# UM ESTUDO SOBRE SISTEMAS DE DETECÇÃO DE INTRUSÃO BASEADOS EM REDES NEURAIS ARTIFICIAIS

DOMARYS CORRÊA[1];
MARILTON AGUIAR[2];

*[1]Universidade Federal de Pelotas (UFPel)– ddscorrea@inf.ufpel.edu.br*
*[2]Universidade Federal de Pelotas (UFPel) - marilton@inf.ufpel.edu.br*

## 1. INTRODUÇÃO

Com o avanço tecnológico computacional e a globalização de informações de modo virtual houve um aumento significativo na utilização de redes para a ligação entre instituições, entidades, empresas e entre estas e seus clientes e fornecedores, aumentado exponencialmente a quantidade e velocidade de troca de dados; como consequência deste aumento tem-se o crescimento acelerado de ataques que visam acesso, manipulação e liberação de informações por pessoas não autorizadas (LIMA, 2005).

Para se combater estes ataques e invasões há uma grande variedade de ferramentas de segurança disponíveis no mercado atual, como antivírus e o firewall, entre outras ferramentas. Porém grande parte destes mecanismos de defesa se baseiam em um script regular de tentativa de invasão, criados para detectar e combater ataques com uma determinada assinatura já conhecida.

Assim como a evolução em termos de software e hardware é crescente, as tentativas maliciosas são alteradas e adaptadas para diversos ambientes, tentando burlar os sistemas de defesa, o que gera um novo tipo de ataque que pode não ser reconhecido por um meio de defesa padronizado.

Este trabalho apresenta um estudo preliminar para a utilização de um agente inteligente para a implementação de um Sistema de Detecção de Intrusão (SDI) que visa o reconhecimento de atividades malignas baseadas em um comportamento diferente do esperado em uma rede juntamento com padrões maléficos reconhecidos.

## 2. METODOLOGIA

Um Sistema de Detecção de Intrusão é uma ferramenta de análise que verifica constantemente os processos ocorridos em uma determinada rede, podendo ser configurado em uma determinada máquina, um ponto da rede ou de forma híbrida entre ambos. Suas implementações geralmente aceitam configurações especializadas de modo a se adequar ao seu ambiente de análise, porém sem agentes inteligentes estas configurações geralmente ficam entre estar atreladas a padrões de ataques ou excesso de recurso computacional.

De acordo com (LIMA, 2002) alguns dos principais problemas que os SDIs sem implementação inteligente encontram são: fragilidade quanto a ataques de negação de serviço em seu servidor; sua implementação não facilita uma atualização e incrementação de configurações em suas capacidades, dificultando a atualização e alteração de assinaturas e comportamentos; e, a necessidade constante de apoio humano especializado e ferramentas de manutenção. Com isso, como apontado, uma possível solução é a utilização de um agente inteligente que possa evoluir conforme a necessidade do ambiente.

Para o estudo do benefício de uma implementação de um Sistema de Detecção de Intrusão Inteligente, foram escolhidos como componentes as Redes Neurais Artificiais ou RNAs (Figura 1). As RNAs se inspiram na rede neural biológica que através de pesos em funções matemáticas e um sistema de processo paralelo e distribuído "aprende" e reconhece padrões similares, sem estar presa a uma determinada definição.

Esta característica de generalizar um conhecimento adquirido capacita este componente inteligente para que possa reagir a estímulos não apresentados anteriormente a ele, geralmente na sua implementação, quando ainda há manipulação e testes dos pesos sinápticos para configuração de resposta ideal.

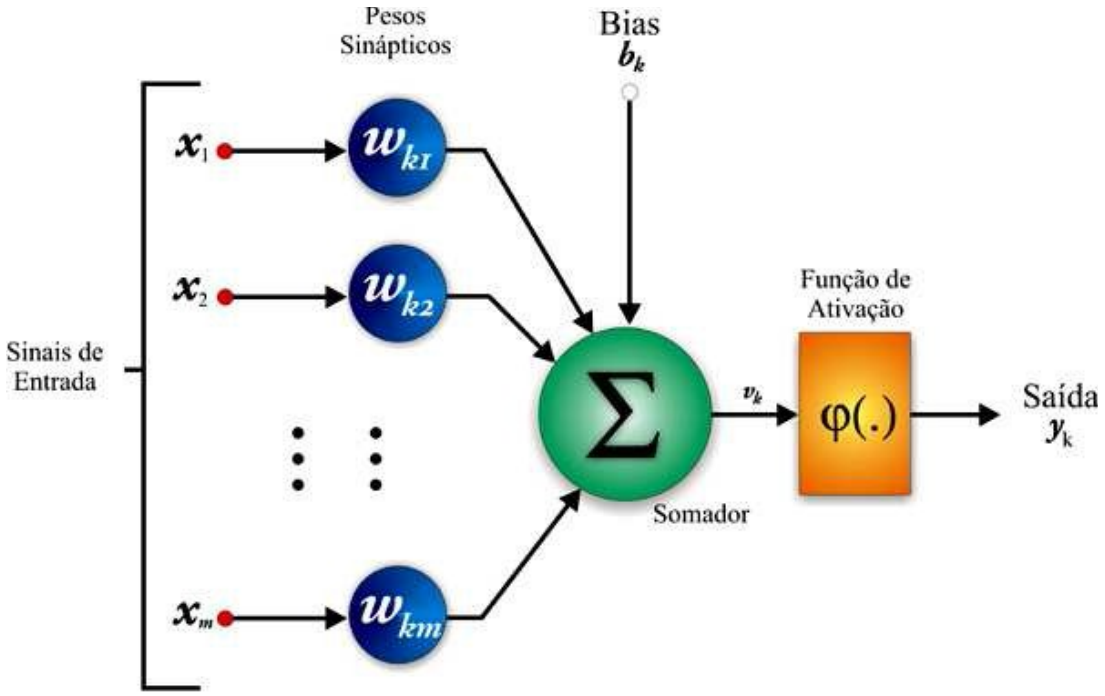


Figura 1. Exemplo de um neurônio artificial segundo (HAYKIN, 2001) utilizado por (LIMA, 2005)

A ideia inicial desta pesquisa é o estudo e implementação de um SDI baseado em detecção por host, em que ele fará uma varredura nos dados recebidos pela máquina no qual esta alocado e nos dados que trafegarem por esta máquina mesmo que não se destinem a ela. O seu foco de ação é um comportamento híbrido entre ações que discordem de um comportamento padrão esperado pelo sistema das máquinas (recursos computacionais) e usuários (direitos de acesso, privilégios, execução de tarefas) e um comportamento de abuso, como assinaturas já conhecidas de invasão e ataque. Sua resposta deve ser uma aviso ao pessoal responsável e um conjunto de ações que visam proteger o sistema e a rede de modo a parar um ataque ou amenizar seus efeitos, se possível sem ter de indisponibilizar serviços essenciais.

O que se espera é um sistema de proteção de alta qualidade, resposta rápida e taxa de erro aceitável, que possa se manter atualizado sem interferência humana e seja capaz de localizar eventos maliciosos e possivelmente maléficos que ainda não são de conhecimento geral.

## 3. RESULTADOS E DISCUSSÕES

Atualmente esta pesquisa está em andamento, sendo feita a sua base e revisão bibliográficas e estudos de alguns casos, já que o modelo de Sistema de Detecção de Intrusão com Redes Neurais Artificias ainda apresenta um grande campo para sua melhoria. Como pode ser observado em ambas as dissertações em que este trabalho se baseou, a implementação deste modelo é possível embora ainda haja uma grande espaço para sua refinação.

## 4. CONCLUSÕES

Foi feita neste trabalho uma apresentação da pesquisa sobre um modelo de um sistema de proteção de redes baseado em agentes inteligentes, um Sistema de Detecção de Intrusão com implementação em Redes Neurais Artificiais, que visa uma amplificação no grau de defesa nas comunicações virtuais. O próximo passo será o estudo e implementação de componentes deste sistema para que se possa começar uma análise mais aprofundada e detalhada e que gere testes com resultados concretos de sua alta capacidade de proteção e resposta rápida.

## 5. REFERÊNCIAS BIBLIOGRÁFICAS

LIMA, I. V. M. **Uma abordagem simplificada detecção de intrusão baseada em redes neurais artificiais.** 2005. Dissertação (Mestrado em Ciência da Computação) – Programa de Pós-Graduação em Ciência da Computação, Universidade Federal de Santa Catarina.

LIMA, C. F. L. **Agentes inteligentes para detecção de intrusos em redes de computadores.** 2002. Dissertação (Mestrado Ciência da Computação) – Curso de Pós-Graduação em Ciência da Computação, Universidade Federal do Maranhão.