Detection of Different DDoS Attacks Using Machine Learning Classification Algorithms

Article *in* Ingénierie des systèmes d information · October 2021

DOI: 10.18280/isi.260505

2 authors:

Dasari Kishore
Kalasalingam Academy of Research and Education
29 PUBLICATIONS **173** CITATIONS
SEE PROFILE

Nagaraju Devarakonda
VIT-AP University
85 PUBLICATIONS **562** CITATIONS
SEE PROFILE

Ingénierie des Systèmes d'Information
Vol. 26, No. 5, October, 2021, pp. 461-468
Journal homepage: http://iieta.org/journals/isi

Detection of Different DDoS Attacks Using Machine Learning Classification Algorithms

Kishore Babu Dasari[1*], Nagaraju Devarakonda[2]

[1] Department of CSE, Acharya Nagarjuna University, Guntur 522510, Andhra Pradesh, India
[2] School of Computer Science and Engineering, VIT-AP University, Amaravati 522237, India

Corresponding Author Email: dasari2kishore@gmail.com

https://doi.org/10.18280/isi.260505

Received: 23 September 2021
Accepted: 25 October 2021

Keywords:
CICDDoS2019, classification algorithms, DDoS attacks

ABSTRACT

Cyber attacks are one of the world's most serious challenges nowadays. A Distributed Denial of Service (DDoS) attack is one of the most common cyberattacks that has affected availability, which is one of the most important principles of information security. It leads to so many negative consequences in terms of business, production, reputation, data theft, etc. It shows the importance of effective DDoS detection mechanisms to reduce losses. In order to detect DDoS attacks, statistical and data mining methods have not been given good accuracy values. Researchers get good accuracy values while detecting DDoS attacks by using classification algorithms. But researchers, use individual classification algorithms on generalized DDoS attacks. This study used six machine learning classification algorithms to detect eleven different DDoS attacks on different DDoS attack datasets. We used the CICDDoS2019 dataset which is collected from the Canadian Institute of Cyber security in this study. It contains eleven different DDoS attack datasets in CSV file format. On each DDoS attack, we evaluated the effectiveness of the classification methods Logistic regression, Decision tree, Random Forest, Ada boost, KNN, and Naive Bayes, and determined the best classification algorithms for detection.

1. INTRODUCTION

A Distributed Denial of Service (DDoS) attacks [1] to prevent legitimate users from accessing an online service or applications by suspending the hosting servers. To generate the attack, the attackers use numerous compromised or controlled sources to generate massive amounts of packets or requests. These requests cause the target system to become overburdened, causing it to operate poorly and become inaccessible to legitimate users.

Based on TCP/UDP protocols, DDoS attacks are divided into reflection-based attacks and exploit-based attacks.

1.1 Reflection-based DDoS attacks

The attacker's identity is hidden in reflection-based DDoS attacks because legitimate third-party components are used. Attackers send packets to reflector servers with the target victim's IP address as the source IP address to overwhelm the victim with response packets. The Transmission Control Protocol (TCP), the User Datagram Protocol (UDP), or a combination can be used in these attacks. SSDP and MSSQL are TCP-based attacks, while NTP TFTP and CharGEN are UDP-based attacks. SNMP, NETBIOS, LDAP, and DNS are examples of attacks that can be carried out using either TCP or UDP.

Simple Service Discovery Protocol (SSDP) [2] amplification floods can be sent to a target system using Universal Plug and Play (UPnP) devices which can access the network devices. *Microsoft SQL (MSSQL)* [3] Server Resolution protocol is used for database instance enumeration service. The service is vulnerable to reflection-based DDoS attacks. Large response messages consume server resources, disrupting the service.

The Network Time Protocol (NTP) [4] is also amplified by sending small packets to internet-connected devices running NTP with a fake IP address of the target. For downloading and uploading files, the Trivial File Transfer Protocol (TFTP) [5] is utilized. A buffer overflow may occur if the attacker tries to read/write excessively long names from/to the server. It's also susceptible to flaws in the format strings. In this vulnerability, the attacker sends a predetermined string as a file name, which can be used to execute malicious code or leak protected data. CHARGEN is used as an amplifier in a Character Generator Protocol (CharGEN) attack [6], which sends small request packets to the target system with a spoofed IP address.

The attacker uses the Simple Network Management Protocol (SNMP) [7] to send a huge number of SNMP queries to a huge number of connected devices, each of which responded with the falsified address. As more devices respond, the attack volume rises until the target network is brought down by the cumulative volume of these SNMP responses. *NetBIOS* [8] is to allow applications on different computers to communicate and establish sessions to access shared resources and communicate with one another through a local area network. On a this-aware network, the NetBIOS Name Service (NBNS) allows for hostname and address mapping. With the lack of an authentication technique in the NetBIOS TCP/IP protocols, workstations running NetBIOS services are vulnerable to spoofing attacks. An attacker might compel a victim system to delete its legitimate name from its name table and not reply to further NetBIOS requests by delivering spoofed "Name Release" or "Name Conflict" messages to it. A denial-of-service attack occurs when the victim is unable to

communicate with other NetBIOS hosts. In *Lightweight Directory Access Protocol (LDAP)* DDoS attack [8], the attacker sends an LDAP request to an LDAP server to produce large replies, with a spoofed sender IP address. *Domain Name System (DNS)* [9] amplification is a reflection-based DDoS attack, which manipulates domain name systems and makes them flood the target system with large quantities of UDP packets, which bring down the target servers.

1.2 Exploitation-based DDoS attacks

These attacks can also be carried out utilizing the exploitation of transport layer protocols. SYN flood is TCP-based, and UDP-Lag and UDP flood are UDP-based exploitation attacks.

SYN flood [7] attack exploits TCP three-way handshake by sending SYN packets rapidly to the victim server. It consumes network bandwidth and deteriorates system performance. The UDP-Lag [10] attack attempts to break the client-server connection. It was carried out using either a lag switch or a network-based program to consume other users' bandwidth. The attacker launches a UDP flood [8] attack by rapidly transmitting a large number of UDP packets to random ports on the remote server. It consumes network bandwidth and deteriorates system performance.

The rest of this paper contains methodology in section 2, results and discussion in section 3, and conclusion in section 4.

2. METHODOLOGY

2.1 Dataset

In this paper, we evaluate classification models on the CICDDoS2019 dataset. The CICDDoS2019 dataset is chosen for this study because it has been evaluated to fill in the gaps in existing DDoS attack datasets. It contains eleven different DDoS attacks datasets [11]. Each data set contains 88 features and millions of records.

2.2 CICFlowMeter

CICFlowMeter is also known as ISCXFlowMeter. It is a bi-flow generator and analyzer for Ethernet network traffic. It can calculate network traffic features in both the forward and backward directions. It generates CSV files from packet capture (PCAP) files.

2.3 Data preprocessing

Preprocessing prepares the data in such a way that it is ready for the training model. First, delete six socket features which are not influencing the target because they differ from network-to-network values. Then, in order to acquire more accurate results, records with missing or infinite are removed. Some machine learning algorithms [12] working with numerical values, so BENIGN and attack labels are encoded with 0 and 1 binary values respectively. Standardize the data using StandardScaler to reduce the training time.

2.4 Classification algorithms

Regression and Classification Algorithms are the two primary categories of supervised machine learning algorithms used for prediction. Regression techniques predict the output continuous values, while classification methods [13] predict the output categorical values. The main objective of this research is prediction of categorical values of Benign and DDoS attacks of target labels in the CICDDoS2019 dataset. In this research, machine learning classification algorithms used to detect DDoS attacks on CICDDoS2019 dataset. Training and testing are two steps in the classification process. Logistic regression, Decision tree, Random Forest, K-Nearest Neighbor, Naive Bayes, and AdaBoost are some of the most common algorithms in the classification. These methods are significantly more accurate than conventional methods for detecting a DDoS attack, in addition to being faster.

2.4.1 Logistic regression

Logistic regression [14] is a classification algorithm for predicting binary classes. The value of the outcome or target variable is categorical. It predicts the probability of binary classes occurring using a logistic function. The logistic function also called the sigmoid function.

Logistic Function:

$$\emptyset(z) = \frac{1}{1 + e^{-z}}$$

$$y = \beta + \beta_1 X_1 + \beta_2 X_2 + \ldots\ldots + \beta_n X_n$$

Here y is the dependent variable and X_1, X_2,...., X_n are dependent variables.

2.4.2 Decision tree

The Decision tree [15] is a tree-structured classifier, where internal nodes hold dataset features, branches provide decision rules, and the leaf nodes contain class labels. The features and criteria may vary depending on the data and the problem's complexity, but the general concept remains the same. Based on the feature set, a decision tree makes a series of decisions to produce an outcome.

2.4.3 Random forest

Random forest [16] is a collection of decision trees trained on different dataset subsets and then averaged to increase predictive accuracy. It is created randomly with a collection of decision trees. Here each node selects a set of features at random to calculate the outcome. The output of individual decision trees is combined in the random forest to produce the outcome.

2.4.4 K-Nearest neighbors

The k-nearest neighbors (KNN) [17] is a supervised machine learning algorithm. It is a similarity-based classifier that assumes that every data point that's close to another is in the same class. The standard Euclidean distance between instances x and y is:

$$d(x, y) = \sqrt{\sum_{k=1}^{n} (x_k - y_k)^2}$$

Here n indicates the total number of features, x_k, y_k are the k^{th} features in x and y respectively.

2.4.5 Naive Bayes

Naive Bayes [18-20] is a supervised machine learning algorithm for classification that is based on the Bayes theorem. Bayes' theorem states the relationship between dependent class variable y and independent feature vector X_1, X_2,...,X_n:

$$P(y/X_1X_2 \ldots\ldots X_n) = \frac{P(y)P(X_1X_2 \ldots\ldots X_n)}{P(X_1X_2 \ldots\ldots X_n)}$$

2.4.6 AdaBoost

AdaBoost (Adaptive Boosting) [21] is a machine learning ensemble model for constructing a strong classifier from a collection of weak classifiers. In supervised learning, boost is used to reduce bias and variance. It works on the principle of learners growing sequentially. It generates several decision trees during the training time. Resulting in the creation of the first decision tree, the records that were mistakenly categorized are given precedence and transmitted as input to the second model. The process is repeated until a set of base learners to work with.

We executed all experiments on Google Colab notebook with 12GB Ram and TPU hardware accelerator.

3. RESULTS AND DISCUSSION

The efficiency of the machine learning classification algorithms is measured with accuracy, precision, recall, F1 score, specificity, and ROC score evaluation metrics.

There are four important terms used in evaluation metrics.

True Positives (TP): In this case, both the predicted and actual values are Positive.

True Negatives (TN): Predicted, and actual values are Negative in this case.

False Positives (FP): In this case, the actual value is Negative but the predicted value is Positive.

False Negatives (FN): In this case, the actual value is Positive but the predicted value is Negative.

3.1 Confusion matrix

The confusion matrix is a key concept in machine learning classification performance. It represents actual and predicted values in tabular form. Predicted and actual values are represented by rows and columns respectively in the table.

3.2 Accuracy

Accuracy is the ratio of the number of correct predictions to the number of all predictions by the classifier. Accuracy tells the proposition of correct predictions out of total predictions.

$$ACCURACY = \frac{TP + TN}{TP + TN + FP + FN}$$

3.3 Precision

Precision is the ratio between the number of True Positives and the number of predicted positives by the classifier. Precision tells the proposition of predicted trues are actually true.

$$PRECISION = \frac{TP}{TP + FP}$$

3.4 Recall

Recall or True Positive Rate (TPR) is the ratio between the number of True Positives and the number of all relevant samples. Recall tells the proposition of actually trues are predicted as true.

$$RECALL/TPR/SENSITIVITY = \frac{TP}{TP + FN}$$

3.5 F1 score

F1 score is a harmonic mean of precision and recall.

$$F1\ Score = \frac{2 * PRECISION * RECALL}{PRECISION + RECALL}$$

3.6 Specificity

Specificity is the ratio between the number of True Negatives and the number of all relevant samples. It is also called True Negative Rate (TNR).

$$SPECIFICITY/TNR = \frac{TN}{TN + FP}$$

3.7 AUC-ROC curve

AUC-ROC (Area Under the Curve-Receiver Operating Characteristics) curve is the most important metric for evaluating the effectiveness of classifiers. The ROC curve plots True Positive Rate (TPR) on the y-axis and False Positive Rate (FPR) on the x-axis. AUC score is between 0 and 1. The classification model can accurately distinguish all classes accordingly if the AUC score is 1. The classification model would predict all positives to be negative and all negatives to be positives if the AUC score is 0.

$$FPR = \frac{FP}{FP + TN}$$

3.8 Cross fold validation

For evaluating machine learning models, cross-validation is a single parameter (k) re-sampling approach. The parameter specifies how many groups the sample data must be divided into. This validation process data set was shuffled and divided into k groups. To test a group data set, consider remaining groups as a training data set. Fit the model like this for training and tests. In this paper, we performed cross-validation with k=5 and calculated accuracy of mean and standard deviation scores.

Tables demonstrate the classification algorithm evaluation metrics accuracy, cross-fold validation, precision, recall, F score, specificity, and ROC-AUC scores for DDOS attack detection.

Table 1 shows the classification algorithms evaluation metrics on the DrDoS_MSSQL dataset. Logistic Regression (LR), AdaBoost, KNN, Naïve Bayes (NB) give better accuracy than others. All classification algorithms give the same precision, recall, F-score values. LR and NB give the best specificity values. LR, NB, and AdaBoost give the best ROC-AUC scores.

Table 2 shows the classification algorithms evaluation

metrics on the DrDoS_SSDP dataset. AdaBoost gives the best accuracy, next KNN gives better accuracy. LR and NB also give good accuracy. LR and NB give the best precision. AdaBoost gives the best recall. AdaBoost, KNN gives the best F-score. LR and NB give the best specificity values. AdaBoost gives the best and LR and NB give better ROC-AUC scores.

Table 3 shows the classification algorithms evaluation metrics on the DrDoS_NTP dataset. LR gives the best accuracy, best precision, best F-score, and best specificity. AdaBoost gives the best recall and best ROC-AUC, but it gives the worst specificity value. NB gives better values in all evaluation metrics.

Table 4 shows evaluation metrics of the classification algorithms on the DrDoS_TFTP attack dataset. LR and NB give the best accuracy, best precision, and best specificity values. AdaBoost gives the best ROC-AUC score. LR, AdaBoost, KNN, and NB give the best values in recall and F-score.

Table 5 shows the classification algorithms evaluation metrics on the DrDoS_DNS attack dataset. LR and NB give the best accuracy, best precision, best specificity values, and better ROC-AUC score. AdaBoost and KNN give the best recall and best F-score values. AdaBoost gives the best ROC-AUC score.

Table 6 shows evaluation metrics of the classification algorithms on the DrDoS_LDAP attack dataset. LR and NB give the best accuracy, best precision, best F-score, and best specificity values. AdaBoost and KNN give the best recall values. NB gives the best ROC-AUC score.

Table 7 shows evaluation metrics of the classification algorithms on the DrDoS_NetBIOS attack dataset. LR, AdaBoost, KNN, and NB give the best accuracy and best F-score values. LR and NB give the best precision and specificity values. AdaBoost gives the best recall and best ROC-AUC score values.

Table 1. Evaluation results of DrDoS_MSSQL attack detection

Classification Algorithms	Accuracy (%)	Precision	Recall	F-score	Crossfold Validation Mean (STD) scores (%)	Specificity	ROC_AUC Score
Logistic Regression	99.97	0.9999	0.9998	0.9999	99.9739 (0.0027)	0.87	0.9691
Decision Tree	99.82	0.9999	0.9984	0.9991	99.8532 (0.0042)	0.66	0.8291
Random Forest	99.82	0.9999	0.9984	0.9991	99.8538 (0.0039)	0.66	0.9417
AdaBoost	99.97	0.9999	0.9999	0.9999	99.9710 (0.0021)	0.66	0.9643
KNN	99.97	0.9998	0.9999	0.9999	99.9631 (0.0016)	0.64	0.9396
Naive Bayes	99.97	0.9999	0.9998	0.9999	99.9739 (0.0027)	0.87	0.9691

Table 2. Evaluation results of DrDoS_SSDP attack detection

Classification Algorithms	Accuracy (%)	Precision	Recall	F-score	Crossfold validation Mean (STD) scores (%)	Specificity	ROC_AUC Score
Logistic Regression	99.95	0.9999	0.9995	0.9997	99.9569 (0.0036)	0.82	0.9413
Decision Tree	99.91	0.9998	0.9992	0.9995	99.9205 (0.0016)	0.47	0.7325
Random Forest	99.91	0.9998	0.9993	0.9995	99.9204 (0.0016)	0.47	0.9115
AdaBoost	99.97	0.9997	0.9999	0.9998	99.9728 (0.0008)	0.19	0.9423
KNN	99.96	0.9998	0.9998	0.9998	99.9698 (0.0027)	0.37	0.9086
Naive Bayes	99.95	0.9999	0.9995	0.9997	99.9569 (0.0036)	0.82	0.9413

Table 3. Evaluation results of DrDoS_NTP attack detection

Classification Algorithms	Accuracy (%)	Precision	Recall	F-score	Crossfold Validation Mean (STD) scores (%)	Specificity	ROC_AUC Score
Logistic Regression	99.66	0.9989	0.9976	0.9983	99.6490 (0.0055)	0.91	0.9601
Decision Tree	98.70	0.9976	0.9892	0.9934	98.7887 (0.0233)	0.80	0.8885
Random Forest	99.32	0.9976	0.9955	0.9966	99.1769 (0.0572)	0.80	0.9561
AdaBoost	99.35	0.9941	0.9993	0.9967	99.3448 (0.0247)	0.50	0.9705
KNN	99.64	0.9984	0.9980	0.9982	99.6241 (0.0051)	0.86	0.9623
Naive Bayes	99.65	0.9985	0.9980	0.9982	99.6311 (0.0037)	0.87	0.9668

Table 4. Evaluation results of DrDoS_TFTP attack detection

Classification Algorithms	Accuracy (%)	Precision	Recall	F-score	Crossfold Validation Mean (STD) scores (%)	Specificity	ROC_AUC Score
Logistic Regression	99.95	0.9997	0.9998	0.9997	99.9504 (0.0014)	0.82	0.9240
Decision Tree	99.81	0.9995	0.9986	0.999	99.8500 (0.0109)	0.67	0.8323
Random Forest	99.81	0.9995	0.9986	0.999	99.8507 (0.0101)	0.67	0.9117
AdaBoost	99.94	0.9996	0.9998	0.9997	99.9350 (0.0068)	0.74	0.9566
KNN	99.94	0.9996	0.9998	0.9997	99.9467 (0.0039)	0.73	0.9119
Naive Bayes	99.95	0.9997	0.9998	0.9997	99.9504 (0.0014)	0.82	0.9520

Table 5. Evaluation results of DrDoS_DNS attack detection

Classification Algorithms	Accuracy (%)	Precision	Recall	F-score	Crossfold Validation Mean (STD) scores (%)	Specificity	ROC_AUC Score
Logistic Regression	99.90	0.9998	0.9992	0.9950	99.8944 (0.0074)	0.83	0.9768
Decision Tree	98.43	0.9995	0.9848	0.9921	98.6987 (0.0180)	0.61	0.8018
Random Forest	98.47	0.9995	0.9852	0.9923	98.7169 (0.0155)	0.61	0.9240
AdaBoost	99.89	0.9994	0.9995	0.9994	99.8864 (0.0050)	0.53	0.9775
KNN	99.89	0.9994	0.9995	0.9995	99.8957 (0.0069)	0.55	0.9066
Naive Bayes	99.90	0.9998	0.9992	0.9995	99.8944 (0.0074)	0.83	0.9768

Table 6. Evaluation results of DrDoS_LDAP attack detection

Classification Algorithms	Accuracy (%)	Precision	Recall	F-score	Crossfold Validation Mean (STD) scores (%)	Specificity	ROC_AUC Score
Logistic Regression	99.92	0.9998	0.9994	0.9996	99.9210 (0.0023)	0.84	0.9535
Decision Tree	99.59	0.9996	0.9963	0.9979	99.6342 (0.0080)	0.66	0.8303
Random Forest	99.59	0.9996	0.9963	0.9979	99.6358 (0.0069)	0.66	0.9440
AdaBoost	99.91	0.9994	0.9996	0.9995	99.8996 (0.0049)	0.53	0.9501
KNN	99.91	0.9995	0.9996	0.9995	99.9193 (0.0033)	0.62	0.9334
Naive Bayes	99.92	0.9998	0.9994	0.9996	99.9210 (0.0023)	0.84	0.9552

Table 7. Evaluation results of DrDoS_NetBIOS attack detection

Classification Algorithms	Accuracy (%)	Precision	Recall	F-score	Crossfold Validation Mean (STD) scores (%)	Specificity	ROC_AUC Score
Logistic Regression	99.96	0.9999	0.9997	0.9998	99.9555 (0.0028)	0.82	0.9430
Decision Tree	99.90	0.9998	0.9992	0.9995	99.9124 (0.0037)	0.60	0.8011
Random Forest	99.90	0.9998	0.9992	0.9995	99.9119 (0.0024)	0.61	0.9285
AdaBoost	99.96	0.9996	1.0	0.9998	99.9559 (0.0012)	0.27	0.9502
KNN	99.96	0.9998	0.9998	0.9998	99.9698 (0.0027)	0.56	0.9186
Naive Bayes	99.96	0.9999	0.9997	0.9998	99.9555 (0.0028)	0.82	0.9430

Table 8. Evaluation results of DrDoS_SNMP attack detection

Classification Algorithms	Accuracy (%)	Precision	Recall	F-score	Crossfold Validation Mean (STD) scores (%)	Specificity	ROC_AUC Score
Logistic Regression	99.95	0.9999	0.9996	0.9998	99.9506 (0.0030)	0.85	0.9017
Decision Tree	99.77	0.9998	0.9979	0.9988	99.7966 (0.0038)	0.6	0.7981
Random Forest	99.77	0.9998	0.9979	0.9988	99.7974 (0.0047)	0.6	0.9176
AdaBoost	99.95	0.9997	0.9997	0.9998	99.9512 (0.0014)	0.32	0.9726
KNN	99.97	0.9998	0.9999	0.9998	99.9631 (0.0016)	0.55	0.9026
Naive Bayes	99.95	0.9999	0.9996	0.9998	99.9506 (0.0030)	0.85	0.9736

Table 9. Evaluation results of DrDoS_SYN attack detection

Classification Algorithms	Accuracy (%)	Precision	Recall	F-score	Crossfold Validation Mean (STD) scores (%)	Specificity	ROC_AUC Score
Logistic Regression	99.98	0.9999	0.9999	0.9999	99.9787 (0.0023)	0.81	0.9433
Decision Tree	99.97	0.9999	0.9998	0.9998	99.9730 (0.0029)	0.6	0.8024
Random Forest	99.97	0.9999	0.9998	0.9998	99.9731 (0.0027)	0.6	0.9505
AdaBoost	99.98	0.9998	1.0	0.9999	99.9750 (0.0020)	0.42	0.9505
KNN	99.98	0.9999	0.9999	0.9999	99.9770 (0.0013)	0.68	0.9505
Naive Bayes	99.98	0.9999	0.9999	0.9999	99.9787 (0.0023)	0.81	0.9433

Table 8 shows evaluation metrics of the classification algorithms on the DrDoS_SNMP attack dataset. KNN gives the best accuracy and best recall values. LR and NB give the best precision and specificity values. LR, AdaBoost, KNN, and NB give the best F-score value. The finest ROC-AUC score value is given by NB.

Table 9 shows the classification algorithms evaluation metrics on the DrDoS_Syn attack dataset. LR, AdaBoost, KNN, and NB give the best accuracy and best F-score values. LR and NB give the best specificity values. AdaBoost gives the best recall value. KNN gives the best ROC-AUC score value. All algorithms give the best precision value.

Table 10 shows the classification algorithms evaluation metrics on the DrDoS_UDP attack dataset. AdaBoost gives the best accuracy, best recall, best F-score values, but it gives poor specificity values. Both LR and NB give the best precision and

best specificity values. In the ROC-AUC score, LR gives the best value, AdaBoost and NB give better results.

Table 11 shows the classification algorithms evaluation metrics on the DrDoS_UDPLAG attack dataset. LR, AdaBoost, KNN, and NB give the best accuracy and F-score values. LR, AdaBoost, and NB give the best precision values. AdaBoost gives the best specificity and ROC-AUC score. LR and NB give better values in both specificity and ROC-AUC scores.

Figure 1 to Figure 11 shows the Roc_Auc score curves of the classification algorithms on eleven different DDoS attacks. In ROC area blue line curve going along 45 degrees diagonal line is called baseline curve, it shows random classifier. Curves above the base line shows better performance, curves below the base line shows poor performance. In ROC_AUC curves, Top-left corner closer curves give the best performance in classification. Hence, Logistic regression, Ada boost and Naive Bayes classifiers show the best performance, KNN and Random Forest classifiers shows moderate performance, while Decision tree classifier shows poor performance in all attacks.

Table 10. Evaluation results of DrDoS_UDP attack detection

Classification Algorithms	Accuracy (%)	Precision	Recall	F-score	Crossfold Validation Mean (STD) scores (%)	Specificity	ROC_AUC Score
Logistic Regression	99.92	0.9999	0.9993	0.9996	99.9238 (0.0029)	0.8	0.9477
Decision Tree	99.76	0.9997	0.9979	0.9988	99.7974(0.0035)	0.54	0.7711
Random Forest	99.76	0.9997	0.9979	0.9988	99.7985 (0.0043)	0.54	0.9024
AdaBoost	99.94	0.9995	1.0	0.9997	99.9380 (0.0015)	0.25	0.9475
KNN	99.93	0.9996	0.9997	0.9997	99.9367 (0.0049)	0.47	0.8946
Naive Bayes	99.92	0.9999	0.9993	0.9996	99.9238 (0.0029)	0.8	0.9475

Table 11. Evaluation results of DrDoS_UDPLAG attack detection

Classification Algorithms	Accuracy (%)	Precision	Recall	F-score	Crossfold Validation Mean (STD) scores (%)	Specificity	ROC_AUC Score
Logistic Regression	99.61	0.9982	0.9978	0.998	99.6135 (0.0202)	0.84	0.9551
Decision Tree	99.46	0.9972	0.9973	0.9973	99.4450 (0.0310)	0.76	0.8764
Random Forest	99.46	0.9972	0.9973	0.9973	99.4450 (0.0310)	0.76	0.9512
AdaBoost	99.61	0.9982	0.9978	0.998	99.6139 (0.0317)	0.85	0.9542
KNN	99.61	0.9981	0.998	0.998	99.6030 (0.019%)	0.83	0.9514
Naive Bayes	99.61	0.9982	0.9978	0.998	99.6135 (0.0202)	0.84	0.9551

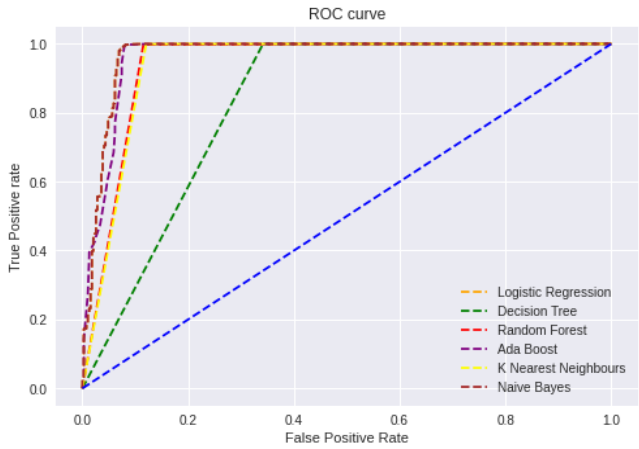

Figure 1. Classifiers ROC curves of DrDoS_MSSQL attack

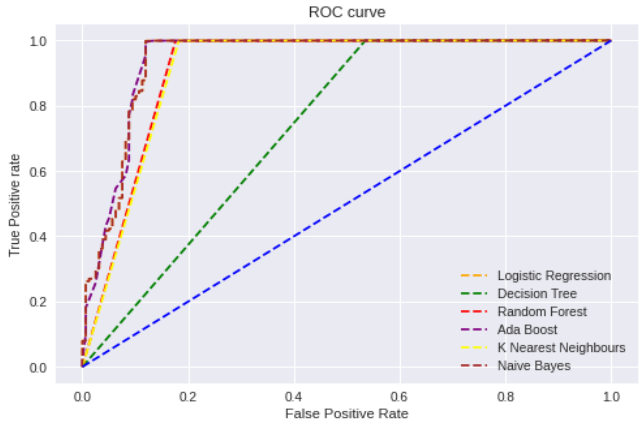

Figure 2. Classifiers ROC curves of DrDoS_SSDP attack

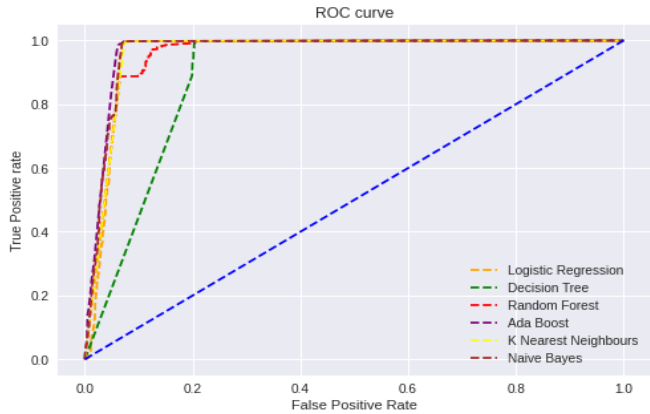

Figure 3. Classifiers ROC curves of DrDoDS_NTP attack

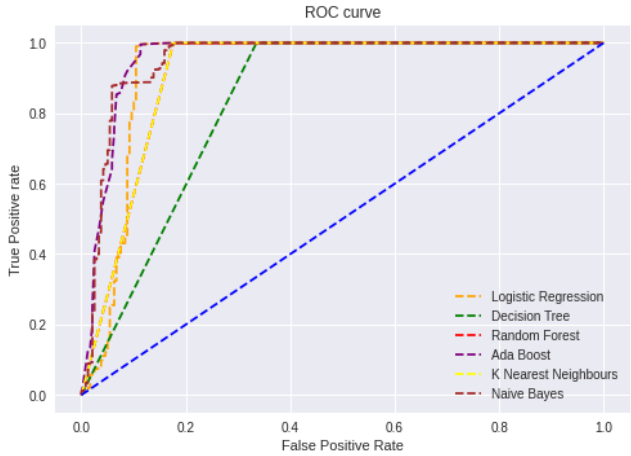

Figure 4. Classifiers ROC curves of DrDoS_TFTP attack

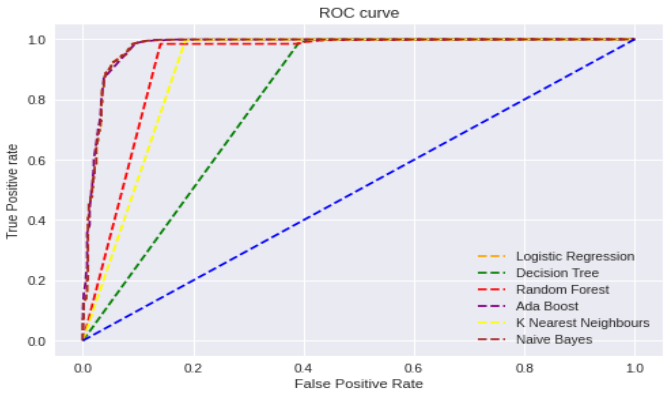

Figure 5. Classifiers ROC curves of DrDoS_DNS attack

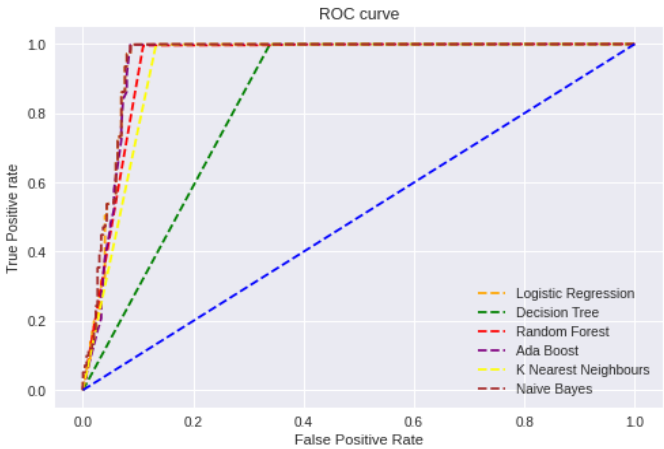

Figure 6. Classifiers ROC curves of DrDoS_LDAP attack

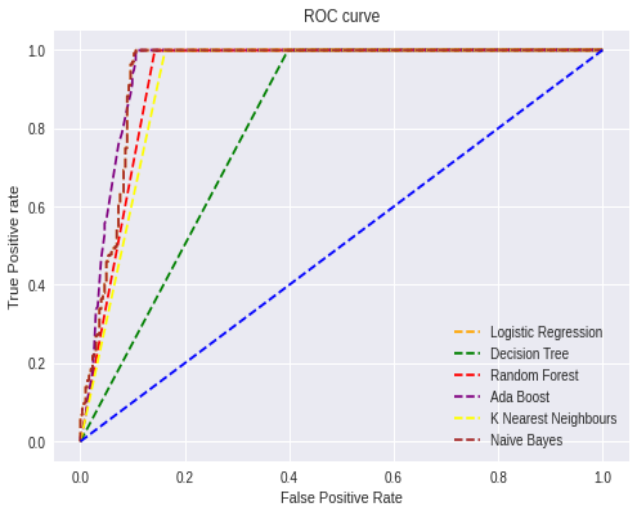

Figure 7. Classifiers ROC curves of DrDoS_NetBIOS attack

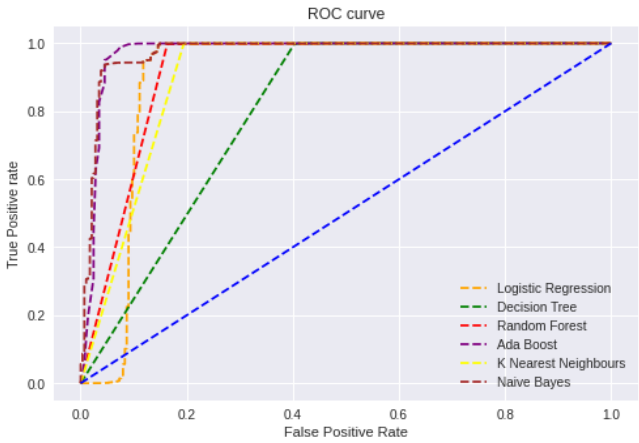

Figure 8. Classifiers ROC curves of DrDoS_SNMP attack

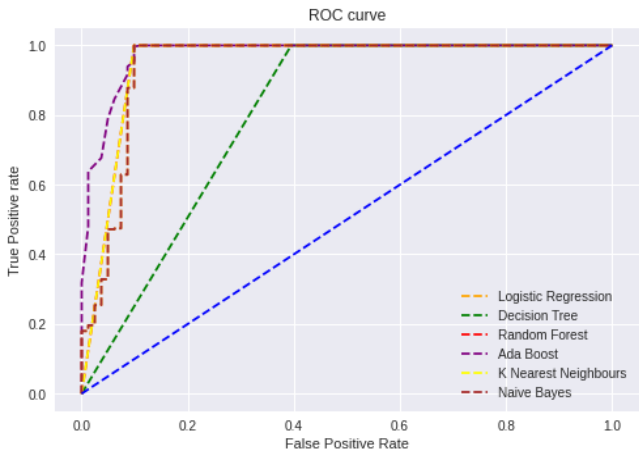

Figure 9. Classifiers ROC curves of DrDoS_Syn attack

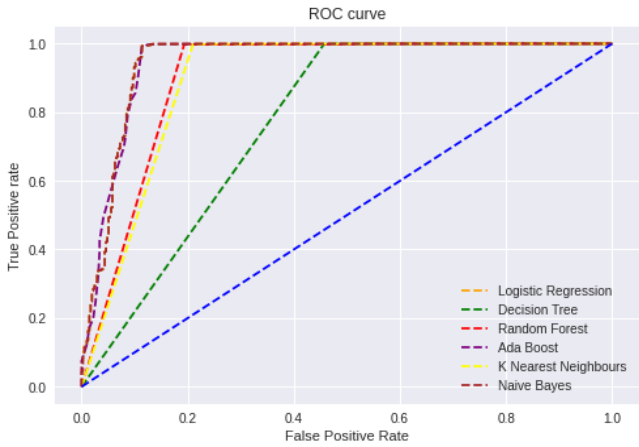

Figure 10. Classifiers ROC curves of DrDoS_UDP attack

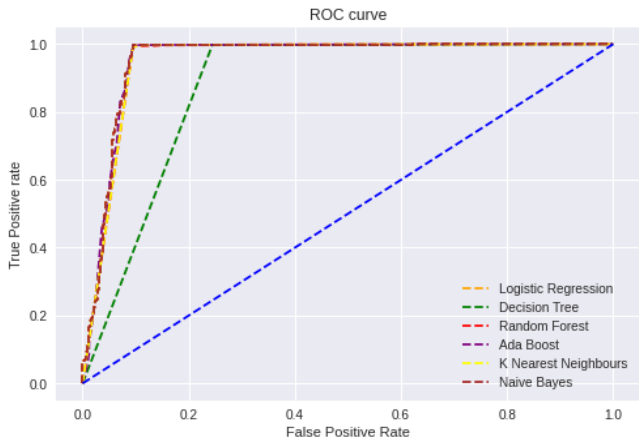

Figure 11. Classifiers ROC curves of DrDoS_UDPLAG attack

4. CONCLUSIONS

This paper presented a comparison of the performance of six machine learning classification algorithms on eleven individual different DDoS attacks datasets. Unfortunately, the most common effective DDoS attack detection method for all DDoS attacks has yet to be identified. Some DDoS attacks have common effective methods and some attacks have different effective methods. Decision tree and random forest

algorithms gave poorer results than others. Logistic regression, Ada Boost, KNN, and NB show good results.

In this paper, classification algorithms applied to different individual DDoS attack datasets get the best scores in all metrics with google colab TPU processor which is a powerful hardware accelerator and 12GB RAM. This configuration is more expensive. All datasets are big data size. The idea of next research would be to use feature selection to reduce data [22] and detect DDoS attacks using low-cost hardware.

REFERENCES

[1] Dasari, K.B., Devarakonda, N. (2018). Distributed denial of service attacks, tools and defense mechanisms. International Journal of Pure and Applied Mathematics, 120(6): 3423-3437. http://dx.doi.org/10.1007/978-3-319-97643-3_3

[2] Kwang, P. (2017). A countermeasure technique for attack of reflection SSDP in Home IoT. Journal of Convergence for Information Technology. https://doi.org/10.22156/CS4SMB.2017.7.2.001

[3] Kshirsagar, D., Kumar, S. (2021). A feature reduction based reflected and exploited the DDoS attack detection system. Journal of Ambient Intelligence and Humanized Computing. https://doi.org/10.1007/s12652-021-02907-5

[4] Suvra, D.K.S., Sen, T., Hossain, M.I., Rahman, A., Mou, M.M. (2020). Real-time performance analysis on DDoS attack detection using machine learning. Brac University. http://hdl.handle.net/10361/14730.

[5] Tuan, T.A., Long, H.V., Son, L.H., Kumar, R., Priyadarshini, I., Son, N.T.K. (2020). Performance evaluation of Botnet DDoS attack detection using machine learning. Evolutionary Intelligence, 13: 283-294. https://doi.org/10.1007/s12065-019-00310-w

[6] Mirchev, M.J., Mirtchev, S.T. (2020). System for DDoS attack mitigation by discovering the attack vectors through statistical traffic analysis. International Journal of Information and Computer Security, 13(3-4): 309-321. http://dx.doi.org/10.1504/IJICS.2020.10029285

[7] Chen, W.W., Zhang, H.Y., Zhou, X.S., Weng, Y.J. (2021). Intrusion detection for modern DDoS attacks classification based on convolutional neural networks. Computer and Information Science, 45-60. https://doi.org/10.1007/978-3-030-79474-3_4

[8] Amaizu, G.C., Nwakanma, C.I., Bhardwaj, S., Lee, J.M., Kim, D.S. (2021). Composite and efficient DDoS attack detection framework for B5G networks. Computer Networks, 188: 107871. https://doi.org/10.1016/j.comnet.2021.107871

[9] Moubayed, A., Aqeeli, E., Shami, A. (2020). Ensemble-based feature selection and classification model for DNS typo-squatting detection. IEEE Canadian Conference on Electrical and Computer Engineering (CCECE). https://doi.org/10.1109/CCECE47787.2020.9255697

[10] Swami, R., Dave, M., Ranga, V. (2021). Detection and analysis of TCP-SYN DDoS attack in software-defined networking. Wireless Personal Communications, 118(100): 2295-2317. http://dx.doi.org/10.1007/s11277-021-08127-6

[11] Singh, K.J., Thongam, K., De, T. (2018). Detection and differentiation of application-layer DDoS attack from flash events using fuzzy-GA computation. IET Info. Secure, 12(6): 502-512. https://doi.org/10.1049/iet-ifs.2017.0500

[12] Durgam, R., Devarakonda, N., Nayyar, A., Eluri, R. (2021). Improved genetic algorithm using machine learning approaches to feature modelled for microarray gene data. In book: Soft Computing for Security Applications (pp. 859-872). http://dx.doi.org/10.1007/978-981-16-5301-8_60

[13] Sharafaldin, I., Lashkari, A.H., Hakak, S., Ghorbani. A.A. (2019). Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy. IEEE 53rd International Carnahan Conference on Security Technology, Chennai, India, pp. 1-8. https://doi.org/10.1109/CCST.2019.8888419

[14] Yan, Y.D., Tang, D., Zhan, S.J., Dai, R., Chen, J.W., Zhu, N.B. (2019). Low-rate dos attack detection based on improved logistic regression. IEEE21st International Conference on High-Performance Computing and Communications, pp. 468-476. https://doi.org/10.1109/HPCC/SmartCity/DSS.2019.00076

[15] Lakshminarasimman, S., Ruswin, S., Sundarakandam, K. (2017). Detecting DDoS attacks using decision tree algorithm. Fourth International Conference on Signal Processing, Communication and Networking (ICSCN), pp. 1-6. https://doi.org/10.1109/ICSCN.2017.8085703

[16] Chen, Y., Hou, J., Li, Q.M., Long, H.Q. (2020). DDoS attack detection based on random forest. 2020 IEEE International Conference on Progress in Informatics and Computing (PIC), pp. 328-334. https://doi.org/10.1109/PIC50277.2020.9350788

[17] Dong, S., Sarem, M. (2019). DDoS attack detection method based on improved KNN with the degree of DDoS attack in software-defined networks. IEEE Access, 8: 5039-5048. https://doi.org/10.1109/ACCESS.2019.2963077

[18] Singh, N.A., Singh, K.J., De, T. (2016). Distributed denial of service attack detection using Naive Bayes classifier through info gain feature selection. ICIA-16: Proceedings of the International Conference on Informatics and Analytics, pp. 1-9. https://doi.org/10.1145/2980258.2980379

[19] Peneti, S., Hemalatha, E. (2021). DDOS attack identification using machine learning techniques. International Conference on Computer Communication and Informatics (ICCCI), pp. 1-5. https://doi.org/10.1109/ICCCI50826.2021.9402441

[20] Mishra, P., Varadharajan, V., Tupakula, U., Pilli, E.S. (2019). A detailed investigation and analysis of using machine learning techniques for intrusion detection. IEEE Commun. Surv. Tutor., 21(1): 686-728. https://doi.org/10.1109/COMST.2018.2847722

[21] Vuong, T.H., Nguyen, V., Ha, Q.T. (2021). N-Tier machine learning-based architecture for DDoS attack detection. Intelligent Information and Database Systems, 375-385. http://dx.doi.org/10.1007/978-3-030-73280-6_30

[22] Mekala, S., Rani, B.P. (2020). Kernel PCA based dimensionality reduction techniques for preprocessing of Telugu text documents for cluster analysis. International Journal of Advanced Research in Engineering and Technology, 11(11): 1337-1352. https://doi.org/10.34218/IJARET.11.11.2020.121