Universidade Federal de Santa Catarina
Centro Tecnológico
Departamento de Informática e Estatística

Rômulo Radowitz

Detecção de Intrusão em Redes Móveis AD HOC, baseado em Redes Neurais Artificiais

Prof. Dr. João Bosco Mangueira Sobral

Florianópolis, Novembro de 2009

Detecção de Intrusão em Redes Móveis AD HOC, baseado em Redes Neurais Artificiais

Projeto de Pesquisa para elaboração do Trabalho de Conclusão de Curso apresentado como exigência para a obtenção do título de Bacharel em Sistemas de Informação à Universidade Federal de Santa Catarina – UFSC, no curso de Sistemas de Informação.

Banca Examinadora

_____

Prof. Dr. João Bosco Mangueira Sobral (Orientador)

Universidade Federal de Santa Catarina

_____

Dr. Igor Vinícius Mussoi de Lima (Membro)

Universidade Federal de Santa Catarina

_____

Rogério Ferraz (Membro)

Koerich Engenharia de Telecomunicações

Florianópolis, Novembro, 2009

Agradecimentos

À minha família que, desde cedo investiu na minha educação, escolas particulares e cursos, mesmo muitas vezes, tendo de batalhar para conseguir os recursos necessários.

À Thaty, minha namorada que além de me agüentar nos momentos de stress, me apoiou e auxiliou em tudo que necessitei.

Aos meus amigos e companheiros de trabalho, que diretamente e indiretamente me auxiliaram na execução deste trabalho.

Ao professor Bosco, que com sua vasta experiência, me guiou na execução deste trabalho.

Resumo

Este trabalho visa demonstrar um modelo de um sistema de intrusão de redes móveis AD HOC, que devido suas características possui um elevado risco de segurança, baseado em redes neurais que são utilizadas para aprendizagem do sistema, identificando e armazenando possíveis invasões e propondo ações ativas aos ataques realizados.

Dentro deste modelo serão efetuadas análises sobre a eficiência deste modelo para indicar a viabilidade de utilização deste projeto sobre o aspecto das vulnerabilidades do modelo de rede utilizado neste trabalho. Estas análises serão realizadas através de uma utilização prática do protocolo pró-ativo OLSR.

Também serão demonstradas fundamentações teóricas sobre os temas relevantes aos aspectos do projeto, a fim de facilitar o entendimento e a aplicação dos conceitos utilizados.

Palavras Chaves: Segurança de Redes, Redes Neurais Artificiais, Detecção de Intrusão, redes móveis Ad Hoc.

Abstract

This paper demonstrates a model of a system intrusion of mobile ad hoc networks, due to its characteristics have a high security risk, based on neural networks that are used to learning the system, storing and identifying possible intrusions and proposing actions to active attacks carried out.

Within this model will be made analysis on the efficiency of this model to indicate the feasibility of using this design on the appearance of the vulnerabilities of the network model used in this study. These tests will be carried out through a practical use of the proactive protocol OLSR.

Also shown are theoretical predictions on the topics relevant to aspects of the project in order to facilitate the understanding and application of concepts.

Words Keys: Security of Nets, Artificial Neural Nets, mobile Detention of Intrusion, nets Ad hoc

Lista de Acrônimos

MANET – Mobile Ad Hoc Network

OFDM – Orthogonal Frequency Division Multiplexing

OLSR – Optimized Link State Routing Protocol

AODV – Ad Hoc On-demand Distance Vector

IANA – Internet Assigned Numbers Authority

AODV – Ad Hoc On-Demand Distance Vector

UDP – User Datagram Protocol

TCP – Transmission Control Protocol

IP – Internet Protocol

TC – Topology Control

MPR – Multipoint Relay

RREP – Route Request

RREQ – Route Reply

RERR – Route Error

IDS – Intrusion Detection System

NIDS – Network Intrusion Detection System

HIDS – Host Intrusion Detection System

I-IDS – Intelligent Intrusion Detection System

CIDF - Common Intrusion Detection Framework

IA – Inteligência Artificial

RNA – Rede Neural Artificial

DHCP – Dinamic Host Configuration Protocol

IETF – Internet Engineering Task Force

MID – Multiple Interface Declaration

HNA – Associated Networks and Host

ANSN – Advertised Neighbor Sequence Number

TTL – Time to Live

LQ – Link Quality

ETX – Expected Transmission Count

IDWG – Intrusion Detection Working Group

Lista de Ilustrações

Lista de Tabelas

Sumário

1. Introdução

Atualmente ocorre uma revolução no mundo corporativo, onde cada vez mais, a informação é valorizada e o vazamento de dados ou informações pode se tornar um fator crítico para as corporações. Por isto na mesma crescente em que novas tecnologias de segurança da informação são desenvolvidas, a sofisticação de ataques e intrusões cresce, com mais recursos e com mais inovações.

Sobre este cenário se questiona o quanto pagar para proteger as informações estratégicas. Elevando este contexto ao crescimento da utilização de redes sem fio, que sem dúvida são mais vulneráveis a ataques e invasões, torna-se fundamental uma elevada política de segurança.

Uma das tecnologias muito pesquisadas e desenvolvidas está os sistemas de detecção de intrusão, que visam identificar ataques e intrusões e alertar usuários.

O objetivo deste trabalho é aprimorar as técnicas de detecção de intrusão, utilizando uma abordagem sobre redes neurais, que proporcionarão uma análise dinâmica de prováveis ataques.

1.1 Metodologia

Para a realização deste trabalho, adotou-se a seguinte metodologia:

- Pesquisar definições e propriedades de sistemas de detecção de intrusão;

- Avaliar propriedades relativas à adaptação do sistema de detecção de intrusão com as redes sem fio Ad Hoc;

- Compreender e avaliar a utilização de redes neurais para a detecção de intrusão;

- Avaliar o modelo perante os modelos convencionais e comparar a eficácia da utilização em redes móveis com a abordagem proposta pela defesa de tese em que este presente trabalho está baseado;

- Realizar experimentos de ataques avaliando a eficiência deste modelo;

1.2 Trabalhos Relacionados

Este trabalho foi inspirado na linha de pesquisa iniciada por meio da defesa de mestrado Uma Abordagem simplificada de detecção de intrusão baseada em redes neurais artificiais (Lima, 2005), que consiste no desenvolvimento de um protótipo funcional de um IDS utilizando os conceitos de rede neural para melhorar a eficiência do modelo.

Em (Shaeffer 2003) também é proposto um sistema de detecção de intrusão baseado em redes neurais e avaliado o modelo com uma abordagem prática. No trabalho de (TAMASHIRO 2007)) é desenvolvido importantes pontos de segurança em redes sem fio móveis avaliando os protocolos de roteamento para redes sem fio Ad Hoc móveis. Já na dissertação (Silva 2004) é proposto uma extensão para o modelo IDWG para detecção de intrusão em Ambientes Computacionais.

1.3 Estrutura do Trabalho

No capítulo seguinte é apresentada uma visão geral sobre a conceituação teórica dos sistemas de detecção de intrusão, demonstrando suas abordagens e visões fundamentais para desenvolvimento do projeto, como abordagem do protótipo, forma de detecção de intrusão, a classificação dos IDS e tipos existentes.

No capítulo três, são apresentadas as teorias das redes neurais, tentando sempre vincular cada conceito com a utilização prática deste trabalho, delimitando este amplo tema ao aprendizado de máquina e as redes neurais artificiais.

No quarto capítulo serão demonstrados os conceitos das redes Ad Hoc, aplicações práticas existentes e suas vulnerabilidades, bem como é demonstrando os protocolos utilizados, focando o estudo de dois dos protocolos mais utilizados atualmente o AODV e o OLSR.

Já no quinto capítulo é demonstrado o modelo do sistema de detecção de intrusão para redes móveis Ad Hoc, através da definição das configurações da rede neural utilizada, das configurações da rede Ad Hoc utilizadas, bem como o protocolo de controle de rede. Também é definida a forma de captura de pacotes, que será utilizada para avaliação e classificação das seções da rede

No sexto capítulo são demonstrados os experimentos práticos realizados sobre a rede Ad Hoc, bem como sobre o sistema de detecção de intrusão, apresentando o desempenho de cada um destes itens e uma análise sobre itens positivos e negativos identificados neste trabalho.

Na ultima seção deste trabalho, é realizada a conclusão sobre os objetivos deste trabalho, sobre a eficiência do modelo e o desenvolvimento de possíveis atividades futuras que não foram abordadas neste trabalho.

2. Sistemas de Detecção de Intrusão

Há uma grande variedade de dispositivos e softwares para proteção de sistemas de informações, sendo que a indústria de software vem se esforçando para garantir a segurança de usuários e aplicações. Uma das diversas abordagens existentes para garantir esta segurança, são os softwares de

antivírus, que varrem os arquivos e identificando padrões, ou seja, padrões conhecidos são identificados como vírus. Porém em situações de vírus novos, com um padrão desconhecido, há uma falha de segurança.

Quando se trata de ataques a redes e servidores, existem outras formas de contramedida, como o *Firewall* e os identificadores de intrusão. O *Firewall* é um dispositivo que bloqueia portas sobre um conjunto de regras, analisando pacotes com valores de porta no cabeçalho do protocolo, desta forma trabalhando sobre um modelo estático, simplesmente descartando estas conexões.

Então basicamente, os sistemas de detecção de intrusão, representam uma camada a mais de segurança e foram criados com a finalidade de detectar e informar o administrador da rede de um possível ataque. Os identificadores de intrusão vasculham todo o tráfego de rede, verificando os pacotes recebidos e analisando padrões e estados que possam identificar possíveis ataques, desta forma, passando de uma abordagem estática para uma abordagem dinâmica.

Neste aspecto, as características desejáveis de um IDS são apresentadas a seguir, baseadas no trabalho de (Shaeffer 2003):

- Ser um sistema tolerante a faltas;

- Impor o mínimo de impacto no sistema durante o processo de análise de pacotes;

- Observar desvios do comportamento normal;

- Funcionar continuamente se supervisão humana;

- Apresentar alarmes condizentes com o tráfego analisado;

Este último ponto levanta a questão sobre os erros prováveis de um IDS que podem ser categorizados em:

- Falsos positivos – Ação Classificada como Anômala (Possível intrusão) quando é uma ação legítima;

- Falsos negativos - Quando ocorrem uma intrusão e o IDS permite o tráfego;

- Erros de subversão – Alteração no IDS por um provável intruso a fim de criar falsos negativos;

2.1 Classificação do IDS e Projeto

Um IDS pode ser classificado de acordo seus métodos de detecção, arquitetura, comportamento de pós-detecção, e freqüência de uso conforme

representado na figura 1. Todas estas variáveis precisam ser consideradas em um planejamento de implementação de um IDS, já que de acordo com características da aplicação, necessitarão de diferentes funcionalidades e comportamento. Nas próximas seções deste capítulo, as classificações pertinentes a implementação deste projeto serão descritas.

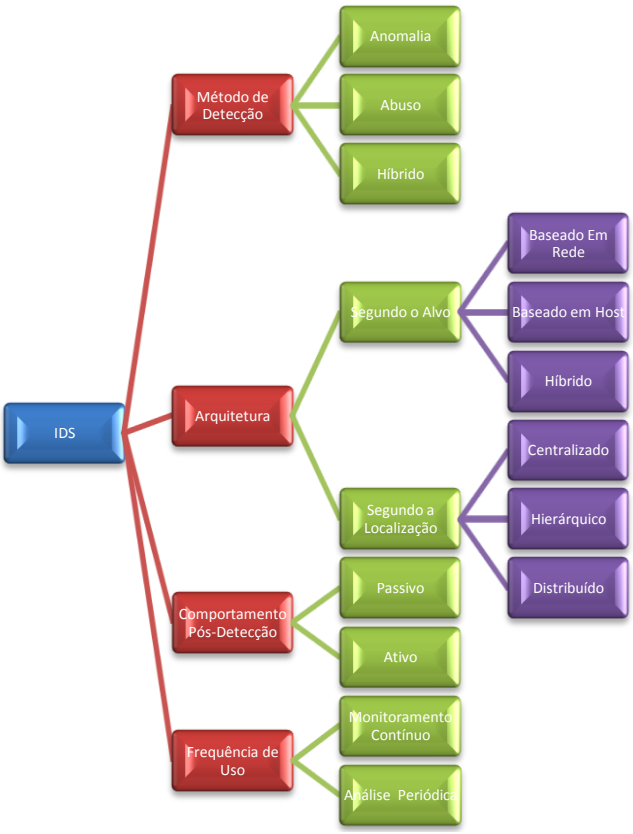

Figura 1 - Classificação das Abordagens de IDS

2.2 Tipos de Arquitetura de um IDS

Antigamente, as grandes redes possuíam um modelo centralizado utilizando os grandes *Mainframes*. Neste contexto surgiram os primeiros IDS baseados em *Host*.

Com a evolução dos computadores e da utilização de novas hierarquias de rede distribuídas, houve uma grande necessidade de mudança de foco no tratamento dos IDS, assim surgiu o *Network-Based* IDS. Nos trabalhos de (Shaeffer 2003) e (SILVEIRA 2007) são realizados estudos sobre esta arquitetura dos IDS.

A arquitetura *Host-Basead* IDS, ou HIDS são sistemas de intrusão geralmente mais antigos, que são instalados e funcionam sobre um sistema operacional de um Host. Este modelo possui mecanismos e procedimentos de análise que identificam uma provável intrusão, com a base em recursos locais

como o registro de *log* do sistema operacional, além de indícios de atividades fora de um padrão normal, como acessos rejeitados, alterações de privilégio do sistema operacional.

Porém, este modelo, também apresenta uma série de limitações. No caso de um ataque que tenha ocorrido em todos os dispositivos ao redor do IDS não serão detectados. Como se trata de uma aplicação instalada no sistema operacional do Host pode afetar o desempenho do elemento em questão, além de que uma unidade pode ter facilmente seu banco de logs comprometido em ataques ou defeitos.

Cabe citar que neste modelo, além de ser necessária a instalação individual em cada *host*, também necessita de que todos os *Hosts se conectem* a um banco de assinaturas para atualizar seu banco individualmente, gerando assim um grande trafego que pode ser potencializado, de acordo com o tamanho e modelo da rede.

Na figura 2 é apresentado o modelo de I-IDS aplicado no host de uma rede genérica.

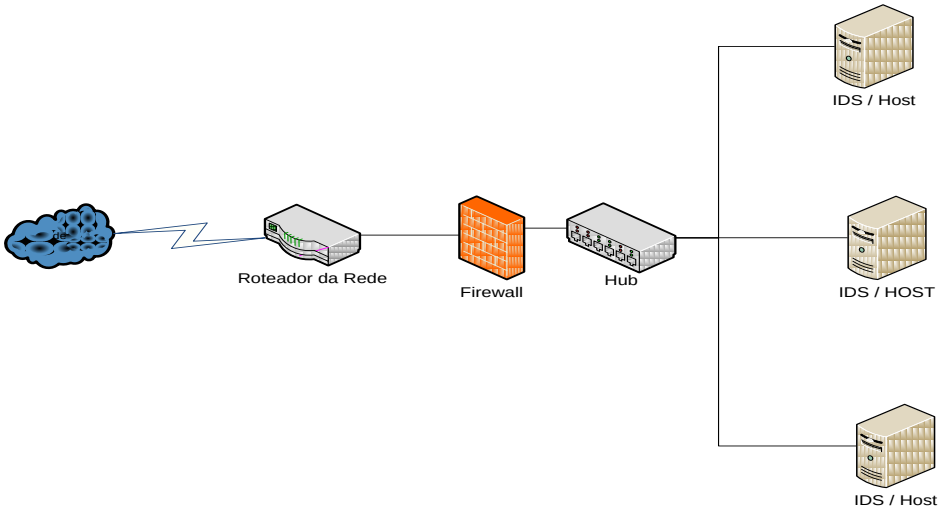

Figura 2 - IDS Baseado em Host

O Network-Based IDS ou NIDS é o modelo mais utilizado, que basicamente trabalha sobre os pacotes de rede como origem de dados, utilizando um adaptador de rede em modo promíscuo (Figura 3) que faz a varredura do tráfego de dados em sensores ou estações de gerenciamento.

Os sensores são componentes alocados estrategicamente na rede, para monitorar todo o tráfego consumido naquele ponto. Nesta situação a disposição de sensores e o correto planejamento de utilização destes dispositivos certamente irão impactar na eficiência do sistema.

As características de um NIDS, tipicamente são de analisar o tráfego da rede para procurar assinaturas de ataques com a possibilidade de alertar o administrador ou mesmo tomar alguma contra medida automática para preservação da rede, em um ou mais locais estratégicos da rede.

A seguir são destacados alguns pontos estratégicos deste modelo em relação ao HIDS:

- Custo – Permite a análise em pontos estratégicos da rede sem a necessidade de implementação em todos os hosts, desta forma acarretando em um menor custo de implementação e gerenciamento;

- Análise de Pacotes – Examina todos os cabeçalhos dos pacotes em busca de sinais de atividade suspeita, assim identificando ataques específicos que o modelo HIDS não detectaria;

- Eliminação de Evidências – Como uma intrusão gera tráfego na rede, neste modelo as evidências (tráfego gerado) não podem ser eliminadas;

Mas este modelo também possui pontos críticos de utilização. O mais significante é a utilização em redes de altíssima velocidade como backbones, pois nesta situação o custo de infra-estrutura para análise do tráfego em tempo real, sem prejudicar o sistema, seria bastante elevado ao ponto de inviabilizar o projeto.

Outro ponto a ser considerado é que os dados transmitidos criptografados não seriam facilmente detectados, a menos que esta confidencialidade fosse quebrada, o que na maioria das novas tecnologias, se torna inviável.

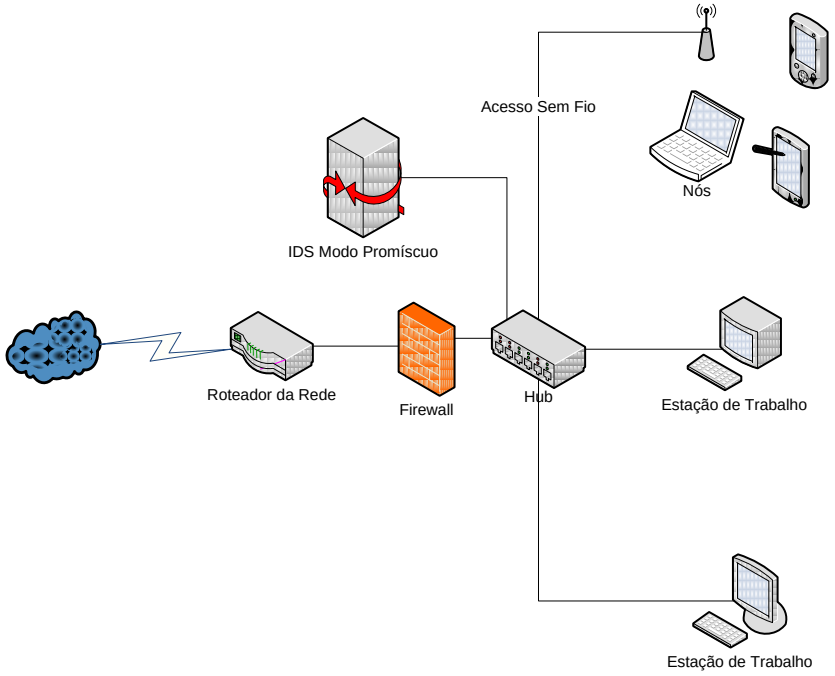

Figura 3 - IDS Baseado em Rede

2.3 Formas de Detecção

As formas de detecção de intrusão são classificadas sobre dois aspectos, a categoria que analisa as informações baseadas em eventos passados

(conhecimento), e a categoria que analisa o estado corrente do sistema (comportamento).

Os sistemas baseados em conhecimento são programados para auditoria com o propósito de, sobre demanda ou, em momentos programados buscar por anomalias conhecidas e reportá-las ao administrador da rede. Esta classificação geralmente busca padrões de ataques conhecidos ou inconsistências que não podem ser geradas por operação normal.

Teoricamente a grande vantagem deste modelo é o fato de gerar uma baixa quantidade de falso positivo, pois possuem em sua base de assinaturas ataques já conhecidos, desta forma minimizando a ocorrência de falsos positivos.

Esta forma também visa à redução dos dados gerados, pois ao invés de tentar analisar informações em um grande nível de detalhamento, efetua a exclusão dos dados teoricamente irrelevantes, produzindo somente um relatório reduzido. Em contra partida, o número de falsos positivos, neste modelo, pode ser elevado se não houver a atualização contínua das assinaturas.

Sistemas de detecção de intrusão baseados em comportamento assumem que um evento pode ser detectado observando um desvio de comportamento, do próprio sistema e dos usuários. Ele tende a produzir uma quantidade elevada de falsos positivos e resultados difíceis de ser interpretados.

O principal ponto positivo deste modelo, é que novos ataques e vulnerabilidades podem ser identificadas, já que não depende de regras expositivamente declaradas.

Segundo (KUMAR 1995), este modelo apresenta quatro estados de detecção:

- Intrusivo e anômalo: a atividade é intrusiva e é apontada como tal por ser também anômala, são conhecidos como os verdadeiros positivos;

- Não intrusivo e não anômalo: a atividade não é anômala e não é apontada como intrusiva, são denominados como verdadeiros negativos;

- Intrusivo mas não anômalo: a atividade é intrusiva, mas, como não é anômala não é reportada como tal, gerando uma falha em sua detecção, são consideradas como falsos negativos;

- Não intrusivo, mas anômalo: atividade não é intrusiva, porém como é anômalo, o sistema entende que se trata de uma atividade intrusiva, reportando de forma incorreta tal fato, estes são denominados falsos positivos;

2.4 Arquitetura Genérica de um NIDS

Atualmente há uma grande quantidade de arquiteturas de NIDS, porém há uma tentativa de padronização de um modelo genérico, que é apoiado pelo IETF. O CIDF, que é demonstrado na figura 4, foi desenvolvido por um grupo de trabalho denominado IDWG. Ele define um conjunto de componentes que estabelecem um modelo genérico de um sistema de detecção de intrusão.

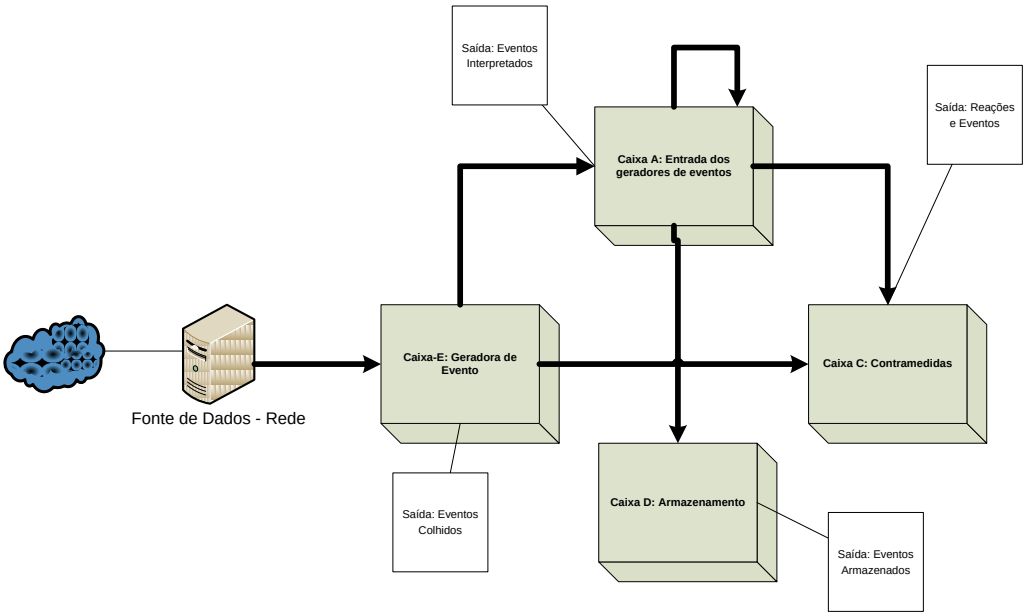

Figura 4 - Arquitetura Genérica NIDS

A tarefa da “caixa-E” é prover informações sobre eventos ao restante do sistema, como tráfego. Esta caixa representa os sensores do IDS, sem estas entradas geradas, o sistema não possuiria informações suficientes para chegar a uma conclusão dos eventos ocorridos. A “Caixa-A” analisa a entrada dos geradores de eventos, onde nossa pesquisa está concentrada, ou seja, na criação de novas formas de gerar estes eventos, através de redes neurais. Este componente deve possui sempre a atualização de assinaturas de ataques.

Já a “Caixa-D” define os meios utilizados para armazenar as informações de segurança e disponibilizá-las para uma oportunidade posterior. A “Caixa-C” é responsável pela contramedida de um ataque ou intrusão, esta contra medida pode ser bem variável, e classificadas como ativa ou passiva. As contramedidas passivas são como só alertar o administrador e as ativas pode-se citar ações como desconectar uma conexão TCP, modificar lista de filtragens de roteamento.

2.5 Considerações

Este capítulo apresentou uma visão geral sobre os detectores de intrusão, destacando suas principais características e classificações, visando compor a fundamentação teórica, que será utilizada no modelo de implementação. Os IDS são ferramentas que, realmente podem melhorar o nível de segurança de

usuários comuns e grandes empresas e corporações, mas é necessário avaliar detalhadamente as questões de projeto e as características desejadas, para que estes sistemas não causem um forte impacto no e desempenho da rede.

3. Redes Neurais Artificiais

A inteligência artificial é um grande campo de pesquisa que atravessa diversas áreas, sendo definida por (RUSSELL e Stuar Jonathan 2004) como o estudo de agentes que receberam percepções do ambiente e executam ações. Cada agente programa uma função que mapeia seqüência de percepções em ações, que podem ser representadas de diversas maneiras entre elas as redes neurais e sistemas de teoria de decisão.

Dentro de diversos artefatos o computador eletrônico digital tem sido os preferidos. Sobre este escopo será utilizado às redes neurais artificiais neste presente trabalho.

Também é fundamental considerar que as redes neurais artificiais foram inspiradas no comportamento dos neurônios biológicos e nos sistemas nervosos. Considerando estas características e estrutura as RNAs possuem como forte característica, o processamento de informação distribuído e paralelo.

O modelo artificial pioneiro de neurônio biológico foi proposto por McCulloch e Pitts em 1943, após a definição deste modelo várias oportunidades, com cunho em problemas reais, foram utilizadas.

Entre as muitas áreas de aplicação de Redes Neurais, a principal é o reconhecimento de padrões. Do ponto de vista humano, o reconhecimento de um padrão, seja ele qual for, compreende a técnica pela qual uma pessoa, uma vez havendo aprendido a reconhecer determinado assunto, poderá reconhecê-lo outra vez, mesmo que o que ela esteja observando possua variações em relação ao primeiro modelo. Da mesma forma funciona com as redes neurais.

Nas seções seguintes do capitulo três serão abordadas um resumo teórico deste assunto, voltado para utilização do modelo deste trabalho, desta forma serão apresentados somente definições básicas que envolvam diretamente o objetivo deste trabalho.

3.1 Definição de Neurônios Artificiais

Uma rede neural artificial é nada mais que um componente que simula o funcionamento de um neurônio, e devem funcionar de acordo com seu funcionamento, ou seja, recebendo e retransmitindo informações.

Um aspecto comum da implementação de redes neurais é considerar o cérebro como um dispositivo computacional paralelo, muito diferente dos computadores seriais tradicionais. McCulloh e Pitss propuseram uma unidade binária com limiar de ativação como o modelo computacional de um neurônio.

O neurônio matemático calcula uma soma ponderada de n sinais de entrada xj, com j = 1,2,3,...,n, e gera uma saída de 1 se a soma está acima de um certo limiar u.

O processo computacional envolvido com uma rede neural artificial é desenvolvido através de um neurônio artificial ou um elemento de processamento, recebendo entradas de um grande número de outros neurônios artificiais ou de fonte de estimulo externo.

MacCulloch interpretou um neurônio artificial como sendo um circuito de entradas binárias combinadas por somas ponderadas, desta forma produzindo uma entrada efetiva, que pode ser representado pela figura 5, que é inspirada em seu estudo.

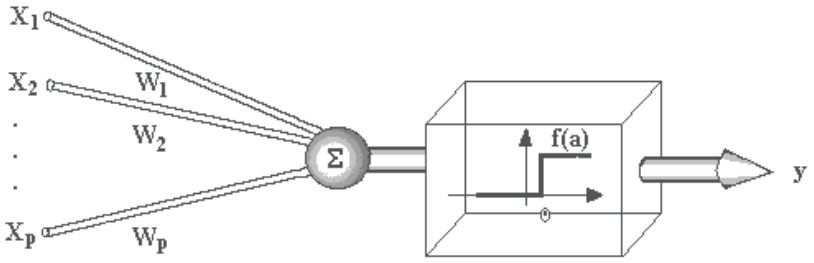

Figura 5 - Modelo de Neurônio Artificial

A função básica de um neurônio é formar as entradas e retornar uma saída, caso este valor seja maior que o valor da soma. Dentro desta expectativa, no modelo geral, as entradas são combinadas usando uma função para produzir um estado de ativação do neurônio, sendo que as entradas chegam através dos dentritos possuindo um peso atribuído pela sinapse.

O valor de ativação é uma soma ponderada e constitui um argumento. Este modelo neuronal tem sido generalizado de muitas maneiras. Uma delas é através da utilização de uma função de ativação que não seja necessariamente a função degrau. A função de ativação, que define o neurônio é geralmente não linear, sendo que o valor resultante da função de ativação é à saída do neurônio. A magnitude da saída, e os pesos da conexão, determinam o efeito da unidade.

Os três componentes essenciais de um sistema computacional baseado em redes neurais artificiais são a função de ativação, a arquitetura e a regra geral de treinamento. Um dispositivo computacional para implementar simulações de cadeias neurais artificiais, de um modo parecido com o cérebro humano, consiste de diversas unidades neurais citadas acima, conectadas umas as outras.

3.2 Processos de Aprendizagem

Como não basta conectar neurônios para que eles forneçam um resultado útil é necessário um método para treiná-los. O conhecimento da rede neural

artificial se concentra nos pesos definidos para as conexões sinápticas da rede, formando uma representação compacta e distribuída desse conhecimento e proporcionando capacidades de generalização e adaptabilidade à rede neural. Porém, esta organização não baseada em regras impossibilita às redes neurais de explicar de forma abrangente o processo computacional pelo qual tomou a decisão exposta por suas saídas. Em (HAYKIN 2001) o processo de aprendizagem é detalhado e classificado conforme os seguintes parágrafos.

Baseando-se no conceito que a característica mais importante das redes neurais é a habilidade de avaliar um ambiente e melhorá-lo. Isto geralmente é realizado sobre um processo que ajusta os pesos, e chega a uma solução generalizada.

A aprendizagem em redes neurais é caracterizada pela capacidade que as redes possuem de modificar o seu comportamento em resposta a eventos ou situações que ocorrem no ambiente externo e que fornecem um conjunto de entradas, o qual pode ser associado a um conjunto de saídas desejadas ou não, ou seja, de modo mais pratico o treinamento consiste em reforçar bons comportamentos, que devem ser repetidos e reprimir os maus. Através de um algoritmo de treinamento, este conjunto de entrada acarreta um ajuste dos pesos da rede, produzindo um conjunto de resposta adequado que concorda com os padrões de entrada ou como os padrões armazenados pela rede. Após a execução consistente e correta deste aprendizado, a rede torna-se capaz de compor similaridades e generalizar situações que ainda não foram aprendidas. Durante o processo de treinamento da rede, é muito mais importante a monitoração de quanto tempo ela deve ficar treinando, pois um treinamento muito prolongado pode levá-la a um estado de especialização, nesta situação, a rede pode perder a capacidade de generalização, pois tende a decorar os padrões de entrada.

O comportamento de uma rede neural, depois de treinada, é determinado pelos pesos existentes entre as conexões de seus neurônios e as funções de ativação usadas para treinamento da rede. Estas funções são consideradas os limiares de ativação da rede. Toda rede neural possui uma topologia que está ligada diretamente ao problema que se deseja resolver, a complexidade deste problema e as outras abordagens.

Pode ser visto que o processo de aprendizagem é fundamental para não criar um modelo equivocado. Outro fato fundamental é a maneira pela qual uma rede neural se relaciona com o ambiente, sendo apresentados os seguintes paradigmas:

- Independência de quem aprende – As RNAs aprendem através de contatos analogia, exploração e por descoberta;

- Aprendizagem Supervisionada – É caracterizada por indicar explicitamente o comportamento bom e o comportamento ruim. Para cada exemplo apresentado uma correção é introduzida depois de observar a saída da rede. Os pesos são determinados de maneira que uma rede produza respostas o mais próximo possível das repostas corretas conhecidas;

- Aprendizagem não supervisionada – É Caracterizada pelo fato de que para se modificar os valores das conexões sinápticas não se usa informações se a resposta da rede foi correta ou não. Por outro lado utiliza um esquema, que para exemplos semelhantes, a rede responda de modo semelhante. Ela explora a estrutura adjacente, ou correlações entre padrões dentro do conjunto de dados, e os organiza dentro das categorias, a partir daquelas correlações;

- Aprendizagem por correção de erro – É aplicável para treinamento de redes neurais com aprendizado supervisionado, e é tratado determinando o sinal de erro entre a resposta gerada e a resposta desejada e então realizar ajustes nos pesos sinápticos de forma a minimizar este erro;

- Aprendizado baseado em memória – As situações apresentadas à rede são corretamente classificadas e armazenada em uma memória que servirá como base nas próximas classificações;

- Aprendizado Competitivo – Os neurônios de determinada rede neural competem entre si através de um processo de inibição mútua, de forma que esta competição determine apenas um neurônio ativo que será à saída da RNA;

A capacidade de retreinar uma rede neural fornece características muito interessantes. Sempre que se queira introduzir um novo padrão para que ela passe a reconhecê-lo, basta retreiná-la, só que agora com este novo padrão fazendo parte do conjunto de padrões de treinamento. Esta característica fornece uma habilidade de adaptação que é necessária em algumas aplicações, quando o conjunto de padrões que a rede terá que reconhecer não é constante, mas pode apresentar variações no decorrer do tempo. Em um sistema de reconhecimento de caracteres esta é uma propriedade pouco útil, já que seria extremamente difícil ocorrer mudanças nas letras que formem o alfabeto, já em um sistema de detecção de intrusão, esta característica é de fundamental importância, pois confere ao sistema este poder de adaptabilidade.

3.3 Topologias das Redes Neurais

A definição da topologia de rede neural é um fator significativo para a definição deste projeto, desta forma é apresentado cada topologia e seus benefícios para este projeto.

Segundo (RUMELHART 1986), a rede neural deve possuir no mínimo duas camadas, a de entrada de dados e a da saída dos resultados. Como a rede apresenta desempenho muito limitado com somente duas camadas, a adição de uma camada intermediária faz-se necessária. Neste tipo de configuração, cada neurônio está ligado com todos os outros das camadas vizinhas, mas neurônios da mesma camada não se comunicam além da comunicação ser unidirecional, apresentando assim um comportamento estático. As seguintes seções apresentam às principais topologias.

3.3.1 Redes Alimentadas a Diante

As redes alimentadas adiante se caracterizam por não possuir ciclos de realimentação de neurônios, sendo que o processo sináptico ocorre diretamente da camada de entrada em direção a camada de saída.

Esta classificação pode se ramificar também para três aspectos:

- Rede Alimentada Adiante com Camada Única;

- Rede Alimentada Adiante com Múltiplas Camadas;

- Rede Neural Recorrente – São sistemas dinâmicos, ou seja, quando um novo padrão de entrada é apresentado, as saídas dos neurônios são calculadas e devido aos desvios de realimentação, as entradas de cada neurônio são modificadas, o que leva a rede a entrar em um novo estado;

3.3.2 Perceptron

Na família de redes diretas mais comuns os neurônios são organizados em camadas que possuem conexões unidirecionais entre eles. Conectividades diferentes resultam em diferentes comportamentos para a rede. Genericamente falando, redes diretas são estáticas, produzindo a partir de uma entrada, somente um conjunto de valores de saída, ao invés de uma seqüência de valores. Redes diretas são classificadas com ou sem memória, no sentido de que sua resposta para uma dada entrada é independente do estado anterior da rede.

- Perceptron Com Camada Única – Cada neurônio da camada de entrada é diretamente conectado a cada neurônio da camada de saída. Neste caso as entradas da rede são diretamente mapeadas em um conjunto de padrões de saída, não sendo possível a formação de uma representação interna. Porém este modelo possui sérias deficiências já que em situações com entradas similares, mas que façam parte de classificações diferentes, não é identificado. Segundo (HAYKIN 2001) para o perceptron funcionar adequadamente, o padrão a ser classificado, preciso estar linearmente separado;

- Perceptron Com Múltiplas Camadas – Devido a esta limitação foi desenvolvida o modelo com múltiplas camadas, ou seja, com camadas internas. Basicamente, este tipo de rede é composto por neurônios estruturados em uma camada de entrada, uma ou mais camadas ocultas e uma camada de saída, onde o sinal se propaga para frente entre as camadas, realizando funções específicas em cada passo;

3.4 Considerações

A teoria das redes neurais foi desenvolvida entre as décadas de 40 e 50. De lá para cá, se realizou muitos avanços nas pesquisas, entretanto percebe-se que os conceitos fundamentais ainda permanecem O Objetivo deste capítulo foi de apresentar uma visão geral sobre estes conceitos, para que se possa compreender de uma forma mais profunda, como a aplicação I-IDS efetua seu aprendizado e generalização. As classificações e topologias de rede, também representam um ponto fundamental para definição e realização do projeto, já que um planejamento errado destas questões pode comprometer significativamente, a eficiência deste modelo.

4. Redes Móveis Ad Hoc

Neste capítulo são apresentados os conceitos sobre as redes móveis sem fio Ad Hoc, passando por sua definição, características e classificação. Também são apresentados os dois protocolos mais utilizados atualmente o AODV e o OLSR, sendo o segundo utilizado neste trabalho. Nos estudos de (DUARTE e Antonio Alexandre de Castro 2003), (LIMA 2005), (TAMASHIRO 2007), (TONNESEN 2004), (RODRIGUES 2004), (JULIO 2007) as características das redes Ad Hoc são abordadas.

4.1 Definição

Existem duas classificações de redes sem fio, a primeira são as redes com infra-estrutura onde o host móvel, está em contato direto com um ponto de acesso, ou seja, todo o tráfego de dados deve necessariamente passar por um ponto central, mesmo que os equipamentos estejam a uma distância em que poderiam se comunicar diretamente. Na figura 6 este modelo de rede é representado através de uma aplicação bastante utilizada hoje em dia, a telefonia celular, onde mesmo se dois pontos de acesso estiverem localizados a poucos metros um do outro, é necessário que o tráfego vá para o transmissor da infra-estrutura da rede e retorne.

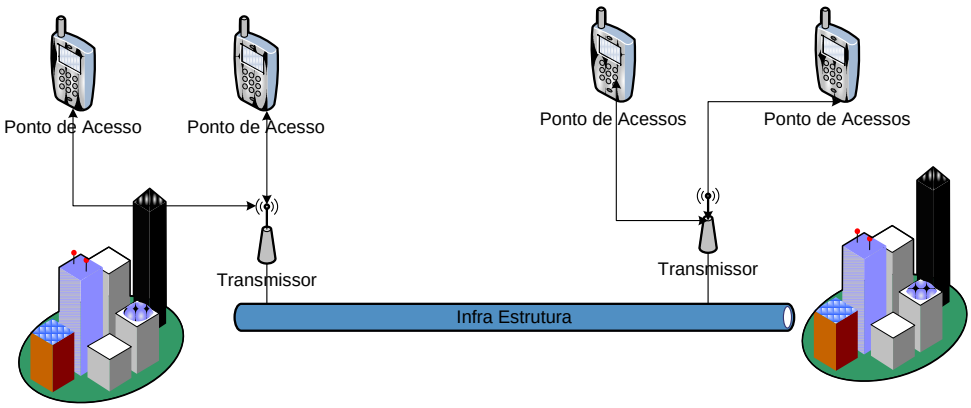

Figura 6 - Arquitetura de Rede com Infra-Estrutura

Na segunda classificação de redes móveis sem fio é a rede Ad Hoc, que é o ponto focal deste trabalho, os dispositivos são capazes de trocar dados diretamente entre si, ou seja, não há pontos de acesso ou estações de suporte a mobilidade, sendo que os nós dependem um do outro para manter a conexão.

Uma rede sem fio Ad Hoc móvel, também conhecida como MANET, é uma rede formada por dispositivos de comunicação móveis (nós) que se comunicam através de enlaces sem fio, na ausência de infra-estrutura fixa e de controle centralizado (backbone ou estação base). A topologia não é predeterminada e a responsabilidade por organizar e controlar a rede é distribuída entre os nós. Estes são responsáveis por descobrir, dinamicamente, com quais podem se comunicar diretamente e por encaminhar pacotes, cujos destinos não estão no raio de alcance de suas origens.

Cada nó de rede é capaz de se movimentar, conectar e transmitir dados dinamicamente e de maneira arbitrária, ou seja, nela cada unidade de rede pode descobrir e manter rotas de comunicação conforme é demonstrado na figura 7, onde cada um dos nós seja um PDA, um computador ou um ponto de acesso se comunica diretamente sem um ponto centralizador. Estas características serão mais detalhadas na seção a seguir.

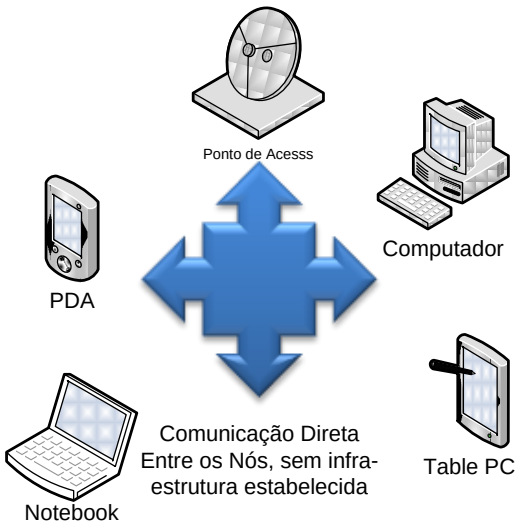

Figura 7 - Arquitetura de Rede Ad Hoc

4.2 Características

A rede Ad Hoc é caracterizada, principalmente devido sua autonomia e a ausência de infra-estrutura. Cada nó de uma rede Ad Hoc se move de forma arbitrária, conseqüentemente alterando a topologia, alterando as rotas e partições da rede.

Outra característica importante é o fato de todos os nós funcionarem como um roteador encaminhando pacotes para destinos que não estão no raio de alcance de suas origens

Para este modelo podem ser citadas diversas outras vantagens:

- Tolerância a Falhas – A ausência de uma estrutura fixa permite uma enorme mutabilidade das rotas, assim não há um ponto único de falhas;

- Conectividade – Dois nós localizados próximos fisicamente podem se comunicar diretamente sem a necessidade de trafegar até um ponto central da rede requerendo um maior tráfego de dados;

- Flexibilidade – Devido a sua característica dinâmica e sem a necessidade de uma pré-existência de infra-estrutura, podem ser rapidamente estabelecidas;

- Instalação Rápida e de Baixo Custo – Devido ao fato de não requerer infra-estrutura, as redes Ad Hoc não possuem a necessidade da passagem de cabos e outras infra-estruturas, que podem encarecer o projeto e a manutenção;

- Implantação Incremental – redes sem fio geograficamente distribuídas baseadas em redes sem fio ad hoc móveis podem ser implantadas de forma incremental, ou seja, não há a necessidade de que toda a rede esteja funcionando para que uma parte possa ser utilizada;

Porém as redes Ad Hoc também possuem pontos críticos que devem ser analisados de acordo com a necessidade de aplicação e que devem ser analisados na fase de projeto da rede:

- Segurança – Devido à disponibilidade do meio físico estar aberta, em termos de acesso, as redes móveis são um desafio a segurança de transmissão de dados, confidencialidade de informações.Há uma maior possibilidade de ataques de escuta, de negação de serviço, de injeção de falsos pacotes ou de modificação dos pacotes;

- Detecção de Falhas e Gerenciamento – Devido sua arquitetura a detecção de falhas e o gerenciamento da rede se tornam mais complexas e mais custosas;

- Implementação dos Protocolos de Roteamento – A complexidade das possibilidades de roteamento dificultam a implementação das redes Ad Hoc;

- Erros de Transmissão – Devido à mobilidade desta categoria de rede, a perda de pacotes está mais susceptível;

- Ausência de Infra-Estrutura – A ausência de infra-estrutura pode ser um fator crítico na utilização em meios mais extremos, como por exemplo, o tempo de vida das baterias dos dispositivos;

- Largura de Banda Limitada – Nesta categoria as redes possuem enlaces com capacidade limitada e inconstante devido a outras variáveis como o acesso múltiplo, interferência, enfraquecimento do sinal;

4.3 Classificação

As Redes AD HOC podem ser classificadas pelos seguintes parâmetros:

- Quanto a Simetria - As redes simétricas são caracterizadas por todos os nós da rede possuir a mesma capacidade, e de dividir as responsabilidades de forma idêntica. Já as redes assimétricas, os nós podem possuir características diferentes, como o raio de transmissão, capacidade de processamento, deslocamento e características de roteamento;

- Quanto ao tráfego de dados - Esta classificação é um dos pontos fundamentais para um projeto de uma rede Ad Hoc, já que de acordo com a necessidade do tráfego, deve ser definido o protocolo utilizado e capacidade dos nós, pois cada rede pode transferir dados normais, ou dados em tempo real de aplicações multimídia;

- Quanto ao método de roteamento – O método de roteamento pode ser utilizado de modo *unicast*, *multicast* ou *geocast* e os métodos de endereçamento podem ser baseados no host, baseados no conteúdo ou até mesmo na capacidade;

- Quanto à taxa de transmissão – A taxa de transmissão necessária deve ser prevista de acordo com a necessidade das aplicações;

- Quanto à segurança necessária – Os requisitos de segurança são pontos fundamentais para o projeto da rede, em determinadas situações há necessidade de elevada segurança como em aplicações militares;

4.4 Utilidade e Aplicações

Historicamente as redes Ad Hoc começaram a ser utilizadas em operações militares, devidos suas características. Com o avanço da tecnologia e pesquisa e também pelas facilidades desta arquitetura, foram desenvolvidas diversas outras aplicações a nível civil, comercial e militar, que são apresentadas na tabela 1.

Tabela 1- Aplicações de Rede Ad Hoc

Aplicações	Serviços
Redes Táticas	Comunicação em operações militares entre soldados de infantaria e veículos, batalhas automatizadas
Redes de Sensores	Monitoramento de Residências, medições de parâmetros como umidade, temperatura, radiação nuclear, monitoração de dados como de atividades sísmicas
Emergências	Operações de Busca e Resgate e a substituição da infra-estrutura fica em caso de terremoto e furações
Ambientes Comerciais	Negócios - acesso dinâmico a arquivos armazenados em uma localização central, escritório móvel Serviços em veículos: transmissão de noticias, condições de estrada, tempo e música, formação de redes entre veículos próximos
Aplicações Educacionais	Configuração de salas de aula virtuais ou salas de conferências Criação de uma rede para comunicação rápida em conferências, encontros e palestras
Redes Mesh	Conexão a Internet em zonas residenciais Auto-Estradas: Comunicação para os automóveis Alternativa rede de celulares
Entretenimento	Acesso a internet em ambientes abertos Jogos entre múltiplos jogadores
Localização de Serviços	Serviços de informação: Localização de serviços como postos de Gasolina
Televisão digital	Aplicações e Extensão dos serviços de Televisão Digital

Fonte: Baseado em (MURTHY e MANOJ 2004)

Outro aspecto importante é a crescente demanda de dispositivos móveis como PDAs, notebooks, celulares e outros dispositivos portáteis com interface a redes sem fio, possibilitando o desenvolvimento desta tecnologia e o seu raio de aplicações.

4.5 Arquitetura da Rede Ad Hoc

A arquitetura de uma rede Ad Hoc é composta basicamente por cinco camadas: física, enlace de dados, rede, transporte e aplicação. As duas primeiras camadas, física e de enlace de dados são definidas pelo padrão 802.11.

A principal função da camada de rede é rotear pacotes de uma máquina origem para uma ou mais máquinas destino. Um algoritmo de roteamento é a parte do software da camada de redes responsável pela decisão sobre a linha de saída a ser usada na transmissão do pacote de entrada (TANENBAUM 1996).

Protocolos usados em redes tradicionais não podem ser utilizados diretamente em rede sem fios Ad Hoc móveis, devido à topologia dinâmica, ausência de infra-estrutura estabelecida para a administração centralizada, enlaces sem fio com limitação da largura de banda e nós com recursos restritos. (TAMASHIRO 2007)

Para a camada de transporte, no caso de rede Ad Hoc, não se pode utilizar diretamente o protocolo TCP devido suas características, como a má

interpretação de perda de pacotes, quebra de enlaces freqüentes, enlaces assimétricos. Existem duas soluções para a camada de transporte, a primeira utilizando o protocolo UDP onde ou através de mecanismos de otimização para o protocolo TCP.

4.5.1 Algoritmos de Roteamento

Nesta seção, serão apresentadas as características desejadas de um algoritmo de roteamento para redes Ad Hoc móveis, e resumidamente os principais protocolos desenvolvidos.

Como o objetivo deste trabalho é utilizar o protocolo OLSR, nesta seção será dado um enforque maiores as características e operação deste protocolo.

Segundo a IETF, existem características específicas que são desejáveis a protocolos e algoritmos de roteamento, em uma rede Ad Hoc. Estas características estão descritas na tabela 2.

Tabela 2 – Características Desejáveis dos Algoritmos Ad Hoc

Característica	Descrição
Operação Distribuída	Propriedade essencial para o roteamento em uma rede Ad Hoc para evitar a centralização que leva à vulnerabilidade.
Protocolo Livre de Loops	O algoritmo de roteamento deve evitar a formação de loops, mesmo que seja por curtos intervalos.
Operação Baseada em Demanda	O algoritmo de roteamento deve ser adaptável às condições de tráfego, ou seja, as rotas são criadas somente quando um nó fonte deseja estabelecer uma comunicação. Se isto for feito de forma inteligente, os recursos de energia e largura de banda serão utilizados de forma mais eficiente. Neste caso o preço pago é o tempo de descoberta de uma rota.
Operação Pró-Ativa	Em alguns momentos, a latência adicionada pela operação baseada na demanda poderá ser inaceitável, por isso, se os recursos de energia e largura de banda permitirem, operações pró-ativas (onde rotas são previamente armazenadas em tabelas de roteamento) serão recomendadas;
Segurança	Se as camadas de rede e de enlace não garantirem segurança, por isso, os protocolos de roteamento MANET estarão vulneráveis a muitas formas de ataques. É necessário então, que haja mecanismos para inibir modificações nas operações dos protocolos.
Operação nos Períodos de Inatividade dos Nós	Como resultado da conservação de energia ou de alguma outra inatividade, os nós devem parar de transmitir e/ou receber dados por um período arbitrário de tempo, sem que isto resulte em maiores conseqüências,
Suporte a Enlaces Unidirecionais	Uma rede Ad Hoc assume enlaces bidirecionais e muitos algoritmos são incapazes de funcionar corretamente sobre enlaces unidirecionais. Entretanto, enlaces unidirecionais podem ocorrer em redes sem fio.

4.5.2 Classificação dos Protocolos

Os protocolos de roteamento possuem diversas classificações que serão descritos a seguir. Na figura 8 também é apresentado um modelo resumido de classificação dos tipos de protocolos Ad Hoc, baseado no trabalho de (TAMASHIRO 2007).

Os protocolos podem ser classificados de acordo com o mecanismo de atualização das informações de roteamento:

Protocolos Pró-Ativos – São aqueles que utilizam tabelas de roteamento para manter a consistência das informações de roteamento em todos os nós. O algoritmo tenta avaliar continuamente as rotas, de modo que quando um pacote necessitar de encaminhamento, a rota já seja conhecida e possa ser utilizada imediatamente. Neste caso, os nós mantêm uma ou mais tabelas com informações referentes à rede e respondem a mudanças na sua topologia propagando atualizações de modo a manter a consistência da rede. Estas atualizações são iniciadas por mecanismos de temporização, o que faz com que haja sempre um número constante de transmissões em andamento, mesmo quando a rede esteja em equilíbrio.

Protocolos Reativos – Criam e mantém rotas somente quando desejado por um nó. Nos algoritmos reativos a rota é determinada sob demanda, ou seja, quando uma rota é requerida, ele inicia algum procedimento de descobrimento de rota. Desta forma, o processo é iniciado por um pacote necessitando encaminhamento. Uma vez que a rota é descoberta, utiliza-se algum procedimento de manutenção de rota para que ela continue ativa. Como a chegada de um pacote necessitando de encaminhamento é algo aleatório, estes protocolos não trocam mensagens a intervalos regulares, o que economiza banda passante e energia. Porém, estes algoritmos apresentam um maior atraso no encaminhamento da mensagem.

Protocolos híbridos – combinam as duas abordagens citadas anteriormente. Para cada nó, é definida uma área, chamada zona de roteamento, que contem os vizinhos pertencentes a uma área geográfica especifica ou distantes, no máximo em n saltos deste nó. Para rotear pacotes dentro de sua zona executam um algoritmo pró-ativo e para fora, reativo.

De acordo com uso de informações temporais para roteamento:

- Utilização do Histórico – as decisões de roteamento são tomadas com base no estado dos enlaces;

- Utilização da Predição – As decisões de roteamento são tomadas com base na suposição do estado futuro dos enlaces, considerando informações como bateria, localização e outros;

De acordo com a organização da topologia:

- Protocolos Flat: todos os nós possuem o mesmo papel durante o roteamento;

- Protocolos com topologia hierárquica: os nós são organizados hierarquicamente e a responsabilidade pelo roteamento restringe-se a alguns nós;

De acordo com os recursos específicos utilizados:

- Protocolos com controle de energia: as decisões de roteamento são tomadas considerando a redução do consumo de energia;

- Protocolos que usam informações geográficas: as posições dos nós são obtidas através de um GPS;

- Protocolos com inundação eficiente: métodos são aplicados para que os pacotes sejam difundidos eficientemente;

De acordo com o tipo de transmissão:

- *Unicast*: Um nó envia pacotes para um único destino;

- *Multicast*: Um nó envia pacotes para um subconjunto de destinos. Baseados na topologia podem ser divididos em *mesh-based* e *tree-based*. Protocolos *mesh-based* constroem uma malha entre os nós, portanto, pode haver vários caminhos entre cada par origem-destino. Protocolos tree-based constroem arvores para conectar os nos e há um único caminho entre cada par origem-destino;

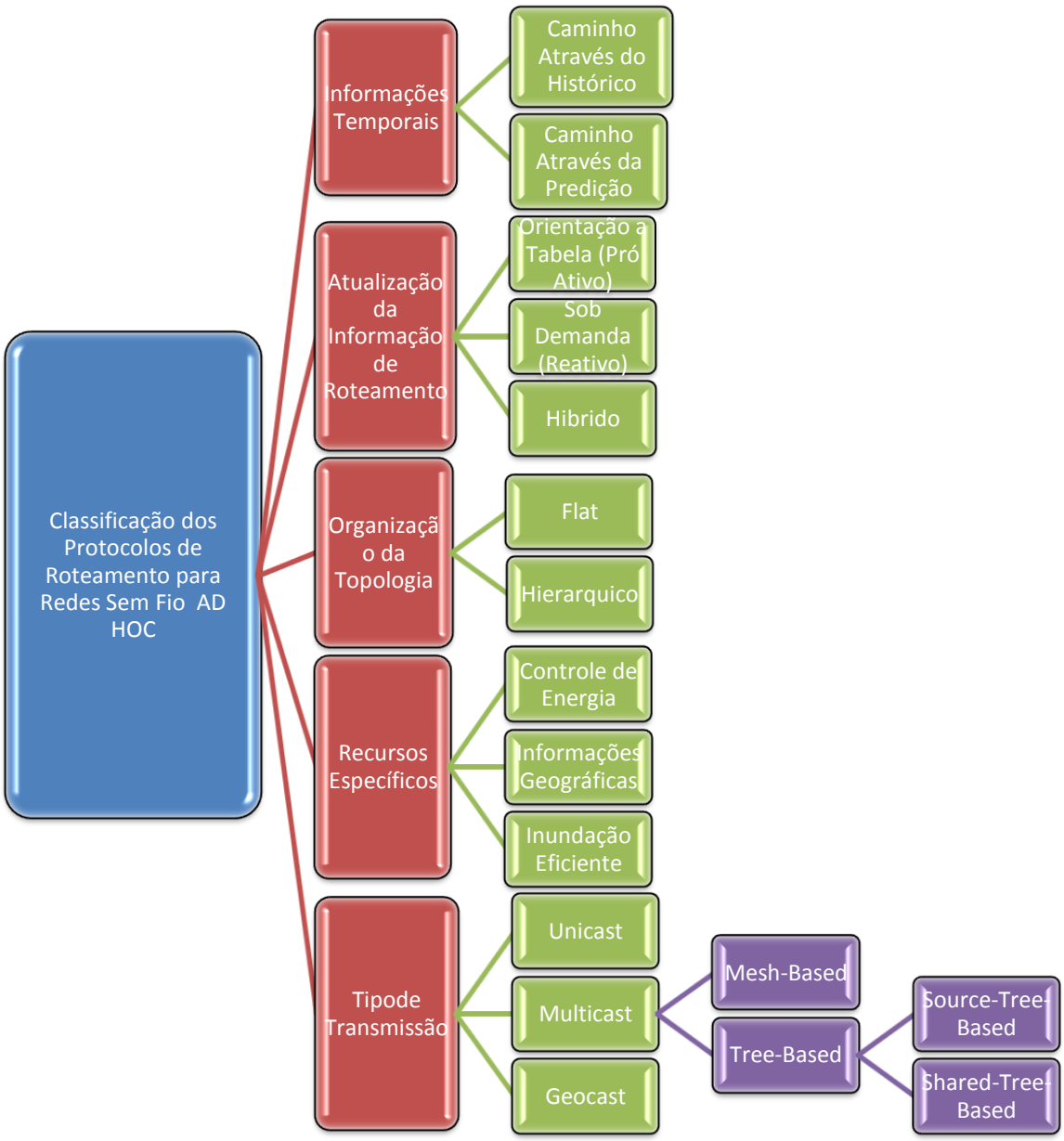

Figura 8 - Classificação de Protocolos Ad Hoc

A seguir é apresentada a tabela 3, que demonstrada os protocolos Ad Hoc desenvolvidos com suas específicas classificações. Alguns possuem características especiais como segurança, que dependendo da aplicação podem trazer benefícios ao projeto, porém como o intuito deste trabalho não é de utilizar ou testar vários protocolos, somente será detalhado o protocolo AODV e OLSR, que porventura possui características importantes a este projeto que serão citadas mais a diante.

Tabela 3 - Protocolos Ad Hoc

<table>
<tr><td colspan="10">Protocolos de Roteamento Ad Hoc</td></tr>
<tr><td colspan="2">Pro-Ativos</td><td colspan="4">Reativos</td><td colspan="4">Híbridos/Outros</td></tr>
<tr><td>DSDV (Flat)</td><td>WRP(Flat)</td><td rowspan="3">AODV</td><td rowspan="3">DSR</td><td>LRM</td><td>ABR</td><td>CEDAR</td><td>STARA</td><td colspan="2">ZRP</td></tr>
<tr><td colspan="2" rowspan="2">CGSR (hierar)</td><td rowspan="2">TORA</td><td>SSR</td><td colspan="4">ZHLS</td></tr>
<tr><td>SSA</td><td colspan="4">SLURP</td></tr>
<tr><td colspan="2">GSR</td><td colspan="4">ROAM</td><td colspan="4">DST</td></tr>
<tr><td colspan="2">STAR (LS)</td><td colspan="4">RDMAR</td><td colspan="4">DDR</td></tr>
<tr><td colspan="2">DREAM (Flat)</td><td colspan="4">LAR</td><td colspan="4" rowspan="5">FSR (descendente do GSR)</td></tr>
<tr><td colspan="2">MMWN</td><td colspan="4">ARA</td></tr>
<tr><td colspan="2">HSR (Hierárquico)</td><td colspan="4">FORP</td></tr>
<tr><td colspan="2">OLSR (LS – Flat)</td><td colspan="4">CBRP</td></tr>
<tr><td colspan="2">TBRPF (LS – Flat)</td><td colspan="4"></td></tr>
</table>

4.6 Protocolo AODV

O On-Demand Distance Vector Routing (AODV) foi padronizado e descrito pelo grupo de trabalho MANET da IETF (RFC3561 2003), onde está disponível toda sua documentação que é descrita resumidamente neste trabalho. Permite a utilização de milhares de nós móveis e a comunicação entre estações, através da cooperação no roteamento de pacotes de dados entre a origem e o destino.

No trabalho de (FILHO 2005), é descrito o protocolo AODV e simulado o funcionamento deste protocolo, bem como explorada diversas brechas de segurança relativas a este protocolo.

Funcionando sobre demanda, possui características não hierárquicas e toda operação é iniciado pela fonte de dados. A idéia é balancear a atualizações das informações de roteamento e a latência, de encontrar uma rota para o destino quando necessário. Com isto tenta minimizar a sobrecarga, com transmissões de informações de roteamento e assim evitando o desperdício de banda, memória e processamento.

De acordo com a classificação citada anteriormente trata-se de protocolo reativo, portando sua utilização não necessita da prévia definição de uma rota, ele é capaz de manter rotas unidirecionais e multidirecionais, também tem por característica um mecanismo de detecção de rotas inválidas. Na próxima seção será demonstrada sua operação de fato.

Iniciando uma demanda de comunicação entre um nó e outro, ou quando a rota armazenada estiver inválida ou em desuso, o protocolo inicia o processo de descoberta de uma rota com o *brodcast* de pedidos de rota (route request – RREQ), estes pacotes são retransmitidos por todos os nós vizinhos ao nó requisitante, que por sua vez, retransmitem aos seus vizinhos. Este processo respeita uma característica conhecida como *Expanding Ring Search* que defini

um critério para o máximo de retransmissões visando evitar uma provável inundação desnecessária de pacotes de pedidos de roda em uma rede.

O valor que está no campo “Número de seqüência do destino” na mensagem RREQ é o ultimo número de seqüência conhecido para o destino requerido e é copiado do respectivo campo na tabela de roteamento. Caso o número de seqüência não é conhecido, o marcador de *unknown sequence number* deve estar ativo na mensagem.O protocolo utiliza tal número de seqüência para assegurar que não ocorram laços durante a busca pela rota.Assim cada nó mantêm uma entrada na sua tabela de roteamento com seu número de seqüência do destino, sempre associado ao endereço de IP do destino.Este número é atualizado toda vez que o nó receber informações novas de mensagem relacionadas ao destino.

Quando o nó destino recebe o pacote com a solicitação de rota, envia um pacote de resposta (route reply – RREP), que é retransmitido em *unicast* pelo caminho reverso criado pelo RREQ. Outro nó, que não tenha o destino, mas que tenha uma rota atualizada para aquele destino também pode responder ao pedido de rota.

Caso a mensagem de RREP contiver um número de seqüência maior ou com o mesmo número de seqüência e com o contador de saltos menor, o nó atualiza a tabela de roteamento para este destino e passa a utilizá-lo.

As falhas no processo de encaminhamento de informação pela rota criada são relatadas através da transmissão de pacotes de erro de rota (route error – RERR), assim todos os dispositivos que constituem a rede podem ter participação ativa nos processos de roteamento e encaminhamento de pacotes, agindo como roteadores.

No processo de transmissão do RREQ os nós intermediários guardam a rota reversa do pedido de utilização futura e descartam pedidos repetidos graças aos números de seqüência de pacotes. De maneira análoga, a transmissão de pacotes RREP pelo nó de destino ou por outro com a rota suficientemente atualizada para o destino leva os nós intermediários a armazenar rotas para o destino requerido. As falhas de enlace no caminho entre o nó requisitante e nó destino são sinalizadas pelos nós intermediários aos seus antecessores pelos pacotes RERR até que se atinja o nó que requisitou, que deve então iniciar um novo processo de descoberta de rota.

O termo Distance Vector diz respeito ao algoritmo utilizado para estimar a menor distância, em termos de número de saltos, de um nó até os outros. Cada nó da rede armazena, para cada destino de rede, a partir de cada vizinho a rota com menor custo distância. Desta forma cada nó da rede garante as que as retransmissões serão feitas pelas rotas mais curtas disponíveis naquele momento.

Abaixo é representado o envio de uma mensagem RREQ do nó A para o nó o F.O nó A repassa a requisição a todos os nós alcançáveis e assim seqüencialmente até alcançar o nó F.

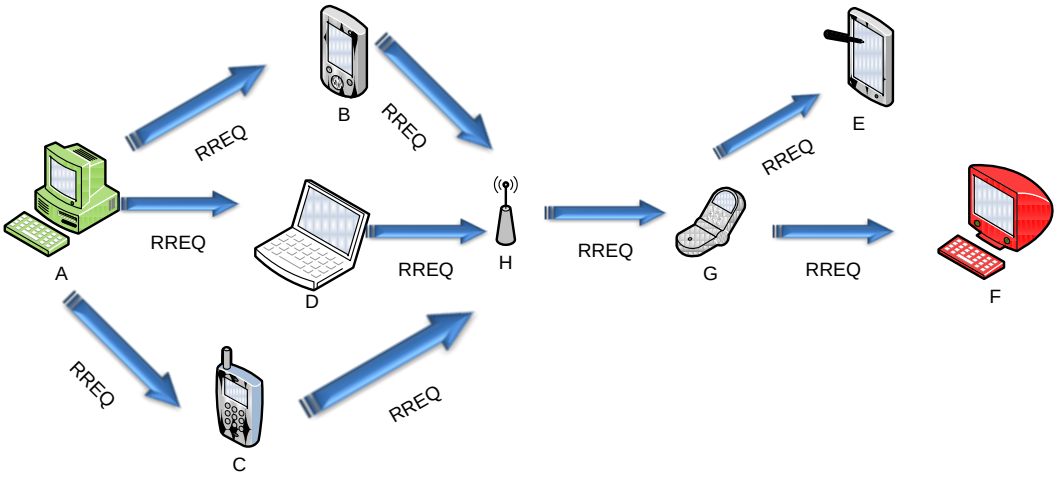

Figura 9 - Fluxo de Mensagens RREQ

Após finalizar o processo de RREQ, o nó F identifica a melhor rota e responde com a mensagem RREP.

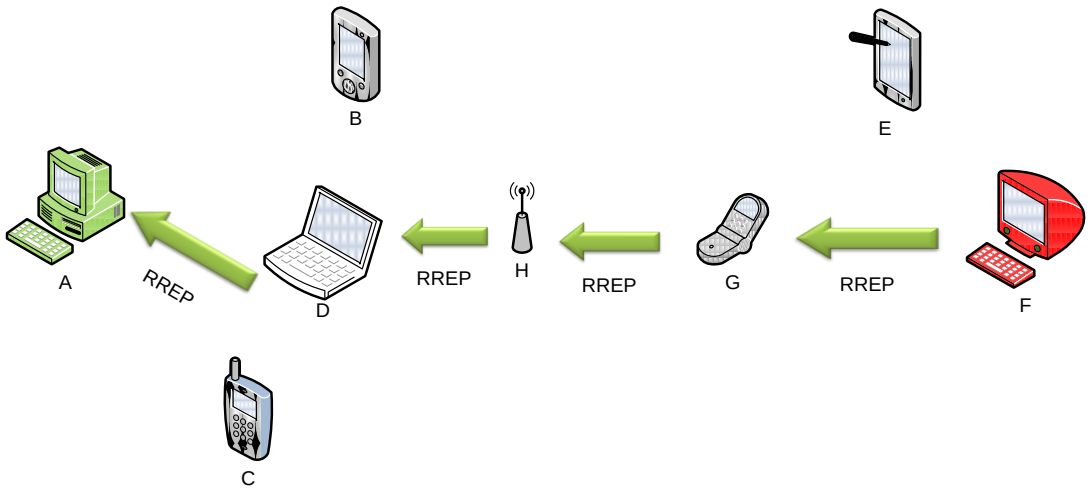

Figura 10 - Fluxo da Mensagem RREP

Todas as rotas descobertas são mantidas em tabelas de roteamento tradicionais de uma entrada por destino, apenas rotas em uso são armazenadas e um mecanismo de espira as rotas não utilizadas recentemente, o objetivo deste esquema é a adaptação do mecanismo ás mudanças na topologia da rede e adicionalmente melhorar a utilização dos recursos do dispositivo e da rede. Outra característica do AODV é o número de seqüência que cada pacote de roteamento carrega e que é associado a cada entrada da tabela de roteamento e serve para determinar a informação de roteamento mais atual e evitar *loops* na construção das rotas, contornando o problema de contagem infinita do algoritmo de vetor de distâncias. O número de seqüência é colocado em cada pacote por seu nó originado, que é responsável por incrementá-lo mono tonicamente a cada nova informação de roteamento recebida ou gerada.

O protocolo AODV também pode utilizar transmissões de mensagens em broadcast voltadas a informar a vizinhança sobre a presença do nó.Abaixo está descrito as informações que ficam registradas na tabela de roteamento dos nós com a utilização do protocolo AODV:

Tabela 4 - Tabela de Roteamento AODV

Item	Descrição
IP do Destino	Endereço de IP do nó destino da rota
Número de Seqüência	Número de Seqüência associado à entrada na tabela
Validade do Número de Seqüência	Indicador da validade do número de seqüência de entrada na tabela
Interface de Rede	Interface de Rede utilizada para enviar pacotes por essa rota
Contagem de Saltos	Números de saltos necessários para alcançar o destino
Próximo Salto	Endereço de IP do nó vizinho par onde serão encaminhados aos pacotes com esse destino
Lista de Percussores	Lista de nós vizinhos que encaminham pacotes para o destino por essa rota
Tempo de Vida	Tempo a partir do qual essa rota irá expirar se ociosa
Flags de Roteamento	Usadas para representar algumas situações da entrada, como reparabilidade, validade e origem
Estado da Rota	Validade das informações dessa entrada na tabela

4.6.1 Formato de uma Mensagem de Requisição de Rota

O formato desta mensagem é ilustrado através da figura 11, ela é constituída de um pacote de 160 bits. Destes 32 bits definem o tipo onde J e R indicam comunicação multicast, G indica se uma RREQ deve ser enviada ao destino por um nó intermediário, D indica que somente um destino pode responder a esta requisição, U representa o número de seqüência do destino desconhecido.

Já os outros 128 bits são campos caracterizados por:

- RREQ ID: Identifica juntamente com o endereço da fonte, um pedido de requisição de rota;

- Contador de Saltos: Informa o número de saltos do nó de origem para o nó corrente;

- Número de Seqüência do Destino (32 bits): Contem o ultimo número de seqüência recebido pela fonte, referente alguma rota para o destino;

- Número de Seqüência da origem (32 bits): Contem o número de seqüência atual;

- Endereço IP Destino (32 Bits): Indica o endereço de IP do nó final da rota;

- Endereço IP Origem (32 Bits): Indica o endereço de IP do nó de origem;

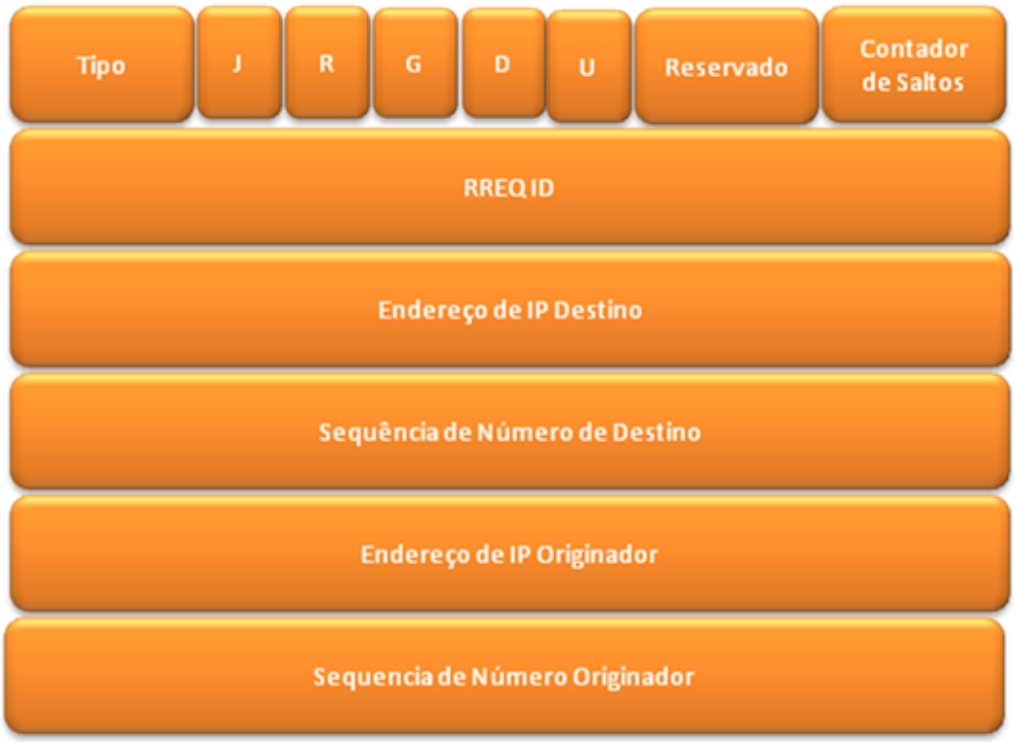

Figura 11 - Formato da Mensagem de Requisição de Rota

4.6.2 Formato de uma Mensagem de Resposta de Rota

A RREP é caracterizada por uma mensagem com forma de um pacote de 160 Bits sendo composta pelos campos abaixo detalhados:

- Tipo R ou A (32 Bits): O R indica comunicação multicast (*Repair*), já o A indica a necessidade de transmissão de uma confirmação de recebimento de resposta (RREP-ACK) pelo nó fonte;

- Tamanho do Prefixo (cinco bits): Especifica que o próximo salto indicado, pode ser usando por algum nó com o mesmo prefixo do destino desejado;

- Contador de Saltos: Informa o número de saltos do nó de origem até o nó corrente;

- Endereço IP Destino (32 Bits): Indica o endereço de IP do nó final da rota;

- Endereço IP Origem (32 Bits): Indica o endereço de IP do nó de origem;

- Número de Seqüência do Destino (32 bits): Contem o ultimo número de seqüência recebido pela fonte, referente alguma rota para o destino;

- Tempo de Vida: Indica o tempo em milissegundos para cada nó receber o RREP, considerando a rota válida;

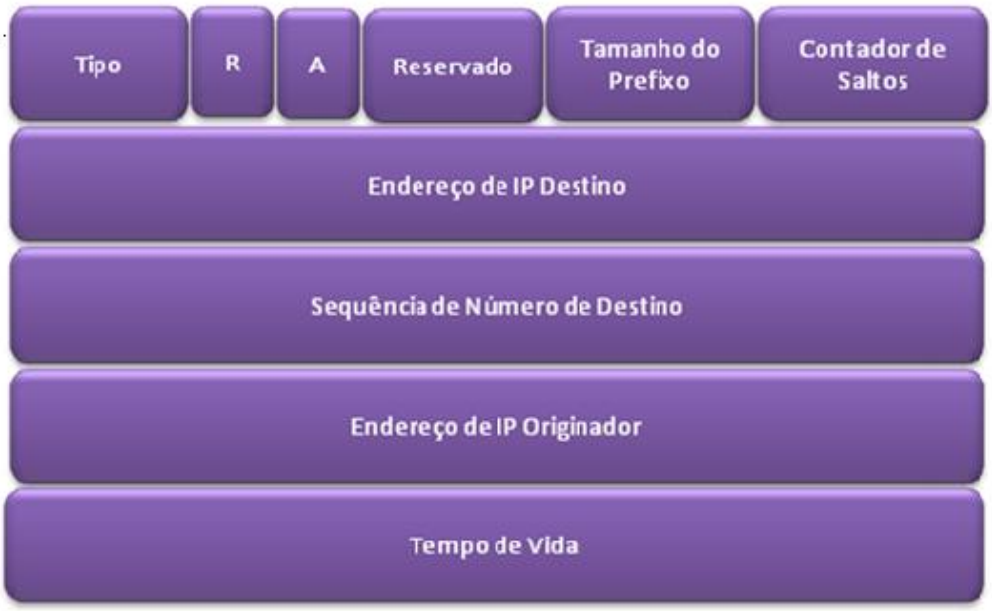

Figura 12 - Formato da Mensagem de Resposta de Rota

4.6.3 Formato de uma Mensagem de Erro de Rota

Esta mensagem é enviada toda vez que ocorre uma quebra do enlace e torna um ou mais vizinhos inalcançável para algum nó de destino. Ela é composta inicialmente pelo campo tipo onde o N indica que um nodo reparou o enlace e que os nós subseqüentes não devem apagar a rota.

O campo contador de destino efetua a contagem do número de destinos inalcançáveis e deve ser no mínimo um. O endereço de IP inalcançável indica

o endereço de IP do destino se tornou invalido, os demais campos seguem o mesmo padrão da RREQ e RREP.

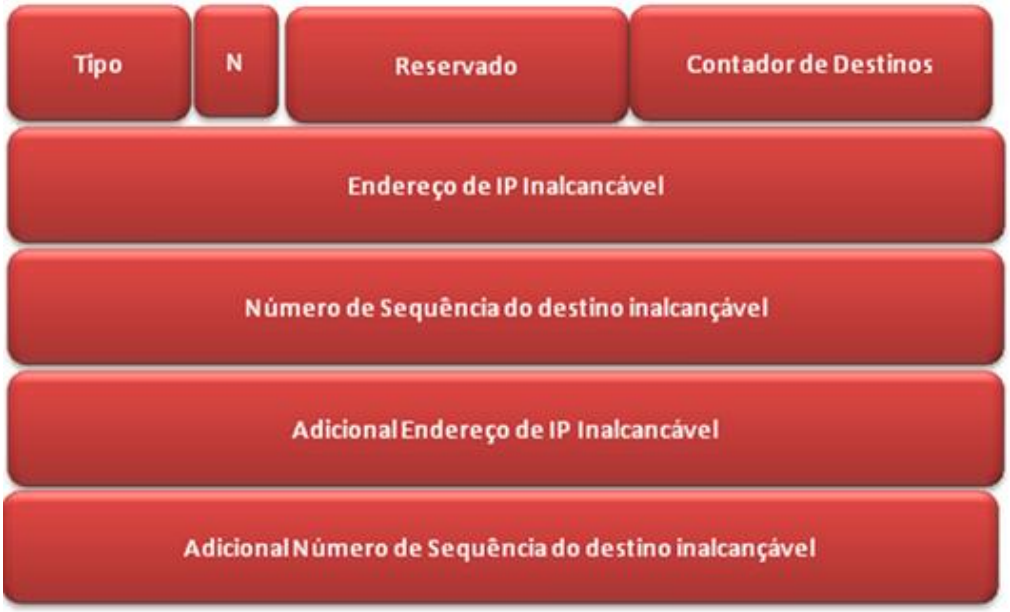

Figura 13 - Formato da Mensagem de Erro de Rota

4.7 Protocolo OLSR

Esta seção descreve aspectos básicos sobre o protocolo OLSR (Optimized Link State Routing), protocolo que foi utilizado na parte prática deste trabalho e está baseado no documento do (Network Working Group 2003).Este protocolo possui características interessantes pois foi projetado para trabalhar de forma totalmente distribuída, desta forma, não dependendo de nenhuma entidade central.Ele não exige a transmissão confiável de mensagens de controle, podendo suportar perdas razoáveis destas mensagens, característica fundamental , já que perdas de pacotes são situações freqüentes em transmissões via rádio.Outra característica deste protocolo não exige a entrega de mensagens em seqüência, isto é realizado através de uma informação de seqüência embutida em cada mensagem.

O OLSR é um protocolo de roteamento proativo, ou seja, ele atualiza informações de topologia com outros nós da rede regularmente. O Conceito chave deste protocolo é o uso de multipoint relays (MPR), que são nós selecionados para encaminhar as mensagens de difusão no processo de inundação do protocolo de roteamento. Somente os nós selecionados como MPRs fazem esta difusão de informação na rede. O uso de MPRs combinado com a eliminação local da duplicidade é usado para minimizar o número de pacotes de controle enviados na rede. O OLSR é projetado para trabalhar em redes de larga escala, onde o tráfego é randômico e esporádico entre um conjunto de nós. Como utiliza o modelo de protocolo pró-ativo , o OLSR é também adequado para os cenários onde pares de nós que se comunicam, mudam constantemente.

Os nós selecionados como MPR possuem também uma responsabilidade especial quando declararem o status da rede, além de identificar rotas com caminhos mais curtos o MPR deve declarar seu status para seus seletores que também são MPRs. Desta forma os MPRs são utilizados para o cálculo da rota e para tornar as inundações efetuadas na rede mais eficientes. Para fins mais didáticos é demonstrado na figura 14, o processo de alagamento normal e comparado com o processo de alagamento com MPR.

Os nós que executam o OLSR utilizam mensagens HELLO, trocadas entre vizinhos de um salto, para detectar e atualizar o seu conjunto de vizinhos. Cada nó, periodicamente faz uma difusão destas mensagens anunciando informações sobre interfaces de vizinhos que são ouvidas e o estado dos enlaces de cada interface. Este estado pode ser simétrico (bidirecional), ou assimétrico (A comunicação foi verificada somente em um sentido).

Cada nó seleciona, de maneira independente, seu próprio conjunto de MPRs, entre seus vizinhos com os quais ele possui um enlace simétrico e que, através dos nós contidos neste conjunto, seja possível, se atingir todos os vizinhos a dois saltos.

Para prover rotas para nós distantes a mais de dois saltos, cada nó mantém informações sobre a topologia de rede. Esta informação é adquirida através de mensagens topology control (TC). Os nós que forem selecionados como MPR por outros nós, periodicamente geram mensagens TC, anunciando a lista de todos os nós seletores. Mensagens TC são disseminadas em toda a rede pelos MPRs. Um campo de números de seqüência de mensagem (SN) é utilizado para evitar processamento duplicado de mensagens. Este campo é gerado como seqüência de números inteiros, incrementada mono tonicamente a cada mensagem gerada.

Cada nó mantém uma tabela de roteamento que permite que dados de um nó, cheguem a outro nó da rede. A tabela de roteamento é definida com base nas informações contidas no conjunto de ligações e na configuração da topologia. Quanto estas características são alteradas a tabela precisa ser atualizada.

No draft da (IETF MANET Working Group 2003) sobre o protocolo OLSR é apresentado todo o algoritmo de transmissão dos pacotes, o algoritmo de inundação e as informações que cada nó armazena nas trocas de mensagens, algoritmo para definição da tabela de roteamento, mas como não é o objetivo deste trabalho explicar profundamente este protocolo, será limitado na descrição do protocolo e formato das mensagens. Na medida em que outros conceitos se tornem necessários para a compreensão deste trabalho, serão apresentados com mais detalhes.

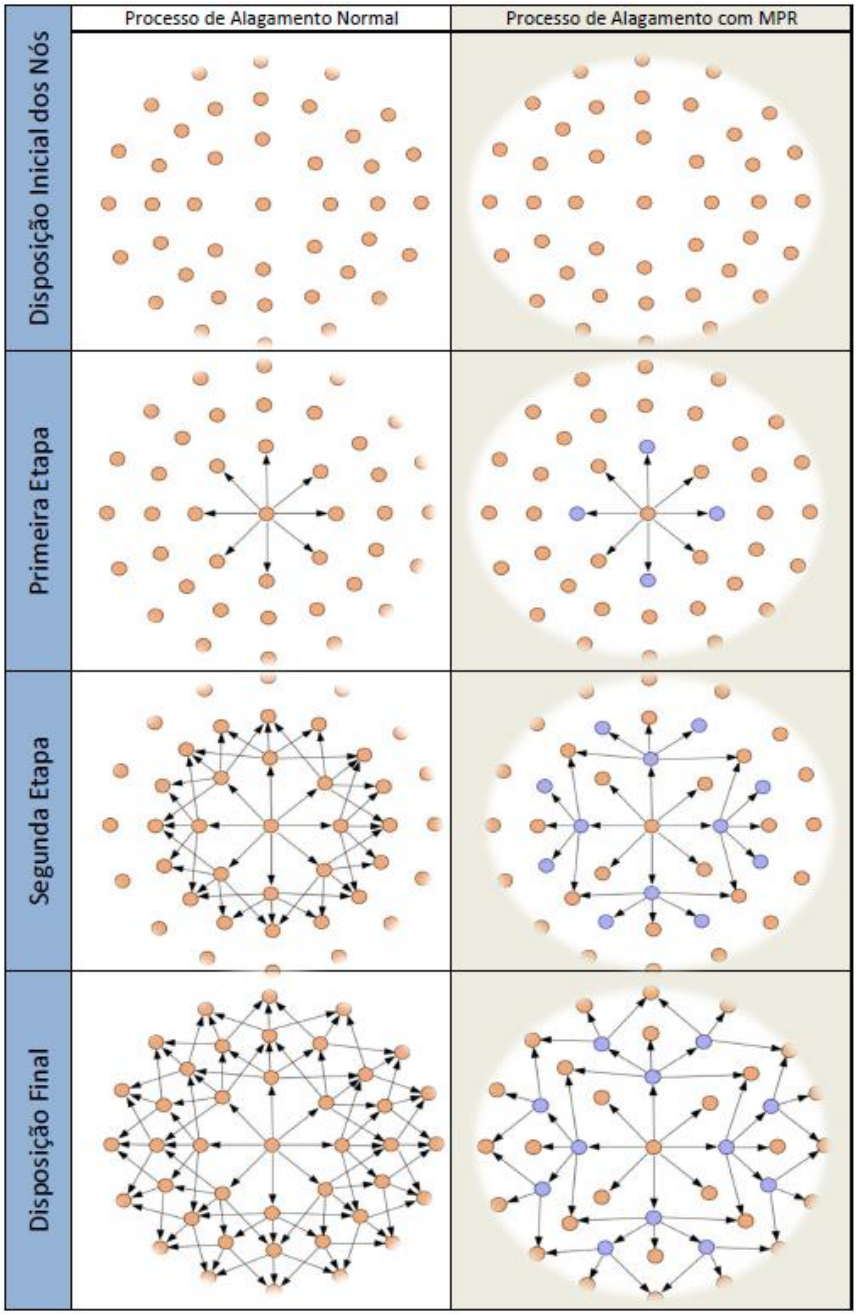

Figura 14 - Demonstração dos Processos de Inundação

4.7.1 Formato do Pacote

Pacotes do OLSR são comunicados via protocolo UDP através da porta 698. O modelo do pacote é apresentado a seguir omitindo o IP e os cabeçalhos do UDP conforme o *draft* (IETF MANET Working Group 2003).

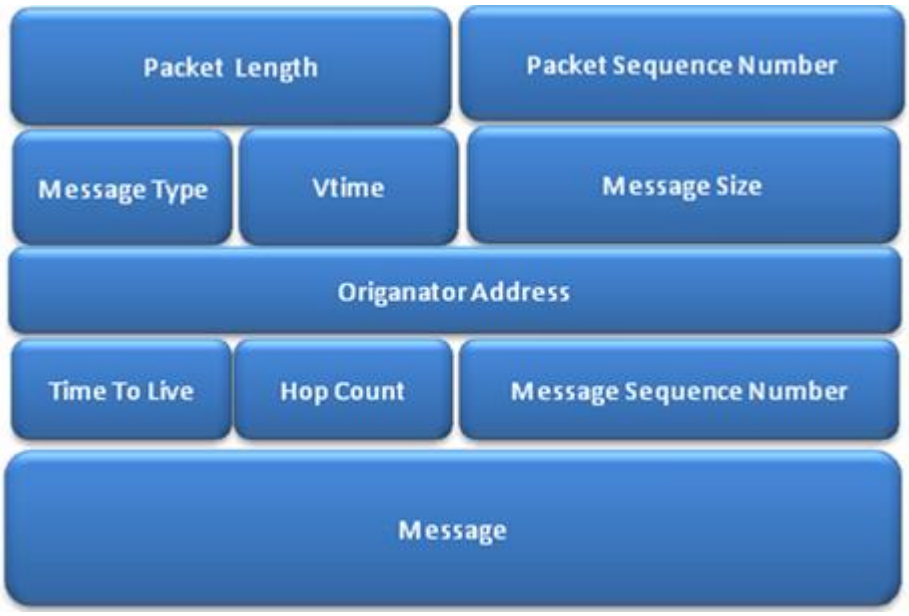

Figura 15 - Formato do Pacote OLSR

Onde:

Packet Length – O comprimento em bytes do pacote

Packet Sequence Number – Deve ser incrementado cada vez que um novo pacote do OLSR for transmitido. Um número de seqüência é mantido para cada interface de tal forma que os pacotes transmitidos através da interface sejam seqüencialmente enumerados. O endereço IP da interface para qual o pacote foi transmitido é obtido através do cabeçalho IP do Pacote.

Message Type – Indica o tipo da mensagem que deve ser encontrada no campo Message do protocolo.

Vtime – Indica por quanto tempo a mensagem deve ser considerada válida após a recepção de um nó, a menos que uma informação mais recente seja recebida.

Message Size – Representa a dimensão da mensagem em bytes.

Originatos Address – Representa o endereço do nó principal que originou a mensagem, ou seja, ao contrário do cabeçalho IP que muda a cada retransmissão, este campo nunca é alterado.

Time to Live – Estes campos contem o número Maximo de saltos que uma mensagem será retransmitida. Antes de ser retransmitida deve ser incrementada por um. Com este processo o autor da mensagem pode limitar o raio de alagamento.

Hop Count – Contem o número de saltos que uma mensagem atingiu. O autor da mensagem encaminha como zero e após isto é incrementada em um para cada salto.

Message Sequence Number – Este campo é utilizado para garantir que uma determinada mensagem não é retransmitida mais de uma vez por qualquer nó, já que ele atribui um número de seqüência único para cada mensagem.

4.7.2 Formato Mensagens MID

Para nós com uma única interface a relação entre o endereço de uma interface e do endereço principal é trivial, mas para uma rede OLSR com múltiplos nós de interface, a relação é definida entre mensagens MID, a qual será apresentada na figura 16.

Cada nó com múltiplas interfaces deve anunciar, periodicamente, informações que descrevem a configuração de interface para outros nós da rede. Isto é possibilitado através da inundação de MIDs a todos os nós da rede através do MPR. Estas mensagens são armazenadas por cada nó e são utilizadas no cálculo da tabela de roteamento.

Esta mensagem é encaminhada conforme o pacote geral apresentado anteriormente, definindo o tipo da mensagem como MID_MESSAGE.

Figura 16 - Formato da Mensagem MID

4.7.3 Formato das Mensagens HELLO

As mensagens HELLO são mecanismos simples para conectar a base local, com a base de informações da vizinhança. A Mensagem HELLO é enviada com o pacote geral conforme descrito anteriormente com o tipo de mensagem definido como HELLO_MESSEGE.

Uma mensagem desta classificação é utilizada para três funções. A medição dos links, a detecção de vizinhos e a seleção de MPRs.

Figura 17 - Formato da Mensagem HELLO

Onde:

HTime – Especifica o intervalo de tempo de emissão do HELLO .

Willingness – Especifica a disponibilidade de um nó de transportar e encaminhar o tráfego para outros nós. Um nó com status *WILL_NEVER* nunca deve ser selecionado como MPR. Um nó com o status *WILL_ALWAYS* deve ser sempre selecionado como MPR, por padrão um nó deve ser anunciado como *WILL_DEFAULT*.

Link Code – Especifica informações sobre a ligação entre a interface do remetente na interface vizinha seguinte. Também especifica a informação sobre o estado do vizinho.

Link Message Size – Tamanho da mensagem em bytes.

Neighbor Interface Address – Um endereço de interface de um nó vizinho.

4.7.4 Formato da Mensagem TC

De acordo com a especificação do protocolo (IETF MANET Working Group 2003), é oferecido basicamente para cada nó, uma lista de vizinhos como os quais ele pode se comunicar diretamente. Baseado neste algoritmo é divulgado a rede a informação de topologia e por conseqüência na construção de rotas. Desta forma, as rotas são construídas através dos links divulgados e das relações entre os vizinhos. Um nó deve ao menos, divulgar as ligações entre si e os nós de seu conjunto MPR.

Uma mensagem TC é envida por um nó da rede para declarar um conjunto de ligações, que deve incluir pelo menos links para todos os nós do seu conjunto de MPR. O número de seqüência ANSN, associado com o conjunto do vizinho declarado também é enviado

Assim o formato da mensagem TC é definido da seguinte forma:

Figura 18 - Formato da Mensagem TC

Onde:

Advertised Neighbor Sequence Number (ANSN) – Um número de seqüência está associado com um anuncio de um vizinho. Cada vez que um nó identifica a atualização de um vizinho, ele incrementa um número seqüencial. Este número é enviado neste campo ANSN da mensagem TC para acompanhar as informações recentes. Quando um nó recebe uma mensagem TC, ele pode decidir com base nos presentes anunciados vizinhos a seqüência do número.

Advertised Neighbor Main Address – Contém o endereço principal de um nó vizinho. Todos os principais endereços vizinhos anunciados pelo nó autor são colocados na mensagem TC.

4.8 Segurança em Redes Móveis AD HOC

A questão de segurança de uma rede móvel AD HOC, conforme já citado, é de fundamental importância, para o projeto da aplicação. Suas características apesar de facilitar uma série de benefícios também tornam a segurança de seus usuários uma questão desafiadora.

As idéias para os mecanismos de segurança em redes AD HOC descendem das abordagens tradicionais dos problemas de segurança das redes convencionais.

No trabalho de mestrado, (TAMASHIRO 2007) é citado que entre todos os ataques possíveis a análise de tráfego é um dos mais problemáticos, pois é de difícil detecção e prevenção.

Como o canal de comunicação para redes sem fio é disponível para usuários legítimos e maliciosos, a possibilidade de ataques é elevada, por isto, para que a rede se torne confiável, deve-se utilizar toda abrangência possível, utilizando os conceitos básicos de segurança como a disponibilidade,

integridade, autenticidade, confidencialidade, não repudio, privacidade, anonimato e robustez.

Há ainda outros aspectos que podem facilitar a vulnerabilidade da rede como as características de topologia dinâmica, ausência de gerenciamento e monitoramento centralizado. Nos estudos de (ROCHA 2004) e (NETTO 2006) são avaliados os aspectos de segurança de redes Ad Hoc, descrevendo os ataques e ações maliciosas específicas sobre este modelo de rede.

Basicamente existem duas classificações para os ataques a este protocolo, quanto à interferência de modo passiva ou ativa e quanto à localização do ataque, externo ou interno. Em um ataque ativo, o atacante interfere na rede e tenta mudar o comportamento normal dos protocolos, já em ataques passivos o atacante somente “escuta” a rede na busca de informações importantes.

Através da análise de tráfego, um atacante pode inferir informações relevantes como os nós origem e destino, localização, topologia, freqüência de comunicação e padrões de movimento. Para a classificação quanto à localização, os ataques externos são realizados por nós externos a rede, que possuem acesso ao meio de transmissão e internos são realizados por nós que fazem parte da rede.

Tabela 5 - Classificação dos Ataques a Redes Ad Hoc

Classificação	Ataques	Descrição
Ativos contra a camada de rede	Bizantino	Um nó intermediário ou um conjunto de nós intermediários comprometidos aliam-se para realizar ataques, como a criação de loops e envio de mensagem de atualização falsas
Ativos contra a camada de rede	Contra o protocolo de roteamento	Estouro da tabela de roteamento por meio da criação de rotas para nós inexistentes, inserção de informações falsas nas tabelas de roteamento por meio de pacotes de atualização ou de roteamento falsos
Ativos contra a camada de rede	Blackhole	O atacante induz os nós a acreditarem que possui o melhor caminho para determinado destino por meio de informações de roteamento falsos, assim podendo interceptar e descartar pacotes
Ativos contra a camada de rede	Consumo de Recursos	Recursos computacionais , de energia são consumidos dos nós presentes na rede
Ativos contra a camada de rede	Wormhole	Dois nós maliciosos estabelecem um túnel entre si, através do qual, podem receber pacotes em uma localização da rede e retransmiti-los em outras, desta forma, possibilita no o controle de algumas rotas
Análise de Tráfego	Análise de Tempo	Se os pacotes são processados e encaminhados na mesma ordem em que são recebidos, um atacante pode inferir quais pertencem á mesma rota ou quais transmissões referem-se a um pacote sendo encaminhado
Análise de Tráfego	Conteúdo do pacote	Um atacante pode identificar e seguir um pacote, quando parte ou todo seu conteúdo permanece inalterado durante sua transmissão
Análise de Tráfego	Volume do pacote	Um atacante pode identificar e seguir um pacote durante sua transmissão, quando pacotes distintos possuem tamanhos diferentes e seus volumes não são alterados ou são modificados de forma padrão pelos nós intermediários
Análise de Tráfego	Reconhecimento de Fluxo	Se os pacotes são vulneráveis a análise de tempo ou se possuem informações em comum, um atacante pode identificar quais pertencem a mesma rota

4.8.1 Segurança no Protocolo AODV

O Protocolo AODV não possui nenhuma medida relativa à segurança implementada, apesar de possuir algumas variações deste protocolo que possuem tais características. Nesta seção são apresentados aspectos relativos a falhas de segurança especializadas a este protocolo, bem como ataques possíveis.

No modelo de operação do AODV a cooperação entre os nós é assumida, assim sendo, ataques maliciosos podem deturpar operações da rede, violando especificações do protocolo. A operação possui uma séria de vulnerabilidades das quais os nós maliciosos podem se aproveitar para modificar, fabricar e personificar mensagens da rede afetando o desempenho e capturar informações.

Usualmente os ataques que visam o encaminhamento de pacotes podem ser descritos como (FILHO 2005):

- Ataques de Modificação – O nó malicioso altera informações de mensagens de roteamento recebidas, gerando informações de rotas falsas, ou tenta atrair para si o trafego da rede, fazendo com que todas as rotas passem por ele, no AODC, o nó malicioso simplesmente diminui o valor do campo Contador de Saltos para provocar esta situação. Com a falsificação do campo de número de seqüência do destino é possível redirecionar o trafego da rede e até mesmo impedi-lo de alcançar seu destino;

- Ataques de Fabricação – O nó malicioso fabrica sua própria mensagem de RREP, RREP, RERR, cada uma tendo uma conseqüência diferente. No caso do RREP, para certo destino tornaria esse nó inalcançável. Caso seja utilizado também um número de seqüência muito alto, esse ataque poderia fazer com que esse nó ficasse inalcançável durante um longo período;

- Ataques de Personificação – O nó malicioso utiliza o endereço de outros nós da rede, fingindo ser quem não é. Como o AODV não possui nenhum tipo de autenticação, não há como saber se o nó é realmente quem ele diz ser;

Os ataques também podem ser classificados como maliciosos de acordo com seu objetivo principal:

- Ruptura de Rota – Visa à quebra de uma rota já estabelecida entre nós da rede ou mesmo a inviabilidade que uma ova rota seja formada;

- Invasão de Rota – significa que o atacante se insere dentro de uma rota e passa a fazer parte do caminho de dados;

- Isolamento de Nós – Faz com que cada nó atacado cesse a comunicação com o resto da rede, tornando-o isolado;

- Consumo Indevido de Recursos – O nó invasor faz com que seja consumida toda banda de rede disponível formando um ciclo entre os nós ou esgotando qualquer outro recurso necessário para o bom funcionamento da rede;

- Impedimento de Serviços - O ataque de Inatividade Seletiva onde não é encaminhado pacotes de dados ou roteamento inadvertidamente;

4.8.2 Segurança no Protocolo OLSR

O Modelo de protocolo OLSR, também não possui medidas especiais de segurança, e pelo fato de ser proativo, torna-se alvo para vários ataques. Nesta seção são descritas questões relativas a estas vulnerabilidades que são baseadas nos trabalhos de (DEUS e Janaína Laguardia 2008), (FRANCESQUINI 2004), (Network Working Group 2003) são realizados estudos sobre as possíveis abordagens de ataques ao protocolo OLSR.

Como o OLSR difunde periodicamente as informações sobre a topologia da rede e através de uma rede sem fio, a topologia pode ser revelada a quem escuta o controle das mensagens. Esta vulnerabilidade pode ser contornada com a atualização de criptografia nas transmissões da respectiva rede.

A integridade da rede também pode ser comprometida por um nó mal intencionado ou com um nó não funcionando adequadamente, injetando tráfego de controle inválido como mensagens HELLO e TC. Isto pode ser contornado com a utilização da autenticação das mensagens.

A seguir são apresentadas situações que podem ocorrer ataques a integridade deste protocolo:

- Nó gera mensagens TC ou HELLO, publicando links de nós não vizinhos;

- Nó gera uma mensagem TC ou HELLO, fingindo ser outro nó;

- Encaminhamento de mensagens de controle alteradas;

- Um nó não transmite mensagens de controle;

- Um nó não seleciona MPRs corretamente;

O OLSR possui métodos de encaminhamento externo de domínios, através das mensagens HNA, que fornecem um mecanismo para interação a domínios externos a rede OLSR como uma conexão ethernet. Neste processo as informações de roteamento podem ser extraídas da tabela de topologia, ou da tabela de roteamento do OLSR e encaminhadas a um domínio externo. Este processo pode ser potencialmente inseguro, devido à má utilização da tabela de roteamento por um possível invasor.

Outro ponto possível de ataques a este protocolo é devido o OLSR não executar qualquer suposição sobre os endereços dos nós, com exceção de que cada nó tenha um endereço único.

O Estouro da Tabela de Roteamento é ataque se baseia no fato de os protocolos de roteamento Ad Hoc pró-ativos, como o OLSR, armazenarem todas as rotas anunciadas pelos seus vizinhos. Nestes protocolos, o nó armazena em sua tabela de roteamento todas as mensagens de rota que recebe periodicamente. A estratégia deste ataque é anunciar diversas rotas para nós inexistentes, de modo a aumentar progressivamente o tamanho da tabela de roteamento, até que ela estoure e o nó não possa mais armazenar as rotas reais. Os protocolos reativos que armazenam diversas rotas para um mesmo destino, também estão expostos a esse tipo de ataque, pois o nó malicioso poderia enviar rotas passando pelos nós inexistentes. Esse ataque é grave no caso de redes Ad Hoc, que possuem recursos limitados, onde tanto o gasto de energia com a recepção de um número excessivo de mensagens, quanto o estouro de *buffer* são cruciais. Para preveni-lo, deve-se limitar o

número máximo de rotas nas tabelas de roteamento, além de só aceitar entradas de nós autenticados.

4.9 Considerações

Este capítulo foi iniciado definindo o conceito de uma rede Ad Hoc, suas características essências e classificações, além de citar e avaliar as diversas possibilidades de aplicações, fato este que levanta uma característica mercadológica importante a pesquisas deste tema.

Dentro dos diversos protocolos existentes para a utilização das redes Ad Hoc, há dois que se destacam pela quantidade de pesquisas e de utilizadores, o protocolo OLSR e o AODV.

Apesar de estes protocolos serem os mais utilizados, os dois não apresentam qualquer nível de segurança. Este ponto somado as características abertas das redes sem fio, pode se tornar um fator impeditivo para aplicações comerciais.

O próximo capítulo descreve os pontos relevantes para o projeto do modelo proposto, sobre os aspectos da rede Ad Hoc, redes neurais e detecção de intrusão.

5. Definição do Projeto

Em (Lima, 2005) foi proposto um modelo para detecção de intrusos em redes de computadores, com a utilização de técnicas de inteligência artificial, utilizando características de reconhecimento de padrões e da generalização para realizar a classificação dos eventos ocorridos.

Seguindo esta linha, a proposta deste trabalho é aplicar o modelo desenvolvido por (Lima, 2005) para a utilização em redes móveis Ad Hoc, classificando as atividades da rede em eventos intrusivos, através do conhecimento obtido durante a fase de treinamento, levantando e simulando ataques específicos para esta modalidade de rede, explorando suas vulnerabilidades. Será avaliada a eficiência especificamente para as redes Ad Hoc, bem como, ações de melhorias para a adaptação a esta modalidade de rede.

Neste capítulo será especificada inicialmente a arquitetura global deste projeto identificando de forma simplificada suas funcionalidades e aplicações, passando pelo detalhamento específico da implementação e implantação da rede Ad Hoc com a utilização do protocolo OLSR. A seguir será apresentado o modelo de captura de pacotes utilizados, bem como suas funcionalidades e características, seguindo para a arquitetura do IDS e as características da rede neural que esta aplicação utiliza.

5.1 Visão Geral do Modelo Proposto

Na figura 19 está representada a arquitetura geral da aplicação proposta neste trabalho baseado basicamente em três pilares, na biblioteca LIBPCAP (MCCANNE e JACOBSON 2002) que possui a função de capturar os pacotes IP trafegados na rede, na aplicação do protocolo OLSR (IETF MANET Working Group 2003) e (TONNESEN 2004) na aplicação de análise do trafego e identificação de intrusão I-IDS (Lima, 2005). Cada módulo será detalhamento apresentado adiante neste capítulo. O modelo proposto possui diversas funcionalidades, que estão representadas na figura 19 na barras verticais. Estas funcionalidades estarão detalhadamente descritas mais adiante.

O desenvolvimento do I-IDS foi realizado no trabalho de (Lima, 2005), para Linux, sendo que para este trabalho foi necessário a adaptação para Windows com o objetivo de testar a interoperabilidade da rede. Para realizar a compilação do código fonte, foi utilizado o Microsoft Visual Studio configurando compilador de C/C++ e adicionado algumas bibliotecas específicas para o Windows (stlpmt45, cc3260mt, borlndmm, bcbsmp60).

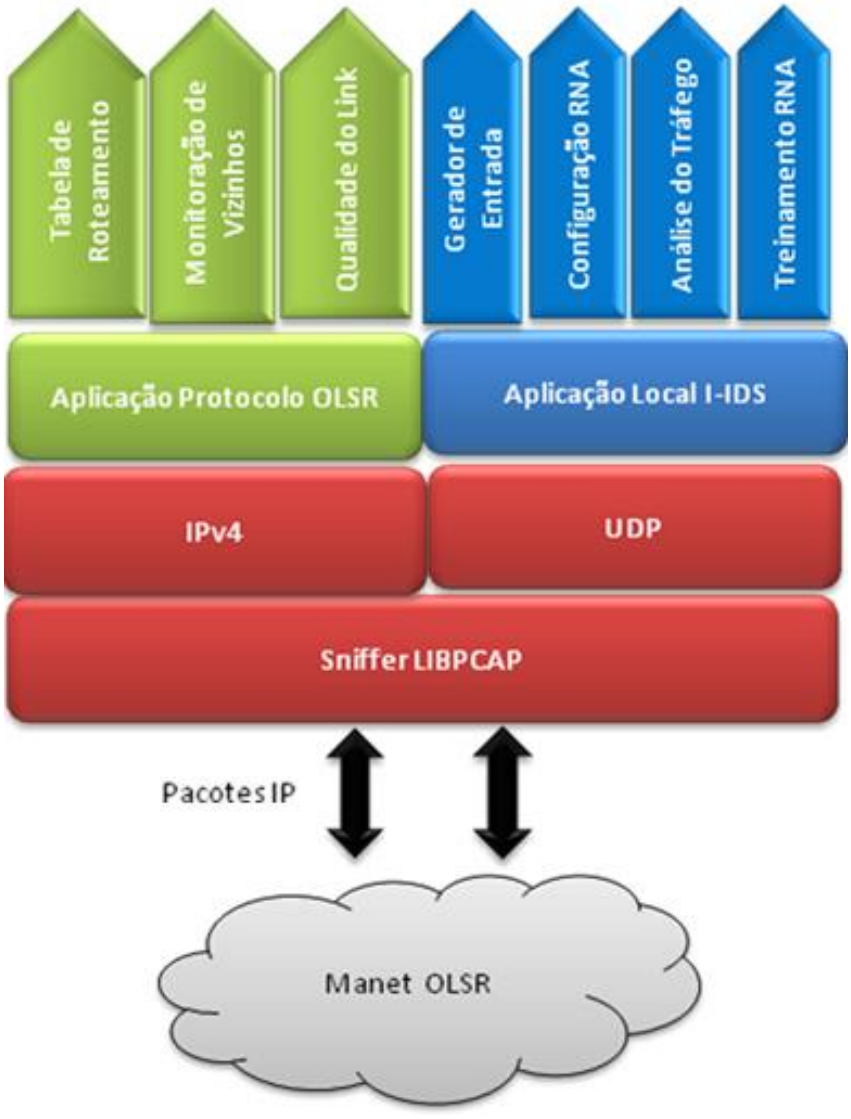

Figura 19 - Arquitetura do Modelo Proposto

A definição de um modelo referencial de sistema de intrusão para rede Ad Hoc atualmente está orientado segundo uma arquitetura em camadas especializadas localizadas em cada nó da rede.

A coleta de dados através do sniffer se destina a capturar diversas informações que estão disponíveis no nó, como o tráfego oriundo da rede, bem como todas as atividades sistêmicas de controle da rede. Neste módulo são realizados diversos tratamentos com o objetivo de reduzir e agregar a informação analisada pelo módulo de detecção de intrusão, otimizando assim o processamento realizado pela aplicação e desta forma possibilitando a detecção de um ataque em andamento.

Aplicação Local I-IDS é o módulo responsável pelo processamento das informações agregadas do módulo do sniffer, tratando o tráfego sem se preocupar a tratar os dados brutos oriundo do tráfego da rede e informação de controle do sistema. Neste módulo são utilizadas funcionalidades das redes neurais que identificam as seções intrusivas. Esta situação é atualizada constantemente com o objetivo de comportar a natureza dinâmica das redes Ad Hoc.

O módulo OLSR tem por objetivo efetuar o controle da rede OLSR, conforme descrito no capítulo anterior, efetuando a atualização da tabela de roteamento através da monitoração dos vizinhos via mensagem HELLO e da qualidade de cada Link a fim de identificar os MPRs e as melhores rotas de comunicação, para que o tráfego multihop ocorra com o menor atraso possível naquele momento.

Para a posterior compreensão do modelo, é fundamental também introduzir o modelo da rede utilizado, sendo representado através da figura 20. Nela é demonstrado que cada identificador de intrusão, módulo de captura de pacotes, e aplicação do protocolo OLSR, foram instalados localmente, cada um efetuando suas devidas funções dentro desta arquitetura global.

Para a utilização da rede Ad Hoc ou Manet OLSR, foi necessário realizar a configuração dos transmissores para que trabalhem desta maneira.

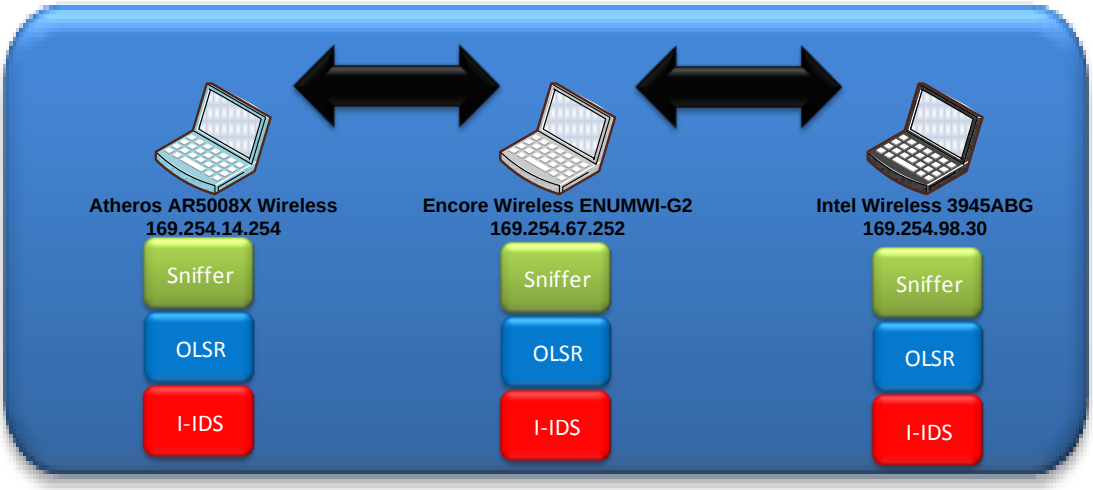

Figura 20 - Arquitetura de Rede Utilizada

5.2 Visão da Rede Móvel Ad Hoc Utilizada

Como foi exposto na tabela 3, há uma variedade grande de protocolos desenvolvidos para redes Ad Hoc, para definir qual o protocolo a ser utilizado neste trabalho, foram avaliadas várias características, como complexidade, nível de documentação, segurança e utilização prática. Foram avaliados detalhadamente os dois protocolos mais utilizados em aplicações comerciais e aplicações cientificas e desta gama de protocolos, foi definida a utilização do protocolo OLSR. Os principais motivos por esta definição do OLSR foram possuir uma boa documentação disponível na IETF, possui utilizações práticas de grande porte como a rede Athens *Wireless Network* em Berlim, que é composta de mais de dois mil nós.

Outro ponto favorável a este protocolo, é o fato de já haver diversas experiências em utilização para as plataformas de sistemas operacionais como MAC OS, Debian Linux, Ubuntu Linux, Unix, Windows 2k/XP/Vista, bem como a utilização outros dispositivos móveis como Smartphone Nokia 770 e iPhone e Google Android.Fato este que pode possibilitar a simulação/utilização em diversos ambientes, avaliando a interoperabilidade deste modelo.

Também foi considerado o fato de que o OLSR possuir diversas implementações em código aberto, desta forma, facilitando a aplicabilidade, desenvolvimento e extensibilidade.

A figura 21 representa a arquitetura do módulo OLSR, com suas funcionalidades e a demonstração do processo de atualização e manutenção da tabela de roteamento, através da monitoração dos vizinhos e da qualidade do link.

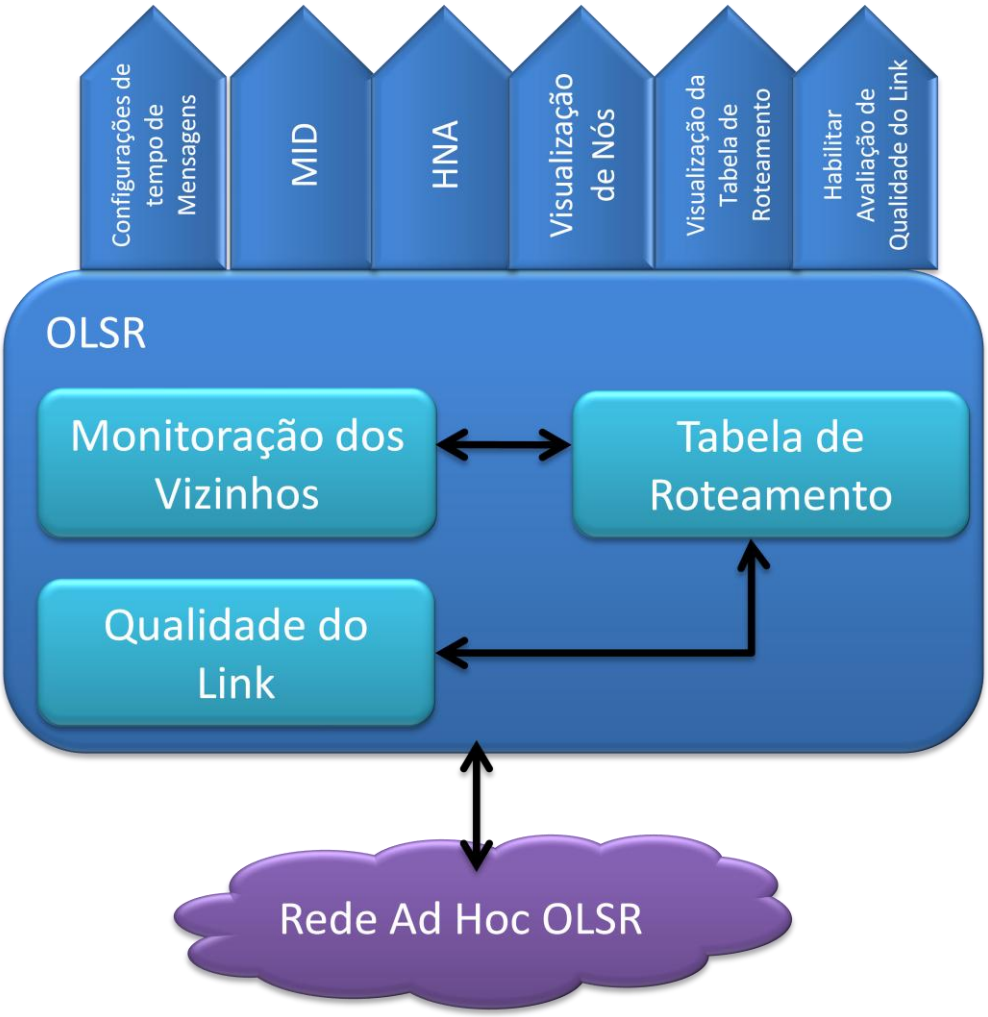

Figura 21 - Processos do Módulo OLSR

O fato do OLSR não possuir controles específicos de segurança também facilitará a simulação inicial dos ataques a rede.

Para a configuração do modelo proposto neste trabalho foi baseada na tese de mestrado de (TONNESEN 2004). Esta implementação do protocolo OLSR está disponível em código aberto, na linguagem C/C++ e é compatível com o modelo RFC3626 (Network Working Group 2003), facilitando a implementação de novas extensões do protocolo e funções auxiliares de roteamento. Também possui facilidades de configuração de múltiplas interfaces de rede para um mesmo nó, assim como configuração das mensagens encaminhadas para a utilização do protocolo HELLO , MID, HNA e TC.

A definição da infra-estrutura utilizada pela rede é apresentada na figura 22. Foram utilizados três notebooks, cada um com características diferentes de configurações e modelos de placa wireless. No nível de sistema operacional foram utilizados dois notebooks com Windows Vista Home, e um com Linux Opensuse 11.1 com Kernel 4.1, justamente para que a interoperabilidade desta proposta fosse avaliada.

Dentro destas avaliações de interoperabilidade houve um sério problema na utilização deste modelo de rede para Windows, pois inicialmente o

roteamento multihop não ocorria. Após uma serie de pesquisa descobriu-se que o roteamento multihop é desabilitado no Windows como padrão, conforme própria documentação da Microsoft. Na documentação também existe um tutorial para liberação deste roteamento.

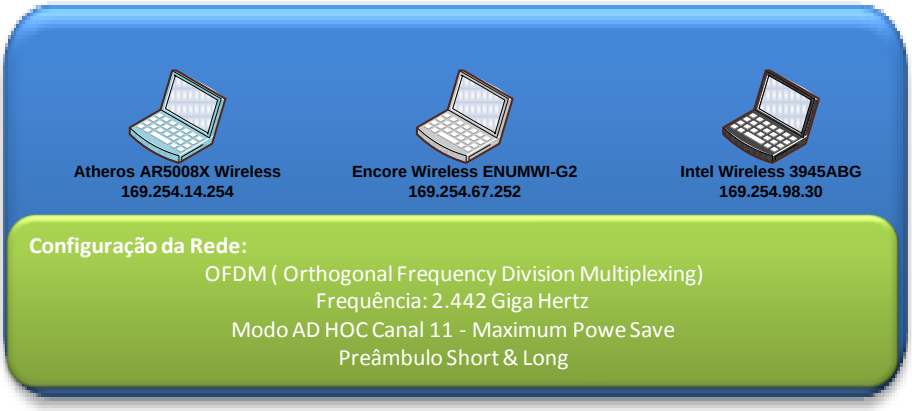

Figura 22 - Configuração do Sinal da Rede Utilizada

Cada nó foi equipado com uma placa para transmissão e recepção do tráfego conforme a figura acima. Os três nós móveis utilizaram a modulação OFDM e foram sintonizados na freqüência de 2.442 Giga Hertz em modo Ad Hoc Canal 11. Foi também utilizado a função de economia máxima de energia para avaliar possíveis diferenças na utilização do protocolo em questão.

Todo o tráfego de comunicação e interação da rede é baseado no protocolo IP sendo transmitido via UDP porta 698. Este protocolo é utilizado devido a suas características de não comprometer o funcionamento da rede com a perda de pacotes, fato bastante propício nas aplicações de rede sem fio, possuir suporte a *broadcasting* e *multicasting*. A porta 698 foi designada pela IANA, como padrão para este tipo de aplicação.

5.3 Visão do Processo de Captura de Pacotes

Baseando na representação da arquitetura geral deste modelo, identifica-se a caixa Sniffer Libpcap como sendo a responsável pela captura de pacotes. Ela possuía a função de ouvir todo o tráfego recebido por cada nó disposto na rede, aplicar filtros específicos para adaptação do tráfego para a rede neural, técnicas de pré-seleção e análise inicial (Lima, 2005). Desta forma sua função estende o objetivo inicial de um sniffer de somente captura de dados, sua funcionalidade prepara os dados para que estes sejam utilizados nas próximas aplicações.

Esta aplicação foi inicialmente implementada no projeto tcpflow (ELSON 2001), que utiliza como base a biblioteca de captura de pacotes denominada libpcap (MCCANNE e JACOBSON 2002) e desenvolvida no protótipo I-IDS (Lima, 2005).

A Libpcap é uma biblioteca de código aberto que fornece uma estrutura portátil para monitoramento da rede em baixo nível. Ela possui várias funções para realizar a captura de pacotes, sendo possível configurá-la na quantidade de pacotes a capturar, o modo de captura (normal ou promiscuo) e como definir sua chamada.

> "Através do modo de operação denominado promiscuo é possível ter acesso a todos os pacotes distribuídos na rede em forma de broadcast, possibilitando que se monitorem atividades que ocorrem entre conexões que não envolvam diretamente a estação de captura (Lima, 2005)".

Sua principal vantagem de utilização para este modelo é fato dela ser programável em diversos pontos, alguns exemplificados nas tabelas 6, 7 e 8, que representam variáveis desta biblioteca que podem ser programáveis. Respectivamente de acordo com o tipo de Link, protocolo de camada de rede e protocolo de camada de transporte. Todas estas variáveis tiveram que ser definidas de acordo com a rede descrita no item anterior deste trabalho.

Tabela 6 - Configuração do Tipo de Link para Captura

Tipo de Link	Alias na LIBPCAP
Ethernet 10/100/1000 Mbs	DLT_ENXXXXMB
Wi-Fi 802.11	DLT_IEEE802_11
FDDI	DLT_FDDI
PPPoE	DLT_PPP_ETHER
BSD LoopBack	DLT_NULL
Point to Point (Dial UP)	DLT_PPP

Tabela 7 - Configuração do Protocolo de Camada de Rede para Captura

Protocolo de Camada de Rede	Valor Ethertype
IPv4	0x800
IPv6	0x86DD
ARP	0x0806
RARP	0x8035
Ethertalk	0x809B
PPP	0x880B
PPPoE Discovery Stage	0X8863
PPPoE Session Stage	0x8864
SNMP	0x814C

Tabela 8 - Configuração do Protocolo da Camada de Transporte para Captura

Protocolo de Camada de Transporte	Valor Ethertype	RFC
ICMP	0x01	RFC792
IGMP	0x02	RFC3376
TCP	0x06	RFC793
Exterior Gateway Protocol	0x08	RFC888
UDP	0x11	RFC768
IPv6 Routing Header	0x2B	RFC1883
IPv6 Fragment Header	0x2C	RFC1883
ICMP para IPv6	0x3A	RFC1883

Na figura 23 é representado o processo do *sniffer* utilizado neste trabalho, que tem a principal função de captura o tráfego da rede Ad Hoc OLSR. Pode ser visto que inicialmente todo o tráfego gerado pelos nós, como o tráfego sistêmico gerado são capturados pelo bloco representado abaixo nomeado como “captura dos pacotes”. A principal justificativa para se capturar todo o tráfego é a que se fosse necessário analisar alguma porta, protocolo ou ponto de controle específico pudesse ser realizado somente filtrando a necessidade, apesar da questão de impacto no processamento dos nós. Estes filtros também foram realizados pelo Wireshark (CACE TECHNOLOGIES s.d.), ferramenta desenvolvida em C que foi utilizada como analisar de pacotes, mas também possuir funcionalidades específicas de captura de tráfego. Todas as possibilidades de filtros e como são efetuados estão disponíveis no site do grupo criador desta ferramenta.

Este tráfego capturado pelo Wireshark também pode ser utilizado no tratamento do fluxo da aplicação realizada por (Lima, 2005), pois a mesma também possuía esta possibilidade de análise de arquivos armazenados

Após a captura do tráfego os dados são passados para o bloco seguinte, conforme a figura 23, que realiza a aplicação dos filtros e a pré- seleção dos dados que são avaliados com o I-IDS.

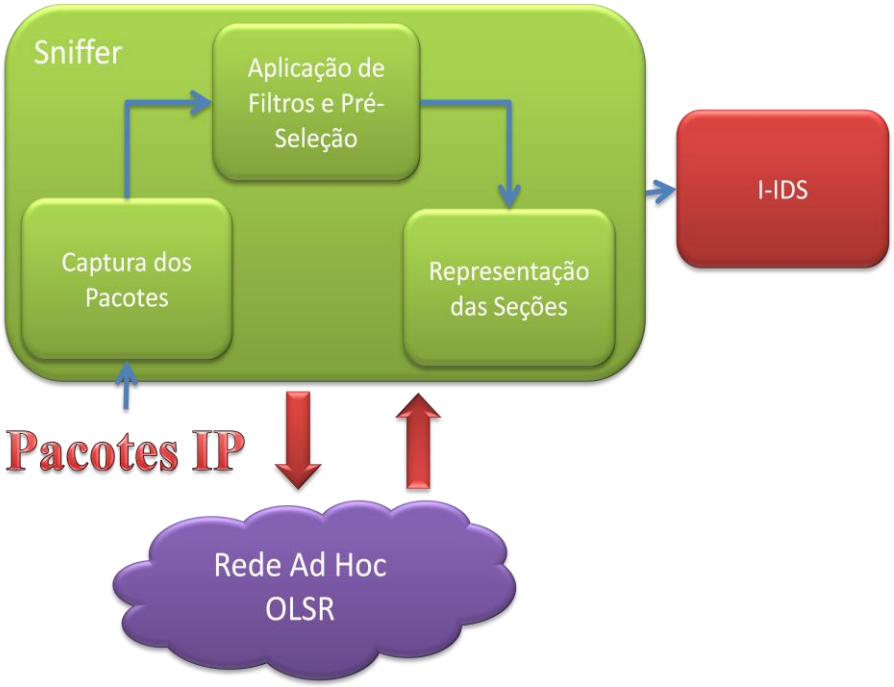

Figura 23 - Processo de Captura de Pacotes

O terceiro bloco da figura 23 visa criar as representações das seções e desta forma repassar ao I-IDS informações padronizadas. Basicamente as seções capturadas são formatadas pela aplicação de sniffer de forma a registrar a seguinte sintaxe: (#####_I-IDS_#####, seguidas pelo protocolo, IP de Origem: Porta, IP de Destino: Porta, #####_I-IDS_#####,:Ordem de coleta:,trafego, e terminadas pelo marcador I-IDS:END).

Para a coleta do tráfego também são utilizados marcadores que representam o fluxo de dados com o endereço de origem para o endereço de destino I-IDS-> e o I-IDS<- em sentido antagônico.

Na figura 24 é representada uma seção UDP coletada pelo módulo de *sniffer*. Para tratar os pacotes capturados e assim chegar à representação abaixo, são levados em consideração os parâmetros contidos em áreas do datagrama como cabeçalho IP, TCP e payload, pois estas informações são subsídios para tratamentos posteriores que irão compor a representação do fluxo de rede. Para montar esta representação é realizado um mapeamento dos dados relevantes em estruturas de dados na memória, visando construir um arquivo para cada seção e para cada sentido do fluxo de dados capturados (Lima, 2005).

A biblioteca LIBPCAP ainda possui diversas possibilidades de programação, filtros e desempenho, que são detalhadas no trabalho de (MONGE 2005).

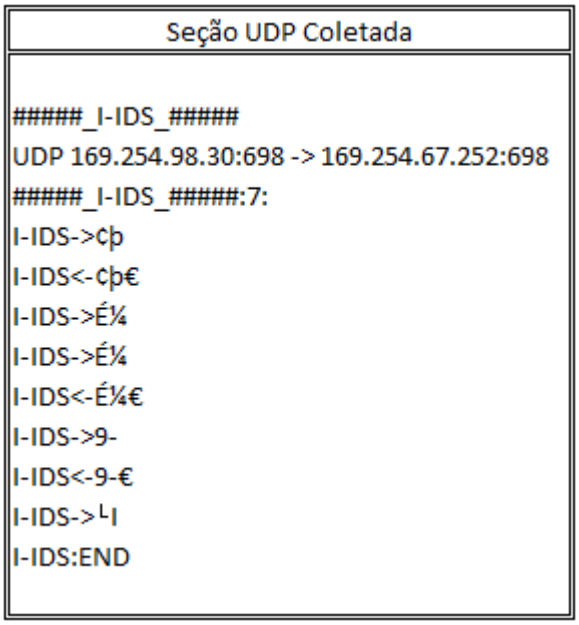

Figura 24 - Seção UDP Coletada

Outra função que facilitou a execução deste trabalho foi à flexibilidade de modularidade desta aplicação no que diz respeito à definição do conteúdo a ser capturado, já que assim facilmente pode-se alterar o foco de análise pelo IDS como, por exemplo, o tráfego de controle da rede Ad Hoc OLSR ou todo o tráfego dos nós.

Após este processo de captura dos dados, filtro e conversão, as representações de seções são repassadas para a utilização da ferramenta I-IDS, que realiza a análise semântica, o pós-processamento, análise neural e monitoração dos eventos intrusivos, conforme será explanado na seção seguinte.

5.4 Visão do Processo de Detecção de Intrusão

Em uma rede com infra-estrutura específica é possível estabelecer de maneira clara e segura todas as fronteiras de tráfego (centralizada ou distribuída), que permite a segmentação de todas as possibilidades de tráfego e assim localizar detectores de intrusão por todo núcleo de comunicação. Esta analise ocorre em tempo real e geralmente é fortemente integrada ao sistema de gerenciamento, que tem a função de alarmar os responsáveis pela segurança da rede, e pode realizar a devida tratativa deste alarme, de forma automática ou manual.

Porém voltando ao modelo deste trabalho, as redes Ad Hoc possuem uma natureza dinâmica e cooperativa, tornando impossível, de maneira clara e segura, que permitam a utilização das ferramentas desenvolvidas para as redes estruturadas, como firewalls, e outros mecanismos de controle de tráfego.

Há também outro fator que deve ser considerado para as redes Ad Hoc, que é a limitação de recursos, seja de energia, banda, processamento ou nós descontínuos.

Devido a estas características nesta modalidade de rede deve-se apresentar um modelo diferenciado das redes com infra-estrutura, onde a solução deve estar voltada as suas características de limitação de recurso, dinamismo e cooperativismo, implantando os IDSs de forma distribuída em cada nó pertencente à rede, que funcionalmente monitoram todas as atividades locais de maneira independente de localização, recursos e sistema operacional.

Com base nas características dinâmicas e cooperativas das redes Ad Hoc, a utilização das redes neurais para este trabalho advém das características de alta capacidade de adaptação, aprendizado e generalização, podendo ser utilizadas tanto para definir sistemas de detecção de anomalias quanto de detecção de abusos.

Para tal desenvolvimento é necessário definir a topologia da rede, seu algoritmo de treinamento, variáveis quantitativas e qualitativas que representem o modelo e também os dados que irão compor o treinamento. Este módulo se relaciona com o sniffer que repassa os dados que são tratados por ele e através da monitoração dos processos alimentam o usuário sobre as informações de intrusão e outras informações que será visto nas seções seguintes. Na figura 25 estão sendo representado o módulo do I-IDS e quatro sub-módulos da aplicação I-IDS, análise semântica, pós-processamento, análise neural e monitoração dos processos que serão detalhadas nas seções a seguir.

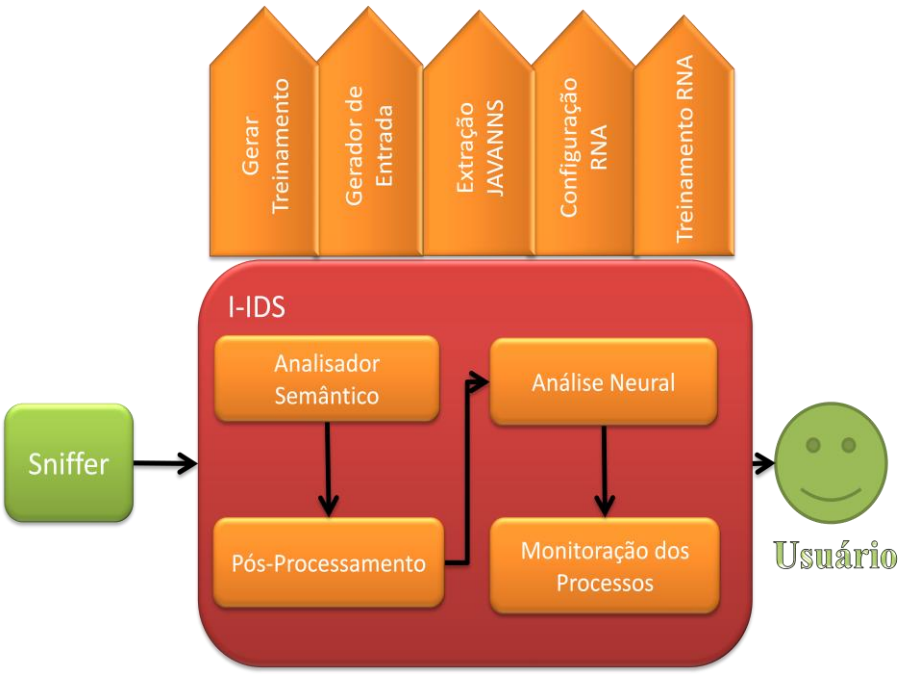

Figura 25 - Processo do Módulo I-IDS

5.4.1 Analisador Semântico

> “O analisador semântico é o módulo que irá processas a representação gerada pelo módulo de captura em busca de strings que podem representar uma atividade suspeita. Esses strings avaliados podem ser a definição de determinados protocolos ou portas envolvidas na conexão, mas tratam-se principalmente das mensagens trocadas entre os nós durante do desenvolvimento da seção analisada. Esta análise é apoiada por determinados arquivos que compõem a base de conhecimento do modelo. Estes arquivos contem às strings que representam atividades suspeitas e seus respectivos identificadores de categoria, os quais são associados a um código binário que será utilizado para compor a representação intermediária da seção (Lima, 2005)”.

A base de conhecimento utilizada neste trabalho foi elaborada principalmente, com base na lista de palavras que foram utilizadas no I-IDS, porém, devido ao foco deste trabalho ser a utilização do I-IDS para redes Ad Hoc e por conseqüência haver particularidades citadas na seção anterior, foi enriquecida esta base de conhecimento com seções simuladas de ataques para rede Ad Hoc, voltadas a protocolos UDP e porta 698.

Também foi adicionada uma série de strings de ataques, intrusões e regras de firewalls do interessante projeto Emerging Threads, que é financiado pela *National Science Foundation* e *Army Research Office.* Trata-se de uma comunidade de código aberto que disponibiliza estas regras, em troca de cada usuário ao detectar novas regras, também as compartilhe. Desta forma, foi incluído na base de conhecimento utilizado neste trabalho, o conteúdo do campo *content* das principais regras voltadas a redes sem fio *e protocolo UDP.*

Estas regras são classificadas de acordo com o modelo de ataque/intrusão e são atualizadas diariamente proporcionando uma fonte importante de novas regras que com certeza surgirão, pois sempre novas formas de ataque estão sendo desenvolvidas. No momento são disponibilizadas quase onze mil regras classificadas conforme a figura 27.

A seguir é apresentado um exemplo de uma regra de ataque a protocolo UDP, voltado a qualquer porta, enriquecendo a base de conhecimento.

alert udp any any -> any any (msg:"ET ATTACK_RESPONSE Bindshell2 Decoder Shellcode (UDP)"; content:"|53 53 53 53 53 43 53 43 53 FF D0 66 68|";content:"|66 53 89 E1 95 68 A4 1A|";distance:0; sid:2009285; rev:2; reference:url,doc.emergingthreats.net/2009285; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode;)

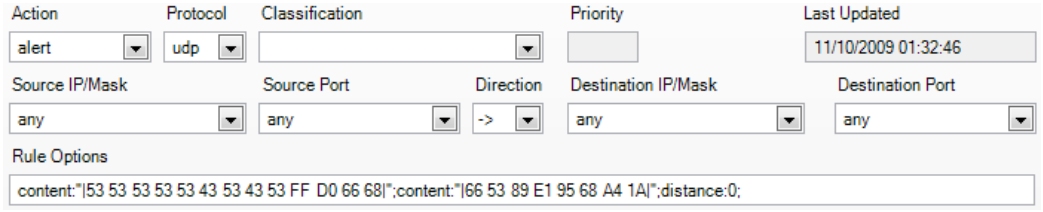

Figura 26 - Composição de Regras de Ataques e Intrusões

De uma forma didática a composição destas regras de ataque/intrusão é composta conforme a figura 26, que separa o conteúdo das regras em campos específicos para análise em um IDS.

Figura 27 - Classificação das Regras de Intrusão e Ataques

Após a definição da base de conhecimento formada por *Strings,* é necessária a composição da representação binária de cada categoria, já que a correta representação binária impacta diretamente sobre o tempo de treinamento e os resultados das análises geradas pela rede neural (LIMA 2005), além de levar a rede a confundir padrões que impactariam diretamente no treinamento da rede.

No modelo implementado por (LIMA 2005), cada categoria definida é associada a um código binário de 16 bits, onde é definido o valor da distância de *hamming* de acordo com o número de combinações necessárias para representar os strings. Esta abordagem advém do trabalho de (CANSIAN 1997).

O processo de representação binária dos strings, figura 28, é também realizado para os protocolos da seção e para a porta utilizada para a conexão. Todo este processo pode ser realizado pelo gerenciador da aplicação I-IDS que realmente facilita a atualização da base de conhecimento, que devido ao grande surgimento de novos ataques, é fundamental.

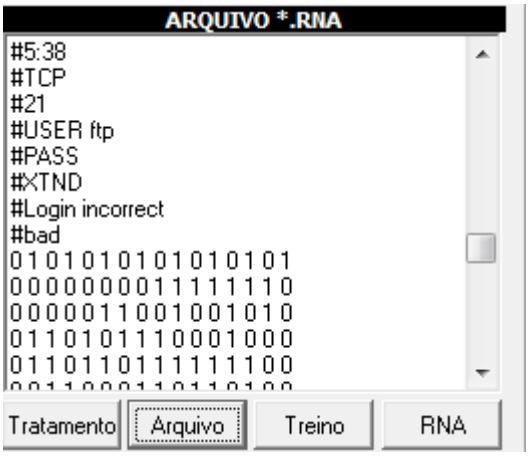

Figura 28 - Representação Binária no I-IDS

5.4.2 Pós Processamento

Este sub-módulo é responsável por compor o vetor de estímulos que será usado como entrada para a rede neural, e que será composto a partir da representação intermediária gerada pelo sub-módulo anterior. Este processo é utilizado tanto para gerar entradas que serão analisadas, quando para gerar entradas que serão utilizadas durante o treinamento supervisionado da rede neural (LIMA 2005).

Para gerar as entradas analisadas cada seção registrada no arquivo e analisado individualmente e gera outro arquivo informando na primeira linha o número de padrões que constam no arquivo e os códigos binários de cada seção dispostos linha por linha.

Na figura 29 este processo é demonstrado conforme circundado em azul, como cada seção possui 16 padrões de 16 bits, o vetor de estímulo possuirá 256 entradas por seção que serão analisadas individualmente pela rede neural.

O conhecimento obtido durante o treinamento será utilizado para definir o grau de suspeita de cada padrão informado pelo vetor de estímulos.

Para gerar as entradas utilizando o treinamento supervisionado da à rede neural utilizada, a opção gerar treinamento da aplicação I-IDS que questionada se cada seção é identificada como seção intrusiva ou normal, definindo como valor -1 para seções normais e 1 para seções intrusivas, ou seja, o sub-módulo de rede neural ao treinar a rede irá utilizar este arquivo de treino para ajustar seus pesos e adquirir conhecimento de acordo com as informações passadas pelo instrutor (LIMA 2005).

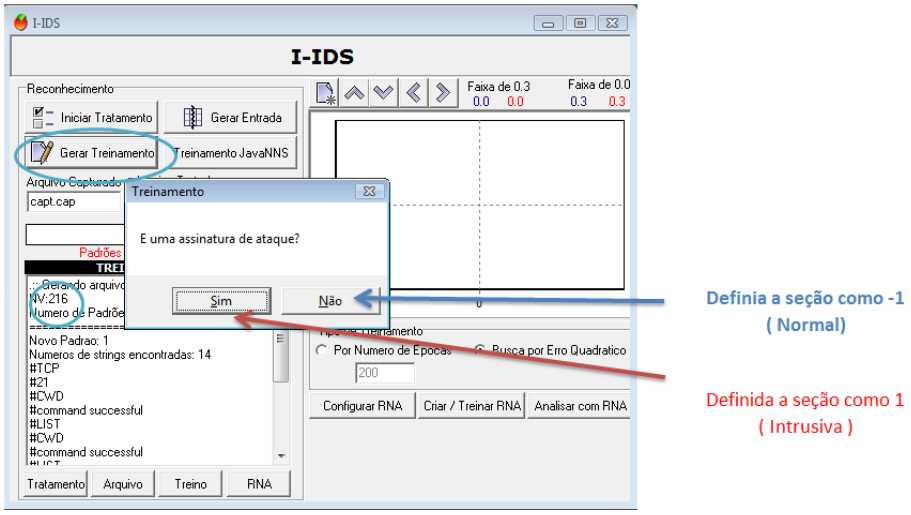

Figura 29 - Pós-Processamento no I-IDS

5.4.3 Análise Neural

Como foi citado, devido as suas características de adaptabilidade e flexibilidade, o módulo de rede neural é o módulo mais importante deste projeto. Portanto é fundamental definir a topologia da rede, seu algoritmo de treinamento, variáveis quantitativas e qualitativas que representem o modelo e também os dados que irão compor o treinamento. Nesta seção serão apresentadas como foram feitas estas definições no I-IDS.

O principal benefício para se aplicar redes neurais no processo de detecção de intrusão é a possibilidade de se definir um pequeno conjunto de padrões para serem usados como arquivo de treino representando assinaturas conhecidas, e que seriam suficientes para viabilizar a detecção de novos ataques a partir de similaridades entre ataques conhecidos (Lima, 2005). Há diversas ocorrências de intrusões ou ataques que são somente evoluídos de ataques já conhecidos, a utilização de redes neurais vem antecipar estes ataques que posam ser realizados.

A aplicação I-IDS foi desenvolvida utilizando redes neurais alimentadas a diante o tipo *multilayer preceptron,* devido à capacidade de resolver problema de forma não linear separadamente. Conforma a avaliação de (Lima, 2005) também foi utilizado para o treinamento o algoritmo de retro propagação de erro *backpropagation,* que após a apresentação de cada padrão, calcula o valor de erro da rede e realiza a retro-propagação, atualizando os pesos sinápticos.

Como o propósito deste trabalho é que o IDS efetue a classificação em apenas duas categorias (Intrusivas e normal) fixou-se a entrada da rede neural em 256 neurônios e a saída em 1 neurônio.A aplicação trata como padrão o valor de saída entre o intervalo de -1 a 0 como atividade normal e valores entre 0 e 1 como atividades intrusivas. Na figura 30 é representado graficamente as atividades classificadas como intrusivas e normais.

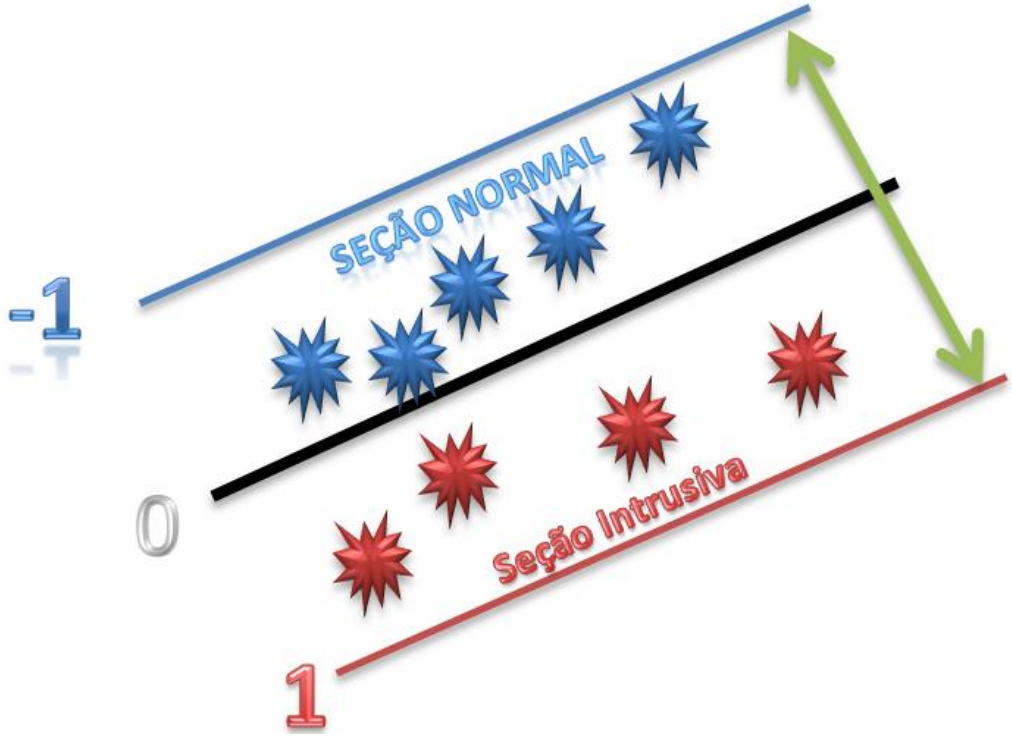

Figura 30 - Classificações das Seções

A aplicação I-IDS possui a flexibilidade de configuração das principais variáveis de configuração da RNA, que é representada na figura 31 e descrita a seguir.

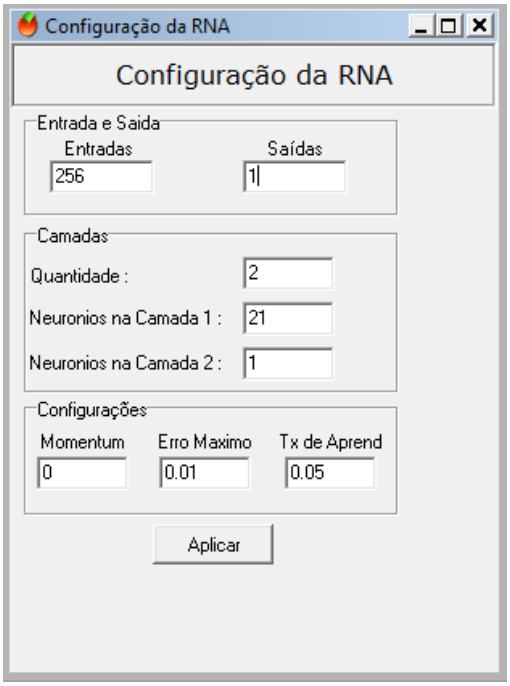

Figura 31 - Configuração da Rede Neural no I-IDS

Onde:

Entradas – Quantidade de Entradas composta pelo vetor de estímulos gerado de módulo de pós-processamento (16 padrões de 16 Bits)

Saídas – Quantidade de saídas da rede que classificam o padrão de entrada

Camada Quantidade – Quantidade de Camadas utilizada na análise. Testes empíricos com a rede neural MLP não demonstram vantagem significativa no uso de várias camadas escondidas.

Neurônios na Camada 1 e 2 – Definição da quantidade de neurônios nas camadas ocultas, que atuam como extrator de características e se conectam ao neurônio de saída, que irá informar o grau de suspeita de cada vetor de estímulo.Para definição foi tomado o devido cuidado na quantidade excessiva , devido a rede memorizar os dados de treinamento,ao invés de extrair as características que permitirão a generalização.

Configurações Momentum – Pode ou não ser utilizado durante o treinamento, pode variar de 0 (Não utilização) á 1.Tem como objetivo aumentar a velocidade de treinamento da rede e reduzir o perigo de instabilidade.

Configurações Erro Máximo – Consiste em encerrar o treinamento após o erro máximo ficar acima do valor pré-definido.

Configuração Taxa de Aprendizado – O parâmetro de taxa de aprendizado pode ter grande influência durante o processo de treinamento a rede neural. Quando mais baixa a taxa de aprendizado, mais lento será o treinamento, mas uma taxa muito alta provoca oscilações no treinamento e impede a convergência do processo de aprendizado.

Para a seleção dos parâmetros da rede neural foi definido como objetivo de obter um modelo que não fosse muito rígido a ponto de não modelar fielmente os dados, mas que também não fosse flexível a ponto de modelar também o ruído presente nos dados.

O treinamento tem como função agregar conhecimento à rede neural, atualizando os pesos as conexões sinápticas de acordo com as informações contidas nos dados de treinamento. A aplicação I-IDS possui dois métodos para definir o momento em que a rede neural deve encerrar o treinamento conforme pode ser visto na figura 32.

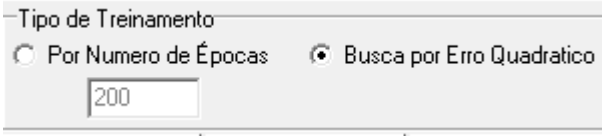

Figura 32 - Configuração do Tipo de Treinamento

O tipo de treinamento realizado por número de ciclos representa o número de vezes em que o conjunto de treinamento é apresentado à rede. Para esta definição foi considerado que um número excessivo de ciclos pode levar à rede a perda do poder de generalização, por outro lado, um pequeno número de ciclos pode não proporcionar o melhor desempenho da rede.

A busca por erro quadrático consiste em encerrar o treinamento após o erro médio quadrático ficar abaixo do valor pré-definido nas configurações da aplicação.

Após o treinamento se concluído é gerado um arquivo de pesos que representa todo o conhecimento adquirido e pode ser persistido até mesmo para outras aplicações. A geração deste arquivo de pesos representa uma forma de persistência de conhecimento adquirido, pois é possível a aquisição de conhecimento carregando os pesos deste arquivo para a rede neural, sem a necessidade de realizar novamente o mesmo treinamento. Desta forma é possível transferir o conhecimento adquirido para outras redes com a mesma estrutura, bastando atualizar seus pesos de acordo com o arquivo estabelecido (Lima, 2005).

Outro ponto bastante positivo da aplicação I-IDS é o fato de ela possibilitar a monitoração do processo de análise e o processo de aprendizado por meio de uma interface gráfica, que além de proporcionar um maior controle ao usuário é mais intuitiva e principalmente facilita a compreensão dos complexos objetivos da aplicação.

5.5 Considerações

A correta definição e planejamento de um projeto são fases fundamentais para se obter o sucesso do projeto. Sobre estes aspectos, o objetivo deste capítulo foi de executar esta definição do projeto deste trabalho, visando obter uma eficiência adequada nos experimentos realizados no capítulo seguinte.

Para isto procurou-se embasar as definições do projeto nos conceitos teóricos vistos anteriormente, utilizando-os como base para a decisão da dos módulos adotados.

Cada um dos módulos foi descrito, abordando suas configurações, deficiências e funcionalidades a fim de descrevê-los de uma forma objetiva e clara, para a posterior compreensão dos experimentos realizados.

6. Experimentos Realizados

Nesta seção são descritas as atividades realizadas sobre a rede Ad Hoc OLSR, o módulo de captura e o sistema de detecção de intrusão I-IDS, buscando demonstrar possíveis diferenciais da utilização do I-IDS na utilização para redes Ad Hoc, sistemas operacionais e abordagens de ataque.

6.1 Experimentos Realizados na Rede

Nos diversos trabalhos pesquisados, poucos se aventuraram a testar uma rede Ad Hoc na prática, em sua maioria utilizavam-se simuladores de rede e é um diferencial destes experimentos realizados neste trabalho.

Obviamente existe uma dificuldade técnica grande de se montar uma rede Ad Hoc OLSR na prática, pois os recursos para tal são altos sendo necessário a alocação de dispositivos de hardware, sejam notebooks computadores, placas de rede adaptáveis a rede Ad Hoc ou outros dispositivos móveis como *SmartPhone* ou PDAs.Também há a dificuldade do espaço físico, que neste caso foi necessário um ambiente bem maior que se esperava no início do trabalho.

Após exaustivos testes com dois nós para compreender e habilitar o funcionamento, foi iniciado o processo de montagem da rede com três nós a fim de realmente validar o funcionamento do protocolo OLSR. Desta forma, a rede foi montada em duas situações, a primeira voltada a somente testar o funcionamento do protocolo OLSR e acompanhar o tráfego de controle do protocolo gerado por cada nó e registrar as mensagens de HELLO e TC emitidas. Para tal foi utilizado uma área menos abrangente onde cada nó enxergava diretamente os outros dois.

Foi avaliada também, a questão da interoperabilidade entre sistemas operacionais (Suse Linux / Back Track quatro e Windows Vista Home) e neste ponto a rede funcionou sem grandes dificuldades, principalmente devido a recente atualização do código fonte da aplicação desenvolvida em C/C++ do OLSR. Como foi citada anteriormente, a maioria das versões do Microsoft Windows vem com o roteamento *Multihop* desabilitado, desta forma em todas as utilizações feitas neste sistema operacional foi necessário a ativação feita no registro do sistema. Caso esta alteração não seja realizada a tabela de roteamento do sistema operacional é atualizada corretamente, mas os saltos multihop, um dos grandes diferenciais das redes Ad Hoc, não ocorrem.

As configurações dos IPs utilizados podem ser realizadas via DHCP, porém talvez não seja algo prático para grandes redes, já que isto poderia se tornar virtualmente impraticável, pois um pedido de DHCP poderia passar por vários nós até ser respondido. O endereço de *broadcast* é convencionado em 255.255.255.255, mas não há razão para especificar explicitamente, já que o OLSR pode sobrescrever o endereço especificado, deve-se apenas garantir que todos os nós utilizem o mesmo endereço de *broadcast*.

Na primeira simulação, foi implantado o protocolo OLSR em cada nó e acompanhado o tráfego gerado, sendo que os nós foram movimentados sem prejudicar o funcionamento da rede, em uma área menor que a representada na imagem, em certos pontos houve certa degradação do sinal, mas sem prejudicar o funcionamento da rede.

O protocolo OLSR não possui nenhum tipo de prevenção a segurança e este fato, pode ser um fator impeditivo para uma implantação real desta modalidade de rede, já que havendo algum atacante nas imediações poderia facilmente se integrar a rede e efetuar ações maliciosas nas redes ou nos nós presentes.

Na figura 33, é apresentada uma mensagem HELLO, encaminhada pelo protocolo OLSR, que por sua vez encaminha pelo protocolo da camada de rede UDP, através da porta 698. Esta mensagem possui o campo Packet Sequence Number que é o identificar único desta mensagem que será utilizado na ordenação das mensagens enviadas pelos nós.

Esta mensagem foi envida do IP 169.254.67.252 para seus vizinhos 169.254.14.254 e 169.254.98.30. Também se podem perceber os campos TTL e Hop Count conforme descrito na seção sobre o protocolo OLSR.

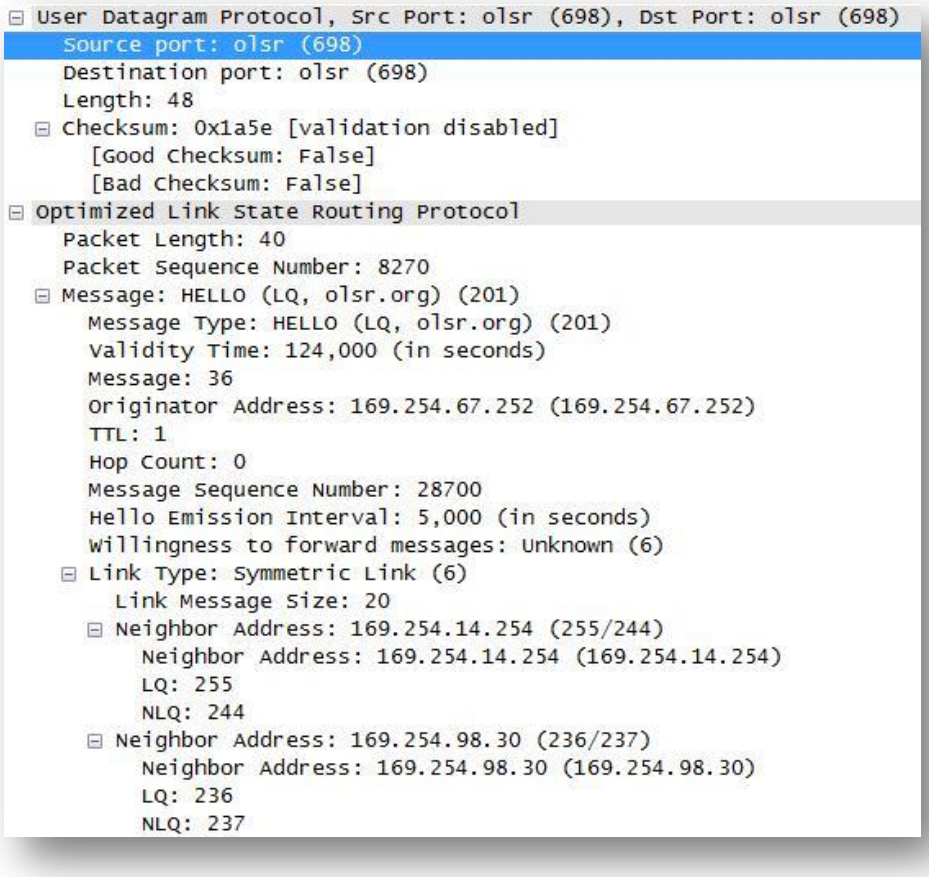

Figura 33 - Pacote UDP Coletado com Mensagem HELLO

Na figura 34 é apresentado um pacote capturado, do protocolo OLSR com uma mensagem TC, que apresenta os campos LQ e NLQ. Estes dois campos não estão padronizados com a especificação da IETF, mas o objetivo é fazer com que um salto com sinal ruim, não seja utilizado caso exista outra rota para o mesmo destino com dois saltos bons.

Na rede OLSR utilizada em Berlin em um nó rodando Linux com processador de 200 MHZ, o protocolo utiliza cerca de 30% da carga do

processador. Na rede implantada neste trabalho houve uma variação insignificante na carga de processamento (menos de 2%), pois além de utilizar nós com capacidade maior, a tabela de roteamento é muito menor (Três Nós), e a movimentação dos nós também é menor.

A demonstração prática do processo de definição dos MPRs é demonstrada na figura 35, nesta situação o nó 169.254.14.254 definiu como a primeira opção de MPR o nó 169.254.98.30, porém este processo seria mais claro se a rede utilizada fosse composta por uma quantidade maior de nós.

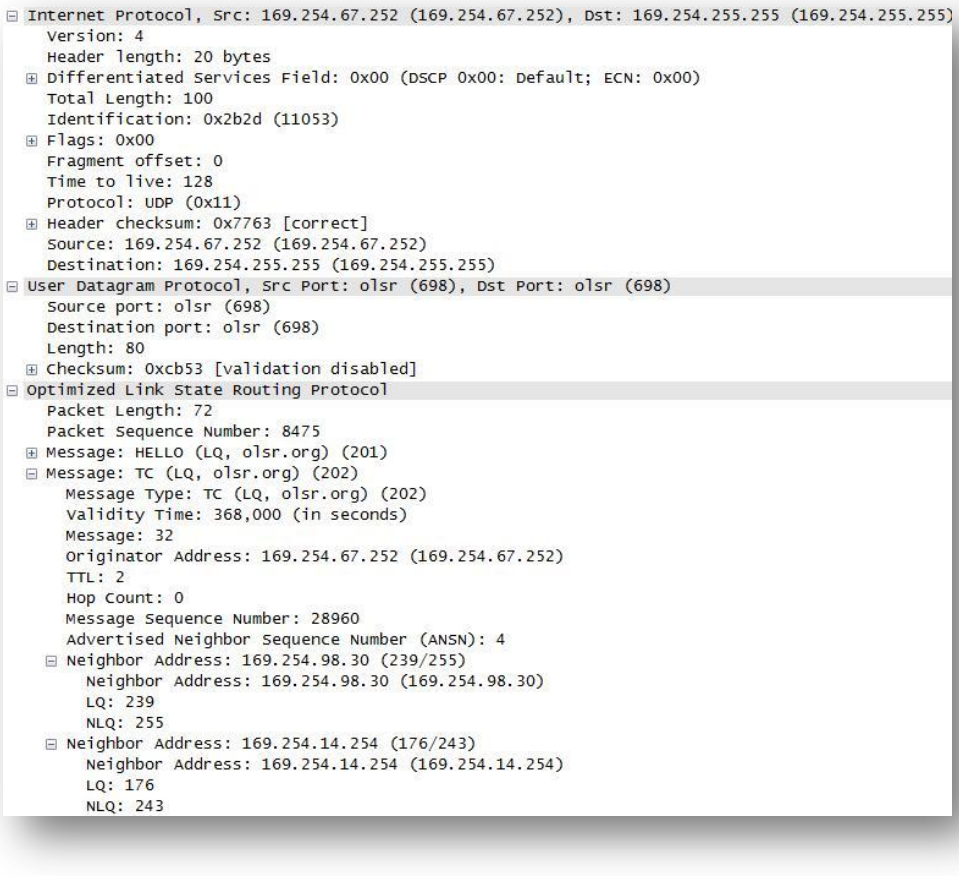

Figura 34 - Pacote UDP Coletado Com Mensagem TC

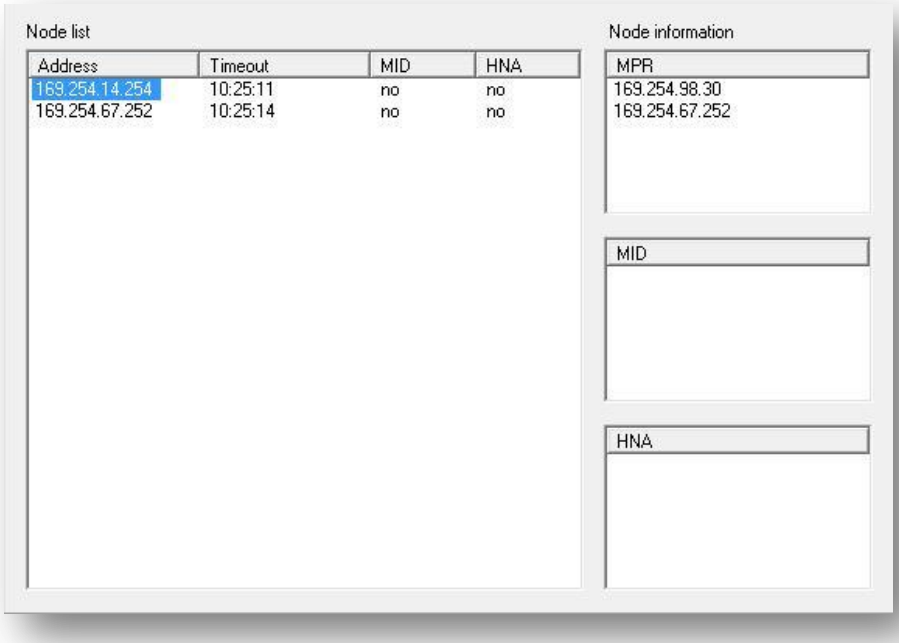

Figura 35 - Interface da Aplicação do Protocolo OLSR - Nós Vizinhos

A segunda implantação da rede, figura 36, teve sua área de atuação ampliada, justamente para testar uma as características do protocolo OLSR, o multihop, fazendo com que o nó 169.254.14.254 enviasse uma mensagem para o nó 169.254.67.252 sem o alcance do sinal direto, ou seja, o 169.254.98.30 teria que efetuar o roteamento da mensagem.

Figura 36 - Ambiente de Simulação da Rede

Ao ativar o nó 169.254.14.254, quase que imediatamente enxergou o nó 169.254.98.30, para depois de cerca de 30 segundos, enxergar o nó 169.254.67.252, ou seja, houve certo atraso na identificação da rota. Depois de estabilizada, foi encaminhada uma mensagem e o executada a o processo

citado no parágrafo anterior, com o nó 169.254.98.30 funcionando como roteador desta mensagem.

A aplicação também registra em seu *log* a possibilidade de saltos e o custo total para definição destes saltos e por conseqüência na rota que será utilizada, conforme a figura 37.

```
--- 10:23:03.780000 ----------------------- TWO-HOP NEIGHBORS

IP addr (2-hop)  IP addr (1-hop)  Total cost
169.254.67.252   169.254.14.254   2.868
169.254.14.254   169.254.67.252   2.917
```

Figura 37 - Possibilidades de Saltos da Rede Utilizada

Como foi citado anteriormente, apesar desta funcionalidade não estar de acordo com o padrão da IEETF, uma funcionalidade muito interessante desta aplicação é o calculo da qualidade do Link que pode varia de 0 a 1 e o ETX que é contagem esperada da transmissão que é calculado por ETX = 1 / (NLQ * LQ).Na figura 38, é demonstrada a tabela de avaliação da qualidade do link.

Source IP addr	Dest IP addr	LQ	ETX
169.254.98.30	169.254.67.252	0.874/0.937	1.220
169.254.98.30	169.254.14.254	0.854/0.960	1.217
169.254.67.252	169.254.98.30	0.937/0.862	1.236
169.254.67.252	169.254.14.254	0.596/1.000	1.677
169.254.14.254	169.254.98.30	0.960/0.862	1.206
169.254.14.254	169.254.67.252	1.000/0.537	1.860

Figura 38 - Configurações dos Links OLSR Possíveis

Outra funcionalidade bastante interessante pela aplicação do OLSR é o acompanhamento do status da alimentação da Energia do nó. A aplicação acompanha especificamente se a energia de cada nó está ativa e qual o percentual disponível de bateria. Para determinadas aplicações com a utilização de dispositivos móveis, ou montagem de redes em situações de emergências, este controle pode se tornar necessário e fundamental.

```
APM info:
      AC status 0
      Battery percentage 91%
```

Figura 39 - Status da Alimentação de Energia do Nó

Também foi executado um teste para avaliar o desempenho em uma aplicação de tempo real, como jogos eletrônicos. Testado sobre a segunda disposição, o jogo eletrônico apresentou um ping de 712 ms para a situação de multihop, ou seja, um tempo muito mais elevado que a comunicação direta.

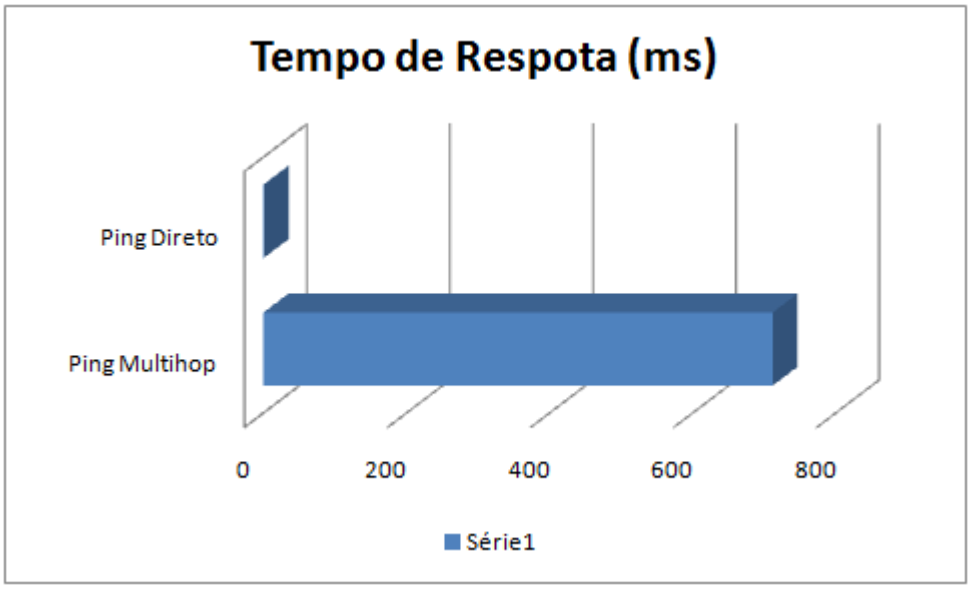

Figura 40 - Tempo de Ping Multihop

6.2 Experimentos Realizados com o Sistema de Detecção de Intrusão I-IDS e Sobre a Rede Ad Hoc

Nesta seção, serão demonstrados os ataques realizados á rede OLSR, com o principal objetivo de alimentar o sistema de detecção de intrusão I-IDS, com o tráfego de situações normais e intrusivas, demonstrando os resultados para as redes Ad Hoc.

Como objetivo secundário também foi realizado alguns testes de ataques específicos a rede Ad Hoc, que serão demonstrados somente para avaliar a questão de segurança desta modalidade de rede. Seguindo os objetivos deste trabalho e o procedimento principal desta seção, foi realizado os passos seguindo o trabalho de (Lima, 2005), para avaliar a aplicabilidade deste modelo de detecção de intrusão para redes móveis sem fio e para comparar os resultados da aplicação para redes estruturadas.

Desta forma foram idealizados dois cenários de captação do tráfego entre dois nós, um com o objetivo de efetuar o treinamento e outro com o objetivo da avaliação.

Nesta abordagem, utilizando dois nós da rede apresentada na seção anterior, foi utilizado um nó para fazer o papel de atacante e outro para fazer o papel de atacado, sendo realizada a captura do tráfego entre os dois nós. A análise dos dados foi limitada nas portas citadas na tabela 9, com o objetivo de limitar o ambiente de testes ao foco deste trabalho.

Tabela 9 - Portas Avaliadas

Porta	Serviço
80	HTTP
8080	HTTP
698	OLSR
53	DNS

Segundo (Lima, 2005), para aprendizado da rede neural é necessário um conjunto de padrões que representes ataques, bem como um conjunto de padrões correspondentes a comportamentos normais, pois estes serviriam de exemplo durante o treinamento supervisionado da rede neural.

Para compor estas amostras, foram capturadas duas categorias de dados. A primeira, não intrusiva, foi capturada com a comunicação normal entre os dois nós em questão, sem risco algum sobre a segurança da rede. Já a segunda com padrões de ataque em que o sistema operacional, Linux Open Suse, foi substituído pelo Linux Back Track 4, pois esta versão do Linux possui uma série de ferramentas de intrusão e ataques passivos como captura de pacotes, análises de vulnerabilidades e ataques ativos.

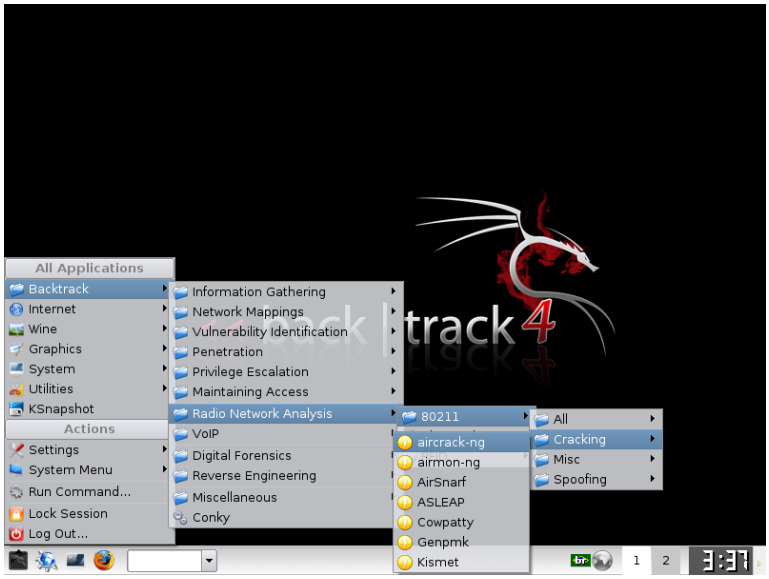

Figura 41 - Linux Back Track e suas Ferramentas

Estas aplicações são de simples utilização, se for considerado em deixar de lado algumas seguranças existentes nos sistemas operacionais utilizados. Desta forma, foram capturadas seções intrusivas através de ataques efetuados a rede com as ferramentas AIRCRACK, AIRSNARF, KISMET, KARMA, WEP_CRACK, MDK2, NMAP, SAINT e NESSUS.

O tráfego normal de comunicação da rede e o tráfego sistêmico foram utilizados como eventos não intrusivos.

Como avaliado por (Lima, 2005), o número de seções capturadas em cada porta deve ser limitado de acordo com o conjunto de padrões de ataques obtidos pelas simulações realizadas, desta forma deve-se fixar a mesma

quantidade de padrões em cada porta monitorada para os padrões normais e para os padrões intrusivos.

Estes padrões devem ser divididos em duas subdivisões. O conjunto Treinamento definido na tabela 10, é o conjunto utilizado durante ao treinamento supervisionado da rede neural, objetivando agregar conhecimento ao módulo de análise. Já o campo Testes é o conjunto definido com a finalidade de testar o conhecimento adquirido na fase de treino, apresentando a rede neural padrões diferentes dos exibidos na fase de treino e estimando a capacidade de generalização.

Tabela 10- Conjuntos de Padrões de Treinamento e Testes

Treinamento				Testes			
Porta	Ataque	Normal	Total	Ataque	Normal	Total	Total Geral
80	41	41	82	8	8	16	98
8080	13	13	26	4	4	8	34
698	14	14	28	7	7	14	42
53	7	7	14	3	3	6	20
Total	75	75	150	22	22	44	194

Seguindo os mesmos procedimentos de treinamento da rede neural e do processo de validação utilizado para acompanhar o aprendizado, que é exposto em (LIMA 2005),a rede neural está pronta para identificar intrusões similares a que ela foi treinada através de inferências a este modelo.Foram definidos dois conjuntos de testes, que não foram apresentados a rede neural a fim de avaliar a eficiência deste modelo para utilização em redes Ad Hoc. Para cada seção analisada o I-IDS apresenta uma análise que varia de -1 a 1, e de acordo com a aproximação da extremidade é classificada como intrusivo ou não intrusivo.

Conforme apresentado na figura 42 o erro quadrático médio variou entre 29,32% e 28,17%. Isto representa que a rede neural soube identificar e classificar corretamente aproximadamente 71% das seções avaliadas. De acordo com a necessidade do usuário, a avaliação de uma seção intrusiva pode ser regulada, ou seja, em sistemas que a segurança é uma situação crítica o limiar de intrusão pode ser extrapolado com a conseqüência de um aumento controlado de falos positivos.

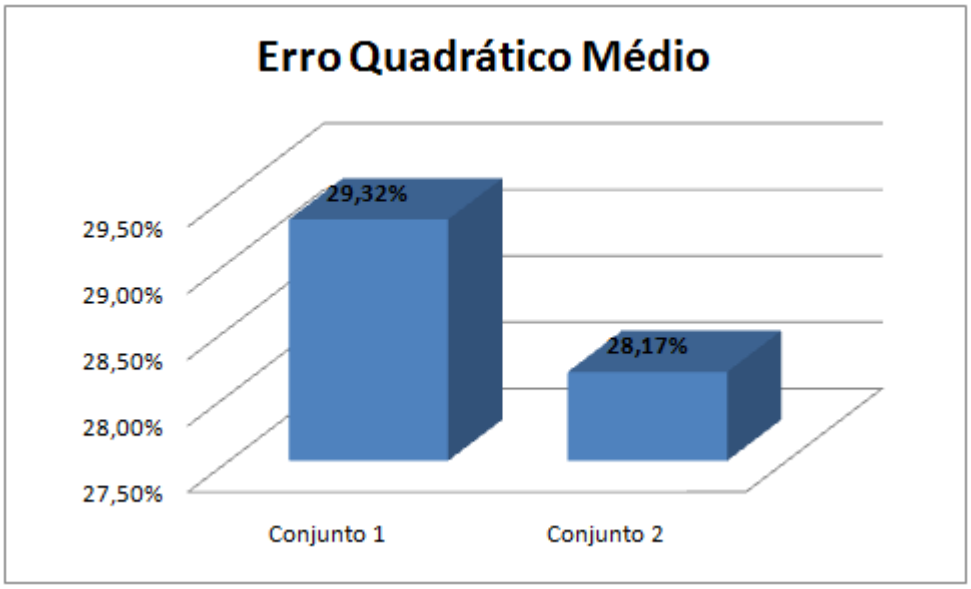

Figura 42 - Erro Quadrático Médio

Os resultados obtidos são satisfatórios e estão dentro do que foi esperado. Isto também confirma que o modelo desenvolvido por (LIMA 2005) pode ser utilizado para redes Ad Hoc devido a sua característica de modularidade de suas configurações e do processo de aprendizagem.

6.3 Considerações

Este capítulo representa a abstração das principais atividades de experimentos, aplicado sobre o modelo proposto. Inicialmente foram descritas as atividades realizadas sobre as redes Ad Hoc OLSR. Nesta seção inicial podem-se comprovar características positivas e negativas de sua utilização. Positivas relacionadas à dinâmica da aplicação, mobilidade dos nós, custo muito baixo de infra-estrutura, abrangência da rede devido aos múltiplos saltos, e negativas, principalmente relacionadas pela falta de segurança e confidencialidade, mas também a dificuldade de utilizar as aplicações em tempo real para múltiplos saltos.

A segunda parte dos experimentos descreve todo o processo de captura do tráfego da rede, execução de ataques a rede, análise do tráfego e resultados. Um dos objetivos deste trabalho, o de avaliar a eficiência do modelo foi demonstrado através do erro quadrático médio obtido que ficou próximo aos 28%, determinando uma eficiência adequada do modelo utilizado. Entretanto na utilização em redes Ad Hoc, este modelo demonstrou que não cobre todas as possibilidades de ataques, necessitando desenvolver e aperfeiçoar o modelo de detecção de forma distribuída.

7. Conclusão

É fato que as redes Ad Hoc possuem questões mercadológicas promissoras devido ao crescimento de dispositivos móveis e redes de sensores em residências e qualquer tipo de aparelhagem eletrônica. Por isto os estudos sobre a segurança destas modalidades de rede também se tornam fundamentais, justificando e evidenciando, o tema deste trabalho.

Como a maioria dos estudos atuais, utiliza simuladores de rede para testar as redes Ad Hoc, em certo ponto, este trabalho pode ser visto uma experiência diferencial, já que a utilização de simuladores de rede abstrai uma série de dificuldades que ocorrem na prática, e omitem situações negativas e positivas desta modalidade de rede.

Conclui-se que a adaptação de um modelo de detecção de intrusão, de uma rede com infra-estrutura para uma rede Ad Hoc é possível, mas às vulnerabilidades e deficiências relacionadas à segurança do OLSR, poderia inviabilizar uma implantação real, para usuários que desejassem o mínimo de segurança e privacidade. Apesar das características positivas de capacidade de auto-organização, modularidade, complexidade, custo e integração das redes Ad Hoc OLSR, a questão da segurança, ainda é um fator crítico que precisa ser pesquisado e desenvolvido, para que haja uma aceitação mercadológica desta categoria de rede.

Os estudos de tempo de respostas de saltos multihop, evidenciaram que o protocolo OLSR não é adequado para aplicações de tempo real como jogos, e que dependendo do projeto deve ser avaliado outro protocolo, para que a suposta aplicação não tenha seu funcionamento prejudicado.

A aplicação I-IDS mostrou-se efetiva devido aos seus recursos de generalização das redes neurais, apresentando resultados satisfatórios também para redes móveis sem fio Ad Hoc. Suas características de modularidade facilitaram a adaptação para este modelo de rede, com a inclusão de ataques específicos a base de conhecimento. Porém com o estudo das deficiências do protocolo OLSR, conclui-se que é necessária, para melhoria da segurança e cobertura de todos os ataques OLSR, uma abordagem diferenciada, utilizando um modelo de detecção de intrusão cooperativo, assim como outras aplicações voltadas a segurança, entre elas, autenticação dos nós e criptografia do tráfego sistêmico.

Dentro destas limitações e benefícios, com este trabalho, pode-se comprovar a viabilidade deste modelo de detecção de intrusão, porém às fragilidades em que uma rede sem fio está sujeita, determinam a necessidade de desenvolvimento de novas características e requisitos de segurança. Algumas destas características estão citadas na próxima seção como sugestão para trabalhos futuros.

8. Trabalhos Futuros

As redes Ad Hoc móveis possuem certas características bem específicas e que para melhorar o desempenho de um IDS, poderiam agregar o desenvolvimento desta aplicação com trabalhos futuros relacionados aos seguintes pontos:

Como um IDS para redes Ad Hoc móveis sem fio necessita ter como requisito básico a coleta do tráfego localmente, poderia ser implementado um módulo de detecção de intrusão global, funcionando paralelamente aos IDSs locais. Formando assim um mecanismo distribuído e cooperativo.

O Desenvolvimento de um IDS vinculado a um protocolo Ad Hoc com artifícios de segurança como autenticação de nós, através de identidade, localização e criptografia.

Como há ferramentas para que em uma rede ad hoc se identifique a localização do nó, poderia se criar um módulo a mais do I-IDS que identificasse a intrusão baseado na localização dos nós.

Atualmente existem ferramentas que possibilitam a quebra, com certo custo do tráfego criptografado. Estas ferramentas poderiam compor mais uma função do I-IDS de foram a analisar também estas criptografias mais simples. IDS.

Devido à restrição na quantidade dos nós, poderia ter-se adotado a utilização de máquinas virtuais, apesar de se perder as características de variação da qualidade do link.

Desenvolvimento de um módulo de resposta ativa de um IDS de forma a isolar o nó suspeito do restante da rede. Para tal podem ser adotados conceitos praticados em redes com infra-estrutura como a “quarentena eletrônica”.

Referências Bibliográficas

CACE TECHNOLOGIES. *WIRESHARK , WINPCAP , WINDUMP , NTAR.* http://www.cacetech.com/ (acesso em 14 de Janeiro de 2009).

CANSIAN, Adriano Mauro. *Desenvolvimento de um Sistema Adaptivo de Detecção de Intrusos em Redes de Computadores.* Tede de Doutorado, São Carlos: Universidade de São Paulo - Institudo de Física de São Carlos, 1997.

DEUS, AREAL PUTINNI JÚNIOR, e Ricardo Staciarini, Rafael Timoteo de Sousa , Flávio Elias Gomes Janaína Laguardia. *A new trust-based extension to the HELLO message improves the choice of routes in OLSR networks.* Brasília, Brazil: University of Brasíılia, 2008.

DUARTE, SOARES, e Otto Carlos Muniz Bandeira Antonio Alexandre de Castro. *Sistemas Detectores de Intrusão em Redes Ad Hoc.* Rio de Janeiro: Universidade Federal do Rio de Janeiro, 2003.

ELSON, J. "tcpflow - TCP Flow recorder." *TCP DUMP Research.* 2001. http://www.circlemud.org/jelson/software/tcpflow/.

FILHO, Gunter Heinrich Herweg. *Simulação de Ataques ao Protocolo de Roteamento AODV.* Trabalho de Conclusão de Curso para Ciências da Computação, Florinópolis: Universidade Federal de Santa Catarina - Departamento de Informática e Estatística, 2005.

FRANCESQUINI, Emilio de Camargo. *Técnicas de detecção de intrusos para redes móveis sem fio.* São Paulo: Universiade São Paulo, 2004.

HAYKIN, Simon. *Redes Neurais - Princípios e Práticas.* Bookman, 2001.

IETF MANET Working Group. *Optimized Link State Routing Protocol.* 3 de Julho de 2003. http://hipercom.inria.fr/olsr/draft-ietf-manet-olsr-11.txt (acesso em 1 de Setembro de 2008).

JULIO, Eduardo Pagani. *Uma Arquitetura de Sistemas de Detecção de Intrusão em Redes Ad Hoc Sem Fio Usando Estenografia e Mecanismos de Repudiação.* Dissertação de Mestrado, Niterói: Universidade Federal Fluminense, 2007.

KUMAR, Sandeep. *Classification and detection of computer intrusions.* Tese de Doutorado, Purdue: Purdue University, 1995.

LIMA, Igor Vinícius Mussoi de. *Uma Abordagem Simplificada de Detecção de Intrusão Baseada em Redes Neurais Artificiais.* Dissertação de Mestrado, Florianópolis: Programa de Pós-Graduação em Ciência da Computação - Universidade Federal de Santa Catarina, 2005.

MCCANNE, CRAIG, e JACOBSON. "PCAP." *Lawrence Berkeley - University of California.* 2002. http://www.tcpdump.org.

MONGE, Alejandro Lopez. *Aprendiendo a programar con Libpcap.* 2005.

MURTHY, Siva Siva Ram, e BS S MANOJ. *Ad Hoc Wireless Networks: Architectures and Protocols.* Saddle River: Prentice Hall, 2004.

NETTO, Roberto Silva. *Detecção de Intrusão Utilizando Redes Neurais Artificiais no Reconhecimento de Padrões de Ataque.* Dissertação de Mestrado, Itajubá: Universidade Federal de Itajubá - Programa de Pós-Graduação em Engenharia Elétrica, 2006.

Network Working Group . *RFC3626 - Optimized Link State Routing Protocol (OLSR).* Outubro de 2003. http://ietfreport.isoc.org/idref/rfc3626/ (acesso em 23 de Dezembro de 2008).

RFC3561, IETF. *Ad hoc on demand distance vector (AODV) routing.* 2003.

ROCHA, Luiz Gustavo Silva. *Uma análise dos Impactos de Ações Maliciosas de Nós no Roteamento em Redes Ad Hoc.* Tese de Mestrado em Ciências Em Engenharia Elétrica, Rio de Janeiro: Universidade Federal do Rio de Janeiro, 2004.

RODRIGUES, Miguel. *Redes Móveis Ad Hoc: Necessidades e Desafios.* Trabalho de Conclusão de Curso de Engenharia de Informática, Porto: Instituto Superior de Engenharia do Porto, 2004.

RUMELHART, Hinton. *Learning internal representations.* MIT, 1986.

RUSSELL, e Peter Norvig Stuar Jonathan. *Artificial Intelligence.* Rio de Janeiro: Elsevier, 2004.

Shaeffer, Carlos Adriani Lara. *Sistema de Detecção de Intrusão Baseado em Redes Neurais.* Dissertação (Mestrado), Florianópolis: Programa de de Pós-Graduação Em Ciências da Computação - Universidade Federal de Santa Catarina, 2003.

Silva, Paulo Fernando da. *Extensão do Modelo IDWG para Detecção de Intrusão em Ambientes Computacionais.* Dissertação de Mestrado, Florianópolis: Universidade Federal de Santa Catarina - Programa de Pós-Graduação em Ciências da Computação, 2004.

SILVEIRA, Fábio Miziara. *Sistema de Detecção de Intrusão por Anomalia No Comportamento para Redes Ad Hoc.* Dissertação de Mestrado, Brasília - Distrito Federal: Universidade de Brasília - Faculdade de Tecnologia - Departamento de Energia Elétrica, 2007.

TAMASHIRO, Clytia Higa. *Uma Análise de Protocolos de Roteamento Anônimo para Redes Sem Fio Ad Hoc Móveis.* Dissertação de Mestrado, Florianópolis: Universidade Federal de Santa Catarina - Programa de Pós-Graduação em Ciências da Computação, 2007.
TANENBAUM, Andrew S. *Computer Networks.* Terceira Edição: Prentice Hall, 1996.
TONNESEN, Andreas. *OLSRD an Ad Hoc Wireless Mesh Routing Daemon.* 2004. http://www.olsr.org/ (acesso em 19 de Dezembro de 2008).