DDoS Analysis and Detection with Machine Learning Algorithms

By Tiffany Tu

Author Bio

Tiffany Tu is a senior at Bellevue High School in Washington state. She hopes to study computer science with a focus on cybersecurity, combating emerging digital threats utilizing machine learning with more projects in the future.

Abstract

Distributed Denial of Service (DDoS) attacks, where compromised systems are used to flood a target with an overwhelming amount of traffic, pose a significant threat to the availability and security of digital networks. As these attacks continue to evolve in sophistication and scale, there is a pressing need to develop effective DDoS detection techniques to mitigate their impact. Utilizing a dataset of benign and dangerous (DDoS) network flows, this research paper evaluates and compares various machine learning techniques for the detection of DDoS attacks to identify the most accurate methodologies to contribute to the security of networked digital infrastructure. The study conducts feature deduction and variable transformation on the dataset and subsequently build and trains multiple different machine learning models. The findings of this research quantify the effectiveness of each machine learning method tested in identifying DDoS attacks. Random Forest (99.24%) performed the best in terms of detection accuracy. Decision Tree was also accurate (98.68%) in detecting DDoS flows, and Logistic Regression was the least precise (71.81%). These results exhibit the importance of selecting appropriate machine learning models to enhance the resilience of network security systems from DDoS attacks. Furthermore, the research underscores the need for further exploration using additional machine learning models to develop more effective and robust detection strategies. Ultimately, the outcomes of this paper contribute to the efforts to detect DDoS attacks and enhance the overall security posture of digital environments.

Keywords: DDoS, DDoS attack, cybersecurity, network flows, machine learning, random forest, decision tree, logistic regression

Introduction

In today's interconnected digital landscape, the magnitude and significance of cyberattacks are skyrocketing, making them an ever-increasing threat. Cyberattacks are malicious actions that target computer systems, networks, or data to compromise, disrupt, or gain unauthorized access (Li & Liu, 2021). They encompass a range of malicious activities, from data breaches to ransomware attacks to phishing scams. However, distributed denial of service (DDoS) attacks have emerged as a particularly formidable menace. These attacks involve overwhelming a target system or network with an enormous volume of traffic, rendering it inaccessible to legitimate users and disrupting critical services (Rubin et al., 2000).

The identification of malicious traffic on computer systems can be achieved by utilizing machine learning algorithms in DDoS attack analysis and detection to enhance computer network security (Kaur et al., 2017). DDoS attack detection modules analyze collected data to assess the security risk posed by network connections, while machine learning algorithms, trained on previous tasks and feedback, enhance their predictive capabilities through adaptive changes (Sarker, 2021).

This study explores different machine learning techniques for detecting and analyzing DDoS attacks while examining and comparing their respective accuracies and suitability. This analysis is conducted in order to (1) safeguard computer networks and online services from disruptive and potentially damaging cyberattacks, (2) protect data integrity, and (3) maintain the overall stability and functionality of the digital ecosystem.

This paper first discusses the technicalities of how a DDoS attack works. Next, it provides a real-world DDoS attack example. Then, it details a relevant dataset and explores methodology along with visualizations. This paper concludes with the performance evaluation and analysis of study results.

Background

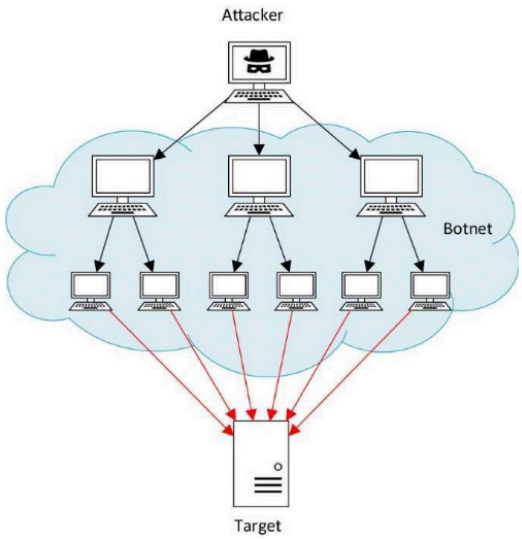
DDoS attacks represent a prevalent and disruptive form of cyberattack, designed to overwhelm and paralyze targeted computer systems or networks. The main technique employed in DDoS attacks involves flooding the target with an overwhelming volume of traffic, rendering it incapable of functioning properly and denying access to legitimate users (Cloudflare, 2023).

As shown in Figure 1, DDoS attacks leverage the power of multiple compromised devices, forming what is referred to as a botnet. These devices have been previously infected with malware, allowing attackers to control them remotely. The attackers command the botnet to send an enormous amount of traffic to the targeted system, exploiting its limitations and overwhelming its resources (Fortinet, 2023).

The traffic used in DDoS attacks can take various forms, such as HTTP requests, UDP or TCP packets, or even illegitimate requests to specific services. The goal is to exhaust the target's processing power, bandwidth, or other critical resources, ultimately causing service degradation or complete unavailability.

The scale and complexity of DDoS attacks have grown significantly over the years, making them a formidable challenge to combat (US Department of Homeland Security, 2023). Mitigating these attacks requires proactive monitoring, detection, and analysis that can identify and filter out malicious traffic while allowing legitimate traffic to reach its intended destination.

Figure 1
DDoS Attack Process



Note. How a distributed denial of service attack works, from the attacker to the target. From A Hybrid ML Approach for Detecting Unprecedented DDoS Attacks, by Mohammad Najafimehr et al., n.d. (https://www.researchgate.net/figure/A-diagram-of-a-DDoS-attack-performed-with-a-botnet_fig1_357168204).

Case Study

In 2018, GitHub, a widely used code hosting platform, experienced one of the largest and most significant DDoS attacks in history (Microsoft, 2023). The attack targeted GitHub's infrastructure, disrupting its services and causing a ripple effect across the internet. The incident shed light on the scale and severity of DDoS attacks and their potential to disrupt even highly resilient online platforms.

The attack on GitHub reached an unprecedented peak traffic volume of 1.35 terabits per second (Tbps), surpassing any previously recorded attack (Kottler, 2018a). It was executed by leveraging a botnet, a network of compromised devices under the control of malicious actors. The attackers harnessed this botnet to flood GitHub's servers with an overwhelming amount of spurious traffic, aimed at exhausting the platform's resources and rendering it inaccessible to legitimate users (Newman, 2018).

The attack on GitHub served as a wake-up call regarding the security vulnerabilities in digital ecosystems and the potential for them to be harnessed for large-scale attacks. Moreover, the GitHub attack underscored the interconnectivity and interdependence of online services. The disruption caused by the attack extended beyond GitHub's own platform, impacting other services that relied on GitHub for code hosting and collaboration. High-profile websites and organizations, including popular streaming services, experienced performance issues and service disruptions due to their reliance on GitHub's infrastructure (Kottler, 2018b).

The consequences of the GitHub DDoS attack were far-reaching. The attack prompted widespread concern and discussion about the state of cybersecurity and the need for enhanced DDoS mitigation strategies. The incident also highlighted the importance of collaboration between online platforms, internet service providers, and security organizations to swiftly identify and mitigate such attacks.

Dataset

This study utilizes data provided by the Canadian Institute for Cybersecurity (CIC) of network flows, sequences of data packets exchanged between a source and destination (Goldberg et al., 1989). DDoS flows that were extracted from different public CIC Intrusion Detection System datasets produced in different years were combined with "benign" flows extracted from the same base datasets and made into a single large dataset used in this study. The dataset used within this research has a total of 12794627 datapoints (rows) and 85 features (columns). Each datapoint corresponds to one network flow (forward or reverse) that is either benign or is part of a DDoS attack (Kaggle, 2019).

The DDoS attack scenarios to create experimental flows in this study's dataset included 50 machines in the attacking infrastructure and 420 machines with 30 servers on the victim side (CIC, 2018).

This study's dataset has no missing or duplicate values. Each feature (variable) in the dataset has a data type of either integers or floats, apart from identifier attributes and the target variable that are string objects. The identifiers provide context about flows, including Flow ID, Source IP, and Destination port. Because identifiers bear little information suitable for building machine learning models in this case, it is not necessary to dig up the data within them, so they can be removed from the predicted variable list.

Continuing with the dimension reduction of our dataset to reduce features not valuable for machine learning models while maintaining the same degree of accuracy, the statistical description of each column was analyzed. The variables with a standard deviation lower than 1 are dropped to reduce homogeneity in the dataset. Additionally, the target variable was changed into binary format to remove all string objects from the dataset, with 0 representing "benign" and 1 representing "DDoS" flows, since this study sought to predict DDoS attacks. The columns that contained an inf (infinity) value were dropped to make machine learning model building more straightforward later. In the process of features extraction, 26 total features

were dropped, and the study moved forward with a dataset with 59 columns, including the target variable.

Visualizations

To visualize the distribution of the study's target variable and display its amount and percentage within the dataset, a histogram was plotted, and a pie chart was created. DDoS = 1; Benign = 0

Figure 2a

Target Variable Distribution: Histogram

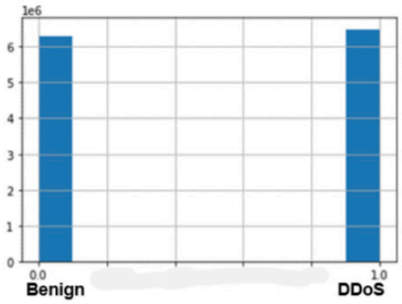
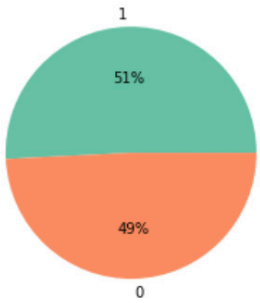


Figure 2b

Target Variable Distribution: Pie Chart

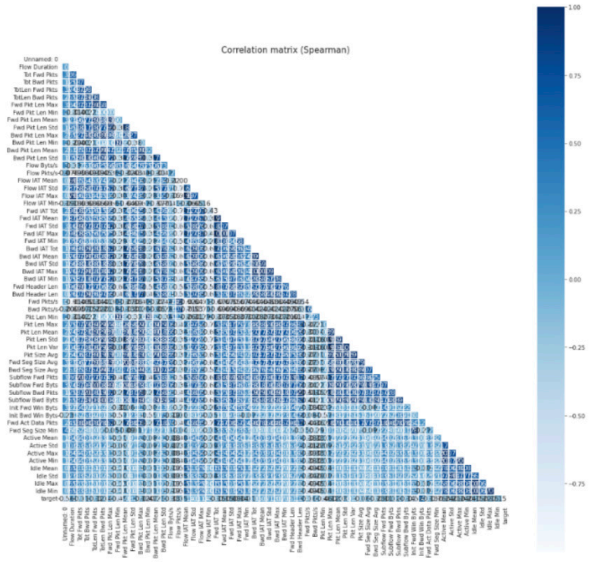


Note. A visual of the target variable's distribution.

To visualize the correlation between the independent variables (features) and the target variable of the dataset, a heat map was created. A heat map shows correlation utilizing colors instead of numbers, with darker colors indicating a higher correlation and lighter colors indicating a lower correlation.

Figure 3

Heat Map of Correlation

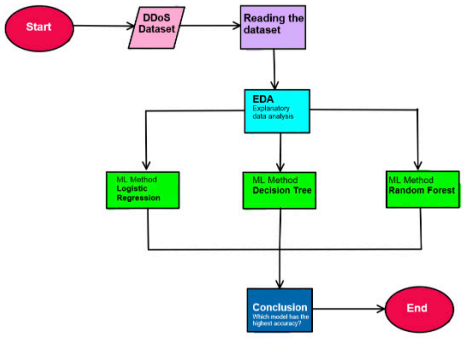


Note. The relationship between independent features (columns) and the target variable.

Methodology

In this research paper, the process of DDoS detection using machine learning algorithms that are appropriate for classification problems is presented, highlighting the different steps and components involved. The methodology for this study is outlined in Figure 4, and to enhance comprehension of the machine learning approach, it illustrates the process from beginning to end.

Figure 4
Methodology Process



Note. The process for the methodology of this study from start to finish. Own work.

Because the data cleaning and EDA process was previously conducted (including feature deduction and variable transformation), the data can be used to train a variety of machine learning (ML) models. Since this research is a classification problem, this study builds several ML algorithms to detect DDoS flows:

Logistic Regression: A machine learning method used for binary classification tasks. It models the relationship between input features and the probability of a specific outcome, employing a logistic function to estimate the likelihood of class membership. It is widely utilized for its simplicity, interpretability, and effectiveness in various domains (Xu et al., 2023).

Decision Tree: A versatile and interpretable machine learning algorithm that uses a tree-like structure to make predictions by recursively splitting the data based on feature values. It creates a series of if-else rules that lead to classifying or predicting the target variable (Xu et al., 2023)

Random Forest: An ensemble ML algorithm that combines multiple decision trees to make predictions. It creates a diverse set of trees by using random subsets of features and samples from the training data. The final prediction is determined by aggregating the predictions of individual trees (Xu et al., 2023)

Although there are existing studies that predict cyberattacks using machine learning techniques, some take fewer input attributes into account to form conclusions. Because this study's machine learning models are trained on datasets that have more than 50 independent variables, a broad range of factors are considered that can lead to more precise predictions about whether a flow is malicious (DDoS) or benign (Khalaf, 2019).

Performance Evaluation

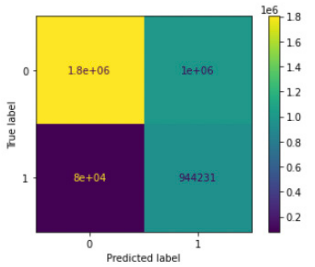
This study utilized machine learning algorithms and classifiers to examine network flows that were either benign or DDoS. After creating each machine learning model, the results of their respective accuracies in detecting DDoS attacks and confusion matrices are below. Accuracy scores are calculated by the ratio of the True Positives (model predicts DDoS as DDoS) and True Negatives (model predicts benign as benign)—the top left and bottom right boxes of the matrix—with the number of total cases.

Logistic Regression

Accuracy score: 71.81%

Figure 5a

Confusion Matrix: Logistic Regression



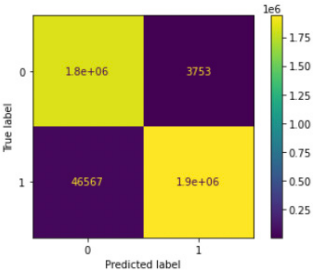
Note. The counts of true positive, true negative, false positive, and false negative predictions of the LR model.

Decision Tree

Accuracy score: 98.68%

Figure 5b

Confusion Matrix: Decision Tree



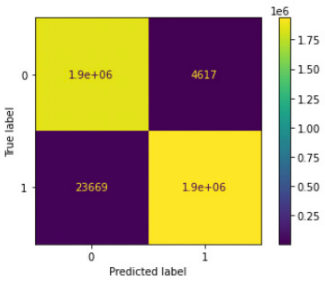
Note. The counts of true positive, true negative, false positive, and false negative predictions of the DT model.

Random Forest

Accuracy score: 99.24%

Figure 5c

Confusion Matrix: Random Forest



Note. The counts of true positive, true negative, false positive, and false negative predictions of the RF model.

The accuracy scores and confusion matrices illustrate that Random Forest has the highest accuracy (99.24%) in predicting if flows are DDoS. However, the accuracy score of Decision Tree is very close to that of Random Forest, standing at 98.68%. Logistic Regression has the lowest accuracy, with a score of 71.81%.

This research highlights the comparative performance of different machine learning techniques in DDoS attack detection. Through analysis of the machine learning accuracy scores, this research shows that Random Forest has the best performance for DDoS detection strategy, with Decision Tree coming at a close second for the detection and identification of DDoS flows. The weakest technique, logistic regression, stands in third place among the techniques tested due to its lowest accuracy score. Thus, Random Forest and Decision Tree can identify flows as part of a DDoS attack in the most accurate manner and are better choices for DDoS detection.

This research provides insights into the selection of appropriate machine learning models for DDoS detection. Those involved in the field of cybersecurity can leverage these findings to make informed decisions regarding the choice of machine learning algorithms for DDoS detection systems, enhancing their ability to identify and mitigate DDoS attacks promptly and accurately, bolstering the overall security of the network infrastructure (Bhuyan, 2014).

Conclusion

DDoS attacks are growing in impact and frequency, and networks and online services are under the threat of disruptive and damaging cyber-attacks (Zargar et al., 2013). Using a single dataset with flows extracted from the Canadian Institute for Cybersecurity's datasets from various years, this research paper seeks to investigate various machine learning techniques for the detection and analysis of DDoS attacks (the identification of dangerous versus benign network flows). The study also pursues the comparison and evaluation of their accuracies, with the aim of identifying the most appropriate techniques to utilize to contribute to the defense of online systems.

The results show that Random Forest (99.24%) performed the best in terms of detection accuracy. Decision Tree was also accurate (98.68%) in detecting DDoS flows, and Logistic Regression was the least precise (71.81%). This analysis highlights the usefulness of different machine learning methods for identifying DDoS; however, further research with a broader range of machine learning models (KNN, SVM, Naïve Bayes, XGB, etc.) is needed to gain a comprehensive understanding of their capabilities and limitations. Exploring diverse techniques can lead to the development of more effective and robust detection tools and strategies. Analyzing and detecting DDoS attacks with machine learning algorithms is key to enhancing proactive security measures and establishing the security of services, critical network infrastructure, and the overall digital realm.

References

Bhuyan, M. H., Kashyap, H. J., Bhattacharyya, D. K., & Kalita, J. K. (2013). Detecting distributed denial of service attacks: Methods, tools and future directions. The Computer Journal, 57(4), 537-556. https://doi.org/10.1093/comjnl/bxt031

DDoS dataset. (n.d.). Kaggle: Your Machine Learning and Data Science Community. https://www.kaggle.com/datasets/devendra416/ddos-datasets

Ddosd. (2022, January 27). Homeland Security. https://www.dhs.gov/science-and-technology/ddosd

F. Lau, S. H. Rubin, M. H. Smith, and L. Trajkovic. (2000). Distributed denial of service attacks. Smc 2000 conference proceedings, 3, 2275-2280. https://doi.org/10.1109/ICSMC.2000.886455

Goldberg, A. V., Tardos, E., & Tarjan, R. E. (1989). Network flow algorithms. https://doi.org/10.21236/ada214689

IDS 2016 | Datasets | Research | Canadian institute for cybersecurity | UNB. (n.d.). University of New Brunswick | UNB. https://www.unb.ca/cic/datasets/ids-2016.html

IDS 2017 | Datasets | Research | Canadian institute for cybersecurity | UNB. (n.d.). University of New Brunswick | UNB. https://www.unb.ca/cic/datasets/ids-2017.html

IDS 2018 | Datasets | Research | Canadian institute for cybersecurity | UNB. (n.d.). University of New Brunswick | UNB. https://www.unb.ca/cic/datasets/ids-2018.html

Khalaf, B. A., Mostafa, S. A., Mustapha, A., Mohammed, M. A., & Abduallah, W. M. (2019). Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods. IEEE Access, 7, 51691-51713. https://doi.org/10.1109/access.2019.2908998
Kottler, S. (2018, March 1). February 28th DDoS incident report. The GitHub Blog. https://github.blog/2018-03-01-ddos-incident-report/

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 7, 8176-8186. https://doi.org/10.1016/j.egyr.2021.08.126
Mahesh, Batta. (2019). Machine Learning Algorithms – A Review. International Journal of Science and Research. DOI: 10.21275/ART20203995

Microsoft 365 Team. (2023, February 17). Top 5 most famous DDoS Attacks. https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/top-5-most-famous-ddos-attacks

Najafimehr, M., Zarifzadeh, S., & Mostafavi, S. (2022). A hybrid machine learning approach for detecting unprecedented DDoS attacks. The Journal of Supercomputing, 78(6), 8106-8136. https://doi.org/10.1007/s11227-021-04253-x

Nast, C. (2018, March 1). GitHub survived the biggest DDoS attack ever recorded. WIRED. https://www.wired.com/story/github-ddos-memcached/

Parneet Kaur, Manish Kumar & Abhinav Bhandari. (2017). A review of detection approaches for distributed denial of service attacks. Systems Science & Control Engineering, 5:1, 301-320. https://doi.org/10.1080/21642583.2017.1331768

Sarker, I. H. (2021). Machine learning: Algorithms, real-world applications and research directions. https://doi.org/10.20944/preprints202103.0216.v1

What is a DDoS attack? DDoS meaning, definition & types. (n.d.). Fortinet. https://www.fortinet.com/resources/cyberglossary/ddos-attack#:~:text=DDoS%20Attack%20Meaning,connected%20online%20services%20and%20sites

What is a DDoS Attack. (n.d.). Cloudflare - The Web Performance & Security Company | Cloudflare. https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. IEEE Communications Surveys & Tutorials, 15(4), 2046-2069. https://doi.org/10.1109/surv.2013.031413.00127