



**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



**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

Todos os direitos reservados. É proibida a reprodução total ou parcial do trabalho sem autorização da universidade, do autor e do orientador.

## 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

1	Introdução.....	15
1.1.	Segurança em Redes de Computadores.....	15
1.2.	Trabalhos anteriores.....	20
1.3.	Organização do texto.....	21
2	Sistemas de Detecção de Intrusão.....	22
2.1.	O que é Detecção de Intrusão ?.....	22
2.2.	Tipos de Sistemas de Detecção de Intrusão.....	23
2.2.1.	Método de detecção.....	24
2.2.2.	Arquitetura.....	27
2.2.3.	Pós-deteção.....	33
3	Ataques e Intrusões.....	35
3.1.	Taxonomia para Ataques e Intrusões.....	35
3.1.1.	Níveis de Privilegio.....	36
3.1.2.	Métodos de Transição e Exploração.....	36
3.1.3.	Transição entre níveis de privilégio.....	37
3.1.4.	Ações.....	38
3.1.5.	Uso da taxonomia para descrever ataques.....	39
3.2.	Categorias de Ataques / Intrusões.....	39
3.2.1.	Negação de Serviço (DOS ou <i>Denial of Service</i> ).....	40
3.2.2.	Usuário para Superusuário ( <i>User to Root</i> ).....	42
3.2.3.	Remoto para usuário ( <i>Remote to User</i> ).....	43
3.2.4.	Reconhecimento ( <i>Probing</i> ).....	44
4	Redes Neurais Artificiais.....	46
4.1.	Modelo de neurônio artificial.....	47
4.2.	Topologia e Arquitetura de Redes Neurais.....	49
4.3.	Redes Neurais Multicamadas.....	49
4.3.1.	Redes Neurais Multicamadas Perceptron (MLP).....	50
4.4.	Algoritmos de Aprendizado.....	52
4.4.1.	Aprendizado Supervisionado.....	53
4.4.2.	Aprendizado Não-supervisionado.....	57
4.4.3.	Aprendizado em lote ("batch").....	57
4.4.4.	Aprendizado Sequencial.....	58
5	Cenários Analisados.....	59
5.1.	Projeto MIT/DARPA 1998-1999.....	59
5.2.	Base de dados para treinamento e testes.....	60
5.3.	Pré-processamento da base de dados.....	67
5.4.	Treinamento e Simulação das redes neurais.....	71
6	Resultados.....	74
6.1.	Matriz de Confusão e Curvas ROC.....	74
6.2.	Classificador Binário.....	77
6.2.1.	Características intrínsecas como entrada.....	77



6.2.2. Todas as características como entrada.....	84
6.2.3. Características Especialistas como Entrada.....	91
6.2.4. Características Temporais como Entrada.....	97
6.3. Classificador por Classes.....	104
6.4. Classificador Preciso para Classe DoS.....	106
6.5. Classificador Preciso para Classe Reconhecimento.....	108
6.6. Classificador Preciso para Classe U2R.....	110
6.7. Classificador Preciso para Classe R2L.....	111
6.8. Comitê de Redes Especialistas.....	114
6.8.1. Decisão por voto majoritário.....	114
6.8.2. Decisão pela Média.....	115
6.8.3. Decisão por algoritmo adaptativo proposto.....	116
6.8.4. Curvas ROC.....	117
7 Conclusão.....	119
Referências Bibliográficas.....	121
Apêndice A Padrões de ataque – Negação de Serviço.....	124
Apêndice B Padrões de ataque – Reconhecimento.....	131
Apêndice C Padrões de ataque – Remoto para local.....	133
Apêndice D Padrões de ataque – Usuário para Super-usuario.....	137
Apêndice E Código fonte desenvolvido.....	139

## Lista de figuras

Figura 1-1 : Vulnerabilidades CERT/CC .....	16
Figura 1-2 : Incidentes CERT/CC .....	17
Figura 1-3 : Incidentes NBSO (mês).....	18
Figura 1-4 : Ataques NBSO (Acumulado).....	19
Figura 2-1 : Classificação SDI .....	23
Figura 2-2 : Transição de estados .....	25
Figura 2-3: Exemplo clássico de solução de detecção de intrusos .....	28
Figura 2-4 – Cabeçalho IP .....	29
Figura 2-5 – Cabeçalho TCP .....	30
Figura 2-6 – Cabeçalho UDP.....	30
Figura 2-7 : Módulos de um SDI.....	32
Figura 3-1 : Descrevendo ataques com a Taxonomia.....	39
Figura 4-1 : Neurônio Artificial .....	47
Figura 4-2 : Funções de ativação: (a) Sinal. (b) Linear por partes. (c) Sigmoidal.....	48
Figura 4-3 : Redes Multicamadas.....	49
Figura 4-4 : Treinamento Supervisionado .....	53
Figura 4-5 : Condição de Parada.....	57
Figura 5-1 – Diagrama da Rede de Simulação .....	60
Figura 5-2 : Pré-processamento dos dados .....	68
Figura 6-1 – Diagrama Venn .....	74
Figura 6-2 : Treinamento 1. DS1 .....	78
Figura 6-3 : Treinamento 1. DS2 .....	79
Figura 6-4 : Treinamento 1. DS3 .....	80
Figura 6-5 : Treinamento 1. DS4 .....	81
Figura 6-6 : Treinamento 1. DS5 .....	82
Figura 6-7 : 1. ROC : TP x FP .....	83
Figura 6-8 : 1. Variação ROC – AC x FP .....	84
Figura 6-9 : Treinamento 2. DS1 .....	85
Figura 6-10 : Treinamento 2. DS2 .....	86
Figura 6-11 : Treinamento 2. DS3 .....	87
Figura 6-12 : Treinamento 2. DS4 .....	88

Figura 6-13 : Treinamento 2. DS5 .....	89
Figura 6-14 : 2. ROC – TP x FP .....	90
Figura 6-15 : 2. Variação ROC – AC x FP .....	90
Figura 6-16 : Treinamento 3. DS1 .....	91
Figura 6-17 : Treinamento 3. DS2 .....	92
Figura 6-18 : Treinamento 3. DS3 .....	93
Figura 6-19 : Treinamento 3. DS4 .....	94
Figura 6-20 : Treinamento 3. DS5 .....	95
Figura 6-21 : 3. ROC – TP x FP .....	96
Figura 6-22 : 3. Variação ROC – AC x FP .....	97
Figura 6-23 : Treinamento 4. DS1 .....	98
Figura 6-24 : Treinamento 4. DS2 .....	99
Figura 6-25 : Treinamento 4. DS3 .....	100
Figura 6-26 : Treinamento 4. DS4 .....	101
Figura 6-27 : Treinamento 4. DS5 .....	102
Figura 6-28 : 4. ROC – TP x FP .....	103
Figura 6-29 : 4. Variação ROC – AC x FP .....	103
Figura 6-30 : Treinamento RN por classe – DS1 .....	104
Figura 6-31 : Treinamento RN Classe DoS – DS1 .....	106
Figura 6-32 : Treinamento RN Classe DoS – DS3 .....	107
Figura 6-33 : Treinamento RN Classe “Probe” – DS1 .....	109
Figura 6-34 : ROC para Comitês – TP x FP .....	117
Figura 6-35 : Variação ROC para Comitês – AC x FP .....	118

## Lista de tabelas

Tabela 3-1 : Privilégios .....	36
Tabela 3-2 : Métodos de Transição e Ataque.....	37
Tabela 3-3 : Ações.....	38
Tabela 3-4 : Categorias de Padrões de Ataque .....	40
Tabela 3-5 : Negação de Serviço .....	42
Tabela 3-6 : User-to-Root.....	43
Tabela 3-7 : Remote-to-User.....	44
Tabela 3-8 : Reconhecimento.....	45
Tabela 5-1 : Características intrínsecas de conexões TCP/IP. ....	61
Tabela 5-2 : Características de conexão por conhecimento especialista.....	62
Tabela 5-3 : Características temporais : janela de 2 segundos.....	64
Tabela 5-4 : Distribuição da base de treinamento .....	65
Tabela 5-5 : Distribuição da base de testes .....	67
Tabela 5-6 : Flags.....	69
Tabela 5-7 : Protocolos.....	69
Tabela 5-8 : Labels .....	69
Tabela 5-9 : Serviços.....	70
Tabela 5-10 : Subconjuntos de Treinamento.....	71
Tabela 5-11 : Cenários analisados para redes MLP .....	72
Tabela 6-1 : Exemplo de Matriz de Confusão .....	75
Tabela 6-2 : CM 1. DS1 .....	78
Tabela 6-3 : Parâmetros 1. DS1 .....	78
Tabela 6-4 : CM 1. DS2.....	79
Tabela 6-5 : Parâmetros 1. DS2 .....	79
Tabela 6-6 : CM 1. DS3.....	80
Tabela 6-7 : Parâmetros 1. DS3 .....	80
Tabela 6-8 : CM 1. DS4 .....	81
Tabela 6-9 : Parâmetros 1. DS4 .....	81
Tabela 6-10 : CM 1. DS5.....	82
Tabela 6-11 : Parâmetros : 1. DS5 .....	82

Tabela 6-12 : Parâmetros 2. DS1 .....	85
Tabela 6-13 : Parâmetros 2. DS1 .....	85
Tabela 6-14 : CM 2. DS2 .....	86
Tabela 6-15 : Parâmetros 2. DS2 .....	86
Tabela 6-16 : CM 2. DS3 .....	87
Tabela 6-17 : Parâmetros 2. DS3 .....	87
Tabela 6-18 : CM 2. DS4 .....	88
Tabela 6-19 : Parâmetros 2. DS4 .....	88
Tabela 6-20 : CM 2. DS5 .....	89
Tabela 6-21 : Parâmetros 2. DS5 .....	89
Tabela 6-22 : CM 3. DS1 .....	92
Tabela 6-23 : Parâmetros 3. DS1 .....	92
Tabela 6-24 : CM 3. DS2 .....	93
Tabela 6-25 : Parâmetros 3. DS2 .....	93
Tabela 6-26 : CM 3. DS3 .....	94
Tabela 6-27 : Parâmetros 3. DS3 .....	94
Tabela 6-28 : CM 3. DS4 .....	95
Tabela 6-29 : Parâmetros 3. DS4 .....	95
Tabela 6-30 : CM 3. DS5 .....	96
Tabela 6-31 : Parâmetros 3. DS5 .....	96
Tabela 6-32 : CM 4. DS1 .....	98
Tabela 6-33 : Parâmetros 4. DS1 .....	98
Tabela 6-34 : CM 4. DS2 .....	99
Tabela 6-35 : Parâmetros 4. DS2 .....	99
Tabela 6-36 : CM 4. DS3 .....	100
Tabela 6-37 : Parâmetros 4. DS3 .....	100
Tabela 6-38 : CM 4. DS4 .....	101
Tabela 6-39 : Parâmetros 4. DS4 .....	101
Tabela 6-40 : CM 4. DS5 .....	102
Tabela 6-41 : Parâmetros 4. DS5 .....	102
Tabela 6-42 : CM por classe - DS1 .....	105
Tabela 6-43 : CM para técnica ganhadora do KDDCup 1999 .....	105
Tabela 6-44 : CM Classe DoS – DS1 .....	107
Tabela 6-45 : CM Classe DoS - DS3 .....	108

Tabela 6-46 : CM Classe Reconhecimento – DS1 .....	109
Tabela 6-47 : CM Classe Reconhecimento – DS2 .....	109
Tabela 6-48 : CM Classe U2R – DS1 .....	110
Tabela 6-49 : CM Classe U2R – DS4.....	111
Tabela 6-50 : CM Classe R2L - DS1 .....	112
Tabela 6-51 : CM Classe R2L – DS5 .....	113
Tabela 6-52 : CM Comitê por voto majoritário.....	114
Tabela 6-53 : Parâmetros Comitê por voto majoritário.....	115
Tabela 6-54 : CM Comitê pela média .....	115
Tabela 6-55 : Parâmetros Comitê pela média.....	115
Tabela 6-56 : CM para Algoritmo de decisão proposto .....	116
Tabela 6-57 : Parâmetros para Algoritmo de decisão proposto .....	117