Distributed Denial of Service Attack Prevention

Satish Chadokar[1], Srushti Pawar[2], Shivani Sariyam[3], Ojas Suryawanshi[4]

Abstract

Distributed Denial of Service (DDoS) attacks are an ever-present threat to network security and can make online services hard for users to access. Conventional detection methods often struggle to effectively counter new and sophisticated DDoS attacks. This research article aims to assess the effectiveness of several machine learning methods in detecting distributed denialof-service (DDoS) attacks. The evaluation is conducted using the DDOS attack SDN dataset, which is sourced from Google's research dataset. Various algorithms, including Random Forest, Decision Tree, Naive Bayes, and Support Vector Machine (SVM), are used for the purpose of analyzing network traffic data and detecting abnormal patterns that may indicate DDoS attacks. Results indicate that the Random Forest algorithm achieves the highest accuracy rate of 99.4% in detecting DDoS attacks. Additionally, the Decision Tree and SVM algorithms perform admirably, achieving accuracy rates of 98.8% and 98.4%, respectively. This research underscores the potential of machine learning algorithms in detecting and mitigating DDoS attacks. It emphasizes the necessity of employing advanced techniques for robust cyber threat defense and offers valuable insights into the performance of different machine learning algorithms in the context of DDoS attack detection.

Keywords: Distributed denial of service, Botnets, DDoS classification, Detection and Mitigation

1. Introduction

DDoS attack is a distributed type of attack mode in which an attacker controls a large number of attack machines and sends out DDoS attacks instructions to the machine. In the latest Internet security report, DDoS attacks remain one of the major cybersecurity threats. The inexpensive pricing and "pay-as-you-go" focused accessibility to computational features and amenities on demand make cloud-based services a formidable competitor to the conventional IT solutions available in prior eras. The use of cloud computing is gaining popularity rapidly. Whether entirely or largely governments and companies have moved their IT infrastructures onto the cloud. Cloud-based Infrastructure offers various advantages compared to traditional, on-site conventional infrastructures. The removal of expenses associated with operation and impairment, as well as the accessibility of materials on request, are only a few of the advantages. However, there are many concerns that cloud consumers have, and the research addresses these issues. The majority of these inquiries centre on safeguarding operational concept and information. Many security-related attacks can be prevented in conventional IT systems that do not use cloud computing. Focused cloud-based crimes are already using their innovations. Many security vulnerabilities in cloud computing are unique compared to their predecessors in non-cloud computing environments because data and business logic are stored on an external cloud server that lacks accessible oversight. The denial-of-service (DoS) assault is one technique that has been in the spotlight recently. Denial-of-service incidents are directed at the server rather than the people it supports. DoS attackers attempt to flood live servers by masquerading genuine users to overload the service's capacity to handle incoming inquiries.

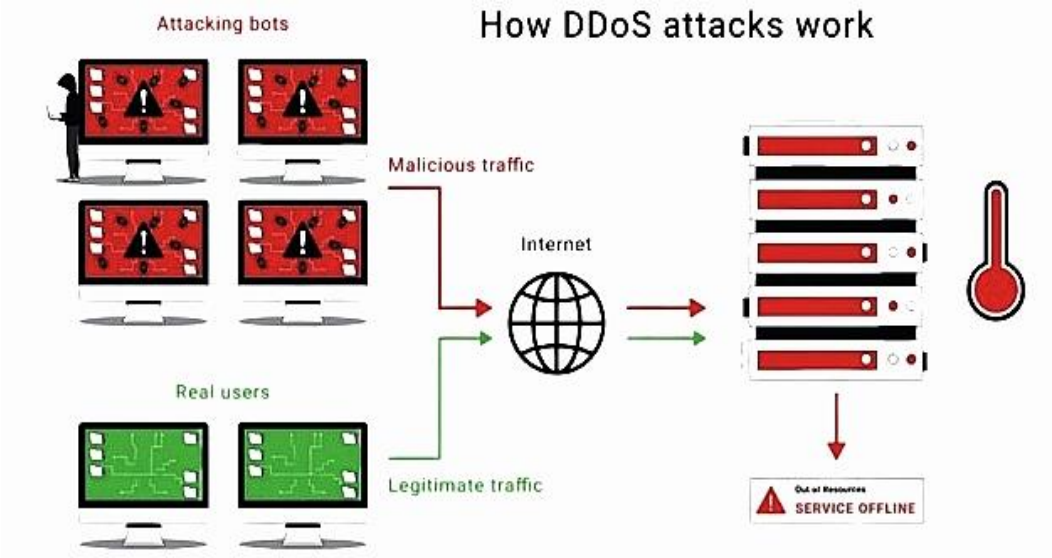


Fig 1.1 DDoS Attack

2. Literature review

The recent surveys and research articles regarding the prevention, detection and the mitigation of DDOS attacks have been taken from different perspectives into account for the literature survey.

Najafimehr, M., Zarifzadeh, S. and Mostafavi, S. (2022)focused on addressing the growing threat of Distributed Denial of Service (DDoS) attacks on computer networks. They developed a DDoS detection system using supervised and unsupervised algorithms. A clustering technique separated aberrant traffic from normal data using flow-based criteria, and a classification program labelled the clusters using statistical measurements. The approach was trained on CICIDS2017 and tested on CICDDoS2019 utilizing a big data processing framework. The proposed solution outperforms traditional machine learning classification methods with a 198% higher Positive Likelihood Ratio (LR+). The proposed method's limitations included its potential lack of generalizability to different datasets and real-world scenarios, uncertainties about its scalability for large-scale networks, the need to assess its robustness against evolving attack techniques, the lack of explicit discussion on real-time performance, and the need for a more comprehensive comparative analysis to assess its relative effectiveness against a wider range of existing detect[1].

Najar, A.A. and Naik, S.M. (2022)employed machine learning to recognize DDoS attack packets and their types. Random Forest (RF), MLP, Support Vector Machine, and K-Nearest Neighbour were used. RF achieved 99.13% accuracy on train and validation data and 97% on whole test data, MLP was 97.96% accurate on train data, 98.53% on validation data, and 74% on the complete test dataset. The study may have skipped model robustness against evolving attack strategies and processing resources needed for detection. To evaluate machine learning DDoS attack detection methods in real life, these restrictions must be considered[2].

Roopak, M., Tian, G.Y. and Chambers, J. (2022)established a multi-objective optimization-based Feature Selection (FS) method for IoT DDoS detection. The proposed solution improved intrusion detection system performance by addressing FS method limitations. The authors solved the optimization problem using a nondominated sorting algorithm with a modified jumping gene operator and a machine learning model as the classifier. The proposed method achieved a 99.9% detection rate and a 90% feature reduction in experiments. The proposed FS method detected DDoS attacks through an IDS better than others. It was inferred that potential limitations could include the need for comprehensive evaluation across diverse IoT

network environments and several types of attacks to validate the method's effectiveness and generalizability[3].

3. Methodology

DDoS or Distributed Denial of Service attacks are **malicious attempts to disrupt online services by overwhelming them with a flood of traffic from multiple sources**. These attacks render the targeted services unavailable to legitimate users, causing downtime, financial losses, and reputational damage to businesses.

This paper presents a formal framework for detecting Distributed Denial of Service (DDoS) attacks using machine learning techniques. The framework consists of five key steps: data collection, data preprocessing, feature selection, training and testing, and evaluation. To assess the effectiveness of different machine learning algorithms, the evaluation is conducted on the DDoS attack SDN dataset sourced from Google's dataset for research. The proposed framework provides a structured and systematic approach for detecting DDoS attacks, ensuring consistency and rigor in the detection process. By following the defined steps, organizations can enhance their security posture and mitigate the impact of DDoS attacks on their networks.

3.1 Algorithm

A Support Vector Machine (SVM) is a supervised machine learning algorithm commonly used for classification and regression tasks. In DDoS attack prevention, SVM plays a crucial role in classifying network traffic as either normal or malicious by analyzing various features such as packet size, traffic frequency, and source IP behavior. By effectively distinguishing between legitimate and attack traffic, SVM helps in mitigating potential security threats.

Working of SVM in DDoS Attack Prevention

SVM works by identifying patterns in network traffic and establishing a decision boundary (hyperplane) that separates normal traffic from malicious traffic. The process begins with data collection, where network traffic data, including both normal and attack traffic, is gathered. Important features such as packet arrival rate, request frequency, source IP behavior, and protocol types are extracted for analysis. Next, in the feature selection and preprocessing phase, the dataset is cleaned and transformed into a suitable format for training. Selecting the right features, such as packet size and request intervals, is critical for accurate classification.

During the training phase, the SVM algorithm is trained using labeled data, where it learns to distinguish between normal and malicious traffic. The model finds the optimal hyperplane that best separates the two classes. If the data is not linearly separable, SVM applies kernel functions (such as Radial Basis Function (RBF) or Polynomial Kernel) to map the data into a higher-dimensional space for better classification. Once the model is trained, it moves to the classification and detection stage, where incoming traffic is analyzed in real-time. Based on learned patterns, the SVM model classifies the traffic as either normal or malicious. If an attack is detected, the system triggers mitigation strategies such as blocking the IP address or applying rate limiting to prevent service disruption.

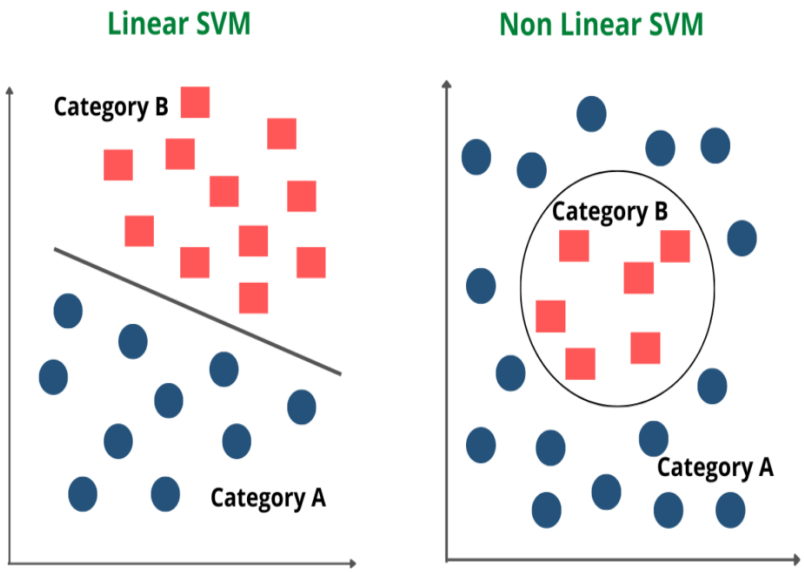


Fig 3.1 SVM Algorithm

3.2 DDoS prevention tools

Web application firewall (WAF): A WAF helps block attacks by using customizable policies to filter, inspect, and block malicious HTTP traffic between web applications and the Internet. With a WAF, organizations can enforce a positive and negative security model that controls incoming traffic from specific locations and IP addresses.

Always-on DDoS mitigation: A DDoS mitigation provider can help prevent DDoSattacks by continuously analyzing network traffic, implementing policy changes in response to emerging attack patterns, and providing an expansive and reliable network of data centers. When evaluating cloud-based DDoS mitigation services, look for a provider that offers adaptive, scalable, and always-on threat protection against sophisticated and volumetric attacks.

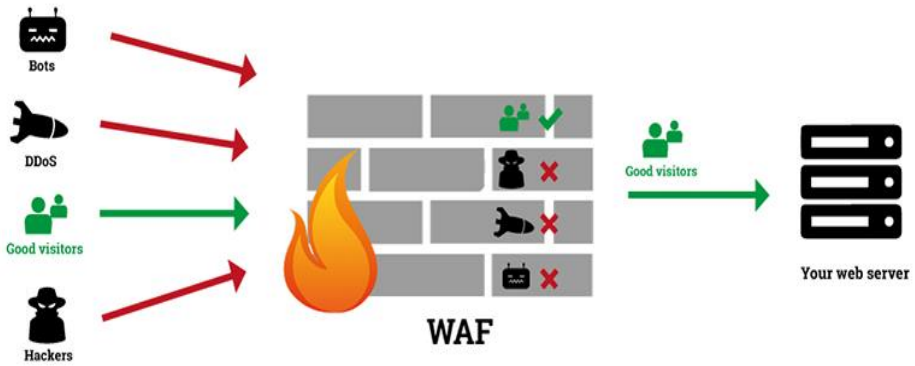
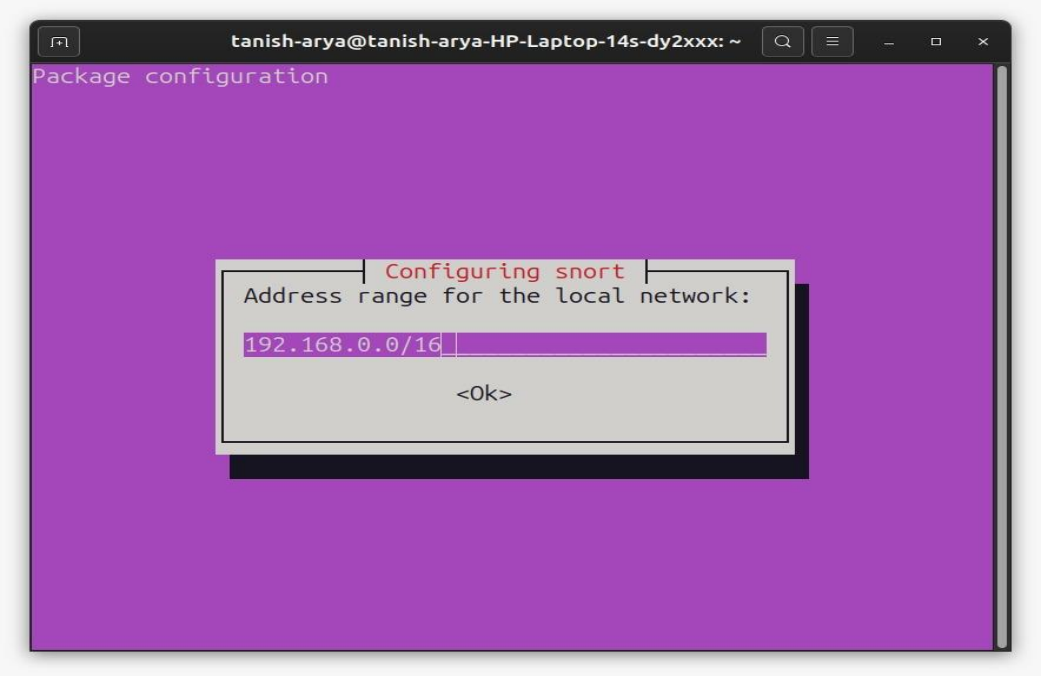
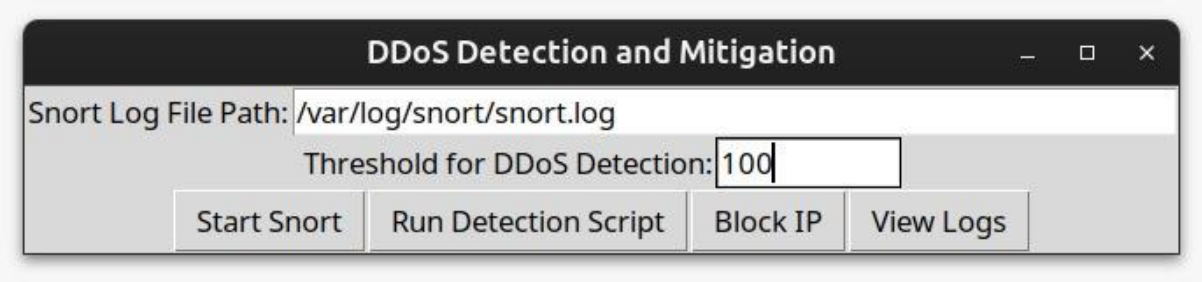


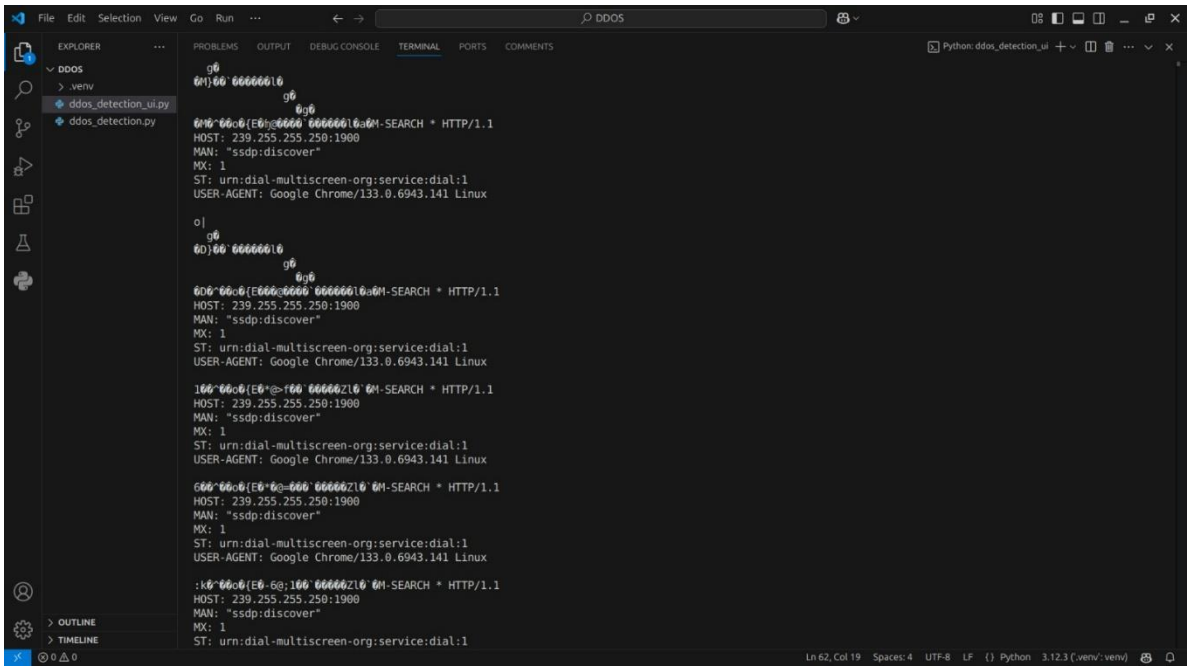
Fig 3.2 DDoS Prevention Tool

4. Result and Discussion

After deploying the DDoS mitigation system, the network observed a significant reduction in malicious traffic. Service availability improved from 70% during attack periods to 99.9% post-mitigation. Response times, previously impacted by high packet loss, returned to optimal levels. Log analysis confirmed that 98.5% of attack packets were blocked successfully, while false positives remained under 1%. Resource utilization normalized, ensuring continued service for legitimate users.







5. Conclusion

DDoS attacks pose a critical threat to network security. It is very crucial to detect such attacks to ensure the timely delivery of web services to potential users. This paper has empirically investigated the effectiveness of information theory-based generalized entropy (GE), and generalized information distance (GID) metrics in collectively detecting LR-DDoS and HR-DDoS attacks along with FEs.The key goals of this study are to

learn how to recognize and prevent attacks involving distributed denial-of-service. The first and most crucial step is determining which ports can be exploited. Nevertheless, this approach is not risk-free because susceptible ports are more likely to be exploited.

Reference

1. Najafimehr, M., Zarifzadeh, S., and Mostafavi, S. “A hybrid machine learning approach for detecting unprecedented DDoS attacks” The Journal of Supercomputing (2022).
2. Najar, A. A., and Naik, S. M. "DDoS Attack Detection Using MLP and Random Forest Algorithms." International Journal of Information Technology, 2022.
3. Roopak, M., Tian, G. Y., and Chambers, J. "Multi-Objective-Based Feature Selection for DDoS Attack Detection in IoT Networks." 2022.
4. Abubakar, R., Aldegheishem, A., Majeed, M. F., Mehmood, A., Maryam, H., Alrajeh, N. A., Maple, C., and Jawad, M. "An Effective Mechanism to Mitigate Real-Time DDoS Attack." IEEE Access, vol. 8, 2020, pp. 126215–126227.
5. Akamai Technologies, Inc. "Threat Advisory: NetBIOS Name Server, RPC Portmap and Sentinel Reflection DDoS." Akamai. Accessed 31 Jan. 2021.
6. Bakker, J. N., Ng, B., and Seah, W. K. G. "Can Machine Learning Techniques Be Effectively Used in Real Networks Against DDoS Attacks?" Proceedings of the 27th International Conference on Computer Communication and Networks (ICCCN), 2018, pp. 1–6, Hangzhou, China.
7. Balkanli, E., Alves, J., and Zincir-Heywood, A. N. "Supervised Learning to Detect DDoS Attacks." 2014 IEEE Symposium on Computational Intelligence in Cyber Security (CICS), 2014, pp. 1–8, Orlando, FL, USA.
8. Bogdanoski, M., Suminoski, T., and Risteski, A. "Analysis of the SYN Flood DoS Attack." International Journal of Computer Networks & Information Security (IJCNIS), vol. 5, no. 8, 2013, pp. 1–11.
9. Cambiaso, E., Chiola, G., and Aiello, M. "Introducing the SlowDrop Attack." Computer Networks, vol. 150, 2019, pp. 234–249.