DDOS Attack Detection and Classification Using Machine Learning

Prof. Rahul Papalkar[a], Purva Patil[a]*, Poloumi Kha[a], Shivam Tiwari[a],
Prof. Pandurang Mohite[a], Prof. Rajkumar Sawant[a]

ABSTRACT: The Internet has brought significant changes to the world, but it has also brought numerous cyberattacks. One of the most dangerous attacks is the (DDoS) Distributed Denial of Services attack, which can halt the normal functionality of services in all computing environments. The DDoS attacks are classified by the position of pivotal attacks that undermine the network's functionality. These attacks have become sophisticated and continue to grow rapidly, making it challenging to describe and address them. These malicious attacks are caused by a network of computers infected with special malware, known as a "botnet," which bombards a server with traffic until it collapses under the strain. The Mirai botnet is one such example, which is largely made up of internet-connected devices such as digital cameras and the DVR players. In our proposed system, we propose machine learning grounded attack discovery from traffic data. This module contains three corridors first, preprocessing; second, detecting the traffic as licit or not using machine learning (CATBOOST and Random Forest); and third, classifying the attack using machine learning (CATBOOST and Random Forest). Eventually, estimate and compare the performances of CATBOOST and Random Forest for traffic classification and attack classification. In the preprocessing step of traffic data, the data is cleaned and filtered to remove any noise or irrelevant information. The performance of the model is evaluated based on metrics such as accuracy, precision, recall, and F1-score. Appropriate data preprocessing can improve the accuracy of the machine learning model. The evaluation of the performance of the model includes metrics such as accuracy, precision, recall, and F1-score.

KEYWORDS: CATBOOST, DDOS Attack, KDD Dataset, Random Forest.

[A] Bharati Vidyapeeth deemed to be University, department of engineering and technology, Navi Mumbai.

*Corresponding Author

E-mail: rrpapalkar@bvucoep.edu.in

E-mail: purvapatil8081@gmail.com

E-mail: poulomikha2000@gmail.com

E-mail: at9324510@gmail.com

E-mail: ptmohite@bvucoep.edu.in

E-mail: rajkumar.sawant@bvucoep.edu.in

DOI:

INTRODUCTION:

A distributed denial of service (DDoS) attack is a type of cyberattack that involves multiple compromised devices, often referred to as a "botnet," which are used to flood a targeted system with traffic. The attacker instructs the botnet to overwhelm the victim's servers and devices with traffic generated by the compromised devices. The flood of incoming messages, connection requests, or malformed packets to the targeted system forces them to slow down or even crash and shut down, thereby denying service to legitimate users or systems. The DDoS attacks are often carried out by attackers who want to disrupt the services of a particular website or online service, cause financial harm, or steal sensitive information.

A DDoS attack can be devastating for organizations, as it can result in significant downtime, loss of revenue, and damage to their reputation. Therefore, it is essential to have effective DDoS mitigation measures in place to protect against these attacks. The proposed system works in three parts. First, preprocessing second, detecting the traffic as licit or not using machine learning (CATBOOST and Random Forest); and third, classifying the attack using machine learning (CATBOOST and Random Forest). Eventually, estimate and compare the performances of CATBOOST and Random Forest for traffic classification and attack classification.

This paper focuses on detecting and classifying the "DDOS" attacks using machine learning algorithms. The study uses a (ML) Machine Learning approach to predict a DDoS attack with a maximum accuracy of 99.997%, which was obtained by using CATBOOST. The paper uses a set of eight supervised machine learning algorithms to detect DDoS attacks and found the best model in terms of accuracy.

LITERATURE REVIEW:

TABLE I
LITERATURE REVIEW

Sr. no	PAPER TITLE	PUBLICATION YEAR	PAPER OUTCOME
1	DDoS Attack Detection Using Recurrent Neural Networks with LSTM.	2019	The study showed that the proposed model outperformed traditional machine learning algorithms such as Random Forest and Support Vector Machines in terms of accuracy, precision, and recall.
2	A hybrid approach for ddos attack detection based on machine learning and deep learning technique	2020	The study showed that the proposed approach achieved high accuracy and F1-score, outperforming traditional machine learning algorithms such as Random Forest and Naive Bayes.
3	Comparative Study of Various Machine Learning Approaches for DDoS Attack Detection	2021	The study showed that Random Forest achieved the highest accuracy among the tested algorithms.

Gap analysis:

1. Ddos traffic can have a wide range of characteristics and patterns, some of which may be categorical in nature (e.g., source ip address, destination port, protocol type). Catboost is known for its ability to handle categorical features effectively and efficiently, which can improve the accuracy and performance of the algorithm.

2. Random forest is an ensemble learning algorithm that combines multiple decision trees to improve the accuracy and reduce the risk of overfitting. This can be useful for ddos classification and detection as it can help capture the complex and non-linear relationships between the features and the attack patterns.

3. Catboost and random forest are both scalable algorithms that can handle large and high-dimensional datasets efficiently. This can be useful for ddos classification and detection as it can help reduce the computational time and resource requirements, especially in real-time detection scenarios.

METHODOLOGY:

This study uses KDD data set in order to train the algorithm and classify DDOS Attacks based on its unique features. The dataset contains many network connection records that were captured over a period, along with labels indicating whether each connection was a normal or abnormal connection.[4] The dataset contains a total of 41 features, including various attributes of the network connection such as the source and destination IP addresses, protocol type, service type, and more. The dataset is divided into three subsets: a training set, a test set, and a validation set.

In ML, the KDD dataset is typically pre-processed and transformed to create a set of features that can be used to train and test a classifier. The features can include a variety of network traffic statistics, such as the number of packets, bytes, and connections, as well as various protocol-related features, such as the type of protocol, source and destination IP addresses, and source and destination ports.

Once the feature set is defined, various ML algorithms can be trained and tested on the KDD dataset to evaluate their performance in detecting network intrusions.

The KDD Cup '99 dataset is a widely used dataset in the field of network intrusion detection. It contains a large number of network traffic records that are labeled as either normal or malicious traffic. In the proposed system dataset is divided into three parts:

1. Normal Traffic: This part of the dataset contains records of normal network traffic that are not associated with any malicious activity. This includes records of web browsing, email communication, file transfers, and other legitimate network activities.

2. Malicious Traffic: This part of the dataset contains records of network traffic that are associated with various types of malicious activity. This includes records of port scanning, denial-of-service attacks, buffer overflow attacks, and other types of network-based attacks.

3. DDoS Traffic: This part of the dataset contains records of network traffic that are specifically associated with distributed denial-of-service (DDoS) attacks. DDoS attacks are a type of attack where a large number of computers are used to flood a target server or network with traffic, causing it to become overloaded and unavailable to legitimate users.

Each record in the dataset contains information about various features of the network traffic, such as packet size, source and destination IP addresses, protocol type, and more. The dataset is often used to train and evaluate machine learning models for network intrusion detection and classification, including models for DDoS detection and classification.

CatBoost and Random forest are two popular machine learning algorithms that can be used for DDoS detection and classification.[4] Both algorithms are capable of handling large amounts of data and dealing with noisy and unbalanced datasets, making them suitable for this task.

1. CatBoost

CatBoost is a machine learning algorithm that is used for classification and regression tasks. It is based on gradient boosting and is known for its ability to handle categorical features and missing values in the data.

2. Random forest

Random Forest is a popular machine learning algorithm that is used for classification, regression, and other tasks. It is based on the concept of ensemble learning, which combines multiple decision trees to create a more powerful model.

3. CatBoost and Random forest for DDoS detection and classification:

   a. Data Preparation: Collect network traffic data and label it as either normal or malicious traffic. The dataset should be divided into a training set and a test set.

   b. Feature Selection: Select the most relevant features that can help distinguish between normal and malicious traffic. Some of the features that can be used for DDoS detection and classification include packet size, packet rate, source and destination IP addresses, protocol type, and more.

   c. Random Forest Model Creation: Create a random forest model using the training dataset. The model will be trained to classify network traffic patterns as either normal or malicious. The number of trees in the forest, the depth of the trees, and other parameters can be adjusted to optimize the performance of the model.

   d. Model Evaluation: Evaluate the performance of the random forest model using the test dataset. The evaluation metrics can include accuracy, precision, recall, F1-score, and ROC-AUC.

   e. CatBoost Model Creation: Create a CatBoost model using the same training dataset. CatBoost is a gradient boosting algorithm that can automatically handle categorical variables, making it particularly suitable for datasets with a mix of categorical and continuous variables.

   f. Model Evaluation: Evaluate the performance of the CatBoost model using the test dataset. The evaluation metrics can include accuracy, precision, recall, F1-score, and ROC-AUC.

   g. Comparison and Fine-tuning: Compare the performance of the random forest and CatBoost models and fine-tune the parameters of the models as needed to optimize their performance.

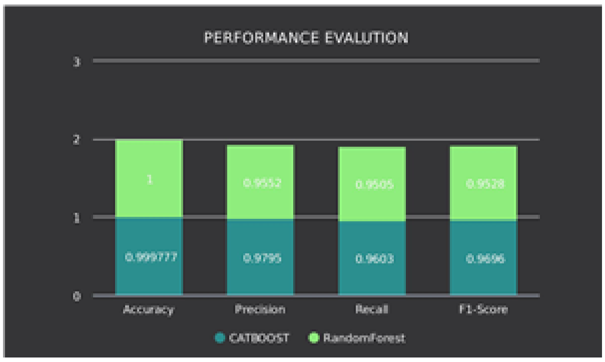


Fig. 1. Comparison between performance of CatBoost and Random_Forest models based on confusion matrix.

The above graph demonstrates the performance of each ML model based on accuracy, precision, recall and f1 score. By comparing the values of these metrics for both random forest and CatBoost models, we can determine which model performs better for DDoS detection and classification.

To compare the performance of CatBoost and Random forest models for DDoS detection and classification in terms of accuracy of prediction in the proposed system we are making use of confusion matrix.

4. Confusion matrix

A confusion matrix is a table that evaluates the performance of a classification model by comparing the predicted class labels of the model with the true class labels of the dataset. It actually shows the number of true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN) for a given classification task. The elements of the confusion matrix are as follows: TP represents the number of instances that are correctly predicted as positive by the model, FP represents the number of instances that are incorrectly predicted as positive by the model, TN represents the number of instances that are correctly predicted as negative by the model, and FN represents the number of instances that are incorrectly predicted as negative by the model. The confusion matrix is a summarized table used to assess the performance of a classification model.

From the confusion matrix, various evaluation metrics can be calculated such as accuracy, precision, recall, F1-score.

a. Accuracy: It measures the proportion of correctly classified instances out of the total instances. Higher accuracy indicates better performance.
Formula: -
(TP + TN) / (TP + TN + FP + FN)[1]

b. Precision: It measures the proportion of true positive instances out of the total instances classified as positive. Higher precision indicates fewer false positives.
Formula: -
TP / (TP + FP)[1]

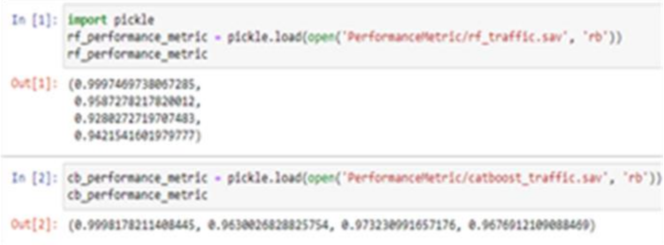
c. Recall: It measures the proportion of true positive instances out of the total positive instances. Higher recall indicates fewer false negatives.
Formula: -
TP / (TP + FN)[1]

d. F1-score: It is the harmonic mean of precision and recall. It provides a balanced measure of the model's accuracy. A higher F1-score indicates better performance.
Formula: -
2 * Precision * Recall / (Precision + Recall)[1]

Overall, the confusion matrix is a useful tool for evaluating the performance of a classification model and can provide insights into the model's strengths and weaknesses. It can help in making informed decisions about how to optimize the model's performance.

RESULT AND CONCLUSION:

The proposed model uses KDD dataset to train and test the algorithm and then predicted the traffic as normal traffic , malicious traffic and ddos traffic(attack).If the traffic is identified as ddos then the proposed model further classifies it into type of ddos attack i.e back ,land ,Neptune ,smurf ,teardrop using Catboost and Random_Forest algorithms.



```
In [1]: import pickle
        rf_performance_metric = pickle.load(open('PerformanceMetric/rf_traffic.sav', 'rb'))
        rf_performance_metric

Out[1]: (0.9997469738067285,
         0.9587278217820012,
         0.9280272719707483,
         0.9421541601979777)

In [2]: cb_performance_metric = pickle.load(open('PerformanceMetric/catboost_traffic.sav', 'rb'))
        cb_performance_metric

Out[2]: (0.9998178211408445, 0.9630026828825754, 0.9732309916571 76, 0.9676912109088469)
```

Fig. 2. Performance metrics of CatBoost and Random forest

TABLE 2
PERFORMANCE EVALUATION

Parameters	CatBoost	Random forest
Accuracy	0.999777	1.000000
Precision	0.9795	0.9552
Recall	0.9603	0.9505
F1-score	0.9696	0.9528

The model is experimented using two classification algorithms CatBoost and Random forest in order to predict and classify DDOS attack. Figure given below shows the performance matrix of the algorithms respectively

From the experimental results given in table, we can see that the Random_Forest algorithm produced the least accurate prediction compared to CatBoost algorithm. It was observed that the classification accuracy among the algorithm has minimium difference. The Random_Forest algorithm provides the lowest overall classification accuracy.[1]

REFERENCE:

1. C M Nalayinil, Dr Jeeva Katiravan - Detection of DDoS Attack using Machine Learning Algorithms. JETIR Research. 2022.
2. Kim, D., Lee, J., Jeon, J., Kim, H., & Park, J. DDoS Attack Detection Using Recurrent Neural Networks with LSTM. International Conference on Information and Communication Technology Convergence (ICTC) pp. 457-460. IEEE 2019.
3. Gao, X., Hu, J., Li, X., Li, C., & Li, Z - A Hybrid Approach for DDoS Attack Detection Based on Machine Learning and Deep Learning Techniques. IEEE Access, 8, 166111-166121. 2020.
4. Das, S. K., Pradhan, S. K., Mohapatra, S., & Patra, M. R. - Comparative Study of Various

Machine Learning Approaches for DDoS Attack Detection. In Advances in Computer Communication and Computational Sciences (pp. 35-45). Springer. (2021).