UFSC - Centro Tecnológico - CTC
Departamento de Informática e Estatística – INE
Distributed Mobile Computing & Network Security

Universidade Federal
de Santa Catarina

Detecção de Intrusão em Redes Ad Hoc Móveis através de Rede Neural Artificial

Rômulo Radowitz, Bch. - radowitz@inf.ufsc.br
Igor Vinicius Mussoi de Lima, Msc. - igormussoi@gmail.com
João Bosco Mangueira Sobral, Dr. – bosco@inf.ufsc.br

Resumo

Este trabalho visa mostrar um modelo de um sistema de detecção de intrusão para redes *ad hoc* móveis sem fio, utilizando o protocolo ativo OLSR. O mecanismo de identificação de intrusão é baseado em uma rede neural, que utilizada para aprendizagem do sistema, identificando, armazenando e avaliando o tráfego da rede, quanto a possíveis intrusões. Mostramos aqui a arquitetura global da aplicação e as características principais de um sistema de detecção de intrusão denominado I-IDS. A eficiência do IDS foi avaliada, simulando ataques de forma a compreender e identificar pontos positivos e negativos desta modalidade de rede.

Arquitetura

A figura 1 mostra uma abstração da arquitetura geral de uso do I-IDS e da aplicação proposta. O módulo *Sniffer* é baseado na biblioteca LIBPCAP, e possui a função de capturar o tráfego da rede e preparar os dados para o módulo da aplicação I-IDS. Este módulo possui a função de analisar o tráfego e classificar cada sessão em intrusiva ou não intrusiva. Também possui a função de efetuar o treinamento da rede neural, que é utilizada nesta classificação.

O módulo, utilizando o protocolo OLSR, tem como objetivo, efetivamente, efetuar o controle da rede, definindo e mantendo uma tabela de roteamento, que é baseado na monitoração dos nodos vizinhos e na qualidade de cada conexão, para definir a melhor rota de comunicação entre dois nodos.

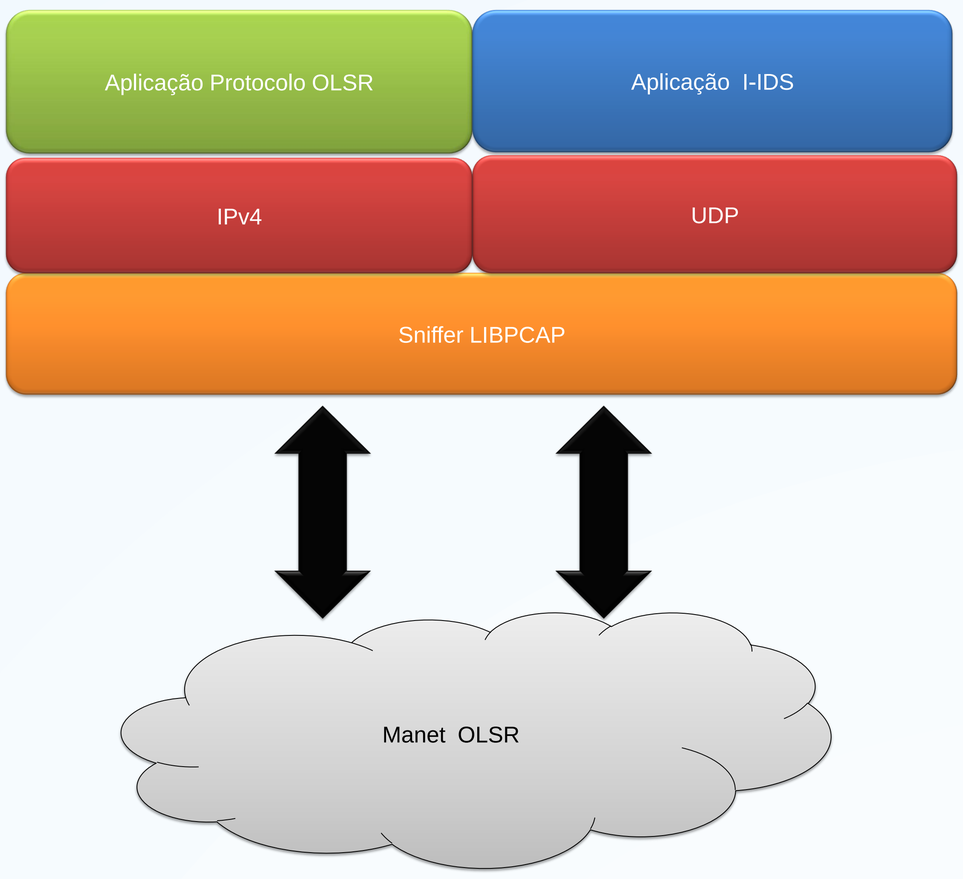

Figura 1 – Arquitetura Geral.

Aplicação Prática do Modelo

A aplicação foi utilizada, com as características de rede mostradas na figura 2. Foram implementados três nodos, cada qual utilizando o sistema de detecção de intrusão I-IDS localmente.

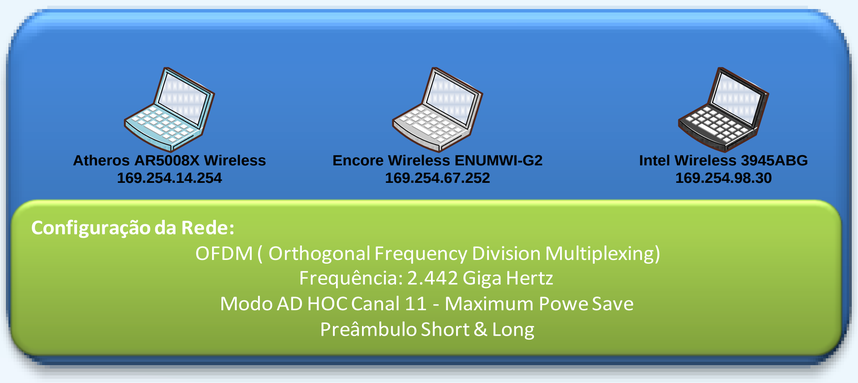

Figura 2 – Aplicação Prática.

Sobre o ambiente da figura 3, foram simulados ataques, através de ferramentas de conhecimento público, sendo que este tráfego foi inicialmente utilizado para treinamento da rede neural. Após o treinamento da rede, foram efetuados ataques que nunca foram apresentados à aplicação. Na avaliação, a eficiência do modelo apresentou um erro quadrático de aproximadamente 29%, fato que representa uma assertividade da classificação em aproximadamente 71% das sessões.

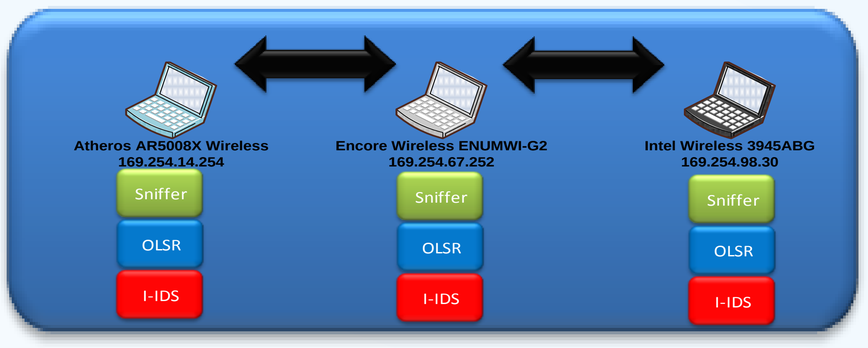

Figura 3 – Ambiente para ataques.

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 dispositivos. Por isto os estudos sobre a segurança destas modalidades de rede também se tornam fundamentais, justificando e evidenciando o tema deste trabalho.

A modularidade das redes *Ad Hoc* OLSR, diminuem a complexidade de manutenção bem como seus custos, permitindo uma solução viável para acessar uma rede de qualquer lugar, devido à facilidade de integração com outras redes. O I-IDS mostrou-se bastante efetivo, devido aos seus recursos de generalização com a rede neural, apresentando resultados satisfatórios para redes *ad hoc* móveis sem fio. Suas características de modularidade facilitaram a adaptação para o modelo de rede *ad hoc* móvel.

DMC–NS
Distributed Mobile Computing
and Network Security