Utilização e avaliação de aprendizado de máquina para detecção de ataques DDoS*

Using and evaluating machine learning to detect DDoS attacks

Leonardo Ravaiani da Silva[1]
Felipe Augusto Lima Reis (Orientador)[2]

Resumo

Os Ataques Distribuídos de Negação de Serviço (DDoS - *Distributed Denial of Service*) são uma ameaça persistente e significativa para a segurança cibernética. Este artigo propõe investigar a detecção de ataques DDoS em redes, utilizando o algoritmo Random Forest. A metodologia inclui a análise do tráfego de rede de uma base de dados, treinamento do algoritmo Random Forest, e avaliação de seu desempenho, incluindo sua velocidade e tempo de execução. Espera-se que os resultados forneçam insights valiosos sobre a eficácia e eficiência do algoritmo Random Forest na detecção de ataques DDoS, contribuindo assim para o fortalecimento da segurança cibernética das redes.

Palavras-chave: Ataques de Negação de Seviço, DoS, DDoS, Aprendizado de Máquinas, Inteligencia Artificial, Random Forest.

*Trabalho de conclusão de curso, Sistemas de Informação, Unidade São Gabriel

[1]Programa de Graduação em Sistema da informação da PUC Minas, Brasil– leonardo.rav@hotmail.com
[2]Instituto de Ciências Exatas e de Informática da PUC Minas, Brasil– felipereis@pucminas.br

Abstract

Distributed Denial of Service Attacks (DDoS) are a persistent and significant threat to cybersecurity. This article proposes to investigate the detection of DDoS attacks in networks, using the Random Forest algorithm. The methodology includes analyzing a database's network traffic, training the Random Forest algorithm, and evaluating its performance, including its speed and execution time. The results are expected to provide valuable insights into the effectiveness and efficiency of the Random Forest algorithm in detecting DDoS attacks, thus contributing to strengthening the cybersecurity of networks.

Keywords: Denial of Service Attacks, DoS, DDoS, Machine Learning, Artificial Intelligence, Random Forest.

1 INTRODUÇÃO

Nos últimos anos, a crescente dependência da sociedade em redes de computadores tem sido acompanhada por um aumento significativo no número e na sofisticação dos ataques cibernéticos. Entre esses ataques, os chamados Ataques Distribuídos de Negação de Serviço (DDoS) emergiram como uma das formas mais prejudiciais de comprometimento da infraestrutura de rede, representando uma séria ameaça à disponibilidade e integridade dos serviços online. Os ataques DDoS se caracterizam pela sobrecarga de tráfego malicioso de um website ou servidor por exemplo, resultando em congestionamento ou inacessibilidade do sistema, negando serviços aos usuários e obstruindo a chegada do tráfego legítimo ao seu destino (DAYAL et al., 2016).

Quando ocorre em larga escala, esse tipo de ameaça pode resultar na desaceleração dos servidores das empresas e de seus respectivos serviços, ocasionando perdas financeiras. Além disso, devido às novas ferramentas e tecnologias empregadas por hackers para realizar ataques DDoS, identificar a fonte ou origem do invasor torna-se desafiador, já que estes chegam de múltiplas fontes. (DALVI et al., 2021)

Detectar e combater ataques DDoS é crucial para manter a segurança das redes e consequentemente, dos usuários. Com a propagação desses ataques, é necessário usar estratégias inovadoras, como algoritmos de machine learning, para obter uma resposta rápida e eficaz. Proteger sistemas e a privacidade dos usuários é essencial para um ambiente online seguro.

A elaboração deste artigo se justifica diante do desafio enfrentado na segurança cibernética. Com a constante evolução das táticas dos agressores e o aumento exponencial na frequência e severidade dos ataques (PERAKOVIĆ et al., 2015), torna-se cada vez mais evidente a necessidade de soluções inovadoras e adaptativas para proteger as infraestruturas de rede. A aplicação de modelos de ML oferece uma abordagem promissora para identificar padrões de tráfego malicioso e distinguir entre atividades legítimas e ataques. Além disso, a capacidade dos algoritmos de ML de aprender com dados históricos e se ajustar a novos padrões de ataque aumenta a eficácia e a agilidade das defesas cibernéticas.

Este trabalho tem como objetivo **desenvolver e avaliar modelos de ML capazes de distinguir entre o tráfego benigno e os ataques DDoS, contribuindo assim para a proteção proativa das redes contra essa forma de ameaça.** Pretende-se analisar como a aplicação de técnicas de ML pode contribuir para a detecção precisa de ataques DDoS, aprimorando a segurança cibernética das redes.

Foram definidos os seguintes objetivos específicos: (i) investigar a eficácia da aplicação de algoritmos de aprendizado de máquina na detecção precisa de ataques DDoS, avaliando sua capacidade de distinguir entre tráfego benigno e malicioso; (ii) treinar o algoritmo Random Forest para análise de tráfego de rede; e, (iii) avaliar o desempenho e a eficiência do algoritmo de ML, considerando métricas como precisão, recall e tempo de execução.

Este trabalho está estruturado em 5 seções, para melhor organização. Na Seção 2, é fornecido o referencial teórico, com explicação de conceitos fundamentais para compreensão do trabalho. A Seção 3, explora trabalhos e sistemas que fundamentaram o desenvolvimento do

projeto. Na Seção 4, descreve-se detalhadamente o método utilizado. Os resultados esperados são apresentados na Seção 5. A Seção 6 contém o cronograma com as atividades previstas para a confecção deste trabalho.

2 REFERENCIAL TEÓRICO

Esta seção pretende apresentar os principais tópicos acerca de segurança cibernética e inteligência artificial.

2.1 Ataques de Negação de Serviço Distribuído (DDoS)

Um Ataque de Negação de Serviço (DoS) ocorre quando um invasor tenta, de forma maliciosa, sobrecarregar um serviço ou recursos de rede usando apenas uma única fonte, tornando-os inacessíveis para usuários legítimos. Por outro lado, quando esse ataque é realizado a partir de múltiplas fontes distribuídas, fica conhecido como Ataque Distribuído de Negação de Serviço (DDoS) (HUSSAIN et al., 2020).

Os ataques DDoS, de acordo com Luo e Han (2019), consiste em enviar uma grande quantidade de pacotes de dados específicos para consumir largura de banda ou recursos do sistema da rede-alvo, levando ao bloqueio ou paralisação da mesma. Este tipo de ataque é realizado por múltiplos nós de origem, em vez de apenas um ou alguns, e é baseado em colaboração distribuída. Os atacantes utilizam centenas de nós controlados para lançar ataques cooperativos em larga escala, degradando ou até mesmo paralisando o desempenho do alvo atacado. Esses ataques são altamente destrutivos, afetam uma ampla gama de usuários legítimos e são difíceis de rastrear e prevenir devido à sua implementação fácil e complexidade de detecção.

2.2 Random Forest

O algoritmo Random Forest é uma técnica de classificação que opera sob supervisão, ou seja, requer dados de treinamento rotulados. Ele consiste em múltiplos pontos de decisão e usa valores aleatórios para criar uma abordagem robusta. Os atributos Gini e Entropia são aplicados dentro do sistema Random Forest para ajudar na tomada de decisões. Este algoritmo é amplamente reconhecido e utilizado no campo de aprendizado de máquina, especialmente em contextos de aprendizado supervisionado. É particularmente útil para lidar com problemas complexos e para melhorar a precisão das previsões. O Random Forest é composto por várias árvores de decisão que empregam um método de votação majoritária para determinar a previsão final, o que geralmente resulta em um desempenho superior (A; DHARMARAJAN, 2022).

2.3 Métricas de Avaliação em Aprendizado de Máquina

Alguns dos critérios mais utilizados para avaliar o desempenho de algoritmos de machine learning incluem a acurácia, que avalia a proporção de classificações corretas feitas pelo modelo, a precisão, que indica a proporção de classificações corretas da classe positiva, e a sensibilidade, que representa a eficácia do modelo em prever a classe positiva. O F1-score, uma medida harmoniosa entre precisão e sensibilidade, é aplicado em conjuntos de dados desbalanceados. A métrica Área Sob a Curva ROC (AUC - *Area Under The Curve*) é utilizada para avaliar a capacidade de classificação do modelo em conjuntos desbalanceados, onde valores próximos a 1 indicam maior precisão. Por fim, a Taxa de Aceitação Falsa (FAR - *False Acceptance Rate*) reflete a taxa de classificações incorretas de conexões normais, sendo valores abaixo de 10% considerados promissores para o modelo (SOUSA; SILVA, 2022).

3 TRABALHOS RELACIONADOS

Dias et al. (2023) apresenta a integração de microsserviços em um ambiente Kubernetes, combinada com técnicas de aprendizado de máquina para otimizar a detecção de ataques DDoS em Redes Definidas por Software (SDN - *Software Defined Networking*). A arquitetura proposta envolve a utilização de modelos de machine learning, como o Random Forest, para analisar o tráfego de rede e identificar padrões maliciosos que indicam a presença de ataques DDoS. Essa abordagem permite a detecção eficaz dos ataques, enquanto a implementação em microsserviços no Kubernetes proporciona melhor isolamento de recursos e desempenho para cada componente do sistema. Dessa forma, a combinação de microsserviços e machine learning contribui para uma detecção mais precisa e eficiente dos ataques DDoS em redes SDN. Os resultados obtidos indicam a eficácia da abordagem e sugerem a continuação de estudos na área de segurança de redes SDN em nuvem, incluindo a implementação de outros modelos de classificação e a comparação com outras abordagens.

Naing e Thwel (2023) investiga a eficácia de diversos algoritmos de aprendizado de máquina na classificação de ataques de negação de serviço distribuídos (DDoS). Conduzido por pesquisadores do Laboratório de Pesquisa em Segurança Cibernética da Universidade de Estudos de Computação em Yangon, Myanmar, a pesquisa aponta que o classificador de Regressão Logística se destaca como o mais eficaz na identificação de ataques DDOS. Utilizando um conjunto de dados abertos de ataques DDoS, os pesquisadores compararam o desempenho de algoritmos como Stochastic Gradient Classifier, Support Vector Machine (SVM), k-Nearest Neighbor (kNN), Naïve Bayes e Regressão Logística. O estudo ressalta a importância de aprimorar métodos de proteção contra ataques DDoS e destaca a necessidade de identificar e classificar esses ataques de forma eficiente para assegurar a integridade e confidencialidade dos sistemas de computadores e redes.

Matsui e Goya (2021) destacam como o DevOps, aplicado no contexto do MLOps,

enfrenta desafios ao integrar processos de machine learning com práticas de integração e entrega contínuas (CI/CD). Eles ressaltam a importância de frameworks e arquiteturas específicas para lidar com esses cenários, visando otimizar a operação e o desenvolvimento de sistemas de aprendizado de máquina em produção. Por sua vez, Gonçalves (2020) concentra-se na aplicação de uma ferramenta de machine learning para prever falhas em equipamentos na indústria de papel, visando evitar paradas não programadas, reduzir custos de manutenção e melhorar a eficiência operacional. Esses estudos contribuem para o entendimento e aplicação de tecnologias avançadas, como o MLOps e a Indústria 4.0, para aprimorar a gestão de ativos e promover a disponibilidade e confiabilidade dos equipamentos industriais.

4 MÉTODO

A parte de análise do algoritmo, neste caso o Random Forest, envolverá algumas etapas. Inicialmente, serão coletados e preparados os dados de tráfego de rede, incluindo amostras de tráfego benigno e de ataques DDoS. Em seguida, o algoritmo Random Forest será implementado e treinado utilizando os dados preparados. Após o treinamento, o modelo será avaliado. Durante a avaliação, serão registradas métricas como precisão, recall, e F1-score. Os experimentos serão conduzidos em um ambiente controlado, replicando condições reais de rede sempre que possível, a fim de garantir a validade e a robustez dos resultados obtidos.

A avaliação do desempenho do algoritmo Random Forest também incluirá testes específicos para mensurar sua velocidade e tempo de execução na detecção de ataques DDoS. Para isso, serão realizados experimentos cronometrados onde o algoritmo será submetido a uma carga de trabalho simulando condições verdadeiras de tráfego de rede. Serão registrados o tempo necessário para que o algoritmo processe e classifique um conjunto específico de dados de tráfego, bem como a velocidade média de processamento.

5 RESULTADOS ESPERADOS

Os resultados esperados com esse estudo são centrados na avaliação do modelo de aprendizado de máquina Random Forest para segurança dos usuários, visando distinguir o tráfego malicioso do benigno. O artigo será uma continuação do Trabalho de Conclusão de Curso feito por Santos (2023), ex-aluno do curso de Sistemas de Informação da PUC Minas, e será focado em analisar o algoritmo proposto acerca de seu desempenho, evidenciando sua precisão, recall e tempo de execução. Espera-se também uma análise mais precisa e eficiente do tráfego de rede, proporcionando uma detecção mais rápida e confiável de ataques DDoS. Espera-se que os resultados obtidos forneçam uma compreensão aprofundada do potencial e das limitações desse algoritmo específico para a detecção de ataques DDoS em cenários reais de rede. Por fim, espera-se que os *insights* obtidos contribuam para aprimorar a eficácia das defesas cibernéticas

contra ameaças DDoS, fornecendo assim uma base sólida para futuras pesquisas e desenvolvimentos no campo da segurança cibernética.

6 CRONOGRAMA

Para desenvolvimento do projeto, foi definido o cronograma disponível na Tabela 1. As atividades foram delineadas considerando as etapas necessárias para a construção do projeto, e as datas de entrega foram estabelecidas conforme os requisitos e cronograma de atividades da disciplina de Trabalho de Conclusão de Curso.

Tabela 1 – Cronograma de atividades previstas.

Atividades	Fevereiro	Março	Abril	Maio	Junho
1. Definição do tema	×				
2. Levantamento bibliográfico		×	×		
3. Análise de algoritmos de ML		×	×		
4. Testes de desempenho			×	×	×
5. Melhorias e correções				×	×
6. Preparação para defesa					×
7. Redação do TCC		×	×	×	×

Referências

A, U. N.; DHARMARAJAN, K. Diabetes prediction using random forest classifier with different wrapper methods. In: *2022 International Conference on Edge Computing and Applications (ICECAA)*. [S.l.: s.n.], 2022. p. 1705–1710.

DALVI, Jai et al. Ddos attack detection using artificial neural network. In: **2021 International Conference on Industrial Electronics Research and Applications (ICIERA)**. [S.l.: s.n.], 2021. p. 1–5.

DAYAL, Neelam et al. Research trends in security and ddos in sdn. **Security and Communication Networks**, v. 9, n. 18, p. 6386–6411, 2016. Disponível em: <https://onlinelibrary.wiley.com/doi/abs/10.1002/sec.1759>.

DIAS, Victor et al. Detecção de ataques ddos em redes sdn utilizando aprendizado de máquina: Uma abordagem em microsserviços. In: **Anais Estendidos do XXIII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais**. Porto Alegre, RS, Brasil: SBC, 2023. p. 141–152. ISSN 0000-0000. Disponível em: <https://sol.sbc.org.br/index.php/sbseg_estendido/article/view/27287>.

GONÇALVES, Pedro Henrique Cantelli. Aplicação de ferramenta de machine learning para predição de falhas em equipamentos em indústria de papel. Universidade Tecnológica Federal do Paraná, 2020.

HUSSAIN, Faisal et al. Iot dos and ddos attack detection using resnet. In: **2020 IEEE 23rd International Multitopic Conference (INMIC)**. [S.l.: s.n.], 2020. p. 1–6.

LUO, Wenliang; HAN, Wenzhi. Ddos defense strategy in software definition networks. In: **2019 International Conference on Computer Network, Electronic and Automation (ICCNEA)**. [S.l.: s.n.], 2019. p. 186–190.

MATSUI, Beatriz; GOYA, Denise. Applying devops to machine learning processes: A systematic mapping. In: **Anais do XVIII Encontro Nacional de Inteligência Artificial e Computacional**. Porto Alegre, RS, Brasil: SBC, 2021. p. 559–570. ISSN 2763-9061. Disponível em: <https://sol.sbc.org.br/index.php/eniac/article/view/18284>.

NAING, Soe Kalayar; THWEL, Tin Thein. A study of ddos attack classification using machine learning classifiers. In: **2023 IEEE Conference on Computer Applications (ICCA)**. [S.l.: s.n.], 2023. p. 108–112.

PERAKOVIĆ, Dragan; PERIŠA, Marko; CVITIĆ, Ivan. Analysis of the iot impact on volume of ddos attacks. **XXXIII Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju–PosTel**, v. 2015, p. 295–304, 2015.

SANTOS, Davi Jorge Leite. **Aplicação do algoritmo Random Forest para classificação de tráfego de rede benigno em meio a ataques DDoS UDP**. 2023. Tese (Trabalho de conclusão de curso) — Pontifícia Universidade Católica de Minas Gerais, PUC Minas São Gabriel, disponível em <http://bib.pucminas.br:8080/pergamumweb/vinculos/0000ba/0000ba97.pdf>.

SOUSA, Welton Thiago Martins; SILVA, Carlos Alexandre. Análise de desempenho em algoritmos de aprendizagem de máquina na detecção de intrusão baseada em fluxo de rede usando o conjunto de dados unsw-nb15. **Revista de Sistemas e Computação-RSC**, v. 12, n. 2, 2022.