Detecção de Intrusão em Redes Ad Hoc Usando Técnicas de Reconhecimento de Padrões

Ed' Wilson Tavares Ferreira[12], Ruy de Oliveira[1], Gilberto Arantes Carrijo[2], Nelcileno Virgílio de Souza Araújo[3]

[1]Departamento de Informática – Instituto Federal de Mato Grosso (IFMT)
Rua Zulmira Canavarros, 95 - Centro– 78.005-200 – Cuiabá – MT - Brasil

[2]Faculdade de Engenharia Elétrica – Universidade Federal de Uberlândia (UFU)
Uberlândia – MG - Brasil

[3]Departamento de Ciência da Computação - Universidade Federal de Mato Grosso (UFMT) – Cuiabá – MT - Brasil

{edwilson,roliveira}@inf.cefetmt.br, gilberto@ufu.br, nelcileno@yahoo.com.br

Abstract. *The ad hoc wireless networks are very vulnerable to attacks by malicious users, mainly because of the cooperation among their nodes. The methods for detection of attacks are grouped into two categories: analysis of anomalies and signatures. The former detects possible new attacks, which have not been previously discovered, while the latter depends on prior knowledge about the attacks to classify them. This paper presents a proposal for use of wavelets and neural networks to detect and classify attacks. Evaluations by simulation and environmental testing are also presented, and results indicate that this approach is very promising.*

Resumo*. As redes ad hoc sem fio são muito vulneráveis a ataques de usuários mal intencionados, sobretudo, devido à necessidade de cooperação entre os nós que a compõem. Os métodos para detecção de ataques são agrupados em duas categorias: análise de anomalias e assinaturas. Enquanto o primeiro possibilita detectar ataques novos, que não tenham sido descobertos previamente, o segundo depende de conhecimento prévio para classificar os ataques. Este trabalho apresenta uma proposta de uso de wavelets e redes neurais para detecção e classificação de ataques. Avaliações realizadas por meio de simulação e ambiente de testes também são apresentadas, e os resultados obtidos indicam que esta metodologia é muito promissora.*

1. Introdução

As redes ad hoc sem fio, com múltiplos saltos, são constituídas por nós autônomos com capacidade de mobilidade e não dependem de gerenciamento centralizado. O custo dessas redes é reduzido, a instalação e configuração são rápidas e fáceis de serem realizadas. Os serviços de redes são providos pelos próprios nós, onde cada nó contribui com o encaminhamento de pacotes oriundos de seus vizinhos, mantendo a rede funcional. Mesmo quando uma rede possui controle administrativo único, como no caso de uma rede montada em operações militares ou de operações de resgate, cada nó possui autonomia, e a cooperação não pode ser garantida [Félegyházi, Hubaux *et al.* 2006].

Como a comunicação entre os nós é realizada através de um meio comum, o ar, todas as vulnerabilidades intrínsecas das redes sem fio são herdadas pelas redes ad hoc. Além disso, essas redes possuem fragilidades específicas relativas à segurança em função de seu funcionamento, associadas principalmente à ausência de infra-estrutura e a necessidade de encaminhamento colaborativo de pacotes.

A intrusão é definida como uma ação que procura comprometer a confidencialidade, integridade ou a disponibilidade de um recurso. Um IDS (*Intrusion Detection System*) deve ser capaz de identificar ações maléficas, mas sem comprometer o funcionamento normal da rede [Wu e Tseng 2007]. Em geral, as soluções tradicionais de IDS não podem ser empregadas diretamente nas redes ad hoc, devido às características peculiares dessas redes.

De acordo com a abordagem adotada para detectar atividades suspeitas, os IDS podem ser agrupados em duas categorias: detecção por anomalias e por abuso (ou assinatura). A primeira consiste em metodologias que procuram determinar variações nas atividades em relação a um padrão de comportamento. Já a segunda consiste em procurar por padrões de ataques conhecidos nos dados de auditoria.

Comparando-se as duas categorias do parágrafo anterior pode-se dizer que a desvantagem da primeira categoria refere-se ao alto número de falso-positivos, e da segunda é a necessidade de conhecimento prévio dos ataques. Com relação às vantagens, a primeira categoria pode detectar mesmo ataques não conhecidos, ou seja, novos ataques, enquanto que a segunda categoria exige baixo poder de processamento na detecção.

Esse trabalho apresenta um IDS com duas camadas: a primeira baseada em wavelets, para detecção de comportamentos anômalos, e a segunda em redes neurais, para classificação dos ataques.

As transformadas de wavelets podem identificar até mesmo as mudanças sutis em uma função (ou conjunto de dados). Essa capacidade permite detectar variações do comportamento na rede, podendo ser um indício de ataque. As redes neurais, depois de treinadas, não necessitam de grande poder computacional para reconhecimento de padrões. Esses métodos, utilizados em conjunto, permitem então reconhecer e classificar alterações oriundas de ataques na rede.

As redes em malha sem fio são um tipo particular de redes ad hoc, com suporte a múltiplos saltos e roteamento. Uma característica das redes em malha é que seus nós principais são fixos e em geral instalados nos topos dos edifícios, não havendo preocupação com o consumo de energia pelo nó. Por isso, embora tais nós não tenham alto poder computacional, eles podem ser empregados satisfatoriamente na coleta dos dados de auditoria para aplicação da proposta desse artigo.

As demais seções do artigo estão organizadas da seguinte forma: na seção 2 são apresentados os trabalhos relacionados. Na seção 3 é detalhada a proposta de um IDS em duas camadas para redes ad hoc sem fio. Seção 4 apresenta a avaliação de desempenho dessa proposta, e finalmente na seção 5 apresentam-se as conclusões deste artigo.

2. Trabalhos Relacionados

Encontra-se na literatura muitos trabalhos que apresentam propostas de IDS, de uso geral, baseados em wavelet e redes neurais. Porém essas propostas fazem uso dos métodos isolados, sem integração entre eles.

A proposta de [Huang, Thareja *et al.* 2006], [Kim, Reddy *et al.* 2004] e [Magnaghi, Hamada *et al.* 2004] baseiam-se no uso de wavelet para um IDS em roteador de borda. Nessa abordagem, é possível identificar apenas anomalias entre os hosts interno e externo, pois o tráfego entre os nós internos não passam pelo roteador, e por isso não podem ser identificados.

É apresentado por [Hamdi e Boudriga 2007] uma proposta de IDS baseado na detecção de comportamento anômalo em redes com fio. Um módulo classificador cria um perfil da rede que é atualizado constantemente. A detecção é realizada comparando o estado atual com o perfil gerado previamente. Mudanças sutis na rede podem não ser identificadas por esta técnica. Este tipo de IDS consome mais recursos computacionais do que os baseados em assinaturas.

Outras abordagens para IDS, baseados em RNA (Redes Neurais Artificiais) também são encontrados em grande número na literatura. De certa forma, as abordagens são parecidas, a exemplo de [Ahmad, Ansari *et al.* 2008], [Song, Zhang *et al.* 2008], [Yu, Chen *et al.* 2007] e [Mafra, Da Silva Fraga *et al.* 2008]. Neste último, os autores usam duas camadas (Mapas de Kohonen e *Support Vector Machine*), a primeira faz a classificação enquanto que a segunda executa a detecção propriamente dita. Essas abordagens foram empregadas em redes com fio, com a obtenção dos dados de auditoria diretamente de roteadores de borda.

A proposta de [Karygiannis, Antonakakis *et al.* 2006] faz a detecção de nós maliciosos em MANET (*Mobile Ad Hoc Network*) através de um conjunto de métricas e representação por grafos. O sistema percorre todos os nós da rede e realiza testes de encaminhamento de pacotes para a rede local ligada ao nó. Se não houver hosts conectados à rede local dos nós, o sistema poderá concluir que está acontecendo algum tipo de ataque, certamente isso é uma desvantagem desta proposta.

A sugestão apresentada em [Xiao, Hong *et al.* 2006] baseia-se no uso de firewalls em nós da rede. Tais nós são responsáveis pelo controle de ingresso na rede, mas esse procedimento é baseado em endereço MAC. Atualmente é muito simples a clonagem de endereços MAC, desta forma, a proposta é ineficiente.

A abordagem proposta nesse trabalho, para um IDS em duas camadas, aproveitando as vantagens de cada método, em duas fases. Na primeira fase, verificam-se comportamentos anômalos na rede e, caso seja detectado, é iniciado o procedimento para classificação do ataque.

3. Proposta de Uso da Transformada de Wavelet e Redes Neurais para Detecção de Ataques em Redes Ad Hoc Sem Fio

Conforme discutido em [Mishra, Nadkarni *et al.* 2004], um IDS para redes ad hoc sem fio deve ser capaz de funcionar continuamente e de forma transparente para os usuários. Além disso, um IDS deve consumir poucos recursos dos hosts e dos enlaces de rádio, e por fim ser capaz de comunicar-se com outros IDS.

Muitas propostas de IDS dependem de conhecimento prévio dos padrões de ataque, através de detecção de abusos. Essa estratégia baseia-se na identificação de padrões de ataques conhecidos. Abordagens desse tipo não são suficientes, sobretudo em função do grande número de novas técnicas de ataque desenvolvidas diariamente, além da facilidade de utilização até por usuários leigos. Essas técnicas apresentam também elevado número de falso-positivos, ao diagnosticar mudanças no tráfego como possíveis ataques. Portanto, métodos alternativos se fazem necessários, como o proposto aqui.

3.1. **Transformadas de Wavelet**

A transformada de Fourier permite decompor um sinal estocástico em um conjunto de sinais regulares. No domínio de Fourier são conhecidas as componentes principais do sinal, porém não é conhecido o período em que isso ocorreu. As transformadas de wavelet são capazes de decompor um sinal e realizar a análise de freqüência e de tempo simultaneamente. É possível identificar quais componentes de freqüência trazem maior contribuição para o sinal e também em qual período isso ocorre.

Tendo um sinal constituído por um conjunto de métricas colhidas em uma rede ad hoc sem fio, pode-se então empregar as técnicas de processamento digital de sinais. A análise com a transformada de Fourier, para detecção de comportamentos anômalos não é viável, porque se poderia identificar um possível ataque, mas não quando ele ocorreu. Por outro lado, as wavelets podem ser empregadas, pois não possuem tal deficiência.

Para realizar a análise por wavelets, faz-se uso de uma função de protótipo, chamada de wavelet mãe. Essa função matemática tem média zero e é muito sensível a mudança de valores de entrada, e assim, variações da entrada serão detectadas como oscilações produzidas pelas wavelets.

A definição matemática da transformada contínua de wavelet (CWT – *Continuous Wavelet Transform*) é apresentada na Equação 1. As variáveis reais “a” e “b” representam, respectivamente, os parâmetros de escala (contração ou dilatação) e de deslocamento.

A função *f(t)* é a função (contínua ou discreta) em que será aplicada a transformada de wavelet. Na abordagem proposta, são os dados de auditoria obtidos a partir do tráfego da rede.

$$CWT(a,b) = \int_{-\infty}^{+\infty} f(t)\psi^{*}_{a,b}(t)dt \quad \textbf{(1)}$$

A função $\psi_{a,b}(t)$ é a wavelet, matematicamente é definida como apresentada na Equação 2. O asterisco indica que se trata do conjugado complexo da função.

$$\psi_{a,b}(t) = \frac{1}{\sqrt{a}}\psi\left(\frac{t-b}{a}\right), a \neq 0, b \in \Re \quad \textbf{(2)}$$

As transformadas de wavelets são formadas por diferentes famílias de equações com aplicações em várias áreas de conhecimento [Jansen e Oonincx 2005]. Escolhido então a wavelet $\psi_{a,b}(t)$, e aplicada sob uma função, ou conjunto de dados $f(t)$, os valores obtidos na transformada contínua da wavelet CWT(a,b) são conhecidos como coeficientes. As variações desses coeficientes estão relacionadas com a variação dos

dados de entrada. Quando ocorrem pequenas variações na função de entrada *f(t)* obtemos coeficientes de baixa amplitude. Enquanto variações abruptas acarretam em coeficientes de alta amplitude. Dessa forma, sempre que a wavelet apresentar altos coeficientes, pode haver uma suspeita que a rede encontra-se sob ataque ou tenha ocorrido um evento inesperado (quebra do enlace, movimentação do nó) que causou um distúrbio no sinal.

Exatamente por conta dessa sensibilidade da transformada wavelet em detectar variações no fluxo analisado, é que se torna muito importante a sua configuração, a fim de se minimizar o número de falsos positivos.

3.2.**Redes Neurais Artificiais**

A pesquisa sobre redes neurais artificiais teve início nos anos 40, através dos estudos de [Mcculloch e Pitts 1943], com analogia entre células vivas e o processo eletrônico, através da simulação do comportamento do neurônio biológico. Seu objetivo é representar computacionalmente o cérebro humano. Em redes neurais, o neurônio também é chamado de unidade ou nó. O modelo possui um conjunto de pesos, uma unidade de soma ou viés (correspondente à sinapse do neurônio biológico) e uma função de ativação ou de transferência [Cheriet, Kharma *et al.* 2007].

Uma característica importante das redes neurais é a capacidade de aprendizado. Neste processo, a rede adquire a habilidade de responder a estímulos, através do ajuste de parâmetros internos. Existem várias técnicas para o aprendizado da rede: aprendizado por correção de erro, aprendizado baseado em memória e aprendizado competitivo. A representação do conhecimento da rede relaciona-se com os pesos definidos para as conexões e sua formação da base de conhecimento.

As redes neurais possuem alta capacidade de reconhecimento de padrões, que tem por objetivo a classificação em categorias. Essa característica, aliada à competência de generalização, permite o uso das redes neurais em IDS. Porém, somente reconhecerá ataques para os quais foram previamente treinadas. Além disso, o uso de redes neurais tem um processamento muito intenso na fase de treinamento que exige muito do poder computacional e energético do nó. Em contrapartida, na fase operacional ocorre, relativamente, uma baixa demanda dos recursos do nó.

3.3.**Modelo Proposto**

Nesse trabalho é proposto o uso de um IDS local com detecção híbrida, em duas camadas. A primeira verifica comportamentos anômalos, enquanto que a segunda, classifica os ataques. A primeira camada analisa a rede, através de uma transformada de wavelet. Quando os coeficientes da wavelet ultrapassam certo limiar, indicando um comportamento anômalo, a segunda camada é utilizada para classificar o possível ataque.

Várias métricas podem ser utilizadas (em conjunto ou de forma separada), para compor o perfil de funcionamento da rede. Exemplos de métricas importantes incluem:

- Banda Disponível ou Utilizada;
- Número de Conexões Ativas;
- Número de Fluxos Ativos;

- Número de Pacotes Transmitidos ou Recebidos;
- Quantidade de Bytes Transmitidos ou Recebidos;
- Taxa de Transmissão.

Há sempre um limiar separando um comportamento normal de um comportamento anômalo. Neste artigo, o limiar é dado pelo desvio padrão da distância euclidiana entre os coeficientes da transformada de Wavelet.

A distância euclidiana entre os coeficientes é definida pela Equação 3,

$$D_e = \sqrt{(C_a - C_b)^2 + (t_a - t_b)^2} \quad \textbf{(3)}$$

Onde:

C_a – indica o valor do coeficiente da transformada de Wavelet no dado auditado a.

C_b – indica o valor do coeficiente da transformada de Wavelet no dado auditado b.

t_a – indica o tempo em que o valor do coeficiente da transformada de Wavelet foi calculado no dado auditado a.

t_b – indica o tempo em que o valor do coeficiente da transformada de Wavelet foi calculado no dado auditado b.

Como a diferença entre os tempos t_a e t_b sempre será 1, pois os dados são auditados de 1 em 1 segundo, podemos desconsiderá-la e reduzir a distância euclidiana à Equação 4.

$$D_e = \sqrt{(C_a - C_b)^2} \quad \textbf{(4)}$$

A distância euclidiana foi escolhida por mostrar quando ocorre uma alteração nos valores dos coeficientes. Sendo assim, quanto maior o valor da distância euclidiana entre dois coeficientes, maiores são as chances de ocorrer um comportamento anômalo no tráfego da rede. Mas como calculamos a distância euclidiana para todos os valores dos coeficientes, precisamos obter uma medida da dispersão estatística que indique o quão longe os valores calculados se encontram do valor médio. Esta medida define o limiar de um comportamento normal.

O algoritmo da primeira camada, de forma simplificada é apresentado na Figura 1. Os dados de auditoria, que serão utilizados para cálculo da métrica, são obtidos através da captura do tráfego na rede. Note que o algoritmo fica continuamente executando para auditar os dados e calcular os coeficientes relacionados. A seguir, a distância euclidiana entre os coeficientes é calculada, assim como seu desvio padrão, que é o limiar proposto no nosso algoritmo. Para valores maiores que o limiar, um comportamento anômalo é inferido, que ativa o algoritmo de redes neurais para classificar o possível ataque.

A segunda camada é formada por um conjunto de quatro redes neurais artificiais. Essas redes foram treinadas para reconhecer quatro classes distintas de ataques, conforme apresentados na Tabela 1.

```
Algoritmo IDS_Wavelet_e_Redes_Neurais
Declare S – Conjunto de dados auditados no tráfego da rede
        C – Conjunto de coeficientes da transformada Wavelet
        DE – Conjunto de valores correspondente a distância euclidiana entre os coeficientes da transformada Wavelet
        Limiar – valor máximo para considerar uma função f(t) como comportamento normal
Início
      Repita Enquanto Houver Dados de Auditoria
      S = Dados de Auditoria
      C = Calcular Coeficientes Wavelet(S)
      DE = Calcular Distância Euclidiana(C)
      Limiar = Calcular Desvio-Padrão(DE)
      Se (C > Limiar) Então
            Utilizar Redes Neurais para confirmar ataque
      Fim (Se)
Fim
```

Figura 1. Algoritmo Proposto

Cada conjunto de redes neurais é formado por um MLP (*Multilayer Perceptron*) e treinado com algoritmo *back propagation*. Há 41 neurônios na camada de entrada, 20 neurônios na camada oculta e um neurônio na camada de saída. O valor de ativação do neurônio da camada de saída é de 0,8, com o uso da função de tangente hiperbólica. Uma descrição sobre o funcionamento do MLP pode ser encontrada em [Yao 1999] e [Pal e Mitra 1992].

Tabela 1. Classe de Ataques

Classe	**Significado**	**Descrição**
U2R	Aumentar Privilégios	Acesso não autorizado com intuito de aumentar privilégios.
R2L	Remoto para Local	Tentativa de acesso remoto não autorizado, por exemplo, pelo uso de quebra de senhas.
Probe	Sondagem	Tentativa de identificar serviços ativos através de varreduras de portas.
DoS	Negação de Serviço	Caracteriza-se pelo envio de grande número de solicitações a um mesmo host, em curto período de tempo.

A prova de conceito foi realizada utilizando-se o software Matlab [The Matworks 2008], que é um ambiente voltado para cálculos numéricos com ferramentas capazes de reproduzir importantes classes de processos dinâmicos, permitindo a execução de cálculos matemáticos de forma simples, enquanto estende a possibilidade de reproduzir um cenário simulado. Neste artigo foi empregado o MatLab para implementar o mecanismo de detecção baseado em anomalia, através da biblioteca *Wavelet Toolbox* e a classificação de possíveis ataques detectados, através da biblioteca *Neural Network Toolbox*.

4. Avaliação de Desempenho

Para validar o IDS proposto, diversos experimentos foram realizados. No primeiro experimento, apresentado na Figura 2, a ferramenta NCTUns [Wang, Chou *et al.* 2003] foi utilizada para simular um ataque de negação de serviço (*DoS – Denial of Service*) sobre a rede. Há cinco nós na rede que estão a uma distância de 200 metros dos seus vizinhos. Os ataques ocorrem no período entre 100 e 150 segundos a partir do início da simulação.

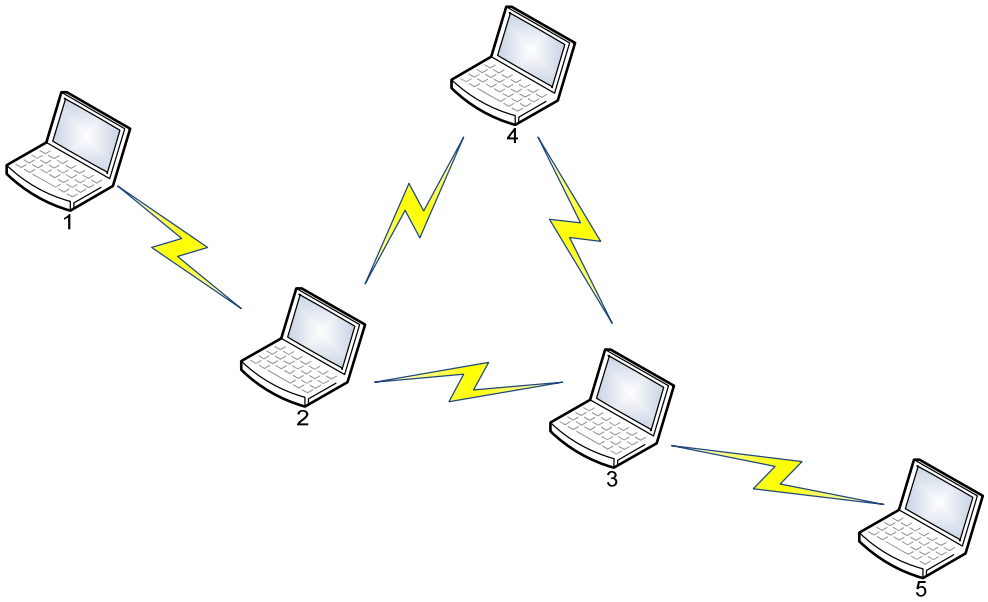


Figura 2. Topologia Simulada

O objetivo do experimento foi gerar dados para auxiliar na escolha de uma família apropriada de wavelet. A Figura 3 mostra a comparação dos resultados para as famílias de wavelets Daubechies, Symlets, Coiflets e Meyer. Observa-se que todas as famílias avaliadas podem detectar as perturbações no sinal de forma efetiva.

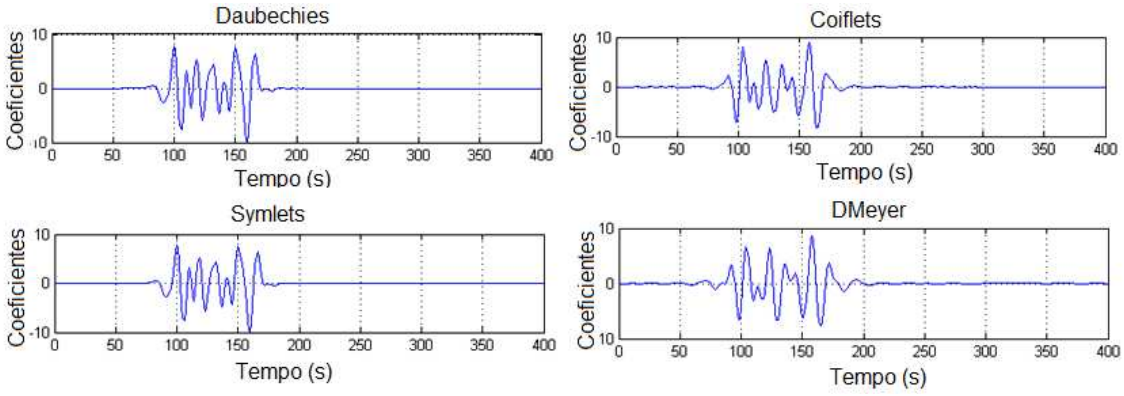


Figura 3 Família de wavelets (coeficiente x tempo)

Em outro experimento, um ambiente de teste foi montado com uso de três equipamentos: dois notebooks e um aparelho celular, todos com interface de rede sem fio, cujas configurações são apresentadas na Tabela 2 e a topologia na Figura 4. Todos os três equipamentos possuem conectividade entre si, formando uma rede ad hoc sem fio.

Tabela 2. Configuração do Laboratório

Equipamento	1	2	3
Tipo	Notebook	Notebook	Smartphone HTC Touch
Sistema Operacional	Linux Fedora 8	Windows XP XP2	Windows Mobile 6.0 Pro
Interface de Rede	IEEE 802 a/b/g	IEEE 802 a/b/g	IEEE 802.11b/g
Função	Atacante	Vítima	Host na rede
Softwares Utilizados	Nmap e Servidor Web	Navegador de Internet e Sniffer de Rede	Navegador de Internet

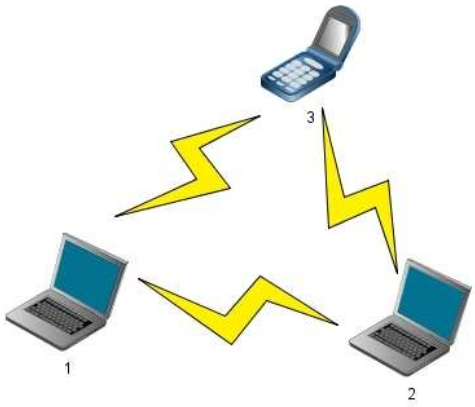


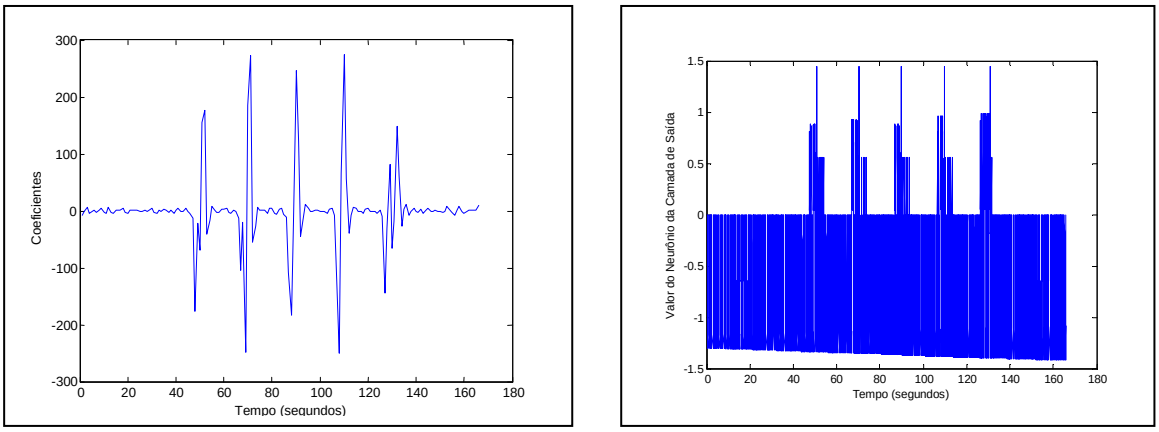
Figura 4. Cenário de testes

Os testes foram realizados com ataques do tipo TCP/RPC (*Remote Procedure Call*), durante os períodos indicados na Tabela 3. Esse tipo de ofensiva foi escolhido pela sua popularidade nos dias atuais e por ser comum sua utilização para enumeração de serviços que estão sendo executados no nó alvo.

Tabela 3. Períodos do Ataque TCP/RPC

Ataques	Período (em segundos)
Primeiro	Entre 47 a 50
Segundo	Entre 67 a 69
Terceiro	Entre 86 a 89
Quarto	Entre 106 a 108
Quinto	Entre 126 a 130

Após a coleta, os dados de auditoria foram submetidos ao mecanismo baseado em wavelet do IDS e foram obtidos os coeficientes apresentados na Figura 5.(a), onde é possível verificar cinco momentos de perturbações no sinal que correspondem aos cinco intervalos dos ataques. Dessa forma, a wavelet foi capaz de detectar, satisfatoriamente, a anomalia.



(a) Camada Wavelet (Coeficientes x Tempo)

(b) Camada Rede Neural (Valores do neurônio da camada de saída x Tempo)

Figura 5. Resultados experimentados pelo IDS híbrido proposto no cenário de ataque TCP/RPC.

Durante o funcionamento dos testes, todos os pacotes que trafegaram pela rede foram capturados, que totalizaram 17.317. Desse conjunto, 1000 pacotes foram selecionados para treinamento, e 350 para testes de validação da segunda camada do IDS. Todos os pacotes foram então apresentados à segunda camada para classificar o ataque. A classificação positiva é obtida quando o valor do neurônio da camada de saída é próximo de seu valor de ativação, nesse caso 0,8.

Para facilitar a comparação entre os resultados das duas camadas, os valores do neurônio da camada de saída foram agrupados e apresentados no mesmo período de tempo de observação da rede, isso provocou um pequeno deslocamento no gráfico, como mostrado na Figura 5.(b). Ainda na Figura 5.(b), observa-se que a rede neural classificou de forma satisfatória os cinco ataques realizados.

4.1. **Eficiência de Detecção**

Para medir a eficiência da detecção de ataques, fez-se uso da base de dados apresentada na Competição Internacional de Mineração de Dados (KDD - *Knowledge Discovery in Database*) de 1999 [Lippmann, Haines *et al.* 2000]. O conjunto de dados foi originado a partir da captura de pacotes durante nove semanas, em uma rede real. Para utilização da base do KDD foi necessário um pré-processamento, para agrupar os ataques em categorias.

O treinamento das redes neurais foi realizado de acordo com os parâmetros apresentados na Tabela 4. Foi considerado margem de erro de até 30% para a verificação dos acertos. O tempo gasto de treinamento foi elevado, porém, em todos os testes, a detecção foi muito rápida, a classificação aconteceu com tempo inferior a um segundo. Os cálculos foram executados com um computador equipado com Processador Intel Core 2 DUO T5500 com 2GB de RAM e Sistema Operacional Windows Vista Business, sem utilização de recursos de *Multithreading*.

Tabela 4. Parâmetro de Criação e Treinamento das Redes Neurais

Classe	Época	Amostras	Erro Quadrático Médio	Taxa de Acerto	Tempo Utilizado
U2R	100	15000	$5{,}23x10^{-05}$	99,83%	00:19:34
R2L	100	15000	$1{,}14x10^{-12}$	100,00%	00:02:48
Probe	1000	30000	$2{,}70x10^{-04}$	99,37%	06:40:02
DoS	1000	30000	$1{,}16x10^{-04}$	99,76%	06:37:41

Cada registro da base, composto por 41 colunas, representa uma conexão, e já contém a correta classificação do tráfego (normal ou ataque). Assim, é possível medir a eficiência da proposta e comparar com outros trabalhos, como apresentado na Tabela 5. As comparações foram realizadas a partir do treinamento do conjunto de redes neurais com 30000 amostras e 1000 épocas.

Tabela 5. Comparação com diversos trabalhos

Proposta	Taxa de Acerto
Anomalous Payload-based IDS [Bolzoni, Zambon *et al.* 2006]	93,70%
HPCANN [Liu, Yi *et al.* 2007]	77,49%
MADAM ID [Lee e Stolfo 2000]	77,97%
Multi-level Hybrid Classifier [Xiang e Lim 2005]	89,19%
Polvo-IIDS [Mafra, Da Silva Fraga *et al.* 2008]	96,55%
Proposta desse artigo	96,10%

A taxa de acerto médio foi calculada através da comparação entre os dados reconhecidos pela proposta deste trabalho e as classificações já efetuadas na base de dados do KDD.

A avaliação de desempenho de um IDS também pode ser realizada pelo cálculo de outras métricas. Verdadeiros Positivos (*TP – True Positives*): o IDS identifica uma ação maléfica corretamente. Verdadeiro Negativo (*TN – True Negatives*): o IDS identifica uma ação normal corretamente. Falso Positivo (*FP – False Positives*): o IDS identifica uma ação normal como sendo maléfica. Falso Negativo (*FN – False Negatives*): O IDS identifica uma ação maléfica como sendo normal. A Taxa de Detecção (*DTR – Detection Rate*) é definida como TP/(TP+FN), a Taxa de Falso Positivo (*FPR – False Positive Rate*) é definida como FP/(TN+FP) e por fim, Exatidão Global (*AO – Overall Accuracy*) é definida como (TP+TN)/(TP+TN+FP+FN).

Para realizar o cálculo das métricas, como apresentados na Tabela 6 foram utilizados para treinamento das redes neurais um conjunto de 10.000 amostras, com critério de parada igual a 100 época ou erro 10^{-6}, enquanto que os testes foram executados com 50.000 amostras, com todos os dados oriundos do KDD. Algumas verificações com 400.000 amostras também foram executadas, porém não houve mudança significativa dos resultados. Utilizou-se os recursos de *Multithreading* do computador, com isso, o tempo médio de treinamento foi reduzido para 167 segundos, mantendo-se o tempo médio de classificação de meio segundo.

Tabela 6. Análise de desempenho

Tipo	TP (%)	TN (%)	FP (%)	FN (%)	DTR (%)	FPR (%)	AO (%)
U2R	0	99,99	0	0,002	0	0	99,99
R2L	0	99,80	0	0,136	0	0	99,86
Probe	0	98,34	0	1,66	0	0	98,34
DoS	30,79	64,67	0,06	4,38	87,52	0,10	95,54
Média	-	-	-	-	21,88	0,02	98,43

Pela Tabela 6, é evidente que o modelo proposto de IDS teve uma taxa muito baixa de falso positivo e possui uma capacidade de detecção efetiva. Também, podemos observar que em todos os testes, foram detectados com uma exatidão global (OA) superior a 95%. Os resultados apresentados servem para reforçar a eficiência do nosso modelo proposto de IDS

4.2.**Análise dos Resultados Obtidos**

As anomalias detectadas pelo mecanismo de wavelet encorajam mais pesquisas sobre seu uso em IDSs. O principal problema parece ser a possibilidade do alto número de falsos positivos. Isto é, variações tal como a movimentação de um nó na rede pode ser erroneamente detectada como anomalia. Dessa forma, avanços nesta questão são certamente necessárias. Com relação ao desempenho das redes neurais, embora o nível de classificação tenha sido muito bom, os requisitos de processamento continuam sendo uma preocupação, principalmente na fase de treinamento.

Acredita-se que se a rede ad hoc sem fio for configurada como uma rede em malha, o uso de redes neurais na classificação de ataques pode ser viável, pois nesse caso, os nós da rede pertencente ao *backbone* são fixos e, assim, podem ser implementados com máquinas robustas que suportam a exigência computacional das redes neurais na fase de treinamento. Finalmente, os bons resultados da comparação com as abordagens existentes indicam que a proposta desse artigo é tão efetiva quanto às outras no cenário avaliado. Entretanto, para resultados mais conclusivos outros cenários devem ser testados.

5. Conclusões

Neste trabalho foi apresentada uma proposta de um IDS baseado em Wavelets e Redes Neurais Artificiais, para detecção e classificação de anomalias causadas por ataques em redes ad hoc sem fio.

A análise por wavelet permite divisões sucessivas em aproximação e detalhe. Esse método possui a capacidade de ajuste adaptativo e pode detectar anomalias de baixa, média e alta intensidade. Mesmo pequenas anomalias ao longo do tempo, poderão ser identificadas através do uso de wavelet.

É necessário o treinamento das redes neurais, antes de sua utilização. Após esta fase, a classificação ou reconhecimento de padrões, que indicam o ataque é relativamente simples e rápido. Quando um novo tipo de ataque é descoberto, torna-se necessário treinar novamente a rede neural.

A abordagem híbrida, utilizada neste trabalho, permite fazer uso das melhores características de cada técnica, sendo essa uma das principais contribuições. Além disso, o uso conjunto permite a redução de falso-positivos, se comparado com a utilização isolada da primeira camada. Contudo, a utilização de redes neurais na classificação de ataques deve ser empregada com a limitação de ser implementada em redes em malha sem fio, pois o aprendizado das redes neurais demanda processamento que é algo escasso quando tratamos de redes ad hoc sem fio.

Os resultados obtidos aqui permitem concluir que os métodos empregados são promissores, pois um bom nível de detecção foi conseguido nas avaliações apresentadas.

Como trabalho futuro pretende-se aplicar outros métodos de reconhecimento e classificação de padrões, tais como: *naive-bayes*, lógica *fuzzy*, quantificação vetorial, nesta abordagem híbrida de IDS. Como também, avaliar esta proposta em uma rede ad hoc sem fio real, fora de um ambiente controlado de laboratório.

Referências Bibliográficas

Ahmad, I., M. A. Ansari, *et al.* (2008). "Performance comparison between backpropagation algorithms applied to intrusion detection in computer network systems": World Scientific and Engineering Academy and Society (WSEAS) Stevens Point, Wisconsin, USA. 47-52 p.

Bolzoni, D., E. Zambon, *et al.* (2006). "POSEIDON: a 2-tier Anomaly-based Network Intrusion Detection System", Proceedings of the 4th IEEE International Workshop on Information Assurance (IWIA). 144-156 p.

Cheriet, M., N. Kharma, *et al.* (2007) "Character Recognition Systems - A Guide for Students and Practioners", Hoboken: John Wiley & Sons, Inc

Félegyházi, M., J. P. Hubaux, *et al.* (2006) "Nash Equilibria of Packet Forwarding Strategies in Wireless Ad Hoc Networks", IEEE Transactions on Mobile Computing, p.463-476.

Hamdi, M. e N. Boudriga. (2007) "Detecting Denial-of-Service attacks using the wavelet transform", Computer Communications v.30, n.16, p.10.

Huang, C. T., S. Thareja, *et al.* (2006). "Wavelet-based real time detection of network traffic anomalies", Workshop on Enterprise Network Security and the 2nd International Conference on Security and Privacy in Communication Networks, Baltimore, MD, USA. 1-7 p.

Jansen, M. H. e P. J. Oonincx. (2005) "Second Generation Wavelets and Applications", London: Springer

Karygiannis, A., E. Antonakakis, *et al.* (2006) "Detecting Critical Nodes for MANET Intrusion Detection Systems", 2nd International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, June, v.29.

Kim, S. S., A. L. N. Reddy, *et al.* (2004) "Detecting Traffic Anomalies through Aggregate Analysis of Packet Header Data", LECTURE NOTES IN COMPUTER SCIENCE, p.1047-1059.

Lee, W. e S. J. Stolfo. (2000) "A framework for constructing features and models for intrusion detection systems", ACM Transactions on Information and System Security (TISSEC), v.3, n.4, p.227-261.

Lippmann, R., J. W. Haines, *et al.* (2000) "The 1999 DARPA off-line intrusion detection evaluation", Computer Networks, v.34, n.4, p.579-595.

Liu, G., Z. Yi, *et al.* (2007) "A hierarchical intrusion detection model based on the PCA neural networks", Neurocomputing, v.70, n.7-9, p.1561-1568.

Mafra, P. M., J. Da Silva Fraga, *et al.* (2008). "POLVO-IIDS: Um Sistema de Detecçao de Intrusao Inteligente Baseado em Anomalias", SBSeg2008, Gramado. 201-214 p.

Magnaghi, A., T. Hamada, *et al.* (2004). "A wavelet-based framework for proactive detection of network misconfigurations": ACM New York, NY, USA. 253-258 p.

Mcculloch, W. S. e W. Pitts. (1943) "A logical calculus of the ideas immanent in nervous activity", Bulletin of Mathematical Biology, v.5, n.4, p.115-133.

Mishra, A., K. Nadkarni, *et al.* (2004) "Intrusion detection in wireless ad hoc networks", Wireless Communications, IEEE [see also IEEE Personal Communications], v.11, n.1, p.48-60.

Pal, S. K. e S. Mitra. (1992) "Multilayer perceptron, fuzzy sets, and classification", Neural Networks, IEEE Transactions on, v.3, n.5, p.683-697.

Song, G., J. Zhang, *et al.* (2008). "The Research of Dynamic Change Learning Rate Strategy in BP Neural Network and Application in Network Intrusion Detection". 513-513 p.

The Matworks. (2008) "Matlab 7 Getting Started Guide", Natick, MA: Matworks

Wang, S. Y., C. L. Chou, *et al.* (2003) "The Design and Implementations of the NCTUns 1.0 Network Simulator", Computer Networks, v.42, n.2, p.175-197.

Wu, S. e Y. Tseng. (2007) "Wireless Ad Hoc Network - Personal-Area, Local-Area, and the Sensory-Area Networks", Boca Raton: Auerbach Publications

Xiang, C. e S. M. Lim (2005). "Design of Multiple-level Hybrid Classifier for Intrusion Detection System", 2005 IEEE Workshop on Machine Learning for Signal Processing. 117-122 p.

Xiao, H., F. Hong, *et al.* (2006) "Intrusion Detection in Ad-hoc Networks", Journal of Communication and Computer, v.3, n.1, p.42-47.

Yao, X. (1999) "Evolving artificial neural networks", Proceedings of the IEEE, v.87, n.9, p.1423-1447.

Yu, L., B. Chen, *et al.* (2007). "An Integrated System of Intrusion Detection Based on Rough Set and Wavelet Neural Network", Third International Conference on Natural Computation: IEEE Computer Society. 194 - 199 p.