

Faculdades Integradas de Caratinga

Ciência da Computação

ANÁLISE DO ALGORITMO SAND PARA INICIALIZAÇÃO DE PESOS DE REDES NEURAIS ARTIFICIAIS

Autor: Vinícius Campista Brum

Orientador: Jacson Rodrigues Correia da Silva

Caratinga, 2012



Agenda

- Introdução
- Objetivo geral
- Objetivos específicos
- Referencial teórico
- Metodologia
- Análise de resultados
- Conclusão
- Trabalhos futuros
- Principais referências



Introdução

- o Crescimento da Internet
- o Segurança Computacional
- o Ferramentas para segurança
 - Sistemas de Detecção de Intrusão
- o Vulnerabilidades
- o Aplicação de Inteligência Artificial
 - Rede Neural Artificial
- o Necessidade constante de melhorias



Objetivo geral

- Analisar a utilização do algoritmo SAND para inicialização de pesos de Redes Neurais Artificiais buscando melhorias quanto a tempo de treinamento e taxas de acerto;
- Buscar melhorias para uma técnica já existente.



Objetivos específicos

- Estudo sobre Sistema Imunológico Artificial
- Estudo sobre Redes Neurais Artificiais
- Estudo sobre a junção das técnicas
- Estudo sobre bases de dados
- Estudo de ferramentas para implementação
- Implementações e testes



Referencial teórico

- Sistema Imunológico Artificial
 - Histórico
 - Objetivo
 - Tipos de resposta
 - Inato
 - Adaptativo
 - Anticorpos
 - Diversidade imunológica



Referencial teórico

o Rede Neural Artificial

- Histórico
- Características
 - Arquitetura ou estrutura
 - Algoritmos de treinamento
 - Funções de ativação



Referencial teórico

- SAND (*Simulated Annealing approach for Diversity*)
 - Histórico
 - Objetivo
 - Representações
 - Espaço de formas de Hamming
 - Espaço de formas Euclidiano
 - Mutações
 - Ponto único
 - Múltiplos pontos



Referencial teórico

o NSL-KDD

- Histórico
- Objetivo
- Estrutura dos dados
- Grupos
 - KDDTrain+
 - KDDTest+
 - KDDTest-21



Metodologia

- o Mecanismos de implementação
 - Linguagem Python
 - Biblioteca FANN (*Fast Artificial Neural Network Library*)
 - Utilizadas em outros trabalhos
 - Livres
 - Características



Metodologia

- o Implementação do algoritmo SAND
 - Representação
 - Espaço de formas Euclidiano
 - Mutações
 - Ponto único
 - Múltiplos pontos



Metodologia

- o Implementação do algoritmo SAND
 - Análise de mutação
 - Distância euclidiana entre o vetor médio e o centro de coordenadas
 - Condições de parada
 - 5000 gerações
 - 99,5% de diversidade



Metodologia

- o Implementação da Rede Neural Artificial
 - Arquitetura ou estrutura
 - *Feedforward* de múltiplas camadas
 - 41 neurônios de entrada
 - 25 neurônios na camada oculta
 - 2 neurônios de saída



Metodologia

- o Implementação da Rede Neural Artificial
 - Algoritmos de treinamento
 - Aprendizado supervisionado
 - *Backpropagation*
 - Funções de ativação
 - Funções por camada
 - *SIGMOID_STEPWISE* para camada oculta
 - *SIGMOID* para camada de saída



Metodologia

- o Testes isolados com algoritmo SAND
 - Testar processo de diversificação
 - Populações aleatórias
 - Populações apresentadas na fonte principal do algoritmo
 - Populações de baixa diversidade



Metodologia

- o Testes com algoritmo SAND sobre a Rede Neural Artificial
 - Mutações de ponto único e múltiplos pontos
 - Aplicação do algoritmo para cada camada da rede neural
 - Geração de 10 redes neurais diversificadas a partir da rede original para cada tipo de mutação



Metodologia

- o Treinamento e execução das redes neurais
 - Treinamento
 - Número de épocas
 - MSE (*Mean Square Error*)
 - Execução
 - Taxa de acerto
 - KDDTest-21
 - KDDTest+



Metodologia

- o Dados utilizados para treinamento e execução
 - NSL-KDD
 - Treinamento
 - KDDTrain+_20Percent
 - Execução
 - KDDTest-21
 - KDDTest+
 - KDDTrain+



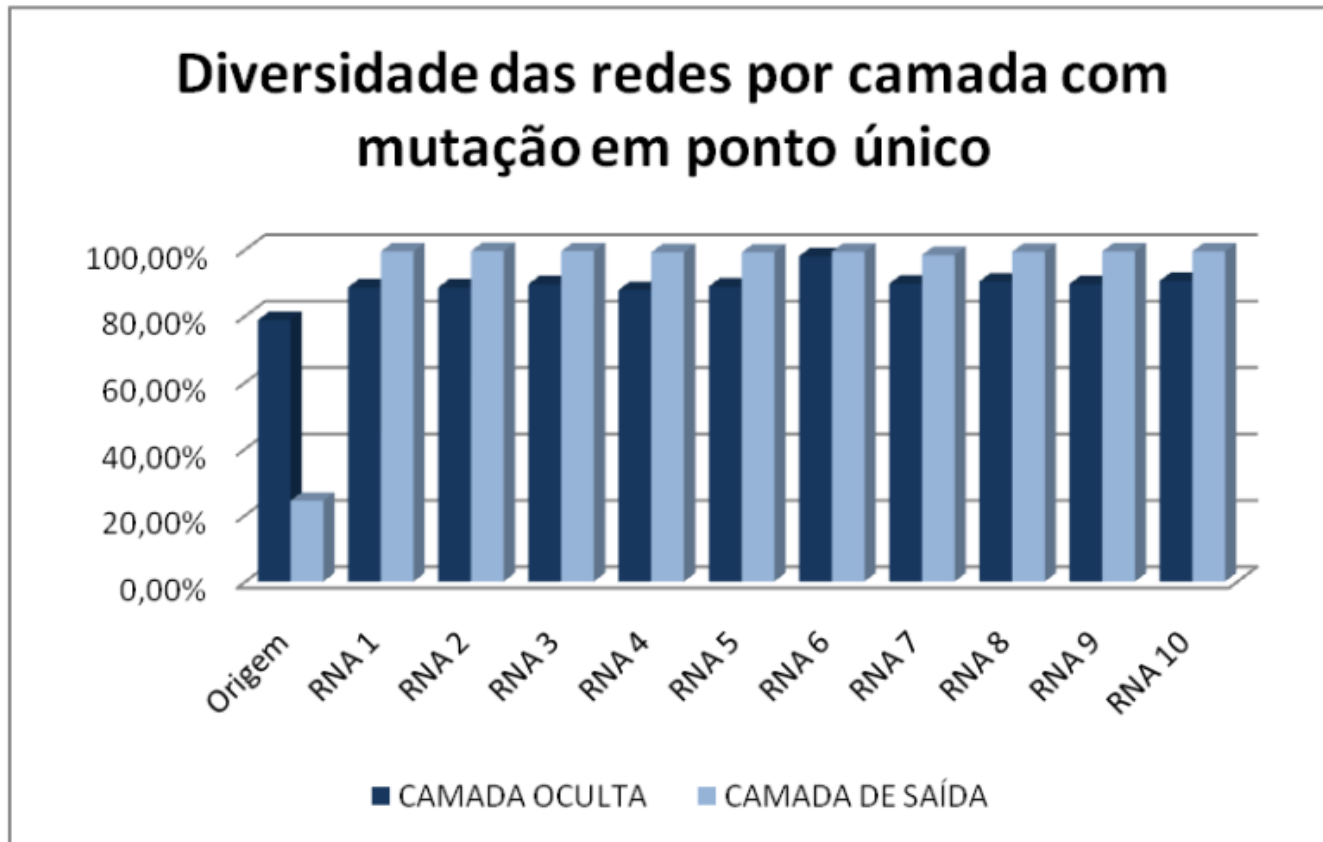
Análise de resultados

o Mutação de ponto único

– Diversificação

- Aumento de diversidade entre 9,03 e 19,18 pontos percentuais na camada oculta
- Aumento de diversidade entre 73,99 e 75,19 pontos percentuais na camada de saída
- Melhor caso foi apresentado pela RNA 6
 - 78,78% para 97,96%
 - 24,35% para 99,32%

Análise de resultados





Análise de resultados

o Mutação de ponto único

– Treinamento

- Nenhum caso reduziu o número de épocas
- Dois casos apresentaram redução de MSE
 - RNA 2: 0,172 para 0,168
 - RNA 6: 0,172 para 0,171



Análise de resultados

RNA	Épocas	MSE
Origem	200	0,172
1	200	0,175
2	200	0,168
3	200	0,188
4	200	0,190
5	200	0,188
6	200	0,171
7	200	0,196
8	200	0,220
9	200	0,198
10	200	0,176



Análise de resultados

o Mutação de ponto único

– Execução

- Quatro casos apresentaram melhorias quanto a taxa de acerto
- Melhorias entre 1% e 3% na base KDDTest-21
- Melhorias entre 1% e 2% na base KDDTest+
- Melhor caso foi apresentado pela RNA 6
 - 3% na base KDDTest-21
 - 2% na base KDDTest+

Análise de resultados

RNA	KDDTest-21	KDDTest+	KDDTrain+_20Percent	KDDTrain+
Origem	63,00%	80,00%	99,00%	99,00%
1	64,00%	81,00%	99,00%	99,00%
2	65,00%	82,00%	99,00%	99,00%
3	59,00%	78,00%	99,00%	99,00%
4	59,00%	78,00%	100,00%	99,00%
5	62,00%	80,00%	99,00%	99,00%
6	66,00%	82,00%	99,00%	99,00%
7	60,00%	79,00%	99,00%	99,00%
8	55,00%	76,00%	97,00%	97,00%
9	56,00%	77,00%	99,00%	99,00%
10	64,00%	81,00%	99,00%	99,00%



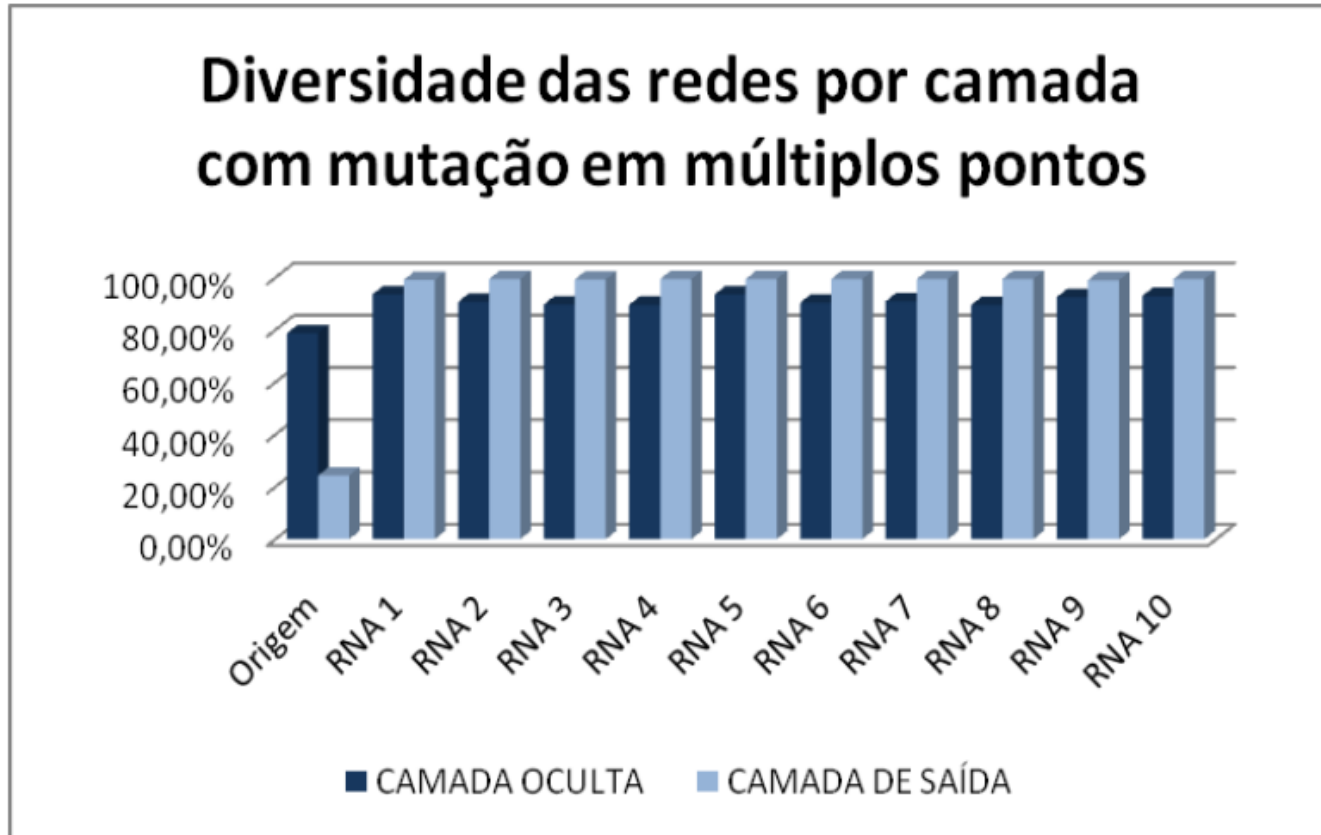
Análise de resultados

o Mutação em múltiplos pontos

– Diversificação

- Aumento de diversidade entre 10,8 e 14,85 pontos percentuais na camada oculta
- Aumento de diversidade entre 74,69 e 75,16 pontos percentuais na camada de saída
- Melhor caso foi apresentado pela RNA 1
 - 78,78% para 93,63%
 - 24,35% para 99,11%

Análise de resultados





Análise de resultados

o Mutação em múltiplos pontos

– Treinamento

- Nenhum caso reduziu o número de épocas
- Cinco casos apresentaram redução de MSE
 - RNA 9: 0,188 para 0,154
 - RNA 2: 0,188 para 0,166
 - RNA 1: 0,188 para 0,169
 - RNA 6: 0,188 para 0,183
 - RNA 8: 0,188 para 0,183



Análise de resultados

RNA	Épocas	MSE
Origem	200	0,188
1	200	0,169
2	200	0,166
3	200	0,221
4	200	0,204
5	200	0,203
6	200	0,183
7	200	0,204
8	200	0,183
9	200	0,154
10	200	0,220



Análise de resultados

o Mutação em múltiplos pontos

– Execução

- Cinco casos apresentaram melhorias quanto a taxa de acerto
- Melhorias entre 2% e 8% na base KDDTest-21
- Melhorias entre 2% e 4% na base KDDTest+
- Melhor caso foi apresentado pela RNA 9
 - 8% na base KDDTest-21
 - 4% na base KDDTest+

Análise de resultados

RNA	KDDTest-21	KDDTest+	KDDTrain+_20Percent	KDDTrain+
original	59,00%	78,00%	99,00%	99,00%
1	64,00%	81,00%	100,00%	99,00%
2	65,00%	82,00%	99,00%	99,00%
3	56,00%	77,00%	99,00%	99,00%
4	57,00%	78,00%	99,00%	99,00%
5	57,00%	78,00%	99,00%	99,00%
6	61,00%	80,00%	99,00%	99,00%
7	57,00%	77,00%	99,00%	99,00%
8	63,00%	80,00%	99,00%	99,00%
9	67,00%	82,00%	99,00%	99,00%
10	55,00%	76,00%	99,00%	99,00%



Conclusão

- A utilização do algoritmo SAND pode gerar resultados muito interessantes como redução de MSE (*Mean Square Error*) e aumento de taxas de acerto;
- Mutações em pontos múltiplos são mais interessantes que mutações em ponto único;
- É necessário analisar o percentual de diversidade e a distribuição dos indivíduos;
- É possível aumentar a eficiência e confiabilidade de ferramentas como o Sistema de Detecção de Intrusão.



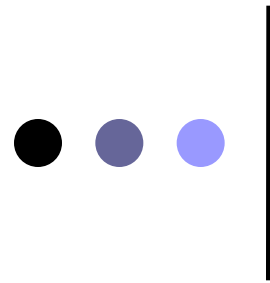
Trabalhos futuros

- Utilização de novos conceitos de mutação;
- Utilização de mais técnicas de Inteligência Artificial;
- Aplicação do algoritmo para outras técnicas de Inteligência Artificial;
- Desenvolvimento de um Sistema de Detecção de Intrusão utilizando as técnicas e conceito apresentados;
- Utilização de outras bases de dados.



Principais referências

- o DE CASTRO, L. N. **Engenharia Imunológica: desenvolvimento e aplicação de ferramentas computacionais inspiradas em Sistemas Imunológicos Artificiais.** Tese (Doutorado) – Faculdade de Engenharia Elétrica e de Computação, Universidade Estadual de Campinas, Campinas, 2001;
- o SILVA, Jacson R. C. **Sistemas de Detecção de Intrusão com técnicas de Inteligência Artificial.** Dissertação (Mestrado) – Universidade Federal de Viçosa, Viçosa, 2011;
- o UCHÔA, Joaquim Q. **Algoritmos Imunoinspirados aplicados em Segurança Computacional:** utilização de algoritmos inspirados no Sistema Imune para Detecção de Intrusos em redes de computadores. Tese (Doutorado) – Universidade Federal de Minas Gerais, Belo Horizonte, 2009.



Obrigado pela atenção!!