Detecção de anomalias em tráfego de redes por modelos supervisionados de aprendizado de máquina

Detection of network traffic anomalies by supervised machine learning models

Breno da Silva Lima*, Luiz Fernando Carvalho†

RESUMO

Quando se trata de segurança e tecnologia, existe um cenário onde sempre haverá avanços a serem feitos conforme a sociedade progride, principalmente nos meios digitais. Sendo assim, cria-se o objetivo de entender os conceitos utilizados no tráfego de redes, assim como a construção de um SDI (sistema de detecção de intrusões) junto a conhecimentos de aprendizado de máquina para detectar ataques e anomalias em redes de computadores. Visto a necessidade de garantir essa segurança, durante o período de um ano foram realizadas diferentes atividades que representam os cenários de ataques, e com o uso da linguagem de programação Python para aplicar os conceitos de aprendizado de máquina, notou-se uma significativa acurácia na detecção dos ataques por meio da SDI criado.

Palavras-chave: segurança de rede, detecção de anomalias, aprendizado de máquina.

ABSTRACT

When it comes to security and technology, there is a scenario where there will always be advances to be made as society progresses, especially in digital media, thus creating the goal to understand the concepts used in network traffic, as well as construction of an SDI (intrusion detection system) together with machine learning knowledge to detect attacks and anomalies in computer networks. Given the need to ensure this security, during a period of one year, different activities were carried out that represent the attack scenarios, and with the use of the python programming language to apply the concepts of machine learning, a significant accuracy in the detection of attacks through the created SDI.

Keywords: network security, anomaly detection, machine learning.

1 INTRODUÇÃO

Com o alto número de fluxos de informações que os sistemas de hoje em dia carregam, detectar uma intrusão na rede pode economizar uma grande quantidade de recursos e tempo, logo, se torna de interesse que sistemas que controlam um fluxo de informações possam se prevenir de ataques como um DDoS (ataque distribuído de negação de serviço, do inglês *Distributed Denial of Service*), que sobrecarregam o servidor e o impede de continuar o seu trabalho de forma correta (PATCHA, 2007). Em um mundo cada vez mais conectado, surge a necessidade de se estar atento a possíveis ameaças, e como a citada acima, o DDoS, existem diversas outras fontes de problemas quando se trata de segurança digital (HAMAMOTO, 2018). No

* Engenharia da Computação, Universidade Tecnológica Federal do Paraná, Apucarana, Paraná, Brasil; brenolima@alunos.utfpr.edu.br
† Universidade Tecnológica Federal do Paraná, Campus Apucarana; luizfcarvalho@utfpr.edu.br

geral, tem-se um cenário passível de ataques de diferentes formas, então, como proteger a rede de tantos ataques distintos que podem ser feitos?

É possível demonstrar que, um sistema de detecção de intrusões construído a partir dos conceitos de aprendizado de máquina, irá compreender os padrões presentes nos dados fornecidos a ele, informações essas que representam cenários de ataques e não ataques (JUNIOR, 2018). Junto a isso, uma vez tendo o modelo treinado, ele pode ser replicado para cenários reais e identificar se há alguma anomalia presente em sistemas de empresas ou corporações. A construção de tal modelo irá primeiro levar em conta os dados apresentados, e, uma vez tendo estabelecido o cenário no qual o programa irá aprender, os conceitos de aprendizado de máquina são aplicados.

Entre os assuntos presentes em aprendizado de máquina, este trabalho visa compreender o comportamentos dos modelos supervisionados, ou seja, aqueles modelos que precisam de uma interação humana para funcionar, seja para alimentá-los com os dados certos e rotulados, ou avaliá-los de forma correta. Diferentes conceitos de modelos foram aplicados, dentre eles o *knn* (k-ésimo vizinho mais próximo, do inglês *k-nearest neighbors*), Árvore de Decisão, Random Forest, Máquina de Vetores de Suporte e Perceptron Multicamadas. Após os treinos, métodos avaliativos foram aplicados para se concluir qual dos modelos apresentaria uma performance mais elevada.

2 MÉTODO

No ano de 2020 até 2021, durante o período de um ano da pesquisa, foram realizadas diferentes atividades que representavam o cenário de ataques formados nos dados dispostos para estudo, sendo o objetivo maior criar um SDI (sistema de de detecção de intrusões) para os dados fornecidos pela UNB (University of New Brunswick). Os dados de “DDoS Evaluation Dataset (CIC - DDoS 2019)” (UNB, 2019) foi o alvo principal do estudo.

Nas informações presentes nos dados há diferentes tipos de ataques DDoS para estudos, tais como ataques NTP, DNS, LDAP, MSSQL, NetBIOS, SNMP, SSDP, UDP, UDP-Lag, WebDDoS, SYN e TFTP, somando no total 12 tipos distintos de ataques DDoS. Todos possuem o mesmo objetivo, ameaçar a segurança de uma rede ao oferecer dados maliciosos com intenção de sobrecarregar os recursos dos servidores. Os dados de treino são formados por 16598 linhas e 87 colunas, já o de teste é constituído por 7193 linhas e 88 colunas. Os conjuntos de dados irão descrever o cenário do tráfego da rede, e a partir daqueles casos identificados como ataques ou não ataques, o modelo de aprendizado de máquina irá traçar padrões entre os dados para distinguir entre instâncias de tráfego malicioso ou legítimo.

Os dados fornecidos foram avaliados e redistribuídos de forma que facilite o manuseio das operações futuras, ou seja, problemas como maldição da dimensionalidade (quantidade excessiva de atributos), valores faltantes e separação do atributo desejado (rótulo) como resposta foram tratados. Para tal, métodos como

ACP (Análise do Componente Principal, do inglês *Principal Component Analysis*) e seleção de atributos por meio da Random Forest foram usados para solucionar a maldição da dimensionalidade.

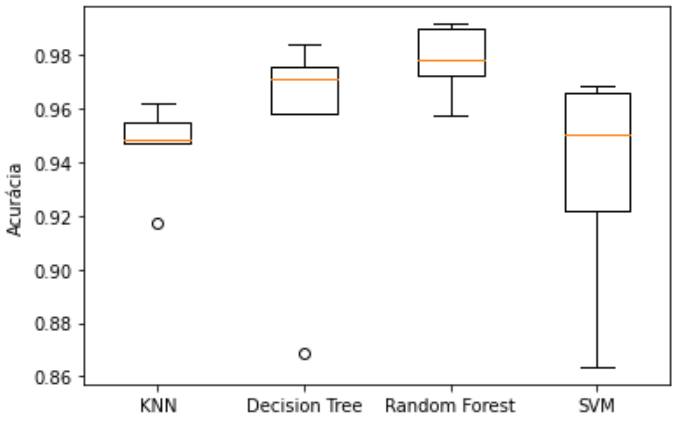
Diversos modelos foram treinados a partir dos dados como fonte de estudo para compreender como cada um se comporta, sendo esses o *knn*, que mensura a distância dos dados de treino com o de teste para gerar uma resposta. Junto a isso, foi utilizado o algoritmo de Árvore de Decisão, um algoritmo que analisa os atributos presentes nos dados e os divide em ramos para formar respostas. O algoritmo Random Forest também foi aplicado, sendo ele um conjunto de diferentes árvores de decisões que aprendem e escolhem os dados de forma aleatória. Máquina de Vetores de Suporte foi um outro modelo testado, e assim como o Perceptron Multicamadas, ambos demonstraram ter uma melhoria ao aprender com os dados normalizados.

Em seguida ao estudo dos diferentes modelos de aprendizado de máquina e como eles se comportam visto os dados apresentados e seus parâmetros, o modelo que apresentou a melhor performance foi escolhido e então gerou-se o resultado final para os dados de teste.

3 RESULTADOS

Para avaliação dos modelos, a validação cruzada foi aplicada para conseguir um resultado com maior precisão. Como os modelos podem aprender de formas diferentes cada vez que são treinados, eles podem desconsiderar informações importantes, ou até mesmo selecionar dados não relevantes para sua indução. Portanto, para prevenir tais possibilidades, modelos diferentes são treinados para que então haja maior diversidade no processo de aprendizagem e seja possível mensurar uma média da acurácia das diferentes aprendizagens dos modelos na validação cruzada, como demonstrado na figura 1.

Figura 1 – Acurácia dos modelos



Fonte: Autoria própria (2021)

Diferentes resultados das validações cruzadas dos modelos são exibidas, onde o eixo horizontal representa os modelos, e o vertical a acurácia. Para a avaliação de cada modelo foi utilizado o método

f-measure para indicar a acurácia das respostas oferecidas por eles, um método que leva em consideração não apenas a quantidade de acertos, mas o quanto o modelo errou. Nos gráficos da figura 1, destaca-se a linha horizontal na cor laranja contida em cada boxplot, a qual representa a mediana dos resultados gerados após várias execuções do modelo. Por meio desse valor é possível verificar que os melhores resultados foram atingidos pela Random Forest

Por último, o modelo de Perceptron Multicamadas foi construído utilizando os dados já preparados, e para os seus parâmetros, o método de pesquisa de grade aleatória foi aplicado. A otimização dos parâmetros consistiu em treinar o modelo utilizando parâmetros inicialmente aleatórios para então otimizá-los. Ao final dos testes, a acurácia para o modelo Perceptron de Multicamadas junto ao método avaliativo *f-measure* foi de 95%.

A Tabela 1 apresenta o resultado de cada modelo estudado, sendo representado por sua mediana dos valores avaliados pelo *f-measure*.

Tabela 1 – Resultado dos modelos

Modelo	f-measure(%)
KNN	94,9
Árvore de Decisão	97,3
Random Forest	97,7
Máquina de Vetores de Suporte	95
Perceptron Multicamadas	96,8

Fonte: Autoria própria (2021).

O modelo com maior acurácia apresentado nos testes foi o de Random Forest com um valor de 97,7% de acerto de acordo com o *f-measure.*

4 CONCLUSÃO

A partir dos dados apresentados, pode-se afirmar que há uma significativa solução para o problema de DDoS apresentado nos dados. Sendo assim, o modelo de Random Forest que apresenta um acerto de 99% é uma excelente proposta como prevenção de ataques a sistemas. Empresas ou corporações que optassem por utilizar o modelo como uma camada de segurança dentro de seus sistemas, estariam mais protegidos.

AGRADECIMENTOS

Gostaria de agradecer à Fundação Araucária pela bolsa oferecida, junto ao agradecimento ao meu professor Luiz Fernando por me guiar nesse processo de aprendizado.

REFERÊNCIAS

HAMAMOTO, A.H., CARVALHO, L.F, SAMPAIO, L.D.H., ABRÃO, T., PROENÇA, M.L. **Network Anomaly Detection System using Genetic Algorithm and Fuzzy Logic**, Expert Systems with Applications, v. 92, p. 390-402, 2018.

JUNIOR, Gilberto Fernandes; RODRIGUES, Joel J. P. C; CARVALHO, Luiz Fernando; AI-MUHTADI, Jalal F; JUNIOR, Mario Lemes Proença. **A comprehensive survey on network anomaly detection.** Telecommun Syst., 2018.

PATCHA, Animesh; PARK, Jung-Min. **An overview of anomaly detection techniques: Existing solutions and latest technological trends**. Virginia, 2007.

UNB. **"DDoS Evaluation Dataset (CIC - DDoS 2019)"**. Disponível em: https://www.unb.ca/cic/datasets/ddos-2019.html. Acesso em: 14 set. 2021.