INSTITUTO FEDERAL
SÃO PAULO
Câmpus Presidente Epitácio

VIII MC²T - VIII Mostra Científica, Cultural e Tecnológica

Uma Análise Comparativa de Arquiteturas de Redes Neurais para Detecção de Intrusão por Anomalias em Redes de Computadores

Roberto S. L. Junior[1], Kleber M. Trevisani[2]
1.Discente do Curso Bacharelado em Ciência da Computação – IFSP – Câmpus Presidente Epitácio;
2.Docente do IFSP - Câmpus Presidente Epitácio, Área de Informática.
E-mails: robertojunor.lara@gmail.com, kleber@ifsp.edu.br

Introdução

Os sistemas de detecção de intrusão ou IDS (Intrusion Detection Systems) são sistemas computacionais capazes de perceber a ocorrência de um ataque ou comportamento anormal e produzir uma resposta (CARVALHO, 2005).

O Behavior-Based Intrusion Detection (detecção de intrusão baseada em anomalia) assume que as intrusões podem ser detectadas por meio de desvios de comportamento dos usuários ou dos sistemas. O modelo de normalidade é definido de diversas maneiras e comparado com a atividade em andamento. Qualquer comportamento suspeito, diferente do padrão, é considerado intrusivo. Também são conhecidas como detecção por anomalia (CARVALHO, 2005).

A detecção de intrusão por anomalias tem sido tratada na literatura em diversas propostas que utilizam técnicas de aprendizado de máquina. Henke et al. (2011).

Aprendizado de Máquina (AM) é uma área de inteligência artificial cujo objetivo é o desenvolvimento de técnicas computacionais sobre o aprendizado bem como a construção de sistemas capazes de adquirir conhecimento de forma automática (MONARD, BARANAUSKAS, 2003). Aprendizagem Profunda ou Deep Learning, é uma subárea da Aprendizagem de Máquina, que emprega algoritmos para processar dados e imitar o processamento feito pelo cérebro humano (DATA SCIENCE ACADEMY, 2019).

Metodologia

Inicialmente foi realizada uma revisão bibliográfica sobre várias técnicas utilizadas para implementação de IDS baseado em anomalia. O estudo foi útil para direcionar a seleção das técnicas de aprendizado profundo e arquiteturas de rede a serem utilizadas nos experimentos.

Em seguida, baseando-se em trabalhos relacionados, foram selecionadas três arquiteturas de Redes Neurais para a detecção de intrusão.

O próximo passo foi a implementação de um único algoritmo, alterando somente a implementação da arquitetura de rede neural, cujo código foi baseado nos estudos e implementações de Heaton (2020). Heaton (2020) utilizou uma arquitetura Multilayer Perceptron para realizar a detecção de intrusão baseada em anomalia. Esse tipo de arquitetura está sendo utilizado neste trabalho. Também foram utilizadas as arquiteturas de Rede Neural Convolucional (CNN), baseando-se no trabalho desenvolvido por Vinayakumar, Soman, Poornachandan (2017), e Rede Neural Recorrente (RNN), avaliada no trabalho de Yin et al. (2017).

Um Multilayer Perceptron (MLP) é uma rede neural artificial composta por mais de um Perceptron. Eles são compostos por uma camada de entrada para receber o sinal, uma camada de saída que toma uma decisão ou previsão sobre a entrada, e entre esses dois, um número arbitrário de camadas ocultas que são o verdadeiro mecanismo computacional do MLP (DATA SCIENCE ACADEMY, 2019).

As Redes Neurais Convolucionais (ConvNets ou CNNs) são redes neurais artificiais profundas que podem ser usadas para classificar imagens, agrupá-las por similaridade (busca de fotos) e realizar reconhecimento de objetos dentro de cenas. Mais recentemente, essas redes têm sido aplicadas diretamente à análise de texto (DATA SCIENCE ACADEMY, 2019).

As Redes Neurais Recorrentes (RNN) são um conjunto de algoritmos de redes neurais artificiais.As redes recorrentes incluem um loop de feedback, pelo qual a saída do passo n-1 é alimentada de volta à rede para afetar o resultado do passo n, e assim por diante para cada etapa subsequente (DATA SCIENCE ACADEMY, 2019).

Os experimentos deste trabalho estão sendo desenvolvidos em linguagem Python, utilizando a plataforma Jupyter. A principal biblioteca usada para o desenvolvimento das aplicações é o Tensorflow 2.0.

A base de dados utilizada para os experimentos foi a Knowledge Discovery and Data Mining, conhecida também como KDD Cup 1999 (KDD99).

Resultados

Inicialmente, foram realizados experimentos com a arquitetura Multilayer Perceptron, também baseada na implementação de Heaton (2020), mas invés de 100 épocas, foram usados 1000 épocas para treinamento. Nesse sentido, aplicando o subconjunto de 25% (dados normais), obteve-se um RMSE (Root-mean square error) de 0.24. Já aplicando o conjunto de dados de ataque, obteve-se um RMSE de 0.65.

Para finalizar a pesquisa, ainda é necessário implementar as arquiteturas de Rede Neural Convolucional e Recorrente e obter seus dados de acurácia e desempenho.

Conclusões

As Redes Neurais são técnicas amplamente utilizadas para experimentos de Detecção por Intrusão, uma vez que conseguem analisar grandes quantidades de dados afim de detectar uma anomalia.

Bibliografia

CARVALHO, Luciano Gonçalves de. **Segurança de redes.** Rio de Janeiro: Ciência Moderna, c2005. 79 p. ISBN 8573934379.

HENKE, M. COSTA, C. SANTOS, E. M. SOUTO, E. **Detecção de Intrusão usando Conjunto de k-NN gerado por Subespaços Aleatórios.** Universidade Federal do Amazonas (UFAM), 2011, Amazonas, AM.

MONARD, M. C. BARANAUSKAS, J. **A. Conceitos sobre Aprendizado de Máquina.** 2003.

Data Science Academy. **Deep Learning Book,** 2019. Disponível em: <http://www.deeplearningbook.com.br/>. Acesso em: 19 de setembro. 2020.

HEATON, F. **Applications of Deep Neural Networks.** Disponível em: https://github.com/jeffheaton/t81_558_deep_learning/blob/master/t81_558_class_14_03_anomaly.ipynb. Acesso em: 22 de setembro, 2020.