Leandro Arabi Alexandre

Métodos seguros para comunicação em sistemas de rede sem fio de múltiplos saltos

São José do Rio Preto
2011

Leandro Arabi Alexandre

Métodos seguros para comunicação em sistemas de rede sem fio de múltiplos saltos

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Ciência da Computação, junto ao Programa de Pós-Graduação em Ciência da Computação, Área de Concentração - Sistemas de Computação, do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista “Júlio de Mesquita Filho”, Campus de São José do Rio Preto.

Orientador: Prof. Dr. Adriano Mauro Cansian

São José do Rio Preto
2011

Alexandre, Leandro Arabi.
Métodos seguros para comunicação em sistemas de rede sem fio de múltiplos saltos / Leandro Arabi Alexandre. - São José do Rio Preto : [s.n.], 2011.
52 f. : il. ; 30 cm.

Orientador: Adriano Mauro Cansian
Dissertação (mestrado) - Universidade Estadual Paulista, Instituto de Biociências, Letras e Ciências Exatas

1. Computação. 2. Redes de computadores – Medidas de segurança. 3. Redes *ad hoc*. 4. Redes *mesh*. 5. Roteamento (Administração de redes de computadores). I. Cansian, Adriano Mauro. II. Universidade Estadual Paulista, Instituto de Biociências, Letras e Ciências Exatas. III. Título.

CDU – 004.056

Ficha catalográfica elaborada pela Biblioteca do IBILCE
Campus de São José do Rio Preto - UNESP

Leandro Arabi Alexandre

Métodos seguros para comunicação em sistemas de rede sem fio de múltiplos saltos

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Ciência da Computação, junto ao Programa de Pós-Graduação em Ciência da Computação, Área de Concentração - Sistemas de Computação, do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista “Júlio de Mesquita Filho”, Campus de São José do Rio Preto.

Banca Examinadora

Prof. Dr. Adriano Mauro Cansian
UNESP – São José do Rio Preto
Orientador

Prof. Dr. Alex Sandro Roschildt Pinto
UNESP – São José do Rio Preto

Profa. Dra. Kalinka Regina Lucas Jaquie Castelo Branco
USP – São Carlos

São José do Rio Preto
07/Novembro/2011

Dedico este trabalho

Aos meus pais, Leila e Valdemar, minha avó materna, Adélia, e ao meu irmão Ricardo, pelo incentivo, compreensão e amor durante todos os tempos.

AGRADECIMENTOS

Aos meus pais, Leila e Valdemar, meu irmão Ricardo e minha avó Adélia, por sempre me apoiarem e me incentivarem para chegar até onde cheguei.

Ao meu orientador, Prof. Dr. Adriano Mauro Cansian, pela orientação pessoal e acadêmica, pelo apoio durante os anos que permaneci no Laboratório ACME! e pelas horas de descontração.

Aos meus colegas de laboratório: Maira, André e Isabela em especial pela ajuda no projeto e pela enorme amizade que têm comigo.

Aos companheiros de laboratório, Jorge, Allan, Pedro, Heitor, Adriano, obrigado pelo companheirismo, pelas horas de conversa e estudo.

Aos colegas de sala, pelo companheirismo, horas de estudo, e por toda ajuda em todos esses anos: Carlos Roberto, Cleriston, Eder e Victor.

Aos meus amigos e amigas que sempre me acompanharam, ajudando e me dando forças para fazer tudo que necessário, pela amizade e companhia por todos esses anos: Polyana Cortizo Debiagi, Guilherme Domingues Abrantes, Luciano da Silva Cassemiro e todos outros que não citei aqui.

Aos professores do Departamento de Ciências de Computação e Estatística, pelos conhecimentos passados ao longo desses anos.

“Nunca deixe que lhe digam que não vale
a pena acreditar no sonho que se tem.”
Renato Russo

ÍNDICE

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AODV: *Ad hoc On-demand Distance Vector Routing Protocol*
ARP: *Address Resolution Protocol*
CSMA/CA: *Carrier Sense Multiple Acess with Collision Avoidance*
CTS: *Clear to send*
DCF: *Distributed Coordination Function*
DHCP: *Dynamic Host Configuration Protocol*
DSR: *Dynamic Source Routing Protocol*
IEEE: *Institute of Electrical and Electronics Engineers*
IETF: *Internet Engineering Task Force*
HWMP: *Hybrid Wireless Mesh Protocol*
IP: *Internet Protocol*
LAN: *Local Area Network*
MACAW: *Multiple Access with Collision Avoidance for Wireless*
MANETs: *Mobile Ad-hoc NETworks*
MTU: *Maximum Transmit Unit*
NAV: *Network Allocation Vector*
OLSR: *Optimized Link State Routing Protocol*
PCF: *Point Coordination Function*
QoS: *Quality of Service*
RA-OLSR: *Radio-Aware Optimized Link State Routing Protocol*
RADIUS: *Remote Authentication Dial In User Service*
RFC: *Request for Comments*
RREQ: *Route Request*
RRER: *Route Reply*
RTS: *Request to send*
RTT: *Round-trip Time*
SNMP: *Simple Network Management Protocol*
TCP: *Transmission Control Protocol*
UDP: *User Datagram Protocol*

RESUMO

A utilização de computadores portáteis trouxe a necessidade de criação de redes de acesso sem fio. Mesmo com o padrão 802.11, um dos protocolos responsáveis por gerir os sistemas *wireless*, a mobilidade desejada não era alcançada. Diversas regiões de difícil acesso eram isoladas das redes de comunicação por não existir uma forma eficiente de levar os dados até estas. Pensando nisso, foram criadas as redes sem fio de múltiplos saltos, conhecidas por *wireless mesh* ou *ad-hoc*. Uma rede de múltiplos saltos é composta por diversos dispositivos que se interconectam por meio de conexão sem fio, levando assim a informação para regiões distantes. No entanto, há sérios problemas de segurança que atingem ambas as soluções: redes sem fio ou múltiplos saltos. Baseado no aspecto de segurança da informação, este trabalho apresenta soluções que podem ser utilizadas para fazer roteamento seguro de informações em redes de múltiplos saltos.

Palavras-chave: Redes *ad hoc*. Redes *mesh*. Roteamento. Segurança.

ABSTRACT

The use of laptops brought the need for network wireless access creation. Even with the creation of 802.11 standard, which is one of the responsible for managing the wireless systems, the mobility desired was not enough. Many areas of difficult access were isolated from network communication because they din't have an efficient way to bring data to these areas. To address this, they created the wireless multi-hop, also know as wireless mesh or ad hoc. A wireless multi-hop network is composed of several devices that are interconnected by wireless connection, so they can bring information to distant areas. However, there are serious security issues that affect both solutions: wireless networks or multi-hop. Based on the aspect of information security, this paper presents solutions that can be used to secure routing information in multi-hop networks.

Keywords: Ad hoc networks. Mesh networks. Routing. Security.

Capítulo 1 - Introdução

1.1 Considerações iniciais

Com o surgimento dos computadores, muitas tarefas eram automatizadas pelo simples fato de existir a troca de informação digital entre dois sistemas computacionais, poupando esforço manual para digitar um documento, por exemplo. Porém, a troca era feita de forma manual, via disquete ou até mesmo fitas contendo os dados que desejam ser compartilhados. Para solucionar esses problemas e também proporcionar maior compartilhamento de informações surgiram as redes de computadores.

No início, apenas alguns computadores se conectavam utilizando um protocolo de comunicação próprio, sem padronização. Após algum tempo, a necessidade de interagir com outros sistemas remotos fez com que fosse criada uma padronização para a implantação de uma rede de computadores. Criada a padronização, redes puderam ser interligadas, dando margem à criação de uma grande rede mundial, a Internet.

Mesmo com a interligação de redes de grande porte, determinadas regiões geográficas não possuem os requisitos necessários para que uma rede cabeada possa

ser instalada. Além disso, a criação de computadores portáteis, como *laptops*, celulares e outros dispositivos portáteis, impulsionaram o crescimento da demanda por uma rede sem fio, comumente conhecida como *wireless*.

Não somente foram criadas redes para interligação de computadores, mas também dos periféricos associados a eles. Muitos usuários preferem utilizar um teclado ou impressora sem fio, ato que facilita a organização e manuseio desses dispositivos no dia-a-dia. Além dessas utilizações, sistemas de comunicação sem fio também são implementados nos dias atuais na comunicação entre duas regiões distantes, na utilização de telefonia móvel e na transmissão de dados entre dispositivos dedicados de comunicação.

Em redes sem fio, o objetivo é interligar componentes que estão a um alcance limitado, de acordo com a tecnologia de transmissão utilizada. Essas redes estão se tornando cada vez mais comuns em locais onde a instalação de uma rede *Ethernet* cabeada é considerada trabalhosa, como por exemplo instalações em ambientes antigos, salas de reuniões e conferências, entre outros. A padronização das redes sem fio é definida pelo padrão IEEE 802.11, que abrange a maioria dos sistemas que dispõem de comunicação sem fio.

Embora o advento das redes sem fio trouxe um grande avanço na comunicação de dados, existem locais que não possuem viabilidade técnica para instalação de tais redes, locais como montanhas e instalações urbanas onde é inviável o uso de um cabo para prover conectividade a uma determinada região.

Para solucionar o novo problema criado pela indisponibilidade de acesso físico a um determinado local com uma rede cabeada, foram criadas técnicas que são capazes de interligar dispositivos de rede por meio de comunicação sem fio. Por exemplo, uma cidade pode ter suas estações de controle de trânsito interligadas por redes sem fio, mas para que o custo de levar um cabo até cada estação não inviabilize o projeto, usa-se redes sem fio de múltiplos saltos, também conhecidas como *wireless mesh* ou *ad-hoc*.

Redes *Mesh*, ou redes em malha sem fio, são redes com topologia dinâmica, variável e de crescimento orgânico, que são constituídas por nós cuja comunicação no nível físico é feita através de variantes dos padrões IEEE 802.11 e 802.16 (WiMAX – *Worldwide Interoperability for Microwave Access*). O roteamento nestas redes é dinâmico, uma vez que sua topologia pode mudar constantemente. Redes

deste tipo são consideradas evoluções de redes móveis *ad-hoc*, ou MANETs (*Mobile Ad-hoc NETworks*) (ABELÉM; *et al.*, 2007). Composta por nós, uma rede *mesh* se organiza automaticamente, fazendo com que pessoas e dispositivos tenham acesso a uma estrutura de rede em áreas que não existem estruturas de comunicação.

Esses tipos de rede tem sido muito utilizadas, inclusive em cenários militares (CHLAMTAC; CONTI; LIU, 2003). No entanto, existem diversos problemas de segurança associados ao uso desta tecnologia. Alguns desses problemas são citados em (GLASS; PORTMANN; MUTHUKKUMARASAMY, 2008), e atingem desde níveis da camada física, até a camada de aplicação.

Devido a esses problemas de segurança, o IEEE (*Institute of Electrical and Electronics Engineers*) criou um grupo de trabalho para assegurar a segurança de comunicações que utilizam redes de múltiplos saltos. Para isso foi criado um padrão, o 802.11s, que em 2011 encontra-se em processo de padronização, portanto é um *draft*, não tendo se tornado um RFC ainda. Esse padrão faz uso maciço de tecnologias de criptografia para autenticar e criptografar mensagens, garantindo a integridade de dados trafegados em redes *wireless* de múltiplos saltos. Além disso, outros métodos para assegurar o transporte de informações nestas redes são estudados.

Este projeto faz parte de uma iniciativa do Ministério de Ciência e Tecnologia para a criação dos Institutos Nacionais de Ciência e Tecnologia, ao qual este projeto está vinculado ao INCT-SEC, Instituto Nacional de Ciência e Tecnologia na área de Sistemas Embarcados Críticos (INCT-SEC, 2011). Este projeto é financiado por CNPq e FAPESP através do financiamento ao INCT-SEC, processos 573963/2008-8 e 08/57870-9 e, a nível de mestrado financiado pela CAPES.

1.2 Objetivos

Este trabalho tem como objetivo apresentar uma breve revisão bibliográfica sobre os padrões de redes sem fio, 802.11, como essas redes evoluíram para a comunicação em redes de múltiplos saltos e quais suas principais características de

funcionamento. Além disso, é proposto a utilização de uma técnica para mitigar ataques à infraestrutura deste tipo de redes.

1.3 Organização

Este documento está organizado em cinco capítulos, sendo o primeiro a introdução, que trata de forma ampla o assunto que será desenvolvido nos capítulos posteriores. No segundo capítulo é apresentado o padrão IEEE 802.11, utilizado em redes sem fio convencionais, ou seja, baseadas em um ponto central de infraestrutura. No terceiro capítulo é apresentado o desenvolvimento deste projeto, exibindo as soluções propostas para os problemas de segurança apontados no mesmo capítulo. No quarto capítulo são exibidos os testes preliminares e resultados obtidos com uma ferramenta de simulação. Por fim, capítulo quinto são apresentadas as conclusões obtidas deste trabalho.

Capítulo 2 – Redes sem fio

2.1 Considerações iniciais

Neste capítulo são abordadas as tecnologias de comunicação sem fio baseadas no padrão 802.11, sejam elas convencionais ou redes de múltiplos saltos. São apresentados os aspectos funcionais de redes de múltiplos saltos que permitem a incidência de ataques à sua infraestrutura. Este capítulo também contém informações sobre métodos desenvolvidos para mitigar tipos específicos de ataques em redes de múltiplos saltos.

2.2 Conceitos iniciais

Para focar nos assuntos de redes *wireless*, é necessário primeiro entender alguns termos que são comumente utilizados nesta área. Os primeiros conceitos abordados referem-se a terminologia de como são chamados os elementos de uma rede sem fio. A figura 2.1 ilustra um exemplo de cenário de um ambiente *wireless*.

Figura 2.1 Exemplo de um ambiente de rede sem fio.

De acordo com a legenda apresentada na figuras tem-se as seguintes descrições (KUROSE; ROSS, 2006):

- **Hospedeiros sem fio**: são dispositivos de usuários finais, tais como *notebook*, telefone celular, dispositivos de jogos eletrônicos e outros;
- **Enlaces sem fio**: é um meio ao qual um hospedeiro conecta-se a uma estação base, ou ainda em outro dispositivo. De acordo com a tecnologia utilizada este enlace de dados pode variar;
- **Estação base**: é a parte principal de uma infraestrutura de rede sem fio. É responsável pelo envio e recebimento de dados de hospedeiros e para hospedeiros. Quando um hospedeiro dentro do alcance da estação base, é dito que este encontra-se associado à esta estação;

Em relação ao modo de conexão, quando um hospedeiro está associado com uma estação base, é dito que ele está operando em modo infraestrutura, já que todos os serviços básicos de rede (atribuição de endereço, roteamento, por exemplo) é provido pela estação-base. Caso contrário, na ausência de uma estação-base, os próprios hospedeiros devem fornecer os serviços tais como roteamento, atribuição de endereços, DNS e outros (KUROSE; ROSS, 2006). Tal modo de conexão é chamado *ad hoc*.

2.3 Padrões de LAN sem fio IEEE 802.11

Existem diversos padrões definidos pelo IEEE para LANs sem fio, entre eles, os mais famosos para uso em pequena e larga escala são os padrões 802.11b, 802.11a e 802.11g. Todos são utilizáveis nos dias atuais, mas recentemente foi adicionado mais um padrão, o 802.11n, que aprimorou alguns aspectos de velocidade de conexão e outros parâmetros. A tabela 2.1 exibe alguns parâmetros que diferenciam os padrões em relação às características de camada de enlace e física (KUROSE; ROSS, 2006).

Tabela 2.1 Características dos padrões 802.11.

Padrão	Faixa de frequência de operação	Taxa de dados
802.11b	2.4 ~ 2.485 GHz	Até 11 Mpbs
802.11a	5.1 ~ 5.8 GHz	Até 54 Mpbs
802.11g	2.4 ~ 2.485 GHz	Até 54 Mpbs
802.11n	2.4 ou 5 GHz	Até 600 Mpbs

Nos modelos mencionados acima, os padrões que operam em uma faixa de frequência de 2.4 GHz, a mesma utilizada por alguns telefones sem fio e fornos microondas, são alvos de maiores interferências de sinal. O 802.11b embora utilize uma baixa taxa de transmissão de dados, devido a sua frequência de operação consegue fazer com que o alcance da rede seja maior. Já no caso do 802.11a, a velocidade de transmissão foi priorizada, em detrimento do alcance da rede. Da união dos dois padrões nasceu o 802.11g, que opera em uma faixa de frequência baixa como do 802.11b, mas com taxas de transmissão mais altas, como as do 802.11a.

Já o padrão 802.11n, recentemente ratificado pelo IEEE (IEEE, 2009), tem como objetivo principal melhorar a velocidade de seus antecessores. Utilizando técnicas de camada física, tais como o uso de múltiplas antenas ou MIMO (*Multiple-Input, Multiple-Output*), o novo padrão consegue obter velocidades de até 600 Mpbs (PAUL; OGUNFUNMI, 2008).

2.4 Arquitetura 802.11

O padrão 802.11 tem uma arquitetura de componentes bem definida. Em primeiro lugar tem-se o conjunto básico de serviço, ou BSS (*basic service set*). Um BSS é o conjunto de um ou mais hospedeiros sem fio e uma estação base central, conhecida como ponto de acesso, ou AP (*access point*). Um BSS pode ser do tipo infraestruturado ou não. Na figura 2.2 é possível ver um exemplo de associação de terminais sem fio a um ponto de acesso, criando um BSS operando no modo infraestrutura e a outra variante, um BSS que interliga dispositivos sem fio em conexões *ad hoc (*TANENBAUM, 2003).

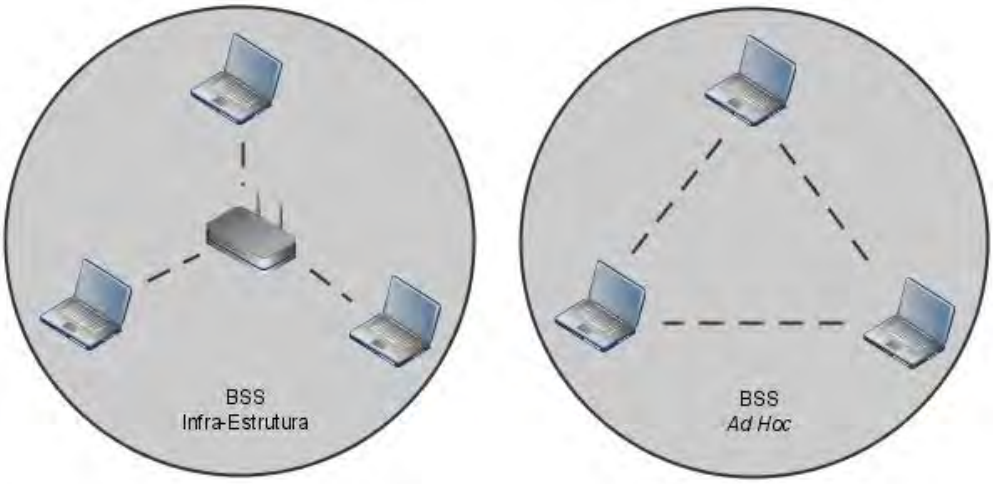

Figura 2.2 Exemplos de BSS Infraestrutura e *Ad Hoc*.

Em um BSS operando em modo de infraestrutura, o ponto de acesso possui uma identificação para que seus clientes possam se associar a ele, é o Identificador de Conjunto de Serviços, ou SSID (*Service Set Identifier*). Esse nome pode ser composto de uma ou duas palavras e é utilizado por um hospedeiro sem fio para se associar ao ponto de acesso. Além deste nome, o administrador do equipamento deve também especificar qual canal de comunicação o AP irá operar (KUROSE; ROSS, 2006). No total o padrão 802.11b possui 11 canais diferentes, onde cada estação base opera em um ou mais canais, de acordo com sua configuração. Um canal possui uma faixa de frequência que será utilizada para transmissão de dados, onde todos possuem sobreposição parcial de frequências, podendo resultar em interferências.

2.5 Redes de múltiplos saltos

Redes de múltiplos saltos são um tipo de rede onde cada nó da rede pode agir como um roteador, independente de estar conectado a outra rede ou não. Essa característica permite que a rede se torne mais confiável, pois pode possuir múltiplos caminhos que serão utilizados em caso de falha em um nó para alcançar um destino. Esse tipo de rede pode ser dividida em duas categorias: MANETs, que são redes móveis *ad*-hoc, e redes *mesh*, onde os nós integrantes da rede geralmente não apresentam movimentação (SAADE; *et al.*, 2008).

Outra diferença de redes *ad hoc* é que essas tem um uso limitado devido ao pouco incentivo de seus participantes para compartilhamento de recursos, uma vez que cada um teria gastos que não serão repostos pelos outros nós da rede, por exemplo a bateria de um *laptop*.

Ao contrário das redes cabeadas convencionais, redes de múltiplos saltos utilizam como conexão principal (*backbone*) a conexão sem fio, que é estendida até seus clientes finais por meio de roteadores ou nós intermediários, como pode ser observado na figura 2.3.

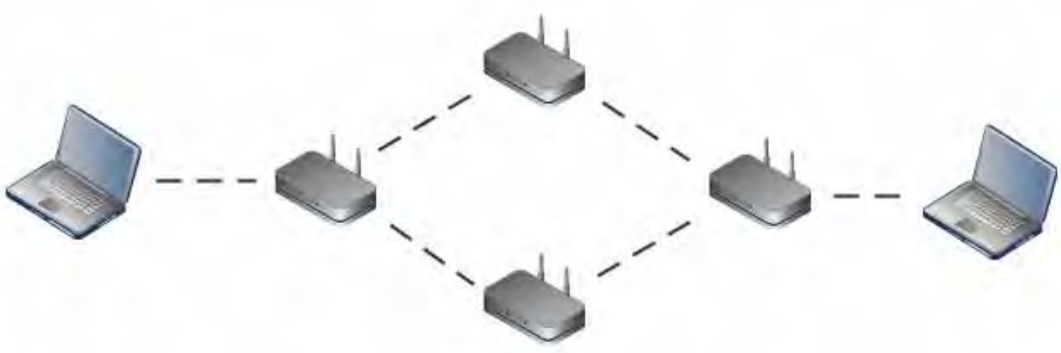

Figura 2.3 *Backbone* de uma rede *wireless* de múltiplos saltos.

Na figura 2.3 é possível observar uma estação no canto esquerdo comunicando-se com outra no canto direito da figura. Toda a comunicação é feita por enlaces de redes sem fio, utilizando roteadores *wireless mesh* para o translado das informações. Além da comunicação, a figura ilustra uma das importantes propriedades destas redes: tolerância a falhas. No caso de um dos caminhos perder o enlace, a rede consegue se comunicar com outros enlaces, refazendo o caminho perdido por outro roteador.

2.6 Comparações entre redes *wireless mesh* e *ad-hoc*

Na figura 2.4 é possível ver uma classificação feita em (ZHANG; LUO; HU, 2006) das redes *wireless* de múltiplos saltos. As categorias de maior uso em redes *wireless* são as *ad hoc, wireless mesh, wireless sensor networks* e redes híbridas (*hybrid wireless networks*). As redes *ad hoc* são predominantemente redes sem infraestrutura e que possuem topologia altamente dinâmica. Redes de sensores são comumente utilizadas para coletar informações de parâmetros físicos e transmiti-las a uma estação central. Já as redes híbridas utilizam ambas as formas de comunicação: redes de múltiplos saltos ou convencionais. E por último, as redes *mesh*, que usam múltiplos saltos em uma malha parcial ou completa.

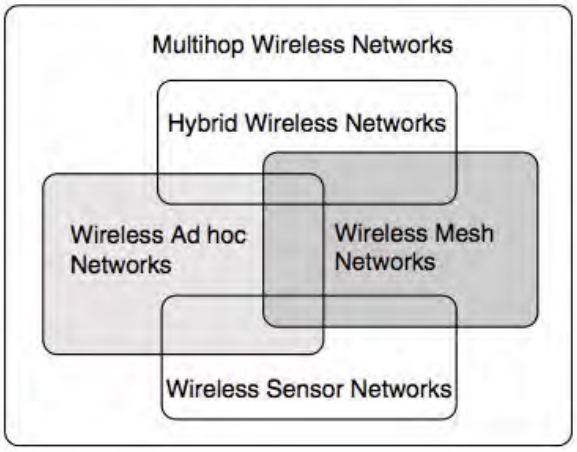

Figura 2.4 Classificação das redes *wireless* de múltiplos saltos (ZHANG; LUO; HU, 2006).

Na tabela 2.2 é possível observar algumas comparações feitas entre *wireless ad hoc* e *wireless mesh*. Uma das principais diferenças é que as redes *ad hoc* são altamente móveis, enquanto redes *mesh* são relativamente estáticas.

Tabela 2.2 Comparação entre *wireless ad hoc* e *mesh* (ZHANG; LUO; HU, 2006).

Aspecto	*Wireless ad hoc*	*Wireless mesh*
Topologia da rede	Altamente dinâmica	Relativamente estática
Mobilidade dos nós	Média para alta	Baixa
Restrições de energia	Altas	Baixas
Aplicações características	Temporárias	Semipermanentes/permanente
Infraestrutura requerida	Sem infraestrutura	Infraestrutura parcial/total

Entrega de pacotes	Por dispositivos móveis	Por dispositivos fixos
Desempenho de roteamento	Roteamento sob-demanda totalmente distribuído	Totalmente/parcialmente distribuído
Nível de dificuldade para instalação	Fácil	Requer algum planejamento
Características de tráfego	Típico de usuário	Típico de sensores e usuários
Cenários comuns de uso	Comunicação tática	Comunicação tática/civil

Um dos aspectos importantes que devem ser levados em consideração a respeito dos cenários de uso é que ao contrário de redes *ad hoc*, redes *mesh* são mais utilizadas para uso militar, como aponta o artigo (SHYV, 2006). As redes *mesh* também são utilizadas em aplicações populares com a finalidade de prover acesso à Internet a custos baixos. Exemplos dessas aplicações são os projetos OLPC (*One Laptop per Child*) (OLPC, 2010) e RUCA (Redes para UCA) (RUCA, 2010). O OLPC tem como objetivo produzir *laptops* de baixo custo e distribuí-los em escolas de uma comunidade, onde seria formada uma rede *mesh* entre os moradores para acessar a rede da escola e assim ganhar acesso a Internet. Já o RUCA é uma iniciativa brasileira para prover acesso ao projeto UCA (Um computador por aluno), semelhante ao projeto da OLPC. No Brasil esse projeto é promovido pelo Ministério da Educação e Casa Civil.

2.7 Algoritmos de roteamento para redes de múltiplos saltos

A principal tarefa de algoritmos de roteamento é selecionar o caminho pelo qual um pacote enviado por um *host* de origem irá percorrer até seu destino, de forma rápida, com um custo mínimo e ser um processo confiável, para não ocasionar perdas de pacotes e outros problemas.

Em geral, os protocolos de roteamento de redes de múltiplos saltos podem ser classificados em baseados em topologia e posição, como é ilustrado na figura 2.5 (ZHANG; LUO; HU, 2006). Os algoritmos baseados em topologia utilizam a disposição da rede para selecionar o caminho entre os nós, já os algoritmos baseados em posição selecionam a rota com informações da posição geográfica dos nós. Ainda existem também algoritmos híbridos, que combinam as duas informações.

Algoritmos baseados em topologia podem ser divididos em dois grupos: os reativos e os proativos, que da junção desses dois origina um algoritmo híbrido. Protocolos reativos calculam uma rota apenas quando ela é necessária, o que reduz o *overhead* na rede mas introduz a latência de transmissão para o primeiro pacote transmitido. Já os algoritmos proativos, todos os nós conhecem as rotas, que são calculadas antes de uma requisição. Se por um lado não há latência, por outro, a manutenção de rotas não mais utilizadas aumenta o *overhead* de mensagens de controle na rede. Os algoritmos híbridos tentam tirar proveito das melhores característica dos dois métodos: roteamento proativo é utilizado para nós próximos e caminhos utilizados com frequência e roteamento reativo somente para nós mais distantes, pouco utilizados (ZHANG; LUO; HU, 2006).

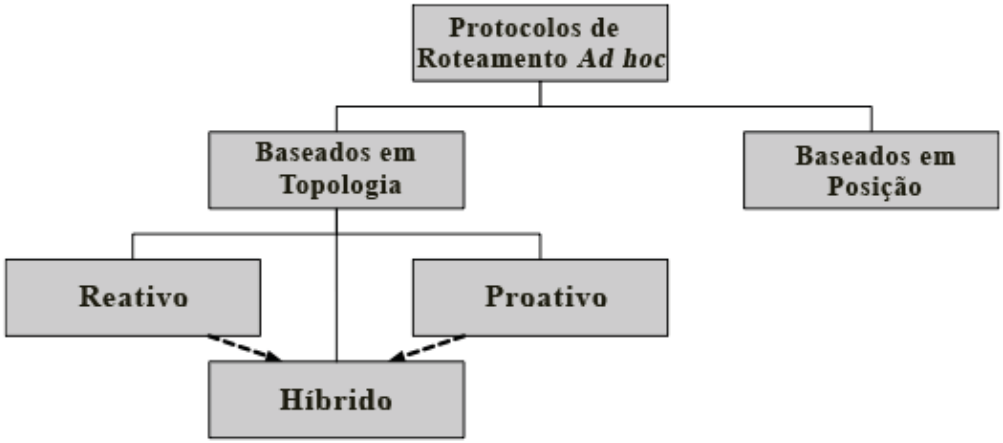

Figura 2.5 Algoritmos de roteamento em redes de múltiplos saltos (ZHANG; LUO; HU, 2006).

Ao contrário das redes convencionais cabeadas onde o roteamento é feito na camada 3 do modelo OSI e TCP/IP, existem esforços para desenvolver protocolos de roteamento para redes *ad hoc/mesh* em camada 2, camada de enlace. Os estudos que sugerem a criação de um protocolo de roteamento em camada de enlace são baseados no padrão 802.11s (HIERTZ, *et al.*, 2007), ainda em fase de padronização pelo IETF (Internet Engineering Task Force).

A alteração do roteamento para a camada de enlace trouxe alguns benefícios como maior acesso a informações de camada de enlace e física, encaminhamento mais veloz, melhorias nos métodos de acesso ao meio em comunicações de múltiplos saltos, entre outras. No entanto, há uma maior dificuldade para implementar o

roteamento em camada 2, informações como o IP não estão disponíveis e também a dificuldade de fazer com que esses *hosts* consigam acessar redes heterogêneas.

Baseado no desempenho de algoritmos de roteamento já existentes para redes *ad hoc*, um algoritmo de roteamento para redes de múltiplos saltos deve possuir as seguintes características (AKYILDIZ; WANG; WANG, 2005):

- Tolerância a falhas: esse item é importante para que a rede consiga se manter ativa em caso de um nó ou enlace falhar. Uma das principais características de redes de múltiplos saltos;
- Balanceamento de carga: habilidade de prover caminhos eficientes e alternativos para cada pacote transmitido;
- Redução da sobrecarga de roteamento: requisito importante para preservar a qualidade da banda de transmissão;
- Escalabilidade: escalabilidade é a capacidade da rede se manter funcionando mesmo com o aumento do número de nós. Essa característica é importante uma vez que a operação da rede não depende de um nó central;
- Suporte a qualidade de serviço (QoS): requisito importante devido a capacidade limitada do canal de transmissão, influência de interferência e ao crescente uso de aplicações de mídia de tempo real.

Com todas essas características, tem-se alguns protocolos de roteamento já consagrados. Exemplos deles são:

- AODV - *Ad hoc On-demand Distance Vector Routing Protocol*: protocolo muito popular no uso de MANETs. É um protocolo reativo, fazendo roteamento sob demanda e só mantêm as rotas ativas, o que reduz a sobrecarga de roteamento na rede mas aumenta a latência do primeiro pacote transmitido. É definido pelo RFC 3561 (PERKINS; BELDING-ROYER; DAS, 2003). Por ser o foco deste trabalho, será detalhado na próxima seção;
- DSR - *Dynamic Source Routing Protocol*: um dos primeiros protocolos de roteamento para MANETs. Protocolo bem conhecido por fazer roteamento reativo, ou seja, só calcula uma rota quando necessário. Definido pelo RFC 4728 (JOHNSON; HU; MALTZ, 2007);

- OLSR - *Optimized Link State Routing Protocol*: protocolo de roteamento proativo popular e utiliza o algoritmo clássico de caminho mínimo. Seu principal objetivo é otimizar o mecanismo de distribuição por *broadcast* na rede. Protocolo definido pelo RFC 3626 (CLAUSEN; JACQUET, 2003).

2.8 AODV (*Ad hoc On-demand Distance Vector Routing Protocol*)

Como mencionado antes, um protocolo de roteamento para redes do tipo *ad-hoc* tem como objetivo principal ter uma rápida e dinâmica adaptação às variações das condições dos enlaces de rede, encontrando rotas de forma eficiente visando evitar o desperdício de banda e minimizar o uso de memória e processamento nos nós que atuam como roteadores (PERKINS; BELDING-ROYER; DAS, 2003).

O AODV é um protocolo de roteamento sob demanda, o que implica em uma maior latência na transmissão de dados pois toda vez que um nó não conhece uma rota válida para um destino, é necessário realizar o procedimento de descoberta de rota. Além disso, a manutenção das rotas existentes é realizada de acordo com os eventos, ao se detectar a queda de um enlace essa informação é repassada aos demais nós (PANDEY; FUJINOKI, 2005).

A tabela de roteamento criada pelo AODV contém os seguintes itens:

- Endereço IP destino;
- Número de sequência do destino;
- Indicador de validade do número de sequência do destino;
- Indicador de validade de rota;
- Interface de rede para alcançar o destino;
- Contador de saltos indicando o número de saltos até destino;
- Próximo nó para esta rota;
- Lista de nós predecessores;
- Tempo de vida (utilizado para manutenção da rota).

Em relação ao processo de descoberta de rotas, este é realizado por um mecanismo de inundação da rede com mensagens RREQ (*Route Request*). Um nó envia uma mensagem desta para seu vizinho contendo seu número de sequência e um

identificador de *broadcast*, caso o vizinho não seja o destino ou não possua rota para o destino solicitado, ele repassa esta mensagem para seus vizinhos, até que a mensagem chegue ao destino solicitado (PERKINS; BELDING-ROYER; DAS, 2003).

Quando o destino recebe uma mensagem RREQ, primeiro é criada uma entrada para o nó anterior, caso essa não exista. Após isso, é checado se a mensagem já foi respondida, essa checagem é feita comparando o identificador de *broadcast*, caso já tenha sido respondida em um intervalo de tempo, a mensagem não será retransmitida para evitar nova inundação na rede. Após a checagem, o nó destino responde com uma mensagem RREP (*Route Reply*) através do caminho reverso que a mensagem chegou. Com isso, não só o nó que originou a mensagem, mas os intermediários também adicionam esta nova rota descoberta em suas tabelas de roteamento (PERKINS; BELDING-ROYER; DAS, 2003).

2.9 Considerações finais

Neste capítulo foram apresentadas, de forma resumida, as características de redes *wireless* 802.11 convencionais e redes de múltiplos saltos. Além disso, neste capítulo foram exploradas informações sobre o funcionamento de redes sem fio de múltiplos saltos, enumerando os tipos de roteamento possíveis de uso nesse tipo de rede. No capítulo seguinte é apresentada uma explanação sobre o desenvolvimento deste projeto, em conjunto com a pesquisa sobre ataques em redes de múltiplos saltos e mecanismos para mitigar ataques em redes sem fio de múltiplos saltos.

Capítulo 3 – Desenvolvimento

3.1 Considerações iniciais

Este capítulo aborda os problemas de segurança da informação que envolvem o transporte de informações em redes sem fio de múltiplos saltos. Aqui são abordados os principais problemas de segurança que levaram ao desenvolvimento deste trabalho. Este capítulo também contém um método que pode ser utilizado para mitigar tais ataques.

3.2 Segurança em redes sem fio de múltiplos saltos

Redes de múltiplos saltos também estão expostas a algumas ameaças básicas de redes cabeadas, tais como a interceptação, modificação, atraso e substituição de mensagens, inserção de mensagens, entre outras. Além desses ataques, ainda existem acessos não autorizados na rede e tentativas de tornar o serviço provido pela rede indisponível, um ataque conhecido como negação de serviço (DoS – *Denial of Service*).

Existem alguns requisitos e recursos definidos como pilares da segurança da informação que podem ser utilizados para defender de ataques mais comuns em redes deste tipo (GOLLMANN, 1999):

- Confidencialidade: o conteúdo da mensagem só é revelada ao seu destinatário;
- Integridade: garantir que o conteúdo da mensagem não foi alterado no transporte até seu destino;
- Autenticação: identificar de fato um emissor como sendo ele mesmo;
- Controle de acesso: assegurar que somente ações autorizadas podem ser executadas;
- Não-repúdio: garantir que um emissor não poderá negar a existência de uma comunicação, ou a emissão de uma mensagem;
- Disponibilidade: assegurar que ações autorizadas sejam executadas.

A proteção da comunicação na maior parte dos casos que envolve confidencialidade, autenticação e integridade de mensagens é feita por meio do uso de criptografia. Isso pode ser feito em diferentes camadas, como enlace, rede, transporte ou ainda na camada de aplicação.

Em redes *wireless* locais existem dois modos de segurança: um com uma chave de acesso pré-definida (*preshared key*) onde todo *host* é configurado com a mesma chave de acesso, muito utilizado em residências e pequenos escritórios, e o outro método é autenticar os usuários e dispositivos utilizando um servidor de autenticação AAA (Autenticação, Autorização e *Accounting* – Contabilidade) (GLASS; PORTMANN; MUTHUKKUMARASAMY, 2008).

Apesar da existência de mecanismos de segurança como os citados acima, ainda existem diversas formas de comprometer uma rede sem fio (GLASS; PORTMANN; MUTHUKKUMARASAMY, 2008). Na figura 3.1 pode-se ver um exemplo de quais ataques podem ser lançados contra cada camada do modelo TCP/IP.

Em redes de múltiplos saltos ainda existe um ataque plausível de acontecer que é um *host* comprometido. Como a comunicação é feita em múltiplos saltos, cada *host* pode encaminhar ou não um pacote, ocasionando um ataque de negação de serviço.

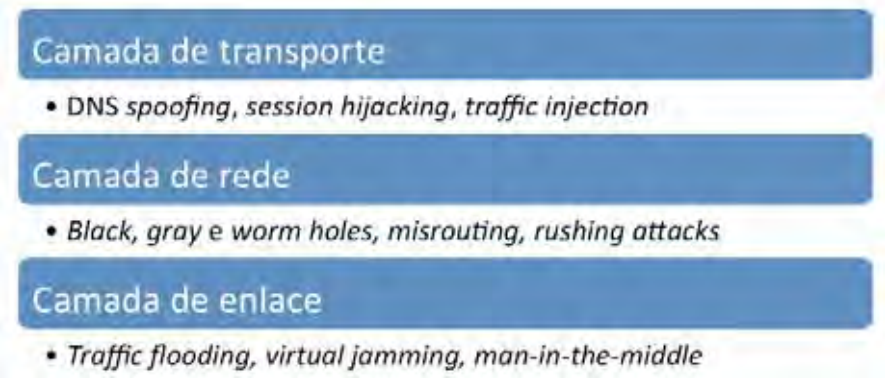

Figura 3.1 Ataques passíveis em redes *wireless* de múltiplos saltos (GLASS; PORTMANN; MUTHUKKUMARASAMY, 2008).

Outra situação plausível de ocorrer é um ataque *man-in-the-middle*, onde uma estação intercepta tráfego de duas outras e com isso consegue acesso aos dados trafegados, podendo inclusive inserir novos dados falsos, alterar dados originais e inclusive não repassar seletivamente algum pacote. Como os ataques destinados a camada de transporte e enlace não são o objetivo deste trabalho, não serão expostos aqui, sendo que é possível encontrar maiores informações sobre esses ataques em (GOLLMANN, 1999).

Outros ataques realizados devido a natureza de múltiplos saltos são os ataques *black hole*, *gray hole* e *worm holes* (GLASS; PORTMANN; MUTHUKKUMARASAMY, 2008). Em cada um deles, um *host* anuncia a sua entrada na rede para participar do roteamento, e escolhe a ação a ser tomada. No *black hole*, a estação anuncia suas rotas mas não repassa nenhum pacote. Já o *gray hole* tem uma operação semelhante ao *black hole*, porém, é seletivo em quais pacotes irá repassar ou não, o que o torna mais difícil de ser detectado. Uma característica comum aos dois ataques é a necessidade de atraírem tráfego para si mesmo, causando maior dano na rede atingida, e para auxiliar nisso podem usar uma técnica conhecida como *rushing attack* para subverter o algoritmo de roteamento, aumentando a probabilidade de ser incluso em uma rota.

Já o *worm hole* é um ataque que pode causar danos severos a rede. É considerado um ataque quando dois nós maliciosos se unem para configurar o *worm hole*, ou túnel (GLASS; PORTMANN; MUTHUKKUMARASAMY, 2008). Quando um dos atacantes recebe um pacote, ele envia este pacote para a outra ponta do túnel. Com o ataque muitos pacotes que deveriam ter outro nó como destino são atraídos

pelos nós atacantes para serem redirecionados através do *worm hole*. Observe a figura 3.2 para entender como o ataque funciona.

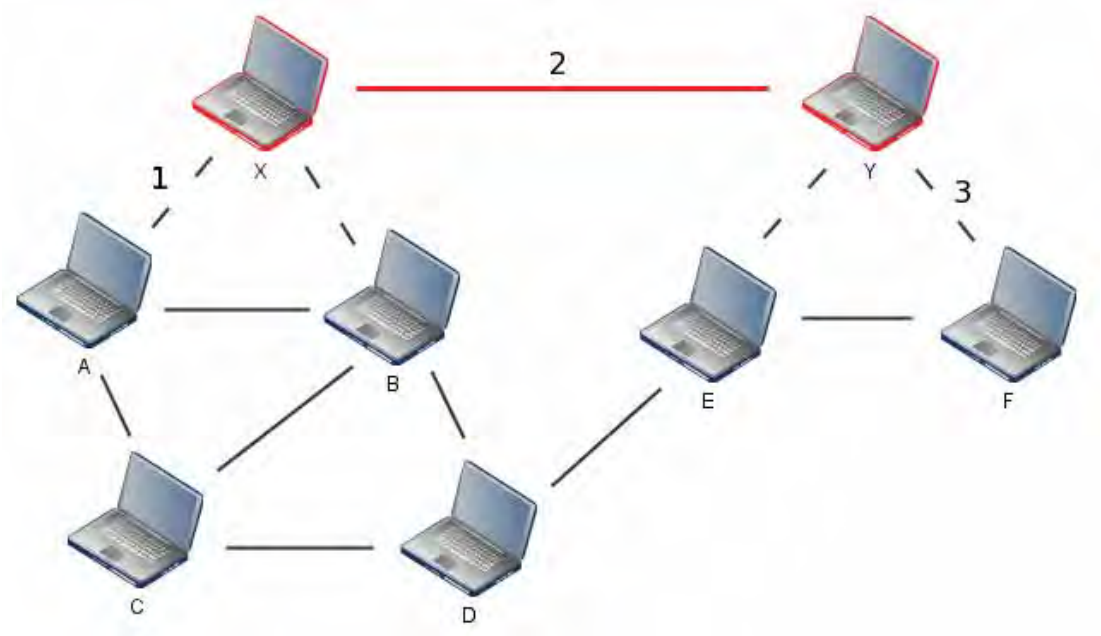

Figura 3.2 Ataque *worm hole*.

Com esse ataque, o atacante não necessita ter posse de uma estação legítima, mas significa uma ameaça a rede. O atacante faz um túnel conectando diferentes partes da rede, enganando estações que irão acreditar que os *hosts* do outro lado da rede são seus vizinhos. Em uma primeira análise isso pode parecer um ato benéfico, pois otimiza o fluxo de tráfego através da rede. No entanto, esse ato permite ao atacante obter as informações trafegadas no *worm hole* e lançar um ataque de negação de serviço, isolando a rede.

Na figura 3.2 tem-se o *host* X e Y fazendo parte da criação do túnel, e a estação A, utilizando o caminho através de 1, agora pensa que E e F são seus vizinhos diretos, o mesmo acontece com B, E e F. Os *hosts* X e Y não participam como *hosts* ativos, apenas na criação de um canal de comunicação que aproxime os dois grupos.

O ataque é possível de ser realizado pois a maior parte dos protocolos de roteamento para redes de múltiplos saltos tem como prioridade o caminho mais eficiente, e a métrica utilizada nestes protocolos é a contagem de saltos. Com isso, os dóis nós criam um canal de comunicação entre eles e, mesmo não sendo adjacentes, eles se anunciam como se fossem vizinhos um ao outro, introduzindo a melhor rota

para os nós ao alcance do rádio dos atacantes. Esse canal de comunicação pode ser criado de duas maneiras:

- Túnel: o ataque utiliza a própria infraestrutura da rede para criar o túnel entre os dois nós. O nó que recebe as informações encapsula os pacotes de requisição de rota e os envia para a outra ponta, onde o segundo nó atacante irá propagar essas informações após remover o encapsulamento criado. Mesmo que os nós atacantes não estejam próximos, os nós ao alcance dos atacantes irão acreditar que não existe nenhum nó no caminho entre os dois atacantes;
- Enlace dedicado: para criar o túnel, os dois nós atacantes fazem uso de um enlace dedicado conectando os dois, podendo ser uma rede cabeada ou um rádio de longo alcance.

Um outro ataque que é foco principal deste trabalho é chamado *selfish* (egoísmo), também conhecido em algumas literaturas por *black hole*. O ataque envolve uma forma que os nós utilizam para conservar seus recursos, uma vez que em redes móveis tais como MANETs, esses nós possuem energia e poder computacional limitado (GLASS; PORTMANN; MUTHUKKUMARASAMY, 2008). O ataque consiste em não participar do processo de roteamento, ou seja, não redirecionar nenhuma mensagem entregue ao nó atacante. Na figura 3.3 é possível observar o cenário para este tipo de ataque.

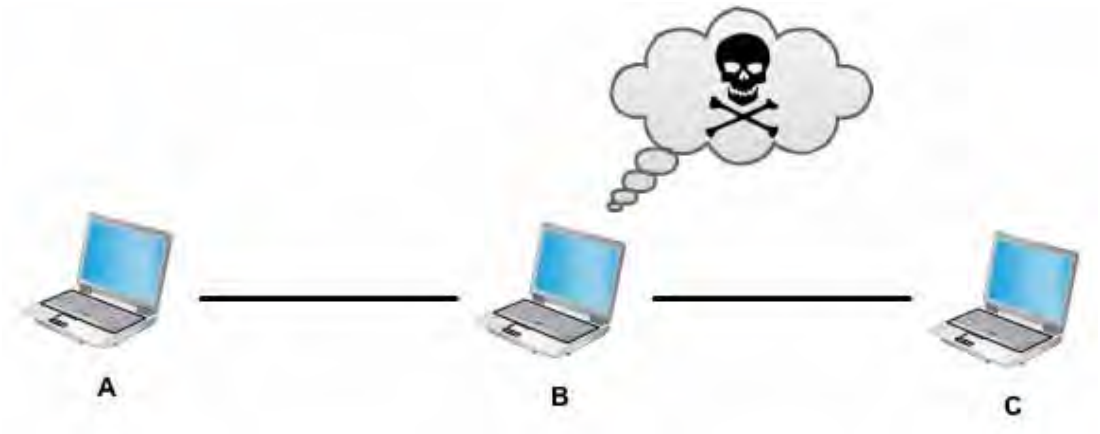

Figura 3.3 Cenário do ataque *selfish*.

O cenário ilustrado pela figura 3.3 é composto de 3 computadores, conectados por meio de enlaces sem fio e utilizando um protocolo de roteamento para redes de múltiplos saltos. Na figura, o nó A está enviando informações para o nó

C. Por estar fora do alcance de seu rádio, as informações são repassadas pelo nó B. Isso representa o comportamento normal da rede. Em um cenário de ataque, o nó B pode descartar, de forma parcial ou total, os pacotes de informação que são repassados a ele com destino a outro nó.

Isso introduz um ataque de negação de serviço na rede, causando perda de dados, redução na vazão de dados (*throughput*), e no pior caso, a decomposição da rede caso o nó atacante seja vital para manter a rede conectada. Um fato importante a ser notado é que este ataque comumente não é executado com a intenção de causar danos à rede, e sim realizado para poupar recursos do nó.

3.3 Detecção de ataques

Em uma rede de múltiplos saltos, todos os nós possuem o mesmo tratamento, ou seja, não existe prioridade sobre nenhum nó. Baseado nisso, detectar e mitigar ataques nestas redes pode ser uma tarefa complexa.

De modo geral, são propostos dois mecanismos para controlar redes de múltiplos saltos:

- Mecanismos baseados em reputação: o método baseia-se na reputação de um determinado nó. Ações como redirecionar um pacote de dados ou controle aumenta a reputação do nó;
- Mecanismos baseados em crédito: métodos deste tipo implementam uma espécie de moeda virtual. Neste caso, para um nó utilizar a rede, enviando um pacote de dados por um determinado grupo de nós, o remetente tem que ter o crédito necessário para realizar a operação (ZHOU, *et al.,* 2009).

Como o foco deste trabalho é mitigar os ataques do tipo *selfish*, foi desenvolvida uma modificação do protocolo de roteamento AODV com o intuito de criar um novo protocolo para ser utilizado em redes sem fio de múltiplos saltos. O novo protocolo, batizado de *ACME! Selfishness Routing System* (ASeR).

Para desenvolvimento deste trabalho, foi desenvolvido um método para mitigar os ataques do tipo *selfish*, baseado em métodos cooperativos com análise de reputação dos nós integrantes do processo de encaminhamento de informações.

3.4 Detecção para *selfish* (egoísmo)

Para realizar a tarefa de identificar e mitigar os danos causados por um nó que está utilizando esta técnica, é proposto um método baseado na reputação dos nós. O método faz detecção pro-ativa, isto é, a checagem da reputação do nó é feita antes de ser tomada uma ação, tal como repassar um pacote de informações ou mensagens de controle.

O mecanismo utiliza métricas locais, armazenadas em cada nó, e coletadas a partir da observação dos vizinhos. Todas as informações coletadas são armazenadas em uma tabela para contabilizar os atos de cooperação dos nós. Por se tratar apenas de um método para detecção de comportamento anômalo, este é inserido como parte do protocolo de roteamento AODV, modificando algumas de suas funções para que o mecanismo possa funcionar de forma adequada.

O funcionamento básico do mecanismo é descrito a seguir:

- É criada uma tabela para armazenar o comportamento dos vizinhos. Nesta tabela são armazenadas as operações que foram realizadas em forma de recompensas em reputação;
- De forma geral, um pacote só é repassado se a reputação do nó anterior não for nula, seja o pacote de dados ou controle cujo emissor é o próprio nó;
- As recompensas por reputação são definidas de acordo com o tipo de pacote: pacotes de controle ou dados;
- Para detectar e atribuir a recompensa por boa reputação, a cada pacote transmitido, a origem o armazena em um *buffer* e espera até que seu vizinho o transmita. Como o meio é compartilhado, a transmissão do vizinho será percebida pela origem, garantindo o aumento do seu nível de cooperação. Caso o nó vizinho não retransmita a informação em determinado tempo (estipulado no *buffer*), sua reputação será zero, identificando um ato de mau-comportamento;
- Caso a reputação do nó seja nula, ele não conseguirá enviar informações. Para resolver este problema, uma vez que o nó não tenha reputação, seu vizinho irá lhe conceder uma reputação temporária, apenas para que ele inicie a transmissão, no entanto, essa concessão é

limitada, podendo ser utilizada apenas algumas vezes em um intervalo de tempo determinado;

Dessa forma, foi desenvolvido um novo protocolo que é composto por alterações no protocolo AODV, criando o *ACME! Selfishness Routing System* (ASeR). O funcionamento básico é composto de 3 etapas, conforme ilustra a figura 3.3.

Figura 3.4 Funcionamento do ASeR.

Como é possível observar na figura 3.3, o funcionamento básico do ASeR consiste em três algoritmos, aplicados em três etapas: recebimento de informações, envio de informações e monitoramento da rede. Os três algoritmos são descritos nas figuras 3.4, 3.5 e 3.6.

Algoritmo 1: *Recebimento de dados*
Checar origem dos dados:
Nó atual é o destino da informação
Conceder valor de cooperação positiva para o nó anterior
Origem é o nó imediatamente anterior e também emissor da mensagem
Checar cooperação:
Cooperação > 0: encaminhar dados para o próximo destino
Cooperação = 0: conceder cooperação temporária e encaminhar
Cooperação = -1: nó realizou algum ataque, não encaminhar
Origem não é o nó anterior (o nó apenas está repassando a mensagem)
Conceder valor de cooperação positiva para o nó anterior e encaminhar

Figura 3.5 Algoritmo 1: Recebimento de informações.

Algoritmo 2*: Envio de informações*

Obter endereço do próximo salto (hop)

Checar cooperação do próximo salto e lista de pacotes não-enviados:

Cooperação != -1 && menos de 10 pacotes não enviados:

Encaminhar o pacote

Inserir pacote na lista de enviados

Cooperação = -1:

Desativar a rota

Iniciar processo de descoberta de nova rota (indica um nó atacante)

Figura 3.6 Algoritmo 2: Envio de informações.

Algoritmo 3*: Monitoramento de pacotes enviados*

Ativar interface de rede em modo promíscuo

Receber pacote

Verificar destino das informações

Se destino é o próprio nó: fazer nada

Se o destino é outro nó e a origem é o próprio nó

Procurar o pacote enviado na lista de enviados

Se o pacote for encontrado na lista

Remover pacote da lista de enviados

Conceder cooperação positiva para o nó que enviou

Figura 3.7 Algoritmo 3: Monitoramento de pacotes enviados.

Com todas as propriedades definidas anteriormente, é criado um método para determinar e punir nós que efetuarem ataques do tipo *selfish*. É importante ressaltar que esse tipo de ataque pode ser feito de duas maneiras:

- Tipo I: O nó que realiza o ataque responde aos pacotes de controle e os repassa, como uma situação normal, no entanto, os pacotes de dados não são repassados aos vizinhos, exceto os criados pelo próprio nó;

- Tipo II: O nó ao receber pacotes de controle não os responde, fingindo estar desligado ou invisível à rede. Os pacotes de dados, assim como o tipo anterior, também não são redirecionados aos vizinhos.

O método proposto visa dar tratamento aos dois tipos de ataques, embora o ataque tipo II seja menos destrutivo à rede pois o nó atacante não responde às mensagens de controle, portanto não faz parte de nenhuma rota para outros destinos da rede.

Um problema encontrado durante o desenvolvimento do método é como dar oportunidade de ingresso à rede para os nós que são localizados nas bordas na topologia. Estes nós só possuem um nó como vizinho, por esse motivo não fazem repasse de informação de nenhum vizinho, apenas solicita informação para ele mesmo. Na tentativa de enviar um pacote, o nó vizinho irá limitá-lo pois ele não possui cooperação positiva, embora possa lhe dar uma cooperação temporária, ainda obteria uma baixa vazão de dados.

Na tentativa de solucionar o problema do nó localizado na borda, é proposto utilizar um campo reservado na mensagem RREQ, do protocolo AODV, para informar a situação do nó. O formato da mensagem pode ser visto na figura 3.3.

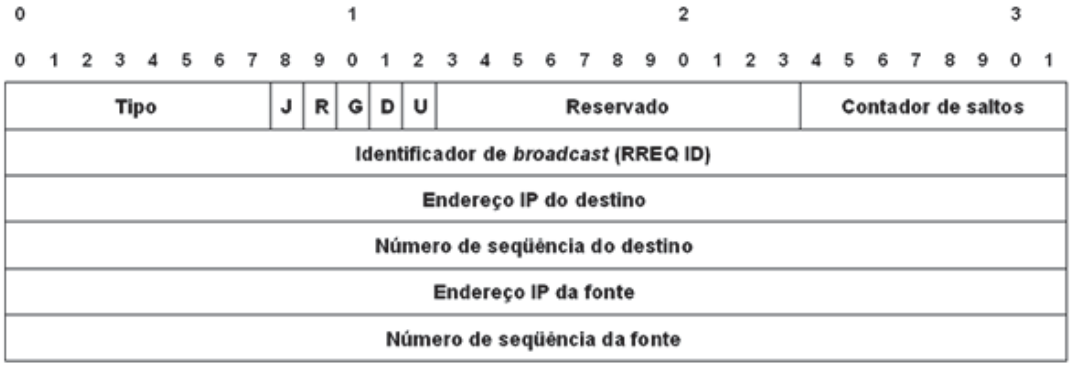

Figura 3.8 Formato da mensagem RREQ.

Na figura 3.8 é possível observar o campo “Reservado” contendo 11 bits de informação. De acordo com o RFC 3561 (PERKINS; BELDING-ROYER; DAS, 2003), o campo é marcado para uso futuro, em toda implementação do protocolo o campo deve ser preenchido com zeros.

Como parte da solução, utilizar um bit do campo reservado faz com que o nó na borda avise seu vizinho de sua situação. Para que o vizinho possa confirmar a

veracidade da informação, o vizinho envia um RREQ com o endereço IP de destino do nó. Caso nenhum outro nó responda sua requisição, isto é, nenhum outro nó possui rota para seu vizinho, então é concedida a condição de nó em borda para o vizinho, permitindo que envie uma maior quantidade de dados sem limitação.

Caso um nó constate que seu vizinho está se comportando de maneira incorreta, aplicando o ataque em questão, a cooperação do vizinho será anulada. Além disso, caso alguma rota contenha o vizinho, a nota será descartada em busca de outra que não possua o nó malicioso.

3.5 Trabalhos relacionados

Motivado pelos problemas de segurança encontrados nos protocolos de comunicação de rede sem fio de múltiplos saltos, o IEEE criou uma força tarefa para desenvolver um novo protocolo, que tenha foco em segurança, para trafegar informações em redes *wireless mesh*. O protocolo ainda está em fase de *draft*, é chamado 802.11s (HIERTZ, *et al.*, 2007).

O padrão 802.11s é um padrão emergente para comunicação em redes sem fio de múltiplos saltos, utilizando a camada de enlace para fazer suas operações. O maior benefício da proposta é que o novo padrão é baseado na extensão dos padrões atuais de redes sem fio, ou seja, o *hardware* utilizado hoje será utilizado com este novo padrão.

Diferente das redes convencionais, o padrão IEEE 802.11s (SAADE; et al., 2008) é inovador pois faz o encaminhamento de pacotes através de múltiplos saltos em nível de camada de enlace, isso tem suas vantagens e desvantagens perante os padrões convencionais para redes sem fio, tais como o IEEE 802.11b e 802.11g.

A escolha da comunicação em nível de enlace deve-se a limitações de recursos de dispositivos sem fio portáteis, como por exemplo alimentação elétrica, processamento e memória. Pensando nisso, o grupo de trabalho do 802.11s propõe que ele seja implementado em camada de enlace para ser leve, em contraste com as implementações tradicionais de roteamento em nível de rede.

A comunicação em enlaces de múltiplos saltos tem um grande benefício que é a adaptabilidade da rede diante situações de falha, de enlace ou equipamento.

Alguns fabricantes utilizam diversas tecnologias para realizar a comunicação entre os roteadores sem fio, tais como o 802.11a, que opera em 5GHz, evitando a poluição de espectro encontrada nas faixas de 2.4GHz devido a grande popularização de equipamentos que utilizam este espectro. Na comunicação com os usuários pode ser utilizada ainda outra tecnologia, como 802.11b ou 802.11g, um padrão já consagrado no mercado e presente na maioria dos dispositivos de comunicação móvel.

Além da iniciativa do IEEE, diversos outros trabalhos na literatura propõe métodos isolados para fazer detecção e mitigar ataques mencionados. Em (LIU; *et al.*, 2009) os autores propõem um método baseado em somas cumulativas para detecção de *selfish*. O trabalho propõe utilizar o método matemático de somas cumulativas para analisar séries temporais homogêneas de eventos de *backoff* em redes sem fio.

Já o trabalho de (WANG; WONG, 2007) tem como objetivo a detecção de ataques *wormhole* em redes ad-hoc. O trabalho apresenta duas abordagens complementares. Em uma primeira instância, o nó compara a contagem de saltos para diferentes rotas para o mesmo destino. Caso haja alguma disparidade, então o método proposto utiliza cálculos matemáticos derivados da distância euclidiana para determinar a existência ou não do ataque.

3.6 Considerações finais

Neste capítulo foram abordados os problemas de segurança da informação que podem impactar sobre o funcionamento de redes sem fio de múltiplos saltos. Foram exibidos alguns ataques passíveis de serem utilizados nessas redes e com atenção especial ao ataque *selfish* ou egoísmo.

O objetivo principal deste capítulo foi apresentar os problemas e uma solução para o ataque mencionado, o método desenvolvido utiliza uma técnica baseada em cooperação entre os nós da rede, onde cada nó que deseja enviar uma mensagem para outro deve cooperar com o restante da rede, também repassando as mensagens de seus vizinhos.

Capítulo 4 – Testes e resultados

4.1 Considerações iniciais

Este capítulo é dedicado aos testes realizados envolvendo o ataque *selfish* em redes de múltiplos saltos. O capítulo aborda o desenvolvimento do mecanismo apresentado para mitigar este ataque, desenvolvimento realizado em um ambiente simulado pela aplicação GloMoSim (GloMoSim, 2011). Após os testes é realizada uma análise dos resultados obtidos.

4.2 Implantação do método

Para testes do método proposto foi utilizado um ambiente de simulação pois é possível obter melhor infraestrutura para testes, sem a necessidade de criar diversos computadores para atuarem como nós. Além disso, um simulador já possui todas as rotinas para testes de topologias e protocolos.

O simulador escolhido para tal é o GloMoSim (GloMoSim, 2011), um simulador completo para ambientes de redes *wireless* e cabeadas. Sua implementação utiliza simulação paralela de eventos discretos (em apenas um

computador) utilizando a linguagem Parsec (Parsec, 2011), uma linguagem de simulação baseada na linguagem C. A escolha do simulador foi baseada em dois trabalhos, (FUJINOKI; PANDEY, 2005) que faz um estudo dos protocolos de roteamento em MANETs utilizando o próprio GloMoSim e (HOGIE; BOUVRY; GUINAND, 2006) que faz uma comparação entre diversos simuladores e mostra quais os mais adequados para as situações. A escolha do ambiente de simulação deve-se ao fato dele ser implementado utilizando a abordagem de camadas, similar ao modelo OSI de camadas para redes de computadores, com isso, a implementação e modificação de um novo mecanismo de redes torna-se menos custosa.

Para a implantação foram inseridas as algumas modificações no protocolo AODV implementado pelo simulador, dentre elas, abaixo são citadas as principais:

- Criação da tabela para armazenar a cooperação dos nós: foi feita utilizando a tabela de vizinhos já em uso pelo simulador, apenas adicionando novos campos para armazenar a cooperação do nó e o horário em que a cooperação foi concedida;
- Criação de uma lista encadeada para armazenar os pacotes enviados: assim como outras funcionalidades do simulador, esta também utiliza uma lista encadeada para armazenar o destino do pacote e o horário que foi enviado. Também foram criadas funções para inserção e remoção de elementos desta lista;
- Modificação da função de envio de dados da camada de rede: para armazenar os dados enviados com o objetivo de checar se os vizinhos irão repassar os dados, importante para conceder cooperação por pacote repassado;
- Criação de uma função para capturar dados em modo promíscuo: em virtude do ambiente ser um meio compartilhado, é possível obter os dados enviados pelos nós vizinhos, confirmando ou não o envio de um pacote originado pelo nó em modo promíscuo;
- Mudanças no processo de escolha de melhor rota: caso a melhor rota possua um nó cuja cooperação é zero, esta rota será descartada.

As configurações de protocolos e definições do simulador utilizadas nos testes seguem abaixo:

- Limite de propagação de sinal: -90 dBm. Qualquer sinal com potência inferior a este valor não será entregue;
- Perda de sinal de propagação: modelo *two-ray*;
- Largura de banda de cada rádio: 2000000 bits/segundo;
- Potência de envio de sinal: 5dBm;
- Potência mínima para recebimento de um sinal: -81 dBm;
- Protocolo de camada de enlace: 802.11;

Para efetuar os testes, um primeiro experimento foi feito para criar o ambiente de simulação que foi utilizado. Este experimento tem como objetivo criar a topologia que será utilizada nos experimentos iniciais. A topologia dos testes apresentados possui 6 nós, inicialmente posicionados de forma aleatória em um espaço de 800 metros de largura e comprimento. Após isso, foi coletada a posição dos nós e criado um arquivo de configuração dos nós para que sempre estejam nesta mesma posição.

Todos os testes iniciais efetuados consistem em 5 minutos de simulação, lembrando que este tempo é simulado, não representa o tempo que o simulador levou para completar o teste. Para simular a transmissão de dados foi utilizado um gerador de dados com taxa constante de envio de pacotes por unidade de tempo, método proveniente do próprio simulador.

A figura 4.1 exibe a posição dos nós para todos os cenários de testes iniciais. A figura foi extraída de uma aplicação Java distribuída em conjunto com o simulador para auxiliar a análise visual da simulação.

Na figura 4.1 é representada a posição dos nós e cada círculo, cujo nó representa o centro, corresponde ao alcance do rádio do nó. Na figura 4.1 é possível observar que o nó 1 possui perfeito alcance aos nós 0 e 2, e na fronteira de seu alcance aos nós 3 e 4, porém, devido aos fatores de degradação de sinal embutidos no simulador, a comunicação direta com os nós 3 e 4 não é utilizada. Já os nós 3 e 4 possuem alcance aos nós 0, 2 e 5. Para os testes efetuados, foi gerado uma taxa constante de tráfego entre os nós 1 e 5.

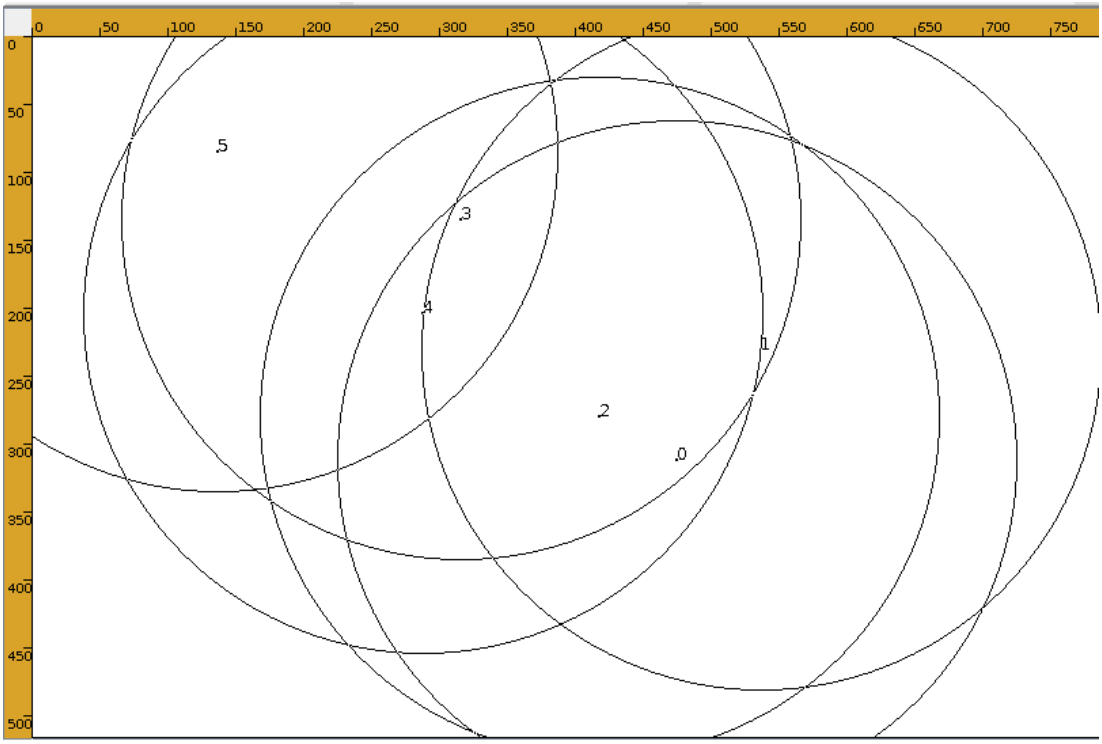

Figura 4.1 Posição dos nós no cenário de teste.

Foram executadas ao todo 3 simulações, que serão descritas nas subseções a seguir.

4.3 Simulação: Cenário I

Este primeiro cenário de teste tem como objetivo mostrar como é o desempenho da rede sem nenhum nó malicioso. A simulação tem duração de 5 minutos, sendo que desde o início da simulação o nó 1 começa o envio de dados ao nó 5. Os dados coletados da simulação são exibidos na tabela 4.1.

Tabela 4.1 Dados obtidos com o Cenário I.

Evento	**Nó 1**	**Nó 2**	**Nó 3**	**Nó 4**	**Nó 5**
Pacotes enviados	300	-	-	-	-
Pacotes recebidos	-	-	-	-	300
Pacotes roteados	-	300	-	300	-
Pacotes de controle	2	2	1	2	1

4.4 Simulação: Cenário II

Este segundo cenário tem como objetivo introduzir o ataque à rede. Seguindo os mesmos parâmetros utilizados no primeiro cenário, o nó 4 irá realizar o ataque *selfish* a partir de 60 segundos de simulação. Os dados obtidos do cenário podem ser visualizados na tabela 4.2.

Tabela 4.2 Dados obtidos com o Cenário II.

Evento	**Nó 1**	**Nó 2**	**Nó 3**	**Nó 4**	**Nó 5**
Pacotes enviados	300	-	-	-	-
Pacotes recebidos	-	-	-	-	60
Pacotes roteados	-	300	-	60	-
Pacotes de controle	2	2	1	2	1

4.5 Simulação: Cenário III

Após os dois cenários anteriores, este último cenário apresenta como é o comportamento da rede com a solução proposta em funcionamento. Os parâmetros para simulação são os mesmos utilizados nos cenários anteriores, com o nó 4 iniciando o ataque aos 60 segundos de simulação.

Tabela 4.3 Dados obtidos com o Cenário III.

Evento	**Nó 1**	**Nó 2**	**Nó 3**	**Nó 4**	**Nó 5**
Pacotes enviados	300	-	-	-	-
Pacotes recebidos	-	-	-	-	289
Pacotes roteados	-	300	229	60	-
Pacotes de controle	2	4	3	2	1

4.6 Comentários sobre os resultados iniciais

No primeiro cenário de testes é possível notar que a taxa de emissão de pacotes é de um a cada segundo, e que nenhum nó teve qualquer tipo de perda de pacotes. A configuração da camada de enlace do ambiente não foi considerada para perda de pacotes pois o intuito deste experimento é comparar o desempenho da rede em condições ideais e em condições de ataque.

No segundo cenário foi inserido o nó atacante na simulação do ambiente. Conforme é possível notar pela disposição dos nós no ambiente, a sequência percorrida dos pacotes originados no nó 1 é a seguinte: 1, 2, 4 e 5. Neste cenário, a partir dos 60 segundos o nó 4 iniciou seu ataque, seja por motivos de economia de recursos ou fins maliciosos. É possível observar que com o protocolo de roteamento padrão o ataque foi efetivo, impedindo que o tráfego de informações originadas no nó 1 fossem entregues ao nó 5. Devido à natureza do protocolo, cada nó tem um papel muito importante no funcionamento da rede, o mau comportamento do nó levou ao colapso da rede.

No terceiro cenário foi utilizado o método proposto, é importante notar que mesmo com o ataque em andamento, o nó 3 pode substituir o nó 4 para repassar as informações ao nó 5, o que não aconteceu no cenário II.

Com o método em funcionamento, foi utilizado para essa simulação um tempo de 10 segundos para que o próximo nó reencaminhe os pacotes. Ao início dos 60 segundos o nó 4 inicia seu ataque, neste momento o nó 2 envia o primeiro pacote que será perdido. Como o tempo de expiração é de 10 segundos, são perdidos dez pacotes até que o nó 2 perceba que seu vizinho está se comportando de maneira inadequada. Neste instante a cooperação do nó 4 é zerada e o nó 2 inicia o processo de roteamento para conseguir uma nova rota. Após a descoberta da nova rota por meio do nó 3 a comunicação é restaurada.

É importante frisar que além do tempo de expiração para o nó vizinho enviar os pacotes, o método também possui uma limitação ao conceder cooperação para um nó vizinho que está com sua cooperação zerada, como é o caso do nó 1. Ao início da simulação nenhum nó havia transmitido nenhuma mensagem, então todos os nós

iniciam o tráfego de informações concedendo ao seu vizinho um valor de cooperação temporária.

4.7 Simulação: Cenário IV

Após os testes iniciais, um novo cenário de simulação foi montado e será utilizado para os próximos testes. O cenário atual possui uma área de simulação para posicionamento dos nós de largura 1 quilômetro e altura 1 quilômetro. Neste cenário o tempo de simulação foi configurado para 1 hora, e a quantidade de nós também aumentou. Foram utilizados 100 nós durante a simulação, todos dispostos de maneira aleatória no espaço de simulação.

Para a simulação de troca de informações foram utilizados 5 servidores HTTP/WEB, posicionados de forma aleatória no ambiente. Além destes, 10 clientes que irão acessar 3 destes servidores de forma aleatória durante o período da simulação. Além desses recursos, um recurso adicional foi utilizado para testar o método proposto. Foi adicionado mais um servidor HTTP/WEB em um ponto distante de outro nó considerado seu único cliente. Dessa forma, o primeiro grupo descrito servirá de tráfego para movimentar a rede, e o segundo será o tráfego que será analisado para detecção de ataques.

Para que a comunicação ocorra entre os dois nós analisados são necessários 7 saltos (*hops*) para que o nó de origem chegue até o destino. Ao longo desse caminho estão dispostos no total 18 nós, incluindo a origem e destino. Todos os nós que estão na posição intermediária entre origem e destino podem atuar como roteadores e com possibilidades de caminhos redundantes.

Em todas as simulações deste cenário os nós observados serão:

- Nó 9: origem da informação, solicita acesso à páginas HTTP no servidor hospedado no nó 5;
- Nó 5: destino da informação, servidor HTTP/WEB, atende às requisições de páginas endereçadas a este servidor.

Todos os ataques aplicados nesta seção tem como início e término aleatórios, sendo que todos os nós que executarem os ataques o fazem em 2/3 do tempo contínuo de simulação, ou seja, todas as simulações realizadas tem duração de uma

hora, os nós atacantes atacam 40 minutos durante o tempo de simulação. O cenário utilizado nestes testes pode ser visualizado na figura 4.2.

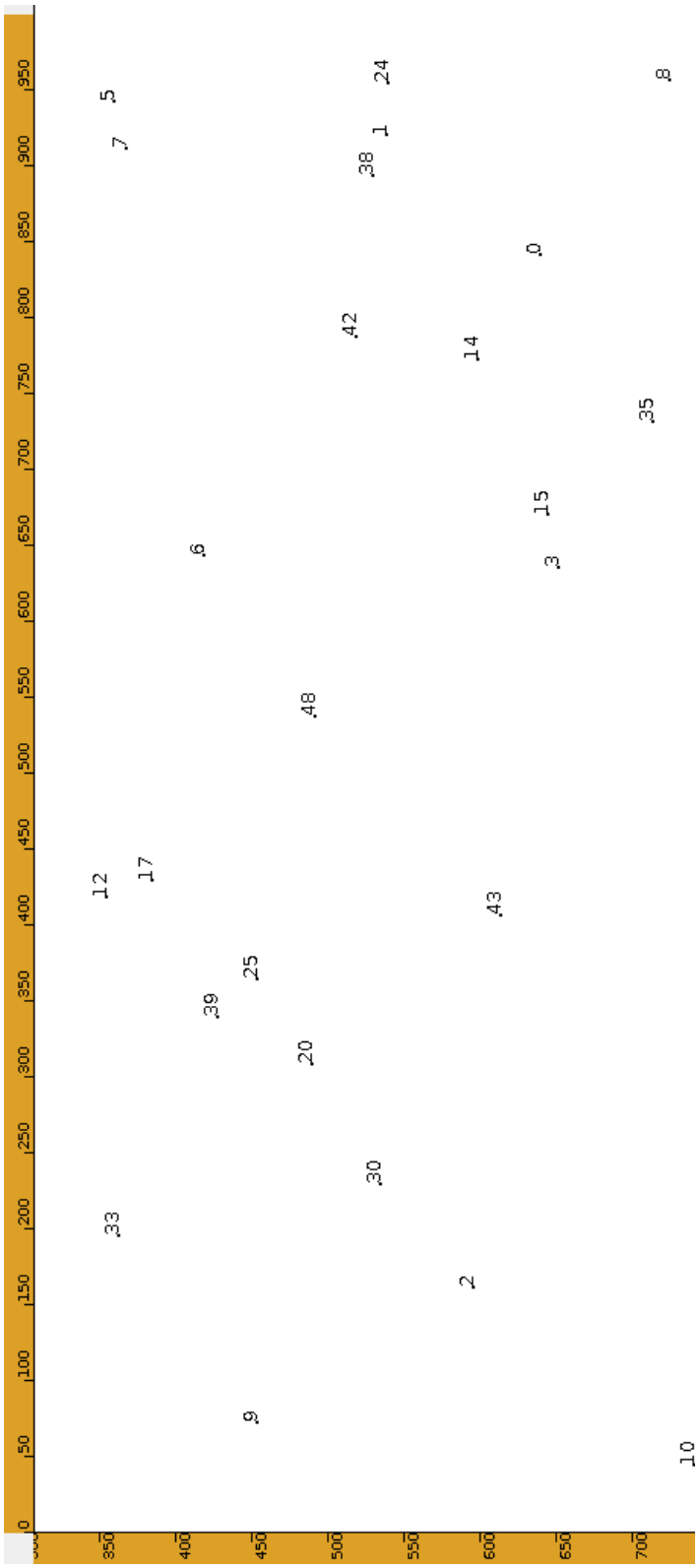

Figura 4.2 Posição dos nós no cenário IV de testes.

4.8 Cenário IV: Simulação 1

Neste primeiro teste será feito o controle da rede, uma simulação sem nenhum nó atacante para que se possa obter dados sobre a quantidade de pacotes trafegada entre origem e destino. Na tabela 4.4 é possível observar os dados resultantes da simulação.

Tabela 4.4 Dados obtidos com o Cenário IV – Nenhum nó atacante.

Evento	**Nó 9**	**Nó 5**
AODV/Enviados	4560	6510
AODV/Recebidos	6342	4380
IP/Enviados	5088	6834
IP/Recebidos	6342	4380
TCP/Enviados	372	6228
TCP/Recebidos	6060	318

Após a obtenção dos dados de controle, é possível aplicar um ataque para comparar o funcionamento do protocolo. Foi escolhido um nó aleatório dentre os 18 que compõe o caminho e efetuada a simulação, os dados podem ser visualizados na tabela 4.5.

Tabela 4.5 Dados obtidos com o Cenário IV – Um nó atacante.

	Controle AODV		**AODV Ataque**				**AODV Modificado**	
Evento	**Nó 9**	**Nó 5**	**Nó 9**	**% relativa**	**Nó 5**	**% relativa**	**Nó 9**	**Nó 5**
AODV/Enviados	4560	6510	2358	65.13	3192	73.14	3620	4364
AODV/Recebidos	6342	4380	2940	69.07	2148	63.89	4256	3362
IP/Enviados	5088	6834	2838	68.22	3420	75.76	4160	4514
IP/Recebidos	6342	4380	2940	69.07	2148	63.89	4256	3362
TCP/Enviados	372	6228	540	46.07	3030	76.59	1172	3956
TCP/Recebidos	6060	318	2778	76.10	402	40.28	3650	998

4.9 Cenário IV: Simulação 2

Neste segundo teste de simulação, todos os parâmetros anteriores foram mantidos, com exceção da quantidade de nós atacantes, desta vez serão 3 nós atacantes. A tabela 4.6 exibe os resultados obtidos.

Tabela 4.6 Dados obtidos com o Cenário IV – Três nós atacantes.

	Controle AODV		**AODV Ataque**				**AODV Modificado**	
Evento	**Nó 9**	**Nó 5**	**Nó 9**	**% relativa**	**Nó 5**	**% relativa**	**Nó 9**	**Nó 5**
AODV/Enviados	4560	6510	978	44.25	1404	48.81	2210	2876
AODV/Recebidos	6342	4380	1194	45.09	846	40.83	2648	2072
IP/Enviados	5088	6834	1278	53.47	1716	53.32	2390	3218
IP/Recebidos	6342	4380	1194	45.09	846	40.83	2648	2072
TCP/Enviados	372	6228	318	38.03	1242	50.08	836	2480
TCP/Recebidos	6060	318	1032	45.70	222	31.26	2258	710

4.10 Cenário IV: Simulação 3

No terceiro teste de simulação, assim como os outros testes, mais nós serão adicionados ao grupo de atacantes. Desta vez serão cinco nós que irão realizar os ataques. Os resultados obtidos com a simulação podem ser visualizados na tabela 4.7.

Tabela 4.7 Dados obtidos com o Cenário IV – Cinco nós atacantes.

	Controle AODV		**AODV Ataque**				**AODV Modificado**	
Evento	**Nó 9**	**Nó 5**	**Nó 9**	**% relativa**	**Nó 5**	**% relativa**	**Nó 9**	**Nó 5**
AODV/Enviados	4560	6510	708	29.54	1182	38.30	2396	3086
AODV/Recebidos	6342	4380	972	33.58	606	26.14	2894	2318
IP/Enviados	5088	6834	1050	41.33	1632	49.69	2540	3284
IP/Recebidos	6342	4380	972	33.58	606	26.14	2894	2318
TCP/Enviados	372	6228	90	10.25	1158	43.53	878	2660
TCP/Recebidos	6060	318	948	38.31	18	2.45	2474	734

4.11 Comentários sobre resultados obtidos

Após as simulações realizadas, foram obtidos dados para comparação entre 4 grupos. O grupo controle, que representa o funcionamento normal do protocolo AODV sem nenhum nó atacante, e outros grupos compostos por atacantes e nós legítimos.

Com os dados coletados é possível observar dois gráficos relativos a cada nó, um representa a quantidade de pacotes TCP enviados, outro, a quantidade de pacotes TCP recebidos. Abaixo, as próximas duas figuras referem-se ao nó 9, origem da informação.

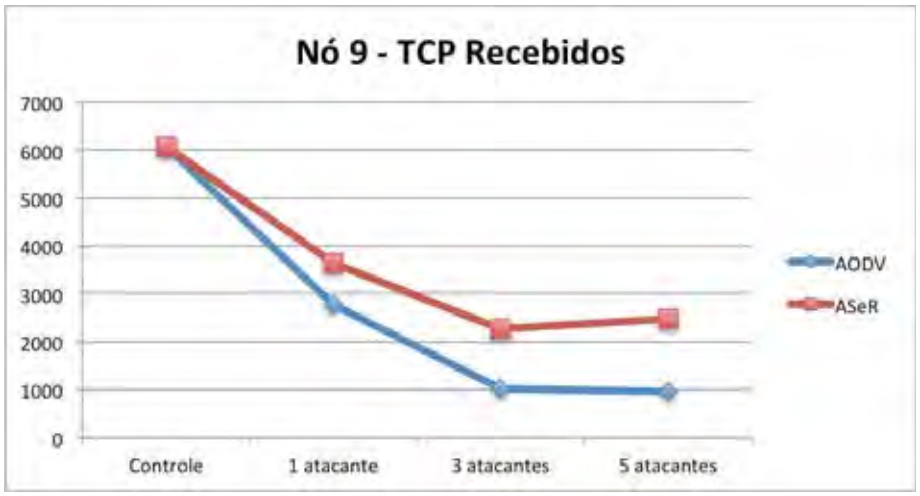

Figura 4.3 Quantidade de pacotes TCP recebidos pelo nó 9.

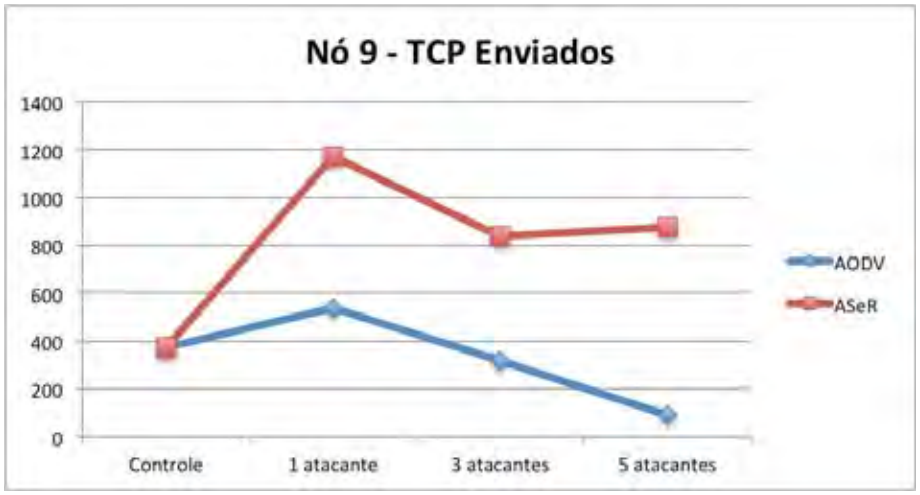

Figura 4.4 Quantidade de pacotes TCP enviados pelo nó 9.

Observando a quantidade de pacotes TCP recebidos pelo nó 9, um consumidor de informação, é possível perceber que durante os testes que receberam

um ou mais nós atacantes a taxa de pacotes foi reduzida, no entanto, a modificação feita no protocolo AODV ainda obteve maior desempenho que o protocolo em questão.

Como este nó tem que requisitar informações, em determinadas situações a quantidade de pacotes TCP enviados aumenta devido a retransmissões necessárias para corrigir os erros na rede.

Também é possível observar os gráficos que representam o desempenho dos testes em relação ao nó 5. As próximas duas figuras referem-se ao nó 5, servidor HTTP/WEB e nó que serve dados ao nó 9.

Figura 4.5 Quantidade de pacotes TCP recebidos pelo nó 5.

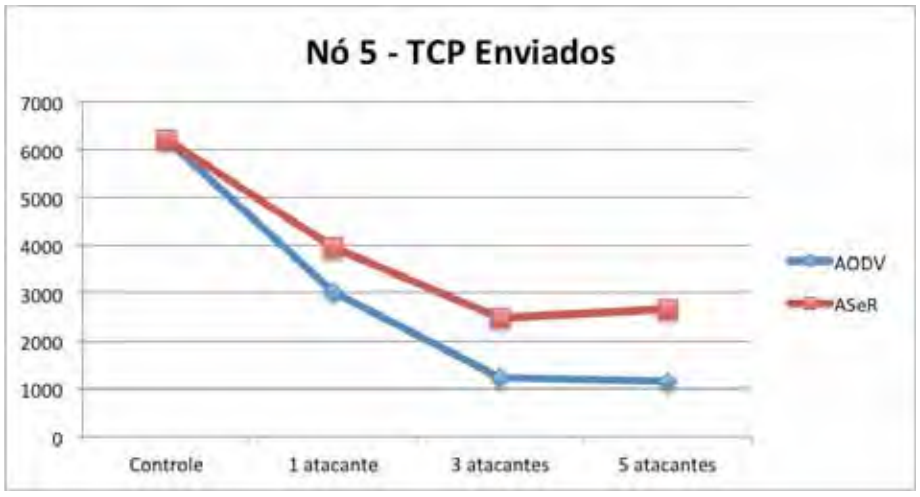

Figura 4.6 Quantidade de pacotes TCP enviados pelo nó 5.

Observando os dados exibidos pelos gráficos do nó 5, o servidor de informações, é possível perceber que a quantidade de pacotes enviados do nó diminui

de acordo com a inserção de atacantes na rede, mas ainda supera o desempenho do protocolo AODV.

4.12 Cenário V: Nó em movimento

Neste cenário de testes foi adicionada a opção de movimentação em um dos nós. O nó 9, cliente HTTP/WEB irá se deslocar a uma velocidade variável de 2 a 6 KM/h, em direção aleatória. A velocidade escolhida representa aproximadamente a velocidade de uma pessoa caminhando, com algumas reduções para transpor obstáculos ou pausas no período de movimentação.

Foram realizadas duas simulações, uma que servirá de controle, representando o protocolo AODV sob nenhum ataque. Uma segunda simulação para representar o protocolo AODV sob ataque e uma terceira que irá testar o desempenho das alterações efetuadas no protocolo.

Os parâmetros para as simulações continuam os mesmos anteriores, mesma quantidade de nós, tempo e dimensões da área de teste. O teste será composto de um nó atacante, realizando o ataque em 2/3 do tempo de simulação proposto.

A tabela 4.8 exibe os resultados obtidos com os testes.

Tabela 4.8 Dados obtidos com o Cenário V (Movimento) – Um atacante.

	Controle AODV		**AODV Ataque**				**AODV Modificado**	
Evento	**Nó 9**	**Nó 5**	**Nó 9**	**% relativa**	**Nó 5**	**% relativa**	**Nó 9**	**Nó 5**
AODV/Enviados	4422	5658	2364	86.15	3006	92.03	2744	3266
AODV/Recebidos	5520	4380	2748	89.22	2166	83.69	3080	2588
IP/Enviados	4878	5808	2856	91.47	3342	97.83	3122	3416
IP/Recebidos	5520	4380	2748	89.22	2166	83.69	3080	2588
TCP/Enviados	1056	5238	576	61.01	2796	97.21	944	2876
TCP/Recebidos	4704	1056	2538	98.98	426	52.07	2564	818

Pelos resultados obtidos na tabela é possível observar que mesmo com os nós em movimento, as modificações propostas ainda se mantêm em melhor desempenho do que o protocolo AODV padrão.

Novamente os padrões de repetições de pacotes TCP se repetiram, assim como os padrões observados no desempenho do protocolo IP.

Assim como os testes sem movimentação dos nós, dois testes adicionais foram feitos, com três e cinco atacantes. As tabelas 4.9 e 4.10 exibem os resultados coletados durante os testes.

Tabela 4.9 Dados obtidos com o Cenário V (Movimento) – Três atacantes.

	Controle AODV		**AODV Ataque**				**AODV Modificado**	
Evento	**Nó 9**	**Nó 5**	**Nó 9**	**% relativa**	**Nó 5**	**% relativa**	**Nó 9**	**Nó 5**
AODV/Enviados	4422	5658	738	45.49	1038	59.79	1622	1736
AODV/Recebidos	5520	4380	990	59.71	642	43.97	1658	1460
IP/Enviados	4878	5808	1026	51.76	1128	59.05	1982	1910
IP/Recebidos	5520	4380	990	59.71	642	43.97	1658	1460
TCP/Enviados	1056	5238	90	12.36	1014	69.73	728	1454
TCP/Recebidos	4704	1056	966	70.20	18	3.11	1376	578

Tabela 4.10 Dados obtidos com o Cenário V (Movimento) – Cinco atacantes.

	Controle AODV		**AODV Ataque**				**AODV Modificado**	
Evento	**Nó 9**	**Nó 5**	**Nó 9**	**% relativa**	**Nó 5**	**% relativa**	**Nó 9**	**Nó 5**
AODV/Enviados	4422	5658	186	28.35	252	37.05	656	680
AODV/Recebidos	5520	4380	144	21.75	90	15.90	662	566
IP/Enviados	4878	5808	504	54.42	534	69.89	926	764
IP/Recebidos	5520	4380	144	21.75	90	15.90	662	566
TCP/Enviados	1056	5238	90	26.16	222	35.46	344	626
TCP/Recebidos	4704	1056	120	19.73	18	7.08	608	254

4.13 Resultados obtidos com nós em movimento

Assim como os resultados obtidos com os nós sem movimento, foram obtidos dados para comparação entre 4 grupos. Esses grupos demonstram o funcionamento normal do protocolo AODV, funcionamento do protocolo AODV sob ataque e o funcionamento do protocolo proposto, ASeR.

Com os dados coletados foram criados dois gráficos relativos a cada nó, representando a quantidade de pacotes TCP enviados e recebidos. As figuras 4.7 e 4.8 referem-se ao nó 9.

Figura 4.7 Quantidade de pacotes TCP recebidos pelo nó 9.

Figura 4.8 Quantidade de pacotes TCP enviados pelo nó 9.

Observando os gráficos é possível inferir que a quantidade de pacotes diminui de forma considerável a medida que novos atacantes são adicionados ao ambiente.

No entanto, ao contrário do comportamento observado no cenário sem movimento, não há aumento na quantidade de pacotes TCP enviado pelo nó.

Da mesma forma, as figuras 4.9 e 4.10 são relativas ao comportamento do nó 5 durante os testes.

Figura 4.9 Quantidade de pacotes TCP recebidos pelo nó 5.

Figura 4.10 Quantidade de pacotes TCP enviados pelo nó 5.

O mesmo comportamento observado no nó 9 é repetido nos gráficos do nó 5. É possível visualizar uma queda acentuada na quantidade de pacotes com a adição de nós atacantes na rede.

Embora o desempenho do ASeR tenha sido superior ao desempenho do AODV, em ambientes com movimentação dos nós o desempenho não foi tão aparente quanto ao cenário sem movimento. É necessário maior estudo para aprimorar o protocolo para funcionamento em ambientes móveis.

4.14 Considerações finais

Neste capítulo foi abordada a implementação do ambiente de testes utilizando um simulador de redes *wireless* e as principais modificações necessárias para que a implementação fosse feita. Para os testes desta solução foram utilizados seis nós, em um espaço de 800 metros de largura e comprimento como primeiros cenários.

Para testes mais aprofundados, foi utilizada uma maior quantidade de nós e maior área de simulação. No último experimento foi adicionada a mobilidade nos nós, permitindo simular situações reais como por exemplo uma pessoa se movendo ou caminhando no ambiente.

Os testes mostraram que o mecanismo é eficiente em ambientes estáticos, no entanto, a configuração dos parâmetros como tempo de expiração e quantidade de cooperação concedidas necessitam ser ajustados para maximizar o desempenho da rede. Em relação ao desempenho do protocolo em ambientes móveis, ainda é necessária maior pesquisa para aprimorar sua ação.

Capítulo 5 - Conclusão

5.1 Conclusões gerais

Com o surgimento da computação móvel foram criadas diversas facilidades para os usuários de computadores e dispositivos móveis, tais como celulares, dispositivos de jogos eletrônicos, e outros. A necessidade de estar sempre conectado impulsionou os pesquisadores a buscar sempre uma forma mais rápida e confiável de transmissão. Até hoje, o padrão 802.11n é considerado o mais rápido para fins domésticos e empresariais. Além da velocidade, usuários buscam também mobilidade.

Como solução para mobilidade foram criadas as redes *wireless* de múltiplos saltos. Hoje são uma realidade e diversas instalações já são consideradas estáveis e funcionais. No entanto, existem problemas de segurança da informação que podem causar severos danos a infraestrutura de rede e seus usuários.

Assegurar a segurança dessas redes é importante devido a suas aplicações práticas diversas, podendo ser utilizadas em setores militares e civil, além de outras aplicações de monitoramento envolvendo sensores.

Para manter a infraestrutura da rede em funcionamento, garantindo que os dados transportados cheguem ao destino e de uma maneira eficiente, este projeto

propõe um novo método para rastrear e punir ações que levem à degradação da rede. Utilizando métodos cooperativos, o método visa dar tratamento igualitário e justo a todos os nós da rede. Como demonstrado, o protótipo da metodologia proposta foi hábil para dar acesso à todos os nós da rede, permitindo que todos tenham uma chance de enviar sua informação e utilizar dos serviços da rede, contanto que também participem para que a rede permaneça em funcionamento.

Embora o projeto tenha mostrado bom funcionamento, ainda são necessários ajustes para um melhor desempenho da rede de transporte de dados e um estudo mais aprofundado sobre outros ataques que podem ser mitigados utilizando métodos cooperativos como este, tais como a tentativa de detectar um ataque do tipo *wormhole* utilizando a abordagem de monitoramento da rede (modo promíscuo) e cooperação de nós.

Uma das principais contribuições deste projeto é o fato de ser uma modificação de um protocolo já existente e consagrado para roteamento em redes sem fio de múltiplos saltos. Os dados obtidos mostram que o desempenho em redes na presença de atacantes pode ser melhor que o protocolo AODV. Por tais motivos, o ASeR pode ser um protocolo a ser utilizado em aplicações em sistemas embarcados críticos. O método simples, sem necessidade de cálculos complexos ou outras operações o torna melhor qualificado para desempenhar essa função do que as alternativas encontradas.

Como resultados iniciais deste projeto, o artigo intitulado “802.11s: Um padrão seguro para redes de múltiplos saltos” (ALEXANDRE; BATISTA; CANSIAN, 2009) foi publicado nos anais do evento *8th International Information and Telecommunication Technologies Symposium*, realizado nos dias 9, 10 e 11 de dezembro de 2009 na cidade de Florianópolis, Santa Catarina, Brasil.

5.2 Dificuldades encontradas

Durante o desenvolvimento deste trabalho algumas dificuldades foram enfrentadas durante o período. Uma das maiores dificuldades encontradas foi a adaptação o protocolo ao simulador.

Para adaptar o protocolo ao simulador foi demandada diversas horas de estudo e entendimento do código do simulador com o intuito de encaixar a solução ao código já existente.

Além do código desenvolvido para que a solução seja eficaz, foi necessário mudar alguns parâmetros de configuração do simulador para que o ataque possa ser aplicado.

Ainda relativo ao simulador, a adaptação só pode ser feita após a escolha adequada do simulador, esta foi feita de acordo com a adaptabilidade do simulador e com pesquisas realizadas na Internet.

5.3 Trabalhos para o futuro

Com a implementação do método desenvolvido, os testes mostraram que é possível obter bons resultados no uso dessa metodologia. No entanto, algumas tarefas ainda são necessárias para que o mecanismo possa operar de forma mais estável e eficiente:

- Aprimoramento das funcionalidades inseridas no código do simulador: consiste em verificar as funções e códigos inseridos no simulador para que a solução possa se integrar de maneira adequada ao simulador. Um exemplo de funcionalidade a ser inserida é a possibilidade de indicar no arquivo de configuração o nó atacante e qual período de tempo ele irá realizar o ataque;
- Testes com parâmetros de tempo: realizar mais testes para descobrir quais são os melhores parâmetros para serem utilizados, como por exemplo, o tempo que cada nó vizinho tem para enviar um pacote antes de ser considerado um nó malicioso, a quantidade de cooperação que deve ser atribuída a um nó em caso de cooperação, etc;
- Movimentação: aprimorar as capacidades do simulador para que se possa obter melhor desempenho em ambientes com nós em movimento, em virtude da baixa taxa de desempenho apresentada nos testes;

- Aumentar os cenários de teste: neste trabalho o foco principal foi o desenvolvimento e implementação do protocolo ASeR, os testes foram realizados em apenas duas topologias. O aumento do número de testes com topologias distintas pode proporcionar dados mais conclusivos sobre o desempenho do protocolo;
- Testes em três dimensões: os testes realizados neste trabalho são realizados em duas dimensões, a única variável encontrada é a distância dos nós. Com o uso proposto em sistemas embarcados, o protocolo precisa ser testado em redes com três dimensões, onde a distância e a altura dos nós também pode influenciar o desempenho.

Após essas tarefas será possível obter uma melhor medida para comparação do método proposto com o desempenho das redes quando não estão sobre ataque.

Referências bibliográficas

ABELÉM, A. J. G.; ALBUQUERQUE, C. V. N.; SAADE, D. C. M.; AGUIAR, E. S.; DUARTE, J. L.; FONSECA, J. E. M.; MAGALHÃES, L. C. S., **Redes *Mesh*: Mobilidade, Qualidade de Serviço e Comunicação em Grupo.** In: VII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSEG 2007), 2007. Rio de Janeiro.

AKYILDIZ, I. F.; WANG, X.; WANG, W., **Wireless Mesh Networks: A Survey**. In: Elsevier Computer Networks, vol. 47, 2005.

ALEXANDRE, L.A.; BATISTA, M. L.; CANSIAN, A. M. **802.11s: Um padrão seguro para redes de múltiplos saltos**. In: 8th International Information and Telecommunication Technologies Symposium, 2009, Florianópolis. ISBN: 978-85-89264-11-2.

CHLAMTAC, I.; CONTI, M.; LIU, J. N. **Mobile ad hoc networking:** imperatives and challenges. In: Elsevier Ad Hoc Networks Journal, 2003.

CLAUSEN, T.; JACQUET, P., **RFC 3626 - Optimized Link State Routing Protocol (OLSR).** Disponível em: < http://www.ietf.org/rfc/rfc3626.txt>. Acesso em: 13 jun. 2011.

FUJINOKI, H.; PANDEY, A. K., **Study of MANET routing protocols by GloMoSim simulator**. In: International Journal of Network Management; 15, Wiley InterScience, 2005.

GLASS, S.; PORTMANN, M.; MUTHUKKUMARASAMY, V. **Securing Wireless Mesh Networks.** In: IEEE Computer Society, 2008.

GloMoSim: Global Mobile Information System Simulation Library. Disponível em: <http://pcl.cs.ucla.edu/projects/glomosim/>. Acesso em: 13 jun. 2011.

GOLLMANN, D. **Computer Security.** John Wiley & Sons ltda., 1999. ISBN 0471978442.

HIERTZ, G. R.; MAX, S.; ZHAO, R.; DENTENEER, D.; BERLEMANN, L., **Principles of IEEE 802.11S.** In: Computer Communications and Networks (ICCCN 2007), IEEE, 2007.

HOGIE, L.; BOUVRY, P.; GUINAND, F., **An Overview of MANETs Simulation**. In: Electronic Notes in Theorectical Computer Science, 150. ELSEVIER, 2006.

HUANG, Y.; *et al.,* **TCP Performance in Coded Wireless Mesh Networks**. In: Sensor, Mesh and Ad Hoc Communications and Networks 2008 (SECON '08), IEEE, 2008.

IEEE. **IEEE Ratifies 802.11n, Wireless LAN Specification to Provide Significantly Improved Data Throughput and Range**. Disponível em: <http://standards.ieee.org/announcements/ieee802.11n_2009amendment_ratified.html>. Acesso em: 12 jun. 2011.

INCT-SEC. **Instituto Nacional de Ciência e Tecnologia em Sistemas Embarcados Críticos.** Disponível em: <http://www.inct-sec.org>. Acesso em: 06 set. 2011.

JOHNSON, D.; HU, Y.; MALTZ, D., **RFC 4728 – The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4**. Disponível em: < http://www.ietf.org/rfc/rfc4728.txt>. Acesso em: 30 maio 2011.

KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a Internet: uma abordagem top-down**. 3ª Edição. Pearson, 2006. ISBN 978-85-88639-18-8.

LIU, C.; SHU, Y.; LI, M.; YANG, O W.W., **A New Mechanism to Detect Selfish Behavior in IEEE 802.11 Ad Hoc Networks**. In: ICC'09. IEEE International Conference On Communications, 2009.

MANDALAS, K.; FLITZANIS, D.; MARIAS, G.F.; GEORGIADIS, P; **A survey of several cooperation enforcement schemes for MANETs.** In: Signal Processing and Information Technology, 2005.

OPEN80211S, **open80211s**. Disponível em: <http://www.open80211s.org/>. Acesso em: 08 jun. 2011.

PANDEY, A.K.; FUJINOKI, H., **Study of MANET routing protocolos by GloMoSim simulator**. In: International Journal of Network Management, Volume 15, edição 6, ACM, 2005.

PAUL, T.K.; OGUNFUNMI, T., **Wireless LAN Comes of Age: Understanding the IEEE 802.11n Amendment**. In: Circuits and Systems Magazine, IEEE, vol. 8, 2008.

PARSEC: Parallel Simulation Environment for Complex Systems. Disponível em: <http://pcl.cs.ucla.edu/projects/parsec/>. Acesso em: 13 de junho de 2011.

PERKINS, C.; BELDING-ROYER, E.; DAS, S., **RFC 3561 - Ad hoc On-Demand Distance Vector (AODV) Routing**. Disponível em: < http://www.ietf.org/rfc/rfc3561.txt>. Acesso em: 08 jun. 2011.

SAADE, D. C. M.; GOMES, A. G.; CARRANO, R. C.; MAGALHÃES, L. C. S.; ALBUQUERQUE, C. V. N.; TAROUCO, L. R., **Multihop MAC: Desvendando o Padrão 802.11s.** In: 8th Brazilian Symposium on Information and Computer System Security (SBSEG 2008), 2008. Gramado.

SHYV, D. J., **Military Usage Scenario and IEEE 802.11s Mesh Networking Standard.** In: Military Communications Conference (MILCOM), IEEE, 2006.

TANENBAUM, A. S., **Redes de computadores.** 4ª edição. Elsevier, 2003. ISBN 85-352-1185-3.

UCA. "**Um Computador por Aluno**". Disponível em: < http://www.inclusaodigital.gov.br/inclusao/links-outros-programas/projeto-um-computador-por-aluno-uca/>. Acesso em: 31 maio 2011.

WANG, X.; WONG, J., **An End-to-end Detection of Wormhole Attack in Wireless Ad-hoc Networks.** In: 31st. Annual International Computer Software and Applications Conference, IEEE, 2007.

ZHOU, W.; WEI, Z.; KANG, M.; NIXON, P.; JIA, L., **A Credit-Based Incentive Mechanism for Recommendation Acquisition in Multihop Mobile Ad Hoc Networks"**. In: Third International Conference on SECURWARE '09, 2009.

Wei Zhou; Zhiqiang Wei; Mijun Kang; Nixon, P.; Lang Jia; , "A Credit-Based Incentive Mechanism for Recommendation Acquisition in Multihop Mobile Ad Hoc Networks," *Emerging Security Information, Systems and Technologies, 2009. SECURWARE '09. Third International Conference on* , vol., no., pp.306-311, 18-23 June 2009

WIFIMESH, **WifiMesh – The FreeBSD Wiki**. Disponível em: <http://wiki.freebsd.org/WifiMesh>. Acesso em: 31 maio 2011.

ZHANG, Y.; LUO, J.; HU, H., **Wireless Mesh Networking: Architectures, Protocols and Standards** (Wireless Networks and Mobile Communications). 1ª edição. Auerbach Publications, 2006. ISBN 08-493-7399-9.