Pontifícia Universidade Católica
do Rio de Janeiro

Renato Maia Silva

Redes Neurais Artificiais aplicadas à Detecção de Intrusão em Redes TCP/IP

Dissertação de Mestrado

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre pelo Programa de Pós-graduação em Engenharia Elétrica do Departamento de Engenharia Elétrica da PUC-Rio.

Orientador: Prof. Marco Antonio Grivet Mattoso Maia

Rio de Janeiro

Abril de 2005

PONTIFÍCIA UNIVERSIDADE CATÓLICA
DO RIO DE JANEIRO

Renato Maia Silva

Redes Neurais Artificiais aplicadas à Detecção de Intrusão em Redes TCP/IP

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre pelo Programa de Pós-Graduação em Engenharia Elétrica do Departamento de Engenharia Elétrica do Centro Técnico Científica da PUC-Rio. Aprovada pela Comissão Examinadora abaixo assinada.

Prof. Marco Antonio Grivet Mattoso Maia
Orientador
Centro de Estudos em Telecomunicações – PUC-RIO

Prof. Rodolfo Sabóia Lima de Souza
Centro de Estudos em Telecomunicações – PUC-Rio

Prof. Ewerton Longoni Madruga
Universidade Estácio de Sá

Prof. José Eugenio Leal
Coordenador Setorial do Centro
Técnico Científico – PUC-Rio

Rio de Janeiro, 26 de abril de 2005

Renato Maia Silva

Graduado em Engenharia Eletrônica e de Telecomunicações pela Pontifícia Universidade Católica de Minas Gerais. Atuação profissional e pesquisa em aspectos de segurança da informação aplicados a redes de computadores e sistemas de telecomunicações.

Ficha Catalográfica

Silva, Renato Maia

Redes neurais artificiais aplicadas à detecção de intrusão em redes TCP/IP / Renato Maia Silva ; orientador: Marco Antonio Grivet Mattoso Maia. – Rio de Janeiro : PUC, Departamento de Engenharia Elétrica, 2005.

144 f. ; 30 cm

Dissertação (mestrado) – Pontifícia Universidade Católica do Rio de Janeiro, Departamento de Engenharia Elétrica.

Inclui referências bibliográficas.

1. Engenharia elétrica – Teses. 2. Internet. 3. Detecção de Intrusos. 4. Segurança da Informação. 5. Redes Neurais. 6. Inteligência Computacional. I. Maia, Marco Antonio Grivet Mattoso. II. Pontifícia Universidade Católica do Rio de Janeiro. Departamento de Engenharia Elétrica. III. Título.

CDD: 621.3

Para Matheus, antes mesmo de nascer, já transformou minha vida enchendo-a de alegria.

Agradecimentos

Ao meu orientador, Professor Marco Antônio Grivet Mattoso Maia pelo apoio, enorme paciência e incentivo para a realização deste trabalho.

À minha querida esposa Kiuza, pelo amor incondicional e companheirismo.

Para meu pai, minha mãe e minhas irmãs por sempre estarem ao meu lado

Ao Professor João Célio Barros Brandão pelo incentivo, e amizade.

Aos amigos e colegas que tanto me ajudaram e apoiaram. Em especial, agradeço ao Tiago Vinhoza, Luis Resende e Arthur Góes. Espero um dia poder retribuir o apoio recebido.

Aos meus sócios Helio e Soraya pela paciência e compreensão durante minhas ausências.

A CAPES pelos auxílios concedidos, sem os quais este trabalho não poderia ter sido realizado.

Resumo

Silva, Renato Maia; Maia, Marco Antonio Grivet Mattoso (Orientador). **Redes Neurais Aplicadas à Detecção de Intrusão em Redes TCP/IP.** Rio de Janeiro, 2005. 144p. Dissertação de Mestrado - Departamento de Engenharia Elétrica, Pontifícia Universidade Católica do Rio de Janeiro.

Ataques e intrusões são uma ameaça constante para empresas e organizações interconectadas através de redes de pacotes e da Internet. Ferramentas tradicionais de detecção de ataques e intrusões dependem de conhecimento prévio sobre as técnicas de ataque não sendo capazes de detectar novas técnicas de ataques. Este trabalho investiga a aplicação de redes neurais artificiais no auxílio à detecção de intrusão em redes de pacotes TCP/IP. Utilizando a capacidade de generalização das redes neurais, espera-se que o sistema detecte novos ataques mantendo uma alta taxa de acertos. É empregado também técnica de comitê de redes neurais especialistas para obtenção de maior precisão e menor taxa alarmes falsos.

Palavras-chave

Internet; Detecção de Intrusos; Segurança da Informação; Redes Neurais; Inteligência Computacional;

Abstract

Silva, Renato Maia; Maia, Marco Antonio Grivet Mattoso (Advisor). **Artificial Neural Networks Applied to Intrusion Detection on TCP/IP Networks.** Rio de Janeiro, 2005. 144p. MSc. Dissertation - Departamento de Engenharia Elétrica, Pontifícia Universidade Católica do Rio de Janeiro.

Computer attacks and intrusions poses significant threats to companies and organizations interconnected through packet networks and the Internet. Most current approaches to intrusion detection rely on previous knowledge of attack patterns and are not capable of detecting new intrusion techniques. This work presents the application of artificial neural networks as a component of an intrusion detection system. Exploring neural networks generalization capabilities the system should be able to detect new attack patterns and sustain a high detection rate. Neural networks ensembles are also used in order to achieve higher accuracy and lower false-positive rates.

Keywords

Internet; Intrusion Detection; Neural Networks; Information Security ; Computational Intelligence

Sumário

Lista de figuras

Lista de tabelas