



UTILIZAÇÃO DE SISTEMAS IMUNOLÓGICOS ARTIFICIAIS NA RESOLUÇÃO DE PROBLEMAS

Trabalho de Conclusão de Curso

Engenharia da Computação

Glauber Nascimento de Oliveira
Orientador: Prof. Sérgio Murilo Maciel Fernandes



UNIVERSIDADE
DE PERNAMBUCO

**Universidade de Pernambuco
Escola Politécnica de Pernambuco
Graduação em Engenharia de Computação**

GLAUBER NASCIMENTO DE OLIVEIRA

**UTILIZAÇÃO DE SISTEMAS
IMUNOLÓGICOS ARTIFICIAIS NA
RESOLUÇÃO DE PROBLEMAS**

Monografia apresentada como requisito parcial para obtenção do diploma de Bacharel em Engenharia de Computação pela Escola Politécnica de Pernambuco – Universidade de Pernambuco.

Recife, janeiro de 2022.

Oliveira, Glauber Nascimento de

Utilização de Sistemas Imunológicos Artificiais na Resolução de Problemas / Glauber Nascimento de Oliveira. - Recife-PE, 2022. xi, 35 f.: il. ; 29 cm.

Trabalho de Conclusão de Curso (Graduação em Engenharia de Computação) Universidade de Pernambuco, Escola Politécnica de Pernambuco, Recife, 2022

Orientador: Prof. Sérgio Murilo Maciel Fernandes
Banca examinadora: Prof. Mêuser Jorge Silva Valença

1. Sistemas Imunológicos Artificiais. 2. Inteligência Artificial. - Recife(PE) I. Título. II. Fernandes, Sérgio Murilo Maciel. III. Universidade de Pernambuco.

MONOGRAFIA DE FINAL DE CURSO

Avaliação Final (para o presidente da banca)*

No dia 16/12/2019, às 11h, reuniu-se para deliberar sobre a defesa da monografia de conclusão de curso do(a) discente **GLAUBER NASCIMENTO DE OLIVEIRA**, orientado(a) pelo(a) professor(a) **SÉRGIO MURILO MACIEL FERNANDES**, sob título Utilização de Sistemas Imunológicos Artificiais na Resolução de Problemas, a banca composta pelos professores:

MÊUSER JORGE SILVA VALENÇA (PRESIDENTE)

SÉRGIO MURILO MACIEL FERNANDES (ORIENTADOR)

Após a apresentação da monografia e discussão entre os membros da Banca, a mesma foi considerada:

Aprovada Aprovada com Restrições* Reprovada

e foi-lhe atribuída nota: 9,0 (Nove)

*(Obrigatório o preenchimento do campo abaixo com comentários para o autor)

O(A) discente terá 30 dias para entrega da versão final da monografia a contar da data deste documento.

AVALIADOR 1: Prof (a) **MÊUSER JORGE SILVA VALENÇA**

AVALIADOR 2: Prof (a) **SÉRGIO MURILO MACIEL FERNANDES**

AVALIADOR 3: Prof (a)

* Este documento deverá ser encadernado juntamente com a monografia em versão final.

*Dedico esta monografia à minha mãe,
por toda a paciência que ela teve comigo
durante todos esses anos de universidade.*

Agradecimentos

A minha mãe e irmã, que sempre me apoiaram durante todos esses anos, mesmo com todos os meus atrasos.

Ao meu orientador, o professor Sérgio Murilo Maciel Fernandes, que me ajudou e me apoiou bastante nesta monografia.

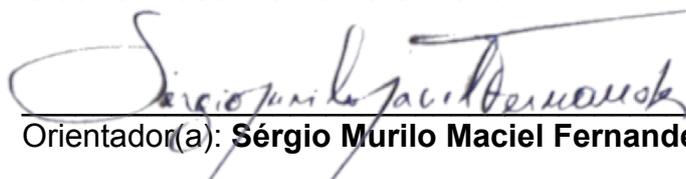
Autorização de publicação de PFC

Eu, **Glauber Nascimento de Oliveira** autor(a) do projeto de final de curso intitulado: **Utilização de Sistemas Imunológicos Artificiais na Resolução de Problemas;** autorizo a publicação de seu conteúdo na internet nos portais da Escola Politécnica de Pernambuco e Universidade de Pernambuco.

O conteúdo do projeto de final de curso é de responsabilidade do autor.



Glauber Nascimento de Oliveira



Orientador(a): **Sérgio Murilo Maciel Fernandes**

Coorientador(a):

Prof, de TCC: **Daniel Augusto Ribeiro Chaves**

Data: 16/12/2019

Resumo

Neste trabalho são analisadas as aplicações de Sistemas Imunológicos Artificiais(SIA) ao longo dos anos. Para tal, foi realizada uma revisão bibliográfica de trabalhos nacionais e internacionais, assim como de livros e artigos a respeito do assunto. Os trabalhos escolhidos e apresentados nesta monografia estão classificados em ordem cronológica ao longo dos anos. Os algoritmos utilizados na implementação dos SIA nesses trabalhos, no caso de trabalhos práticos, ou quais foram propostos, no caso de trabalhos teóricos, são explicados. Alguns dos trabalhos analisados comparam os resultados obtidos utilizando SIA com resultados obtidos utilizando outras técnicas, a fim de mostrar a sua eficácia.

Abstract

In this paper, we analyze the applications of Artificial Immune Systems(AIS) over the years. For such, we made a literature review of national and international papers, as well as books and articles about AIS. The papers chosen and presented on this monograph are classified in chronological order over the years. The algorithms used in the implementation of the AIS in those papers, in the case of practical papers, or that were proposed, in the case of theoretical papers, are explained. Some of the papers analysed compare their obtained results using AIS with other results using other techniques, in order to show its effectiveness.

Lista de Figuras

Figura 1.	Diagrama de blocos do CLONALG	15
Figura 2.	Ciclo de Vida do AIRS	18
Figura 3.	Fase de Censura	21
Figura 4.	Monitoramento	21
Figura 5.	Comparação de um grupo de pixels com $n=3$ e $t=5$	24
Figura 6.	Base de dados	25
Figura 7.	Problema do caixeiro viajante	29
Figura 8.	Configuração do algoritmo CLONALG no OAT	30
Figura 9.	Tabelas de Classificação	32

Lista de Tabelas

Tabela 1. Comparação dos 3 melhores resultados ordenados por Precisão	22
Tabela 2. Comparação dos 3 melhores resultados ordenados por Recall	22
Tabela 3. Comparação dos 3 melhores resultados ordenados por Medida-F	23
Tabela 4. Algoritmo EAISO-GT	26
Tabela 5. Resultados das 10 melhores simulações	27
Tabela 6. Falso Positivo e Falso Negativo	27
Tabela 7. Influência dos Parâmetros	30

Lista de Siglas

IA - Inteligência Artificial

SIA - Sistemas Imunológicos Artificiais

ASN- Algoritmo de Seleção Negativa

AIRS - Artificial Immune Recognition System

SVM - Support Vector Machines

LWL - Locally Weighted Learning

MLP - BP - Multilayer Perceptron: The Backpropagation

SVM - Support Vector Machine

ARB - Artificial Recognition Ball

Sumário

Introdução	12
Fundamentação Teórica	13
Inteligência Artificial	13
Sistema Imunológico	13
Sistemas Imunológicos Artificiais	14
Algoritmo de Seleção Clonal	14
Algoritmo de Seleção Negativa	16
Teoria do Perigo	16
AIRS e AIRS2	16
Trabalhos relacionados	20
Detecção de Vírus	20
Predição de Fraudes e Furtos de Energia	22
Detecção de Invasão na Rede	23
Detecção de Imagens	23
Classificação de E-mails	24
Reconhecimento de Caracteres	24
EAISO-GT	25
Detecção de Spam	27
Problemas de Otimização	28
Detecção de Ataques DDoS	31
Perfuração de Poços de Petróleo	31
Conclusão e Trabalhos Futuros	33
Referências	34

1. Introdução

A área de inteligência artificial vem se popularizando nos últimos anos. Diversa técnicas vêm sendo propostas e utilizadas, e neste trabalho o foco será nos Sistemas Imunológicos Artificiais(SIA), que são baseados no sistema imunológico dos seres humanos. Existem vários algoritmos baseados nos SIA, cada um com uma finalidade diferente. Neste trabalho são descritos os algoritmos que vem sido utilizados, e mostrados trabalhos onde eles foram aplicados.

Os SIA foram criados em 1986 em um artigo escrito por Farmer, Packard e Perelson, "*The immune system, adaptation and machine learning*", porém só em 1994 quando Forrest e Kephart publicaram artigos a respeito que os SIA se tornaram um campo de IA por si só. O primeiro livro a respeito de SIA foi editado por Dasgupta em 1999, num livro chamado "*Artificial Immune Systems and Their Applications*".

Desde então, diversos algoritmos baseados em SIA foram propostos, dentre eles o CLONALG, o Algoritmo de Seleção Clonal e o AIRS. Nos trabalhos aqui apresentados, os autores utilizam-se de um ou mais algoritmos e comparam o seu desempenho com o de outros algoritmos de IA para verificar a viabilidade de utilizá-los.

2. Fundamentação Teórica

2.1. Inteligência Artificial

Inteligência Artificial, também chamada de Inteligência Computacional, é definida por Poole(1998) como o estudo do design de agentes inteligentes. Esses agentes podem ser desde animais a humanos, insetos, organizações, sociedade como um todo, etc. Um sistema inteligente é um sistema que age de maneira inteligente: o que ele faz é apropriado para suas circunstâncias e objetivos, é flexível para ambientes e objetivos que mudam, aprende por experiência e faz escolhas apropriadas dadas as limitações de percepção e computação infinita.

2.2. Sistema Imunológico

Também chamado de sistema imune ou sistema imunitário, o sistema imunológico tem como finalidade defender o organismo contra invasores, que são chamados de antígenos. A resposta imune, que é o nome dado ao processo de defesa do corpo, pode ser de dois tipos: imunidade inata e imunidade adquirida.

A imunidade inata está presente em todos os animais, e serve como primeira linha de defesa contra os antígenos. Essa imunidade já vem desde o nascimento, e permanece inalterado durante toda a vida. Ela é composta por macrófagos e neutrófilos. Caso ela não seja suficiente para eliminar os invasores, a imunidade adquirida entra em ação.

A imunidade adquirida, também chamada de adaptativa, ao contrário da inata, é adquirida ao longo da vida. Ela utiliza linfócitos que podem ser classificados em tipo B e tipo T.

2.3. Sistemas Imunológicos Artificiais

Os Sistemas Imunológicos Artificiais(SIA) são sistemas adaptativos, inspirados pela imunologia teórica e funções imunes observadas, princípios e modelos, que são aplicados na resolução de problemas(CASTRO, 2002). Os algoritmos mais comumente utilizados na aplicação de SIA são:

- Seleção Negativa
- Seleção Clonal
- Algoritmo Genético Imune
- Algoritmos Imunes baseados em Redes Imunes
- Teoria do Perigo

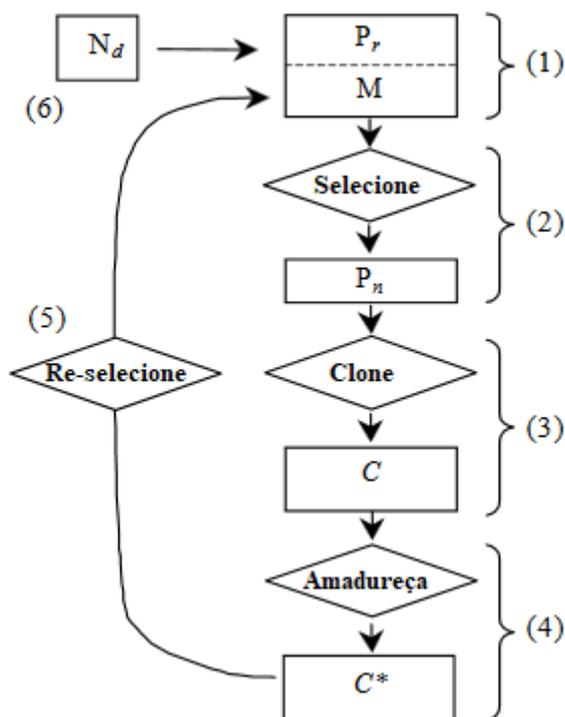
2.4. Algoritmo de Seleção Clonal

Os algoritmos de seleção clonal são inspirados na teoria de seleção clonal da imunidade adquirida, que explica como os linfócitos B e T melhoram suas respostas a antígenos ao longo do tempo, chamado de afinidade de maturação. Algoritmos de seleção clonal são normalmente utilizados para otimização e reconhecimento de padrões. Uma das técnicas de implementação desses algoritmos é conhecida como CLONALG(The Clonal Selection Algorithm), que foi proposta por Castro(2002). Foi verificado por Castro(2002) que esse algoritmo é capaz de realizar aprendizado e manutenção de memória de alta qualidade e também foi capaz de resolver tarefas complexas de engenharia, como otimização multimodal e combinatória. Ao comparar o algoritmo com um algoritmo genético(GA), foi percebido que o CLONALG consegue alcançar um conjunto diversificado de soluções locais ótimas, enquanto que por outro lado o GA tende a polarizar toda a população de indivíduos para a melhor solução candidata.

O CLONALG funciona da seguinte maneira(Castro, 1999):

1. Um conjunto P de soluções candidatas são geradas, compostas de um subconjunto de células de memória M adicionadas a população restante (P_r);
2. Os P_n melhores indivíduos da população P são determinados, baseados numa medida de afinidade;
3. Os n melhores indivíduos da população são clonados, aumentando temporariamente a população de clones C . A quantidade de clones é uma função crescente da medida de afinidade do antígeno;
4. Submeta a população de clones a um esquema de hipermutação, onde a hipermutação é proporcional à afinidade do anticorpo. Uma população amadurecida de anticorpos C^* é gerada;
5. Os indivíduos melhorados são re-selecionados de C^* para comporem o conjunto de memória. Alguns membros do conjunto P podem ser substituídos por outros membros melhorados de C^*
6. Os anticorpos de afinidade baixa d são substituídos da população, mantendo sua diversidade

Figura 1 - Diagrama de blocos do CLONALG



Fonte: Castro(1999)

2.5. Algoritmo de Seleção Negativa

O algoritmo de seleção negativa (ASN) foi proposto por Forrest (1994). Ele é inspirado na geração de células T do sistema imune. Essas células T possuem receptores para detecção de antígenos. Esses receptores são feitos por um processo genético que é pseudo-aleatório, e é altamente provável que alguns desses receptores irão detectar moléculas próprias. Por isso, as células T passam por um processo no timo chamado de seleção negativa, e essas células que reconhecem as proteínas próprias são destruídas. As que não reconhecem as próprias saem do timo e são utilizadas na proteção contra os antígenos.

O algoritmo funciona de maneira similar às células T. Ele gera detectores aleatoriamente, e elimina aqueles que detectam as moléculas próprias. Os detectores são chamados de 'anticorpos'.

2.6. Teoria do Perigo

A Teoria do Perigo, que foi proposta por Polly Matzinger, é uma teoria que descreve o funcionamento do sistema imunológico. De acordo com essa teoria, o sistema imunológico não distingue entre self e non-self, e sim se algo causa dano ou não. Quando células de tecido recebem dano, elas enviam "Sinais de Perigo".

2.7. AIRS e AIRS2

O AIRS (Artificial Immune Recognition System) é um algoritmo inspirado na teoria de seleção clonal de imunidade adquirida. Este algoritmo foi proposto por Andrew Watkins et al. (2004). Ele foi criado especificamente para resolver problemas de classificação. Ele utiliza elementos de outros algoritmos de SIA, dentre eles o Immunos-81 e o CLONALG.

O AIRS2 é uma versão modificada do AIRS, que é mais simples de implementar e possui resultados melhores. Os dois algoritmos possuem resultados

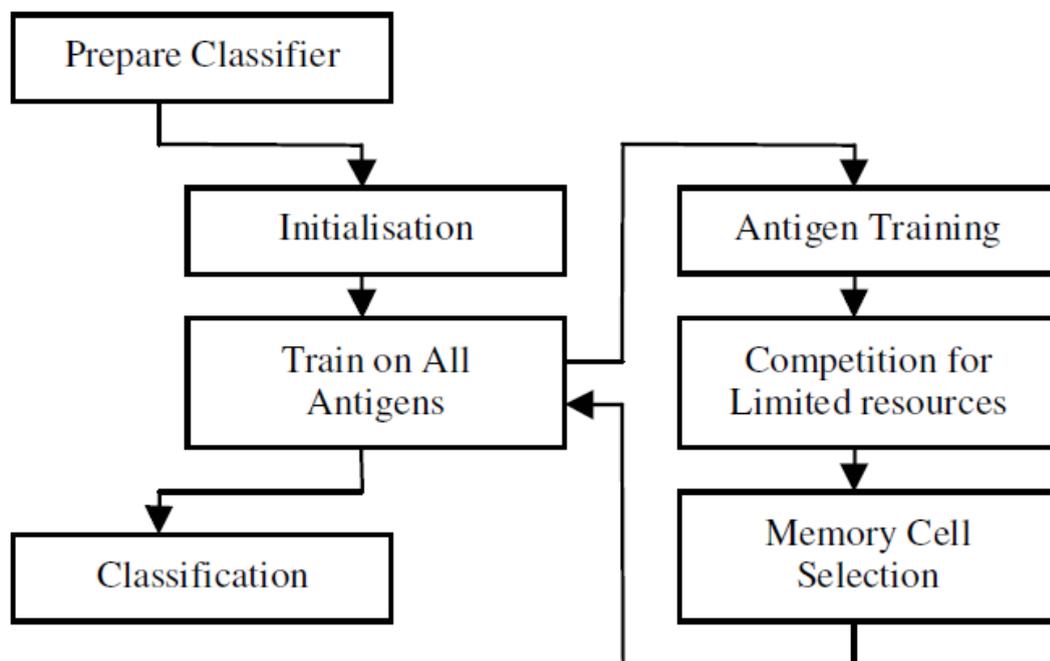
similares no que diz respeito a precisão de classificação, mas o algoritmo AIRS2 fornece uma capacidade de generalização melhor do que o AIRS1 no que diz respeito a redução de dados aprimorada nos conjuntos de dados de treinamento.

O algoritmo AIRS possui as seguintes características descritas por Brownlee(2005):

- Auto-regulação - o algoritmo AIRS aprende uma arquitetura apropriada durante o treinamento, sem depender que o usuário escolha uma
- Performance - o AIRS consegue uma precisão de classificação que fica entre os cinco e oito melhores quando classificado contra outros sistemas de classificação conhecidos
- Generalização - o AIRS faz generalização através de redução de dados, o que faz com que ele precise utilizar menos dados para treinamento
- Estabilidade dos Parâmetros - o AIRS possui vários parâmetros ajustáveis para melhor resolução de problemas específicos.

O ciclo de vida do AIRS é descrito na imagem abaixo:

Figura 2 - Ciclo de Vida do AIRS



Fonte: Brownlee(2005)

A imagem acima mostra o ciclo de vida do AIRS, que é dividido nas seguintes fases:

- **Inicialização:** Preparação dos dados que serão utilizados no processo de treinamento.
- **Treinamento dos Antígenos:** O AIRS só precisa passar pelos dados de treinamento uma vez para preparar o classificador.
- **Competição por Recursos Limitados:** É utilizada para controlar o tamanho do pool ARB e promover os ARBs com maior afinidade ao antígeno que está sendo treinado.
- **Seleção de Células de Memória:** O ARB com a maior pontuação de estimulação normalizada é escolhido para se tornar o candidato à célula de memória.

- **Classificação:** Após o processo de treinamento ser completado, o pool de células de reconhecimento de memória se tornam o núcleo do classificador AIRS.

3. Trabalhos relacionados

3.1. Detecção de Vírus

Em seu trabalho, Stephanie Forrest(1994) apresentou o algoritmo de seleção negativa(ASN) para detecção de vírus. Ela propôs um algoritmo que pudesse distinguir entre *próprio*(usuário legítimo, dados corrompidos, etc) de “outro”, ou não-próprio(usuário não autorizado, vírus, etc). Apesar de ter sido feito inicialmente para detecção de vírus, Forrest percebeu que o algoritmo fosse talvez mais aplicável em outros problemas de detecção de mudanças. Esse algoritmo tem três princípios importantes:

1. Cada cópia do algoritmo de detecção é único, para evitar que, caso um local fique vulnerável, todos fiquem. Por isso, cada local tem um conjunto único de detectores.
2. A detecção é probabilística. Assim, uma intrusão em um local tem pouca chance de funcionar em outros locais.
3. Esse algoritmo aprende o que o “próprio” é, e detecta(probabilisticamente) qualquer coisa que fuja disso.

Esse algoritmo apresenta duas fases:

1. Uma série de detectores é gerada. Cada detector é uma string que não “combina” com nenhum dos dados protegidos. Essa fase é chamada de fase de censura(Figura 1).
2. Os dados protegidos são monitorados comparando-os com os detectores. Se algum dos detectores for ativado é porque alguma mudança ocorreu(Figura 2).

Figura 3 - Fase de Censura

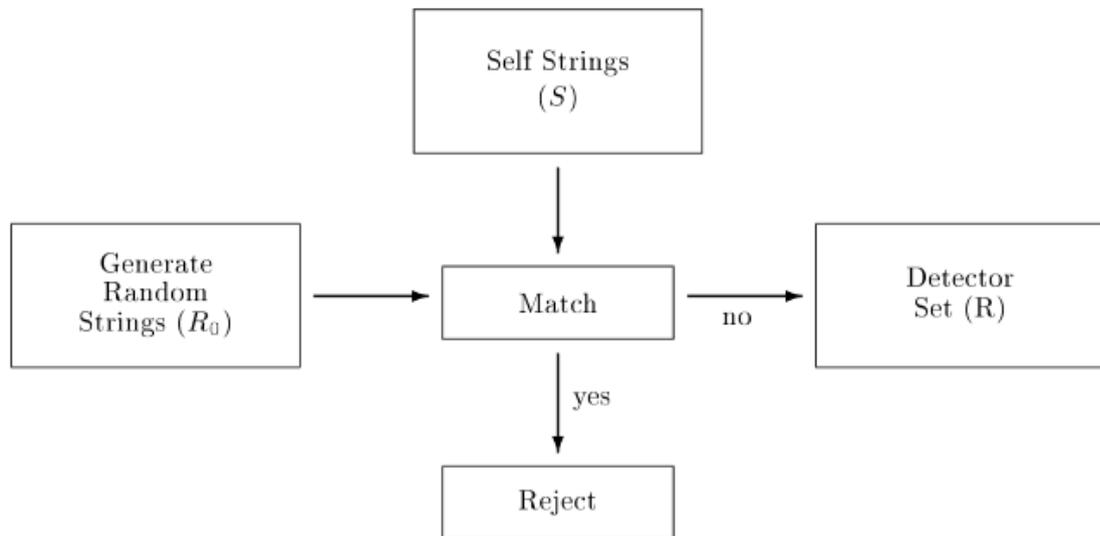


Figure 1: Generation of Valid Detector Set (Censoring) .

Fonte: Forrest(1994)

Figura 4 - Monitoramento

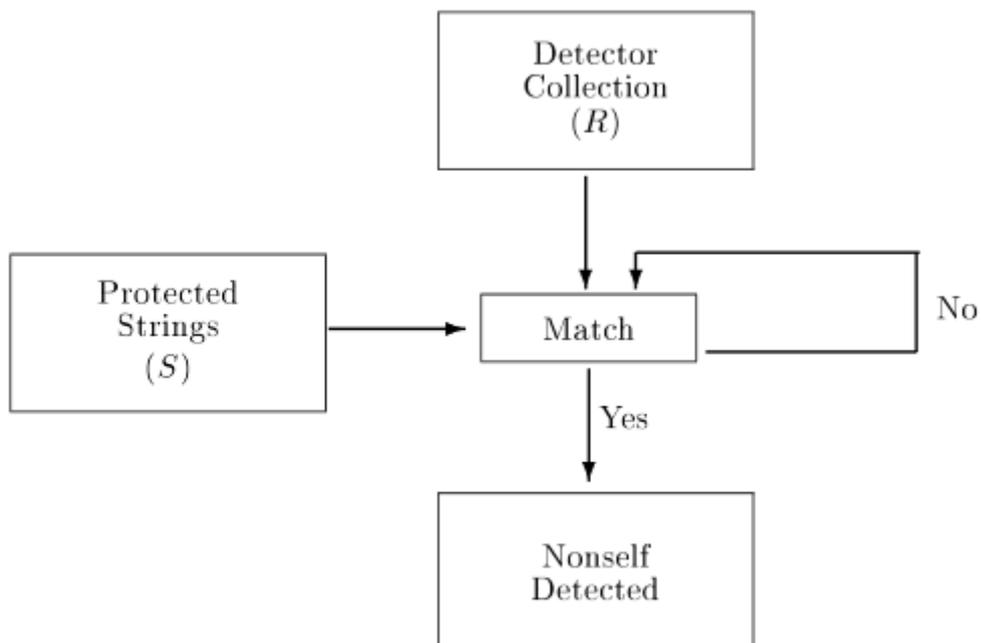


Figure 2: Monitor Protected Strings for Changes.

Fonte: Forrest(1994)

3.2. Predição de Fraudes e Furtos de Energia

Uma das áreas na qual os SIA apresentam resultados satisfatórios é na área de reconhecimento de padrões. Em sua tese, Mauricio Volkweis(2012) utilizou-se do algoritmo *The Clonal Selection Algorithm*(CLONALG), proposto por Castro. Ele aplicou a SIA para prever fraudes e furtos de energia elétrica, e comparou os resultados obtidos com o de 13 outros métodos em 3 aspectos: precisão, recall e medida-f. Em questão de precisão, que diz respeito a fração de instâncias recuperadas que são relevantes, o CLONALG aplicado por Volkweis ficou em terceiro lugar. No recall, também chamado de revocação e que diz respeito a fração de instâncias relevantes que são recuperadas, também ficou em terceiro lugar. Na medida-f, que é a média harmônica ponderada da precisão e revocação, esse algoritmo ficou em primeiro lugar. Com isso, Volkweis concluiu que o SIA para esse problema apresentou um bom balanceamento entre precisão e recall.

Tabela 1 - Comparação dos 3 melhores resultados ordenados por Precisão

#	Algoritmo	Precisão	Recall	Medida-F
1	Fast decision tree learner	50,00%	1,85%	0,0357
2	KNN(K=1)	14,55%	14,81%	0,1468
3	CLONALG	14,00%	72,04%	0,2344

Fonte: Mauricio Volkweis(2012)

Tabela 2 - Comparação dos 3 melhores resultados ordenados por Recall

#	Algoritmo	Precisão	Recall	Medida-F
1	Naive Bayes	10,60%	94,44%	0,1907
2	Voting Feature Intervals	10,25%	90,74%	0,1842
3	CLONALG	14,00%	72,04%	0,2344

Fonte: Mauricio Volkweis(2012)

Tabela 3 - Comparação dos 3 melhores resultados ordenados por Medida-F

#	Algoritmo	Precisão	Recall	Medida-F
1	CLONALG	14,00%	72,04%	0,2344
2	Naive Bayes	10,60%	94,44%	0,1907
3	Voting Feature Intervals	10,25%	90,74%	0,1842

Fonte: Mauricio Volkweis(2012)

3.3. Detecção de Invasão na Rede

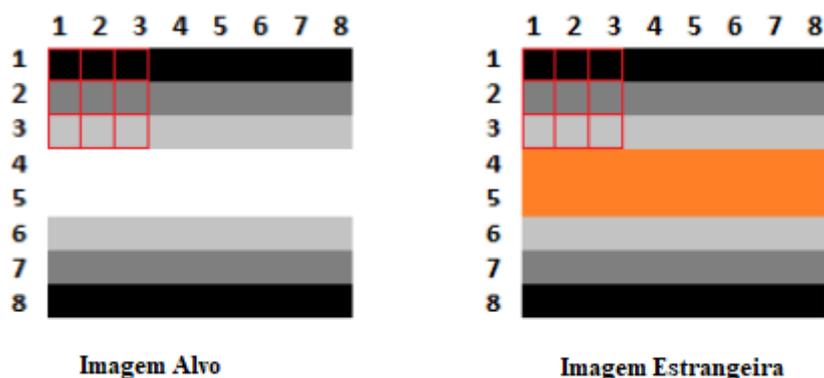
Jungwon Kim(2001) utilizou o *Algoritmo de Seleção Negativa*(ASN) na detecção de intrusos numa rede. Ele se baseou no algoritmo de Forrest e o aplicou em dados reais de uma rede. Um dos problemas encontrados ao utilizar um ASN para esse tipo de aplicação é que esse algoritmo tem um problema severo de dimensionamento: era necessário ter um “próprio” muito grande para poder cobrir os diversos tipos de intrusões de rede, porém ao aplicar-se um “próprio” muito grande no algoritmo, o tempo de computação aumenta muito. Por isso, ele percebeu que era inviável utilizar esse algoritmo para esse propósito, devido a esse tempo necessário para gerar um número suficiente de detectores “próprios”.

3.4. Detecção de Imagens

Stein Keijzers(2013) utilizou o ASN para tentar resolver o problema de procura de imagens similares, que diz que dada uma imagem alvo, imagens similares de uma base de dados grande devem ser detectadas. Para tal, Keijzers designou a imagem alvo como ‘self’, e criou detectores para encontrar qualquer imagem que não fosse ‘self’. Após encontrar as imagens que não são iguais ou parecidas, as que sobraem são as imagens similares. Para verificar se as imagens são iguais ou similares, foram utilizadas diferentes técnicas: comparação direta pixel a pixel(DPS), que compara se os pixels são iguais ou se estão numa variação r dada, tal que o valor v do pixel seja igual a variação $[v-r, v+r]$; comparação de grupos de pixel, tal que em um grupo de n por n pixels é verificado se t pixels desse grupo são parecidos com o da imagem alvo. A imagem abaixo mostra um exemplo dessa

comparação em grupo, onde os valores usados foram $n = 3$, $t = 5$ e $r = 0$, ou seja, os pixels tem que ser iguais para a comparação ter sucesso.

Figura 5: Comparação de um grupo de pixels com $n=3$ e $t=5$



Fonte: Keijzers(2013)

Também foi utilizada a similaridade média de diferença de cor(ACDS), que consiste em pegar a diferença da soma das cores de cada componente de cor e dividir essa diferença pela maior diferença possível, gerando assim uma medida de similaridade entre 0 e 1. Utilizando o mesmo agrupamento da técnica anterior, só que colocando o valor t entre 0 e 1, gera-se uma porcentagem no valor de $100 * t$ de similaridade com a imagem alvo. A técnica de DPS se saiu melhor do que a de ACDS, e Keijzers concluiu que os resultados que ele obteve são bastante similares à uma seleção manual através do olho humano, e portanto o algoritmo ASN pode de fato ajudar na criação de um sistema de busca de imagens similares.

3.5. Classificação de E-mails

Onomza Waziri(2014) utilizou o ASN para propor uma técnica de classificação de e-mails, com o objetivo de reduzir o número de falsos-positivos e criar um detector de spams eficiente. Foram criados detectores para spam e não-spam. Enquanto que a taxa falsa(detecção errada) da técnica proposta foi menor do que a das técnicas tradicionais, a taxa de recall(instâncias relevantes) foi pior.

3.6. Reconhecimento de Caracteres

Fernando Lima(2014) utilizou o ASN para reconhecimento de caracteres manuscritos. Foram utilizadas 200 amostras, e os únicos caracteres utilizados foram os números de 0 a 9, escritos em uma tabela por uma pessoa e digitalizados, como mostra a imagem abaixo.

Figura 6: Base de dados

1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0

Fonte: Lima(2014)

Cada um dos caracteres foi extraído da imagem, gerando assim 200 imagens de tamanho 32x32, que foram posteriormente binarizadas e dilatadas antes de serem analisadas pelo ASN. Além do ASN, foram utilizados outros 3 algoritmos para comparação de resultados. O ASN conseguiu um acerto de 94% em 61,5ms, sendo o segundo algoritmo com maior taxa de acertos, em relação a 3 outros métodos propostos por outros trabalhos que ele estudou. Esses outros métodos utilizaram-se de redes neurais, e obtiveram respectivamente 100%, 93,5% e 73,61% de acerto.

3.7. EAISO-GT

André Ferry Barreira(2010) propôs um algoritmo novo que ele chamou de EAISO-GT(Evolutionary Artificial Immune System Optimization - Game Theory). Esse algoritmo apresenta características de 3 técnicas: Sistemas Imunológicos Artificiais, Algoritmos Evolucionários e Teoria dos Jogos. Ele é uma variação de um

algoritmo proposto por Castro, chamado AISO, e ele foi utilizado em seu trabalho para tentar resolver o problema do caixeiro-viajante.

Tabela 4 - Algoritmo EAISO-GT

<pre>// Algoritmo EAISO-GT 1. Inicia 2. Inicializar aleatoriamente uma população de células 3. Repetir</pre>
<pre>// Características dos Algoritmos Evolucionários // Método de Seleção de Roleta 3.1 Repetir 3.1.1 Selecione uma célula baseado num método de seleção 3.1.2 Gere um número de clones proporcional a adaptabilidade da célula Até que a Condição de Parada 2 seja satisfeita</pre>
<pre>3.2 Mutacione cada clone proporcionalmente à aptidão de sua célula pai 3.3 Determine a aptidão de todos os indivíduos da população</pre>
<pre>// Fase de Interação Social 3.5 Repetir a. Selecionar aleatoriamente duas células b. Pegar o comportamento de cada célula c. Alterar o valor de aptidão da célula de acordo com a tabela de pagamento do jogo Até que a Condição de Parada 3 seja satisfeita</pre>
<pre>3.6 Seleção Clonal 3.7 Determinar as células com a maior aptidão e salvá-las em memória auxiliar Até que a Condição de Parada 1 seja satisfeita 4. A melhor célula da população é a solução para o problema 5. Fim</pre>

Fonte: Barreira(2010)

Para testar o algoritmo, foram realizadas simulações baseadas no problema do caixeiro-viajante(TSP), com o objetivo de minimizar a distância entre as capitais dos estados brasileiros conectadas através de rodovias. O número de vértices que foram definidos foi de 26, o que resulta num total de 7.75×10^{24} possíveis rotas diferentes. Foram realizadas 10 simulações, e o melhor resultado para cada um dos algoritmos testados foi colocado na tabela abaixo.

Tabela 5 - Resultados das 10 melhores simulações

#	Metaheurísticas	(Km)
01	Algoritmo Genético(GA)	27130
02	SIGA	25636
03	AISO	20113
04	AISO-GT	20113
05	EAIISO-GT	20093

Fonte: Barreira(2010)

Pode-se verificar que, pelo menos para esse problema, o algoritmo proposto obteve um resultado melhor do que os outros algoritmos, visto que quanto menor a distância percorrida(km), melhor o resultado.

3.8. Detecção de Spam

Ismaila Idris(2012) utilizou o algoritmo de seleção negativa para a detecção de spam. Foi utilizado um conjunto de dados(data set) composto por 4601 instâncias, onde 39,4% delas eram spam. Esse conjunto de dados por sua vez foi dividido em duas classes: os dados de treinamento e os dados de teste. Os dados de treinamento, como o próprio nome já diz, são usados para treinar os dados, enquanto que os dados de teste são usados para testar o conjunto de dados que foi treinado.

A tabela abaixo mostra os resultados obtidos:

Tabela 6 - Falso Positivo e Falso Negativo

Limiar	Precisão	Falso Positivo	Falso Negativo
0.4	82.7997%	29.9291%	0.1105%
0.5	82.9989%	23.5719%	9.2183%
0.6	86.375%	4.904%	27.5255%

0.7	88.9833%	0.5992%	28.6389%
0.8	89.2658%	0.2252%	29.8358%
0.9	89.2993%	0.1176%	30.6849%

Fonte: Idris(2012)

Como pode ser visto na tabela, com o aumento do limiar, variando de 0.4 a 0.9, a precisão também aumenta, de aproximadamente 82.8% à 89.3%, e há uma redução drástica no falso positivo, de 29.9% para 0.12%, porém há um aumento no falso negativo, de 0.11% para 30.7%.

3.9. Problemas de Otimização

Petar Čisar(2014) em seu paper testou diversos algoritmos de SIA para resolver problemas de otimização. Ele verificou o impacto causado pelos parâmetros dos algoritmos imunológicos na acurácia e velocidade dos cálculos para resolver esses problemas de otimização. Para analisar a performance desses algoritmos, ele utilizou uma ferramenta chamada OAT (*Optimization Algorithm Toolkit*), que serve para desenvolver, avaliar e experimentar algoritmos de otimização.

Os algoritmos que ele testou foram o CLONALG, Algoritmos de Rede Imune e Algoritmos de Células Dendríticas. Para testá-los foi utilizado o problema do caixeiro-viajante usando o OAT como o ambiente de trabalho.

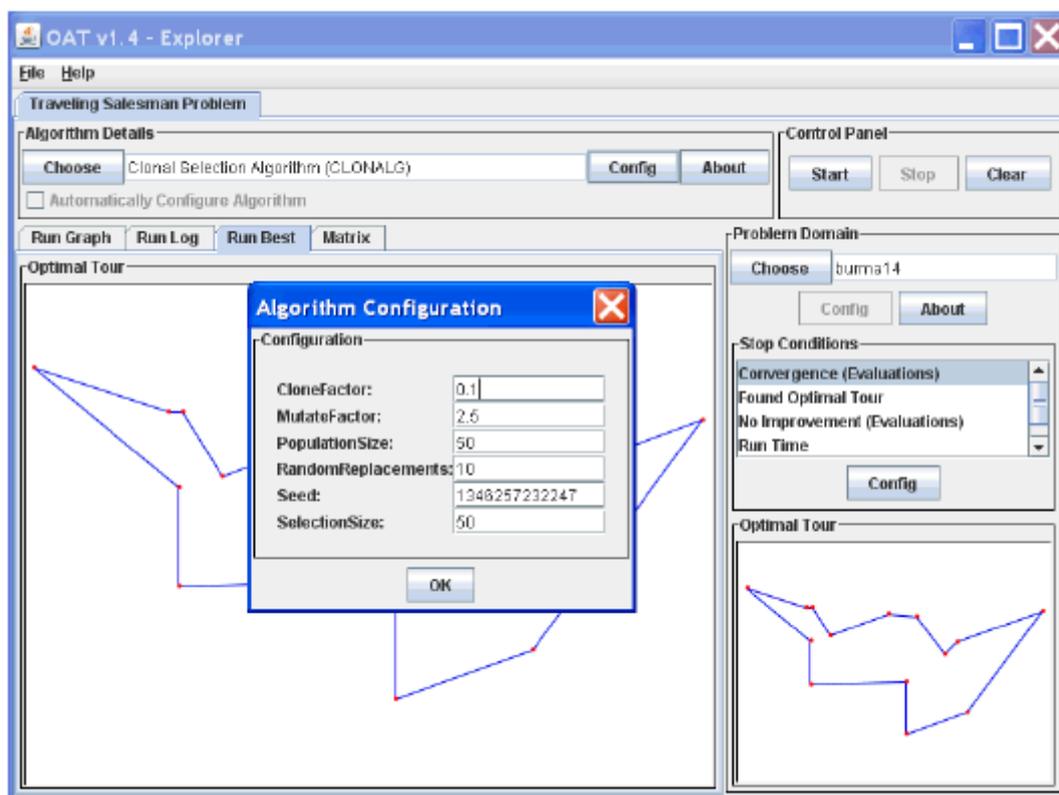
Figura 7 - Problema do caixeiro viajante



Fonte: Ćisar(2014)

A imagem acima mostra o problema do caixeiro-viajante, onde os pontos representam as localizações geográficas de cidades, e a distância entre os pontos é conhecida. A imagem abaixo mostra o programa OAT aberto, e o algoritmo CLONALG sendo configurado para resolver o problema do caixeiro-viajante:

Figura 8 - Configuração do algoritmo CLONALG



Fonte: Ćisar(2014)

Para que a otimização do algoritmo seja considerada finalizada, é preciso que ele encontre o mesmo gráfico do tour ótimo, que aparece no canto inferior direito da imagem acima. Uma tabela contendo diferentes parâmetros e sua influência no tempo para resolução se encontra abaixo:

Tabela 7 - Influência dos parâmetros

Tamanho da População	20	30	40	50	60	70	80
Tempo para resolução(seg)	25	95	1	80	2	20	37
Fator clone	0.1	0.2	0.3	0.4	0.5	0.6	0.7
Tempo para resolução(seg)	83	1	3	1	1	1	1

Fator mutação	2	2.5	3	3.5	4	4.5	5
Tempo para resolução(seg)	<1	80	<1	420	170	<1	>600

Fonte: Ćisar(2014)

Observando os valores acima, foi concluído que o algoritmo CLONALG é bastante sensível a escolha dos parâmetros, ou seja, para poder realmente checar o quão eficiente o algoritmo é, é necessário antes testá-lo com diferentes parâmetros, e escolher o melhor valor.

3.10. Detecção de Ataques DDoS

Mahdi Zamani(2009) utilizou um SIA para detecção de ataques DDoS numa rede wireless. Para isso, foi criado um modelo multi-agente baseado na **Teoria do Perigo** dos sistemas imunes, e os Sinais de Perigo enviados são usados para confirmar se está havendo um ataque ou não.

3.11. Perfuração de Poços de Petróleo

Adriane B.S. Serapião et al(2007) realizaram um trabalho de classificação de operações de perfuração de poços de petróleo, e nele apresentaram duas abordagens de SIA para reconhecimento de padrões: uma por CLONALG e outra por AIRS2. Os resultados obtidos foram então comparados com a classificação feita por um engenheiro de petróleo expert e por outros métodos automáticos, que foram redes neurais, SVM e LWL.

Figura 9 - Tabelas de Classificação

Table 2. Correctness rate for each classification method

Method	Training Set	Test Set
<i>MLP-BP</i>	96.3%	94.9%
<i>SVM</i>	93.7%	92.6%
<i>CLONALG</i>	85.9%	89.0%
<i>Parallel AIRS2</i>	91.2%	92.9%
<i>Lazy LWL</i>	80.5%	81.3%

Table 3. Classification accuracy for each class in the training data

Method	Drilling operations					
	CI	TR	TA	SD	RR	RD
<i>MLP-BP</i>	100%	100%	97.5%	98.1%	89.2%	96.0%
<i>SVM</i>	100%	100%	96.6%	95.8%	83.1%	92.8%
<i>CLONALG</i>	0%	98.7%	85.0%	93.5%	45.5%	96.5%
<i>Parallel AIRS2</i>	57.1%	100%	90.1%	95.6%	69.7%	96.6%
<i>Lazy LWL</i>	0%	0%	91.7%	0%	91.5%	100%

Table 4. Classification accuracy for each class in the test data

Method	Drilling operations					
	CI	TR	TA	SD	RR	RD
<i>MLP-BP</i>	100%	100%	96.2%	98.4%	86.0%	93.8%
<i>SVM</i>	100%	100%	96.6%	94.1%	83.3%	90.7%
<i>CLONALG</i>	0%	100%	89.5%	96.0%	72.8%	97.2%
<i>Parallel AIRS2</i>	100%	100%	91.7%	97.6%	75.4%	98.3%
<i>Lazy LWL</i>	0%	0%	91.7%	0%	93.3%	100%

Fonte: Adriane B.S. Serapião et al(2007)

Como pode ser visto nas tabelas acima, o algoritmo AIRS2 teve um desempenho superior ao CLONALG e Serapião concluiu que esse algoritmo poderia conseguir uma performance similar a do MLP-BP e ao SVM, em problemas com uma melhor distribuição da classe.

4. Conclusão e Trabalhos Futuros

Os Sistemas Imunológicos Artificiais tem ganhado força nos últimos anos. Diversos algoritmos foram criados, como o CLONALG, AIRS2, Seleção Negativa, AISO, etc, e eles tem se mostrado bastante eficientes na resolução de problemas diversos, principalmente nos de classificação, como os apresentados nos trabalhos aqui descritos.

As possibilidades que os algoritmos de SIA apresentam são gigantescas, e eu espero que, ao terminar de ler esse trabalho e ver a diversidade de trabalhos diferentes que utilizaram SIA para diversos fins, o leitor perceba o potencial que os SIA apresentam e, caso deseje utilizá-lo em trabalhos futuros, tenha uma base de trabalhos já feitos para poder se apoiar.

Referências

- POOLE, DAVID; MACKWORTH, ALAN; GOEBEL, RANDY. ***Computational Intelligence: A Logical Approach***. Imprensa da Universidade de Oxford, Nova Iorque, 1998
- DE CASTRO, L.N.; TIMMIS, J. ***Artificial Immune Systems: A New Computational Intelligence Approach***. Springer, 2002
- ASTIAZARA, M.V. ***Sistema Imunológico Artificial para Predição de Fraudes e Furtos de Energia Elétrica***. Tese de Mestrado em Ciência da Computação - Universidade Federal do Rio Grande do Sul, Rio Grande do Sul, 2012.
- LIMA, F.P.A. et al. ***Reconhecimento de Caracteres Manuscritos Utilizando Sistemas Imunológicos Artificiais***, 2014
- DE CASTRO, L.N.; ZUBEN, F.J.V. The Clonal Selection Algorithm with Engineering Applications, In: WORKSHOP PROCEEDINGS OF GECCO, 1., 2000, Las Vegas. ***Workshop on Artificial Immune Systems and Their Applications***. Las Vegas, 2000. p.36-37.
- DE CASTRO, L.N.; ZUBEN, F.J.V. ***Learning and Optimization Using the Clonal Selection Principle***, 2002.
- KIM, J.; BENTLEY, P.J. ***An evaluation of negative selection in an artificial immune system for network intrusion detection***.
- FORREST, S. et al. ***Self-Nonself Discrimination in a Computer***. Proceedings of 1994 IEEE Computer Society Symposium on Research in Security and Privacy.
- KEIJZERS, S. et al. ***Image Similarity Search using a Negative Selection Algorithm***. 2013
- WAZIRI, O. et al. ***A Negative Selection Algorithm Based on Email Classification Techniques***. World of Computer Science and Information Technology Journal, 2013.

BARREIRA, A.F. et al. ***Evolutionary Artificial Immune System Optimization***, 2010

IDRIS, I. ***Model and Algorithm in Artificial Immune System for Spam Detection***. International Journal of Artificial Intelligence & Applications, Vol. 3, No.1, 2012

ČISAR, P.; ČISAR, S.M.; MARKOSKI, B. ***Implementation of Immunological Algorithms in Solving Optimization Problems***, 2014

ZAMANI, M. et al. ***An Artificial Immune System for Detecting DDoS Attacks in Wireless Sensor Networks***. In 14th Int'l Computer Society of Iran Conference (CSICC), Tehran, Iran, 2009.

SERAPIÃO, Adriane et al. ***Artificial Immune Systems for Classification of Petroleum Well Drilling Operations***, 2007.

WATKINS, Andrew et al. ***Artificial Immune Recognition System (AIRS): An Immune-Inspired Supervised Learning Algorithm***. São Paulo, 2004