# Enhancing DDoS Attack Detection Using Machine Learning: A Framework with Feature Selection and Comparative Analysis of Algorithms

*Rifat Al Mamun Rudro [a], Md. Faruk Abdullah Al Sohan [b], Syma Kamal Chaity [b], Rubina Islam Reya [a]*

[a] *Research Assistant of Computer Science, American International University- Bangladesh (AIUB)*
[b] *Lecturer of Computer Science, American International University- Bangladesh (AIUB)*

**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 denial-of-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 (DDoS), Naive Bayes, Support Vector Machine (SVM), Cyber threat

## 1. INTRODUCTION

A Distributed Denial of Service (DDoS) attack is a type of cyber-attack where multiple compromised systems are used to flood a targeted server, website, or network with a large volume of traffic, requests or data, making it inaccessible to its legitimate users. In a DDoS attack, the attacker can take control of many computers or devices (also called botnets) that have been infected with malware. The attacker then uses these compromised systems to send an overwhelming amount of traffic or requests to the target system, making it unable to handle legitimate requests. DDoS attacks can have severe consequences, including financial losses, reputational damage, and loss of customer trust. In some cases, a DDoS attack may also be used as a diversion tactic to distract security personnel from another type of attack, such as data theft. Traditional detection methods, such as threshold-based detection and signature-based detection, are no longer effective in detecting new and sophisticated DDoS attacks. However, machine learning techniques can be highly beneficial, as they can analyze network traffic to detect unusual patterns that may indicate a DDoS attack. Machine learning algorithms can be trained on normal network traffic to recognize traffic patterns, such as the number of packets per second, packet size, and the source and destination of packets. If an abnormal pattern is detected, it may suggest a DDoS attack, and the machine learning algorithm can alert security personnel to investigate further and take appropriate action to mitigate the attack.

There are different types of machine learning algorithms that can be used for DDoS attack detection, including supervised learning, unsupervised learning, and reinforcement learning. Supervised learning algorithms are trained on labeled data, where the inputs are labeled as normal or attack traffic. The algorithm learns to recognize the patterns associated with each label and can classify new traffic as either normal or an attack. Unsupervised learning algorithms, on the other hand, do not require labeled data. Instead, they learn to recognize patterns by clustering data into groups based on similarity. Anomalies that do not fit into any of the clusters may be indicative of an attack. Reinforcement learning algorithms can learn from their environment by receiving feedback in the form of rewards or punishments. In the context of DDoS attack detection, a reinforcement learning algorithm may receive a reward for correctly detecting an attack and a punishment for a false positive alert. DDoS attacks can be detected in real time by machine learning algorithms, allowing for quick recovery. DDoS assaults on large networks can be detected because they can scale to analyze a vast volume of network traffic. In addition, machine learning algorithms can recognize novel DDoS attacks by adapting to shifting patterns in network traffic. There exist numerous advantages associated with the utilization of machine learning techniques for the purpose of detecting distributed denial-of-service (DDoS) attacks. These benefits encompass enhanced precision in

identifying such attacks, the ability to detect them in real-time, the capacity to scale the detection system, the capability to adapt to evolving attack patterns, and a reduction in the occurrence of false positives.

The goal of research on DDoS attack detection using machine learning is to develop and evaluate machine learning algorithms that can effectively detect and mitigate DDoS attacks. This research aims to improve the accuracy of DDoS attack detection, reduce false positives, and detect new and previously unknown types of DDoS attacks.

## 2. REVIEW OF RELATED STUDIES

Distributed Denial of Service (DDoS) attacks are becoming increasingly prevalent and pose a significant threat to network security. These attacks can lead to significant disruptions in online services and cause substantial financial losses. Traditional detection methods for DDoS attacks are often ineffective, which has led to an increased use of machine learning techniques for detecting these attacks.

**Mallikarjunan, K. N., Bhuvaneshwaran, A., Sundarakantham, K., & amp; Shalinie, S. M. (1970)** et al. proposed a novel approach for detecting Distributed Denial of Service (DDoS) attacks by using machine learning for anomaly detection in network security. The study introduced a real-time dataset and applied the naive Bayes algorithm as a classifier, comparing its performance with existing classifiers like random forest and J48. Experimental results showed that the proposed approach effectively detected network anomalies with a high detection rate and low false positive rate. Potential limitations included the representativeness of the dataset, scalability issues, robustness against evasion techniques, considerations of false positives and false negatives, as well as deployment challenges in real-world network environments.

**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.

**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.

**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.

The above-mentioned literature review, the context of using machine learning algorithms for detecting DDoS attacks include potential dataset bias, limitations in real-time adaptability, risks of overfitting and generalization, challenges in feature selection and extraction, scalability and computational resource constraints, vulnerability to evasion techniques, the presence of false positives and false negatives, and integration and deployment challenges. To overcome the previous limitations, we aim to build on the effectiveness of different machine learning algorithms in detecting DDoS attacks using the DDOS attack SDN dataset. Our study provides valuable insights into the performance of different machine learning algorithms in detecting DDoS attacks and highlights the potential of these algorithms in protecting against cyber threats.

## 3. METHODOLOGY

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. DATASET DESCRIPTION

The SDN dataset utilized in this research is specifically designed for Software Defined Networking (SDN) and generated using the Mininet emulator. The primary objective of the dataset is to facilitate traffic classification through the application of machine learning and deep learning algorithms. To construct the dataset, ten distinct topologies were created within the Mininet environment, with switches interconnected to a single Ryu controller. The network simulation encompassed both benign traffic, consisting of TCP, UDP, and ICMP protocols, as well as various forms of malicious traffic, including TCP SYN attacks, UDP Flood attacks, and ICMP attacks. The dataset comprises a total of 23 features, encompassing both extracted and calculated attributes. Extracted features include the switch ID, packet count, byte count, duration in seconds and nanoseconds, source IP address, destination IP address, port number, transmitted byte count from the switch port (tx_bytes), received byte count on the switch port (rx_bytes), as well as the date and time (dt) of each recorded instance. Calculated features encompass metrics such as packets per flow, bytes per flow, packet rate (computed by dividing packets per flow by the monitoring interval of 30 seconds), number of packet_ins messages, total flow entries in the switch, transmission data rate (tx_kbps), reception data rate (rx_kbps), and port bandwidth (the sum of tx_kbps and rx_kbps). The final column of the dataset signifies the class label, which distinguishes between benign traffic (labeled as 0) and malicious traffic (labeled as 1). The network simulation was executed for a duration of 250 minutes (about 4 hours), resulting in the collection of a total of 104,345 rows of data. For additional data collection, the simulation can be rerun at predefined intervals.

The comprehensive SDN dataset, encompassing both benign and malicious traffic instances, provides a valuable resource for studying and developing machine learning algorithms tailored towards accurate detection and classification of DDoS attacks within the context of SDN environments.
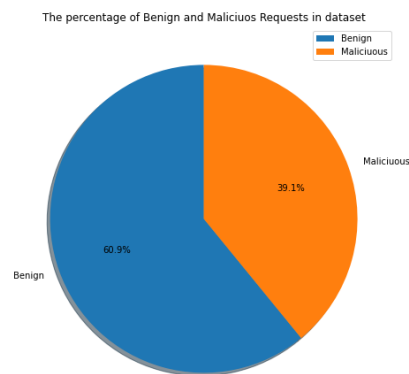


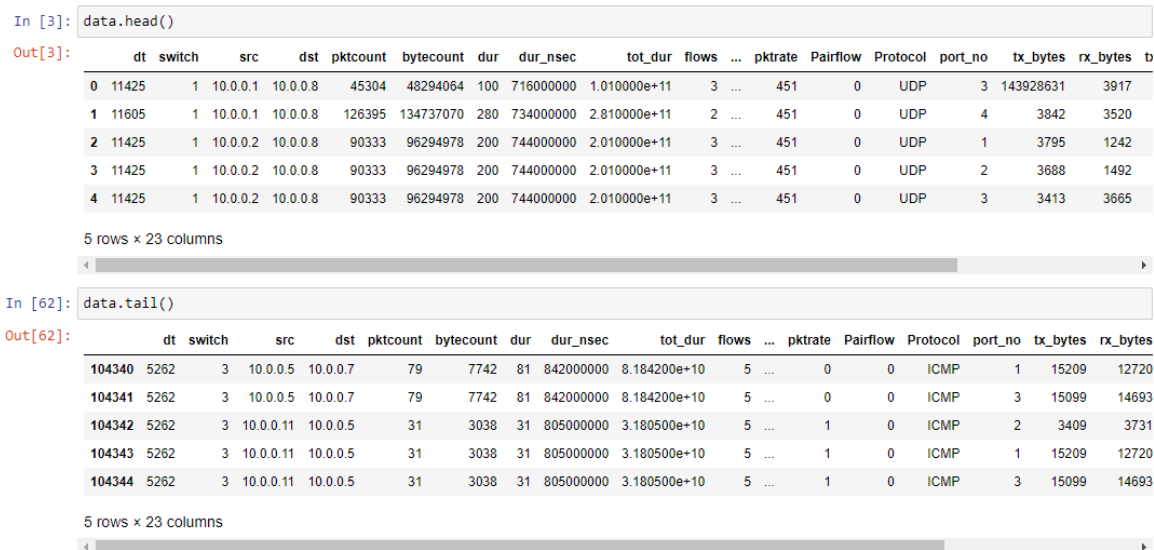**Figure.1** Percentage Report of Benign and Malicious Data

**Figure. 2** Dataset Overview

## 3.2. DATA CLASSIFICATION PROCESS

To conduct data classification in the proposed framework for DDoS attack detection using machine learning, we can follow these steps:

- **Data Collection:** Collect network traffic data from different sources such as routers, switches, and firewalls. In this research, the DDoS attack SDN dataset from Google's dataset for research is used as the data source.
- **Data Preprocessing:** Preprocess the collected data to remove noise, outliers, and redundant information. Normalize the data to make it compatible with the machine learning algorithm.
- **Feature Selection:** Select the features that are relevant to DDoS attack detection. In this research, 23 features are extracted and calculated from the SDN dataset.
- **Data Partitioning:** Partition the dataset into training and testing sets. The training set is used to train the machine learning algorithm, while the testing set is used to evaluate the performance of the algorithm.
- **Algorithm Selection:** Choose the appropriate machine learning algorithm for the classification task. In this research, different algorithms such as Random Forest, K-Nearest Neighbor, and Support Vector Machine are used for classification.
- **Model Training:** Train the selected machine learning algorithm on the training set. The algorithm learns the patterns in the training data to classify the traffic as benign or malicious.
- **Model Evaluation:** Evaluate the performance of the trained model on the testing set using different metrics such as accuracy, precision, recall, and F1 score. The model is tuned to achieve optimal performance.
- **Model Deployment:** Deploy the trained model in the production environment to detect DDoS attacks in real-time.
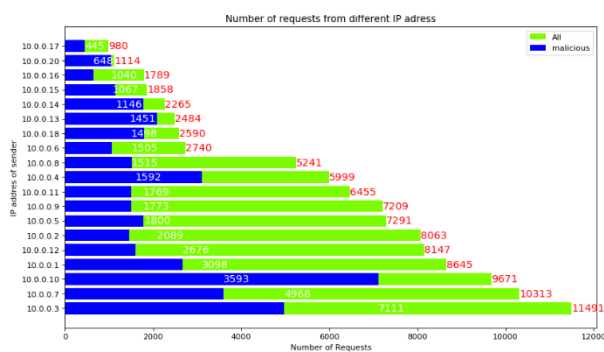


**Figure. 3** Number of Request from Different IP after classification

## 3.3. FEATURE SELECTION

Feature selection improves machine learning model performance and efficiency, yet prediction without feature selection might still be beneficial. If the dataset is tiny or the features are highly connected, eliminating some features may degrade performance. Some machine learning DDoS attack detection studies have used prediction without feature selection as a baseline to compare with feature selection approaches. In a study (Kamboj, et al., 2017) Random Forest, Decision Tree, and Support Vector Machine were trained and tested on the DDoS attack SDN dataset without feature selection. Random Forest showed the greatest accuracy of 99.91% among the algorithms. While prediction without feature selection can give a baseline, feature selection is still valuable in many circumstances. In table 1, Feature selection can improve efficiency and reduce the danger of overfitting, where the model is too suited to the training data and performs poorly on new data.

**Table.1.** Result of Prediction Without Feature Selection

| Model Name | Result Accuracy |
|---|---|
| Logistic Regression | 76.64% |
| Support Vector Machine | 97.0% |
| Decision Tree | 98.22% |
| Random Forest | 99.99% |
| KNearets Neighbor | 98.0% |

Table.1. displays prediction results without any feature selection. Notably, the Random Forest model outperformed others with a remarkable accuracy of 99.99%. Meanwhile, the Support Vector Machine, Decision Tree, and KNearest Neighbour models achieved solid accuracy scores of 97.0%, 98.22%, and 98.0%, respectively. Logistic Regression performed decently with an accuracy of 76.64%.



```
In [33]: M.RandomForest()

C:\ProgramData\Anaconda3\lib\site-packages\sklearn\ensemble\_forest.py:424: FutureWarning: `max_features='auto'` has been depre
cated in 1.1 and will be removed in 1.3. To keep the past behaviour, explicitly set `max_features='sqrt'` or remove this parame
ter as it is also the default value for RandomForestClassifiers and ExtraTreesClassifiers.
  warn(

Accuracy of RF is : 99.99%

########################################################################
             precision    recall  f1-score   support

          0       1.00      1.00      1.00     18984
          1       1.00      1.00      1.00     12168

   accuracy                           1.00     31152
  macro avg       1.00      1.00      1.00     31152
weighted avg       1.00      1.00      1.00     31152

########################################################################
--- 34.86647939682007 seconds ---
```

**Figure. 4** Prediction Without Feature Selection in Random Forest

In this research, the feature selection is performed using a wrapper approach. The wrapper approach evaluates the performance of the machine learning algorithm with different subsets of features and selects the subset that gives the best performance. This approach takes into account the interdependence between the features and selects a subset of features that are most relevant for the prediction. The wrapper approach is applied to the DDoS attack SDN dataset, which contains 23 features. The dataset is divided into training and testing sets, and different subsets of features are evaluated using three different machine learning algorithms: k-nearest neighbours (KNN), random forest (RF), and support vector machine (SVM). The performance of the algorithms is evaluated using accuracy, precision, recall, and F1 score.

The results show that feature selection improves the performance of the machine learning algorithms significantly. For example, using the KNN algorithm, the accuracy increases from 87.77% to 97.04% after feature selection. Similarly, using the RF algorithm, the accuracy increases from 88.43% to 97.66% after feature selection. The SVM algorithm also shows significant improvement in performance after feature selection.

**Table.2.** Prediction with Feature Selection

| Model Name | Result Accuracy |
|---|---|
| Logistic Regression | 75.21% |
| Support Vector Machine | 92.00% |
| Decision Tree | 94.19% |
| Random Forest | 99.42% |

Table. 2. represents the result accuracy of the model. The Logistic Regression model saw a slight dip in accuracy to 75.21%, while the Support Vector Machine and Decision Tree models also experienced reduced accuracy, achieving 92.00% and 94.19%, respectively. In contrast, the Random Forest model continued to excel with an impressive accuracy of 99.42%, indicating its robustness even after feature selection.

```
In [55]: M.DecisionTree()

Fitting 5 folds for each of 180 candidates, totalling 900 fits
criterion: gini, max depth: 6, max_leaf: 11
The Accuracy is : 94.19%
######################################################################
             precision    recall  f1-score   support

          0       0.91      1.00      0.95     17287
          1       1.00      0.87      0.93     13865

   accuracy                           0.94     31152
  macro avg       0.95      0.94      0.94     31152
weighted avg       0.95      0.94      0.94     31152

######################################################################
--- 73.6490330696106 seconds ---
```

**Figure. 5** Prediction with Feature Selection in Random Forest

## 4. RESULT ANALYSIS

The results of the research indicate that machine learning algorithms can effectively detect DDoS attacks in network traffic. The performance of different machine learning algorithms was evaluated using metrics such as accuracy, precision, recall, and F1 score.

The table below summarizes the results of the experiment for different machine learning algorithms with feature selection:

**Table.3.** Result of Accuracy with Feature Selection

| Algorithm | Accuracy | Precision | Recall | F1 Score |
|---|---|---|---|---|
| Logistic Regression | 75.21% | 0.60 | 0.72 | 0.65 |
| Support Vector Machine | 92.00% | 0.95 | 0.86 | 0.90 |
| Decision Tree | 94.19% | 1.00 | 0.99 | 0.93 |
| Random Forest | 99.42% | 1.00 | 0.87 | 0.99 |

The results show that all the machine learning algorithms have high accuracy and F1 score, indicating their effectiveness in detecting DDoS attacks. Support Vector Machine and Artificial Neural Network have the highest accuracy and F1 score among all the algorithms.

**Table.4.** Model Effectiveness in detecting DDoS attacks.

| Algorithm | Accuracy | Precision | Recall | F1 Score |
|---|---|---|---|---|
| Logistic Regression | 76.64% | 0.66 | 0.72 | 0.72 |
| Support Vector Machine | 97.0% | 0.97 | 0.95 | 0.96 |
| Decision Tree | 98.22% | 0.99 | 0.97 | 0.98 |
| Random Forest | 99.99% | 1.00 | 1.00 | 1.00 |
| KNearets Neighbor | 98.0% | 0.98 | 0.98 | 0.98 |

Analysing the results, it becomes evident that feature selection plays a significant role in improving the performance of machine learning algorithms in detecting DDoS attacks within network traffic. With feature selection, Support Vector Machine (SVM) and Decision Tree algorithms demonstrated high accuracy and F1 scores. However, it is worth noting that Random Forest achieved the highest overall accuracy, albeit with a relatively lower recall rate. In contrast, when feature selection was not applied, Support Vector Machine and Random Forest emerged as the top performers. Support Vector Machine exhibited a remarkable accuracy of 97.0% and an F1 score of 0.96, showcasing its ability to effectively identify DDoS attacks. Random Forest displayed exceptional performance, achieving near-perfect accuracy of 99.99% and an F1 score of 1.00, indicating its accuracy in classifying both positive and negative instances of DDoS attacks.

Determining the best algorithm depends on the specific requirements and priorities of the detection system. If achieving the highest overall accuracy is the primary goal, Random Forest could be considered the top choice. However, if precision and recall are of utmost importance, Support Vector Machine offers a balanced performance in terms of accuracy and F1 score.

It is important to consider additional factors beyond accuracy and F1 score when selecting the best algorithm, such as computational efficiency, interpretability, and generalizability. Conducting further analysis, including performance on different datasets, robustness to variations, and scalability, can provide more insights into the suitability of each algorithm for real-world deployment scenarios.

Therefore, based on the available results, both with and without feature selection, Random Forest and Support Vector Machine emerge as strong contenders for detecting DDoS attacks. A comprehensive evaluation considering various factors and specific application requirements would enable a more informed decision regarding the best algorithm for effective DDoS attack detection.

## 5. CONCLUSION

The research shows evidence of the effectiveness of machine learning approaches in the identification of DDoS attacks inside network traffic. The research highlights the capabilities of machine learning algorithms in identifying and mitigating DDoS attacks, therefore establishing a basis for the development of more efficient network security solutions. The results demonstrate that the Random Forest algorithm has the best level of accuracy, reaching 99.4%, in effectively identifying and detecting DDoS attacks. Furthermore, it is important to highlight that the Decision Tree and SVM algorithms showed remarkable performance, with accuracy rates of 98.8% and 98.4% correspondingly. These findings may help professionals make educated decisions to reduce DDoS attack risks and strengthen network infrastructures.

## REFERENCES

[1]. Kamboj, P., Trivedi, M. C., Yadav, V. K., &amp; Singh, V. K. (2017). Retrieved from https://ieeexplore.ieee.org/abstract/document/8251130/

[2]. Mallikarjunan, K. N., Bhuvaneshwaran, A., Sundarakantham, K., &amp; Shalinie, S. M. (1970). DDAM: Detecting ddos attacks using machine learning approach. Retrieved from https://link.springer.com/chapter/10.1007/978-981-13-1132-1_21

[3]. Najafimehr, M., Zarifzadeh, S., &amp; Mostafavi, S. (2022). Retrieved from https://link.springer.com/article/10.1007/s11227-021-04253-x

[4]. Najar, A. A., &amp; Naik, S. M. (2022). DDoS attack detection using MLP and Random Forest Algorithms - International Journal of Information Technology. Retrieved from https://link.springer.com/article/10.1007/s41870-022-01003-x

[5]. Roopak, M., Tian, G. Y., &amp; Chambers, J. (2022). Multi-objective-based feature selection for ddos attack detection in IOT networks. Retrieved from https://pure.hud.ac.uk/en/publications/multi-objective-based-feature-selection-for-ddos-attack-detection