Rede neural ARTMAP-*Fuzzy*: computação inteligente aplicada na detecção de intrusos em redes de computadores.

Francisco Diego Garrido da Silva[1]

Resumo. O presente trabalho aborda o emprego de um método computacional da área de inteligência artificial aplicado à detecção de intrusos em uma rede de computadores. O método utilizado foi uma rede neural artificial com aprendizado supervisionado do tipo ARTMAP-*Fuzzy*, que faz uso das características de estabilidade e plasticidade da Teoria da Ressonância Adaptativa. Foi utilizado o KDD99 como base de dados a serem analisados. Esta base de dados foi criado por meio de um tráfego de rede em ambiente militar, onde foi explorado inúmeras vulnerabilidades simulando vários tipos de ataques, porém, para este trabalho, foi utilizado apenas o ataque do tipo Denial of Service. O método de detecção atuou de forma satisfatória, permitindo ao término da pesquisa, demonstrar resultados positivos quanto a sua utilização. Este trabalho contribui de forma significativa para o incentivo de aplicação de métodos de inteligência artificial na área de redes de computadores, mais especificamente a área de segurança de redes.

Palavras-Chave: Inteligência Artificial; Redes Neurais Artificiais; ARTMAP-*Fuzzy*; Detecção de Intrusos.

Abstract. ARTMAP-Fuzzy Neural Networks: intelligent computing applied to intruders detection in computers networks. This paper discusses the use of a computational method of artificial intelligence area applied to intrusion detection in a computer network. The method used was a supervised learning artificial neural network ARTMAP-Fuzzy type, which makes use of the characteristics of stability and plasticity of Adaptive Resonance Theory. The KDD99 was used as a database to be analyzed. This database was created through a network traffic in a military environment, which was explored numerous vulnerabilities by simulating various types of attacks, however, for this work, it was only used the attack Denial of Service type. The detection method worked satisfactorily, allowing the final of the research, demonstrated positive results regarding its use. This work contributes significantly to the promotion of the application of artificial intelligence methods in the area of computer networks, specifically the network security area.

Keywords: *Artificial Intelligence; Artificial Neural Network; ARTMAP-Fuzzy; Intrusion Detection.*

1 Introdução

Métodos de Inteligência Artificial têm sido cada vez mais utilizados em diversas áreas do conhecimento, e em redes de computadores não é diferente. Há diversos problemas que

[1]Mestre em Engenharia Mecânica pela UNESP e docente do IFSP, Campos Salto, diego@ifsp.edu.br.

estão tendo como solucionadores o referido método. Entre estes problemas, pode-se destacar a detecção de intrusos em redes de computadores.

O presente trabalho tem como objetivo a utilização de um tipo de Inteligência Artificial, da área das Redes Neurais Artificiais (RNA) conhecido como ARTMAP-*Fuzzy*, que propõe oferecer um bom resultado para o problema de detecção de intrusão dentro de uma rede de comunicação de dados. Busca aprofundar as bases teóricas no desenvolvimento deste método, desde as origens até sua concepção, e a sua aplicação prática. Neste caso o problema escolhido será apenas um cenário para demonstrar a eficácia do método.

Por meio de pesquisa, constataram-se publicações utilizando métodos de inteligência artificial aplicado à segurança computacional, e neste trabalho específico o método é direcionado à detecção de intrusos em redes de computadores. Araújo *et al* (2015), aplicam a rede ARTMAP-*Fuzzy* na detecção de intrusos, utilizando a ferramenta de programação WEKA, e demostra ótimos resultados neste artigo. Silva (2008), em sua tese de doutorado, faz diversas contribuições quanto a utilização de RNAs na detecção de intrusos. Carpenter e Grossberg (1987) abordam o início deste tipo de rede, sendo possível obter as bases para implementação do algoritmo. Haykin (2001) oferece um conteúdo sólido e extenso sobre o assunto. Silva, Spatti e Flauzino (2010), abordam o assunto de RNA de forma mais objetiva e com diversos exemplos práticos. Russel e Norvig (2013), por fim, abordam o assunto de forma minuciosa, assim como Luger (2013).

Além desta breve introdução e das considerações finais, o artigo foi subdividido em outras três seções. No capítulo 2, a seguir, buscou-se apresentar os principais conceitos da área de Inteligência Artificial e Redes Neurais Artificias. O capítulo 3 foi destinado à uma breve análise do método ARTMAP-*Fuzzy*. O capítulo 4, por fim, apresenta os detalhes da aplicação do método proposto na detecção de intrusos em redes de computadores.

2 Inteligência artificial

O termo “Inteligência Artificial” (IA), cunhado em meados de 1956, logo depois da Segunda Guerra Mundial, foi atribuído para a ciência que tenta não somente compreender, mas também “construir” entidades inteligentes, e esta tem se desenvolvido de forma eficiente em diversas áreas do conhecimento (LUGER, 2013). Em 1.950 foi escrito um dos primeiros artigos tratando sobre inteligência de máquina, cujo autor foi o matemático britânico Alan Turing. Naquela ocasião ele fez a seguinte afirmação: “Eu proponho a considerar a questão ‘máquinas podem pensar?’ Isto deveria iniciar com a definição dos significados dos termos ‘máquinas’ e ‘pensar’ [...]” (TURING, 1950, v. 59, p. 433).

Definir IA é algo muito complexo, pois envolve questões que até hoje estão em busca de uma resposta, porém quando se restringe a sua aplicação, delimita sua abrangência, torna-se mais aceitável seu entendimento. Neste sentido, Luger (2013) afirma que a IA pode ser definida como o ramo da Ciência da Computação que se ocupa da automação do comportamento inteligente. Russel e Norvig (2013), por sua vez, apresentam algumas definições de IA, divididas em quatro categorias, que abordam processo de pensamento e raciocínio, comportamento, proximidade ao desempenho humano e racionalidade, conforme apresentado no Quadro I.

Quadro I: Definições de IA organizada em categorias. Fonte: Russel e Norvig (2013, p.4).

Pensando como um humano	**Pensando racionalmente**
"O novo e interessante esforço para fazer os computadores pensarem (...) máquinas com mentes, no sentido total e literal." "[automatização de] atividades que associamos ao pensamento humano, atividades como a tomada de decisões, a resolução de problemas, o aprendizado..."	"O estudo das faculdades mentais pelo uso de modelos computacionais." "O estudo das computações que tornam possível perceber, raciocinar e agir."
Agindo como seres humanos	**Agindo racionalmente**
"A arte de criar máquinas que executam funções que exigem inteligência quando executadas por pessoas." "O estudo de como os computadores podem fazer tarefas que hoje são melhor desempenhadas pelas pessoas."	"Inteligência computacional é o estudo do projeto de agentes inteligentes." "IA... está relacionada a um desempenho inteligente de artefatos."

Analisando a história da IA, pode-se perceber que houve ciclos de sucesso, otimismo impróprio e quedas devido a entusiasmos e subvenção, mas também houve ciclos de introdução de novas abordagens criativas e de melhoramento sistemático das melhores estratégias. Leva-se em conta que a IA evoluiu mais significativamente nos anos 2000, devido aos avanços tecnológicos nas experiências e na comparação das abordagens (RUSSEL; NORVIG, 2013).

2.1 Redes neurais ARTMAP-*Fuzzy*

Segundo Haykin (2001), o termo Redes Neurais Artificiais (RNA), teve sua motivação de pesquisa devido a sua forma peculiar de trabalho, pois é projetada para modelar a maneira como o cérebro realiza uma tarefa particular ou função de interesse. Diversos pesquisadores tem se dedicado a esta área, porém com maiores avanços a partir da década de 90, pois a ideia de se construir algo dotado de inteligência é um sonho antigo das áreas de engenharia e

ciências. Segundo Silva, Spatti e Flauzino (2010), sistema considerados inteligentes tem sido utilizado em diversos casos, como avaliação de imagens captadas por satélites, classificação de padrões de escrita e de fala, reconhecimento de faces em visão computacional, controle de trens de grande velocidade, previsão de ações no mercado financeiro, identificação de anomalias em imagens médicas, identificação automática de perfis de crédito para clientes de instituições financeiras e controle de parelhos eletrônicos e eletrodomésticos, como máquina de lavar roupa, microondas, geladeiras etc.

2.1.1 Neurônio biológico

Operando em paralelo, os elementos processadores biológicos regem o processamento de informações no cérebro humano, tendo como objetivo a produção de ações apropriadas para cada uma de suas funcionalidades, sendo elas pensar e memorizar. O neurônio é a célula elementar do sistema nervoso cerebral e tem seu papel resumido a conduzir impulsos sob determinadas condições de operação. Conforme a Figura 1, o neurônio é divido em três partes principais: dendritos, corpo celular e axônio (SILVA; SPATTI; FLAUZINO, 2010).

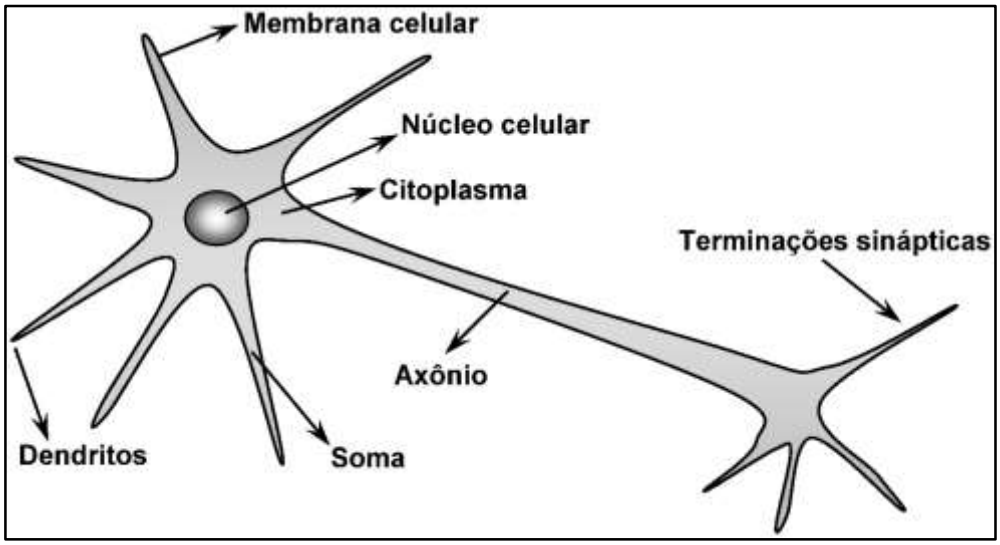

Figura 1: Neurônio Biológico. Fonte: Silva, Spatti e Flauzino (2010, p.29).

As sinapses, conexões que viabilizam a transferência de impulsos elétricos do axônio de um neurônio para os dendritos de outros, são responsáveis por mediar as interações entre os neurônios e podem ser consideradas como uma conexão simples que pode impor ao neurônio receptivo uma excitação ou inibição, mas não ambas. Neste caso, a plasticidade pode ser atribuída a dois mecanismos: a criação de novas conexões sinápticas entre neurônios e a modificação das sinapses existentes, onde as razões para o uso de potenciais de ação para a comunicação entre neurônios se baseiam na física dos axônios (HAYKIN, 2001).

2.1.2 Arquiteturas das redes neurais

A organização e a interconexão dos neurônios definem a arquitetura de uma RNA e está diretamente ligado com o modelo do algoritmo de aprendizagem utilizado para treinar a rede. Esses arranjos são estruturados por meio do direcionamento das conexões sinápticas dos neurônios. De maneira geral, uma RNA pode ser dividida em três partes, denominadas de camadas, conforme Quadro II.

Quadro II: Tipos de camadas de uma RNA. Fonte: Silva, Spatti e Flauzino (2010).

Camada de Entrada	É a camada responsável pelo recebimento de dados, sinais, característica ou medições advindas do meio externo, sendo que tais entradas (amostra ou padrões) são geralmente normalizadas em relação às faixas de variações dinâmicas produzidas pelas funções de ativação. Esta normalização implica numa melhor precisão numérica frente às operações matemáticas realizadas pela rede.
Camadas Ocultas (Intermediárias, invisíveis ou escondidas)	São aquelas compostas de neurônios que possuem a responsabilidade de extrair as características associadas ao processo ou sistema a ser inferido. Quase todo o processamento interno da rede é realizado nessas camadas.
Camada de Saída	Esta camada é também constituída de neurônios, sendo responsável pela produção e apresentação dos resultados finais da rede, os quais são advindos dos processamentos efetuados pelos neurônios das camadas anteriores.

Considerando a disposição do neurônio, suas formas de interligação e a constituição de suas camadas, podem ser divididos quanto a sua arquitetura em:

- Redes reticuladas: a localização espacial dos neurônios está diretamente relacionada com o processo de ajuste de seus pesos e limiares;
- Redes recorrentes ou realimentadas: os dados de saída podem ser utilizados como dados de entrada de outros neurônios das camadas anteriores; e
- Redes *feedforward*: os dados fluem das unidades de entrada para as unidades de saída.

2.1.2.1 Processos de treinamento e aspectos de aprendizado

Uma das principais capacidades de uma RNA é o aprendizado a partir da apresentação de amostras que identificam o comportamento do sistema. E após a rede ter aprendido a relação entre as entradas e as saídas desejadas, a rede se mostra capaz de generalizar soluções. Pode-se entender por generalizar, a capacidade de obter as saídas próximas das desejadas a partir de um sinal qualquer de entrada. Neste sentido, segundo Martins (2010), o treinamento pode ser dividido em dois aspectos, a saber:

- Aprendizagem Supervisionada: a rede é treinada a partir de padrões de entradas e saídas. O treinamento acontece por um agente externo (professor) que informa à rede a resposta desejada para o padrão de entrada especificado. O professor adquire conhecimento da rede, na forma de mapeamento de entrada-saída. Dentre algumas redes que possuem este tipo de treinamento, pode-se citar a rede *Adaline*, que utiliza o algoritmo de aprendizagem *Backpropagation*, a rede *Groosberg*, a rede ARTMAP e a rede ARTMAP-*Fuzzy*.
- Aprendizagem Não Supervisionada: exclusivamente, o treinamento depende de vetores de entradas. Este treinamento não possui um agente externo (professor) informando à rede a resposta desejada para o padrão de entrada apresentado. A partir desta ideia a rede projetada deverá ser capaz de efetuar seu aprendizado através de um processamento estatístico dos padrões de entrada juntos de seus respectivos resultados na saída. Podem-se citar como exemplos, as redes: *Hopfield*, *Kohonen* e ART.

3 Rede ARTMAP-*Fuzzy*

A ARTMAP-*Fuzzy* possui uma arquitetura estável e plástica, que garante uma vantagem com relação a outros tipos de RNA. Ao contrário do que acontece com a maioria das redes neurais, ela permite a inclusão de um módulo de treinamento continuado, o qual habilita a extração de conhecimento sem a necessidade de reiniciar o processo de treinamento quando novos padrões são apresentados. Esta característica torna possível um uso reduzido de padrões de entrada na fase de treinamento, durante a análise da aplicação, a extração do conhecimento é contínua, sendo um exemplo de um sistema que busca melhoramento a todo tempo (CARPENTER et al; 1992).

A ARTMAP-*Fuzzy* é um sistema de aprendizagem supervisionado composta de um par de módulos ART (*Adaptive Resonance Theory*) (CARPENTER; GROSSBERG, 1987), ART_a-*Fuzzy* e ART_b-*Fuzzy*, interconectados por um módulo de memória associativa inter-ART. Esta arquitetura de RNA incorpora a teoria *fuzzy* por meio do operador lógico AND *fuzzy* (^), habilitando o sistema neural de aprendizagem, em resposta aos padrões de entradas binários e analógicos, durante os intervalos [0 1], (CARPENTER et al; 1992).

Martins (2010) afirma que um mecanismo interno chamado *match-tracking* é responsável pelo processo auto regulatório da rede neural, no qual maximiza a generalização e minimiza o erro. Quando a rede neural faz uma predição errada, por meio de uma conexão

associativa instruída, o parâmetro de monitoramento do módulo ART_a-*Fuzzy* é incrementado no mínimo necessário para corrigir o erro dele mesmo na próxima busca pela ressonância. A Figura 2 ilustra a arquitetura da ARTMAP-*Fuzzy*.

Segundo Carpenter *et al* (1992), a arquitetura ARTMAP-*Fuzzy* possui três parâmetros principais para o desenvolvimento, chamados:

- Parâmetro de escolha α ($\alpha > 0$): Opera na categoria de seleção;
- Taxa de treinamento β ($\beta \in [0\ 1]$): Controla a velocidade de adaptação da rede;
- Parâmetro de monitoramento (ρ_a, ρ_b e $\rho_{ab} \in [0\ 1]$): controla a ressonância da rede, nomeado os parâmetros responsáveis pelo número de categorias criado.

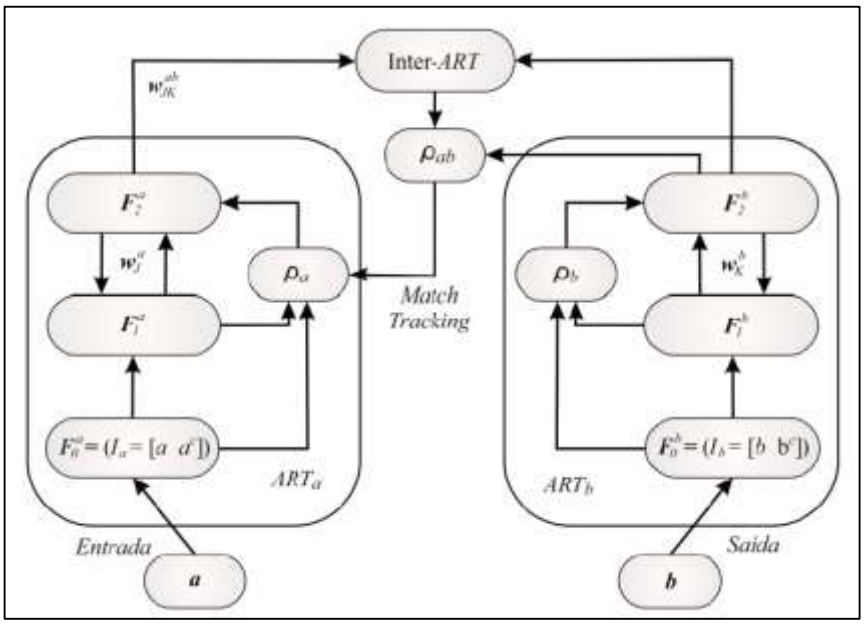

Figura 2: Estrutura da rede neural ARTMAP-*Fuzzy*. Fonte: Carpenter *et al* (1992, p.8).

Se ρ possui um valor alto, a rede neural torna-se mais seletiva reduzindo sua capacidade de generalização. Se ρ possui um valor pequeno, é reduzido o número de categorias criado, maximizando a capacidade de generalização da rede ARTMAP-*Fuzzy*.

4 Aplicação da rede ARTMAP-*Fuzzy* na detecção de intrusos

O objetivo deste trabalho é utilizar uma rede do tipo ARTMAP-*Fuzzy* na detecção intrusos em uma rede de computadores. A aplicação deste tipo de RNA neste problema, é um diferencial comparado a outras técnicas. Pode-se citar como principal vantagem o fato de possuir uma decisão mais robusta, já que a ARTMAP utiliza a lógica *Fuzzy* na sua operação. O sistema proposto neste trabalho deve ser capaz de detectar o seguinte tipo de ataque em uma rede de computadores: Ataque de Negação de Serviço.

4.1 Ataques de negação de serviço

De acordo com Silva (2008), os ataques do tipo Negação de Serviço, do inglês *Denial of Service* (DoS), tentam reduzir o desempenho, o funcionamento ou interromper sistemas e serviços de rede. O principal objetivo deste tipo de ataque é parar o funcionamento de um serviço ou interromper a atividade de uma estação servidora ou qualquer outro equipamento conectado à rede. Apache2, Back, Land, Mail bomb, SYN Flood, Ping of death, Process table, Smurf, Syslogd, Teardrop e Udpstorm são alguns casos que podem ser citados como exemplos de ataques desta categoria.

Dessa forma é possível inundar a rede fazendo com que os usuários verdadeiros fiquem sem a utilizar, pois também atrapalha a conexão entre duas máquinas. O acesso a um serviço fica totalmente comprometido, daí o nome de "negação de serviço", pois o sistema está muito ocupado tentando atender a uma inundação de solicitações.

4.2 O desenvolvimento do sistema

O sistema para detecção foi implementado em MATLAB, utilizando-se da versão 8.1. Foi escolhida esta plataforma de desenvolvimento devido o potencial para se trabalhar com matriz de dados, além de oferecer diversos recursos para geração de gráficos. Durante as pesquisas por referências bibliográficas, não foi encontrada publicação utilizando-se dessa linguagem para a implementação do código referente a uma rede ARTMAP-*Fuzzy* aplicada em sistema de identificação de intrusão, apenas o uso de algum tipo de ferramenta pronta aplicada a este fim, conforme trabalho desenvolvido por Araújo *et al* (2015).

A importância em se desenvolver o código de um método de inteligência artificial é a possibilidade de conhecer mais profundamente seu funcionamento e ter a flexibilidade de escolher quais tipos de funções utilizar, permitindo identificar qual a melhor escolha para melhorar o resultado obtido.

4.3 Descrições do cenário

A base para aplicação da ARTMAP-*Fuzzy* é chamada KDD99, disponibilizada por Lippmann *et al* (2000). Esta base foi utilizada em uma competição cuja tarefa era construir um detector de intrusão de rede, um modelo preditivo capaz de distinguir entre conexões do tipo *bad*, chamadas de invasões ou ataques, e conexões normais do tipo *good*. Ela contém um padrão de dados para serem analisados, que inclui uma grande variedade de intrusões simuladas em um ambiente de rede militar.

Durante a pesquisa, foi levado em conta o tempo gasto para aprendizagem, taxa de detecção durante a generalização e as taxas de precisão e de erros na detecção. O cenário consiste em:

- Base KDD99
    - Foi utilizado 50% desta base para o treinamento da rede;
    - Foi utilizado os outros 50% da base para a generalização, obtendo a taxa de precisão e a taxa de erro do algoritmo.

De acordo com o Quadro III, pode-se observar os principais parâmetros da rede ARTMAP-*Fuzzy* utilizada na detecção de intrusos.

Quadro III: Parâmetros para a rede neural ARTMAP-*Fuzzy*. Fonte: elaborado pelo autor.

Parâmetro	**Valor**
Parâmetro de escolha α	0,10
Taxa de treinamento β	1,00
Parâmetros de Vigilância (ART_a)	0,92
Parâmetros de Vigilância (ART_b)	0,99
Parâmetro de Vigilância (inter-ART)	1,00

A configuração dos parâmetros foi realizada manualmente por meio de observação dos resultados a cada alteração, buscando assim a melhor configuração, ou seja, aquela que atingisse um maior índice de acerto durante a fase de diagnóstico. Após as devidas configurações, a rede gastou 47 segundos durante o processo de aprendizagem e 26 segundos para efetuar a generalização dos dados. Com relação à correta identificação dos dados como normais e anomalias, obteve um resultado expressivo. Como se vê no gráfico 1, sobre os 100% de dados anômalos, o sistema foi capaz de detectar 79,1% das possibilidades, obtendo 21,9% de erro. Sobre os 100% de dados normais, o sistema obteve êxito em 85% das possibilidades, errando 15% das vezes.

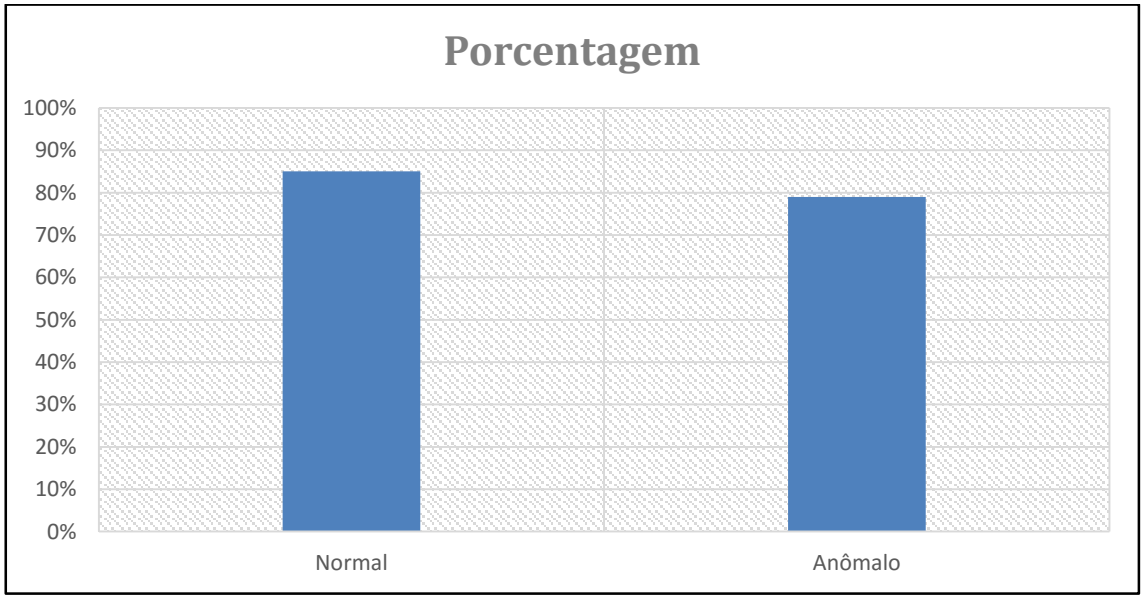

Gráfico 1: Resultados do sistema ARTMAP-*Fuzzy*. Fonte: elaborado pelo autor.

5 Considerações finais

Os resultados apresentados pelo sistema de detecção, mostrou-se de forma satisfatória, apresentando um tempo de aprendizagem menor que 1 minuto (47 segundos), e taxa de 79,1% de acerto em tráfego suspeito (anômalo). Dentro da área aplicada, o sistema utilizando a rede ARTMAP-*Fuzzy* obteve um resultado positivo neste tipo de aplicação. Portanto, acredita-se ter atingido o principal objetivo que é a aplicação de um método de inteligência artificial em um problema presente nas redes de comunicação, problema este relacionado com a detecção de intrusos.

Como melhoria deste trabalho pode-se otimizar a codificação do programa e implementar a aplicação de forma que colete dados em tempo real em uma rede de computadores. Também será interessante realizar testes para um mesmo problema utilizando vários tipos de RNAs, a fim de optar pela de melhor resultado, melhorando a precisão da resposta do sistema, diminuindo a quantidade de falsos-positivos. Além de efetuar comparativos com softwares pré-configurados como o Weka.

6 Referências

ARAUJO, N. V. S. **Kappa-PSO-ARTMAP Fuzzy: uma metodologia para detecção de intrusos baseado em seleção de atributos e otimização de parâmetros numa rede neural ARTMAP Fuzzy**. 2013. 110 f. Tese (Doutorado em Engenharia Elétrica) - Faculdade de Engenharia, Universidade Estadual Paulista – UNESP, Ilha Solteira, 2013.

CARPENTER, G. A. et al. **Fuzzy ARTMAP:** A neural network for incremental supervised learning of anolog multidimensional maps. IEEE Transactions on Neural Network, vol. 3, n. 5, p. 689-713, 1992.

CARPENTER, G. A.; GROSSBERG, S. **A massively parallel architecture for a self-organizing neural pattern recognition machine**. Computer Vision, Graphics and Image Processing, p. 54-115, 1987.

HAYKIN, S. **Redes Neurais**: princípios e prática. Tradução Paulo Martins Engel. 2ª. ed. Porto Alegre: Bookman, 2001.

LIPPMANN, R. et al. **The 1999 DARPA off-line intrusion detection evaluation**. Computer Networks, vol.34, n.4, pp. 579-595, 2000.

LUGER, G. F. **Inteligência Artificial.** Tradução Daniel Vieira. 6.ed. São Paulo: Pearson Education do Brasil, 2013.

MARTINS, J. R. D. **Detecção e classificação de curto-circuitos em sistema de distribuição usando rede neural artificial ARTMAP nebulosa**. Dissertação (Mestrado) – Universidade Estadual Paulista – Faculdade de Engenharia de Ilha Solteira, 2010.

MATLAB (R2013a). 8.1 Version, Mathworks Company.

RUSSEL, S. J.; NORVIG, P. **Inteligência Artificial.** Tradução Regina Célia Simille. 3.ed. Rio de Janeiro: Elsevier, 2013.

SILVA, I. N.; SPATTI, D. H.; FLAUZINO, R. A. **Redes Neurais Artificiais**: para engenharias e ciências aplicadas. São Paulo: Artiliber, 2010.

SILVA, L. S. **Uma metodologia para detecção de ataques no tráfego de redes baseada em redes neurais.** INPE-15175-TDI/1292. Tese (Doutorado em Computação Aplicada) – Instituo Nacional de Pesquisas Espaciais – INPE, São José dos Campos, 2008.

TURING, A. M. Computing Machinery and Intelligence. **Mind,** v.59, p. 433-460, 1950.