UTILIZAÇÃO DE TÉCNICAS DE *DEEP LEARNING* NA DETECÇÃO DE PACOTES MALICIOSOS EM REDES DE COMPUTADORES

Fausto Henrique da Silva Junior; Rogério Bernardes Andrade; Fernando Eduardo Resende Mattioli

Faculdade de Talentos Humanos, Uberaba (MG), e-mail: faustohsjunior@gmail.com,
{rbandrade, fernando.mattioli}@facthus.edu.br.

RESUMO: A detecção de ameaças em sistemas de informação é um dos pilares da segurança da informação. No entanto, a maioria das ferramentas disponíveis atualmente não dispõe de capacidade de aprendizagem, o que leva à constante necessidade de atualização das mesmas. Recentemente, esta necessidade vem sendo explorada por meio de ataques direcionados a sistemas desatualizados. Neste contexto, o uso de ferramentas com capacidade de aprendizagem possui potencial aplicação na segurança destes sistemas. Este artigo apresentada um modelo de classificação baseado em Redes Neurais Artificiais e técnicas de *Deep Learning* para detecção de pacotes maliciosos em redes de computadores. O modelo apresentado foi treinado e testado utilizando-se um dataset público, experimentado em configurações distintas avaliando-se diferentes topologias das redes neurais e funções de ativação. O classificador desenvolvido apresentou resultados superiores a 99% de acerto na detecção dos pacotes maliciosos, o que indica sua aplicação na proteção de sistemas de informação.

PALAVRAS CHAVE: *Deep Learning*; Redes Neurais Artificiais; Segurança de redes.

ON THE USE OF DEEP LEARNING TECHNIQUES IN THE DETECTION OF MALICIOUS PACKAGES IN COMPUTER NETWORKS

ABSTRACT: The detection of threats in information systems is one of the most important elements of information security. However, many of the currently available tools do not present learning capability, which leads to the need for constantly updating and upgrading these tools. Recently, this need has been explored through attacks targeting outdated systems. In this context, the use of learning-based tools has potential application on the security of these systems. This article presents a model based on Artificial Neural Networks and Deep Learning techniques to detect malicious packets in computer networks. The presented model was trained and validated using a public dataset, experimented under distinct configurations, evaluating different neural network topologies and activation functions. The developed classifier presents accuracy above 99% on the detection of malicious packages, which indicates its application on information systems protection.

KEYWORDS: Deep Learning; Artificial Neural Networks; Network security.

INTRODUÇÃO

Estudos recentes revelam que com o crescimento do uso da informação digital, crescem também as ameaças tais como corrupção e roubo de informações além de clonagem de cartões e contas bancárias (GLOBO, 2016). Utilizando conhecimentos técnicos avançados, criminosos virtuais invadem sistemas informatizados de empresas visando a obtenção de lucro. Após a invasão, estes criminosos estorquem as empresas e usuários dos sistemas por meio da criptografia de informações importantes - liberando essas informações mediante pagamento de resgate - ou da venda de informações sigilosas para empresas concorrentes. Alguns dos ataques mais usados para captura de dados e informação digital são os de porta do fundos, conhecidos como vírus, *worms* e *trojan horse* ou cavalo de Tróia.

As ferramentas mais utilizadas para proteger sistemas de informação destas ameaças são firewalls, sistemas de antivírus e criptografia de informações. No entanto, grande parte das ferramentas utilizadas atualmente na proteção de computadores e sistemas de informação depende da atualização constante de seus componentes. Uma vez detectada uma nova ameaça, a correção é disponibilizada para que estas ferramentas sejam atualizadas com as contramedidas apropriadas. Desta forma, a própria necessidade de atualização representa uma ameaça em potencial, explorada recentemente por vários ataques em massa. Neste contexto, o desenvolvimento de ferramentas dotadas de capacidade de aprendizagem constitui um importante tópico para pesquisa.

Dentre as ferramentas computacionais com capacidade de aprendizagem disponíveis atualmente, destacam-se as Redes Neurais Artificiais (RNA). RNA são ferramentas de processamento paralelo, constituídas pela conexão entre unidades de processamento capazes de armazenar conhecimento experimental, se assemelhando ao cérebro humano (HAYKIN, 2001). Mais recentemente, a denominação “Aprendizagem Profunda” (*“Deep Learning”)* é utilizada para descrever RNA com elevado número de neurônios, diferentes

formas de conexão e mecanismos de extração automática de características (PATTERSON, 2017). Estas RNA tem sido utilizadas na resolução de diferentes classes de problemas, área do conhecimento denominada Aprendizagem Profunda (*Deep Learning).* Pesquisas recentes demonstram sucesso na aplicação de técnicas de *Deep Learning* em diversos domínios tais como reconhecimento de imagens, processamento de sinais, visão computacional dentre outros (BANHARNSAKUN, 2018).

Neste contexto, este trabalho apresenta um estudo de caso da utilização de técnicas de *Deep Learning* na detecção de pacotes maliciosos em redes de computadores. Os experimentos realizados - detalhados nas próximas seções deste artigo - demonstram a eficiência destas técnicas no processamento do dataset utilizado.

REFERENCIAL TEÓRICO

Nesta seção serão apresentados os principais fundamentos teóricos utilizados neste trabalho.

Redes Neurais Artificiais (RNA)

Redes neurais artificiais são modelos computacionais baseados no sistema nervoso dos seres humanos (FINOCCHIO, 2014). O conceito de RNA surgiu na década de 1940 a partir dos artigos publicados por Warren McCulloch e Walter Pitts. Nestes artigos é apresentada uma comparação entre células nervosas vivas e um processo eletrônico, simulando o comportamento de um neurônio natural com apenas uma saída (FINOCCHIO, 2014).

As RNA são organizadas em camadas conectadas entre si, sendo cada camada composta por um conjunto de unidades de processamento ou neurônios. Em uma RNA *feedforward*, os neurônios são divididos nas camadas de entrada, intermediária(s) ou oculta(s) e de saída. Cada neurônio se conecta com os neurônios das camadas anteriores por meio de ganhos ou pesos numéricos, sendo a propagação da informação em um único sentido (da camada de entrada em direção à camada de saída).

Os pesos são inicializados com valores aleatórios. Durante a fase de treinamento, vários padrões são apresentados à rede, para que os pesos sejam ajustados proporcionalmente ao erro da rede na classificação de cada padrão. A Fig. 1 apresenta um modelo de RNA com uma camada oculta.

Deep Learning

Deep Learning é uma subcategoria da inteligência artificial (CLAESSON, 2017). A capacidade de processamento apresentada pelos computadores atuais, bem como a quantidade de informações digitais disponíveis possibilitam o treinamento de redes em *Deep Learning* nas mais diversas aplicações, estando disponíveis para desenvolvedores várias bibliotecas e ferramentas para construção destas aplicações (CLAESSON, 2017).

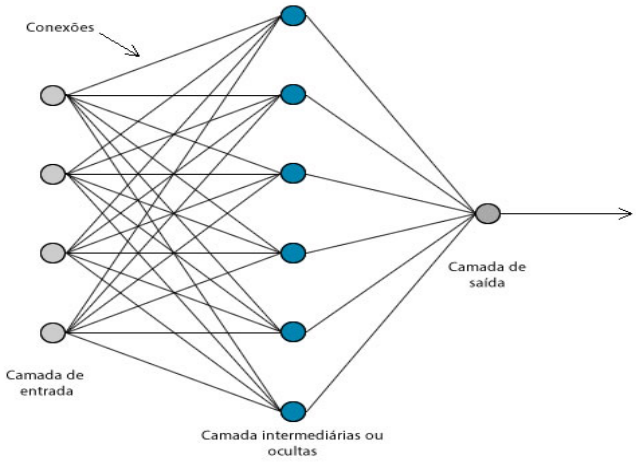

FIGURA 1 - Rede Neural Artificial.
FONTE: Arquivo pessoal do autor.

Funções de ativação

Em RNA o sinal gerado pela combinação linear das entradas e dos pesos das conexões é processado por uma função de ativação para gerar o sinal de saída do neurônio. Dentre as funções de ativação mais utilizadas, destacam-se as funções sigmóide, tangente hiperbólica e ReLU.

A função sigmóide é a mais utilizada em RNA sendo uma função monotônica crescente que apresenta propriedades assintóticas e de suavidade. É uma função com forma de “s”, monotonicamente crescente, que exibe um balanceamento adequado entre comportamento linear e não-linear. A saída da função sigmóide pertence ao intervalo (0, 1). A função sigmóide é apresentada na Eq. 1 e sua curva característica na Fig. 2 (FINOCCHIO, 2014).

$$f(x) = \frac{L}{1 + e^{-k(x - x_0)}} \quad (1)$$

sendo e a base dos logaritmos naturais, x_0 o valor de x no ponto médio da curva sigmóide, L o valor máximo da curva e k a declividade da curva.

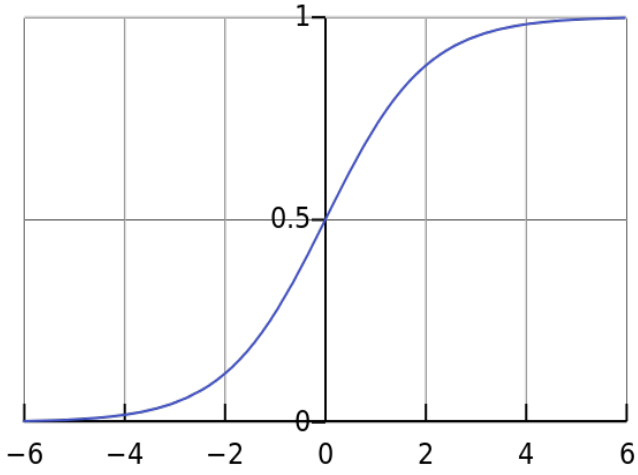

FIGURA 2 - Função sigmóide.
FONTE: Arquivo pessoal do autor.

Em muitos casos a função sigmóide é substituída pela função tangente hiperbólica (TanH), que preserva a forma sigmoidal da função anterior, mas assume valores positivos e negativos, com sua saída pertencendo ao intervalo (-1, 1). A função tangente hiperbólica é apresentada na Eq. 2 e sua curva característica na Fig. 3 (FINOCCHIO, 2014).

$$f(x) = \frac{1 - e^{x}}{1 - e^{-x}} \quad (2)$$

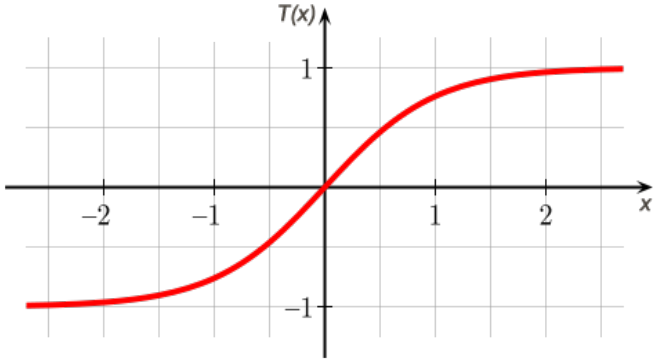

FIGURA 3 – Função TanH.
FONTE: Arquivo pessoal do autor.

Outra função de ativação, utilizada principalmente nos trabalhos que apresentam técnicas de *Deep Learning*, é a função *Rectified Linear Unit* (ReLU). Estudos reportam a melhor eficiência da função ReLU em comparação à função sigmóide para problemas de classificação envolvendo processamento de imagens (FINOCCHIO, 2014). A Eq. 3 apresenta a função ReLU, enquanto a Fig. 4 apresenta sua curva característica (FINOCCHIO, 2014).

$$f(x) = max(0, x) \quad (3)$$

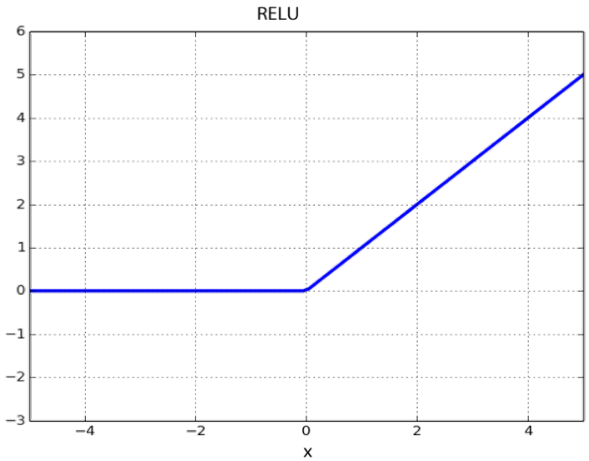

FIGURA 4 - Função ReLU.
FONTE: Arquivo pessoal do autor.

MATERIAIS E MÉTODOS

Os experimentos descritos neste trabalho foram realizados em um computador com processador de 3.3 GHz, 8 GB de memória RAM e sistema operacional Windows. Os classificadores foram implementados utilizando a linguagem de programação Python[1], a biblioteca Tensorflow[2] e o framework Keras[3].

Tensorflow é uma biblioteca *open source* para aprendizagem de máquina, desenvolvida pela empresa Google e lançada em 2015. A biblioteca possui configurações para execução em múltiplas CPUs e GPUs, estando disponível para as plataformas Windows, Linux, Mac, Android e IOS. Dentre os recursos que possibilitam a utilização da biblioteca Tensorflow, destaca-se o framework Keras, criado por François Chollet e escrito na linguagem de programação Python. O framework possui uma integração nativa com o Tensorflow, oferecendo uma abstração de nível superior às funcionalidades da biblioteca.

O dataset utilizado nos experimentos realizados foi criado pela DARPA (*Defense Advanced Research Projects Agency)* em 1998. O dataset é o resultado de um programa de avaliação de métodos para detecção de intrusão coordenado pelos laboratórios MIT Lincoln Labs. O dataset contém dados resultantes de uma ampla variedade de intrusões simuladas em uma rede militar. No total, foram capturados pacotes TCP brutos durante nove semanas de simulações. Finalmente, o dataset apresenta 125000 padrões, nos quais os pacotes são classificados como normais ou maliciosos.

O número total de padrões foi dividido aleatoriamente em dois grupos: 100000 padrões para o treinamento e 25000 padrões para o teste dos classificadores. Cada padrão apresenta 42 características, contendo, dentre outros elementos: duração da conexão, tipos de protocolo (TCP, UDP,ICMP), serviços de rede (HTTP, telnet), número de falhas no login, número de acessos do root, conexões de hosts diferentes e data/hora da coleta do pacote, além da classificação do mesmo (normal ou malicioso).

Treinamento das redes

Foram realizados vários experimentos para se testar a influência de diversos parâmetros na eficiência dos classificadores. Dentre os parâmetros avaliados estão as funções de ativação, número de camadas ocultas e número de neurônios em cada camada. Esta avaliação foi realizada alterando-se apenas um parâmetro por vez, para que se pudesse isolar a contribuição deste parâmetro na eficiência do classificador.

Foram utilizados, inicialmente, 20000 padrões para treinamento e 5000 padrões para teste do classificador. A configuração inicial do mesmo é apresentada na Tabela 1.

Em seguida, o número de padrões de treinamento foi aumentado gradativamente, acrescentando-se 20000 padrões a cada iteração, até se atingir o número de 100000 padrões para o treinamento. Analogamente, o número de padrões de teste foi aumentado gradativamente, acrescentando-se 5000 padrões a cada

1 https://www.python.org/
2 https://www.tensorflow.org/
3 https://keras.io/

iteração, até se atingir o número de 25000 padrões. Ao longo destes testes, diversas topologis de rede foram experimentadas. Após os experimentos realizados, foi definida a melhor configuração da rede com a topologia de 2 camadas ocultas com 1000 neurônios em cada, 150 épocas de treinamento e *batch size* de 1000.

TABELA 1 – Parâmetros iniciais.

Parâmetro	**Valor**
Camadas ocultas	2
Épocas	150
Neurônios nas camadas ocultas	1.000

FONTE: Arquivo pessoal do autor.

RESULTADOS

As Fig. 5, 6 e 7 apresentam as curvas de treinamento obtidas utilizando, respectivamente, as funções de ativação Sigmóide, ReLU e TanH. A acurácia das redes foi medida dividindo-se o número de padrões corretamente classificados pelo número total de padrões de teste (25.000), após cada época de treinamento.

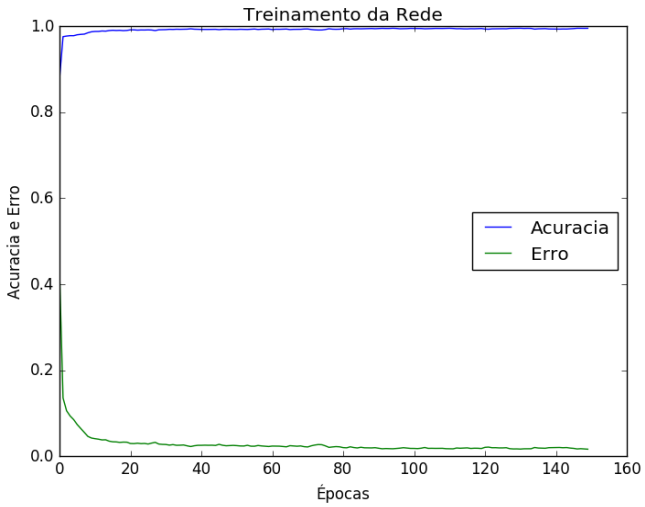

FIGURA 5 - Treinamento com função Sigmóide.
FONTE: Arquivo pessoal do autor.

Nos experimentos realizados foram avaliadas redes com até nove camadas ocultas, com diferentes números de neurônios em cada camada. No entanto, nestes classificadores não foram observadas melhorias significativas na acurácia de classificação. Além deste fato, classificadores com mais camadas demandam tempo maior tanto para treinamento como para execução. Finalmente, os classificadores que apresentaram melhor desempenho são os classificadores com 2 camadas ocultas, contendo 1000 neurônios em cada camada, com função de ativação Sigmóide. Os classificadores foram treinados por 150 épocas, apresentando acurácia superior a 99% na classificação dos pacotes de treinamento e de teste. Deve-se ressaltar que estes padrões de teste foram separados dos padrões de treinamento, sendo, portanto, desconhecidos pela rede. A Tabela 2 apresenta, em resumo, a acurácia obtida para cada uma das funções de ativação avaliadas, em treinamento e em teste da rede.

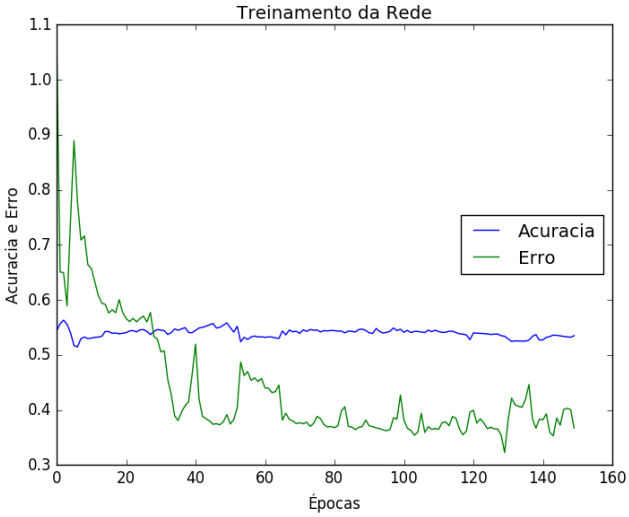

FIGURA 6 - Treinamento com função RELU.
FONTE: Arquivo pessoal do autor.

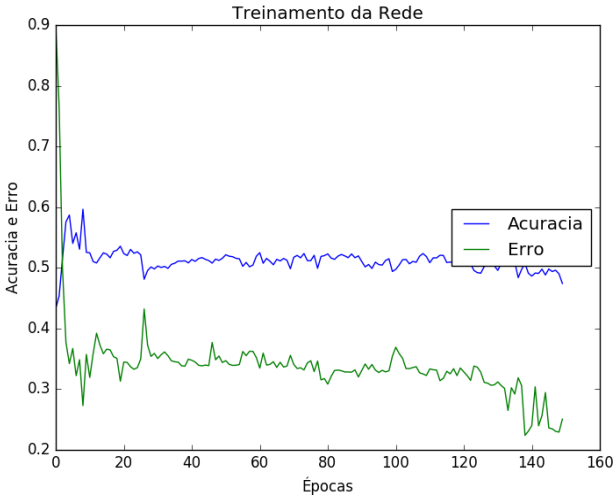

FIGURA 7 - Treinamento com função TanH.
FONTE: Arquivo pessoal do autor.

TABELA 2 – Acurácia (ACC) dos classificadores avaliados.

Etapa	**Função de ativação**			
		Sigmóide	**ReLU**	**TanH**
Treinamento	**Corretos**	97710	53490	45780
	Errados	290	46510	54220
	ACC (%)	99,71	53,49	45,78
Teste	**Corretos**	24920	13350	11300
	Errados	80	11650	13700
	ACC (%)	99,68	53,40	45,20

FONTE: Arquivo pessoal do autor.

CONCLUSÕES

Os experimentos apresentados neste trabalho demonstram a promissora aplicação das técnicas de *Deep Learning* na detecção de pacotes maliciosos em redes de computadores. A rede implementada com a

função de ativação sigmóide foi capaz de detectar tais pacotes com uma eficiência superior a 99% (24.920 pacotes corretamente classificados de um total de 25.000 pacotes analisados). Os resultados apresentados demonstram a eficácia das técnicas desenvolvidas, que podem ser aplicadas em ambientes onde se disponha de meios para capturar os pacotes de rede no formato apresentado. Como uma potencial aplicação em produção, a RNA desenvolvida pode ser utilizada antes do firewall reduzindo assim a sobrecarga de processamento do mesmo. Trabalhos futuros serão conduzidos para se validar as técnicas utilizadas em diferentes datasets e a adaptação das mesmas a sistemas de detecção em tempo real.

REFERÊNCIAS

BANHARNSAKUN, Anan. Towards improving the convolutional neural networks for deep learning using the distributed artificial bee colony method. **International Journal of Machine Learning and Cybernetics**, p. 1-11, 2018.

CLAESSON, Linnéa, HANSSON, Björn, **Deep Learning Methods and Applications**, 2017. Disponível em <http://publications.lib.chalmers.se/records/fulltext/248445/248445.pdf> Acesso em 29 maio 2017.

FINOCCHIO, Marco Antonio Ferreira, **Noções de redes neurais artificiais**, 2014. Disponível em <http://paginapessoal.utfpr.edu.br/mafinocchio/labsi-laboratorio-de-seguranca-e-iluminacao/redes-neurais-artificiais/NOCaO%20DE%20REDES%20NEURAIS%20ARTIFICIAIS.pdf/at_download/file> Acesso em 29 maio 2017.

GLOBO, **Pesquisa mostra que hackers estão agindo livremente no Brasil**, Jornal Nacional, 27 jan. 2016. Disponível em: <http://g1.globo.com/jornal-nacional/noticia/2016/01/pesquisa-mostra-que-hackers-estao-agindo-livremente-no-brasil.html> Acesso em 22 fev. 2017.

GOODFELLOW et al, **Deep Learning Book**, 2016. Disponível em <http://www.deeplearningbook.org/> Acesso em 10 maio 2017.

HAYKIN, Simon. **Redes neurais: princípios e prática**. Bookman Editora, 2007.

PATTERSON, Josh; GIBSON, Adam. **Deep Learning: A Practitioner's Approach**. O'Reilly Media, Inc. 2017.