UNIVERSIDADE FEDERAL DE JUIZ DE FORA
INSTITUTO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE CIÊNCIA DA COMPUTAÇÃO

ESTUDO COMPARATIVO DOS PROTOCOLOS DE ROTEAMENTO SEGURO DE REDES EM MALHA SEM FIO

Wallace Knopp de Menezes Gerheim

JUIZ DE FORA
JULHO, 2010

ESTUDO COMPARATIVO DOS PROTOCOLOS DE ROTEAMENTO SEGURO DE REDES EM MALHA SEM FIO

WALLACE KNOPP DE MENEZES GERHEIM

Universidade Federal de Juiz de Fora
Instituto de Ciências Exatas
Departamento de Ciência da Computação
Bacharel em Ciência da Computação

Orientador: Prof.º Ms. Eduardo Pagani Julio

JUIZ DE FORA
JULHO, 2010

ESTUDO COMPARATIVO DOS PROTOCOLOS DE ROTEAMENTO SEGURO DE REDES EM MALHA SEM FIO

Wallace Knopp de Menezes Gerheim

MONOGRAFIA SUBMETIDADA AO CORPO DOCENTE DO INSTITUTO DE CIÊNCIAS EXATAS DA UNIVERSIDADE FEDERAL DE JUIZ DE FORA COMO PARTE INTEGRANTE DOS REQUISITOS NECESSÁRIOS PARA OBTENÇÃO DO GRAU DE BACHAREL EM CIÊNCIA DA COMPUTAÇÃO.

Aprovada por:

_____

Eduardo Pagani Julio, Mestre

(Presidente)

_____

Eduardo Barrere, Doutor

_____

Ely Edison da Silva Matos, Mestre

JUIZ DE FORA, MG – BRASIL
JULHO, 2010

AGRADECIMENTOS

Agradeço a Deus pela oportunidade de reencarnar e me aprimorar a cada dia.
Aos meus pais, Antônio e Soraya, pelo amor, confiança e apoio em todos os momentos.
Ao meu irmão Douglas, por ser um grande companheiro.
À Luciana, por todo carinho e dedicação.
Às minhas tias, tios e avós, em especial a Tia Vânia, Tia Nilva, Tio Márcio e Vó Ilva por serem presença constante em minha vida.
Ao meu orientador, Eduardo Pagani, pelo conhecimento passado e por seu apoio.
Aos componentes da banca examinadora pela disponibilidade e boa vontade.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

AE	*Address Extension*
AODV	*Ad-hoc On-Demand Vector*
ARAN	*Authenticated Routing for AdHoc Networks*
AS	Associação de Segurança
CAM	Código de Autenticação de Mensagem
DO	*Destination Only*
DoS	*Denial of Service*
DSDV	*Destination Sequenced Distance Vector*
DSR	*Dynamic Source Routing*
GTK	*Group Transit Key*
HWMP	*Hybrid Wireless Mesh Protocol*
IEEE	*Institute of Electrical and Electronics Engineers*
IP	*Internet Protocol*
LAN	*Local Area Network*
MAC	*Media Access Control*
MANET	*Mobile Ad-hoc Networks*
MAP	*Mesh Access Points*
MIM	*Man-in-the-Middle*
MIT	Massachusetts *Institute of Technology*
MP	*Mesh Points*
MPP	*Mesh Portal Points*
MPR	*Multipont Relays*
MR-LQSR	*Multi-Radio Link-Quality Source Routing*
NAT	*Network Address Translation*
OLSR	*Optimized Link State Routing*

PDA	*Personal Digital Assistants*
PREP	*Path Reply Message*
PREQ	*Path Request Message*
PTK	*Pairwise Transient Key*
QoS	*Quality of Service*
RANN	*Root Announcement Messages*
RA-OLSR	*Radio-Aware Optimized Link State Routing*
RDP	*Route Discovery Packet*
REP	*Reply*
RF	*Reply and Forward*
RIP	*Routing Information Protocol*
RREP	*Route Reply*
RREQ	*Route Request*
SAODV	*Secure Adhoc On-Demand Vector*
SAR	*Security-Aware Adhoc Routing*
SHWMP	*Secure Hybrid Wireless Mesh Protocol*
SOSLR	*Secure Optimized Link State Routing*
SRP	*Secure Routing Protocol*
STA	*Stations*
TTL	*Time To Live*
WLAN	*Wireless Local Area Network*
WMN	*Wireless Mesh Networks*
ZRP	*Zone Routing Protocol*

RESUMO

Este trabalho foi realizado com a finalidade de descrever as tecnologias de redes sem fio existentes, apresentando alguns padrões desenvolvidos pelo IEEE, em destaque o 802.11s, funcionamento da sua arquitetura, infra-estruturadas ou *ad hoc,* bem como os tipos de protocolos de roteamento. O estudo é focado nas redes em malha sem fio, abordando seu funcionamento, arquitetura e protocolos de roteamento utilizados. A dinamicidade dessa rede a expõe a diversos tipos de ataques que são abordados no trabalho. A fim de eliminar ou minimizar essas falhas, são estudados os protocolos de roteamento seguro utilizados em redes *ad hoc* e *mesh* e ao final é realizado um estudo comparativo entre os protocolos de roteamento apresentados.

Palavras Chave: Roteamento. Seguro. *Mesh*

ABSTRACT

This study was intended to outline the technologies of existing wireless networks, with some standards developed by IEEE, highlighted the 802.11s, the functioning of its architecture, infrastructure or ad hoc, and the types of routing protocols . The study is focused on wireless mesh networks, discussing their operation, architecture and routing protocols used. The dynamics of this network exposes it to various types of attacks that are covered at work. In order to eliminate or minimize these failures, we have studied the secure routing protocols used in ad hoc networks and mesh and the final is a comparative study between these routing protocols presented.

Key-words: Routing. Secure. Mesh

1 INTRODUÇÃO

As redes sem fio estão se tornando cada vez mais populares devido sua facilidade de acesso, mobilidade e instalação. Em conseqüência disso, seu custo de implantação está se tornando cada vez menor, podendo ser utilizada em shoppings, universidades, domicílios, entre outros.

O modo mais comum de operação das redes sem fio é dependente de uma infra-estrutura que provê acesso a serviços, como o roteamento. Essa característica limita a expansão da rede já que as máquinas devem se limitar ao posicionamento físico dentro da cobertura do ponto de acesso. Em contrapartida, outro modo pode ser utilizado baseando-se no modelo *ad-hoc*. Este não exige a existência de uma entidade provedora de serviços básicos de uma rede estruturada, sendo essa função realizada pelos próprios clientes (nós). A área de cobertura se expande devido às estações se comunicarem por múltiplos saltos. Essas redes devem ser robustas, a fim de garantir o desempenho na comunicação entre os nós sem exigir excessivo consumo de recursos destes, como o processamento, ou da rede, como a banda. O modelo, entretanto, exige forte colaboração entre os participantes.

As redes em malha sem fio são uma evolução das redes *ad-hoc* e têm a particularidade da presença de um *backbone* responsável por estender o alcance do sinal, permitindo também que os participantes não se limitem somente a dispositivos sem fio. Essa característica aliada ao baixo custo de implementação faz com que as redes em malha sem fio sejam utilizadas para os mais variados fins, como por exemplo, em universidades. Por utilizarem múltiplos saltos, tanto para seus usuários quanto no *backbone*, a rede poderá estar sujeita a várias falhas de segurança.

Alguns atributos de segurança são necessários nas redes em malha sem fio para que informações não sejam interceptadas, rotas não sejam desviadas e recursos, de energia e computacionais, não sejam desperdiçados

O foco deste trabalho se dará nos problemas de segurança na camada rede e são abordados algumas soluções de protocolos de roteamento seguro, como o SAODV (*Secure Ad hoc On Demand Vector*), Ariadne, SOLSR (*Secure Optimized Link State Routing*)e o SHWMP (*Secure Hybrid Wireless Mesh Protocol*).

Num primeiro momento serão mostradas as características das redes sem fio, como sua arquitetura e padrões IEEE 802.11, a arquitetura de *ad-hoc* bem como a

apresentação das redes em malha sem fio e alguns protocolos de roteamento. Destaca-se o protocolo HWMP (*Hybrid Wireless Mesh Protocol*) designado pelo IEEE 802.11s como o padrão para redes em malha sem fio.

Dando continuidade ao trabalho, o Capítulo 3 apresenta os atributos desejáveis para garantir a segurança do ambiente de rede e alguns tipos de ataques nas camadas física, de enlace e de rede.

No Capítulo 4 é realizado um estudo dos protocolos de roteamento seguro nas redes em malha sem fio e é feito também um comparativo entre eles.

Finalizando o trabalho, o Capítulo 5 apresenta as considerações finais sobre o conteúdo discutido neste trabalho.

2 REDES SEM FIO

Na década de 70 pesquisas envolvendo uma forma de conectar computadores situados em ilhas diferentes do Havaí culminaram com o desenvolvimento do projeto ALOHANET. A solução era equipar cada terminal com rádios de ondas curtas e que, para transmitir as informações, um terminal deveria esperar o outro terminar o envio para que, assim, pudesse começar o seu. Com esse acontecimento, surgiram as redes sem fio (TANEMBAUM, 2003).

O avanço das pesquisas e de tecnologias aumentou significativamente o uso da comunicação sem fio (*wireless*). Além de eliminar as barreiras geográficas, o que permitiu acesso a regiões rurais, por exemplo, sua utilização é mais fácil se comparada às comunicações cabeadas, bastando os dispositivos se disporem dentro da área de cobertura do sinal.

Neste capítulo são abordados alguns conceitos básicos relacionados às redes sem fio, como sua arquitetura e padrões, que servem de subsídio para a compreensão do objetivo do trabalho. Será analisada também a arquitetura *ad-hoc* e seus tipos de protocolos de roteamento. Por fim, são estudadas as redes *mesh* sem fio e alguns protocolos de roteamento utilizados.

2.1 ARQUITETURA DE REDES SEM FIO

Os sistemas comuns de comunicação sem fio formam redes isoladas e em *stand alone.* A sua expansão permitiu a rápida difusão de aparelhos portáteis e com acesso a redes sem fio, como *notebooks* e *palms*. Para entender a estrutura de uma rede sem fio, é necessário definir os componentes que a integram. Segundo Kurose e Ross (2005), os elementos podem ser descritos da seguinte forma:

- *Enlace sem fio*: Tipo de enlace em que o dispositivo irá se conectar à estação-base. O enlace sem fio utilizará o ar como meio de transmissão dos dados.
- *Hospedeiro sem fio*: São formados pelos usuários, portáteis ou não, que utilizam o ar para transmitirem as informações.

- *Estação base*: É responsável por enviar e receber os dados de um hospedeiro sem fio a outro. Os dois hospedeiros devem estar associados à estação-base de forma que estejam dentro do alcance de comunicação desta. É notável também a utilização das estações base em garantir o acesso a outras redes, como a internet.

Os dispositivos utilizados nas redes sem fio variam desde desktops até celulares, que neste caso dependem de uma estrutura de antenas instaladas em topo de edifícios e em torres.

A arquitetura dessas redes depende de estações estacionárias e de uma infra-estrutura para conectar os dispositivos sem fio. Contudo, em alguns locais não é possível estabelecer esse tipo de arquitetura em decorrência da demografia, custo ou situação de emergência. Numa guerra, por exemplo, as estações que provêem acesso à rede no campo de batalha poderão ser destruídas, não existindo o tempo necessário para sua reconstrução. A utilização de outros dispositivos sem fio, portáteis ou não, como mantenedores da rede garantiria a resiliência desta que, apesar de inexistir as estações base, não perderiam a conectividade entre si.

As redes sem fio podem operar de duas formas, no modo de infra-estrutura ou no modo *ad-hoc*. Em Kurose e Ross (2005) são definidos os modos de operação das redes sem fio:

- *Modo de infra-estrutura*: a topologia é caracterizada pelos hospedeiros utilizarem os serviços da rede em que estão conectados e serem coordenados por uma estação-base, que proverá serviços essenciais como roteamento, NAT (*Network Address Translation*) e resolução de nomes. A Figura 1 mostra cinco clientes utilizando a infra-estrutura sem fio, provida pelo *Acess Point.*

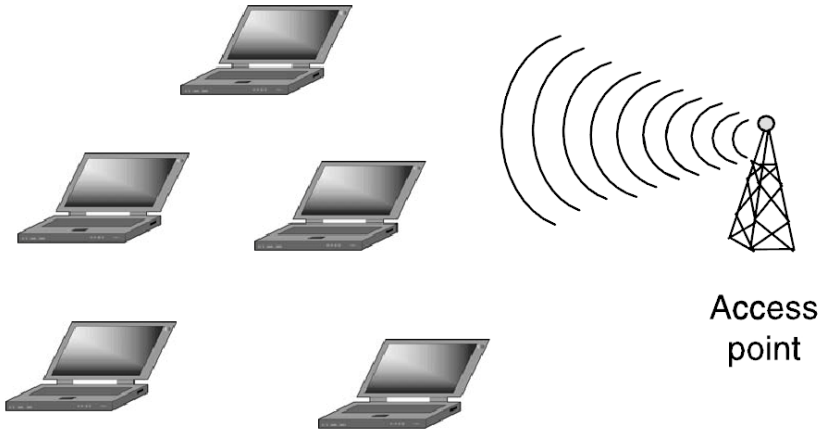

FIGURA 1 – MODO DE INFRA-ESTRUTURA (ANJUM e MOUCHTARIS, 2007)

- *Modo ad-hoc*: é caracterizada pelos hospedeiros não utilizarem uma estação-base como coordenadora dos serviços de rede, sendo os próprios hospedeiros encarregados de re-encaminhar os pacotes entre os demais membros da rede. Neste sentido, os *hosts* são classificados como nós, já que realizam a função de roteador e de *host* (TANEMBAUM, 2003). A Figura 2 ilustra o modo de operação *ad-hoc*, em que diferentes tipos de clientes – um *desktop*, um *laptop* ou um *tablet,* por exemplo - estão conectados entre si, não dependendo, portanto, de uma estação base.

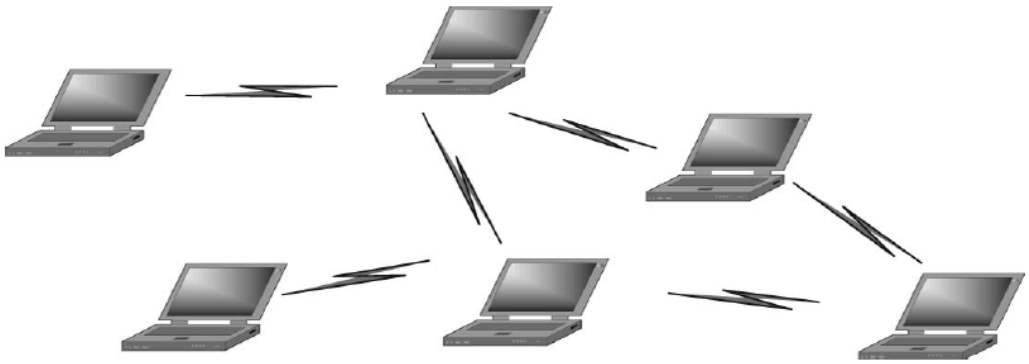

FIGURA 2 – MODO *AD-HOC* (ANJUM e MOUCHTARIS, 2007)

2.2 PADRÃO 802.11

A difusão das LANs (*Local Area Networks*) sem fio originou um problema de compatibilidade. Um hospedeiro que possuía um equipamento sem fio de uma determinada marca poderia não se comunicar com a estação-base caso ela estivesse equipada com um equipamento de outra marca. A fim de se seguir uma norma de serviço para as LANs sem fio, o IEEE (*Institute of Electrical and Electronics Engineers*) desenvolveu o padrão 802.11 (TANEMBAUM, 2003).

O padrão possui descrições que envolvem o desempenho, qualidade de serviço, segurança, interoperabilidade e compatibilidade de WLANs (*Wireless Local Area Network*).

A Tabela 1 relaciona o padrão 802.11 à sua descrição:

TABELA 1 – PADRÕES 802.11 (NAKAMURA E GEUS, 2007)

Padrão IEEE	**Descrição do padrão**
802.11a	Descreve redes que atuam com banda de 5 GHz e com taxa máxima de 54 Mbps em cada canal.
802.11b	O padrão descreve redes que atuam com banda de 2,4 GHz e que atingem 11 Mbps por canal. É o mais utilizado em produtos WLAN.
802.11d	É destinado a promover o uso do 802.11 em países que não suportam o padrão corrente.
802.11e	Utilizado pelos padrões 802.11a, 802.11b e 802.11g, foi desenvolvido para fornecer QoS, oferecendo vídeo e áudio em demanda e serviços de acesso de alta velocidade a VOIP
802.11g	Comercializados ao final de 2002, os produtos desenvolvidos com este padrão possuem desempenho e compatibilidade com o 802.11b e velocidade similar ao 802.11a. Atua nas bandas de 2,4 GHz e 5 GHz.
802.11h	Adéqua o 802.11a às normas da União Européia. Atua na banda de 5 GHz e trata mecanismos de controle de energia.
802.11i	O padrão amplia mecanismos de segurança e autenticação. Fornece formas de criptografia robustas, mecanismos de autenticação e um mecanismo de distribuição de chaves. Além do ponto de acesso e do cliente, o padrão define um servidor de autenticação como qual o ponto de

	acesso deverá se comunicar.
802.11j	Utilizado nas bandas de 4,9 GHz e 5 GHz, adéqua o 802.11 às normas japonesas.
802.11X	Define um framework de controle ao acesso à rede com base em portas.

2.3 PADRÃO 802.11s

A crescente difusão de redes *ad-hoc* exige que normas que tratem de padrões para essas redes sejam pensadas a fim de garantir a integração, desempenho e segurança entre equipamentos dessa natureza. Para isto, um grupo do IEEE, publicou, em 2006, um *draft* em que estão descritos padrões para dispositivos e protocolos. Como pode ser observado em Saade *et al* (2008, p.23), o padrão estabelece "(...) novos formatos de quadros, trata de questões como segurança e gerenciamento, assim como uma série de otimizações necessárias para a montagem de redes em malha de múltiplos saltos no nível de enlace. Além disso, boa parte de seu conteúdo é dedicada à descrição de protocolos para encaminhamento de quadros na rede em malha."

Vários protocolos de roteamento foram desenvolvidos e são abordados no Capítulo 4. Entretanto, inicialmente, dois protocolos de roteamento foram propostos para serem utilizados: o RA-OLSR (*Radio-Aware Optimized Link State Routing*), baseado no OLSR (*Optimized Link State Routing*), e o HWMP, baseado no AODV(*Ad hoc On Demand Vector*).

O 802.11s adotou o HWMP como protocolo padrão e a métrica *Airtime Link Metric* para a seleção do caminho considerando a qualidade de um enlace sem fio. Saade *et al* (2008) afirma que a métrica representa "(...) a quantidade de tempo necessária para a transmissão de um quadro, levando em consideração a taxa de transmissão, o overhead imposto pela camada física e a probabilidade de retransmissão do quadro(...). A forma de cálculo desta taxa de erros, no entanto (...) não é descrita pela norma".

Uma extensão é adicionada aos quadros 802.11 para se adequar ao padrão. A Figura 3 ilustra o formato geral de um quadro 802.11 em que o campo *Mesh Header* está incluso. A Figura 4 mostra detalhes do campo *Mesh Header.*

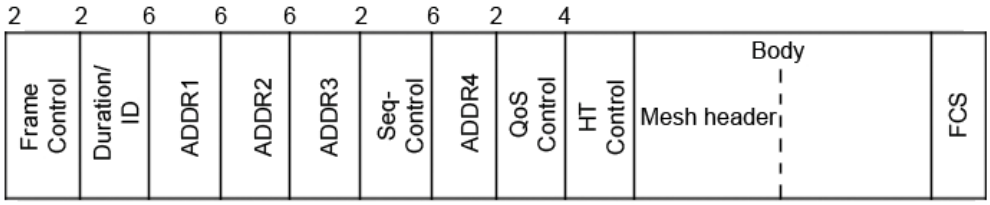

FIGURA 3 – ESTRUTURA DO QUADRO 802.11s (Fonte: SAADE *et al,* 2008)

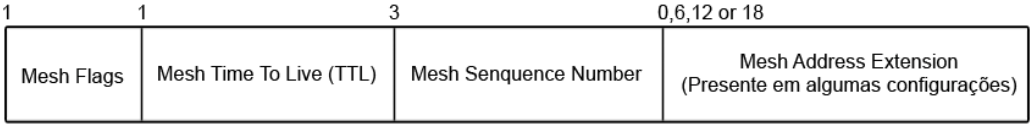

FIGURA 4 – *MESH HEADER* (Fonte: SAADE *et al,* 2008)

O primeiro campo, *Mesh Flags*, é o responsável por definir os dois primeiros bits que determinam a quantidade de endereços MAC (*Media Access Control*) em *Mesh Address Extension*. Este pode variar de 0 a 3 indicando um campo de 0, 6, 12 ou 18 bytes, visto que o endereço contém 6 bytes.

O campo *Mesh TTL* representa a quantidade de saltos que um quadro poderá fazer dentro da rede, sendo decrementado em cada nó a que passar evitando, portanto, que loops ocorram.

O *Mesh Sequence Number* identifica o quadro, prevenindo, desta forma, que duplicatas do quadro sejam retransmitidas pela rede.

Por se tratar de um padrão ainda em desenvolvimento, várias melhorias devem ser implementadas para prover os recursos esperados nas redes *mesh*.

2.4 ARQUITETURA *AD-HOC*

As redes que suportam o modo de operação *ad-hoc* são também denominadas de MANETs (*Mobile Ad-hoc Networks*) visto serem sistemas autônomos, de *hosts* móveis, conectados a uma rede sem fio e que não apresentam suporte de uma infra-estrutura fixa ou de um administrador central (SESAY, 2004). Nesse tipo de rede, todos os *hosts*, ou nós, podem se mover livremente já que estão conectados de forma dinâmica entre si. Esta característica permite que a rede se auto-construa, já que a qualquer momento novos dispositivos sem fio podem ser integrados, e se auto-recupere, no caso

de uma conexão com um dispositivo ser perdida podendo ser estabelecida com outro. Desta forma, caso o *host* deseje se movimentar e o nó ao qual se está conectado não conceder o alcance de sinal de rádio necessário, aquele buscará outro *host* ao qual deverá se conectar.

Anastasi, Conti e Gregori (2005) definem que em redes operando em modo *ad-hoc* os dispositivos móveis dos usuários devem agir de modo cooperativo de forma que os serviços de uma rede infra-estruturada também sejam obtidos em uma rede *ad-hoc*.

2.4.1 Tipos de Protocolos de Roteamento

Em contraste com camada de enlace, que se responsabiliza por encaminhar os quadros pelo meio físico, a camada de rede é a responsável pela transferência dos pacotes da origem para o destino (TANEMBAUM, 2003).

Em geral, o roteamento em redes *ad-hoc* é multisalto visto que os *hosts* podem não estar dentro do raio de comunicação das antenas umas das outras. Devido à dinamicidade das conexões nas MANETs, as rotas são quebradas com grande facilidade. Os algoritmos devem ser, portanto, adaptáveis às mudanças freqüentes de topologia

A seguir são abordados três tipos de protocolos utilizados: pró-ativos, reativos e híbridos.

2.4.1.1 Protocolos pró-ativos

A fim de garantir que a topologia da rede esteja atualizada, os protocolos pró-ativos são construídos para que os nós troquem mensagens de forma constante. Apropriando da definição de Farias e Bezerra (2006, p.5), "(...) [protocolos pró-ativos] exigem que todos os nodos da rede mantenham a rota de todos os possíveis destinos de modo que, quando houver necessidade do envio de um pacote de dados, a rota seja conhecida para ser usada, imediatamente". Dessa forma, as tabelas de roteamento contêm o caminho mais curto para cada nó dentro da rede. Esse tipo de protocolo demanda grande utilização de recursos de energia e de banda, já que necessita de constante processamento de mensagens a serem enviadas. Essa característica é prejudicial visto que os nós podem não conter recursos de energia, banda e

processamento suficientes que garantam o bom desempenho para a rede. Fazem parte da lista de protocolos pró-ativos o DSDV *(Destination Sequenced Distance Vector)*, OLSR e o WRP (*Wireless Routing Protocol*).

2.4.1.2 Protocolos reativos

Farias e Bezerra (2006) definem protocolos reativos como "(...) protocolos onde os nodos descobrem os destinos sob-demanda, ou seja, não necessitam de uma rota para os destinos até que precisem enviar pacotes dados para os destinos". Sendo assim, os protocolos reativos enviam mensagens de controle da topologia da rede sob demanda, buscando uma rota para o destino somente quando necessitam enviar pacotes de dados para este. Essa característica permite que a utilização dos recursos de energia dos nós e a banda da rede sejam utilizadas de forma eficiente. DSR (*Dynamic Source Routing*) e AODV fazem parte dos protocolos reativos.

2.4.1.3 Protocolos híbridos

Apenas parte dos nós atualizam periodicamente as informações de rotas dos destinos. Os protocolos híbridos buscam integrar as melhores características dos protocolos pró-ativos e reativos (FARIAS E BEZERRA, 2006). Faz parte da lista de protocolos híbridos o ZRP (*Zone Routing Protocol*) e o HWMP.

2.5 REDES *MESH* SEM FIO

Redes *mesh* são uma expansão das redes *ad-hoc*, mantendo sua auto-configuração, auto-recuperação e a conectividade em malha (AKYILDIZ e WANG, 2005). Se por um lado redes *ad-hoc* são aplicadas em situações aonde não exista qualquer infra-estrutura de comunicação, as redes *mesh* se beneficiam da existência de um *backbone*. Este é formado basicamente de roteadores que têm a responsabilidade de encaminhar todo o tráfego realizado através dos múltiplos saltos.

As WMNs (*Wireless Mesh Networks*) são caracterizadas por serem formadas de roteadores e clientes *mesh*. Duas características dos roteadores possibilitam a alta disponibilidade da rede: múltiplas interfaces de rede e pequena, ou nenhuma,

mobilidade. A primeira característica permite a integração entre vários tipos de redes IEEE802 garantindo acessibilidade em qualquer situação. Já a segunda elimina um sério problema dessa arquitetura: os baixos recursos de energia. Por serem fixos, os roteadores podem ser facilmente alimentados eliminando restrições como o esgotamento de energia pelo demasiado processamento.

Segundo Akyildiz e Wang (2005), apesar de ser uma extensão das redes *ad-hoc*, as redes em malha sem fio possuem a particularidade de possuírem baixo custo, facilidade de manutenção, robustez, confiabilidade, grande cobertura de serviço, entre outros. Devido a essas características as redes em malha estão sendo amplamente utilizadas em redes comunitárias, empresas, universidades, centros de pesquisa a fim de prover acesso a estudantes e usuários freqüentadores dessas regiões. Podem ser citados os projetos ReMesh (ReMesh, 2010) em Niterói/RJ (desenvolvido pela parceria da Universidade Federal Fluminense, Universidade Federal do Pará, a Pontifícia Universidade Católica do Paraná e a Universidade Tecnológica Federal do Paraná, que vem sendo financiado pela Rede Nacional de Ensino e Pesquisa), o RoofNet (RoofNet, 2010) desenvolvido pelo MIT (Massachusetts *Institute of Technology*), o CiscoMesh (CiscoMesh, 2010) desenvolvido pela Cisco, entre outros.

2.5.1 Arquitetura

Akyildz, X. Wang e W. Kiyon (2005) classificam a arquitetura das redes *mesh* em:

- *WMNs de infra-estrutura/Backbone*: Nessa arquitetura, os roteadores *mesh*, formam o *backbone* de acesso para os clientes *mesh*. Podem ser utilizados diversos padrões do IEEE802, como o *wireless* e o Ethernet. Caso os clientes estejam utilizando tecnologias de rádio iguais às utilizadas pelos roteadores, podem se comunicar diretamente com estes. Caso contrário, devem se conectar a um roteador que possua o mesmo padrão. Os roteadores *mesh* tem a capacidade de se auto-configurarem e auto-recuperarem entre si. Com a função de gateway, os roteadores podem prover acesso à internet. A Figura 5 ilustra os integrantes do *backbone*. Os *Mesh Router* são os roteadores responsáveis por

aumentarem a cobertura do sinal e prover o acesso em malha. Os *Mesh Router* com função de *gateway/bridge* se responsabilizam de garantir o acesso à rede e à internet (caso haja) aos *Wired Clients* (clientes com interface Ethernet) e aos *Wireless Clients* (clientes sem fio).

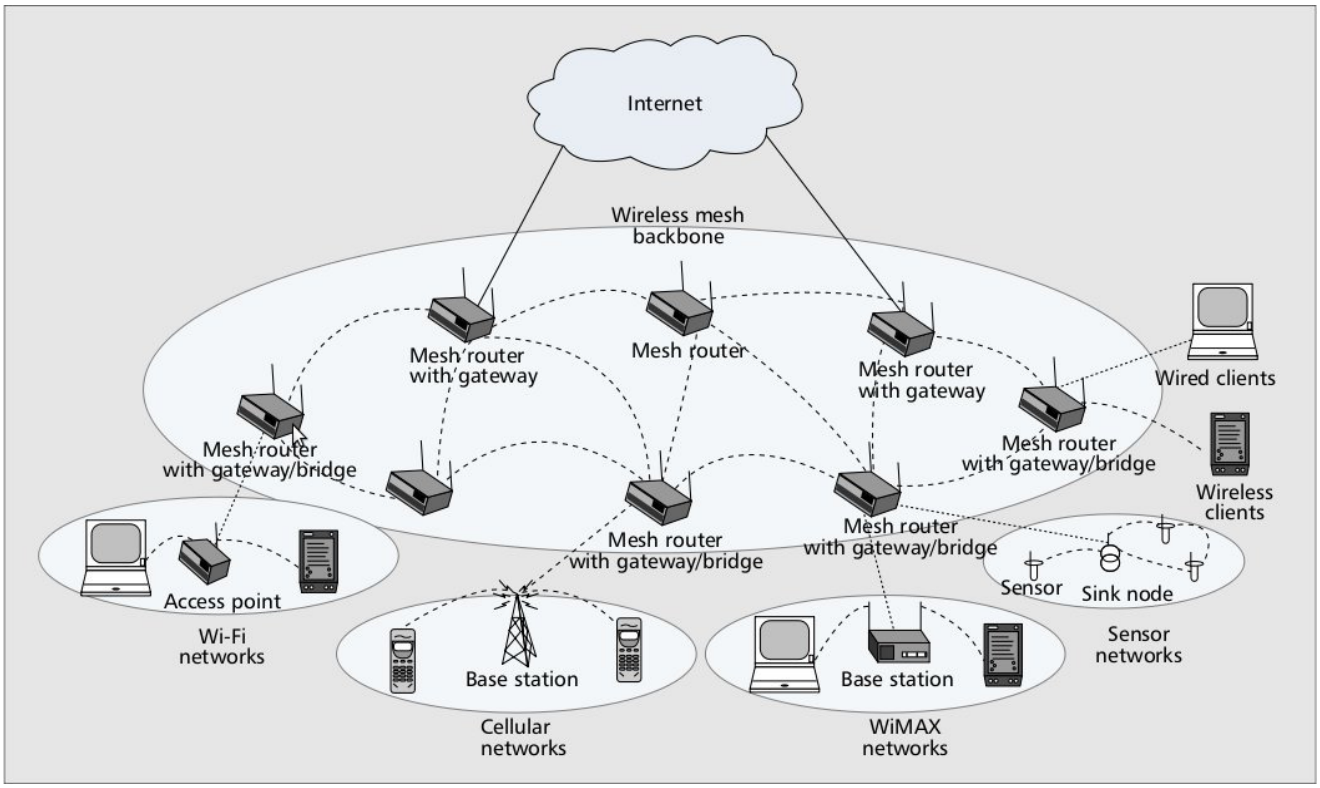

FIGURA 5 – ARQUITETURA DE *BACKBONE* (AKYILDIZ e WANG, 2005)

- *Clientes WMNs:* Operando em modo *ad-hoc*, os *Mesh Clients* utilizam a arquitetura *peer-to-peer* para comunicarem entre si. Dessa forma, não são necessários roteadores *mesh* já que os *Mesh Clients* são equipados com pelo menos um dispositivo de rádio. Tais clientes são responsáveis pelo roteamento e configuração da rede *mesh* exigindo, por isso, que seus equipamentos sejam mais robustos. A Figura 6 ilustra uma comunicação entre *Mesh Clients* operando em modo *ad-hoc* e os clientes os dependendo destes como provedores de serviço.

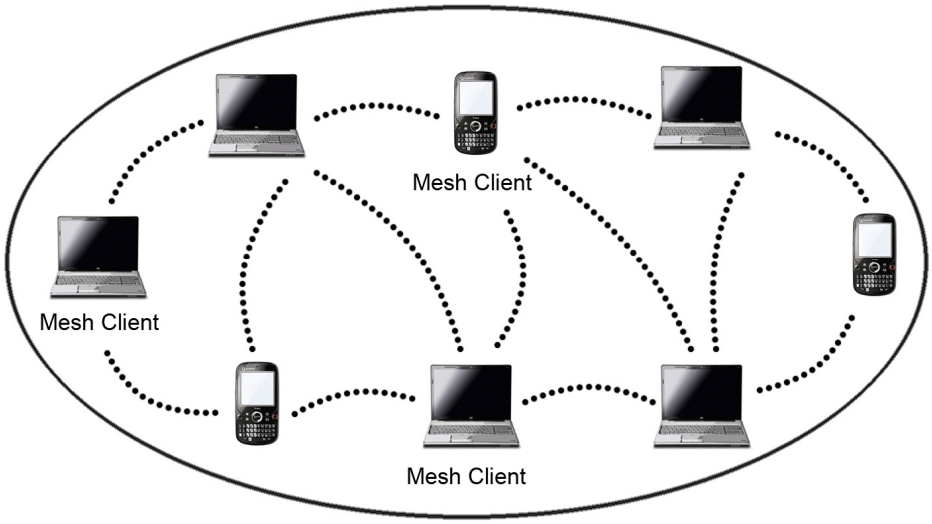

FIGURA 6 – ARQUITETURA DE CLIENTE (Fonte: AKYILDZ, X. WANG e W. KIYON, 2005)

- *WMNs híbridas:* Essa arquitetura combina características dos dois. Nela, os clientes podem acessar a rede através de roteadores *mesh*, permitindo conectividade a outras redes, e conectar-se diretamente a outros clientes, provendo maior conectividade e cobertura da WMN, como demonstrado na Figura 7.

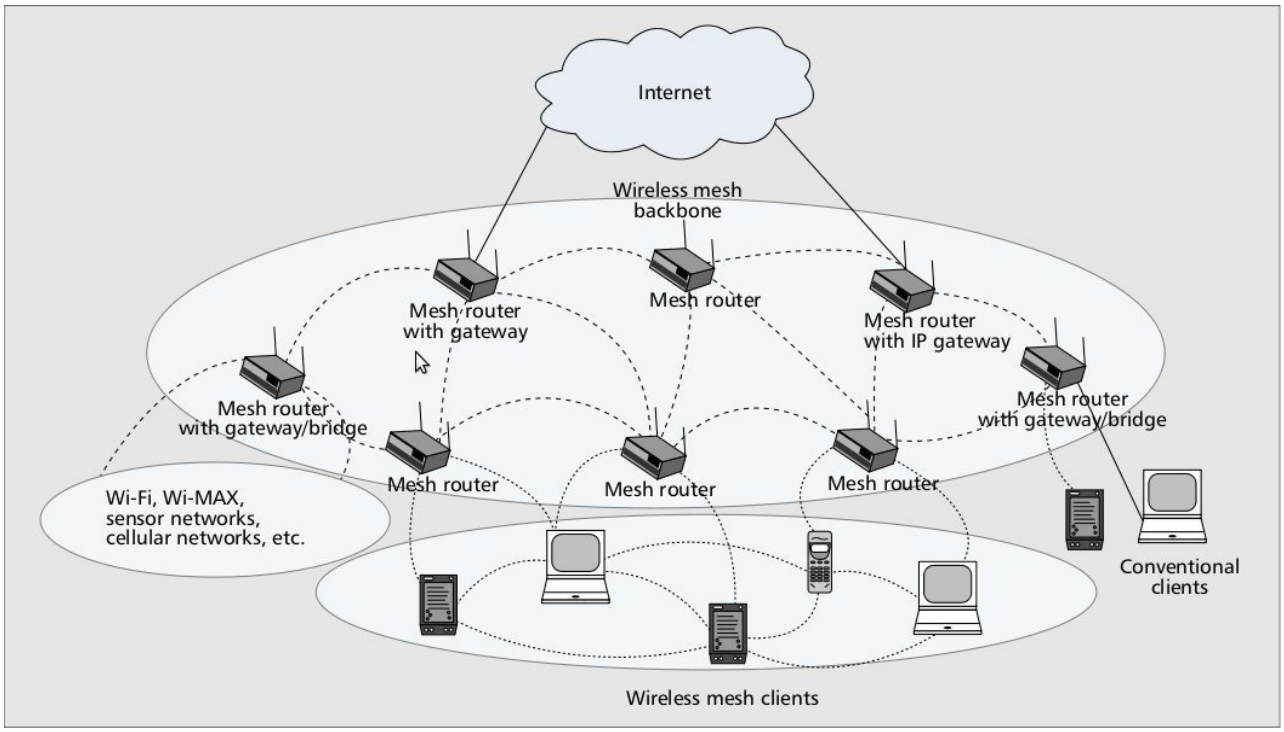

FIGURA. 7 – ARQUITETURA HÍBRIDA (AKYILDIZ e WANG, 2005)

2.5.2 Protocolos de Roteamento

As MANETs e as WMNs apresentam particularidades como visto nas seções anteriores. Contudo, as duas seguem alguns princípios básicos que justificam um estudo aprofundado de alguns protocolos de roteamento das MANETs. Bahr (2007) cita algumas semelhanças, que seguem:

- Em ambas as redes a comunicação entre os nós se dá por múltiplos saltos sem fio em um grafo de rede em malha.
- Os protocolos de roteamento das duas redes são auto-recuperáveis permitindo caminhos diversos pela rede sem fio, se adaptando à mobilidade dos nós.
- Os nós intermediários são retransmissores dos pacotes de uma origem até um destino.
- Provêem grande flexibilidade e aumentam a confiabilidade da rede mesmo em condições adversas.

O estudo dos protocolos de roteamento das redes *ad-hoc* é fundamental já que alguns deles serviram de subsídio para os protocolos das redes em malha, como por exemplo o HWMP (utilizado pelo padrão IEEE802.11s), que sofreu adaptações do SAODV e OLSR, e o MR-LQSR (*Multi-Radio Link-Quality Source Routing*), adaptado do DSR.

Os protocolos citados a seguir não abordam problemas de segurança como autenticidade, integridade e a segurança no processo de descoberta de rota. Contudo, eles são a base para as versões seguras.

2.5.2.1 OLSR (*OPTIMIZED LINK STATE ROUTING*)

Em Clausen, Hanse, Begrmann (2003) é definido o protocolo OLSR como sendo um aperfeiçoamento do algoritmo de estado de enlace para redes sem fio. Através dele é usada a técnica de *flooding* para todos os nós permitindo que as rotas para seus vizinhos sejam atualizadas. Apesar de eficiente, essa técnica ocasiona envio de mensagens HELLO duplicadas pela rede.

No protocolo OLSR existem três mecanismos utilizados para descoberta de uma rota ótima, a serem considerados (CLAUSEN, HANSE, BEGRMANN, 2003):

- *Reconhecimento de vizinhos:* A vizinhança de um determinado nó é descoberta através de mensagens do tipo HELLO que são periodicamente emitidas. Através dessas mensagens é possível ainda descobrir o estado da conexão com cada nó.
- *Mensagens flood:* Nessa técnica o problema de envio de mensagens duplicadas pela rede diminui com a adoção dos MPRs (*Multipont Relays*), que encaminham o tráfego de controle de seus vizinhos. O nó MPR é eleito por seus vizinhos, denominados seletores, e será o responsável por encaminhar as mensagens de estado de enlace pela rede, permitindo, pois, a redução do overhead ocasionado pelo tráfego de controle.
- *Informações da topologia:* Após os vizinhos serem reconhecidos e do flooding ser realizado, os nós MPR enviam mensagens de controle via broadcast (TC-*message*) que são responsáveis por obterem informações da topologia da rede. Nessas mensagens constam os endereços do MPR e de seus seletores.

2.5.2.2 DSR (*Dynamic Source Routing*)

O protocolo DSR (*Dynamic Source Routing*) enquadra-se na categoria de protocolos reativos, ou seja, aqueles que operam sob demanda. Em Johnson, Maltz e Broch (2001) o protocolo DSR é definido como auto-organizável e auto-configurável devido a duas propriedades:

- *Descoberta de rotas:* quando um nó deseja enviar pacotes para um destino e ainda não conhece uma rota para este, o mecanismo é utilizado para a descoberta de rotas. A origem envia um pacote RREQ (*Route Request*) por broadcast com a informação do endereço de destino. Caso o nó intermediário não tenha recebido o pacote anteriormente, adiciona seu endereço ao pacote e retransmite por broadcast, caso contrário irá

descartá-lo imediatamente. Ao receber o pacote, o destino retorna um pacote RREP (*Route Reply*) incluindo o endereço acumulado de rotas utilizadas para o RREQ.

- *Manutenção das rotas:* o mecanismo é utilizado durante o envio de pacotes do nó de origem para o destino caso a rota não possa mais ser utilizada, por exemplo, caso um nó tenha saído da vizinhança. Neste caso, outra rota conhecida pode ser usada para alcançar o destino ou, caso não se conheça, novamente é feita a descoberta de rotas.

Quando os nós estão praticamente imóveis ou quando as rotas já são conhecidas, o overhead de pacotes na rede causado pelo DSR é baixo. Caso os nós estejam se movendo rapidamente ou o tipo de conexão se altere durante o envio de pacotes, o overhead aumenta somente para a rota em uso.

Cada nó possui as rotas descobertas armazenadas em *cache* o que permite rápida recuperação no caso de mudança da topologia. Caso a rota não seja encontrada em *cache*, é utilizado o algoritmo de descoberta de rotas.

2.5.2.3 DSDV (*DESTINATION SEQUENCED DISTANCE VECTOR*)

Segundo He (2002), o protocolo DSDV é uma adaptação do RIP (*Routing Information Protocol*) para redes *ad-hoc* e adiciona o atributo *sequence number* em cada entrada da tabela RIP. É através desse parâmetro que os nós móveis distinguem as rotas antigas das novas.

Os objetivos que o protocolo tenta alcançar são o impedimento da criação de loops no algoritmo de vetor de distâncias utilizado pelo RIP e o rápido ajuste da topologia da rede enquanto os nós se movimentam (AGUIAR *et al,* 2008).

Em cada nó existe uma tabela de roteamento que constam todos os destinos possíveis, as métricas, o próximo salto (*hop*) e o número de sequência gerado pelo destino. Quando alguma mudança na topologia é identificada, os nós enviam pacotes de atualização de rota por *broadcast* e os vizinhos as retransmitem incrementando sua métrica. A tabela de roteamento de um nó somente é alterada após um período de espera em que o pacote com a melhor rota chegará do destino. Caso vários pacotes do mesmo destino cheguem nesse período, o que tiver o *sequence number* mais recente será

utilizado. Caso tenham o mesmo *sequence number*, o que tiver a menor métrica será considerado (HE, 2002)

.

2.5.2.4 AODV (*AD-HOC ON-DEMAND VECTOR*)

O algoritmo AODV enquadra-se na categoria de protocolos reativos. Segundo Tanembaum (2003), esse algoritmo busca o caminho mínimo entre um nó e o destino, leva em conta a largura de banda e o gasto de energia dos equipamentos. Cada nó armazena em sua tabela de roteamento apenas uma rota por destino, ou seja, um nó mantém informações sobre um destino somente se ele se comunica com esse nó ou se é um nó intermediário.

Ao desejar enviar uma mensagem a um nó, o nó de origem verifica se já possui uma rota para ele. Caso não possua, transmitirá por *broadcast* um pacote RREQ que possui campos para a origem e destino. Ao chegar a um nó intermediário este verifica na sua tabela se a solicitação já foi processada. Caso positivo, irá descartar o pacote ou, caso contrário, a atualizará para que não haja duplicatas. O nó, então procura uma rota para o destino na sua tabela e, caso possua, retorna um pacote RREP para a origem a informando. Novas rotas são atualizadas se o *Número de sequencia de destino* armazenado na tabela de roteamento do nó é maior ou igual ao *Número de sequencia de destino* contido no pacote (TANEMBAUM, 2003).

Caso o nó intermediário não conheça uma rota para o destino requerido, incrementa o contador de saltos, extrai as informações do pacote para adicionar à sua tabela de rotas inversas e retransmite por broadcast o RREQ. O processo se realiza até que chegue ao destino que então transmitirá o pacote pela rota inversa até que chegue a origem.

A Figura 8 demonstra o processo de descoberta de rotas no AODV.

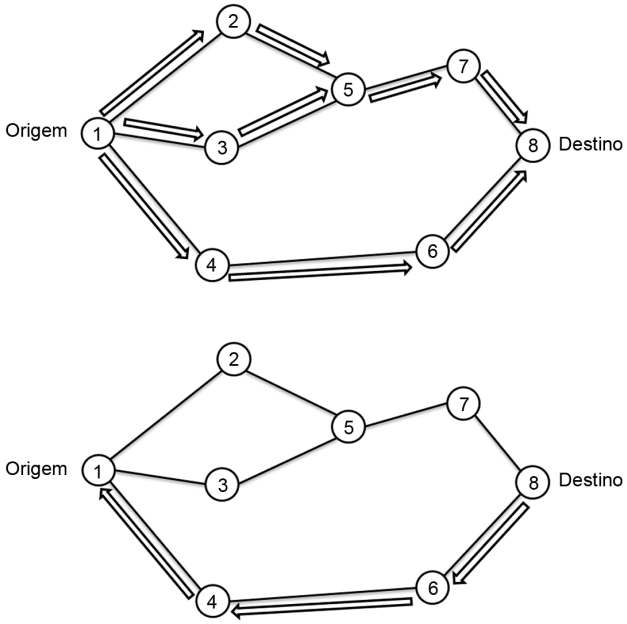

FIGURA 8 – DESCOBERTA DE ROTAS NO AODV (Fonte: JÚNIOR e DUARTE, 2003)

2.5.2.5 HWMP (*HYBRID WIRELESS MESH PROTOCOL*)

A expansão das redes em malha sem fio exigiu que um padrão fosse discutido a fim de que normas para o roteamento e a segurança, por exemplo, fossem estabelecidas. O protocolo de roteamento padrão definido pelo IEEE 802.11s é o HWMP que se enquadra na categoria de protocolos híbridos, baseado no AODV e SOLSR e incorpora o conceito de roteamento na camada de enlace.

A estrutura de uma rede *mesh* definida pelo IEEE 802.11s está ilustrada na Figura 9. Os roteadores *mesh*, que formam o *backbone* (nuvem mesh), são representados pelos MP (*Mesh Points*), MAP (*Mesh Access Points*) e os MPP (*Mesh Portals*). A diferença entre eles está na sua função. Os primeiros são responsáveis somente por participarem do processo de roteamento dentro do *backbone*, os MAP se caracterizam por proverem o acesso sem fio aos clientes *mesh* – STA (*Stations*) – e os MPP são os portais responsáveis pela integração do IEEE 802.11s com outros padrões IEEE 802.

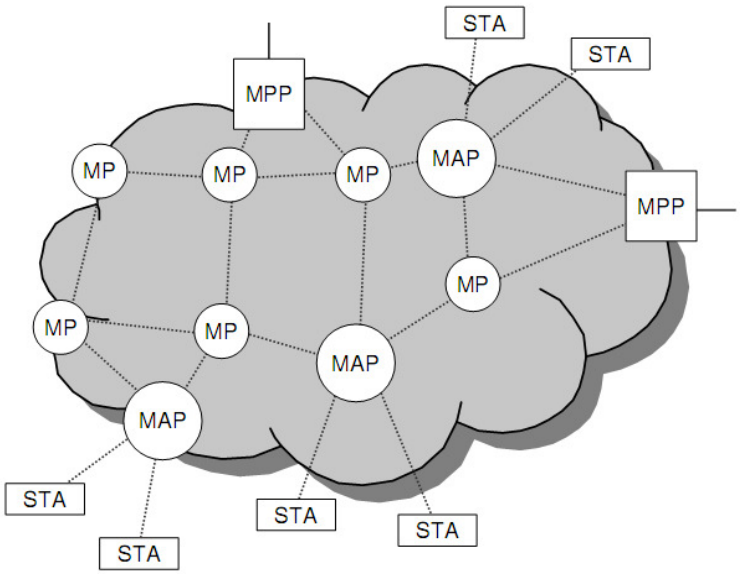

FIGURA 9 – ESTRUTURA DA REDE IEEE 802.11s (BAHR, 2007)

Quando operado em modo reativo, o protocolo assume uma postura semelhante ao AODV. O pacote PREQ (*Path Request Message*) seguirá, por difusão, pelo melhor ou o mais novo caminho até um destino, que irá retornar um pacote PREP (*Path Reply Message*) da mesma forma do PREQ. Quando é operado de forma pró-ativa, cada nó calcula antecipadamente uma topologia em árvore em que a raiz será um nó que se anuncia como tal. O modo pró-ativo pode ser realizado de duas formas: o nó raiz emitirá periodicamente mensagens PREQ ou emitirá mensagens do tipo RANN (*Root Announcement Messages*), que são as mensagens emitidas pelo nó que se anuncia como a raiz. Saade *et al* (2008, p. 27) reforça a vantagem da característica híbrida do protocolo afirmando que "(...) em certas circunstâncias, apesar de disponível de antemão, o caminho entre dois nós em uma topologia em árvore pode não ser o caminho ótimo e, neste momento, a descoberta sob demanda pode ser empregada, fornecendo um caminho alternativo mais apropriado."

Os MPP e MAP são os responsáveis por retransmitir os pacotes para fora da rede mesh, não tendo conhecimento, portanto, dos MP de um destino fora da rede. Essa relação se estende para os clientes fora da nuvem mesh, que não tem conhecimento dos MP. Para isso, os MPP e os MAP devem traduzir os pacotes de rotas que saem ou que entram da nuvem mesh. Os campos *Proxied Source MAC Address* e *Proxied Source MAC Address* são responsáveis por caracterizarem se os pacotes estão sendo usados na descoberta de rotas dentro e fora da nuvem. Estes somente são utilizados se a *flag* AE

(Address Extension) for utilizada (BAHR, 2007). Os pacotes PREQ e PREP estão descritos na Figura 10 e Figura 11, respectivamente.

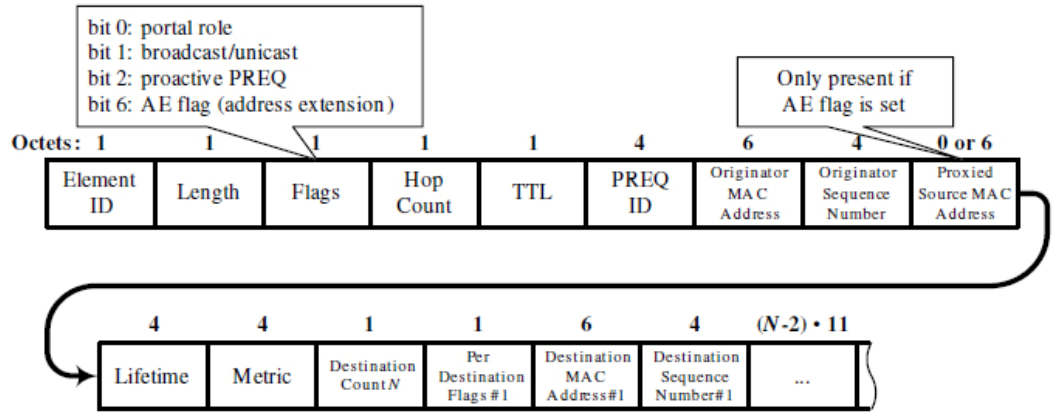

FIGURA 10 – ESTRUTURA DO PREQ (BAHR 2007)

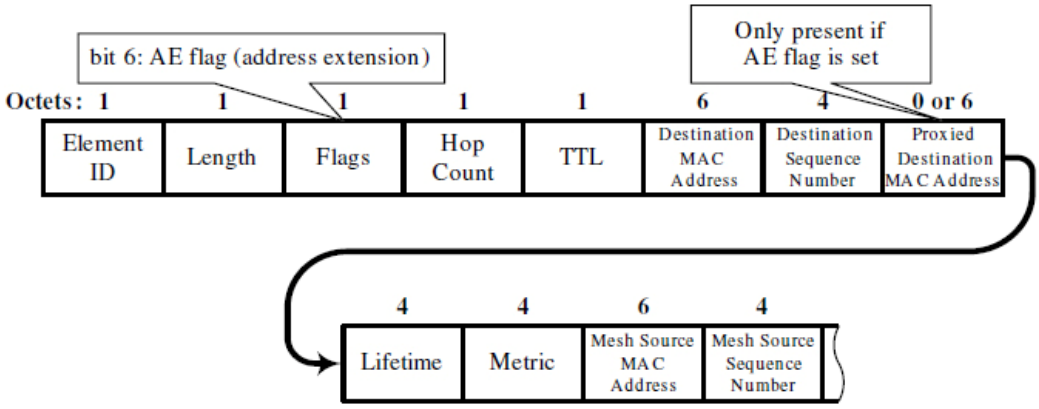

FIGURA 11 – ESTRUTURA DO PREP (BAHR (2007)

A descoberta de rotas sob demanda se inicia após a origem gerar um pacote PREQ contendo o endereço MAC do destino e o encaminha por broadcast. Ao receber o pacote, o nó intermediário verifica se conhece um caminho para o destino. Caso positivo, retorna uma mensagem PREP para a origem. Caso contrário, retransmitirá o pacote por broadcast. O processo irá se repetir até que se chegue ao nó destino. A cada manipulação do PREQ os nós aprendem a rota inversa, que será utilizada no encaminhamento dos PREP para o nó de origem.

No cabeçalho PREQ existem duas *flags* que definem a quantidade de pacotes recebidos pela origem, que são o DO (*Destination Only)* e o RF (*Reply and Forward).* A primeira *flag* é utilizada pelo nó de origem caso não queira que os nós intermediários

respondam o PREQ, sendo possível somente o nó de destino responder ao pacote. A segunda, RF, caso seja utilizada sem o DO, o nó intermediário poderá responder a requisição e deverá retransmitir o pacote. Caso não seja utilizada juntamente com este, poderá responder à requisição e não deverá retransmitir o pacote.

Caso a descoberta de rotas seja pelo modo pró-ativo, dois métodos podem ser adotados: utilizando mensagens RANN ou PREQ.

No método baseado em PREQs, o MP raiz deve ser previamente configurado para operar dessa forma e irá gerar periodicamente mensagens PREQ com as *flags* DO e RF ativadas, caracterizando um pacote PREQ pró-ativo. Os nós que receberem o pacote atualizam seu cabeçalho com os valores de *Hop Count* (contagem de saltos) e *Metric* (métrica – utilizando o *Airtime Link Metric*) e o retransmitem até que todos os nós da rede sejam notificados.

Já no método que utiliza mensagens RANN para atualização de rotas, o nó raiz inunda a rede com pacotes RANN. Os nós intermediários que desejarem ter o nó raiz como tal, devem responder, por *unicast*, a este com um pacote PREQ. O nó raiz, portanto, retornará aos nós intermediários um PREP, em que será estabelecida uma rota do nó raiz para o nó intermediário. Saade *et al* (2008) reforça a utilização dos pacotes RANN afirmando que o "(...) [mecanismo] introduz um passo adicional e pode ser vantajoso se comparado com o mecanismo PREQ apenas se uma pequena porção dos MPs deseja estabelecer caminhos com o nó raiz."

2.6 CONCLUSÃO

Neste capítulo foi estudada a arquitetura das redes sem fio, podendo ser operadas em modo infra-estruturado ou não, caracterizando, portanto as redes *ad-hoc*. Nas redes sem infra-estrutura é necessário que os nós colaborem entre si para garantir os serviços da rede. Foi estudado o IEEE 802.11s, que, apesar de ainda ser um *draft*, tem grandes possibilidades de ser adotado como padrão para redes em malha sem fio. Foram analisadas também as redes *mesh* que, por terem características dinâmicas de crescimento da topologia, são suscetíveis a variados tipos de ataques, abordados no Capítulo 3.

Alguns protocolos utilizados em redes mesh foram analisados, como o AODV, DSR, DSDV, OLSR – que são também utilizados em redes *ad hoc* – e o protocolo padrão definido pelo IEEE802.11s, HWMP.

3 SEGURANÇA

As WMNs são redes de baixo custo, que crescem muito rapidamente e de forma dinâmica. Por utilizarem transmissão broadcast e dependerem de um nó intermediário, os clientes *mesh* estão sujeitos a várias vulnerabilidades. Alguns tipos de ataques nessas redes assemelham-se ao de WLANs por utilizarem o padrão 802.11. Caso o atacante não seja de origem externa à rede será, portanto, de origem interna. Nesse caso o atacante pode ter conhecimento das chaves e das informações de autenticação, o que dificulta a prevenção de ataques.

As camadas de aplicação e de transporte não são abordadas no presente trabalho, posto que as soluções de contramedidas em segurança são implementadas nos *hosts*. Dessa forma, o enfoque será dado nas camadas Física, Enlace e de Rede já que estas formam o núcleo da rede.

3.1 ATRIBUTOS PARA A SEGURANÇA

O bom funcionamento de redes, cabeadas ou sem fio, dependem de algumas técnicas empregadas nas informações trafegadas no meio. Essa necessidade deverá garantir que a informação seja exatamente igual àquela que foi enviada e que o emissor e o destinatário sejam legítimos. Alguns atributos devem ser observados para que uma comunicação segura possa ser estabelecida:

- Confidencialidade: Apropriando a interpretação de Kurose e Ross (2005, p. 513): “Somente o remetente e o destinatário devem poder entender o conteúdo da mensagem transmitida”. O conceito de confidencialidade se aplica na garantia de que a mensagem enviada pelo emissor somente pode ser compreendida pelo remetente. Para não comprometer a mensagem ela deve ser codificada para que um nó malicioso não a intercepte e de uma forma que só o nó que recebê-la possa decodificar.
- Integridade: Ocasionalmente a mensagem pode sofrer alguma interferência, seja pelo meio, seja através de um ataque, em que dados podem ser injetados ou removidos da mensagem. A integridade é a propriedade que garante que os dados recebidos pelo destino são

exatamente iguais aos dados enviados pela origem (KUROSE e ROSS, 2005).

- Autenticação: É a propriedade que garante a identidade de ambas as partes da comunicação (KUROSE e ROSS, 2005). Em um meio, como em redes sem fio, a facilidade da intrusão é grande e pode colocar em risco a autenticidade dos clientes. Segundo a definição de Nakamura e Geus (2007, p. 363), "A autenticação pode ser realizada com base em alguma coisa que o usuário sabe, em algo que o usuário possui ou determinada característica do usuário." A abordagem de alguns protocolos de roteamento seguro utiliza de chaves secretas digitais para realizar a validação mútua. Nas WMNs a confiança na autenticidade entre nós vizinhos é de extrema importância visto que variados ataques podem ocorrer com a intrusão de um nó malicioso na rede ou com a personificação de um nó legítimo.
- Não-repúdio: Entende-se por não-repúdio ou não-repudiação "A propriedade segundo a qual nenhuma parte de um contrato pode negar mais tarde tê-lo assinado (...)" (TANEMBAUM 2003, p. 804). Dessa forma é impedido que uma entidade de uma comunicação possa negar sua participação na operação.
- Disponibilidade: A propriedade está relacionada à existência do serviço quando for requisitada pelos clientes (ANJUM e MOUCHTARIS, 2007). Independentemente do momento que um cliente fizer a requisição, o serviço deverá estar à disposição para ser utilizado. Certos tipos de ataques, como os de DoS (*Denial of Service*) dificultam a manutenção deste atributo.

3.2 TIPOS DE ATAQUES

A localização dos roteadores *mesh* geralmente é exposta, como em topos de edifícios, para que seu sinal possa cobrir uma grande área. Apesar de sua movimentação ser limitada, o acesso ao meio de transmissão expõe os roteadores *mesh* a algumas falhas de segurança visto que seus serviços não apresentam a proteção encontrada por uma rede cabeada. Dessa forma, um atacante poderá facilmente conseguir acesso a eles

e as informações da rede são analisadas por ele. Os ataques podem sem agrupados em duas categorias principais, ativos ou passivos. Um ataque é considerado passivo se o atacante não interfere no funcionamento da rede, ou seja, não altera ou destrói as informações retidas. Caso contrário, é considerado um ataque ativo. Segundo Winget, Rahman (2008) os ataques em redes *mesh* podem ser classificados da seguinte forma:

- *Eavesdropping*(escuta): Nesse tipo de ataque os clientes não conseguem perceber que estão sendo interceptados. Caracterizado como um ataque passivo, o *eavesdropping* tem como objetivo obter informações as quais o atacante não possui permissão legal de acesso.
- *Forgery* (falsificação): É um tipo de ataque ativo que tem como objetivo redirecionar ou alterar alguma informação dos frames sem que o atacante seja percebido.
- *Masquerading:* O atacante responde às requisições de clientes da rede como sendo uma estação válida. Dessa forma o atacante poderá enviar e/ou receber pacotes usando a identidade de outro cliente da rede.
- *Man-in-the-Middle:* Considerado um ataque ativo, o MIM (*Man-in-the-Middle*) pode ter características dos três ataques acima. Por exemplo: o atacante poderá se colocar no maio de dois nós passando-se por x para y e por y para x.
- Negação de Serviços (DoS): Também caracterizado como um ataque ativo, a negação de serviços tem por objetivo inundar o(s) cliente(s) com tráfego até que este(s) trave(m) ou reinicie(m), forçando a reestruturação da rede. Em redes *mesh* a prevenção desse tipo de ataque torna-se praticamente impossível, devido à dinamicidade dos nós.

3.2.1 Camada Física

Em Wu *et al* (2006) são relacionados dois tipos de ataques aos quais a camada física está sujeita: *eavesdropping* e *jamming*.

No primeiro, por serem utilizadas comunicações em rádio frequência, os ataques tornam-se de fácil realização. Um *host* malicioso poderá facilmente se colocar dentro da área de cobertura da rede sem fio e interceptar uma comunicação. Dessa

forma, o atacante poderá visualizar informações sigilosas e propagar mensagens falsas na rede.

No segundo tipo de ataque, por *jamming*, o atacante emitirá sinais rádio frequência a fim de sobrecarregar o tráfego *wireless* e interromper a comunicação do(s) *host*(s). Esse tipo de ataque pode ser realizado de forma constante, em que o dispositivo emite o sinal jammer de forma contínua, ou de forma reativa, acontecendo a interferência somente quando o dispositivo perceber a utilização do canal sem fio (XU *et al*, 2005)

3.2.2 Camada de Enlace

Para compreender melhor os tipos de ataques na camada de enlace, se faz mister conhecer a definição desta trazida por Tanembaum (2003, p. 196):

> A função da camada de enlace de dados é fornecer serviços à camada de rede. O principal serviço é transferir dados da camada de rede da máquina de origem para a camada de rede da máquina de destino (...) A tarefa da camada de enlace de dados é transmitir os bits à máquina de destino, de forma que eles possam ser entregues à camada de rede dessa máquina (...)

Sendo assim, os dados recebidos pelo nó de destino devem estar em conformidade com os dados fornecidos pelo nó de origem. Os atacantes, ao desobedecerem às regras de acesso ao canal, visam enfraquecer a cooperação e a confiança entre os nós.

Alguns ataques a que a camada de enlace está sujeita são analisados, visto que é de fundamental importância para que se possam diminuir as chances de ruptura do enlace.

3.2.2.1 *Eavesdropping* passivo

Nesse tipo de ataque, um intruso se insere na rede e coleta informações sobre suas propriedades ou de informações de clientes legalmente associados. Em redes sem fio, esse tipo de ataque torna-se fácil de acontecer na medida em que o *host* malicioso não necessita conectar-se fisicamente a rede e efetivar o ataque. As WMNs estão mais propícias a este tipo de escuta devido a sua dinamicidade e facilidade de crescimento.

A fim de se coibir esse tipo de ataque, alguns métodos que garantam a confidencialidade dos dados utilizando técnicas de criptografia podem ser utilizados.

3.2.2.2 *Jamming*

O *jamming* da camada de enlace tem o mesmo objetivo que o da camada física: a negação de serviço. Como destacam Naveed, Kanhere e Jah (2008), o ataque não só consiste na transmissão constante de bits aleatórios, como também de cabeçalhos de frame MAC focado nos protocolos da camada de rede, como AODV, OLSR e DSDV. Dessa forma, a vítima acreditará que o canal está ocupado e ficará off-line da rede por um momento até buscar acesso novamente. O ataque pode ainda ser utilizado para explorar a rede em busca de informações da sua topologia e influenciar o desempenho dos protocolos da camada de transporte. O *jamming* é efetivo mesmo com a utilização de criptografia WEP (*Wired Equivalent Privacy*) e WAP já que o sensor *jammer* monitora o tamanho, tempo de resposta e sequência do pacote, que servem para análise para o atacante.

3.2.2.3 MAC *spoofing*

"Uma propriedade interessante dos endereços MAC é que não existem dois adaptadores com o mesmo endereço" (KUROSE e ROSS, 2005). Ao contrário do que afirmam Kurose e Ross, o endereço MAC de uma interface de rede pode ser forjado podendo ser utilizado para vários tipos de ataques, definindo, portanto, o MAC *Spoofing* (NAKAMURA e GEUS, 2007). A falsificação do endereço MAC de destino dos frames transmitidos é facilmente realizada devido à utilização de técnicas que alteram as informações de fabrica dos dispositivos de rede podendo, dessa forma, forjar um dispositivo autorizado. Naveed, Kanhere e Jah (2008) esclarecem que o MAC *Spoofing* pode limitar os recursos de banda de um nó, ocasionando DoS, e sobrecarregar o processamento do dispositivo móvel, ocasionando, consequentemente, a limitação de recursos energéticos da vítima.

A utilização de algoritmos que garantam a integridade dos dados e dos cabeçalhos, realizando verificações nos pacotes transmitidos, inibe o ataque de MAC *spoofing*.

3.2.2.4 *Replay attack*

O ataque apresentado por Naveed, Kanhere e Jah (2008) é considerado do tipo *man-in-the-middle* em que o nó malicioso pode estar externa ou internamente à rede. Na primeira situação, o atacante escuta a comunicação entre dois nós legítimos da rede (nós A e B, Figura 12) e, ao coletar informações, poderá ganhar acesso aos recursos desta. Neste caso, o nó B é levado a acreditar que o próprio atacante é um nó legítimo (nó A, Figura 12). Caso seja um nó interno da rede, o ataque será similar ao anterior, com a diferença que o nó malicioso é um *hop* intermediário dentro da rede e ganhará acesso a um recurso não permitido a ele.

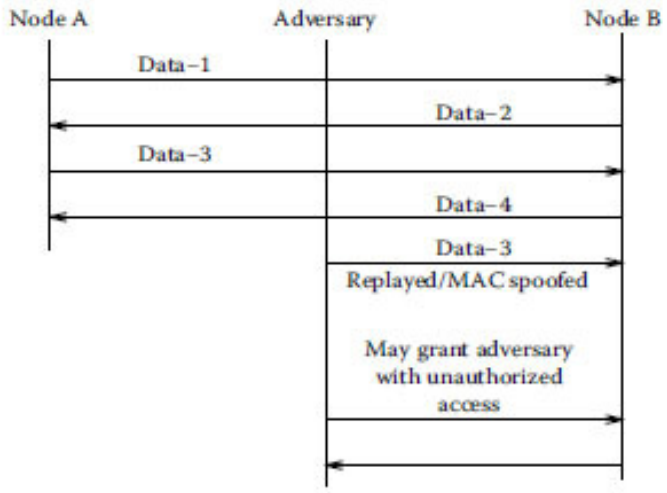

FIGURA 12 – REPRESENTAÇÃO DO *REPLAY ATTACK* (NAVEED, KANHERE E JAH, 2008)

3.2.2.5 Pré-Computação e combinação parcial

Nos ataques acima descritos foram abordadas vulnerabilidades de segurança na camada MAC. Contudo, outros tipos de ataques devem ser abordados como os que envolvem os mecanismos que garantem segurança a camada MAC. Neste contexto, Naveed, Kanhere e Jah (2008) descrevem a pré-computação como a computação prévia de um grande número de informações, como textos e chaves, a fim de agilizar o processo de decriptação.

Já combinação parcial está relacionada com o método de descoberta de palavras chave por força bruta e explora a complexidade de algoritmos de encriptação. No método em questão o atacante tem conhecimento parcial da palavra chave, o que facilita o processo de descoberta. Como exemplo do *partial matching,* Naveed, Kanhere e Jah (2008) citam o protocolo 802.11i, em que parte do cabeçalho da camada MAC é transmitido em texto plano e parte é criptografada. Qualquer conhecimento de parte das palavras irá expor o endereçamento MAC.

Contramedidas que garantam integridade e autenticidade através da criação periódicas de novas chaves inibem os ataques de pré-computação, combinação parcial e de escuta.

3.2.3 Camada de Rede

Bem como a camada de enlace, a camada de rede está sujeita a sérios ataques que influenciam o desempenho, disponibilidade, confiabilidade e segurança das redes *mesh*.

Ao se comprometer a camada o atacante poderá, segundo Wu *et al* (2006), desviar e controlar o tráfego a fim reter a banda, inserir-se no caminho entre dois pontos, re-encaminhar os pacotes para um nó com baixo desempenho ou inexistente, criar loops, congestionar e particionar a rede. A Figura 13.b demonstra o nó M entre os nós X e Y após corromper as tabelas de roteamento destes (Figura 13.a) e todo o tráfego entre eles será analisado por M, que está numa posição privilegiada.

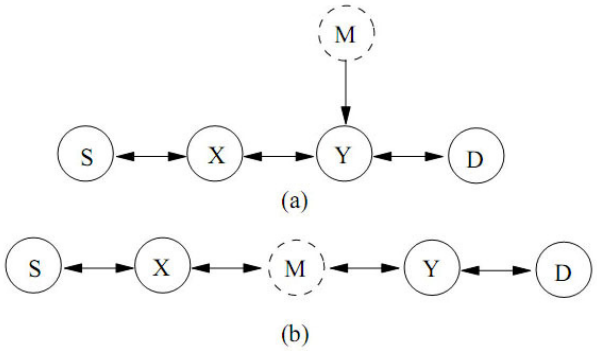

FIGURA 13 – INSERÇÃO DO ATACANTE NA REDE (WU et al, 2006)

Os ataques nessa camada têm o objetivo de causar a indisponibilidade das rotas, escuta da conexão ou afetar o encaminhamento dos pacotes. Abaixo, são descritos alguns possíveis tipos de ataques nessa camada.

3.2.3.1 *Wormhole*

Em Hu *et al* (2003) é realizada a definição do ataque que consiste no captura de pacotes por um nó malicioso em um local da rede e encaminhados para outro local em que são, posteriormente, retransmitidos. O ataque é feito em cooperação entre dois ou mais atacantes que utilizam um túnel através do meio, cabeado ou sem fio, utilizando protocolos reativos. Naveed, Kanhere e Jah (2008) destacam que durante a fase de descoberta de rotas as mensagens do tipo ROUTE REQUEST são redirecionadas entre os nós maliciosos através do túnel tornando-os, dessa forma, parte da rede. A Figura 14 demonstra a situação em que o túnel foi formado e os nós M1 e M2 se incluíram no caminho entre o emissor S e o destino D. Os objetivos do ataque são vários, visto que os nós se colocam em posições privilegiadas dentro da rede podendo, inclusive, romper a comunicação entre os nós legítimos.

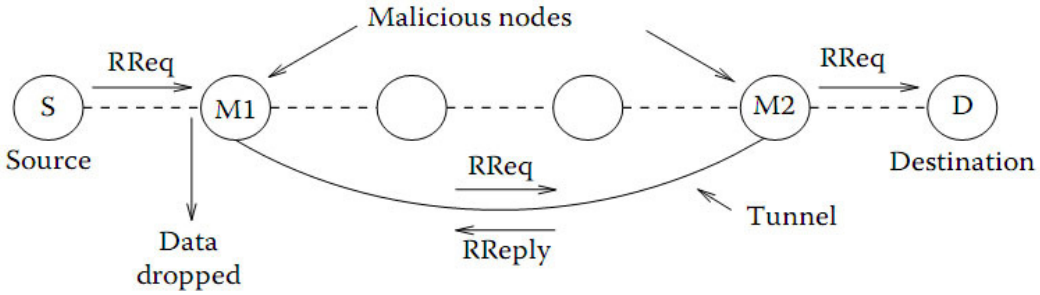

FIGURA 14 – TÚNEL CARACTERÍSTICO DO ATAQUE *WORMHOLE* (NAVEED, KANHERE E JAH, 2008)

3.2.3.2 *Rushing*

O ataque é realizado em cooperação de dois atacantes para se formar um túnel para o *wormhole* (WU *et al* 2006). O ataque é caracterizado pelo canal entre os dois nós propagar os pacotes mais rápido que o utilizado pelos nós legítimos. Ao desviar o

caminho entre a fonte e o destino os atacantes podem descartar os pacotes e comprometer, consequentemente, as tabelas de rotas dos nós legítimos.

3.2.3.3 *Overflow* da tabela de rotas

O ataque descrito em Wu *et al* (2006) ocorre durante a fase de descoberta de rotas e é caracterizado pela inundação (*flooding*) de rotas inexistes na tabela de roteamento da vítima evitando, portanto, que novas rotas sejam estabelecidas. O ataque se mostra bastante efetivo na medida em que atualização das rotas em redes *mesh* sem fio é constante.

3.2.3.4 *Black hole*

Em Al-Shurman, Yoo, Park (2004) é definido o ataque em que o nó malicioso utiliza o protocolo sob demanda da rede para anunciar-se como sendo o menor caminho para um determinado destino. Caso a resposta da requisição realizada pelo nó legítimo não chegue antes da enviada pelo atacante, o ataque se efetivará.

Na Figura 15, o nó M está realizando o ataque *black hole* em sua vizinhança. Seus vizinhos direcionam pacotes a ele acreditando que seja o menor caminho. O nó malicioso poderá, então, descartar os pacotes ou iniciar o ataque *man-in-the-middle*.

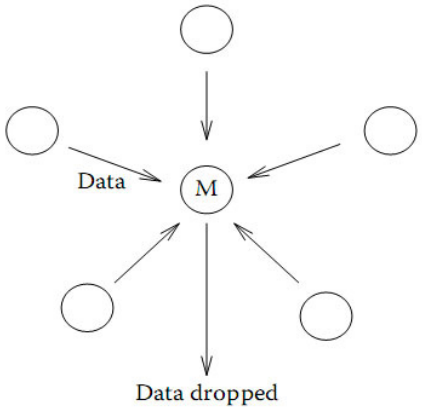

FIGURA 15 – *BLACKHOLE* (NAVEED, KANHERE E JAH, 2008)

3.2.3.5 *Grey hole*

O ataque é semelhante ao *black hole* com a diferença que nem todos os pacotes são descartados pelo atacante. Essa característica seletiva o torna efetivo e bastante difícil de ser identificado já que o atacante procura esconder o ataque no fato de que alguns serviços da rede podem estar instáveis, não caracterizando, assim, o ataque.

3.2.3.6 *Sybil*

O ataque tem por objetivo criar identidades falsas de nós legítimos utilizando somente um dispositivo de rede (NAVEED, KANHERE, JAH, 2008). O atacante poderá forjar outra uma identidade falsa ou utilizar uma identidade de outro nó. Os nós autorizados da rede ao adicionarem às suas rotas as identidades falsas submetem a comunicação a vulnerabilidades como diminuição do desempenho da rede.

3.3 CONCLUSÃO

O estudo das propriedades desejáveis para se garantir a segurança, como o não-repúdio, integridade e autenticidade são essenciais para a implementação de ambientes seguros em redes.

A facilidade do acesso ao meio nas redes em malha sem fio expõe os nós a vários tipos de ataques nas diversas camadas de rede. Neste capítulo foram abordados alguns ataques realizados nas WMNs e algumas contramedidas.

A cooperação entre os nós é uma característica importante e que deve ser mantida a fim de que o roteamento não seja influenciado por um nó malicioso, que poderá desde interceptar informações até esgotar os recursos do nó.

4 PROTOCOLOS DE ROTEAMENTO SEGURO

Como visto no Capítulo 3, as redes *mesh* sem fio apresentam várias vulnerabilidades decorrentes das camadas física, de enlace e de rede. Para não comprometer o roteamento dessas redes os protocolos devem ser robustos e garantir alguns dos atributos de segurança. A natureza dinâmica das WMNs exige que os protocolos de roteamento garantam a colaboração entre os nós já que estes são retransmissores de pacotes. A facilidade de inserção de clientes nas redes em malha sem fio exige que medidas que garantam a segurança sejam tomadas a fim de prevenir ou detectar a presença de intrusos.

Os métodos de segurança na camada de rede buscam garantir a integridade da transmissão da informação e dos dados trafegados. Para isso, segundo Wu *et al* (2006), são utilizas algumas primitivas de criptografia, como funções *hash* e assinaturas digitais. A autenticidade, seja fim a fim, seja a cada salto, é outra premissa garantida pelos protocolos seguros da camada que, por exemplo, evitam que um nó malicioso não modifique ilegalmente as mensagens de rotas trocadas pelos nós legítimos. Sendo assim, o foco do estudo do capítulo será dado a segurança nessa camada.

4.1 SOLSR (*SECURE OPTIMIZED LINK STATE ROUTING*)

O protocolo SOLSR descrito por Hafslund *et al* (2004) é uma extensão do OLSR e por isso enquadra-se na categoria de protocolos pró-ativos. A cada salto, a implementação segura do OLSR assina o pacote de controle com chaves simétricas e o nó seguinte realiza a autenticação. Um atacante, portanto, não obterá êxito ao tentar realizar um ataque do tipo *spoofing*. O objetivo é prover a integridade dos pacotes por um percurso confiável e a segurança do roteamento das mensagens, ao invés de confidencialidade. Entretanto, o protocolo não garante as assinaturas do emissor e do destinatário, ponto a ponto, já que a verificação é realizada em 1-*hop* e cada nó autenticará o pacote utilizando as chaves sendo que sua assinatura será criada através de uma função *hash*. Caso o nó não possua a chave secreta não poderá reproduzir a assinatura do emissor ocasionando, dessa forma, o descarte dos seus pacotes pelos clientes que utilizam o SOLSR. A Figura 16 demonstra o esquema de uma mensagem assinada trocada entre os nós. Segundo Hafslund et al(2004), os campos *Scheme* e

Algoritms definem como o *hash* para a assinatura será gerada (campo *Signature*, na Figura 10).

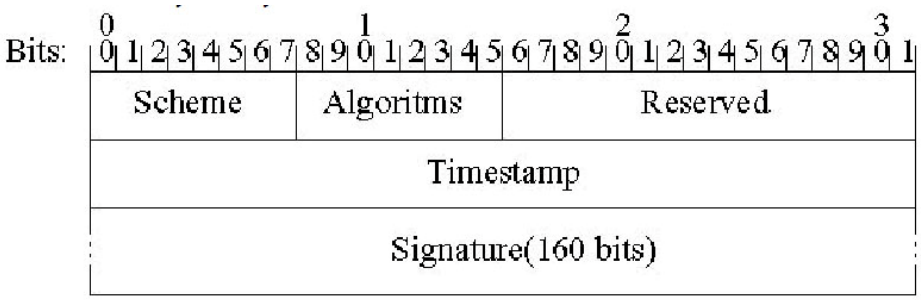

FIGURA 16 – ESTRUTURA DA MENSAGEM DE ASSINATURA NO SOLSR (HAFSLUND et al, 2005)

A transmissão utilizando os próprios pacotes OLSR aumenta a compatibilidade entre os nós que não estão utilizando SOLSR. O cabeçalho contém, ainda, um campo para o *timestamp* que é a técnica que adiciona o instante em que o pacote foi enviado para que o destino faça sua verificação. Somente são aceitos os pacotes se o *timestamp* do pacote imediatamente posterior for maior que o seu sucessor. Essa técnica é útil já que mensagens desatualizadas trafegadas pela rede podem não refletir com exatidão o verdadeiro estado dos nós ou do *link*. O *timestamp* garante que a rota seja a mais atual e previne ataques de replicação já que os pacotes que falharem na verificação são descartados. Contudo, a técnica não previne ataques de DoS pois um nó malicioso poderá sobrecarregar a rede com trocas de *timestamp* levando o(s) nó(s) a deixar(em) de verificar as mensagens verdadeiras desse tipo, caracterizando o ataque.

4.2 SAODV (*SECURE ADHOC ON-DEMAND VECTOR)*

O protocolo SAODV (Secure Adhoc On-Demand Vector), em Zapata e Asokan (2002), é uma extensão do AODV, sendo por isso reativo, e garante a segurança do processo de descoberta de rotas provendo integridade, autenticidade e o não-repúdio.

É necessário que as chaves públicas dos nós sejam previamente divulgadas por uma unidade autenticadora para que, a cada transmissão dos pacotes RREQ e RREP possa ser analisado a autenticidade dos dados. O protocolo utiliza cadeias *hash* para autenticar o contador de saltos do AODV e assinaturas digitais para prover a

autenticação dos dados não mutáveis do cabeçalho, que são todos os campos do AODV menos o contador de saltos e todos os campos do SAODV menos o campo *Hash*. Dessa forma, pode-se garantir também a integridade e o não-repúdio dos pacotes. A Figura 17 ilustra o formato do cabeçalho das mensagens utilizadas pelo SAODV.

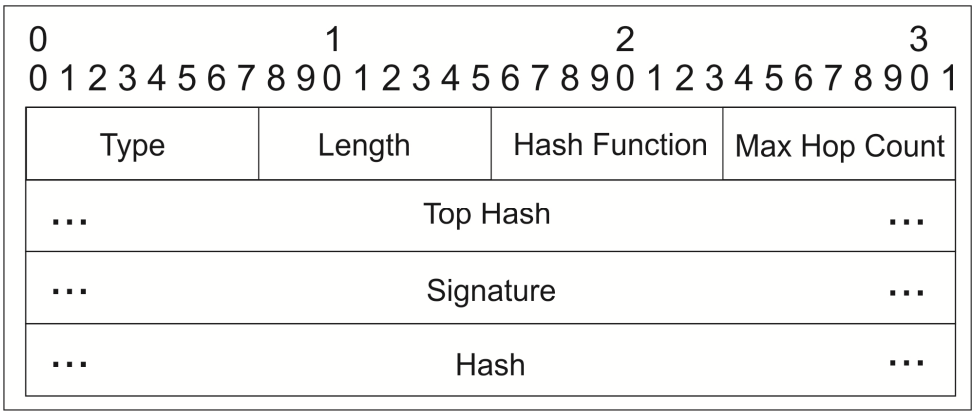

FIGURA 17 – CABEÇALHO SAODV (Fonte: ZAPATA e ASOKAN, 2002)

Quando um pacote RREQ ou RREP é gerado, pela origem ou destino respectivamente, o campo *hash* da mensagem é iniciado com uma variável aleatória (*seed*) e o campo número máximo de saltos (*Max Hop Count*) com o valor igual o TTL (*Time To Live*) do cabeçalho IP (*Internet Protocol*). O campo *Top Hash* receberá o resultado da aplicação da função *hash* sobre o *seed* um número de vezes igual ao Max *Hop Count*. Ao receber o RREQ ou o RREP, o processo de autenticação do número de saltos se dará na aplicação função *hash* um número de vezes igual à diferença entre Max *Hop Count* e o número de saltos do AODV. Em seguida o campo será comparado com o *Top Hash* e, caso os valores divirjam o pacote será descartado, caso contrário, o nó aplica a função *hash* ao campo *Hash* e retransmite por broadcast.

Sendo assim, não irá obter êxito o nó malicioso que tentar alterar o valor do campo utilizando uma cadeia *hash* diferente.

4.3 SRP (*SECURE ROUTING PROTOCOL*)

O protocolo SRP (*Secure Routing Protocol*), descrito por Papadimitratos e Haas (2002), foi desenvolvido para ser uma extensão aos protocolos comumente utilizados, em especial o DSR e o ZRP. Sua aplicação é importante, pois garante a

consistência das rotas mesmo com a presença de nós maliciosos na rede, através de uma relação de confiança entre o emissor e o destinatário. A comunicação bi-direcional necessita que exista uma AS (Associação de Segurança) entre os dois nós, como por exemplo, uma chave secreta comum, a fim de que o tráfego seja controlado em ambas as direções.

A Figura 18 ilustra o cabeçalho do SRP, que é anexado junto ao de outro protocolo. O campo TYPE define o tipo de mensagem a ser gerada, RREP ou RREQ por exemplo. O QUERY IDENTIFIER é um número gerado aleatoriamente e o QUERY SEQUENCE NUMBER é um número que cresce monotonicamente e que é mantido, em dispositivo de armazenamento, para cada rota segura existente a outro nó. Por fim, o CAM (Código de Autenticação de Mensagem) é uma função *hash* gerada utilizando o endereço do emissor, do destino, o QUERY IDENTIFIER e a chave secreta que o nós em questão utilizam.

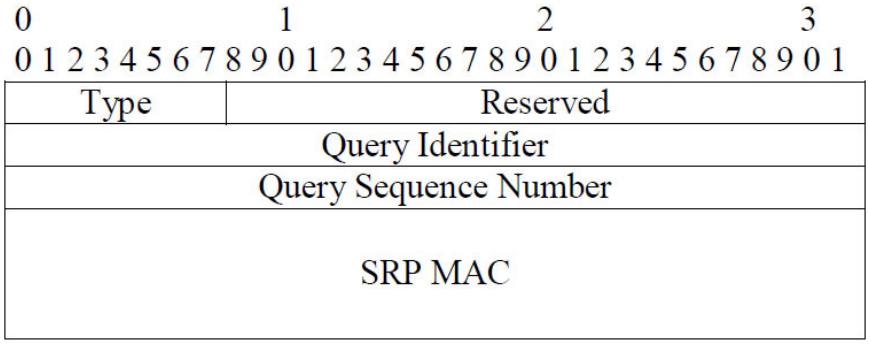

FIGURA 18 – CABEÇALHO DO SRP (PAPADIMITRATOS e HAAS)

Ao ser iniciada a descoberta de rotas pelo nó, um CAM será gerado e o cabeçalho SRP será adicionado à mensagem, como o RREQ. Ao chegar a um nó intermediário, este a analisa e verifica se já viu o pacote anteriormente. Em caso positivo, irá ignorar a mensagem. Caso contrário, irá extrair o QUERY IDENTIFIER, o QUERY SEQUENCE NUMBER, adicionará seu endereço á mensagem e retransmitirá via *broadcast*. Na resposta a uma requisição de rota, o cabeçalho será do tipo RREP e voltará pelo mesmo caminho que percorreu durante a descoberta de rota. Ao chegar ao nó de origem, este irá extrair o CAM e irá verificar a integridade do pacote, já que somente a origem e o destino terão acesso à chave secreta que irá decodificar o CAM. Por utilizar uma AS, garante-se também a autenticidade entre os nós.

O protocolo permite que cada nó controle a prioridade de serviço de uma requisição. Caso um nó gere várias requisições sua prioridade será baixa. Em contrapartida, caso sua taxa de geração seja baixa, sua prioridade será alta. O mecanismo previne que um *flood* ocorra já que o atacante terá baixa prioridade ou até mesmo será descartado do serviço.

4.4 ARIADNE

Considerado um protocolo de roteamento reativo, o Ariadne, descrito por Hu, Perrig e Johnson (2005) foi desenvolvido com base no DSR e utiliza criptografia simétrica como método de autenticação. A aplicação do protocolo visa uma rede em que possam existir nós com baixos recursos computacionais e de energia, como, por exemplo, Palms e PDAs (*Personal Digital Assistants*), já que não utiliza métodos convencionais de assinatura de chaves.

Para compreender o funcionamento do protocolo é necessário entender o método de autenticação Tesla, já que o Ariadne o utiliza para autenticação ponto-a-ponto das mensagens pelo método de difusão. Segundo Júnior e Duarte (2003), o protocolo Tesla necessita que haja uma sincronização fraca entre os *clocks* dos nós da rede para que seja estimado o tempo médio para a mensagem chegar ao destino. Cada um gera uma cadeia *hash,* a partir de uma semente aleatória, que será utilizada posteriormente para autenticação das mensagens. A origem divulga o último valor da cadeia gerada e a utilizará nos sentido inverso para autenticar suas mensagens. Ao enviar uma mensagem, a origem calcula o tempo médio e, após decorrido esse tempo, divulgará a chave utilizada. A receber a mensagem, o destino aplica a função *hash* sobre a chave, chegando no valor final da sequencia. Dessa forma é confirmado que somente o emissor conhecia a chave Tesla utilizada para autenticar a mensagem recebida. Caso haja atraso no recebimento da mensagem e a chave foi revelada antes do destino receber a mensagem, o pacote será descartado. Hu, Perrig e Johnson (2005) estimam que o tempo médio calculado não interfira na segurança do protocolo Ariadne. Contudo, se esse tempo for muito baixo, a probabilidade de ocorrerem descartes será maior.

O Ariadne utiliza três mecanismos de segurança que são mostrados na Figura 19.

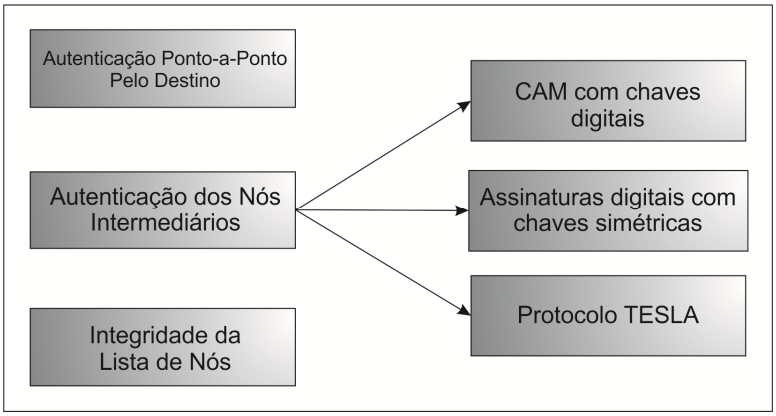

FIGURA 19 – MECANISMOS DE SEGURANÇA DO ARIADNE

4.4.1 Autenticação Ponto-a-Ponto Pelo Destino

Para o nó de destino garantir a legitimidade das mensagens, a origem inclui um CAM nos pacotes utilizando chaves simétricas. Dessa forma, quando o destino receber RREQ poderá garantir a autenticidade da origem.

4.4.2 Autenticação dos Nós Intermediários

O protocolo provê autenticação pela origem de cada nó intermediário listado no RREP. Para isto, três técnicas são utilizadas:

- Utilização de CAM com chaves digitais: Apesar de ser a mais eficiente, exigiria pares de chaves secretas entre todos os nós da rede.
- Utilização de assinaturas digitais com chaves assimétricas: O método é o mais dispendioso já que exigirá maior processamento dos nós na verificação das chaves públicas à cada *hop*.
- Utilização do protocolo Tesla: A autenticação é feita por difusão em que o método utilizado de geração do CAM é através do protocolo Tesla.

O formato do cabeçalho de uma mensagem RREQ esta descrito na Figura 20. O campo *source* contém o endereço de origem e *destination* o endereço de destino. O *id* é configurado pela origem com um valor não recentemente utilizado para evitar

duplicatas. No campo *time interval* consta o tempo médio do Tesla calculado pela origem, o *hash chain* é inicializado com o CAM e o *node list* e *CAM list* são inicializados com zero e guardam a lista dos nós e CAMs por que passou a mensagem, respectivamente Hu, Perrig e Johnson (2005).

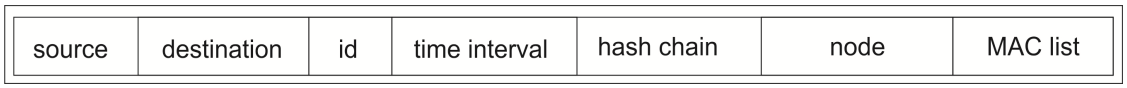

Figura 20 – Cabeçalho do RREQ do Ariadne (Fonte: CUNHA, 2008)

Ao receber uma requisição de rota, o nó intermediário verifica se já viu anteriormente a mensagem. Para isto, analisa o par <*source*, *id*> e se o *time interval* é válido. Caso já tenha visto ou o *time inteval* já esgotou, irá descartar o pacote. Caso contrário, adiciona o seu endereço ao *node list,* o CAM ao *CAM list,* altera o valor do *hash chain* e retransmitirá Hu, Perrig e Johnson (2005). Ao chegar ao destino, este verificará se o valor final da cadeia *hash* está correto e se as chaves Tesla ainda são válidas (ou seja, se ainda não foram divulgadas). Caso positivo, irá computar o CAM da resposta utilizando a chave compartilhada entre o destino e a origem e retornará pela rota reversa Cunha (2008).

O formato da mensagem de resposta, RREP, está definido na Figura 21. O *dest CAM* é calculado usando a chave compartilhada com o nó de origem. Cada nó adiciona sua chave Tesla à mensagem e, ao recebê-la, a origem verificará sua autenticidade.

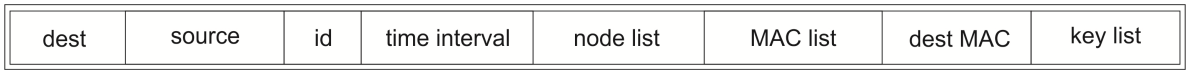

FIGURA 21 – CABEÇALHO DO RREP DO ARIADNE (Fonte: CUNHA, 2008)

4.4.3 Integridade da Lista de Nós

A autenticação entre os nós não é suficiente para garantir a segurança do protocolo já que um nó malicioso poderá alterar a lista de clientes nos pacotes. Para isto, também são utilizadas cadeias *hash* a fim de prover a integridade das mensagens a cada salto.

4.5 ARAN (*AUTHENTICATED ROUTING FOR ADHOC NETWORKS*)

O ARAN (*Authenticated Routing for AdHoc Networks*), Sanzgiri, *et al* (2002), baseado no AODV e DSR, é um protocolo reativo que fornece segurança ao roteamento através da utilização de certificados criptografados e chaves assimétricas. Os certificados são gerados por uma entidade confiável e distribuídos para cada nó antes de se conectar a rede, sendo que, para cada nó é designado somente um certificado. A cada certificado gerado, antes de ser autenticado pelo servidor, é adicionado o IP e chave pública do nó a ser certificado, o *timestamp* e o tempo de expiração daquele. A utilização desse mecanismo garante autenticidade, integridade e não-repúdio na troca de mensagens de roteamento prevenindo, desta forma, ataques do tipo *Arp Spoofing*, *Man in the Middle* e *Sybil*.

A origem inicia o processo de descoberta de rotas com a criação e autenticação do pacote RDP (*Route Discovery Packet*), que contém seu certificado, o tipo do pacote, o endereço IP do destino, *nonce* e o *timestamp* e o envia por broadcast. Ao receber o pacote, os nós vizinhos utilizam a chave pública da origem para conferir a autenticidade da origem, verificam se o certificado não expirou e se já processaram aquele pacote. Caso positivo, o descartam, caso contrário, assinam-no, adicionam seu certificado e retransmitem por broadcast. Esse processo se repete até que chegue ao nó de destino. Contudo, o certificado e a assinatura do nó de origem no pacote permanecem sem alteração, diferentemente dessas informações dos nós intermediários, que são removidas a cada salto.

O processo de retorno do pacote de resposta REP (*Reply*) é semelhante ao *Route Discovery Packet* com a diferença da transmissão ser feita por *unicast* Após autenticar o RDP, o destino adiciona ao pacote o seu certificado, o tipo, o IP da origem, o *nonce* e o *timestamp*. O pacote é autenticado e enviado pelo caminho reverso até a origem. Esse processo garante a autenticação a cada salto e fim-a-fim e previne o não repúdio.

4.6 SAR (*SECURITY-AWARE ADHOC ROUTING*)

O SAR (*Security-Aware Adhoc Routing*) foi projetado para ser uma extensão aos protocolos reativos, como o AODV e DSR, e assegurar que os nós possuam a

segurança necessária para processarem ou reencaminharem pacotes. Yi, Naldurg e Kravets (2002) elucidam que o protocolo tem o objetivo de incorporar métricas de segurança às mensagens de roteamento, que podem ser através de níveis hierárquicos de confiança ou por requisitos de segurança.

Os níveis de confiança podem ser estabelecidos a partir de um sistema de distribuição de assinaturas digitais, compartilhamento de chaves ou certificados digitais. Dessa forma, somente os nós que estiverem no mesmo nível podem trocar mensagens já que os nós maliciosos não têm como decifrar as mensagens daquele nível.

As métricas que envolvem requisitos de segurança são obtidas adicionando técnicas como o *Timestamp* e números de sequência, como relacionados na Tabela 2. Cada atributo poderá ser incorporado ao protocolo de roteamento, contudo, elas geraram um custo para a rede, como por exemplo, *overhead* de banda, *overhead* de CPU.

TABELA 2 – CLASSIFICAÇÃO DE NÍVEIS DE SEGURANÇA

Propiedade	**Técnica**
Tempo	*Timestamp*
Ordenação	*Sequence number*
Autenticidade	*Password*, certificado
Autorização	Credencial
Integridade	Assinatura digital
Confidencialidade	Criptografia
Não-repúdio	*Hash chains*

Para evitar que um nó possa alterar o seu nível ou alterar o nível do pacote RREQ a que por ele passar e comprometer a segurança se faz necessário que exista uma entidade distribuidora de chaves a fim de garantir a encriptação do atributo e a integridade do mesmo.

A descoberta de rotas se inicia adicionando ao pacote RREQ o campo RQ_SEC_REQUIREMENT, que indica o nível de segurança da rota desejada pelo nó e é imutável. Ao receber o pacote, o nó intermediário é verificado se satisfaz ao nível. Caso não satisfaça, o pacote será descartado, caso contrário, o retransmitirá de modo semelhante ao AODV atualizando o campo RQ_SEC_GUARANTEE, que indica o nível máximo de segurança suportado pela rota. Ao chegar ao destino, é garantida que a rota traçada foi a que atendeu o nível de segurança exigido. O valor

RQ_SEC_GUARANTEE é, então, copiado para o RP_SEC_GUARANTEE, no RREP, o que indica o valor máximo de segurança suportada pelo caminho que foi armazenada em *cache*. A fim de se evitar que as informações das mensagens não sejam alteradas indevidamente, ao receber o pacote, o protocolo compara o valor do RP_SEC_GUARANTEE ao do RQ_SEC_REQUIREMENT. O pacote será retransmitido de volta se a comparação estiver em conformidade com o nível exigido.

4.7 SHWMP (*SECURE HYBRID WIRELESS MESH PROTOCOL*)

O protocolo padrão descrito pelo IEEE802.11s, HWMP, trata da segurança entre os MPs, contudo, não garante autenticação ponto a ponto. Essa falha permite alguns ataques, como *flooding*, redirecionamento de rota e *spoofing*, tornando o HWMP vulnerável. A proposta de Islam *et al* (2008), denominada SHWMP é uma alternativa ao protocolo de roteamento padrão e faz autenticação a cada salto utilizando chaves simétricas. O protocolo em questão utiliza GTK (*Group Transit Key*) para criptografar as mensagens enviadas por *bradcast* geradas com o PREQ, PTK (*Pairwise Transient Key*) para criptografar as mensagens *unicast* geradas pelo PREP e RANN. Aplica também a técnica de *Merkle Tree*, um mecanismo que atribui a cada nó de uma árvore um valor *hash*, utilizado para a autenticação dos campos mutáveis das mensagens PREQ, PREP e RANN. Com o esquema de segurança citado anteriormente é garantida a confidencialidade (através do GTK e PTK), não-repúdio (através do *Merkle Tree*).

Os campos não mutáveis do pacote PREQ são o *Hop Count, TTL, Metric* e o *Per Destination Flag#.* Já dos pacotes PREP e RANN são o *Hop Count, TTL, e Metric.*

A descoberta de rotas no modo reativo tem início a partir do nó de origem, que gera a *Merkle Tree* tendo como parâmetro o valor da função *hash* aplicada nos campos não mutáveis do PREQ. Em seguida, o nó gera um CAM com a árvore criada e o transmite por broadcast juntamente com os campos mutáveis que necessitam ser autenticados pelo caminho e o PREQ, com os campos não mutáveis criptografados. Ao receber o PREQ, os vizinhos tentam autenticar os campos mutáveis e criam um CAM com a chave GTK compartilhada. Em seguida comparam o CAM computado com o CAM recebido do nó de origem. Caso os valores sejam iguais, o nó intermediário terá certeza de que os valores são autênticos e vieram da mesma origem que criou a árvore (ISLAM *et al*, 2008).

Os MPs intermediários, então, devem atualizar os valores dos campos mutáveis e gerar uma nova *Merkle Tree* com os campos atualizados. Os campos não mutáveis devem ser decriptados e encriptados novamente com a chave GTK para broadcast. Ao receber o PREQ, o destino deve atualizar os campos mutáveis, gerar sua *Merkle Tree* e retransmitir por *unicast* pelo caminho reverso utilizado pelo PREQ (ISLAM *et al*, 2008).

Quando adotado o modo pró-ativo, os pacotes RANN são encaminhados utilizando a chave GTK a fim criptografar os dados não mutáveis e autenticar os campos mutáveis utilizando a *Merkle Tree.* Ao receber um pacote RANN, o nó que desejar obter um caminho para o nó raiz deverá responder à raiz, por *unicast,* um PREQ utilizando a chave PTK. O nó raiz, ao receber o PREQ, responde também por *unicast* um PREP (ISLAM *et al*, 2008). Dessa forma, é criado um meio seguro entre os dois nós.

4.8 COMPARATIVO ENTRE OS PROTOCOLOS DE ROTEAMENTO SEGURO

Esta seção apresenta comparações entre os protocolos abordados de roteamento seguro em redes *mesh*, SOLSR, SAODV, SRP, Ariadne, ARAN, SAR e a extensão segura para o padrão HWMP, o SHWMP. São analisadas as seguintes características desejáveis de um ambiente seguro: autenticação, confidencialidade, integridade e não-repúdio.

Conforme a Tabela 3 pode-se perceber que a autenticação é um importante atributo de segurança que os protocolos de roteamento em redes *mesh* incorporaram. O atributo pode ser aplicado em cada salto, verificando a autenticidade de cada nó, ou somente entre a origem e o destino. O Ariadne apresenta uma particularidade em relação aos outros protocolos, a autenticação através do protocolo Tesla, o que necessitará da sincronização do tempo entre os nós da rede. O SOLSR, ao contrário do Ariadne, não necessita de sincronização para realizar a autenticação apesar de assumir que os *clocks* estejam em freqüências semelhantes.

TABELA 3 - AUTENTICAÇÃO

Protocolo	**Forma de Autenticação**
SOLSR	A cada nó
SAODV	A cada nó
SRP	Fim a fim
Ariadne	Fim a fim/ a cada nó
ARAN	Fim a fim/ a cada nó
SAR	A cada nó
SHWMP	A cada nó

A Tabela 4 demonstra os métodos de geração de criptografia para realizar a autenticação. Como visto, podem ser utilizadas chaves simétricas e/ou assimétricas. Apesar de serem mais seguras, as chaves assimétricas necessitam de maior poder de processamento pelos nós.

Por ser um protocolo híbrido, o SHWMP pode ser utilizado em situações em que o modo reativo ou o pró-ativo é mais favorável. Em cada situação, o protocolo utiliza envio de mensagens por *unicast* ou *broadcast.* Para isso, são utilizadas chaves do tipo GTK – para *broadcast* – ou PTK – para *unicast* – para criptografar os pacotes.

TABELA 4 – MÉTODO DE CRIPTOGRAFIA

Protocolo	**Método de Criptografia**
SOLSR	Chaves simétricas
SAODV	Chaves assimétricas
SRP	Chaves simétricas
Ariadne	Chaves simétricas/assimétricas
ARAN	Chaves assimétricas
SAR	Chaves simétricas/assimétricas
SHWMP	Chaves simétricas

Conforme análise da Tabela 5, outra característica de segurança adotada é a integridade. Os protocolos utilizam, em geral, assinaturas digitais o que exige que seja realizado o *Message Disgest* da mensagem utilizando a chave privada do nó que está assinando. O Ariadne, o SRP e o SHWMP utilizam Código de Autenticação de Mensagem para checar a integridade das mensagens já que as cadeias *hash* são comparadas.

TABELA 5 – INTEGRIDADE

Protocolo	**Integridade**
SOLSR	Assinaturas digitais
SAODV	Assinaturas digitais
SRP	Código de Autenticação de Mensagem
Ariadne	Assinaturas digitais/ Código de Autenticação de Mensagem
ARAN	Assinaturas digitais
SAR	Assinaturas digitais
SHWMP	Código de Autenticação de Mensagem

A propriedade da confidencialidade não é atendida por todos os protocolos, conforme a Tabela 6. Por utilizarem certificados digitais, somente o ARAN, SAR e o SHWMP garantem o atributo.

TABELA 6 – CONFIDENCIALIDADE

Protocolo	**Confidencialidade**
SOLSR	Não garante
SAODV	Não garante
SRP	Não garante
Ariadne	Não garante
ARAN	Utilização de criptografia
SAR	Utilização de criptografia
SHWMP	Utilização de criptografia

O não-repúdio não é garantido em todos os protocolos de roteamento seguro mesmo sendo uma propriedade útil para as WMNs visto que isolam os nós mal intencionados. Como pode ser percebido na Tabela 7, somente o SAODV, SHWMP, ARAN e o SAR garantem o não repúdio, pois utilizam chaves assimétricas e/ou necessitam de certificados digitais.

Para garantir o não repúdio, o SHWMP utiliza do mecanismo *Merkle Tree,* que garante a identidade dos nós da rede mesh.

TABELA 7 – NÃO-REPÚDIO

Protocolo	**Não-repúdio**
SOLSR	Não garante
SAODV	Utiliza chaves assimétricas
SRP	Não garante
Ariadne	Não garante
ARAN	Utiliza certificados digitais/ Utiliza chaves assimétricas
SAR	Chaves assimétricas
SHWMP	*Merkle Tree*

A Tabela 8 apresenta um resumo comparativo dos atributos de segurança garantidos pelos protocolos de roteamento seguro em redes *mesh.*

TABELA 8 – RESUMO COMPARATIVO

Atributos	**SOLSR**	**SAODV**	**SRP**	**Ariadne**	**ARAN**	**SAR**	**SHWMP**
Autenticação	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Criptografia	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Integridade	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Confidencialidade	Não	Não	Não	Não	Sim	Sim	Sim
Não-Repúdio	Não	Sim	Não	Não	Sim	Sim	Sim

A TABELA 9 mostra os tipos de ataques à camada de rede prevenidos pelos protocolos seguros estudados.

O *Rushing Attack* e o W*ormhole* são dois tipos de ataques dificilmente de serem identificados. A vulnerabilidade é decorrente da falta de autenticação dos dados mutáveis dos protocolos. O SWHMP, por autenticar os dados verificando os códigos de autenticação de mensagem, é eficiente na proteção ao ataque.

Os ataques *Grey Hole* e *Black Hole* são evitados pelos protocolos devido ao mecanismo de autenticação. O atacante não conseguirá adicionar falsas rotas ao pacote já que não é capaz autenticar a mensagem. Já o *Overflow Attack* e o *Sybil Attack* são evitados quando o pacote é assinado a cada salto.

TABELA 9 – ATAQUES PREVINIDOS

Ataques	SOLSR	SAODV	SRP	Ariadne	ARAN	SAR	SHWMP
Sybil	Protege	Protege	Protege	Protege	Protege	Protege	Protege
Grey Hole	Proteje	Proteje	Protege	Protege	Proteje	Proteje	Proteje
Black Hole	Protege	Proteje	Protege	Protege	Protege	Protege	Protege
Overflow	Protege	Protege	Não proteje	Não protege	Não proteje	Proteje	Protege
Rushing	Não identificado	Não protege	Não protege	Não protege	Não protege	Não identificado	Protege
Wormhole	Não identificado	Não protege	Não protege	Não protege	Não protege	Não identificado	Protege

4.9 CONCLUSÃO

Neste capítulo foram abordados alguns protocolos seguros utilizados em redes *mesh*, híbridas ou não. Foram analisados seus métodos de descoberta de rotas e as implementações que garantem atributos de segurança. Ao final é realizado um comparativo entre os protocolos de roteamento seguro tendo como foco os atributos de segurança desejáveis e alguns ataques realizados na camada de rede.

Com base nos atributos comparados e nos tipos de ataques prevenidos, foi percebido que, por garantir autenticação e a integridade das mensagens de roteamento, os protocolos estudados se portam bem frente aos ataques à camada de rede.

Apesar de o HWMP ser o protocolo padrão utilizado pelo IEEE 802.11s, ainda é vulnerável a alguns ataques. Em sua versão segura, o SHWMP, como pode ser percebido na Tabela 8 e Tabela 9, supre algumas deficiências de segurança do padrão, podendo ser aplicado em situações em que se deseje garantir a proteção àqueles ataques.

5 CONSIDERAÇÕES FINAIS

No estudo deste trabalho foi percebido que as WMNs (*Wireless Mesh Netorks*) têm grande utilidade em diversas aplicações. Seu sucesso será possível devido seu grande potencial na expansão da área de cobertura dos roteadores sem fio, podendo abranger áreas que são demograficamente inacessíveis. Seu custo também é um atrativo visto que os próprios participantes são responsáveis por aumentar a conectividade da rede através dos múltiplos saltos. Como foi visto, essa característica, entretanto, expõe o *backbone* e seus nós a graves falhas de segurança.

O trabalho ainda abordou alguns padrões desenvolvidos pelo IEEE que definem a arquitetura das redes sem fio. Foram destacados também o padrão 802.11, por tratar especificamente das redes *mesh*, e seu protocolo de roteamento padrão, HWMP.

Como visto, as camadas física, de enlace e de rede estão sujeitas a vários tipos de ataques e várias técnicas foram desenvolvidas para prover segurança a essas camadas. Entretanto, garantir as propriedades de segurança, como autenticidade, integridade e não-repúdio, exigirá maior esforço por parte dos nós, que podem não possuir alto processamento e reservas adequadas de energia. Essa característica vai de encontro ao objetivo das WMNs que é a expansão da cobertura de sinal provida pelos próprios utilizadores da rede.

Nas redes em malha sem fio, a participação e colaboração entre os nós garantem a escalabilidade e a segurança da rede visto que a acessibilidade dos nós aos recursos da rede se dará pelos próprios nós. Desta forma, o trabalho se propôs a estudar e comparar os protocolos de roteamento seguro a fim de que se possam realizar melhores planejamentos de redes tendo em vista as propriedades de segurança garantidas por cada protocolo.

Como proposta de trabalhos futuros, sugere-se realizar estudos e comparativos de outros protocolos de roteamento seguro em redes *mesh* híbridas, como o *Secure Routing Protocol for Infrastructure Base Wireless Mesh* (SRPM) e o *Cross Layer Secure and Resource-Aware on Demand Routing* (CSROR).

REFERENCIAS BIBLIOGRÁFICAS

AGUIAR. E. S. *et al*. Segurança em Redes Mesh: Tendências, Desafios e Aplicações. Minicursos do Simpósio Brasileiro de Segurança 2008. 2008.

AKYILDIZ, I.F; WANG, X. A survey on wireless mesh networks. IEEE Communications Magazine, 2005.

_____; _____; WANG, W. Wireless mesh networks: a survey. Computer Networks , 2005.

AL-SHURMAN, M.; YOO, S.M.; PARK, S. Black Hole Attack in Mobile Ad Hoc Network. Proceedings of the 42nd annual Southeast regional conference. 2004.

ANASTASI,G.; CONTI, M.; GREGORI, E. IEEE 802.11 Ad Hoc Networks: Protocols, Performance, And Open Issues. Mobile Ad hoc networking. 2005.

ANJUM, F.; MOUCHTARIS. P. Security for Wireless Ad Hoc Networks. United States of America: Wiley, 2007. 247p.

BAHR, M. Update on the hybrid wireless mesh protocol of IEEE 802.11s. IEEE Conference on Mobile Adhoc and Sensor Systems. 2007.

CISCOMESH. Disponível [Online] http://www.cisco.com/en/US/netsol/ns621/networking_solutions_package.html, 08 jul.2010.

CLAUSEN, T. H.; *et al*. The Optimized Link State Routing Protocol Evaluation through Experiments and Simulation. IEEE Symposium on" Wireless Personal Mobile Communications. 2003.

CUNHA, S. R. Protocolos de roteamento seguro para MANETs: características do Ariadne e do SAODV, e comparativo de desempenho e eficácia entre o Ariadne e o DSR. Joinville: SOCIESC, 2008. 50p.

FARIAS, M.M.; BEZERRA, E. A. Protocolo de roteamento para redes Wireless Mesh. 2006. 15p. Programa de Pós-Graduação em Ciência da Computação, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2007.

HAFSLUND, A.; *et al*. Secure Extension to the OLSR protocol. Proceedings of the OLSR Interop and Workshop. 2004.

HE, G. Destination-Sequenced Distance Vector (DSDV) Protocol. Networking Laboratory, Helsinki University of Technology. 2002.

HU, Y.C.; PERRIG, A.; JOHNSON, B. Packet Leashes: A Defense against Wormhole Attacks in Wireless. IEEE Societies INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. 2003.

_____; _____; _____. Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks. Wireless Networks. 2005

ISLAM, M.; *et al*. A Secure Hybrid Wireless Mesh Protocol for 802.11 s Mesh Network. Computational Science and Its Applications. 2008

JOHNSON, D.B.; *et al*. DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks. Ad hoc networking. 2001.

JÚNIOR, A. A.; DUARTE, O. C. M. B. Segurança no Roteamento em Redes Móveis Ad Hoc. Seminário de Tópicos Especiais em Redes de Computadores. 2003

KUROSE, J. F.; ROSS, K. W. Redes de Computadores e a Internet: Uma Abordagem Top-Dow. 3. ed. São Paulo: Pearson, 2005. 634p.

NAKAMURA, E. T.; GEUS, P. L. Segurança de Redes em Ambientes Cooperativos. São Paulo: Novatec, 2007. 482p.

NAVEED, A.; KANHERE, S. S.; JHA S. K. Attacks and Security Mechanisms. In: ZHANG, Y.; ZHENG, J.; HU, H.; Security in Wireless Mesh Networks. 2008. p. 111-144.

PAPADIMITRATOS, P.; HAAS, Z.J. Secure routing for mobile ad hoc networks. SCS Communication Networks and Distributed Systems Modeling and Simulation Conference. 2002.

REMESH. Disponível [Online] http://mesh.ic.uff.br/, 08 jul.2010.

ROOFNET. Disponível [Online] http://pdos.csail.mit.edu/roofnet/doku.php, 08 jul.2010.

SAADE, D. C. M.; et al. Multihop MAC: Desvendando o Padrão 802.11s. 26º Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos. 2008.

SANZGIRI, K.;*et al*. A secure routing protocol for ad hoc networks. Proceedings of the 10 th IEEE International Conference on Network Protocols. 2002.

SESAY, S.; YANG, Z.; HE, J. A Survey on Mobile Ad Hoc Wireless Network. Information Technology Journal. 2004.

TENENBAUM, A. S. Redes de Computadores. 14. ed. Rio de Janeiro: Campos, 2003. 945p.

WINGET, N.-C.; RAHMAN, S. Security in Wireless LAN Mesh Networks. Security in Wireless Mesh Networks. 2008.

WU, B.; *et al*. A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks. Wireless Network Security. 2006.

XU, W.; *et al*. The feasibility of launching and detecting jamming attacks in wireless networks. Wireless Network Security. 2005.

YI, S.; NALDURG, P.; KRAVETS, R. A Security-Aware Routing Protocol for Wireless Ad Hoc Networks. Urbana. 2002

Zapata, M.G.; Asokan, N. Securing ad hoc routing protocols. Proceedings of the 1st ACM workshop on Wireless security. 2002.