataques externos, nos quais os atacantes que não pertencem à rede *mesh* podem sobrecarregar a rede ou injetar informações erradas.
- Ataques internos, os quais possibilitam ameaças mais severas a partir de um dos nós da rede, o que é mais difícil de ser prevenir.

É válido ressaltar que esses ataques podem atingir diferentes camadas de protocolos. Além disso, pode-se ter ainda ataques passivos, os quais pretendem roubar informação e escutar às escondidas a comunicação dentro da rede, e ataques ativos, os quais modificam as informações. Os principais ataques são:

a)*Easvesdropping*

É um ataque passivo caracterizado pela escuta do tráfego sem modificação dos dados, sendo que o atacante aproveita-se do meio inseguro com o objetivo de roubar informações, podendo descobrir pontos críticos da rede e executar ataques ativos.

Geralmente a proteção contra ataques de espionagem é uma responsabilidade das camadas superiores do modelo OSI (*Open Systems Interconnection*), no entanto, caso não haja criptografia em nível de roteamento, a topologia da rede pode ser facilmente descoberta

b)Ataque bizantino ou alteração de mensagens de roteamento

É um ataque ativo onde, um ou mais nós maliciosos trabalham conjuntamente para gerar problemas como *loops* e falsos pacotes de roteamento, além da escolha de caminhos (rotas) não-ótimos.

Redes baseadas em protocolos de roteamento como OLSR (*Optimized Link State Routing Protocol*) e AODV (*Ad hoc On-demand Distance Vector*) sempre confiam em informações passadas pelos nós vizinhos a rede, ficando suscetível a tomar decisões de roteamento incorretas caso existam nós enviando informações incorretas para a rede.

Este ataque é de difícil detecção, pois para os reais nós da rede, o funcionamento está correto, embora de fato esteja apresentando anomalias do tipo pacotes falsos, alterados e descartados.

c)Estouro da tabela de roteamento

É um ataque ativo que se baseia no fato de protocolos pró-ativos armazenarem todas as rotas anunciadas pelos nós vizinhos.

O objetivo deste ataque é realizar o anúncio de diversas rotas para nós inexistentes, de modo que a tabela de roteamento aumente progressivamente a tal ponto que ela estoure e os nós não consigam mais armazenar as rotas reais.

Este ataque pode ser grave em redes em que os nós possuem recursos escassos, onde a recepção de um número excessivo de mensagens e o estouro de *buffer* são cruciais.

d)Replicação de pacotes

É um ataque ativo que possui dois objetivos principais: ocupar o meio de transmissão e aumentar o desperdício de recursos. Para alcançar este objetivo um nó envia réplicas de pacotes antigos ou atuais para a rede, impedindo a transmissão de outros nós nos momentos em que está enviando as réplicas.

e)“Envenenamento” de c*ache*

Similar ao ataque de estouro de tabela de roteamento, esse ataque aproveita-se de protocolos de roteamento reativos como o AODV, que mantém rotas para nós em *cache*. O objetivo é “envenenar” a *cache* de roteamento realizando anúncios falsos de rotas para nós reais.

f)Inundação de mensagens *HELLO*

É um ataque ativo onde o nó malicioso envia mensagens *hello*, informando que o nó possui enlaces de boa qualidade com determinados destinos, atingindo assim um grande número de nós, que por terem recebido a mensagem, o colocam na lista de vizinhos e podem escolhê-lo para encaminhamento de dados, podendo fazer com que vários nós da rede apontem suas rotas de encaminhamento para um nó inalcansável.

A prevenção para estes ataques e muitos outros que não são tão difundidos, é por exemplo a limitação do número máximo de rotas nas tabelas de roteamento, autorização, assinaturas digitais, uso de múltiplos caminhos e utilização de pacotes de investigação.

Algumas destas técnicas de prevenção já são utilizadas em protocolos de roteamento mais robustos que propõem implementações de segurança. Estes protocolos e as técnicas utilizadas serão descritos no item 2.5.

Baseado na Figura 2.5a abaixo, vislumbra-se dois exemplos de ataques realizados por um mesmo atacante. No primeiro, o AP_2 é invadido e no segundo, acontece um ataque DoS, baseado em inundação (*jamming),* entre o AP_5 e o AP_6.

O atacante corrompendo o AP_2 pode obter seus dados e comprometer a integridade e confidencialidade de todo o tráfego que passe por ele, assim como de todos os clientes

associados aos AP_2, AP_3 e AP_4. Por outro lado, um ataque DoS é um modo muito simples e eficiente para partiiconar uma rede sem fio, forçando a sua reconfiguração.

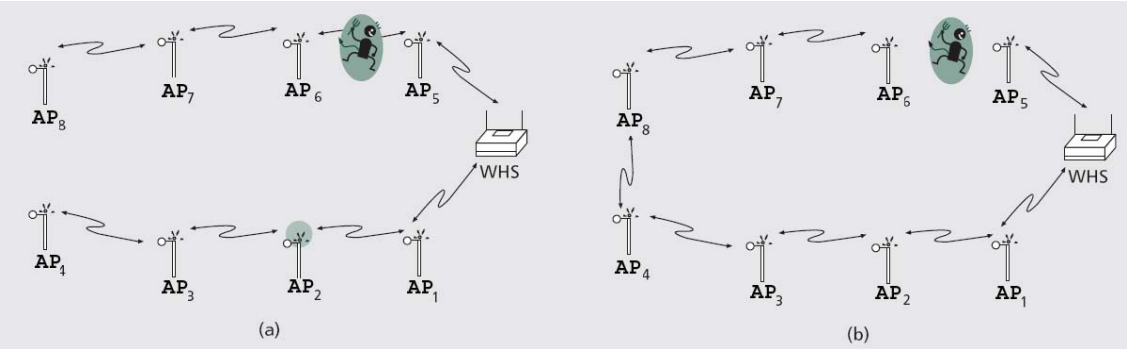

Figura 2.5. Exemplo de ataques em redes *mesh* (Fonte [Salem e Hubaux 2006])

É imperativa a descoberta desses ataques em busca de uma reação de acordo com a sua necessidade. Uma possível reação para o ataque de um AP invadido (Figura 2.5a) pode ser a substituição, pelo operador de rede, por outro íntegro (Figura 2.5b), entretanto, nem sempre isso é possível.

A descoberta e anulação do atacante que esteja inundando a rede podem ser ações trabalhosas, dependendo da capilaridade da rede. Além da dificuldade na localização física e lógica do atacante, ainda que ele seja encontrado, o operador de rede pode não ter permissão para acessar a máquina que está sendo utilizada por ele. Neste caso, a reconfiguração da rede é inevitável.

As mudanças de conectividade podem afetar o desempenho do roteamento na rede e aumentar o número de saltos a partir de um AP de/para o WHS. Por exemplo, na Figura 2.5a, AP_6 estava há dois saltos de distância do WHS e após a reconfiguração da rede, Figura 2.5b, passou a estar há sete saltos.

2.2.2. Desafios

De forma generalizada, são quatro as principais limitações em uma rede sem fio ou em qualquer sistema que tenha dispositivo móvel (*notebooks*, *PDAs*, aparelhos celulares etc):

- Capacidade do processador: costuma ser menor nos dispositivos móveis, tornando o processamento computacional mais lento e demorado.
- Capacidade de bateria: costuma ser limitada, não sendo recomendável o uso dos dispositivos móveis para a realização de processamento de aplicações que necessitem de grande poder computacional.
- Mobilidade: os dispositivos podem, durante sua utilização, estarem em movimento, o que pode produzir uma maior latência na convergência da rede.
- Largura de banda: no geral, costuma ser limitada.

Através da relação dessas limitações com as redes *mesh*, surgem metas a serem alcançadas para superarem os desafios criados:

- Os enalces na rede *mesh* serão propensos a ataques ativos, passivos e distorções de mensagens. Desta forma, os ataques ativos podem resultar na violação da

disponibilidade, integridade e autenticação na/da rede. Os ataques passivos podem comprometer a confidencialidade na/da rede.

- Existe a possibilidade de um nó da rede ser comprometido, em função da falta de proteção física. Conseqüentemente, a rede fica suscetível a ataques maliciosos de fora e de dentro da rede.
- Em função do dinamismo que mudanças freqüentes na topologia da rede podem ocasionar, essa natureza *ad hoc* pode prejudicar a relação de confiança entre os nós da rede.
- Os dispositivos de baixo custo possuem limtações das suas capacidades de armazenamento/memória e de processamento computacional, desta forma, os esquemas tradicionais de segurança não são aplicáveis nas redes *mesh*.

Não se tem como esgotar todos os desafios de segurança em redes *mesh*, entretanto, optou-se pela abordagem de três focos [Salem e Hubaux 2006], conforme mencionado no item 2.1.

Além disso, é válido ressaltar que o assunto segurança em um nível de abstração maior nas redes *mesh* possuem semelhanças com qualquer outro sistema de comunicação e também será abordado abaixo [Siddiqui e Hong 2007].

2.2.2.1. Descoberta de APs corrompidos

As redes *mesh* faezm uso, no geral, de dispositivos de baixo custo que não podem ser protegidos contra remoção e alterções/modificações. Um atacante pode capturar um AP e modificá-lo de diversas formas, ainda que remotamente. Por outro lado, um WHS é assumido como protegido fisicamente.

Desra forma, pelo menos quatro tipos de ataques podem ser visualizados:

- A simples remoção ou substituição de um AP da rede. A proteção física de um AP é crucial. Este ataque pode ser descoberto pelo WHS ou pelos APs vizinhos quando uma mudança incomum na topologia da rede for vista, bem como se a topologia da rede for permanentemente monitorada.
- Um ataque passivo. A obtenção de acesso ao AP capturado sem modifica-lo é um ataque passivo de difícil descoberta, uma vez que nenhuma mudança é realizada no AP. Entretanto, o atacante terá total controle do AP corrompido e poderá ter acesso a todo o tráfego que passar por ele.
- A obtenção de acesso ao AP corrompido com a realização de modificações na sua configuração.
- A clonagem do AP corrompido e a instalação de réplicas em alguns locais estrategicamente escolhidos na rede *mesh*, que permitam ao atacante injetar falsos dados ou desconectar partes da rede, podendo comprometer seriamente o mecanismo de roteamento utilizado na rede.

2.2.2.2. Roteamento seguro através de múltiplos saltos

Através de um mecanismo de roteamento inseguro, o atacante pode alterar a topologia da rede, conseqüentemente afetar ao seu funcionamento. Um ataque desse tipo pode ter orígem “racional” ou “malicioso”.

Por exemplo, um atacante malicioso pode querer dividir a rede, ou isolar um AP ou uma determinada região geográfica coberta pela rede. No caso de um atacante racional, este pode querer forçar o tráfego por um AP específico na rede para monitorar o tráfego de um determinado cliente móvel ou região.

Um ataque ao mecanismo de roteamento inseguro pode ser realizado pelo atacante através de modificações nas mensagens trocadas, inclusive as de controle, alterando assim os seus estados ou ainda o estado de um AP na rede, em especial através de ataques de DoS, os quais representam um modo simples e eficiente para atacar APs corrompidos.

Para prevenir ataques contra as mensagens, pode-se usar protocolos de roteamento seguros, conforme será abordado no item 2.5.2. Se o atacante escolher modificar o estado de um ou mais APs na rede, o ataque poderá ser descoberto e a rede reconfigurada.

2.2.2.3. Justiça

Nas redes *mesh*, todos os APs usam o mesmo WHS como saída de/para a rede infra-estrturada, comumente sendo a Internet. Desta forma, o processamento realizado pelos APs pode variar, dependendo significativamente da sua posição dentro da rede e da própria topologia da rede.

Os APs que estejam há mais de dois saltos do WHS podem ser penalizados em seu acesso, por exemplo os clientes podem não conseguir enviar/receber tráfego, caso não haja nessa rede um mecanismo de qualidade de serviço implementado.

Entreatnto, simplesmente garantir banda para um AP, não é a melhor solução para as redes *mesh*. Considere a Figura 2.6 abaixo, onde uma política justa por AP conduziria os fluxos 1, 2, e 3 cada, tendo a mesma banda compartilhada, sem levar em consideração o número de clientes associados a cada um do APs.

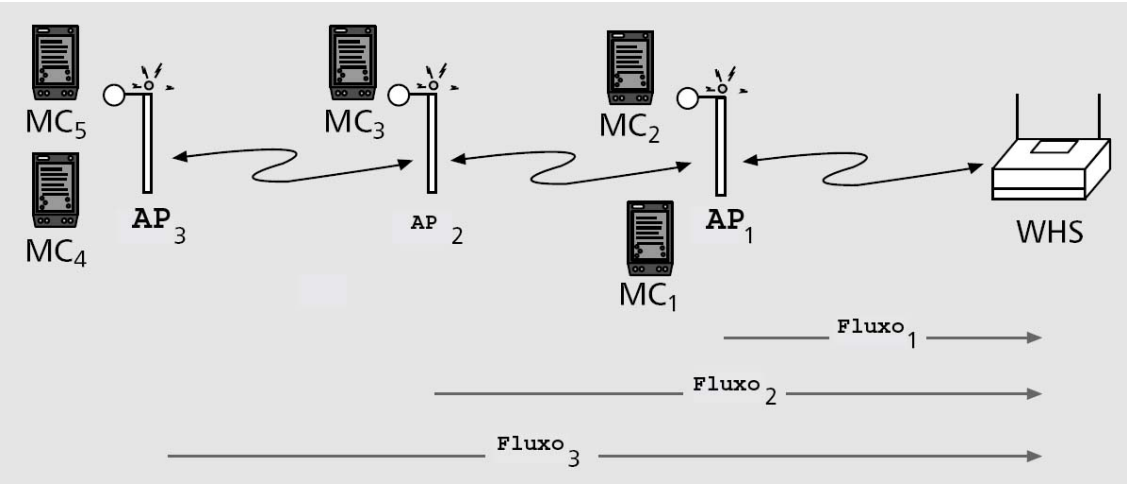

Figura 2.6. Problema de injustiça (Fonte [Salem e Hubaux 2006])

O conceito de justiça é relacionado ao número de saltos entre os APs e o WHS. Isto significa que se o atacante conseguir aumentar o número de saltos entre um determinado AP e o WHS, poderá diminuir a banda compartilhada por esse AP.

Uma possível solução contra este ataque poderia ser a reconfiguração periódica da rede, uma vez que alguns APs são fixos (os que compõem o *backcbone* da rede *mesh*) e possuem um poder computacional maior que os dispositivos dos clientes/usuários, o

operador da rede pode definir, baseado no tráfego da rede, a melhor configuração para esta, definindo as rotas ótimas.

Uma vez que a rede tenha uma configuração ótima, é possível usar algum tipo de mecanismo para assegurar justiça de/por clientes/usuários e otimizar a utilização da largura de banda na rede.

2.2.2.4. Disponibilidade

Disponibilidade assegura o acesso aos serviços de rede ainda que esta esteja sob ataque, não sendo considerado como um problema da importância da confidencialidade e integridade, porém a sua garantia é um assunto relacionado com segurança.

Além disso, os processos exigidos para prevenir os efeitos de perda de disponibilidade estão relacionados aos mecanismos de segurança, uma vez que o conceito básico de disponibilidade é assegurar que os usuários autorizados tenham acesso contínuo à informação do sistema, sem interrupções. A disponibilidade em uma rede *mesh* pode ser atingida através de:

a)Inundação de sinal (*Signal Jamming*)

Nas camadas física e de acesso ao meio, um atacante pode prejudicar a disponibilidade da rede inundando um canal de comunicação utilizado.

b)Ataque DoS/DdoS (*Denial of Service /Distributed Denial of Service*)

Podem ser lançados em qualquer camada de uma rede *mesh* ou ainda através de um atacante externo à rede ou até mesmo a partir de um nó interno.

c)Ataque de esgotamento de bateria

A duração de uma bateria é um dos parâmetros mais críticos para a maioria dos nós de uma rede sem fio. Ataque de esgotamento de bateria também conhecido como *"sleep deprivation attack"* é uma ameaça real e em algumas situações, mas prejudiciais que um ataque DoS.

2.2.2.5. Autenticidade

Autenticidade permite a um nó da rede assegurar a identidade do nó com o qual se esteja estabelecendo uma comunicação. Sem autenticidade, um atacante poderia mascarar um nó da rede, ganhando acesso sem autorização a recursos e informações, interferindo no funcionamento da rede.

Com a implementação de conceitos como sistemas onipresentes, a quantidade de nós em uma rede *mesh* pode ser significativa. Entretanto os mecanismos de autenticação habituais envolvem sistemas centralizados que administram através de restrições (listas de acessos) ou certificados, o acesso na/da rede.

Desta forma, em uma rede *mesh*, a presença de um servidor centralizado, nem sempre é viável ou possível, em função da característica de dinamismo e crescimento orgânico, porém existem algumas formas, como por exemplo: Associação Temporária Segura (*Secure Transient Association*) e *Imprinting*.

2.2.2.6. Integridade

O conceito de integridade assegura que os conteúdos dos dados são preservados durante uma transferência entre emissor/receptor, garantindo desta forma que uma mensagem recebida foi a mesma enviada originalemnte, ou seja, não foi alterada de forma intencional ou não, durante a transmissão.

Os mecanismos comuns para assegurar a integridade de dados geralmente baseiam-se no uso de funções *hash* e de mensagens, criptografia ou uma combinação entre eles.

a)Criptografia e assinaturas digitais

Quando os nós suportam (possuem poder computacional e bateria suficiente) o uso de assinaturas digitais, chaves públicas de criptografia podem ser utilizadas para que os nós gerem a chave privada e através dela troquem mensagens seguras e protegidas.

b)Compartilhando pares de chaves (*Pair-Wise Key Sharing*)

Se o nó tiver limitações de poder computacional e/ou capacidade de bateria, mecanismos com criptografia simétrica também podem ser utilizados.

2.2.2.7. Confidencialidade

O conceito de confidencialidade é a garantia de que dados estejam sendo acessados pelos usuários/clientes que são autorizados a isso. Para garantir confidencialidade, primeiramente é necessário que a autenticidade da informação seja válida. Uma vez que a autenticidade seja garantida, a confidencialidade estará associada a mecanismo que use criptografia.

2.2.3. Metas

Objetivando a segurança em redes *mesh*, alguns atributos são considerados e desejados, como por exemplo: roteamento seguro, sistemas de detecção de intrusão, gerenciamento confiável e de chaves [Siddiqui e Hong 2007].

2.2.3.1. Roteamento seguro

Para garantir disponibilidade da rede, os protocolos de roteamento devem ser robustos contra atques malicioasos e suportar a topologia dinâmica da rede *mesh*. A maioria desses protocolos assume uma colaboração confiável entre os dispositivos envolvidos na comunicação, mas existem várias ameaças de segurança que surgem a partir de falhas nos protocolos e/ou da falta de mecanismos de autenticação. Alguns ataques em protocolos de roteamento são apresnetados na Tabela 2.1 abaixo.

Tabela 2.1. Ataques durante o roteamento (Fonte [Siddiqui e Hong 2007])

Fase do roteamento	Ataques
Descoberta de rotas	Estouro das tabelas de rotas.
Manutenção das rotas	Mensagens de controle com falsas rotas.
Encaminhamento dos dados	Descarte de dados; Consumo de recursos; *Worms* etc.

Há duas fontes de ameaças aos protocolos de roteameno. A primeira a partir de atacantes externos, injetando na rede informações erradas de roteamento, podendo dividir uma rede ou introduzir carga excessiva de tráfego causando retransmissões e um

roteamento ineficiente. A segunda é o tipo mais severo de ameaças, pois é originada a partir de nós comprometidos na própria rede, anunciando informação incorreta aos outros nós.

Para proteger a rede do primeiro tipo de ameaça, os nós podem proteger as informações de rotemaneto da mesma maneira que os dados são protegidos, porém essa defesa é ineficaz contra ataques a partir de servidores corrompidos. A descoberta de um nó comprometido através de informações de roteamento é difícil em uma rede *mesh* em virtude da carcaterística da possibilidade de mudanças dinâmicas na sua topologia.

Uma idéia básica seria transmitir informação redundante por rotas adicionais para a descoberta e correção de erros.

2.2.3.2. Sistemas de Detecção de Intrusão

Algumas das carecterísticas das redes *mesh*, como por exemplo a ausência de um ponto centralizado para gerenciamento e monitoração, não possibilitam que as técnicas tradicionais de detceção de intrusão (*IDS - Intrusion Detection System*) sejam utilizadas.

Sistemas de deteção de intrusão são sistemas de defesa contra atividades hostis em uma rede de computadores e procuram previnir contra ataques que visam comprometer sistemas de segurança [Mishra 2004]. As prevenções envolvem tantos alertas das mais variadas formas como ações executadas pelo próprio sistema de detecção de intrusão como bloqueio de portas ou conexões suspeitas.

Nas redes *mesh* a cooperação é muito importante para suportar as funções básicas da rede. Desta forma mecanismos baseados em *tokens* podem ser utilizados para garantir esta cooperação.

Um sistema de detecção de intrusão coleta informações das atividades de todos os nós e a partir disso, analisa-as para determinar se há qualquer atividade que esteja violando as regras de segurança. Uma vez que seja detectada uma atividade incomum ou que seja conhecida como um ataque, algum tipo de alarme é gerado para alertar ao administrador de segurança. Além disso, o sistema de detecção de intrusão pode iniciar uma resposta à atividade maliciosa.

Para as redes *mesh*, uma solução de detecção de intrusão pode depender da própria infra-estrutura de rede, podendeo ainda ser classificada como:

a)Stand-alone

O sistema de detecção de inrusão roda de forma independente e isolada em cada nó para a detecção de intrusões.

b)Distribuído e cooperativo

Todo nó participa da detecção de intrusão e através de um agente que é executado em todos eles, identifica possíveis intrusões e inicializa respostas a elas.

c)Hierárquico

Nós *"Clusterheads"* atuam como pontos de controle para prover a funcionalidade aos seus nós associados.

Um sistema de detecção de intrusão pode ainda ser dividido em três categorias:

a)Detecção de Anomalias

Em um sistema de detecção de anomalias é criado um perfil de uma atividade normal do sistema. Qualquer atividade do sistema que estiver fora do perfil é tratada como uma possível intrusão. A grande desvantagem para redes sem fio é que o perfil de atividades deverá ser constantemente atualizado e as discordâncias do perfil criado, terão de ser resgistradas, isto pode causar uma sobrecarga em dispositivos com baixo poder de processamento.

b)Detecção de abusos

Na detecção de abusos, as decisões são tomadas baseadas em uma base de conhecimento de um modelo de processo intrusivo e vestígios de prováveis intrusões.

c)Detecção baseada em especifidades

Sistemas de detecção de intrusão baseados em especificidades definem uma série de diretivas que descrevem o correto funcionamento de um determinado programa ou protocolo e os monitora de acordo com as diretivas. Esta técnica é a que provê maior capacidade de detecção prévia de ataques e o menor número de falsos positivos.

As formas de respostas a intrusões para redes *mesh* dependem do tipo de intrusão, dos protocolos de rede utilizados e aplicações em uso na rede. Algumas respostas são: reinicialização dos canais de comunicação entre nós, identificação de nós comprometidos da rede e reorganização da mesma, notificação de usuários para que os mesmos possam realizar suas próprias investigações e tomar as devidas ações e como última ação do IDS, pode-se reiniciar a a requisição de autenticação de todos os nós da rede.

2.2.3.3. Gerenciamento Confiável e de Chaves

Confidencialidade e segurança são dois conceitos mutuamente dependentes que não devem ser separados. As redes *mesh* baseiam-se em relações de confiança entre seus nós vizinhos. Como o ambiente global é cooperativo, estas relações de confiança são extremamente suscetíveis a ataques. Além disso, a ausência de infra-estrutura de confiança fixa, recursos limitados, meio sem fio compartilhado e vulnerabilidades físicas, torna o estabelecimento de uma confiança inviável.

Desta forma, nas redes *mesh* as caracteísticas de gerenciamento confiável em oposição aos mecanismos tradicionais e centraliozados, são: confiança em evidências incertas e incompletas, confiança na troca de informações das localidades, computação distribuída e avaliação de confiança empregada individualmente.

Para superar estes problemas, confidencialidade está sendo estabelecida em redes *mesh* usando por exemplo a pré-configuração dos nós com chaves criptográficas ou a presença de uma autoridade certificadora.

Todos os esquemas baseados em chaves de criptografia demandam um serviço de gerenciamento de chaves, sendo responsável por manter o histórico das relações entre as chaves e os nós, estabelecendo uma confiança mútua e comunicação segura entre os nós.

Gerenciamento de chaves através de um canal de comunicação inseguro possui um risco alto a ataques. Existem três tipos de gerenciamento de chaves que podem ser aplicados em redes *mesh*: uma autenticação via certificado, árvores de certificação e a combinação de ambos.

2.3. Aspectos de Roteamento

Os protocolos de roteamento para redes *mesh* têm papel importante no que diz respeito à comunicação entre as partes envolvidas. Este tipo de rede é caracterizado pela presença de nós moveis e fixos interconectados através de enlaces sem fio formando uma rede de múltiplos saltos.

Alguns pontos importantes devem ser considerados para que estes protocolos sejam desenvolvidos de uma forma a aproveitar as características da topologia em questão. Estes pontos incluem topologias dinâmicas – nós podem se mover livre e randomicamente dentro de uma mesma rede ou entre redes; recursos limitados como banda (na realidade, as redes sem fio ainda estão trabalhando nas faixas de MHz) e energia (equipamentos portáteis são operados a bateria); segurança – nós não participantes da rede podem "escutar" as transmissões; e escalabilidade – devido ao alto *overhead* advindo do grande número de nós presente na rede [Held 2005].

Observa-se que, para que os protocolos de roteamento ofereçam um serviço de qualidade, eles devem considerar métricas multidimensionais [Faccin et al. 2006] para que a melhor rota seja selecionada de acordo com a aplicação e cenário onde os mesmos estão atuando.

É importante frisar que as redes *mesh* tiveram suas origens nas redes *ad hoc* e devem ser capazes de se auto administrar, configurar e restabelecer no caso de perda de enlaces [Bruno et al. 2005]. Portanto, este tipo de rede demanda protocolos de roteamento que, também, tenham estas características.

De acordo com [Murthy e Manoj 2004], os protocolos podem ser classificados considerando vários aspectos que podem ser baseados:

a)Nos mecanismos de atualização de informação.

b)No uso de informação temporal.

c)Na topologia.

d)Na utilização de rotas específicas.

A classificação utilizada neste mini-curso é a baseada nos mecanismos de atualização de informação. Neste tipo de classificação os protocolos são divididos em roteamento:

a)Pró-ativo

Onde os nós trocam tabelas de roteamento periodicamente mantendo informações sobre toda a topologia com cada nó conhecendo o menor caminho para cada outro nó da rede. Os protocolos mais comumente utilizados são o DSDV (*Destination Sequenced Distance Vector*) [Perkins 1994] e o OLSR (*Optimized Link State Routing*) especifidaco pela [RFC3626 2003].

b)Reativo

Com as rotas sendo estabelecidas sob demanda, ou seja, rotas são criadas quando solicitadas pelo transmissor sendo o DSR (*Dynamic Source Routing*) [Song 2005] e o AODV (*Ad Hoc On-Demand Vector*) definido pela [RFC3561 2003] os mais utilizados.

c)Híbridos

Que combinam as melhores características dos protocolos pró-ativos (roteamento dentro da mesma zona) e reativos (roteamento para fora da zona). Como exemplo deste tipo de roteamento tem-se o ZRP (*Zone Routing Protocol*) [Haas 1997] [Haas e Pearlman 1998] e o CEDAR (*Core-Extraction Distributed Ad hoc Routing*) [Sivakumar et al. 1998].

A maioria dos protocolos de roteamento nas redes *mesh* funciona de forma cooperativa onde os nós conhecem seus vizinhos. Com isso, aplicações maliciosas podem parar a rede facilmente inserindo atualizações erradas nas tabelas de roteamento.

As soluções de protocolos de roteamento seguros são específicas para combater ataques ou grupo de ataques, classificando-se em soluções baseadas em criptografia e/ou em adaptações de protocolos existentes.

Para aumentar a segurança das redes *mesh*, duas estratégias precisam ser adotadas: embutir mecanismo de segurança nos protocolos de roteamento; e desenvolver sistemas de monitoramento e resposta perante descobertas de ataques e quedas de serviços.

2.3.1. Protocolos de Roteamento não seguros

Para cada necessidade pode-se empregar um protocolo de roteamento e esta característica deve-se ao fato de que um único protocolo não consegue ajustar-se a cenários diferenciados, muito menos a vários padrões de tráfego.

Protocolos de roteamento pró-ativos adequam-se muito bem em redes sem fio de banda larga, baixa escalabilidade e de considerável mobilidade dos nós, enquanto que protocolos reativos adequam-se melhor em redes de banda estreita, alta escalabilidade com baixa mobiliade de nós. Já os protocolo híbridos procuram adequar-se a redes em ambas as situações.

Dentre as soluções de protocolos de roteamento existentes para redes *ad hoc* e redes *mesh* encontram-se como propostas os protocolos OLSR, DSR, DSDV, AODV, ZRP e ZHLS (*Zone-Based Hierarchical Link State*) [Joa et al. 1999].

2.3.1.1. OLSR

Este protocolo é uma versão melhorada do clássico algoritmo de estado de enlace para atender as necessidades de redes sem fio. Assim, o protocolo herda a estabilidade do algoritmo clássico com a vantagem de ter as rotas disponíveis imediatamente devido sua natureza pró-ativa.

O ponto principal deste protocolo está na utilização dos MPRs (*Multipoint Relays*) que é um subconjunto de nós vizinhos selecionados responsáveis pelo encaminhamento de tráfego de controle. Com isso, o *overhead* proveniente do tráfego de controle é reduzido se comparado com o mecanismo de inundação clássico onde cada nó retransmite cada mensagem quando o mesmo as recebe.

Os nós MPRs devem anunciar para a rede, em suas mensagens de controle, que são deste tipo com o intuito de informar sua alcançabilidade aos nós que o elegeram como MPR. Neste protocolo, somente os nós MPR podem gerar informação de estado de enlace, minimizando, assim, o número de mensagens de controle na rede.

Como um nó MPR deve reportar sobre somente os enlaces entre ele mesmo e os nós que o selecionaram como nó MPR, isso leva a outra vantagem deste protocolo se

comparado ao algoritmo de estado de enlace clássico, já que as informações de estado de enlace parciais encontram-se distribuídas na rede. Esta informação é usada para os cálculos de melhor rota em termos de números de saltos.

O OLSR define três tipos básicos de mensagens:

a)*Hello:* transmitidas entre os vizinhos e são utilizadas para obter informações de enlace, detecção de vizinhos e sinalização MPR;

b)*Topology control:* são sinalizações (anúncios de estado de enlace) feitas pelo OLSR. A transmissão destas mensagens é otimizada de várias formas usando MPRs;

c)*Multiple interface declaration:*– responsável em informar sobre a presença de mais de uma interface em um nó. Essas mensagens listam todos os endereços IP usados por este nó.

2.3.1.2. DSR

É um protocolo de roteamento pró-ativo, onde um remetente determina a seqüência completa das estações responsáveis pelo transporte de pacotes até um destinatário.

Diferente dos protocolos existentes em redes *ad hoc*, o DSR não realiza freqüentemente os anúncios de rota. Ao invés disso, quando uma estação necessita de uma rota para um destino, ela faz uma consulta nas informações em *cache* e nos resultados obtidos com o protocolo de descoberta de rotas.

Assim, para enviar um pacote para outra estação, o remetente constrói uma "rota de origem" no cabeçalho do pacote, informando o endereço de cada estação, através do qual o pacote será encaminhado ordenadamente até alcançar o destino.

O remetente então transmite o pacote no enlace sem fio para a estação que estiver a distância de um salto e identificada na "rota de origem".

Quando esta estação recebe o pacote, se ela não for o destinatário do pacote, ela simplesmente retransmite para a próxima estação identificada.

Cada nó móvel da rede armazena em *cache* as rotas que foram descobertas. Se a rota não for encontrada em *cache*, o remetente então usa o protocolo de descoberta de rotas, que permite que o nó remetente envie uma solicitação de rota e fique recebendo pacotes de outros nós até que a informação de rota retorne.

O nó poderá armazenar o pacote original em ordem para transmitir enquanto a rota estiver em processo de descoberta, ou descartar o pacote.

2.3.1.3. DSDV

É um protocolo de roteamento pró-ativo que tenta manter a simplicidade do algorítimo de vetor distância e ao mesmo tempo corrigir dois problemas que impediam seu uso nas redes *ad hoc*: o primeiro problema é a possível criação de *loops* pelo algoritmo de vetor de distância. Já o segundo é a necessidade de um ajuste mais rápido da topologia da rede a medida que seus nós se movem.

O DSDV possui o atributo de número de seqüência, para cada entrada na tabela de roteamento do protocolo RIP (*Routing Information Protocol*) convencional. Através da utilização deste novo atributo, os nós móveis podem identificar que a informação de uma rota está desatualizada evitando a formação de *loops* no roteamento.

Cada nó em uma rede *ad hoc* mantém uma tabela que lista todos os possíveis destinos dentro da rede. Cada entrada nesta tabela contém o endereço de um possível destino, a menor distância conhecida (normalmente em número de saltos) para aquele destino e o endereço do nó vizinho que será o primeiro salto neste caminho mais curto para aquele destino.

A distância para o destino é conhecida como *metric* nas entradas da tabela. Quando um nó estiver realizando o roteamento de um pacote para algum destino, o nó transmite o pacote para o roteador (nó) vizinho indicado, e cada roteador usa sua própria tabela para realizar o próximo salto do pacote em busca do seu destino.

2.3.1.4. AODV

Este protocolo combina características do DSR (mecanismos sob demanda de descobrimento e manutenção de rotas) e do DSDV (roteamento salto a salto, números de seqüência e atualizações periódicas) [Broch et al. 1998].

Quando um nó deseja enviar dados a um destino e ainda não tem rotas para o mesmo, o nó fonte inicia o processo de descoberta de rota. Via *broadcast*, o pacote RREQ (*Route Request*) é enviado a todos os vizinhos do nó fonte e cada vizinho, por sua vez, encaminha aos seus vizinhos até que o destino ou nó intermediário, que contenha esta rota, seja alcançado.

Para evitar *loops* e ter rotas recentes, o AODV utiliza números de seqüência. Cada nó tem seu próprio número de seqüência e uma identificação de *broadcast* – incrementado para cada RREQ gerado pelo nó – que vão juntos com o número de seqüência mais recente do destino, distinguindo, assim, cada RREQ.

Desta forma, os nós intermediários somente respondem ao RREQ se tiverem uma rota com número de seqüência maior ou igual ao presente no RREQ. Durante o encaminhamento do RREQ, cada no intermediário armazena em sua tabela de rotas o endereço do vizinho do qual ele recebeu o RREQ primeiramente com o objetivo de descartar copias do mesmo RREQ e estabelecer um caminho reverso até a fonte.

Uma vez que o RREQ chega ao destino/nó intermediário, este envia um pacote RREP (*Route Reply*) ao vizinho do qual ele recebeu o primeiro RREQ e este processo continua até que RREP chegue à fonte.

O protocolo AODV periodicamente envia mensagens *hello* para saber se há novos nós na sua vizinhança e estas mensagens podem ser utilizadas com o objetivo de manter a conectividade local.

2.3.1.5. ZRP

É um protocolo de roteamento híbrido, que faz uso das vantagens de um protocolo pró-ativo e das vantagens de um protocolo reativo.

A especificação do protocolo não define se há um protocolo pró-ativo ao qual o ZRP herda peculiaridades, mas é possível identificar algumas características próprias como o fato de necessitar que sejam enviadas mensagens periódicas para manter o roteamento local; suporte a dispositivos de fabricantes diferentes, desde que cada um tenha um IP único associado a cada interface de rede.

O protocolo é naturalmente distribuído e não depende de uma unidade central e ainda existe a prevenção de *loops* no roteamento através de número de seqüência e de endereço de origem.

2.3.1.6. ZHLS

É um protocolo de roteamento híbrido onde a rede é dividida em zonas sem sobreposição. Ao contrário de outros protocolos hierárquicos, não existe um representante da zona (*zone-head*).

Define dois níveis de topologia: nível do nó e nível da zona.

A topologia de nível do nó informa como os nós de uma zona estão conectados fisicamente entre si. Um enlace virtual entre duas zonas existe se pelo menos um nó de uma zona está fisicamente conectado a um nó de outra zona.

A topologia de nível da zona informa como as zonas estão conectadas. Existem dois tipos de pacotes de estado de enlace (LSP – *Link State Packet*), que são o "*node LSP*" e "*zone LSP*".

O "*node LSP"* de um nó contém a informação dos seus nós vizinhos e é propagado dentro da sua zona, enquanto que o "*zone LSP"* contém a informação da zona e é propagado globalmente.

Desta forma cada nó possui um conhecimento total sobre a conectividade dos nós da sua zona e somente a informação da conectividade zonas do resto da rede. Então dado a identificação da zona e do nó de um destino, o pacote é roteado baseado na identificação da zona até que este chegue na zona correta, quando então é roteado baseado na identificação do nó.

O par <id. zona, id. nó> do destino é suficiente para o roteamento, portanto é adaptável para mudanças de topologia.

2.4. Aspectos de Gerenciamento

As facilidades proporcionadas pelas redes tendem a estimular o crescimento das mesmas, provendo necessidades de manutenção e planejamento. Em um ambiente com poucas máquinas conectadas em rede, uma única pessoa é capaz de gerenciá-las. Mas, considerando um ambiente onde a rede esteja distribuída entre várias salas, ou até mesmo prédios distintos, a manutenção torna-se mais difícil consumindo tempo e recursos.

Em redes de longa distância, a tarefa de gerenciamento é inerentemente mais complexa e indispensável, uma vez que cobre uma grande área geográfica e envolve um grande número de equipamentos e usuários dependentes de seus serviços. Além disso, com a grande utilização e a heterogeneidade das redes, tem havido a necessidade de um esquema que ofereça soluções de gerenciamento de redes coerentes e estruturadas, permitindo o monitoramento e o controle de equipamentos [Kurose 2006].

Do mesmo modo que ocorre com os demais temas da área de redes, há diferentes possibilidades para o gerenciamento, organizadas na forma de arquiteturas de gerenciamento onde são especificadas e propostas por organismos de padronização.

O gerenciamento de redes *mesh* é uma tarefa significativamente mais complexa do que controlar redes com infra-estrutura cabeada, também é diferente de gerenciar redes puramente do tipo *ad hoc*. As redes *mesh* por serem um tipo híbrido de rede, com

características de redes infra-estruturadas e *ad hoc*, não são atendidas por completo pelas ferramentas existentes, pois estas são usualmente desenvolvidas frente a um conjunto de requisitos pertencentes ao tipo de rede infra-estruturadas ou do tipo *ad hoc* [Karpijoki 2001].

Como breves exemplos destas diferenças nas características, as redes infra-estruturadas possuem topologias totalmente fixa, e com enlaces que sofrem pouca variação de desempenho, por outro lado, as redes *ad hoc* possuem uma forte limitação no fornecimento de energia por não terem nenhuma ligação com alguma infra-estrutura fixa e também devido a grande mobilidade dos nós.

Diferentemente das redes cabeadas, as redes *mesh* ainda não tem um padrão público definido pelos órgãos reguladores. Como conseqüência, não existe uma grande quantidade de ferramentas de gerência voltadas para redes *mesh*. As ferramentas encontradas são desenvolvidas normalmente por fornecedores que buscam atender as suas soluções *mesh* específicamente, como [MotoMesh 2008].

Outro ponto negativo, é que essas ferramentas específicas desses fornecedores, não possuem código aberto, ou até mesmo uma licença GPL (*General Public License*) que permita a realização de adaptações necessárias a outras redes.

Um importante problema em redes *mesh*, está relacionado ao processo de coleta de dados, este processo causa sobrecarga (*overhead*) [Badonnel 2005]. Redes que utilizam enlaces segundo o padrão IEEE 802.11 [802.11 2007], possuem uma limitada largura de banda, que pode sofrer grandes variações e, portanto, as mensagens de gerência não devem consumir uma porção significativa do meio de comunicação.

A solução mais simplista para extrair as informações da rede, considerando que as ferramentas de gerência serão implementadas ao nível de aplicação, é acessar individualmente cada ponto da rede e, assim, recolher os dados desejados.

Esta técnica pode resultar em uma utilização ineficiente dos recursos de comunicação da rede, levando a uma grande sobrecarga. A quantificação deste impacto negativo gerado pela troca de mensagens torna-se difícil de predizer ou controlar, pois a qualidade dos enlaces de comunicação pode variar de uma maneira muito dinâmica. Simplesmente impor um limite de vazão no tamanho das mensagens pode não ser uma solução viável.

Uma rede *mesh* tem como vantagem possuir na sua topologia pontos fixos, que formam um *backbone* (infra-estrutura de comunicação utilizada pelos clientes). Ou seja, a maior parte da comunicação da rede passa, ou deve passar, por estes equipamentos. Outras características adicionais destes pontos são, em sua maioria, alimentação irrestrita de energia, posicionamentos fixo, e acesso de gerência por um terminal remoto através de múltiplos saltos.

Uma questão que deve ser levantada para o gerenciamento de redes *mesh* é relativa a tarefa de monitoramento, o que deve ser observado é a propriedade temporal da informação [Duarte 2008]. Esta propriedade é determinada pelos requisitos de gerência. Por exemplo, a tarefa de visualizar a topologia da rede, em tempo real, necessita que as informações sejam processadas em tempo, o mais real possível, senão a representação não será precisa o suficiente. De outra forma, um outro exemplo é a tarefa de obter o historico de estatísticas de algum ponto fixo, que possui uma restrição de tempo muito baixa.

Para proteção dos mecanismos básicos de operação da rede a solução mais intuitiva é proteger suas trocas de mensagens, assim como deve ser feito com as informações dos usuários da rede. Para tanto devem ser adotados esquemas de criptografia adaptados para estes ambientes.

Sendo assim, chega-se ao ponto mais vulnerável do sistema de segurança que é o gerenciamento das chaves do esquema de criptografia. Por razões de eficiência um bom esquema faria uso de chaves simétricas para a autenticação, e dentro desse contexto, o estabelecimento seguro de chaves simétricas que seriam posteriormente utilizadas para a comunicação entre os nós.

Este esquema de chaves deve levar em conta características como: as propriedades da autoridade da rede, acessibilidade de um nó em relação a rede, o comportamento da fase de inicialização do esquema, o tipo de relação entre os nós, o tipo de relação entre os nós e a(s) autoridade(s) da rede e a distribuição da confiança na rede.

Dentro desse contexto são empregados esquemas de criptografia, como assinaturas digitais, com infra-estrutura de chave pública, onde cada nó possui um par de chaves (uma pública e a outra privada), e uma entidade confiável, denominada autoridade de certificação.

Esta entidade fica responsável pela associação confiável entre os nós da rede e suas chaves públicas. Enquanto um nó tem confidencialmente sua chave privada, a sua chave pública deve ser anunciada na rede. Cabe ressaltar que o próprio serviço de certificação também possui um par de chaves pública/privada. A diferença nesta abordagem para redes *mesh* é que a responsabilidade de gerenciamento de chaves será distribuída numa comunidade de nós, os quais também precisam ser gerenciados [Tamashiro 2007].

A chave pública do serviço de certificação é conhecida por todos os nós integrantes da rede, mas a chave privada do serviço e dividida e compartilhada entre *n* nós que passam a ser denominados de servidores, que serão as autoridades da rede. Todos os nós da rede podem submeter pedidos de chaves públicas da rede e renovações da própria chave para este serviço de certificação distribuído.

A partir das idéias tratadas acima, serão abordados a seguir os gerenciamentos específicos necessários para se prover uma maior segurança em uma rede *mesh*.

2.4.1. Gerenciamento de Segurança

Tanto redes *mesh*, quanto *ad hoc*, são muito vulneráveis a ameaças de segurança, devido aos nós serem facilmente manipulados, e sinais interceptados, falsificados e etc. Atualmente protocolos, tais como SNMPv3 (*Simple Network Management Protocol v3*), implementam alguns mecanismos de proteção contra escutas e alguns ataques usando transmissões *unicast* seguras [Stallings 1998]. No entanto, há algumas formas de comunicações adicionais que precisam ser consideradas, para assim desenvolver uma maior segurança.

Um protocolo de gerenciamento deve acompanhar constantemente os nós da rede visando determinar se eles são confiáveis ou não. Esta informação deve ser utilizada para determinar se os dados coletados são confiáveis ou sem valor. Da mesma maneira, cada gestor deve ser capaz de determinar se alguma rede esta trocando informações confiáveis ou não.

Outra consideração em relação ao gerenciamento de segurança, diz respeito ao processo de coleta de dados, a fim de se fazer uma coleta de dados eficaz, usando uma árvore de abrangência [Stallings 1998]. Isso permite que um nó intermediário possa combinar dados de diferentes nós (de um nível mais abaixo) antes que repasse as informações para um nó de nível superior, assim diminuindo o tráfego de informações de gerenciamento da rede. Um problema com este modelo é a possibilidade de uma violação de segurança.

A formação de *cluster* é a forma mais lógica de divisão de uma rede, a fim de simplificar a tarefa de gerenciamento [Chen 1999]. Essa divisão facilita na descentralização do gerenciamento que torna a rede mais tolerante a falhas e com mensagens eficientes.

Para se manter o baixo *overhead* de mensagens, é mais vantajoso não se tentar manter a par de todos os movimentos de todos os nós da rede. Acredita-se que o *overhead* na coleta de tais informações não se justifica, e na maioria dos casos, não é totalmente necessária. Em vez disso, responder aos movimentos apenas quando há mudanças significativas na topologia, torna-se a maneira mais viável de se fazer a coleta de dados necessária.

2.4.2. Gerenciamento de Grupos e Membros

A segurança das redes mais tradicionais baseia-se na existência de uma estrutura permanente, especializada na administração da rede, que define a política de segurança e fornece a infra-estrutura necessária para as suas aplicações. Em redes *mesh*, todos os serviços, incluindo uma infra-estrutura de segurança, devem ser criados e administrados pelos nós que decidiram formar a rede [Maki 2000].

Um conceito básico em muitas redes *mesh* e *ad hoc*, é um grupo de usuários ou nós da rede. Um grupo é um conjunto de entidades que querem se comunicar uns com os outros e de cooperar para algum efeito, ou objetivo. A necessidade de formar um grupo poderia ser uma partilha de aplicação, localização física, ou tarefas administrativas que alguns nós associam uns com os outros e etc.

O gerenciamento de membros dos grupos envolve adicionar e remover nós, no grupo, assim como fornecer um método para autenticar os membros do grupo. Um nó pode revelar a sua filiação em um grupo para nós que não são membros do grupo também. As mais importantes funções de segurança para um grupo são os seguintes [Maki 2000]:

- Autenticação mútua dos membros do grupo.
- Autenticação dos membros do grupo de forasteiros.
- Autenticação dos papéis, em especial com os membros da filiação de gestão.

Grupos em redes *mesh* devem lidar com características especiais de redes *mesh*, e *ad hoc* também. Como conseqüência, os grupos devem ser geridos tão atenciosamente quanto possíveis, independentemente da rede fixa e de serviços e uns com os outros. A gestão deve ser distribuída e tolerante a falhas de segurança física. Os grupos devem ser fáceis de construir e se modificarem.

Os nós de uma rede *mesh* são muitas vezes expostos a perigos físicos, e, independentemente de qualquer garantia, é provável que algumas chaves privadas ou

equipamentos que as contenham, possam cair nas mãos de atacantes (indivíduos mal intencionados com relação à integridade da rede).

A reconstituição do grupo é uma maneira segura e, muitas vezes a mais recomendável para continuar apenas com os membros considerados confiáveis na rede [Maki 2000]. No entanto, pode-se adquirir a reconstituição em pleno tempo em que alguns dos nós confiáveis possam estar ocasionalmente fora de alcance. Os membros de um grupo ainda necessitam de alguns mecanismos de cancelamento imediato da filiação, sem sacrificar a adesão dos demais, ainda membros confiáveis.

Infelizmente, cancelar uma adesão que já tenha sido concedida não é uma tarefa simples. Os certificados dos membros podem ser criados, armazenados e verificados simultaneamente em diferentes partes do sistema, característica que torna esse cancelamento um trabalho de certa forma complexo e árduo. Existem algumas formas de se eliminar os membros não confiáveis: reconstituição do grupo, expiração de membros e extinção de membros.

a) Reconstituição de grupo

Para substituir um grupo por um novo, uma nova chave de grupo deve ser gerada e novos certificados de membros e liderança devem ser emitidos para os antigos membros.

A reconstituição pode ser feita periodicamente, ou quando tenham ocorrido mudanças suficientes na composição do grupo. Devido à sua simplicidade conceitual, a reconstituição de grupos deve ser usada como a principal proteção contra membros comprometidos.

É possível a criação do novo grupo, enquanto o antigo ainda esta funcional e, progressivamente, se promover a passagem do antigo para o novo. Dessa forma, a nova chave de grupo e os novos certificados podem ser propagadas para todos os nós necessários antes que a antiga chave de grupo seja abandonada.

b) Expiração de membros

A expiração de certificados pode ter um período de validade que é decidido pelas autoridades da rede. Ao optarem por curtos períodos de validade dos certificados, os líderes do grupo podem rever periodicamente o *status* dos membros.

O mecanismo de expiração tem a grande vantagem de uma vez que um membro com certificado expirado, pode ser simplesmente tirado do grupo. Por outro lado, os membros que querem manter-se membros do grupo têm que periodicamente obter novos certificados.

O mecanismo de expiração também depende se os *clocks* de cada nó da rede estão sincronizados. É significativo lembrar que o nó que emite os certificados de curta duração tem que examinar periodicamente a confiabilidade dos membros.

Assim, com o tempo de vida limitado mantém-se uma consciência dos riscos de segurança e protege-se contra a acumulação de longo prazo do comprometimento de membros. Os nós que geram os certificados podem adaptá-los em função do custo de distribuição dos certificados e renovando a probabilidade de uma solução de compromisso, para cada membro.

c) Extinção de membros

A extinção de membros permite que a rede possa reagir imediatamente contra a possibilidade de uma falha de segurança. No entanto, quando é feita uma decisão de revogação de uma adesão, as informações sobre a revogação devem ser propagadas para todas as partes do sistema onde as certificações podem estar sendo utilizadas.

Uma distribuição pouco eficaz ao longo das conexões pode causar que a informação sobre uma revogação de adesão não chegue a todas as entidades que dela necessitam. Atrasos na propagação da revogação de dados também podem ser consideráveis.

Pode-se dar a todos os líderes de um grupo o direito de revogar si próprio e de qualquer outro líder e membro do mesmo grupo. Eles fazem isto através da assinatura de listas de revogação de chaves de grupo pares. As listas que lhes são propagadas no esforço de uma melhor forma a todos os membros do grupo e para outras partes que possam verificar o grupo adesão.

Os membros deverão ser revogados apenas quando existe uma razão para suspeitar que a chave privada foi descoberta por um nó intruso a rede. O custo da distribuição de listas a revogação é bastante elevado para algumas coisas, mas há situações de emergência em que se torna um mecanismo viável.

Líderes podem ser revogados, mas a operação afetará também todos os membros certificados pela chave revogada. Se a chave privada de um líder foi comprometida, o intruso na posse da chave pode revogar outros membros e lideres. Portanto, num caso em que dois líderes revoguem uns aos outros, é impossível saber qual líder é que teve sua chave comprometida. Por conseguinte, ambas as chaves deve ser revogada, para se precaver com relação a intrusos com “poderes” de líder na rede.

2.4.3. Gerenciamento de Confiança

Confiança e segurança são dois conceitos mutuamente dependentes, que não podem ser separados. Por exemplo, confiança não pode ser garantida sem o controle de comunicações seguras, da mesma forma como atributos de segurança requerem uma criptografia confiável para se realizar as tarefas desempenhadas da rede.

A medida que o ambiente da rede é cooperativo, as relações de confiança entre os nós são extremamente vulneráveis aos ataques. Além disso, a ausência de uma infra-estrutura fixa, os recursos limitados, disponibilidade e conectividade passageira, compartilhamento do meio sem fio e vulnerabilidade física, faz com que o estabelecimento de confiança se torne praticamente uma tarefa complexa [Siddiqui et al. 2008].

Sendo assim, as propriedades únicas de confiança na gestão de uma rede *mesh*, em oposição à maneira tradicional são: provas de confiança não completas, computação distribuída e a confiança na avaliação é empregada individualmente.

Para superar estas características a confiança em redes *mesh* deve ser estabelecida usando uma série de pressupostos incluindo a pré-configuração dos nós com chaves secretas, ou da presença de uma autoridade central, ou um conjunto destas. Uma confiança direta pode ser estabelecida entre as duas partes usando técnicas de autenticação. A terceirização da cofidencialidade pode ser implementada utilizando certificado de autoridade, que é computacionalmente uma solução mais cara e difícil de aplicar, devido à natureza das redes m*esh* ser um tipo híbrido de rede.

Em redes m*esh* a confiança e a distribuição são restritas apenas as interações locais. Cada nó deve agir como um agente autônomo, o que torna a decisão sobre a confiança uma avaliação individual. As decisões são baseadas em informações que se tenham obtido, por si só ou de seus vizinhos. Ainda não é confiável um único nó em uma rede m*esh*, devido a fraca segurança física e de disponibilidade, com isso se deve distribuir confiança para um conjunto de nós. Partindo do princípio que qualquer n + 1 nós improvavelmente estarão todos comprometidos, se tem o consenso de que, pelo menos, n + 1 nós são confiáveis.

2.4.4. Gerenciamento de Chaves

Muitos objetivos da segurança podem ser obtidos utilizando mecanismos criptográficos. Por outro lado, os mecanismos criptográficos desenvolvidos para redes *mesh* e *ad hoc*, bem como para as redes tradicionais, confiam que o gerenciamento das chaves criptográficas está sendo realizado de forma apropriada.

Em redes *mesh* o gerenciamento de chaves é um grande desafio. Os mecanismos tradicionais de gerenciamento de chaves não são adequados para as redes *mesh* e *ad hoc*, uma vez que necessitam de uma entidade confiável central, conhecida da como AC (Autoridade Certificadora) [Capkun 2003].

O principal problema de qualquer sistema de segurança baseado em chaves públicas é fazer com que a chave pública de cada usuário da rede seja disponibilizada para os demais usuários de forma que sua autenticidade seja verificada. Esse problema é ainda maior nas redes *mesh* e *ad hoc*, pois, como já foi dito, não existe o papel de uma autoridade central na rede [Asokan 2000]. Outra característica é que eles podem ser particionados devido o dinamismo em sua topologia.

Uma abordagem amplamente utilizada para a solução dos problemas de gerenciamento de chaves públicas é o uso de certificados de chaves públicas. Um certificado de chave pública é uma estrutura de dados na qual a chave pública é associada a uma identidade por meio da assinatura digital do emissor do certificado.

De certa forma é uma questão problemática utilizar uma única AC em uma rede *mesh*, uma vez que a AC é responsável pela segurança da rede inteira, esta se torna um ponto vulnerável da rede. Caso a AC fique indisponível, os nós da rede não podem obter as chaves públicas atuais dos outros nós, e como conseqüência, não podem estabelecer uma comunicação segura com os demais nós.

Além disso, se uma AC fica comprometida, um atacante pode assinar certificados falsos usando uma chave privada obtida da AC comprometida e, personificar qualquer outro nó, ou ainda, revogar os certificados válidos. Muitos *frameworks* de gestão de redes usam um AC virtual.

No entanto, é importante notar que nenhuma destas abordagens tem sido apresentada para fornecer soluções eficazes em diversos ambientes. Estas limitações vêm principalmente do fato de que a maior parte das abordagens tentam adaptar soluções de ambientes cabeados com adequações para enfrentar os desafios específicos em redes *mesh*.

A princípio, a participação do nó estabelece que uma chave no *framework* de gestão deve basear-se em um grande número de nós para a disponibilidade, mas um grupo de pequenos nós para segurança [Becker 1998]. Dada a vulnerabilidade física dos nós

móveis em redes *mesh*, não é eficaz a carga em único nó com a responsabilidade de proporcionar um serviço de segurança como a gestão das chaves.

Uma forma natural de resolver este problema é a distribuição dos serviços de segurança sobre vários nós. No entanto, igualdade de distribuição de funcionalidades de segurança ao longo demais nós conduz a um sistema vulnerável. Esta observação leva a duas questões importantes quanto à participação dos nós na chave gerenciamento:

- Em primeiro lugar, quantos nós devem participar? A participação de uma fração maior dos nós na rede pode melhorar a disponibilidade e tolerância à falhas. No entanto, sem uma reflexão cuidadosa, uma maior participação pode levar a uma maior vulnerabilidade.
- Como os nós devem participar? Quando um serviço de segurança está dividido entre um grande número de nós a igualdade de responsabilidades, e a disponibilidade do serviço também aumenta, uma vez que há mais nós que um usuário final que possa entrar em seu contato.

No entanto, isso também ajuda os nós "adversários" a localizar esses nós e comprometer a segurança do serviço. Por isso, a igualdade de distribuição de funcionalidade para vários nós pode degradar a segurança global da rede. Em vez disso, o núcleo das funcionalidades do serviço de segurança deve ser distribuído a um conjunto restrito e seguro de nós, proporcionando uma maior segurança e um nível aceitável de disponibilidade.

Os demais nós, que fazem parte de um nível menor, tem a funcionalidade de melhorar a disponibilidade dos principais nós. Comprometendo qualquer destes nós de baixo nível, não devem comprometer a segurança global da rede, e sim afetarão a capacidade do núcleo do serviço.

A utilização de uma terceirização TTP (*Trusted Third Party*) faz com que tenha um princípio fundamental de gestão do *framework*, que deverá melhorar a qualidade de autenticação das chaves. Uma vez que não há garantias sobre o comportamento dos nós participantes, qualquer autenticação baseada em tais relações casuais pode não ser confiável para a segurança de aplicações. A TTP proporciona uma confiança que pode ser usado como base para as relações de ainda mais confiança. Uma vez que cada nó que confia no TTP, a autenticação fornecida pela TTP é confiável com um elevado nível de confiança.

Essencialmente, sem uma autenticação confiável, não há mais nenhuma garantia de serviço que possa ser construído de modo a garantir um nível elevado de confiabilidade. Por conseguinte, a utilização de uma terceirização, é fundamental em qualquer rede *mesh* com fortes requisitos de segurança.

Dentro deste contexto de gerenciamento de chaves serão mostrados a seguir tópicos com pontos relevantes em relação ao gerenciamento de chaves, visando um aumento na segurança de uma rede *mesh*.

a)Infra-estrutura de chave pública

A utilização de chaves de criptografia pública exige que as autenticidades das chaves públicas possam ser estabelecidas. Uma simples abordagem exige que qualquer um dos dois usuários que desejam se comunicar, devem trocar suas chaves públicas e, desta forma,

exige que a distribuição inicial de n (n-1) chaves públicas. No entanto, se há uma terceirização para emitir os certificados a cada um dos usuários, apenas a chave pública do TTP precisa ser distribuída a cada um dos usuários.

b)Distribuição de chaves

O principal objetivo do gerenciamento de chaves é compartilhar uma chave com um grupo de participantes. Para tanto, quatro operações podem ser necessárias: a pré-distribuição, o transporte, a arbitração e o acordo de chaves.

A pré-distribuição de chaves consiste da distribuição das chaves pelos nós interessados antes do início da comunicação. Isto exige que todos os nós da rede sejam previamente conhecidos, embora não seja exigido que todos participem sempre da rede [IEEE 2000].

No transporte de chaves, as entidades trocam chaves para se comunicar. O método mais simples para essa fase se chama KEK (*Key Encription Key*) [Bird 1995], e consiste em criptografar a nova chave com o segredo compartilhado, e apenas os nós que possuírem esse segredo podem obter a nova chave. No caso de não existir uma chave previamente conhecida por um grupo, mas existir uma infra-estrutura de chave pública, essa nova chave pode ser trocada criptografando-a com a chave pública do nó que irá recebê-la.

A distribuição de chaves utiliza um arbitrador (distribuidor) central para criar e distribuir chaves entre os participantes, o que a torna uma especialização da fase de transporte. Em sistema infra-estruturado, um ponto central é escolhido para exercer a função de arbitrador.

No entanto, em redes *mesh* e *ad hoc*, esta função centralizada de arbitrador é proibitiva por causa da ausência de infra-estrutura e restrições de recursos. Entre esses está a necessidade do arbitrador estar sempre ativo e acessível, sob pena de negação de serviço, caso o nó se mova ou saia da rede.

A utilização de réplicas da base de dados para resolver o problema da negação de serviço aumentaria o número de nós guardando os segredos da rede, gerando mais pontos de vulnerabilidade, além de ser uma solução que acarretaria uma maior saturação à rede.

Finalmente, o acordo de chaves corresponde à troca de chaves posterior ao início da rede. Serão estabelecidos segredos entre nós através de chaves assimétricas, se elas estiverem disponíveis. Isto é necessário para realizar uma comunicação segura dentro da rede, embora seja uma operação muito custosa, devido a sua complexidade de manutenção destas chaves assimétricas.

c)Gerenciamento dinâmico de chave

Uma alternativa que pode enriquecer o gerenciamento de chaves é o mecanismo de gerenciamento dinâmico, os quais necessitam, em sua maioria, de um sistema de distribuição ordem para iniciar o processo pré-existente [Lin 1997].

O mecanismo de pré-distribuição de chaves deve distribuir um conjunto de chaves secretas para cada nó antes que os nós fiquem ativos na rede. Depois que os nós são implantados, o regime de pré-distribuição pode fornecer garantias de que dois nós partilham uma chave secreta com uma determinada fração de seus vizinhos, esta fração é um dos parâmetros fundamentais do regime de pré-distribuição, pois garante que há uma certa confiabilidade entre os nós vizinhos, ou no mínimo uma fração deles.

Dessa forma, um nó pode criar, ou receber, uma chave secreta compartilhada com todos, ou alguns, nós vizinhos. A fim de tornar o sistema dinâmico, os nós desencadeiam este processo para cada conjunto de vizinhos. Enquanto dois conjuntos de vizinhos consecutivos de um nó se sobrepõem, os nós, nesta sobreposição podem ser usados para estabelecer chaves com todos os novos nós do novo conjunto de vizinhos, assim tornando o processo mais dinâmico.

d) Gerenciamento de chave de grupo

O gerenciamento de chaves de grupo inclui atividades para criação e manutenção da chave do grupo. Manutenção das atividades consiste em mudar a chave do grupo devido a adição, exclusão ou devido ao uso de chave do grupo durante longos períodos de tempo [Anton 2002].

O estabelecimento de uma chave de grupo pode ser centralizado, também chamada de distributivo, isto ocorre quando uma entidade é responsável por gerar as chaves de grupo e distribuí-las para os outros membros do grupo. Esta abordagem tem a vantagem de ser simples.

Já em um estabelecimento distribuído, também chamado de contributivo, todos os membros do grupo contribuem para o grupo de geração de chaves. Esta abordagem é tolerante a falhas e diminui os riscos de geração viciosa de chave por uma única entidade. Uma variação desta abordagem consiste em ser parcialmente contributivo o que permite a um subgrupo de ser responsável por gerar a chave do grupo.

Um grupo pode ser estático ou dinâmico. Um grupo dinâmico permite a exclusão de membros, bem como a adição de novos membros. Chave para a gestão dinâmica de grupos pode proporcionar sigilo, quando os membros que deixam o grupo são incapazes de calcular o futuro grupo chaves.

2.5. Soluções Propostas

Muitas técnicas de segurança em redes *mesh* foram adaptadas ou trazidas das redes sem fio convencionais.

No entanto, várias destas técnicas de segurança, ou são específicas para a camada de aplicação como por exemplo, utilizar protocolos como HTTPS (*HyperText Transfer Protocol Secure*), SSH (*Secure Shell*) e SFTP *(Secure File Transfer Protocol)* ou são políticas de segurança, onde o usuário é quem tem a obrigação ou necessidade de seguir.

As técnicas de segurança voltadas para a camada de transporte existem em menor número, porém, mais eficientes, ou pelo menos impõem a responsabilidade de segurança da rede para a tecnologia, passando mais confiabilidade aos usuários da rede.

Na camada de rede do modelo TCP/IP, as técnicas de segurança focam nos protocolos de roteamento, onde os mais usados e conhecidos como OSLR, WRP (*Wavelength Routing Protocol*) [Murthy e Garcia 1996], CGSR (*Cluster-Head Gateway Switch Routing*) [Chiang et al. 1997], FSR (*Fisheye State Routing*) [Pei et al. 2000], DSR, AODV e TORA (*Temporally Ordered Routing Algorithm*) [Royer e Toh 1999].

Esses protocolos possuem grande aceitação por suas funcionalidades vitais, como rápida alocação da tabela de rotas em casos de mudança de disposição da rede, escalabilidade e controle reduzido de *overhead*. Porém, estes protocolos não têm um tratamento adequado contra técnicas MITM (*Man In The Middle*), DoS (*Denial of*

Service), *eavesdropping* (conhecido como escuta passiva) e ataques de inserção de informações de rota errôneas na rede.

2.5.1. Arquiteturas

O anonimato vem recebendo uma crescente atenção pela literatura, como por exemplo [Rahman et al. 2006] e [Seys e Preneel 2006], deivido ao fato do usuário querer garantir sua privacidade ao usar a rede. Por outro lado, a autoridade de rede requer um anonimato condicional que permita um rastreamento.

[Sun et. al 2008] propõe uma arquitetura de segurança com o objetivo de assegurar nas redes *mesh*, um anonimato incondicional para os usuários confiáveis e o rastreamento de usuários não confiáveis. Essa arquitetura proposta busca solucionar os conflitos entre a demanda pelo anonimato e a necessidade de rastreamento, além de garantir requisitos fundamentais de segurança, incluindo autenticação, confidencialidade, integridade de dados, e não-repúdio. Especificamente, as contribuições principais são: A modelagem do sistema; O projeto de um sistema de anonimato baseado em tickets com a propriedade para garantir rastreamento; Controle de acesso de anônimos através da relação dos tickets com pseudônimos, sendo o processo de revogação simplificado e; Adoção de um sistema de detecção de intrusão hierárquico basedao em criptografia para autenticação intra-domínio.

Em [Li 2007], a arquitetura ISA *(Identity-based Security Architecture*) é proposta, eliminando a necessidade por distribuição de chave públicas baseadas em certificados, introduzindo um mecanismo de descoberta de vizinhança. Habilita ainda a possibilidade de atualização eficiente de chaves através de mesnagens *broadcast*.

[Zhang e Fang 2006] identifica as necessidades de segurança em redes *mesh* e em seguida, propõe a arquitetura ARSA (*Attack-Resilient Security Architecture*), a qual elimina a necessidade do estabelecimento de acordos bilaterais e interações em tempo real entre as operadoras.

Em [Lin et al. 2008], é proposto um paradigma de projeto para uma arquitetura de autenticação e resiliência em redes *mesh* denominada TUA (*Threshold User Authentication*).

2.5.2. Protocolos de Roteamento Seguros

Os protocolos mais conhecidos que propõem técnicas de segurança em nível de transporte são SOLSR (*Secure Optimized Link State Routing Protocol*) [Hong e Fu 2005], SAODV (*Secure Ad Hoc On-Demand Distance Vector*) [Zapata 2002], SRP (*Secure Routing Protocol*) [Hu e Perrig 2004], Ariadne [Hu et al. 2005], SEAD (*Secure Eficient Ad Hoc Distance Vector Routing Protocol*) [Hu et al. 2003], ARAN (*Authenticated Routing for Ad Hoc Networks*) [Mahmoud et al. 2005], SLSP (*Secure Link State Protocol*) [Papadimitratos 2003] e o RM-AODV (*Radio Metric Ad Hoc On-Demand Distance Vector*) [Takeda et al. 2005]. Abaixo, os principais protocolos seguros serão abordados.

2.5.2.1. SOLSR

É uma extensão segura do protocolo de roteamento OLSR, onde a idéia é assinar cada pacote de controle do OLSR, com chaves simétricas, com o objetivo de garantir a autenticidade das mensagens.

Um diferencial do SOLSR é que a autenticação é realizada salto a salto. Isso garante a segurança, inclusive de campos que são atualizados por nós intermediários, como o número de saltos e o campo TTL (*Time To Live*).

É necessária somente uma assinatura por salto, levando-se em conta que muitas mensagens de roteamento são encapsuladas em um único pacote do OLSR. Em contrapartida, a abordagem salto a salto não garante assinaturas fim-a-fim, já que um pacote recebido por um nó terá sido assinado pelo nó anterior e não pelo nó de origem.

Todavia, o protocolo determina que os nós devem somente encaminhar pacotes originados de nós confiáveis. Por conseqüência os nós de uma determinada rota serão confiáveis, dois a dois.

O processo de assinar digitalmente utiliza uma função *hash* com chave, de forma que um nó que não tenha acesso à chave secreta não poderá reproduzir a assinatura do nó emissor.

O SOLSR possui mensagens determinadas para acomodar as assinaturas, de forma que se garante a compatibilidade com nós que não estejam operando a versão segura do OLSR. O protocolo, para evitar ataques de replicação, utiliza também a técnica de *timestamp* que nada mais é que uma seqüência de caracteres que denotam data e hora que um determinado evento ocorreu, utilizado exclusivamente para realizar *logging* de eventos.

2.5.2.2. SAODV

É uma extensão do protocolo AODV que garante segurança no processo de descobrimento de rotas.

A idéia básica neste protocolo é usar assinaturas para autenticar a maioria dos campos dos pacotes RREQ e RREP, e usar cadeias de *hash* para autenticar a contagem de saltos.

A assinatura digital garante autenticação fim-a-fim dos campos que mantém informações imutáveis da mensagem e que devem ser assinados pelo nó de origem antes do envio da mensagem.

Porém, o campo número de saltos (*Hop Count*) deve ser decrementado a cada salto pelas estações intermediárias. Nesse caso, a cadeia de *hash* autentica o campo número de saltos a cada salto, garantindo a integridade do algoritrmo de vetor de distâncias. No processo de enviar mensagens, o nó de origem inicializa o campo *hash* com uma variável aleatória, o campo número máximo de saltos com o valor desejado e o campo *top hash* com o resultado da aplicação da função *hash* sobre a variável um número de vezes igual ao número máximo de saltos.

Quando um nó intermediário receber a mensagem, poderá autenticar o campo número de saltos, aplicando a mesma função *hash* um número de vezes igual a diferença entre número máximo de saltos e número de saltos sobre o campo *hash* e comparando o resultado com o campo *top hash*.

Os campos sendo iguais, pode-se assegurar que o campo número de saltos não foi modificado, então, o nó intermediário deverá incrementar o campo número de saltos em 1 e aplicar a função *hash* no campo *hash* antes de reencaminhar a mensagem. De outra forma, a mensagem será descartada.

Dessa maneira, o mecanismo de cadeias de *hash* impossibilita que um nó malicioso altere o número de saltos da mensagem de roteamento, uma vez que não se pode obter os valores anteriores da seqüência, levando em conta a característica unidirecional da função *hash*.

2.3.5.3. SRP

Foi projetado para manter e normalizar o roteamento correto em redes *ad hoc* onde ocorrem mudanças freqüentes e pode haver nós maliciosos, mas que não agem em conjunto para realizar ataques DDoS.

O protocolo foi desenvolvido como uma extensão, que pode ser aplicada em alguns protocolos de roteamento reativos existentes, especialmente o DSR.

No SRP, o nó inicia o procedimento de descoberta de rota identifica e descarta respostas contendo informações de roteamento falsas e ainda evita recebê-las, garantindo a obtenção de informações da topologia da rede corretamente.

Para isso considera-se a existência de uma AS (*Security Association*) entre os nós comunicantes, como uma chave simétrica compartilhada. Além disso, supõe-se que os nós possuem uma única interface de rede, com uma correspondência biunívoca entre os endereços IP e o da interface.

Ao iniciar o procedimento de descoberta de rota, o nó de origem deve gerar um MAC (*Message Authentication Code*), usando uma função *hash* com chave que recebe como argumentos de entrada o cabeçalho IP, os campos básicos da mensagem de roteamento e a chave secreta compartilhada entre os nós de origem e destino. As estações intermediárias são responsáveis por encaminhar a mensagem até o seu destino final.

Quando o nó de destino recebe a mensagem de roteamento, é verificada a integridade da mensagem e é assegurada a autenticidade da origem, uma vez que o MAC só pode ser calculado pelos nós que possuem a chave secreta, garantindo que somente a origem poderia ter computado o MAC recebido. Caso a mensagem recebida seja autêntica e integra, o nó destino envia uma mensagem de resposta ao nó de origem realizando o mesmo procedimento feito pelo nó de origem.

O nó de origem recebendo a mensagem de resposta, verifica sua integridade usando o MAC computado pelo nó de destino e descarta a resposta se ela não tiver o mesmo identificador da mensagem inicial.

O protocolo possui um mecanismo que regula as requisições de descoberta de rota. Cada nó mede as freqüências de requisições realizadas pelos seus vizinhos e mantém uma fila na qual a prioridade de atendimento às requisições é inversamente proporcional à freqüência com que elas são feitas.

Caracterizando assim, um mecanismo de *feedback* negativo que controla a freqüência de requisições realizadas pelos nós vizinhos, impedindo ataques nos quais o nó malicioso inunda a rede com requisições de descoberta de rota, já que o atacante será o último a ser atendido ou será ignorado, devido sua baixa prioridade de atendimento.

Uma das desvantagens do SRP é a ausência de autenticação das mensagens de erro, embora o nó malicioso só consiga prejudicar rotas às quais ele pertence. Outra desvantagem é que, como o protocolo não previne ações maliciosas em conjunto, ele não está imune aos ataques de atração e descarte de pacotes.

O protocolo possui o diferencial da imunidade aos ataques que modificam a origem do pacote ou simulam identidades. Isso se deve ao protocolo NLP (*Neighbor Lookup Protocol*) de descoberta de vizinhos, que integra o SRP, mantendo um mapeamento dos endereços da subcamada de acesso ao meio MAC e da camada de rede dos nós da rede.

2.3.5.4. Ariadne

É um protocolo de roteamento reativo seguro para redes móveis *ad hoc*, baseado no protocolo DSR.

Para ser utilizado, o protocolo necessita de uma sincronização fraca de tempo entre os nós da rede, de modo que um nó possa estimar o tempo de transmissão fim-a-fim para qualquer nó da rede.

Faz-se necessário um mecanismo para o estabelecimento de chaves secretas entre os nós comunicantes e um meio de fazer a distribuição de uma chave pública TESLA (um mecanismo eficiente de autenticação *broadcast* que requer uma sincronização fraca de tempo entre os nós) autêntica para cada nó.

O protocolo provê autenticação ponto-a-ponto das mensagens de roteamento usando um MAC e uma chave secreta compartilhada pelas duas entidades.

Para garantir a autenticação fim-a-fim do esquema de descoberta de rota, o nó de origem calcula um MAC da mensagem usando a chave secreta conhecida exclusivamente pelos nós de origem e destino.

Dessa maneira, assegura-se que a mensagem foi transmitida do nó de origem e que as informações de roteamento não foram alteradas. Antes de enviar a mensagem, o nó de origem estipula um tempo máximo para o atraso fim-a-fim, inserindo esta informação na mensagem, em conjunto com uma lista de nós e uma lista de MACs, ambas inicialmente vazias.

Após o término do tempo estimado o nó de origem irá divulgar sua chave TESLA. Assim, quando uma estação intermediária recebe a mensagem, ela verifica se o tempo de divulgação da chave já esgotou.

Sendo positivo o resultado, descarta-se a mensagem, caso contrário, insere-se o endereço na lista de nós. A integridade da lista de endereços é obtida através do mecanismo de cadeias de *hash*, usando um esquema similar utilizado pelo SAODV.

Neste instante é calculado um novo *hash* sobre o campo *hash chain*. A estação intermediária ainda utiliza sua chave TESLA atual para computar o MAC da mensagem, que é inserido na lista de MACs.

A mensagem modificada é reenviada para os vizinhos recursivamente pelas estações intermediárias até chegar ao nó de destino.

Ao receber a mensagem, o nó de destino, verifica se o valor final da cadeia de *hash* está correto e se as chaves TESLA já foram divulgadas, caso a mensagem recebida seja válida, o nó de destino calcula o MAC da resposta usando a chave secreta compartilhada com o nó de origem e envia a mensagem de resposta para a origem. Ao final da rota reversa, a origem autentica a resposta antes de aceitá-la.

2.3.5.5. SEAD

Diferentemente do Ariadne, o SEAD é um protocolo pró-ativo, que é baseado no protocolo de vetor distância DSDV.

Foi desenvolvido para suportar a existência de nós com baixa capacidade de processamento e possui defesas contra ataques de negação de serviço onde o atacante visa esgotar recursos da vítima, como banda passante e processamento e até mesmo bateria.

Utiliza-se uma técnica de cadeia de *hash* para autenticar os campos número de saltos e número de seqüência. A cadeia é criada aplicando-se repetidas vezes uma função *hash* a um valor aleatório inicial e assume-se a existência de algum mecanismo que permita que um nó distribua um elemento autenticado da cadeia para seus vizinhos.

Um elemento autenticado da cadeia de *hash* é utilizado para garantir uma atualização segura das mensagens de roteamento. Os elementos seguintes da cadeia podem ser autenticados aplicando-se sobre eles a função *hash* um número determinado de vezes.

2.3.5.6. ARAN

É um protocolo de roteamento reativo que utiliza certificado digital para garantir autenticação, integridade e não-repúdio de mensagens de roteamento em uma estrutura de rede *ad hoc*.

Baseado em métricas lógicas de roteamento e certificados, este protocolo é imune a alteração de mensagens por *arpspoofing* e mensagens de roteamento geradas por ferramentas como o *ettercap* [Ornaghi e Valleri 2008], que é um *sniffer* para realizar ataques do tipo *Man In The Middle*.

Existem dois estágios que podem ser utilizados pelo protocolo ARAN. No primeiro a rota encontrada entre a origem e o destino, não tem garantia de ser a menor rota possível, levando em consideração a quantidade de nós intermediários na rota. Já o segundo estágio, exige maior processamento e consumo de banda, garantindo que a rota utilizada é a menor possível.

Entretanto, o segundo estágio é opcional, o que é aceitável, levando em conta que a rota encontrada no primeiro estágio, mesmo podendo não ser a menor, é a com menor tempo de retardo entre a origem e o destino.

Quando um nó origem necessita de uma rota para um destino qualquer, inicia-se o processo de descoberta de rota. Cria-se um pacote contendo seu certificado digital assinando-o, e encaminhando-o através da rede por *broadcast*, sendo que apenas o nó destino da requisição poderá responder a mesma.

Os nós vizinhos a origem da requisição, receberão o pacote e validarão sua assinatura. Tratando-se de um pacote assinado devidamente, esse vizinho, por sua vez, assina o pacote e inclui seu certificado no mesmo, sem remover nenhum dado do pacote original.

Os próximos vizinhos recebem o pacote de requisição, antes que ele chegue ao destino, e seguirão o mesmo procedimento, validar o certificado do nó vizinho que enviou o pacote, remover o certificado do nó vizinho que enviou o pacote, incluir o próprio certificado no pacote e encaminhar o pacote através da rede.

Alcançando o nó destino, a requisição é mais uma vez validada com seu certificado, sendo que dessa vez, o certificado do nó origem também é validado.

Sendo considerados válidos, o destino criará um pacote de resposta para a requisição e o encaminhará de volta à origem da requisição.

No momento em que a origem da requisição recebe a resposta enviada pelo destino, verifica-se a autenticidade do pacote, tendo em vista que apenas o destino poderia ter respondido sua requisição.

Essa limitação tem por objetivo garantir maior segurança, evitando a formação de *loops* em uma rota, além de uma possível perda na eficiência no processo de requisição de rotas. O protocolo exige a criação de uma entrada na tabela de roteamento, para cada par origem-destino.

A grande diferença no funcionamento do primeiro estágio do protocolo ARAN, para seu segundo estágio, é a necessidade de que todos os nós intermediários, entre a origem e o destino da requisição, assinem o pacote antes de encaminhá-lo através da rede, porém sem remover a assinatura do pacote vizinho que o encaminhou anteriormente.

Dessa forma, alcançando o nó destino, o pacote de requisição irá conter o caminho completo desde a origem.

2.3.5.7. SLSP

É um protocolo de roteamento reativo seguro baseado em estado de enlace que foi proposto pelos criadores do SRP. Leva-se em consideração a existência de um par de chaves assimétricas para cada interface de rede em um nó e de um sistema de gerenciamento das chaves públicas dos nós.

O SLSP compõe-se de três procedimentos: distribuição de chaves públicas, descoberta de vizinhos e atualização dos estados dos enlaces.

O procedimento de distribuição das chaves públicas é feito de forma distribuída, a fim de evitar o uso de um servidor central de gerenciamento de chaves. Cada nó envia por difusão um pacote de distribuição de chaves públicas

A garantia de segurança no nível de roteamento agregada a uma garantia de segurança em nível de aplicação garante um mínimo de confidencialidade em uma rede *mesh*.

2.3.5.8. Resumo comparativo entre os protocolos seguros

As tabelas abaixo, ver Tab. 2.2 e 2.3, apresentam um comparativo dos protocolos seguros apresentados.

Tabela 2.2. Resumo comparativo dos protocolos seguros

Parâmetros	ARAN	Ariadne	SAODV
Tipo	Reativo	Reativo	Reativo
Algorítimo de Criptografia	Assimétrico	Simétrico	Assimétrico
Protocolo Origem	AODV/DSR	DSR	AODV
Sincronização	Não	Sim	Não

Autoridade Certificadora	Necessita CA	Necessita KDC	Necessita CA
Autenticação	Sim	Sim	Sim
Confidencialidade	Sim	Não	Não
Integridade	Sim	Sim	Sim
Não-repudiação	Sim	Não	Sim
Anti-spoofing	Sim	Sim	Sim
Ataques DoS	Não	Sim	Não

Tabela 2.3. Resumo comparativo dos protocolos seguros

Parâmetros	**SEAD**	**SLSP**	**SRP**	**SOLSR**
Tipo	Pró-Ativo	Pró-Ativo	Pró-Ativo	Pró-Ativo
Algorítimo de Criptografia	Simétrico	Assimétrico	Simétrico	Simétrico/Assimétrica
Protocolo Origem	DSDV	ZHLS	DSR/ZRP	OLSR
Sincronização	Sim	Não	Não	Sim
Autoridade Certificadora	Necessita CA	Necessita CA/ KDC	Necessita CA	Necessita KDC
Autenticação	Sim	Sim	Sim	Sim
Confidencialidade	Não	Não	Não	Não
Integridade	Não	Sim	Sim	Sim
Não-repudiação	Não	Sim	Não	Não
Anti-spoofing	Não	Sim	Sim	Sim
Ataques DoS	Sim	Sim	Sim	Sim

2.5.3. Mecanismos de Detecção de Intrusão, Autenticação e Contabilização

Como soluções de segurança envolvendo autenticação, cita-se os protocolos WADP (*Wireless Dual Authentication Protocol*) [Zheng et al. 2004] e SUMP (*Secure Unicast Messaging Protocol*) [Janies et al. 2006].

Contabilização ou bilhetagem é tratada em [Xiao 2008] e [Zhu et al. 2007].

O primeiro proporciona um estudo do estado da arte a respeito de contabilização. Descreve e analisa aplicações, propondo uma arquitetura denominada *A-NET*, com uma análise voltada para redes *ad hoc* e rede *mesh.*

O segundo apresenta o esquema SLAB *(Secure Localized Authentication and Billing),* o qual visa manter a segurança e o desempenho do sistema em termos de resiliência, capacidade, *handoff* entre domínios, autenticação e latência. É demonstrado matematicamnete.

[Zhang et al. 2008] apresenta um esquema de descoberta de anomalias chamado RADAR (ReputAtion-based Scheme for Detecting Anomalous Nodes in WiReless Mesh Networks). Devido à infra-estrutura especial e o modo de comunicação, descoberta de intrusão em redes *mesh* é especialmente desafiadora, pois requer considerações particulares de projeto. Inicialmente apresenta conceitos gerais, caracterizando e quantificando *statu*/perfis dos nós em termos de métricas de desempenho, em seguida apresenta o esquema proposto.

Em [Li et al. 2006], é proposto uma solução para a autenticação de pontos de acesso em redes *mesh* no modo infra-estruturado, combinando 802.1X/EAP e gráfos dos nós vizinhos. Realiza simulações para avaliar a proposta.

[Kim e Bahk 2008] apresenta a arquitetura Meca *(Mesh Certification Authority)*, a qual é uma arquitetura, para autoridades certificadoras distribuídas, desenvolvida para redes *mesh.* Utiliza o esquema FVSR (*Fast Verifiable Secret Redistribution*) para atualizar compartilhamentos secretos e para a mudança de participantes. A arquitetura proposta reduziu o *overhead* existente utilizando *multicast.* Consegue prover atualização de certificações, exclusões e verificação de *status* de forma mais segura e eficiente. Ao basear-se no fato de que roteadores *mesh* possuem potência suficiente e são fixos, faz com que todos estes sejam capazes de trabalhar como nós autoridade certificadora distribuída e o uso de *multicast* traz uma significante melhora no desempenho da rede.

Em [Islam et al. 2008] é proposto um esquema de autenticação anônima entre o cliente/usuário e o roteador *mesh* para preservar a privacidade, identidade e segurança na comunicação em redes *mesh*.

Direta ou indiretamente relacionados ao tema, citam-se ainda [Krebs et al. 2008], [Kim e Bahk 2008], [Graffi 2006] e [Krebs et al. 2008].

2.6. Comentários Finais e Tendências Futuras

Atualmente, as redes *mesh* são vistas como uma tecnologia promissora para próxima geração das redes sem fio [Ju et al. 2007]. Algumas aplicações estão estimulando o seu rápido desenvolvimento, porém é necessário que sua inserção no mercado seja fortalecida e que pesquisas científicas sejam realizadas para sua melhoria.

O principal atrativo das redes *mesh* é o de prover uma rede comunitária de acesso banda larga com infra-estrutura sem fio, oferecendo acesso a Internet a baixo custo para comunidades que, por exemplo, possuem baixas condições econômicas.

Nas redes *ad hoc*, questões de segurança já vêm sendo estudadas há certo tempo, como por exemplo em [Zhou e Haas 1999], [Lou e Fang 2004], [Rahman et al. 2006] e [Raya e Hubaux 2007]. Entretanto, nas redes *mesh*, segurança ainda é um tema muito novo e pouco abordado.

A principal diferença entre as redes *ad hoc* e as redes *mesh* reside no fato de que os nós das redes em malha sem fios têm localização fixa, embora suas localizações não sejam predeterminadas. Os algoritmos de roteamento, portanto, têm muita semelhança entre si.

Observa-se que, cada protocolo tem características próprias que atendem as mais variadas exigências. Entretanto a utilização do protocolo de roteamento correto depende do cenário o qual ele será utilizado. Portanto, a escolha correta se dá após estudos detalhados sobre a topologia da rede para que o protocolo escolhido atenda as necessidades da rede em

questão. E como as redes *mesh* são compostas de nós moveis e fixos, um protocolo híbrido ou a combinação de protocolos reativos e pró-ativos é a solução mais aconselhável [Lee et al. 2006].

O MHRP (Multi-path Hybrid Routing Protocol) é um dos poucos protocolos híbridos propostos para redes *mesh* [Siddiqui et al. 2007]. É válido ressaltar ainda [Hamid e Khant 2006], um dos poucos trabalhos que propõe um protocolo de roteamento para ser utilizado em ambientes 802.16.

Atualmente, encontram-se várias linhas de pesauisa dentro do tema segurança em redes *mesh*, além do que foi aboradao neste capítulo, como por exemplo [Mogre et al. 2007] e [Hamid et al. 2008]. O problema começa a ser estudado matematicamente, como por exemplo em [Li et al. 2007], onde conceitos de processos estocásticos são abordados.

As redes em malha sem fio podem ser construídas baseadas em tecnologias existentes. Algumas empresas já têm à venda produtos, porém, tentativas em laboratórios e experiências com redes em malha sem fio existentes provam que o desempenho delas ainda é distante quando comparado com o que é esperado.

Pelo fato de não existir um padrão único para a construção de redes *mesh* e sim várias opções incluindo soluções acadêmicas e comerciais, são inúmeras as propostas encontradas na literatura tentando solucionar as questões apresentadas.

Mesmo após a especificação do futuro padrão IEEE 802.11s [Hertz et al. 2008] que permitirá a transmissão em múltiplos saltos no nível de enlace, resolvendo os problemas de mobilidade e comunicação em grupo, as soluções propostas no nível de rede continuarão sendo investigadas, pois são necessárias para permitir o uso de equipamentos já existentes nas redes *mesh* atuais e futuras.

Os desafios nas redes *mesh* existem e estão relacionados a todas as camadas de rede, daí a grande relevância do termo *cross-layer* para a academia, sendo segurança o menos desenvolvido até o momento.

Semelhante as redes *ad hoc*, porém em um maior nível, as redes em malha sem fio ainda possuem deficiências em soluções eficientes e escaláveis de segurança devido a vários fatores: sua arquitetura de rede distribuída, vulnerabilidade de canais e nós no méio sem fio compartilhado e a possibilidade de mudanças dinâmicas na topologia da rede.

Os ataques podem ocorrer na camada de rede através dos protocolos de roteamento, na atualização errada de informações, causando facilmente falhas na rede. O atacante pode se mover furtivamente na rede representando um nó legítimo, sem seguir as especificações necessárias ao protocolo de roteamento. Também podem ocorrer nos protocolos de acesso ao meio.

Uma forma de resposta aos ataques amplamente aceita é autenticação e autorização. Nas redes sem fio tradicionais serviços AAA (*Authentication, Authorization, and Accounting*) são utilizados diretamente nos pontos de acesso ou através de *gateways*, sendo executados por um servidor centralizado como RADIUS (*Remote Authentication Dial-In User Service*), o qual por ser um esquema centralizado não é aplicável nas redes em malha sem fio.

Além disso, o gerenciamento seguro de chaves nas redes em malha sem fio é muito mais difícil que nas redes sem fio tradicionais porque não há nenhuma autoridade central ou servidor para gerenciar as chaves de segurança. Desta forma, gerenciamento de chaves

nas redes em malha sem fio precisa ser executado dentro de um ambiente distribuído, porém seguro. Portanto um esquema distribuído de autenticação e autorização, com gerenciamento de chaves precisa ser validado para as redes em malha sem fio.

Adicionalmente, para garantir segurança nas redes em malha sem fio, duas estratégias precisam ser consideradas: mecanismos de segurança embutindos nos protocolos de roteamento e de acesso ao meio e mecanismos de segurança que monitorem a rede, detectem ataques e/ou quebra de serviços, bem como possam responder aos mesmos de forma ágil e segura.

Nas redes em malha sem fio, para um protocolo de rede seguro, um esquema seguro através de múltiplas camadas é desejado, uma vez que um ataque pode ocorrer simultanemaente em diferentes camadas de protocolos. Neste caso, um *framework* baseado no conceito de *cross-layer* para um sistema de monitoração precisa ser desenvolvido, sendo uma linha de pesquisa desafiadora uma vez que envolve o projeto e a implementação, com o uso de informações cruzadas e relacinadas, bem como através de algoritmos diversos de detecção de intrusão.

Um sistema de detecção de intrusão para redes *ad hoc* deve atender dois requisitos básicos: Eficácia (Que define como fazer o IDS realizar uma classificação correta de atividades malignas e benignas) e Eficiência (Como fazer o IDS funcionar de tal forma que haja o menor custo para a rede e opere todas as funcionalidades esperadas).

A ausência de uma infraestrutura física facilita o sucesso de um ataque de negação de serviços em uma infraestrutura de rede sem fio. De tal maneira o desenvolvimento de uma arquitetura de um IDS é um fator desafiador uma vez que sem um ponto de auditoria centralizado como roteadores, um IDS para redes *mesh* torna-se limitado utilizando somente o tráfego de entrada e saída dos nós da rede como fonte de informações de auditoria.

Um requisito fundamental é quanto a questão dos algorítimos utilizados pelos IDSs, pois estes são naturalmente distribuídos o que dificulta uma auditoria correta da rede pois, considera-se que um nó da rede possa visualizar somente uma porção do tráfego da rede. Levando em consideração que as redes *mesh* possuem roteamento dinâmico e os nós da rede podem mover-se livremente, existe a possibilidade de nós serem capturados como nós maliciosos. Se o algorítimo do IDS for cooperativo, torna-se necessário identifcar quais nós são confiáveis.

Em redes sem fio não é viável trafegar dados para IDSs como em redes cabeadas, pois é necessário conservar largura de banda. Questões como largura de banda e tempo de bateria podem influenciar a eficiência e a eficácia dos IDSs, pois a disponibilidade de dados de auditoria parcial torna difícil a tarefa de distinguir uma ataque de um comportamento real.

As técnicas de detecção de ataques, conhecidas para redes estruturadas, são ineficientes em redes em malha sem fio. Como sinal de amadurecimento das redes *mesh*, áreas que antes tinham uma abordagem simplista passaram a receber propostas mais rebuscadas. Comercialmente, existem soluções ofertadas, como por exemplo Tropos [Tropos 2008] e Meshdynamics [Meshdynamics 2001].

A principal aplicação que vem sendo avaliada e estudada nas redes *mesh* é VoIP (*Voice over IP*), como pode ser visto em [Xian e Huang 2007], onde já trata inclusive a questão de segurança em redes *mesh.*

A grande tendência dos estudos em redes *mesh*, independente de ser em segurança ou não, diz respeito a alocação e utilização de múltiplos rádios e canais, como por exemplo em [Haq et al. 2007] e [Naveed e Kanhere 2006]. Além disso, assim como gerenciamento é um assunto associado a segurança [Duarte et al. 2007] e [Siddiqui et al. 2008], gerenciamento de mobilidade também começa a ser estudado, como por exemplo em [Huang et al. 2007].

Referências Bibliográficas

802.11, IEEE (2007). IEEE Standard for Information Technology Telecommunications and Information Exchange between Systems-local and Metropolitan Area Networks Specific Requirements parte 11: Wireless lan medium access control (mac) and physical layer (phy) specifications. IEEE Std 802.11-2007 (Revisão de IEEE Std 802.11-1999).

802.11s, IEEE (2008) "Task Group S. Status of Project IEEE 802.11s". Disponível em <http://www.ieee802.org/11/Reports/tgs_update.htm>. Acessado em Junho de 2008.

Akyildiz, I. F.; Wang, X. e Wang, W. (2005) Wireless Mesh Networks: a Survey. Comput. Netw. ISDN Syst. Janeiro.

Anton, E.R. Duart, O.C. (2002) "Group key establishment in wireless ad hoc networks". In E.R. Workshop em Qualidade de Serviço e Mobilidade. Novembro.

Asokan N., Ginzborg P., (2000) "Key Agreement in Ad Hoc Networks", Computer Communications Volume 23.

Badonnel, R., State, R., and Festor, O. (2005) "Management of mobile ad hoc networks: information model and probe-based architecture". Int. J. Netw. Manag.

Becker K., Willie U., (1998) "Communication complexity of group key distribution", Proceedings of 5th ACM Conference on Computer and Communications Security, ACM Press.

Bird R., Gopal I., Herzberg A., Janson P., Kutten S., Molva R. , Yung M., (1995) "The KryptoKnight family of light-weight protocols for authentication and key distribution". IEEE/ACM Transactions on Networking, Volume 3 , Issue 1, Fevereiro.

Breuel, Cristiano Malanga. (2004) "Redes em Malha sem Fios". Instituto de Matemática e Estatística - Universidade de São Paulo (USP), Dezembro. Disponível em: <http://grenoble.ime.usp.br/movel/Wireless_Mesh_Networks.pdf>. Acessado em Janeiro de 2007.

Broch, J., Maltz, D., Johnson, D., Hu, Y. E Jetcheva, J. (1998) "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols". Proceedings of the 4th Annual ACM/IEEE International Conference on Mobile Computing and Networking. Outubro.

Bruno, R., Conti, M. e Gregori, E. (2005) "Mesh Networks: Commodity Multihop Ad Hoc Networks". IEEE Communications Magazine. Março.

Capkun, S., Buttyan, L., and Hubaux, J.-P. (2003). "Self-organized public-key management for mobile ad hoc networks". IEEE Transactions on Mobile Computing,

Chen, W., Jain N., Singh S., (1999) "ANMP: Ad Hoc Network Management Protocol", IEEE Journal on selected areas in communications, Vol. 17, No. 8, Agosto.

Chiang, C., Wu, H., Liu, W., Gerla, M. (1997) “Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel”. IEEE Singapore International Conference on Networks (SICON), pp. 197-211, Abril.

Duarte, J. (2008) “Escalabilidade, Gerência e Mobilidade para Redes Mesh de Acesso à Internet”. Dissertação de Mestrado, instituição Universidade Federal Fluminense – UFF.

Duarte, J.L.; Passos, D.; Valle, R.L.; Oliveira, E.; Muchaluat-Saade, D.; Albuquerque, C.V. (2007). “Management Issues on Wireless Mesh Networks”. Latin American Network Operations and Management Symposium (LANOMS), pp. 8 – 19. Setembro.

Faccin, S., Wijting, C., Kneckt, J. e Damle, A. (2006) “Mesh WLAN Networks: Concept and System Design”. IEEE Wireless Communications. Abril.

G. Pei, M. Gerla, Tsu-Wei Chen (2000) "Fisheye State Routing: A Routing Scheme for Ad Hoc Wireless Networks," IEEE ICC, vol. 1, pp. 70 -74.

GT-Mesh (2006) “RT1 – Termo de referência e estado da arte”. Disponível em <http://mesh.ic.uff.br>. Acessado em Junho de 2008.

Haas, Z. e Pearlman, M. (1998) "The zone routing protocol (ZRP) for ad hoc networks". Internet-Draft, draft-ietf-manet-zone-zrp-04.txt. Agosto.

Haas, Z.J. (1997) “A new routing protocol for the reconfigurable wireless networks”, IEEE Computer Society. Vol 2. pp. 562-566.

Hamid, Md. Abdul; Islam, Md. Shariful; Hong, Choong Seon. (2008). “Misbehavior Detection in Wireless Mesh Networks”. International Conference on Advanced Communication Technology (ICACT), Vol. 2, pp. 1167 – 1169, Fevereiro.

Hamid, Md. Abdul; Islam, Md. Shariful; Hong, Choong Seon. (2008). “Developing Security Solutions for Wireless Mesh Enterprise Networks”. IEEE Wireless Communications and Networking Conference (WCNC) 2008, pp. 2549 – 2554, Abril.

Hamid, Z., Khant, S. (2006) “An Augmented Security Protocol for WirelessMAN Mesh Networks”. IEEE.

Haq, A., Naveed, A., Kanhere, S. (2007) “Securing Channel Assignment in Multi-Radio Multi-Channel Wireless Mesh Networks”. IEEE Communications Society subject matter experts for publication in the WCNC 2007 proceedings.

Harada, Eduardo. (2006) “Wireless Mesh Networks: Uma tecnologia que promete”, Disponível em <http://sisnema.com.br/Materias/idmat017459.htm>. Acessado em Junho de 2008.

Held, G. (2005) “Wireless Mesh Networks”. 1ª Edição. USA, Auerbach Publications – Taylor & Francis Group.

Hiertz, G., Zang, Y., Max, S., Junge, T., Weiss, E., Wolz, B. (2008) “IEEE 802.11s: WLAN Mesh Standardization and High Performance Extensions”. IEEE Network, Junho.

Hong, F.; Fu, L. H. C. “Advanced Information Networking and Applications”, IEEE Computer Society, vol. 1. 2005, pp. 713-718.

Hu, Y. C., Perrig, A. (2004) “A Survey of Secure Wireless Ad Hoc Routing”, IEEE Computer Society, vol. 2, pp. 28-29.

Hu, Y. C., Perrig, A., Johnson, D. B. (2005) “Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks”. Portal ACM. vol. 11, pp. 21-38.

Hu, Y. C., Perrig, A., Johnson, D. B., (2003) “SEAD: Secure Efficient Distance Vector Routing for Mobile wireless ad hoc networks”. IEEE Computer Society. vol. 1. pp. 3-13.

Huang, R., Zhang, C., Fang, Y., (2007) “A Mobility Management Scheme for Wireless Mesh Networks”. IEEE Communications Society subject matter experts for publication in the IEEE GLOBECOM 2007 proceedings.

IEEE (2000). IEEE Standard Specifications for Public-Key Cryptography. IEEE Std 1363-2000.

Islam, Md. Shariful; Hamid, Md. Abdul; Hong, Choong Seon; Chang, Beom-Hwan . (2008). “Preserving Identity Privacy in Wireless Mesh Networks”. International Conference on Information Networking (ICOIN) pp. 1 – 5, Janeiro.

Janies, J.; Chin-Tser Huang; Johnson, N.L. (2006) “SUMP: A Secure Unicast Messaging Protocol for Wireless Ad Hoc Sensor Networks”. IEEE International Conference on Communications (ICC), Vol. 8, Issue , pp. 3663 – 3669, Junho.

Joa-Ng, M., Lu, I. T. (1999) “A Peer-to-Peer zone-based two-level link state routing for mobile Ad Hoc Networks”. IEEE Journal on Selected Areas in Communications, Special Issue on Ad-Hoc Networks, pp.1415-25, Agosto.

Jongtack, Kim; Saewoong, Bahk. (2008) “Distributed Certification Authority in Wireless Mesh Networks”. IEEE Consumer Communications and Networking Conference (CCNC), pp. 267 – 271, Janeiro.

Ju, N., Ju,D., Santhanam, L., He, B., Wang, J., Agrawal, D., (2007) “Wireless Mesh Networks: Current Challenges and Future Directions of Web-in-The-Sky”. IEEE Wireless Communications, Agosto.

K. Graffi (2006) “A Security Framework for Organic Mesh Networks,” Master’s thesis, TU-Darmstadt, Maio.

Karpijoki ,V. (2001), “Security in ad hoc networks”, no “Seminar on Network Security.

Kim, J., e Bahk, S. (2008) “MeCA: Distributed Certi.cation Authority in Wireless Mesh Networks”. IEEE Communications Society subject matter experts for publication in the IEEE CCNC 2008 proceedings.

Krebs, M., Krempels, K., Kucay, M. (2008) “Service Discovery in Wireless Mesh Networks”. IEEE Communications Society subject matter experts for publication in the WCNC 2008 proceedings.

Krebs, Martin; Krempels, Karl-Heinz; Kucay, Markus (2008) “Service Discovery in Wireless Mesh Networks”. IEEE Wireless Communications and Networking Conference (WCNC), pp. 3093 – 3098, Abril.

Kurose, James F, Ross, Keith W. (2006) “Redes de Computadores e a Internet – Uma abordagem Top-Down”. Addison Wesley. 3ª Edição.

Kyasanur, P., So, J., Chereddi, C., Vaidya Nitin H., (2007) “Multi-Channel Mesh Networks: Challenges and Protocols”, University of Illinois at Urbana-Champaign.

Disponível em <http://www.hserus.net/~cck/pubs/wcom.pdf>. Acessado em Junho de 2008.

Lee, M., Zheng, J., Ko, Y. e Shrestha, D. (2006) "Emerging Standards For Wireless Mesh Technology". IEEE Wireless Communications. Abril.

Li, Guangsong (2007) "An Identity-Based Security Architecture for Wireless Mesh Networks". NPC Workshops. IFIP International Conference on Network and Parallel Computing Workshops, pp. 223 - 226, Setembro.

Li, X., Yang, W., Moon, S., Mal, J. (2006) "Authentication Method for 802.11s Infrastructure Mode". IEEE.

Li, Xiang-Yang; Wu, Yanwei; Wang, WeiZhao. (2007) "Stochastic Security in Wireless Mesh Networks via Saddle Routing Policy". International Conference on Wireless Algorithms, Systems and Applications, pp. 121 – 128.

Lin C., (1997) "Dynamic key management schemes for access control in a hierarchy", Computer Communications, Vol 20, No 15, Dezembro.

Lin, X., Lu, R., Ho, P., Shen, X., Cao, Z. (2008 "TUA: A Novel Compromise-Resilient Authentication Architecture for Wireless Mesh Networks". IEEE Transactions on Wireless Communications, Vol. 7, No. 4, Abril.

Lou, W., Fang, Y. (2004) "A Survey on Wireless Security in Mobile Ad Hoc Networks: Challenges and Possible Solutions", edited by X. Chen, X. Huang and D.-Z. Du, Kluwer Academic Publishers/Springer.

Luiz, A., Júnior, O. (2005) "Infra-estrutura e Roteamento em Redes Wireless Mesh", Pontifícia Universidade Católica do Paraná – PUC-PR.

Mahmoud, A., Sameh, A.,El-Kassas, S. (2005) "Reputed authenticated routing for ad hoc networks protocol (reputed-ARAN)". IEEE Computer Society, pp. 258-259.

Maki S., Aura T., Hietalahti M. (2000) "Robust membership management for ad-hoc groups." In Proc. 5th Nordic Workshop on Secure IT Systems (NORDSEC 2000), Reykjavik, Iceland.

Meshdynamics Home Page (2001) "High Performance Outdoor Wireless Mesh Networking". Disponível em <http://www.meshdynamics.com/>. Acessado em Junho de 2008.

Mishra, A., NAadkami K., Patcha, A. (2004) "Intrusion detection in wireless ad hoc networks". IEEE Wireless Communications, vol. 11. pp 48-60.

Mogre, Parag S., Graffi, K´alm´an, Matthias Hollick, and Ralf Steinmetz (2007) "AntSec, WatchAnt, and AntRep: Innovative Security Mechanisms for Wireless Mesh Networks". 32nd IEEE Conference on Local Computer Networks (LCN), pp. 539 – 547, Outubro.

MotoMesh (2008). Disponível em <http://www.motorola.com/business/v/index.jsp?vgnextoid=ef98fde3807f6110VgnVCM1000008406b00aRCRD> . Acessado em Junho de 2008.

Murthy, C. e Manoj, B. (2004) "Ad Hoc Wireless Networks: Architectures and Protocols". 1ª Edição. USA, Prentice Hall Professional Technical Reference.

Naveed, A., Kanhere, S. (2006) “Security Vulnerabilities in Channel Assignment of Multi-Radio Multi-Channel Wireless Mesh Networks”. IEEE Communications Society subject matter experts for publication in the IEEE GLOBECOM 2006 proceedings.

Ornaghi, A., Valleri, M. (2008) “Etercap”. Disponível em <http://ettercap.sourceforge.net>. Acessado em julho de 2008.

Papadimitatos, P., Haas, Z. J. (2003) “Secure link state routing for mobile ad hoc networks”. IEEE Computer Society. pp 379-383.

Perkins, C. E. (1994) “Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers”. Portal ACM, vol. 24, pp 234-244.

Rahman, S. M. M., Inomata, A., Okamoto, T., Mambo, M., Okamoto, E. (2006) “Anonymous secure communication in wireless mobile ad-hoc networks”. Proc. 1st Intl. Conf. on Ubiquitous Convergence Technology, pp. 131–140, Dezembro.

Raya, M., Hubaux, J-P. (2007) “Securing vehicular ad hoc networks,” Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Networks, vol. 15, no. 1, pp. 39–68.

RFC 3561 (2003), “Ad hoc On-Demand Distance Vector (AODV) Routing”. Disponível em <http://www.ietf.org/rfc/rfc3561.txt>, visitado em julho de 2008.

RFC 3626 (2003), “Optimized Link State Routing Protocol (OLSR)”. Disponível em <http://www.ietf.org/rfc/rfc3626.txt>, visitado em julho de 2008.

Royer, E., Toh, C. (1999) “A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks”. IEEE Personal Communications, pp. 46 – 55, Abril.

S. Murthy and J. J. Garcia-Luna-Aceves (1996) “An Efficient Routing Protocol for Wireless Networks”. ACM Mobile Networks and App. J., Special Issue on Routing in Mobile Communication Networks, pp. 183–97, Outubro.

S. Seys and B. Preneel, (2006) “ARM: Anonymous routing protocol for mobile ad hoc networks”. Proc. 20th Int’l Conf. on Advanced Information Networking and Applications (AINA), pp. 133–137, Abril.

Salem, B. N.; Hubaux, J.-P.; (2006) “Securing Wreless Mesh Networks”. IEEE Wirelesss Communications. Abril.

Salem, N. B. and Hubaux, J-P. (2006) “Securing Wireless Mesh Networks”, in IEEE Wireless Communication, Vol 13, Issue 2, pp. 50 – 55, Abril.

Siddiqui, M. S., Amin, S. O., Hong, C. S., (2008) “An Efficient Mechanism for Network Management in Wireless Mesh Network”. 10th International Conference on Advanced Communication Technology (ICACT), Vol 1, pp. 301 – 305, Fevereiro.

Siddiqui, M. S., Amin, S. O., Kim, J., Hong, C., (2007) “MHRP: A secure multi-path hybrid routing protocol for wireless mesh network”

Siddiqui, M. S., Hong, C. S. (2007) “Security Issues in Wireless Mesh Networks”. International Conference on Multimedia and Ubiquitous Engineering (MUE), pp. 717 – 722, Abril.

Sivakumar, R., Sinha, P. e Bharghavan, V. (1998) "Core extraction distributed ad hoc routing (CEDAR) specification". Internet-Draft, draft-ietf-manetzone-cedar-00.txt. Outubro.

Song, R., Korba, L., Yee, G. (2005) “AnonDSR: efficient anonymous dynamic source routing for mobile ad-hoc networks”. Portal ACM. pp 33-42.

Stallings W., (1998) “Snmp, SnmpV2, Snmpv3, Rmon 1 e 2”. Addison-Wesley Longman Publishing Co., Inc. Boston, MA, USA

Sun, J., Zhang, C., Fang, Y. (2008) “A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks”. IEEE INFOCOM 2008.

Takeda, S., Yagyu, K., Aoki, H., Matsumoto, Y. (2005) “Multi-Interface Oriented Radio Metric On-Demand Routing Protocol for Layer-2 Mesh Network”. IEICE Technical Report RCS2005-59, Julho.

Tamashiro, C. (2007) “Uma Análise de Protocolos de Roteamento Anônimo para Redes Sem Fio Ad Hoc Móveis”. Dissertação de Mestrado, instituição Universidade Federal de Santa Catarina – UFSC.

Tropos Home Page (2008) “ Wireless Broadband You Control”. Disponível em <http://www.tropos.com/>. Acessado em Junho de 2008.

Xian, Y., Huang, C. (2007) “Securing VoIP Services in Multi-Hop Wireless Mesh Networks”. IEEE ISWCS.

Xiao, Yang (2008) “Accountability for Wireless LANs, Ad Hoc Networks, and Wireless Mesh Networks”. IEEE Communications Magazine, pp 116 a 126, Abril.

Xue, Q., Ganz, A. (2005) “QoS routing for Mesh-based Wireless LANs”, Department of Electrical and Computer Engineering - University of Massachusetts. Disponível em <http://www-unix.ecs.umass.edu/~qxue/publ/WMR_April(IJWIN).pdf>. Acessado em Junho de 2008.

Zapata, M. G. (2002) “Secure ad hoc on-demand distance vector routing”. Portal ACM. vol. 6. pp. 106-107.

Zhang, Y., Fang, Y. (2006) “ARSA: An attack-resilient security architecture for multihop wireless mesh networks,” IEEE J. Select. Areas Communications, vol. 24, no. 10, pp. 1916–1928, Outubro.

Zhang, Z., Nait-Abdesselam, F., Ho, P., Lin, X. (2008) “RADAR: a ReputAtion-based Scheme for Detecting Anomalous Nodes in WiReless Mesh Networks”. IEEE Communications Society subject matter experts for publication in the WCNC 2008 proceedings.

Zheng, X., Chen, C., Huang, C., Matthews, M., Santhapuri, N. (2004) “A Dual Authentication Protocol for IEEE 802.11 Wireless LANs”. Disponível em <http://www.cse.sc.edu/~huangct/iswcs05cr.pdf >. Acessado em Junho de 2008.

Zhou, L, Haas, Z. J. (1999) “Securing ad hoc networks,” IEEE Network Magazine, vol. 13, no. 6, pp. 24–30, Dezembro.

Zhu, H., Lin, X., Lu, R, Ho, P., Shen, X. (2007) “Secure Localized Authentication and Billing for Wireless Mesh Networks”. IEEE Communications Society subject matter experts for publication in the IEEE GLOBECOM 2007 proceedings.