International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307 OPEN ACCESS

Available Online at : www.ijsrcseit.com
doi : https://doi.org/10.32628/IJSRCSEIT

Detecting Denial of Service Attacks using Machine Learning

Vivek Nagargoje, Vaibhav Patil, Chandrakant Kokane, Giri Anant, Sandesh Sabale, Sumit Kekan

Department of Information Technology Nutan Maharashtra Institute of Engineering and Technology Pune, India

ARTICLEINFO

Article History:

Accepted: 15 Nov 2023
Published: 30 Nov 2023

Publication Issue
Volume 9, Issue 6
November-December-2023
Page Number
139-143

ABSTRACT

Distributed Denial of Service (DDoS) attacks continue to pose a severe threat to the availability and integrity of online services. This report explores the application of machine learning techniques as a means of enhancing the detection capabilities against these evolving cyber threats. Beginning with an overview of the DDoS landscape, the report delves into the key objectives of utilizing machine learning, including the identification of relevant features, exploration of supervised and unsupervised learning approaches, and examination of challenges such as imbalanced datasets and adaptive attacks. Through a comprehensive literature review and analysis of real-world case studies, this report evaluates the effectiveness of various machine learning models in mitigating DDoS attacks. Furthermore, it discusses challenges related to imbalanced datasets and adaptive attacks, proposing strategies for improvement. The report concludes with insights into future directions for research and development, emphasizing the need for adaptive and real-time detection mechanisms to combat the ever-changing nature of DDoS threats.

Keywords : Machine Learning, Natural Language Processing, Deep Learning

I. INTRODUCTION

In the dynamic landscape of cyberspace, the threat of Distributed Denial of Service (DDoS) attacks looms large, posing formidable challenges to the uninterrupted operation of online services. Characterized by a distributed network of compromised devices flooding a target with traffic, DDoS attacks can lead to service disruptions, financial losses, and compromised user experiences. The increasing frequency and sophistication of these attacks necessitate innovative and adaptive detection mechanisms.

This report addresses the imperative need for robust DDoS detection through the lens of machine learning techniques. As traditional rule-based and signature-based methods struggle to keep pace with the rapidly evolving nature of DDoS attacks, machine learning emerges as a promising avenue for enhancing detection capabilities. By leveraging the power of algorithms to discern patterns and anomalies within network traffic, machine learning holds the potential to provide timely and accurate identification of DDoS threats.

II. LITERATURE SURVEY

Paper 1: "Investigation on Efficient Machine Learning Algorithm for DDoS Attack Detection"
Authors: R. Sahila Devi, R. Bharathi, P. Krishna Kumar
Description: The paper explores the challenges posed by

Distributed Denial of Service (DDoS) attacks in the context of Internet of Things (IoT). DDoS attacks are acknowledged as innovative and complex threats to IoT development due to their inherent difficulty in detection using existing technologies. The study focuses on leveraging Machine Learning (ML) algorithms for effective DDoS traffic detection, utilizing the CICDoS2019 dataset for testing popular ML methods. Additionally, the authors propose a hybrid ML DDoS detection approach incorporating estimator functions. The research emphasizes the need for enhancing the framework for multi-classifying different DDoS attack types in future studies and suggests testing hybrid algorithms with updated DDoS attack datasets.

Paper 2: "A Review on DDoS Attack Detection in SDN using ML."
Authors: Ritu Raj, Sandeep Singh Kang
Description: This paper provides an overview of the security challenges introduced by Software Defined Networking (SDN) and its vulnerability to Distributed Denial of Service (DDoS) attacks. SDN, while offering simplicity in network control, has concurrently increased security risks. The paper focuses on the prevalence of DDoS attacks in SDN environments and conducts a comprehensive review of various machine learning approaches employed for their detection. The authors highlight the significance of identifying and mitigating DDoS threats in SDN to ensure secure network operation. The research contributes to understanding the landscape of ML techniques applied to DDoS detection in the context of SDN architecture.

Paper 3: "NetBIOS DDoS Attacks Detection with Machine Learning Classification Algorithms"
Authors: Srinivas Mekala, Kishore Babu Dasari
Description: Focusing on the detection of Distributed Denial of Service (DDoS) attacks specifically in the context of NetBIOS, this paper addresses the severity of these attacks in making systems or network resources temporarily or permanently unavailable. The study proposes the use of machine learning algorithms for the detection of NetBIOS DDoS attacks, conducting experiments on the NetBIOS_DDoS dataset sourced from the CIC-DDoS2019 evaluation dataset. To optimize computational efficiency, the paper employs correlation methods such as Pearson, Spearman, and Kendall for feature selection. Evaluation of classification algorithms, including Logistic Regression, Decision Tree, Random Forest, Ada Boost, Gradient Boost, K-Nearest Neighbour, Naive-Bayes, and Multilayer Perceptron, reveals that the Multilayer Perceptron with Pearson uncorrelated feature subset exhibits the best performance for NetBIOS DDoS attack detection. The research underscores the importance of early-stage DDoS attack detection for mitigating financial and reputational impacts.

Paper 4: "A Comprehensive Review on Detection of DDoS Attacks using ML in SDN Environment."
Authors: Shaveta Gupta, Dinesh Grover
Description: This comprehensive review paper delves into the transformation brought about by virtualization, particularly focusing on Software Defined Networking (SDN). SDN, while providing a straightforward network control method, introduces new security challenges, with Distributed Denial of Service (DDoS) attacks being a prevalent threat. The paper compares various machine learning techniques employed for detecting DDoS attacks within the SDN environment. It emphasizes the need for robust detection mechanisms to secure servers, considering the ease with which DDoS attacks can be initiated by impacting the server, leading to network-wide failures. By offering an overview of existing machine learning methodologies, the paper contributes to the understanding of strategies for mitigating DDoS threats in SDN environments.

Paper 5: "ML based D3 R: Detecting DDoS using Random Forest."

Authors: Anagha Ramesh, Ramza Haris, Sumedha Arora Description: Addressing the significant security risk

posed by Distributed Denial of Service (DDoS) attacks to cloud servers and websites, this study introduces the application of the Random Forest algorithm for DDoS detection. By collecting network traffic data as input, the paper analyzes the performance of Random Forest in detecting and preventing DDoS attacks. The results demonstrate the effectiveness of Random Forest in enhancing cloud security and minimizing the damage caused by DDoS attacks. The research contributes insights into the application of specific machine learning algorithms, such as Random Forest, for real-time detection and prevention of DDoS attacks in cloud environments

Paper 6: "Evaluation and Analysis: Internet of Things using Machine Learning Algorithms for Detection of DDoS Attacks."

Authors: Anshika Sharma, Himanshi Babbar

Description: The paper addresses the increasing security threats faced by Internet of Things (IoT) systems, with a particular focus on the prevalence of Distributed Denial of Service (DDoS) attacks. Recognizing the challenges in predicting and detecting these attacks, the study conducts an analysis of various existing machine learning (ML) algorithms used for predicting and detecting DDoS attacks. Utilizing datasets such as ToN-IoT, CICDDoS2019, and BoT-IoT, the paper deploys four different ML algorithms: K-Nearest Neighbour (KNN), Naive Bayes (NB), Decision Tree (DT), and Random Forest (RF). The evaluation identifies the decision tree and random forest classifiers as providing the highest levels of accuracy. The research aims to discuss security concerns associated with DDoS attacks and proposes ML-based solutions for their mitigation in IoT systems.

Paper 7: "DDoS Attack Detection and Analytics" Authors: B. Geluvaraj, Santhosh Krishna B V'M. Umesh, Vishnu Girish G, Yasir Yaqoob

Description: This paper explores Distributed Denial of Service (DDoS) attacks, emphasizing their use to overwhelm a target system or website with excessive traffic, rendering it unavailable to legitimate users. DDoS attacks are identified as potential tools for extortion, political purposes, and compromising systems through denial of service. The study conducts experiments on a local test server using the Tor Hammer tool for simulating DDoS attacks, generating new datasets stored in CSV format. To identify network behavior, the paper employs classification algorithms, including SVM, DT, KNN, and Logistic Regression. The research contributes to the understanding of network behavior during DDoS attacks and explores the application of machine learning for their detection and analytics.

Paper 8: "An Empirical Study of Intelligent Approaches to DDoS Detection in Large Scale Networks"

Authors: Xiaoyu Liang, Taieb Znati

Description: This paper presents an empirical evaluation of Machine Learning (ML)-based Distributed Denial of Service (DDoS) detection techniques, addressing the persistent challenges posed by these attacks on the Internet. The study focuses on understanding the performance of a class of ML-based techniques under different attack scenarios, utilizing various performance metrics. The paper highlights the impact of the "Class Imbalance Problem" on ML-based DDoS detection and suggests the need for method-oriented feature selection models to enhance the capabilities of ML-based detection techniques. The results underscore the complexity of DDoS detection, with no single technique outperforming all others in all test cases. Additionally, the research emphasizes the importance of addressing the class imbalance problem to improve ML- based DDoS detection capabilities.

Paper 9: "AI-based DDoS Attack Detection of SDN Network in Mininet Emulator"

Authors: Aditya Raj Yadav, Anant P Jain, Shankar T, A. Rajesh, Sivasankar Perumal, Geoffrey Eappen

Description: This paper focuses on the security challenges posed by Distributed Denial of Service (DDoS) attacks in Software Defined Networking (SDN) environments. Using the Mininet SDN emulator and controllers, the authors aim to study Artificial Intelligence (AI)-based DDoS attacks on SDN networks and explore potential solutions using Machine Learning (ML). The Mininet emulator, along with the Pox controller based on Transmission Control Protocol (TCP), Iperf3, and Hping3, is utilized for testing scenarios, evaluating the emulator and controller's performance by monitoring throughput. The paper explores the concept of entropy to create ML classifiers for interpreting DDoS attacks based on changes in network entropy. The study contributes to understanding the application of AI and ML in detecting and preventing DDoS attacks in SDN environments using emulators for experimental analysis.

Paper 10: "Securing IoT Against DDoS Attacks Using Machine Learning"

Authors: M. A. Mahmood, A. M. Zeki

Description: With the expansion of the Internet of Things (IoT), cyber-attacks on IoT systems have become a significant concern for security, privacy, and availability. One of the common threats faced by IoT systems is the Denial of Service (DOS)/Distributed Denial of Service (DDoS) attacks, impacting the availability of IoT services. This paper aims to provide a review of Machine Learning (ML) models proposed by researchers for detecting DOS/DDOS attacks in IoT systems. The review focuses on the deployment methodology of ML models, detection methodologies, datasets used for training and testing, and overall performance. By summarizing existing research, the paper contributes to understanding the landscape of ML- based approaches for securing IoT against DDoS attacks.

III. EXISTING SYSTEM

Arbor Networks: Arbor Networks offers solutions for DDoS detection and mitigation, including the Arbor Cloud service. They use a combination of anomaly detection and behavioral analysis to identify and mitigate DDoS attacks.

Radware: Radware provides DDoS protection solutions that leverage machine learning algorithms to detect and mitigate various types of DDoS attacks. They focus on behavior-based detection and real-time threat intelligence.

Akamai Kona Site Defender: Akamai's Kona Site Defender is a web application firewall (WAF) that includes DDoS protection capabilities. It uses machine learning algorithms to analyze traffic patterns and identify anomalies indicative of DDoS attacks.

Cloudflare: Cloudflare offers DDoS protection services that include machine learning-based threat detection. They use a global network and behavioral analysis to identify and mitigate DDoS attacks in real-time.

Imperva Incapsula: Imperva Incapsula provides a cloud- based application delivery service with DDoS protection features. They use machine learning to analyze traffic patterns and identify malicious behavior.

Radware DefensePro: Radware's DefensePro is a DDoS protection solution that combines signature-based detection with behavioral analysis and machine learning algorithms to identify and mitigate DDoS attacks.

F5 Silverline DDoS Protection: F5's Silverline DDoS Protection is a cloud-based service that uses machine learning and real-time analytics to detect and mitigate DDoS attacks. It offers a combination of behavioral analysis and signature-based detection.

IV. REFERENCES

[1]. [Srinivas Mekala and Kishore Babu Dasari, "NetBIOS DDoS Detection With ML," InCACCT 2023.

[2]. Shaveta Gupta and Dinesh Grover, "DDoS Detection in SDN: A Comprehensive Review," ICAIS 2021.

[3]. Anagha Ramesh et al., "ML-based D3 R: Detecting DDoS using Random Forest," CCGridW 2023.

[4]. Anshika Sharma and Himanshi Babbar, "IoT DDoS Detection with ML Algorithms," IITCEE 2023.

[5]. B. Geluvaraj et al., "DDoS Attack Detection and Analytics," ICONAT 2023.

[6]. Xiaoyu Liang and Taieb Znati, "Empirical Study of Intelligent DDoS Detection," ICNC 2019.

[7]. Aditya Raj Yadav et al., "AI-based DDoS Detection in SDN," ViTECoN 2023.

[8]. [8] M. A. Mahmood and A. M. Zeki, "Securing IoT Against DDoS with ML," SCS 2020.

[9]. Kokane, Chandrakant D., and Sachin D. Babar. "Supervised word sense disambiguation with recurrent neural network model." Int. J. Eng. Adv. Technol.(IJEAT) 9.2 (2019).

[10]. Kokane, Chandrakant D., Sachin D. Babar, and Parikshit N. Mahalle. "Word Sense Disambiguation for Large Documents Using Neural Network Model." 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT). IEEE, 2021.

[11]. Kokane, Chandrakant, et al. "Word Sense Disambiguation: A Supervised Semantic Similarity based Complex Network Approach." International Journal of Intelligent Systems and Applications in Engineering 10.1s (2022): 90-94.

[12]. Kokane, Chandrakant D., et al. "Machine Learning Approach for Intelligent Transport System in IOV-Based Vehicular Network Traffic for Smart Cities." International Journal of Intelligent Systems and Applications in Engineering 11.11s (2023): 06-16.

[13]. Kokane, Chandrakant D., et al. "Word Sense Disambiguation: Adaptive Word Embedding with Adaptive-Lexical Resource." International Conference on Data Analytics and Insights. Singapore: Springer Nature Singapore, 2023.

Cite this article as :

Vivek Nagargoje, Vaibhav Patil, Chandrakant Kokane, Giri Anant, Sandesh Sabale, Sumit Kekan, "Detecting Denial of Service Attacks using Machine Learning", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 6, pp.139-143, November-December-2023.