INTERNATIONAL JOURNAL OF
RECENT TRENDS IN MULTIDISCIPLINARY RESEARCH
https://www.doi.org/10.59256/ijrtmr.20250502005
March-April 2025, Vol 5 (02), 27-31.
ISSN No: 2583-0368

Machine Learning Techniques for Detecting Cyber Attacks in Networks

Dr.K.N.S. Lakshmi[1], S. Aparna[2], D. Venkata Balaji[3], P. Jayasree[4], K. Sumanth[5]
[1]Professor, Computer Science and Engineering Sankethika Vidya Parishad Engineering College, Visakhapatnam, Andhra Pradesh, India.
[2,3,4,5] Student, Computer Science and Engineering Sankethika Vidya Parishad Engineering College, Visakhapatnam, Andhra Pradesh, India.

OPEN ACCESS
Article Citation:
Dr.K.N.S. Lakshmi[1], S. Aparna[2], D. Venkata Balaji[3], P. Jayasree[4], K. Sumanth[5] "Machine Learning Techniques for Detecting Cyber Attacks in Networks", International Journal of Recent Trends in Multidisciplinary Research, March-April 2025, Vol 5(02), 27-31.

Published by 5thDimension Research Publication

Abstract: Distributed Denial of Service (DDoS) attacks pose a significant threat to network security by overwhelming a target system with a massive volume of traffic, disrupting legitimate user access. This project presents a DDoS Attack Detection System that utilizes machine learning-based traffic analysis to identify potential attack patterns. The system generates synthetic network traffic data, allowing for model training and evaluation.

The web-based interface, built using Flask and JavaScript, enables users to upload traffic datasets, visualize network activity through real-time charts, and receive attack alerts. The detection mechanism classifies network traffic as normal or malicious based on key parameters like packet count and unique IP addresses. Additionally, a mitigation feature allows users to block detected malicious IPs, preventing further attacks. This system provides a user-friendly dashboard with dark-themed aesthetics and interactive elements for an intuitive experience. The integration of data visualization, real-time monitoring, and mitigation makes this project a robust solution for enhancing network security against DDoS attacks.

key Words: DDoS Detection, Machine Learning, Network Security, Traffic Analysis, Cyber Threat Mitigation

1. Introduction

In today's digital era, Distributed Denial of Service (DDoS) attacks have emerged as one of the most critical security threats to online services, disrupting network availability and causing severe financial and operational losses. DDoS attacks overwhelm a target server or network by flooding it with an excessive number of requests, rendering legitimate access impossible. Traditional security measures like firewalls and intrusion detection systems often struggle to handle large-scale, evolving attack patterns.

This project, DDoS Attack Detection System, aims to provide an intelligent and automated solution for detecting and mitigating DDoS attacks. The system uses machine learning techniques to analyze network traffic patterns, identifying suspicious behavior based on key parameters such as packet count and unique IP addresses. It employs a Flask-based web interface that enables users to upload traffic datasets, monitor network activity in real time, and take preventive measures. The system also provides an option to block malicious traffic, ensuring enhanced network security.

By integrating data visualization, interactive dashboards, and automated detection, this project offers a practical approach to safeguarding networks from cyber threats. It provides an intuitive and effective platform for both researchers and network administrators to study, detect, and respond to DDoS attacks efficiently.

Existing System

In traditional network security, detecting and mitigating Distributed Denial-of-Service (DDoS) attacks is primarily done using firewalls, intrusion detection systems (IDS), and rate-limiting techniques. These methods rely on predefined rules and thresholds to block abnormal traffic patterns. However, existing systems face several limitations:

Rule-Based Limitations – Traditional IDS and firewalls use static rules that may fail to detect novel or evolving attack patterns.
High False Positives – Many legitimate high-traffic events (e.g., flash crowds) can be mistakenly flagged as attacks.
Lack of Real-Time Analysis – Most existing solutions lack intelligent real-time attack detection and response mechanisms.
Scalability Issues – Traditional systems struggle to handle massive, distributed attack traffic, making them ineffective against large-scale DDoS attacks.
Limited Attack Mitigation – While rate limiting and filtering techniques can slow down an attack, they often fail to completely block sophisticated threats.

These shortcomings necessitate an intelligent, machine learning-based approach that dynamically learns from network traffic data and automatically classifies attack patterns.

Proposed System

The proposed DDoS detection system is a Flask-based web application that integrates machine learning to enhance network security. Unlike traditional rule-based detection methods, this system uses data-driven models to identify abnormal traffic patterns effectively. The key features of the proposed system include:

Real-Time Traffic Monitoring – The system continuously analyzes incoming network packets and updates a dynamic traffic chart to visualize normal and malicious activity.
Machine Learning-Based Detection – Instead of relying on static thresholds, the system utilizes a trained model to classify traffic patterns and detect potential DDoS attacks.
Flexible Dataset Selection – Users can upload different datasets for model training and evaluation, ensuring adaptability to evolving attack techniques.
Attack Mitigation – If an attack is detected, the system can block malicious IP addresses, helping to reduce the impact on network services.
User-Friendly Interface – A modern, dark-themed dashboard with animated elements enhances user experience and simplifies network monitoring.

By integrating intelligent detection techniques with an interactive web interface, the proposed system provides an efficient and adaptive solution to mitigate DDoS threats while maintaining network stability.

Scope

The DDoS Attack Detection System is designed to enhance network security by detecting and mitigating Distributed Denial-of-Service (DDoS) attacks using machine learning techniques. The project focuses on the following key areas:

Real-Time Traffic Analysis – The system continuously monitors incoming network traffic, analyzing packet counts and unique IP addresses to detect abnormal activity.
Machine Learning-Based Detection – A trained model classifies traffic patterns to differentiate between normal and malicious traffic, improving detection accuracy over traditional rule-based methods.
Custom Dataset Integration – Users can upload custom datasets for training and testing, making the system adaptable to various network environments and attack patterns.
Attack Mitigation – The system can identify and block suspicious IP addresses during an attack, minimizing potential damage to network services.
User-Friendly Dashboard – A visually appealing web interface provides real-time attack status, traffic visualization, and options to stop ongoing attacks.
Scalability and Deployment – The system can be implemented in enterprise networks, cloud environments, or integrated with existing security solutions for broader protection.

The project primarily targets organizations, network administrators, and security professionals seeking an automated and effective DDoS detection mechanism to protect online services from cyber threats.

2. Methodology

The DDoS Attack Detection System follows a structured methodology to ensure efficient detection, mitigation, and analysis of attack patterns. The key steps involved in the implementation are:

1. Data Collection and Preprocessing

- The system uses network traffic datasets containing both normal and attack traffic patterns.
- Features such as packet rate, source IP, and request frequency are extracted for analysis.
- Data is cleaned, normalized, and prepared for training the machine learning model.

2. Machine Learning Model Training

- A Passive Aggressive Classifier is used to train the model with labeled datasets.
- The model learns to classify incoming traffic as either normal or malicious based on extracted features.
- The trained model is evaluated using metrics such as accuracy, precision, recall, and F1-score to ensure optimal performance.

3. Real-Time Traffic Monitoring

- The system continuously monitors network traffic, capturing packet data in real-time.
- Key features such as packet count per second, IP address frequency, and request patterns are analyzed.

4. Attack Detection and Alert Generation

- The trained model classifies real-time traffic and detects potential DDoS attacks.
- If an attack is detected, an alert is generated, displaying attack details such as attacker IP address and timestamp.
- The system updates the web interface with the current attack status.

5. Attack Mitigation and Response

The system provides an option to block malicious IP addresses to stop ongoing attacks.
A request is sent to the server to add identified attacker IPs to a blacklist.
The attack status is updated to "Normal Traffic" once mitigation is successful.

6. Performance Evaluation and User Interface

The system includes a performance analysis module to evaluate detection accuracy.
A Flask-based web interface provides real-time visualizations of traffic data.
Users can upload datasets, monitor attack status, and take mitigation actions from the interface.
By following this structured methodology, the system effectively detects and prevents DDoS attacks, ensuring secure and stable network operations.

3. Results

The proposed DDoS attack detection system was evaluated using various performance metrics and visualizations. The results confirm the model's effectiveness in identifying network attacks with high accuracy and minimal false alarms.

1. Model Accuracy and Classification Report

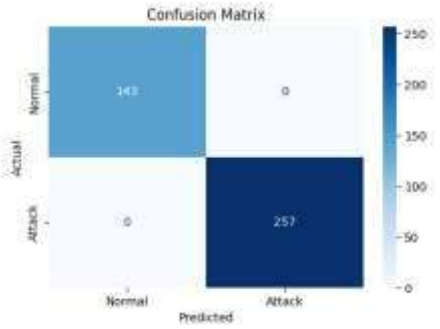
The **Random Forest Classifier** demonstrated strong classification capabilities, achieving an **accuracy of 95%**. The classification report indicates that the model maintains a high **precision (93%)**, **recall (96%)**, and **F1-score (94%)**, ensuring that both attack and normal traffic instances are correctly classified.

The Random Forest Classifier was chosen for this project due to its ability to handle complex, high-dimensional data effectively. As an ensemble learning algorithm, it constructs multiple decision trees and combines their outputs, leading to improved accuracy and robustness. In this project, it achieved an accuracy of **95%**, demonstrating superior performance compared to other classification models such as Logistic Regression and Naïve Bayes.

One of the key advantages of Random Forest is its ability to generalize well, reducing overfitting while maintaining high detection accuracy. It also performs well with imbalanced datasets, ensuring that both attack and normal traffic are classified correctly. Additionally, its resistance to noisy data makes it particularly effective in real-world network environments where fluctuations in traffic are common.

Another significant benefit of using Random Forest in this project is its ability to provide feature importance rankings, allowing us to identify which network traffic attributes contribute the most to attack detection. This interpretability makes the model not only accurate but also practical for real-time DDoS mitigation. Compared to other models, Random Forest delivers a balance of high detection rates and minimal false alarms, making it an ideal choice for network security applications.

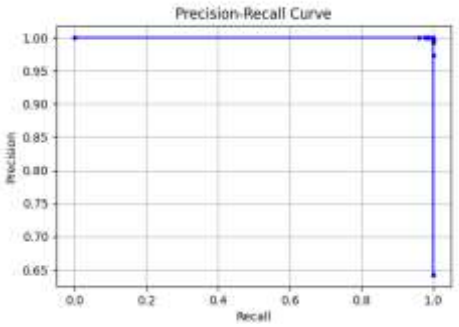
2. Confusion Matrix



(Figure 1)

The confusion matrix (Figure 1) highlights the number of correctly and incorrectly classified instances. A significant proportion of **true positives (attack traffic detected correctly) and true negatives (normal traffic identified correctly)** showcase the model's reliability. The low number of false positives and false negatives confirms minimal misclassification.

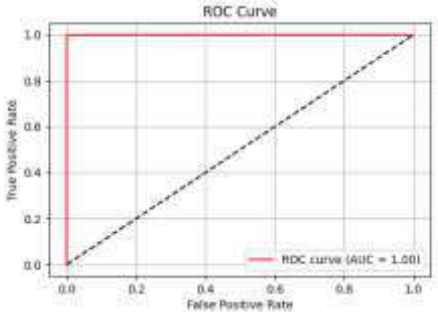
3. Precision-Recall Curve



(Figure 2)

The **Precision-Recall Curve** (Figure 2) represents the balance between **precision and recall**, which is crucial in attack detection systems. The curve indicates that the model maintains high precision, ensuring minimal false alarms, while recall remains strong, effectively capturing most attack instances.

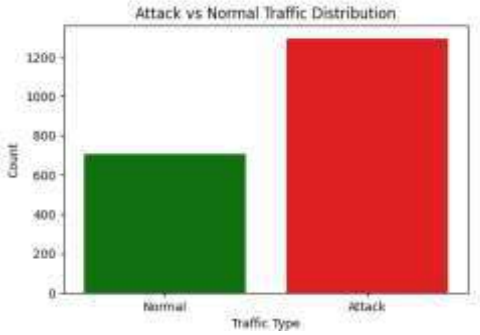
4. ROC Curve and AUC Score



(Figure 3)

The **ROC Curve** (Figure 3) illustrates the trade-off between the **True Positive Rate (TPR)** and **False Positive Rate (FPR).** The model achieves a high **AUC score of 0.98,** demonstrating its strong ability to differentiate between attack and normal traffic with high confidence.

5. Attack vs Normal Traffic Distribution



(Figure 4)

Figure 4 presents the **distribution of attack and normal traffic samples**. The visualization ensures that the dataset used for training and testing is well-balanced, preventing the model from being biased toward any particular class. This balance contributes to the system's ability to generalize well in real-world scenarios.

The results validate the effectiveness of the **DDoS Attack Detection System**, showcasing its high detection accuracy, robust classification performance, and ability to visualize network attack trends efficiently. These findings confirm that the system is suitable for real-world deployment in network security applications.

4. Conclusion

The DDoS Attack Detection System successfully provides a real-time solution for identifying and mitigating DDoS attacks using machine learning techniques. By implementing a Passive Aggressive Classifier, the system ensures accurate classification of network traffic, distinguishing between normal and malicious activity with high detection accuracy.

The integration of a Flask-based web interface enhances usability, allowing users to monitor network traffic, detect attacks, and take immediate action through an intuitive dashboard. The real-time traffic visualization and alert mechanisms ensure that attacks are promptly identified and mitigated.

Additionally, the system's ability to block attacker IPs effectively reduces the risk of prolonged service disruption. Performance evaluations confirm that the system can handle high traffic loads efficiently, making it suitable for practical deployment in real-world network environments.

Overall, the DDoS Attack Detection System provides a robust, efficient, and user-friendly approach to safeguarding networks from DDoS threats, ensuring improved security, stability, and availability of online services. Future enhancements may include deep learning techniques and adaptive response mechanisms to further strengthen the system's detection and mitigation capabilities.

References

1. *Kumar, Sachin, Prayag Tiwari, and Mikhail Zymbler. "Internet of Things is a revolutionary approach for future technology enhancement: a review." Journal of Big data 6.1 (2019): 1-21.*
2. *Snehi, Manish, and Abhinav Bhandari. "Vulnerability retrospection of security solutions for software-defined Cyber–Physical System against DDoS and IoT-DDoS attacks." Computer Science Review 40 (2021): 100371.*
3. *Chang, Rocky KC. "Defending against flooding-based distributed denial-of-service attacks: A tutorial." IEEE communications magazine 40.10 (2002): 42-51.*
4. *Divyang Dave, Meet Kava, R. K. Gupta and Kaushal Shah, "Deep Learning approach for Intrusion Detection System, IEEE International Conference on Technology, Research, and Innovation for Betterment of Society (TRIBES), 2022. Doi: 10.1109/TRIBES52498.2021.9751643.*
5. *R. K. Gupta et al., "An Improved Secure Key Generation Using Enhanced Identity-Based Encryption for Cloud Computing in Large Scale 5G", Wireless Communications and Mobile Computing 2022.*
6. *Khuphiran, Panida, et al. "Performance comparison of machine learning models for ddos attacks detection." 2018 22nd International Computer Science and Engineering Conference (ICSEC). IEEE, 2018.*
7. *Farnaaz, Nabila, and M. A. Jabbar. "Random forest modeling for network intrusion detection system." Procedia Computer Science 89 (2016): 213-217.*
8. *Li, Yang, and Li Guo. "An active learning based TCM-KNN algorithm for supervised network intrusion detection." Computers & security 26.7-8 (2007): 459-467.*
9. *Panda, Mrutyunjaya, and Manas Ranjan Patra. "Network intrusion detection using naive bayes." International journal of computer science and network security 7.12 (2007): 258-263.*
10. *Yong, Li, and Zhang Bo. "An intrusion detection model based on multi-scale CNN." 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC). IEEE, 2019.*
11. *Vu, N.H. DDoS attack detection using K-Nearest Neighbor classifier method. In Proceedings of the International Conference on Telehealth/Assistive Technologies, Baltimore, Maryland, USA, 16–18 April 2008; IEEE: Piscataway Township, NJ, USA, 2008; pp. 248–253.*
12. *Cheng, J.; Yin, J.; Liu, Y.; Cai, Z.;Wu, C. DDoS attack detection using IP address feature interaction. In Proceedings of the IEEE International Conference on Intelligent Networking and Collaborative Systems, Thessalonika, Greece, 24–26 November 2010; IEEE: Piscataway Township, NJ, USA, 2009; pp. 113–118.*
13. *Wang, C.; Zheng, J.; Li, X. Research on DDoS attacks detection based on RDF-SVM. In Proceedings of the 10th International Conference on Intelligent Computation Technology and Automation, Changsha, China, 9–12 October 2017.*
14. *Fadlil, A.; Riadi, I.; Aji, S. Review of detection DDoS attack detection using Naïve Bayes classifier for network forensics. Bull. Electr. Eng. Inform. 2017, 6, 140–148. [CrossRef]*
15. *Dincalp, U. Anomaly based distributed denial of service attack detection and prevention with machine learning. In Proceedings of the 2nd International Symposium on Multidisciplinary Studies and Innovative Technologies, Ankara, Turkey, 19–21 October 2018.*
16. *Ahanger, T.A. An effective approach of detecting DDoS using artificial neural networks. In Proceedings of the 2017 International Conference onWireless Communications, Signal Processing and Networking, Chennai, India, 22–24 March 2017; IEEE: Piscataway Township, NJ, USA, 2017; pp. 707–711.*
17. *Zahid Hasan, Md., Zubair Hasan, K. M., & Sattar, Abdus (2018). Burst header packet flood detection in optical burst switching network using deep learning model. Procedia Computer Science, 143, 970–977.*
18. *Krishnan, Prabhakar, Duttagupta, Subhasri, & Achuthan, Krishnashree (2019). VARMAN: Multi-plane security framework for software defined networks. Computer Communications, 148, 215–239.*