# Optimized t-Test Feature Selection for Real-Time Detection of Low and High-Rate DDoS Attacks

Original Scientific Paper

**Raghupathi Manthena**
Research Scholar, Department of Computer Science and Engineering,
Jawaharlal Nehru Technological University Hyderabad, Telangana, India
mraghu30@gmail.com

**Radhakrishna Vangipuram***
Department of Information Technology,
VNR Vignana Jyothi Institute of Engineering and Technology, Hyderabad, Telangana, India
radhakrishna_v@vnrvjiet.in

*Corresponding author

***Abstract*** *– Distributed Denial of Service (DDoS) attacks stand out as a serious threat, capable of disrupting online services and businesses. The main aim of Distributed Denial of Service (DDoS) attacks is to make system services unavailable to the legitimate users. To detect these attacks, intrusion detection systems (IDS) continually monitor the network traffic. During this process, the IDS system generates high false positive rates while distinguishing low-rate DDoS (LRDDoS) and high-rate DDoS (HRDDoS) attack traffic from legitimate traffic. The idea behind feature selection is that picking the right network features is a key part of interpreting the difference between normal traffic and LRDDoS or HRDDoS attack traffic. This means the IDS performance will automatically get better. In this paper, we propose a scalable feature selection method that utilizes the statistical t-test to identify an optimal feature subset from original feature set at a low computational cost. We strongly hypothesize that the proposed feature selection method yields an optimal feature subset and the machine learning classifiers trained on this feature set can effectively distinguish benign, LRDDoS, and HRDDoS network traffic. We evaluated the proposed method on the publicly available benchmark datasets CICIDS2017, CICIDS2018, and CICDDoS2019, utilizing twelve supervised machine learning classifiers. Among the twelve classifiers, the Extra Tree Classifier (EXT) demonstrated superior performance, achieving an average accuracy of 96.50%, precision of 96.58%, and an F-Score of 96.50% across the four sample test datasets (D1, D2, D3, and D4). The proposed method showed consistent and superior performance in distinguishing the LRDDoS, HRDDoS, and benign traffic to the state-of-the-art existing works over the four test datasets.*

***Keywords****: t-Test, Feature selection, DDoS traffic, LRDDoS, HRDDoS, CICDDoS2019, Balanced accuracy*

*Received: December 5, 2024; Received in revised form: February 26, 2025; Accepted: April 3, 2025*

## 1. INTRODUCTION

As our dependence on technology continues to rise, the importance of cybersecurity has surged to unprecedented heights. The Internet of Things (IoT), cloud computing, mobile devices, and the widespread use of digital communication have all contributed to an exponential increase in the attack surface for cyber-attacks [1]. Among all the cyberattacks, Distributed Denial of Service (DDoS) attacks stand out as a serious threat, capable of disrupting online services and businesses.

Attackers carry out these network attacks by overwhelming the networks or server's resources (CPU, memory, bandwidth, etc.) with massive traffic because of which even a legitimate user will not able to access services of network or server. According to the NetScout threat report H1 2024, DDoS attacks rose 12.8% compared to H2 2023 NetScout threat report. The longest attack lasted for over an hour, resulting in a count of 825,217 DDoS attacks. Furthermore, in less than 5 minutes, the number of DDoS attacks increased to 4,137,582. In this paper, we attempt to categorize modern DDoS attacks into two groups based on rapid disruption of network or server services. The first group of DDoS attacks are high-rate DDoS (HRDDoS) attacks, which make the services unavailable within short period of time. The second category of attacks consists of low-rate DDoS (LRDDoS) attacks. In this kind of network attack, attackers ex-

ploit potential logic errors or vulnerabilities in the service to send the malicious requests. These malicious requests slowly make the server unavailable for legitimate users. Some research works focus on model building instead of feature selection tasks, as mentioned in [2]. These types of models result in high false positive rates.

Research works [3-5] developed an IDS system to detect DDoS attacks applying feature selection and machine learning techniques. These research studies evaluated learning machines on the CICDS2017 dataset. However, the limitation is that the CICDDoS2017 dataset does not represent a wide range of DDoS attacks. Also, the dataset only included a limited number of DDoS samples, failing to cover full spectrum of DDoS classes. Though studies [6-8] propose feature subsets to identify DDoS attacks they are not better representative features for LRDDoS and HRDDoS attacks.

Usually, most research studies directly apply conventional feature selection methods to select the optimal feature subset. These methods are divided into three categories: filter-based, wrapper-based, and embedded methods. Each of these methods have their advantages and limitations. The filter-based methods calculate feature importance using statistical properties without employing machine learning algorithms. The information gain (IG), chi-square, and correlation coefficient (CrC) methods are fast and computationally efficient, making them suitable for high-dimensional data. These methods may ignore interactions among features when feature relationship is complex. Additionally, when working with continuous data, there may be a bias towards more diverse features, which could result in the inclusion of irrelevant features in the subset.

Wrapper methods generate different feature subsets using random selection or heuristic selection. The machine learning algorithm will select the optimal feature subset based on each subset performance. While these methods enhance the performance of a model by using an optimal feature subset, they can be computationally costly when dealing with large datasets, may also limit the model generalizability.

Embedded methods use algorithms like Lasso (L1 regularization), Ridge (L2 regularization), and decision trees to build feature selection right into the model training process. These methods often result in improved generalization and performance of the model. Specific algorithms tailor these methods, potentially limiting their broader applicability and making them less interpretable than filter methods. Thus, feature subsets obtained by conventional feature selection techniques for binary classification of DDoS attacks fail to discriminate LRDDoS and HRDDoS attacks. Therefore, it is essential to identify a more appropriate and optimal feature subset for detection of LRDDoS and HRDDoS attacks.

The problem of accurately distinguishing between legitimate user traffic, LRDDoS and HRDDoS network traffic is the present challenge w.r.t DDoS attacks. Incorrectly identifying attack traffic can lead to system overload or failure, while misclassifying legitimate traffic can cause service disruptions and financial losses. This problem can be addressed using machine learning with t-test feature selection, which helps to identify the most important features to discriminate between benign and attack traffic. By focusing on the relevant features, the system can improve its accuracy in detecting attacks while minimizing errors, ensuring both security and continuous service for legitimate users.

The motivation for this study coins from the gap in the present literature which does not address detection of LRDDoS and HRDDoS variants using machine learning techniques integrated with a lightweight feature selection method. Also, the immense volume of modern network traffic necessitates the immediate need for identification of key features in minimal time and at the same time to obtain high detection accuracy. LRDDoS attacks can gradually merge with legitimate traffic, while HRDDoS attacks result in abrupt and massive data spikes. Thus, for effective detection in both scenarios, it is essential to focus on selecting the most relevant features that can distinguish between low-rate DDoS attack traffic and legitimate user traffic.

At the outset, to address the limitations of conventional feature selection methods, in this research we propose a lightweight feature selection method to obtain an optimal feature subset that detects LRDDoS and HRDDoS attacks by employing the Extra Tree classifier (EXT).

The proposed method is a lightweight solution for selecting significant features with less computation time. Following are highlights of the present work.

- In this research, we propose a light-weight feature selection method that leverages the inferential statistical t-Test to identify optimal feature set to discriminate LRDDoS and HRDDoS attacks.
- Based on the proposed feature selection method, we strongly suggest 58 network traffic features for differentiating low-rate and high-rate DDoS traffic from benign traffic.
- To evaluate the proposed method, we utilized reliable and publicly available benchmark dataset CICDDoS2019. We tested our method on four different testing datasets (D1, D2, D3, and D4) obtained from testing day traffic of CICDDoS2019 dataset to achieve generalizability.
- We evaluated performance of twelve machine learning classifiers on the feature subset identified by our feature selection method. Among all classifiers, the Extra Tree classifier (EXT) performed the best, with an average accuracy of 96.50%, precision of 96.58%, and F-score of 96.50% across four test datasets (D1, D2, D3, and D4).
- On the CICIDS2017 and CICIDS2018 datasets, an accuracy 99.81% and 99.99% is achieved by proposed method.

## 2. RELATED STUDY

In this section, we provide a brief discussion of the popular feature selection methods used to select a subset of features and implement the IDS system. A number of IDS datasets are available publicly, and it is proved that the CICDDoS2019 dataset is the most reliable and contains updated DDoS attack vector instance [6]. This led us to concentrate on the CICDDoS2019 IDS dataset, which has been the subject of evaluation in recent studies.

In cybersecurity, especially when it comes to detecting Distributed Denial-of-Service (DDoS) attacks, the performance of machine learning models largely depends on the quality of the input data. For each class of the CICDDoS2019 dataset DDoS attacks, Sharafaldin et al. [6] suggested a significant feature subset with 24 different features using a weighted standard mean of random forest feature importance. The performance of ID3, Random Forest, and logistic regression machine learning classifiers is evaluated on these 24 features. Overall, ID3 classifier outperformed the other two, achieving a high detection rate of 65% and an accuracy of 78% on more than 7 crore instances. The approach they used did not address the detection of LRDDoS and HRDDoS attacks. They did not discuss the generalizability of their model, which could lead to variations in the rate of DDoS attacks in different network data.

To address the high dimensionality problem, S. Li et al. [7] suggested Truncated Lanczos-Tensor SVD to reduce the dimensionality of large-scale datasets. However, they did not address the adaptability, and practical evaluation of this method. Hajimaghsoodi and Jalili [8] suggested a novel method, i.e., a 3-phase RAD model, to detect DDoS attacks using a statistical approach. The number of features used to evaluate their model remains undisclosed and did not address the low-rate and high-rate DDoS attacks detection. To detect, identify, categorize, and classify IoT DDoS attacks, Jia et al. [9] developed the edge-centric protection system FlowGuard. However, the system has certain drawbacks, including its dependence on artificial datasets, which could potentially impact its real-world applicability, and its use of high-performance edge servers, which could limit its scalability in resource-constrained environments. Maheswari et.al [10], developed an optimized weighted voting-based ensemble model for detection of DDoS attacks in SDN environment. and selected 20 features using statistical analysis. However, in this study they did not discuss the computational cost and detection of high- and low- rate DDoS attacks. The most recent work by S. Mahdavifar and A. A. Ghorbani [11], suggested 22 significant features using the mutual information gain and developed CapsRule method to detect the reflection-based DDoS attacks but they did not study for low rate and high-rate DDoS network attacks. Enock Q.E. et al [12] proposed a feature selection method by integrating mutual information gain, correlation, and random forest feature importance for DDoS attacks detection using RCHT method.

G.C. Amaizu et al. [13] developed the DDoS detection system for 5G and B5G networks, which uses an effective feature extraction technique in conjunction with a composite multilayer perceptron to detect and categorize DDoS attacks. The multilayer perceptron models and feature extraction in real-time applications may increase the computational burden. Cil et al. [14] suggested a deep learning (DL) model that combines feature extraction and classification. Using DNN algorithm, they achieved improved DDoS attack detection and classification. However, for multiclass classification, the model accuracy was lower. In order to construct an effective intrusion detection system (IDS) for detecting and categorizing DDoS attacks, A.A. Najar et al. [15] suggested a feature subset which contains 43 features. The creative feature selection, efficient preprocessing, and comprehensive dataset analysis are important contributions of this study. Although it provides a high detection accuracy and quick detection times, drawbacks include (i) inability to handle unbalanced data, (ii) computational complexity, (iii) dependence on the dataset quality, and (iv) difficulties of extrapolating to other attack types. Wei et.al [16] suggested, a deep learning-based hybrid AE-MLP method to classify the DDoS attacks. They used an autoencoder to denoise the DDoS attacks and then classified them using MLP. Ferrag et.al [17], developed a deep learning-based CNN method to address the classification problems of DDoS attacks in the smart agriculture sector. A. Alashhab et al. [18] suggested an IDS framework utilizing online machine learning (OML) to detect DDoS attacks within software-defined networks (SDN). They identified 22 features using their custom dataset. However, these works did not address the generalizability of the model, low-rate and high-rate DDoS attacks detection. To address the generalizability issue in IDS system, O. Barut et.al [19] developed R1D1T model to classify the DDoS attacks using raw packet data. The R1D1T model converts the data into 1-D image and applies self-attention-based neural networks to perform classification. Despite addressing these issues, the generalizability and computational cost of this model pose serious limitations.

Li et al. [20], developed a mathematical model for detecting and mitigating low-rate DDoS attacks in cloud computing environments, specifically targeting container-based DDoS attacks. However, this work focused on LRDDoS attacks and neglected HRDDoS attacks. They designed their mathematical model based on the number of requests per unit time in the test bed network. Makhduma F. Saiyed et al. [21], designed a lightweight method FLUID, to differentiate DDoS attacks from legitimate traffic. The development of this approach relied on the theories of Kullback-Leibler (KL) divergence and greedy bin-packing information. In this approach, they have achieved an average 90% accuracy on the CICDS2017, CICDDoS2019, and ToN-IoT datasets based on a single threshold value. However, threshold value-based methods may not be suitable to discriminate the LRDDoS and HRDDoS attack traffic from the legitimate traffic.

Raghupathi et al. [22], suggested a feature selection method using independent sample t-test. This method was used to identify significant features for the detection of DDoS attacks and focused solely on binary classification. M. F. Saiyed and I. Al. Anbagi [23], suggested GADAD model to select key features using GAStats method to detect low-rate and high-rate DDoS attacks. However, this model computational time is high.

Thus, the majority of research studies focused on detecting DDoS attacks but did not address for LRDDoS and HRDDoS traffic detection. Few studies [20], [21] and [23] focused on detecting either LRDDoS or HRDDoS attacks. The research literature shows that there has been limited research w.r.t detection of LRDDoS and HRDDoS attacks. Thus, in this paper we mainly focused on addressing three key areas: We aim to (1) identify the significant feature subset with less computational cost and at 95% confidence interval; (2) discriminate between LRDDoS and HRDDoS attacks with high accuracy and precision rates, and (3) develop a generalizable model. The current study addresses low-rate and high-rate DDoS attack detection.

## 3. METHODOLOGY

A key statistical method for determining whether there is a significant difference between the means of two groups is the statistical t-test. It plays a crucial role in the hypothesis testing, which evaluates whether observed differences are genuine or merely due to random chance. Various fields widely employ this straightforward yet powerful technique to derive meaningful insights from data comparisons. Researchers frequently use the t-test to test hypotheses and make inferences about population parameters based on sample data. Using the power of the t-test for statistics, we propose a method to obtain a feature subset that can unearth the difference between DDoS traffic and normal traffic.

The proposed feature selection method utilizes the training dataset ($D_{MxN}$), where $M$ represents the number of instances and $N$ denotes the number of features, as outlined in the algorithm. The preprocessing steps, from step 1 to step 6, involve eliminating static features, those with standard deviation zero, and highly correlated features. The algorithm also eliminates duplicate instances; if they represent less than 0.05% of the total instances of the class label and contain NaN or infinite values. The proposed feature selection method is performed from step 7 to step 14. The feature selection method starts by dividing the preprocessed dataset into three groups: 1. BENIGN, 2. LOW, and 3. HIGH. In step 8, algorithm selects the feature in sequential order from the BENIGN group and the LOW group. Next, we calculated the mean and variance of the current feature using Eq. 1 and Eq. 2 respectively. In Eq.1 and Eq.2 $\bar{x}_{BENIGN}$ and $\bar{x}_{DDoS\ Attack}$ are the mean value of current feature considered from two groups; $\sigma^2_{BENIGN}$ and $\sigma^2_{DDoS\ Attack}$ are variances of the current feature.

$$Mean\ (\bar{x}) = \frac{1}{n}\sum_{i=1}^{n} x_i \tag{1}$$

$$Variance\ (\sigma^2) = \frac{1}{n}\sum_{i=1}^{n} (x_i - \bar{x})^2 \tag{2}$$

$$T_{testscore} = \frac{\bar{x}_{BENIGN} - \bar{x}_{DDoS\ Attack}}{\sqrt{\left(\frac{\sigma^2_{BENIGN}}{n_{BENIGN}} - \frac{\sigma^2_{DDoS\ Attack}}{n_{DDoS\ Attack}}\right)}} \tag{3}$$

Then, $T_{test\_score}$ is computed using Eq.3 wherein variables $n_{BENIGN}$ and $n_{DDoS\ Attack}$ represent the number of samples in respective groups. Here, the $DDoS\ Attack$ can belong to LOW or HIGH group. In the next step, the degree of freedom (DOF) is computed using Eq. 4, and $T_{critical}$ value is obtained from $t_{distribution}$ table with a 95% confidence interval w.r.t DOF.

$$DOF = \frac{\left(\frac{\sigma^2_{BENIGN}}{n_{BENIGN}} + \frac{\sigma^2_{DDoS\ Attack}}{n_{DDoS\ Attack}}\right)^2}{\frac{(\sigma^2_{BENIGN})^2}{n_{BENIGN} - 1} + \frac{(\sigma^2_{DDoS\ Attack})^2}{n_{DDoS\ Attack} - 1}} \tag{4}$$

In the subsequent steps, features that satisfy the given constraint are identified and considered as significant, if $T_{test\_score}$ of the feature is greater than $T_{critical}$ value. From step 8 to step 10, we proceed until we reach ($N$-1)$^{th}$ feature. The same process is repeated by considering HIGH and BENIGN groups to identify significant features for detection of HRDDoS attacks. After identifying significant feature subsets separately for LRDDoS and HRDDoS attacks these feature subsets are merged to obtain the final feature subset. The $T_{test\_score}$ value is determined using the statistical evaluation method described in the Algorithm, where the ability of each feature to discriminate between Benign, Low and High classes is analyzed based on the independent t-Test value.

**Algorithm: Proposed Feature Selection for Detection of Low-rate and High-rate DDoS Network Traffic**

Input: Train dataset $D_{MxN}$

M → Number of instances

N → Number of input features (1 to N-1 are the iput features and Nth feature is the label)

Output: Optimal feature subset F'

**Start**

Step 1: Remove socket features. {Unnamed 0, 'Flow Id', 'Source IP' 'Source Port' , 'Destination IP' , 'Detination Port', 'Protocol' , 'Timestamp' and 'SimilarHTTP'}

Step 2: Removal of duplicate instances

*$D^1$ ← D updated dataset after removing duplicate rows*

Step 3: Removal of *NaN* or *Inf* values contained rows

$D^2 \leftarrow D^1$ updated dataset after removing $NaN$ and Infinity value rows

Step 4: Removal of highly correlated features

{fwd header length (2), subflow fwd packets, subflow fwd bytes, subflow bwd packets, and suflow bwd bytes}

Step 5: Removal of standard deviation is zero fetures

{fwd avg packets/bulk, fwd avg bulk rate, bwd avg bytes/bulk, bwd psh flags, fwd urg flags, bwd urg flags, fwd avg bytes/bulk, bwd avg packets/bulk, and bwd avg bulk rate, fin flag count, psh flag count and ece flag count}

Step 6: Handling the negative values in the dataset

Step 7: Split the dataset into 3 groups based on class labels: BENIGN, 2.LOW and 3. HIGH

Step 8: Calculate mean and variance of current feature from BENIGN group and LOW/HIGH group

Step 9: Calculate $T_{test\_score}$ value of current feature using mean and variance

Step 10: Calculate degree of freedom for current feature

Step 11: Obtain $T_{critical}$ value with respect to degree of freedom at 95% confidence interval

Step 12: If $T_{test\_score}$ value greater than $T_{critical\ value}$, Consider the feature is significant

Step 13: Repeat from step 8 to step 12, until the end of feature set and groups.

Step 14: Return optimal feature subset $F'$

**Stop**

## 4. DATASET

To evaluate the performance of the proposed method, we utilized the CICIDS2017 [24], CICIDS2018 [25], and CICDDoS2019 widely used benchmark IDS datasets. Among these, the CICDDoS2019 dataset satisfies all the eleven properties listed by Gharib et al. [26], making it a reliable IDS dataset. It offers diverse DDoS attack scenarios, including normal traffic, enabling researchers to evaluate the effectiveness of their detection algorithms. Its comprehensive feature set aids in the development of sophisticated methods for feature selection and model training. The training dataset has more than 50 million instances split into 13 class labels. Of these, one label represents benign (legitimate user) traffic, and remaining 12 labels represent various types of DDoS attack traffic. The testing dataset includes more than 20 million instances, categorized into 8 class labels, where one label denotes benign traffic and the other 7 represents different attacks. For our experimentation, we utilized a sample of 399,998 instances for training day dataset and 112,611 instances for testing day dataset to evaluate the proposed method.

**Table 1.** Class distribution of the CICDDoS2019 training dataset utilized for evaluation

| SN | Class Label | Number of Instances |
|---|---|---|
| 1 | BENIGN | 56425 |
| 2 | WebDDoS | 439 |
| 3 | UDP_Lag | 31194 |
| 4 | NetBIOS | 31194 |
| 5 | LDAP | 31194 |
| 6 | MSSQL | 31194 |
| 7 | DNS | 31194 |
| 8 | SYN | 31194 |
| 9 | UDP | 31194 |
| 10 | TFTP | 31194 |
| 11 | NTP | 31194 |
| 12 | SNMP | 31194 |
| 13 | SSDP | 31194 |
| **Total** | | **399998** |

**Table 2.** Class distribution of the CICDDoS2019 testing dataset utilized for evaluation

| SN | Class Label | Number of Instances |
|---|---|---|
| 1 | BENIGN | 56306 |
| 2 | UDP_Lag | 1873 |
| 3 | NetBIOS | 9072 |
| 4 | LDAP | 9072 |
| 5 | MSSQL | 9072 |
| 6 | PortMap | 9072 |
| 7 | SYN | 9072 |
| 8 | UDP | 9072 |
| **Total** | | **112611** |

Tables 1 and 2 depict the class distribution of the training and testing datasets respectively. To ensure generalizability, robustness, reduce overfitting; we have sampled four different testing datasets (D1, D2, D3, and D4) from 20 million testing day network traffic instances, each having 112611 network flow samples. Additionally, we derived a validation dataset ($V_D$) of 112612 samples from 50 million sequential samples of the CICDDoS2019 dataset. Thus, validation and testing datasets contain unique instances and are of same size. For experimental analysis, Classes labels are encoded by encoding benign instances as BENIGN, low-rate attack traffic as LOW, and high-rate attack traffic as HIGH, using Andrew Visualization Plot.

To ensure the generalizability of the proposed method, we have also considered benign, low-rate, and high-rate DDoS instances from publicly available datasets (CICIDS2017 and CICIDS2018). The CICIDS2017 and CICIDS2018 sample datasets information is depicted in Table 3.

**Table 3.** Class distribution of CICIDS2017 and CICIDS2018 datasets used for evaluation

| SN | Dataset | Class Label | Number of Instances | | |
|---|---|---|---|---|---|
| | | | Training | Validation | Testing |
| 1 | CICIDS 2017 | BENIGN | 30065 | 9956 | 9979 |
| | | LOW | 12974 | 4349 | 4265 |
| | | HIGH | 59913 | 20013 | 20074 |
| 2 | CICIDS 2018 | BENIGN | 119981 | 39956 | 40063 |
| | | LOW | 1067 | 328 | 335 |
| | | HIGH | 118952 | 39716 | 39602 |

## 5. EXPERIMENTATION AND RESULTS

In this section, we discuss the experimentation and evaluation results. All the experiments were executed on a Dell PC, which has an i7 Intel processor with 2.2Ghz speed and 16 MB RAM. To simulate the proposed work, the Jupiter notebook IDE and python scripts were utilized.

Fig. 1 illustrates the architecture of proposed system for the detection of LRDDoS and HRDDoS attacks. The training dataset, which initially had 87 features along with the target feature was input to the feature selection algorithm. The preprocessing stage reduced the number of feature dimensions from 87 to 61. During the feature selection phase, the application of a statistical t-Test resulted in 58 significant features in just 0.49 seconds. The 58 features resulted from feature selection algorithm are included in the appendix. For evaluation of the proposed method, 58 features resulted from t-Test are retained w.r.t training, validation and testing datasets and twelve machine learning classifiers were used to measure their classification and prediction performance. The classifiers included AdaBoost, K-Nearest Neighbors (KNN), Linear Discriminant Analysis (LDA), Logistic Regression (LR), Multi-Layer Perceptron (MLP), Naive Bayes (NB), Quadratic Discriminant Analysis (QDA), Random Forest (RF), and Ridge. The performance evaluation metrics considered are Accuracy (Acc), Precision (Prec), Sensitivity (Sns), Specificity (Spe), F-score and Balanced Accuracy (BA) given by Eq.5 to Eq.10 respectively.

$$Acc = \frac{TP + TN}{TP + TN + FN + FP} \tag{5}$$

$$Pre = \frac{TP}{TP + FP} \tag{6}$$

$$Sns\ (or)\ Recall = \frac{TP}{TP + FN} \tag{7}$$

$$Spe = \frac{TN}{TN + FP} \tag{8}$$

$$F - Score = 2 * \frac{Pre * Sns}{Pre + Sns} \tag{9}$$

$$Balanced\ Accuracy = \frac{Sns\ + Spe}{2} \tag{10}$$

Before training the classifiers, we normalized the training dataset using a min-max scalar, which scaled all the data points within the range of 0 and 1. The normalized dataset with 399998 instances, which included 58 features is input to twelve machine learning classifiers for training. These twelve classifiers were then validated using 112612 instances. Table 4 provides a detailed performance analysis of twelve machine learning models on the validation dataset ($V_D$). Subsequently, the performance of machine learning models is evaluated on four distinct testing day subset datasets. The performance results of twelve models on four test datasets (D1, D2, D3, and D4) is depicted using Table 5, Table 6, Table 7 and Table 8 respectively.

**Table 4.** Validation metrics of twelve machine learning models using the CICDDOS2019 validation dataset

| SN | Model | Acc. (%) | Prec. (%) | F-Score (%) |
|---|---|---|---|---|
| 1 | ADB | 78.56 | 78.93 | 78.72 |
| 2 | DT | 82.67 | 82.64 | 82.65 |
| 3 | EXT | 80.92 | 80.98 | 80.94 |
| 4 | KNN | 83.77 | 83.74 | 83.74 |
| 5 | LDA | 77.44 | 78.98 | 77.43 |
| 6 | LR | 80.79 | 81.53 | 80.99 |
| 7 | MLP | 80.25 | 80.45 | 80.32 |
| 8 | NB | 85.23 | 87.50 | 84.44 |
| 9 | QDA | 27.01 | 9.10 | 13.61 |
| 10 | RF | 81.11 | 81.16 | 81.13 |
| 11 | Ridge | 76.88 | 78.62 | 76.99 |
| 12 | XGB | 82.52 | 82.50 | 82.50 |

**Table 5.** Performance metrics of twelve classifiers using the CICDDOS2019 testing day dataset D1

| SN | Model | Acc. (%) | Prec. (%) | F-Score (%) |
|---|---|---|---|---|
| 1 | ADB | 55.18 | 50.43 | 48.87 |
| 2 | DT | 82.17 | 86.86 | 83.99 |
| 3 | EXT | 96.12 | 96.24 | 96.15 |
| 4 | KNN | 88.12 | 92.41 | 89.32 |
| 5 | LDA | 88.10 | 90.99 | 88.97 |
| 6 | LR | 81.22 | 90.72 | 83.73 |
| 7 | MLP | 82.73 | 91.22 | 85.12 |
| 8 | NB | 90.58 | 89.43 | 89.55 |
| 9 | QDA | 44.57 | 73.90 | 31.11 |
| 10 | RF | 90.07 | 90.75 | 90.30 |
| 11 | Ridge | 53.56 | 71.62 | 49.54 |
| 12 | XGB | 95.30 | 95.58 | 95.41 |

**Table 6.** Performance metrics of twelve classifiers using the CICDDOS2019 testing day dataset D2

| SN | Model | Acc. (%) | Prec. (%) | F-Score (%) |
|---|---|---|---|---|
| 1 | ADB | 54.19 | 50.52 | 49.30 |
| 2 | DT | 91.60 | 92.70 | 91.98 |
| 3 | EXT | 96.56 | 96.63 | 96.56 |
| 4 | KNN | 87.09 | 92.15 | 88.46 |
| 5 | LDA | 88.32 | 91.09 | 89.14 |
| 6 | LR | 79.20 | 90.35 | 81.97 |
| 7 | MLP | 80.96 | 90.86 | 83.62 |
| 8 | NB | 92.06 | 91.36 | 91.47 |
| 9 | QDA | 43.67 | 73.26 | 30.39 |
| 10 | RF | 89.65 | 89.74 | 89.62 |
| 11 | Ridge | 53.58 | 60.47 | 49.56 |
| 12 | XGB | 95.31 | 95.63 | 95.43 |

**Table 7.** Performance metrics of twelve classifiers using the CICDDOS2019 testing day dataset D3

| SN | Model | Acc. (%) | Prec. (%) | F-Score (%) |
|---|---|---|---|---|
| 1 | ADB | 54.18 | 48.73 | 48.63 |
| 2 | DT | 85.23 | 89.39 | 86.68 |
| 3 | EXT | 96.67 | 96.73 | 96.67 |
| 4 | KNN | 87.35 | 92.19 | 88.69 |
| 5 | LDA | 88.06 | 91.04 | 88.96 |
| 6 | LR | 79.20 | 90.41 | 82.00 |
| 7 | MLP | 81.16 | 90.90 | 83.81 |
| 8 | NB | 92.04 | 91.23 | 91.35 |
| 9 | QDA | 43.98 | 73.43 | 30.60 |
| 10 | RF | 88.29 | 89.61 | 88.75 |
| 11 | Ridge | 53.51 | 60.54 | 49.55 |
| 12 | XGB | 95.49 | 95.73 | 95.59 |

**Table 8.** Performance metrics of twelve classifiers using the CICDDOS2019 testing day dataset D4

| SN | Model | Acc. (%) | Prec. (%) | F-Score (%) |
|---|---|---|---|---|
| 1 | ADB | 55.16 | 48.98 | 49.23 |
| 2 | DT | 85.12 | 89.36 | 86.60 |
| 3 | EXT | 96.66 | 96.72 | 96.65 |
| 4 | KNN | 87.46 | 92.22 | 88.76 |
| 5 | LDA | 88.12 | 91.08 | 89.01 |
| 6 | LR | 79.12 | 90.39 | 81.94 |
| 7 | MLP | 81.16 | 90.91 | 83.82 |
| 8 | NB | 92.06 | 91.27 | 91.39 |
| 9 | QDA | 43.94 | 73.41 | 30.58 |
| 10 | RF | 89.10 | 89.99 | 89.41 |
| 11 | Ridge | 53.49 | 66.25 | 49.54 |
| 12 | XGB | 95.30 | 95.60 | 95.41 |

From these results, we observed that ADB, QDA and Ridge performance is lower, and the test accuracy ranges between 43% and 55% for these classifiers. With the exception of the EXT model, the accuracy of the remaining models ranged from 80% to 95%. Overall, the EXT model showed superior performance compared to the remaining eleven machine learning models. The EXT tree model outperformed eleven models with an average accuracy of 98.31%, precision of 99.97%, and F-score of 98.29%. Using our method, the model is able to detect benign traffic and HRDDoS attack traffic with an average balanced accuracy of 98%, while LRDDoS attacks are detected with an average balanced accuracy of 91.20% which is very significant. The hyperparameter settings used for EXT classifier are n_estimaters = 10, criterion='gini', max_depth=none, min_samples_split = 2, min_samples_leaf = 1, max_features = 'auto', n_jobs =1, random_state = none.

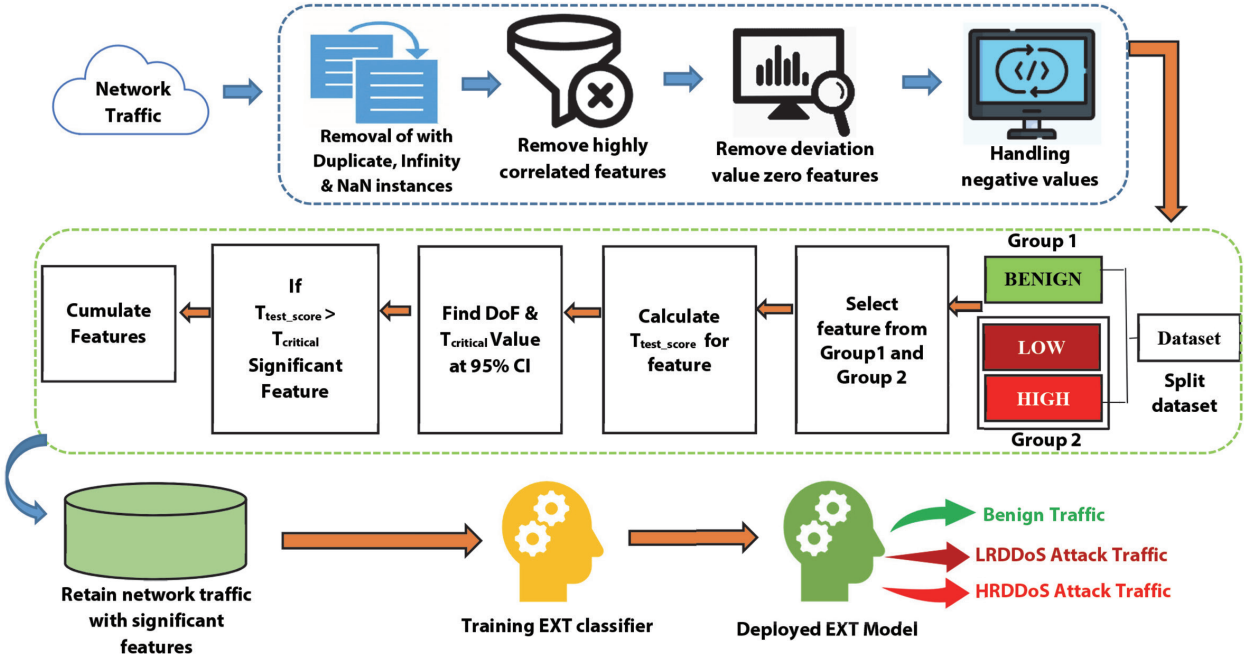



**Fig. 1.** Architecture for detection of low-rate and high-rate DDoS attacks

Furthermore, to analyze the model in-depth we utilized receiver operating characteristics (ROC) curves as an evaluation metric. Fig. 2 depicts ROC curves obtained when the model is evaluated on the four test datasets (D1, D2, D3 and D4).

Table 9 displays the detailed performance results of the EXT model against BENIGN, LRDDoS, and HRDDoS attacks. In this study, we also present the balanced accuracy metric, which reveals the performance of individual classes w.r.t three-class classification.

### COMPARISON WITH EXISTING FEATURE SELECTION METHODS:

We have compared our feature selection method to widely applied methods such as filtering (information gain and variance threshold), embedding (logistic regression), and wrapping (Random Forest Importance and Extra Tree Classifier Importance). Table 10 depicts the comparison of the proposed method to some of the widely used feature selection methods. The Information Gain method identified 32 features and achieved an average accuracy of 74% across four test datasets using the EXT classifier. In contrast, the logistic regression method identified 27 features with an average accuracy of 80%. Similarly, the random forest importance method also reached an average accuracy of 80% with 18 features, while the Extra Tree classifier importance achieved the same accuracy using 17 features. However, our proposed feature selection method outperformed all five methods, achieving an average accuracy of 96.50% using 58 significant features. In Table 10, NOF denotes number of features. Fig. 3 shows comparison of how well the EXT model worked on four testing day datasets using conventional feature selection methods vs. proposed method.

**Table 9.** Performance metrics obtained for validation and four testing day datasets of CICDDOS2019 for the EXT model using the proposed feature selection

| Dataset | Class Label | Sns. (or) Recall (%) | Spe. (%) | Pre. (%) | Acc. (%) | F-Score (%) | BA (%) |
|---|---|---|---|---|---|---|---|
| VD | BENIGN | 99.99 | 99.99 | 99.99 | 99.99 | 99.99 | 99.99 |
| | LOW | 60.24 | 87.07 | 58.03 | 80.93 | 59.12 | 73.65 |
| | HIGH | 63.06 | 87.53 | 65.16 | 80.92 | 64.09 | 75.29 |
| D1 | BENIGN | 96.60 | 99.94 | 99.94 | 98.27 | 98.25 | 98.27 |
| | LOW | 84.24 | 97.97 | 81.69 | 96.63 | 82.94 | 91.10 |
| | HIGH | 98.39 | 96.62 | 95.16 | 97.34 | 96.75 | 97.51 |
| D2 | BENIGN | 96.67 | 99.96 | 99.96 | 98.31 | 98.28 | 98.31 |
| | LOW | 84.24 | 98.40 | 85.03 | 97.03 | 84.63 | 91.32 |
| | HIGH | 99.40 | 96.69 | 95.30 | 97.78 | 97.31 | 98.05 |
| D3 | BENIGN | 96.75 | 99.99 | 99.99 | 98.37 | 98.34 | 98.37 |
| | LOW | 84.13 | 98.51 | 85.87 | 97.11 | 84.99 | 91.32 |
| | HIGH | 99.61 | 96.69 | 95.31 | 97.87 | 97.41 | 98.15 |
| D4 | BENIGN | 96.65 | 99.99 | 99.99 | 98.32 | 98.29 | 98.32 |
| | LOW | 84.17 | 98.53 | 86.08 | 97.14 | 85.11 | 91.35 |
| | HIGH | 99.69 | 96.63 | 95.23 | 97.86 | 97.41 | 98.16 |

**Table 10.** Balanced accuracy of proposed feature selection vs. conventional methods using EXT model

| SN | Feature Selection Method | NOF | D1 (%) | D2 (%) | D3 (%) | D4 (%) | Model | Time (Sec.) for feature selection |
|---|---|---|---|---|---|---|---|---|
| 1 | Information Gain | 32 | 76.23 | 72.57 | 73.71 | 73.66 | EXT | 94.76 |
| 2 | Logistic Regression | 27 | 71.73 | 89.53 | 89.58 | 89.57 | EXT | 4.53 |
| 3 | Variance Threshold | 18 | 82.74 | 80.71 | 81.27 | 81.32 | EXT | 0.55 |
| 4 | Random Forest Importance | 21 | 82.07 | 79.97 | 80.54 | 80.56 | EXT | 174.80 |
| 5 | Extra Tree Classifier Importance | 17 | 81.96 | 79.85 | 80.36 | 80.37 | EXT | 16.78 |
| 6 | Base Line 78 Features | 78 | 82.18 | 80.06 | 80.78 | 80.71 | EXT | - |
| 7 | Proposed | 58 | 96.12 | 96.56 | 96.67 | 96.66 | EXT | 0.49 |

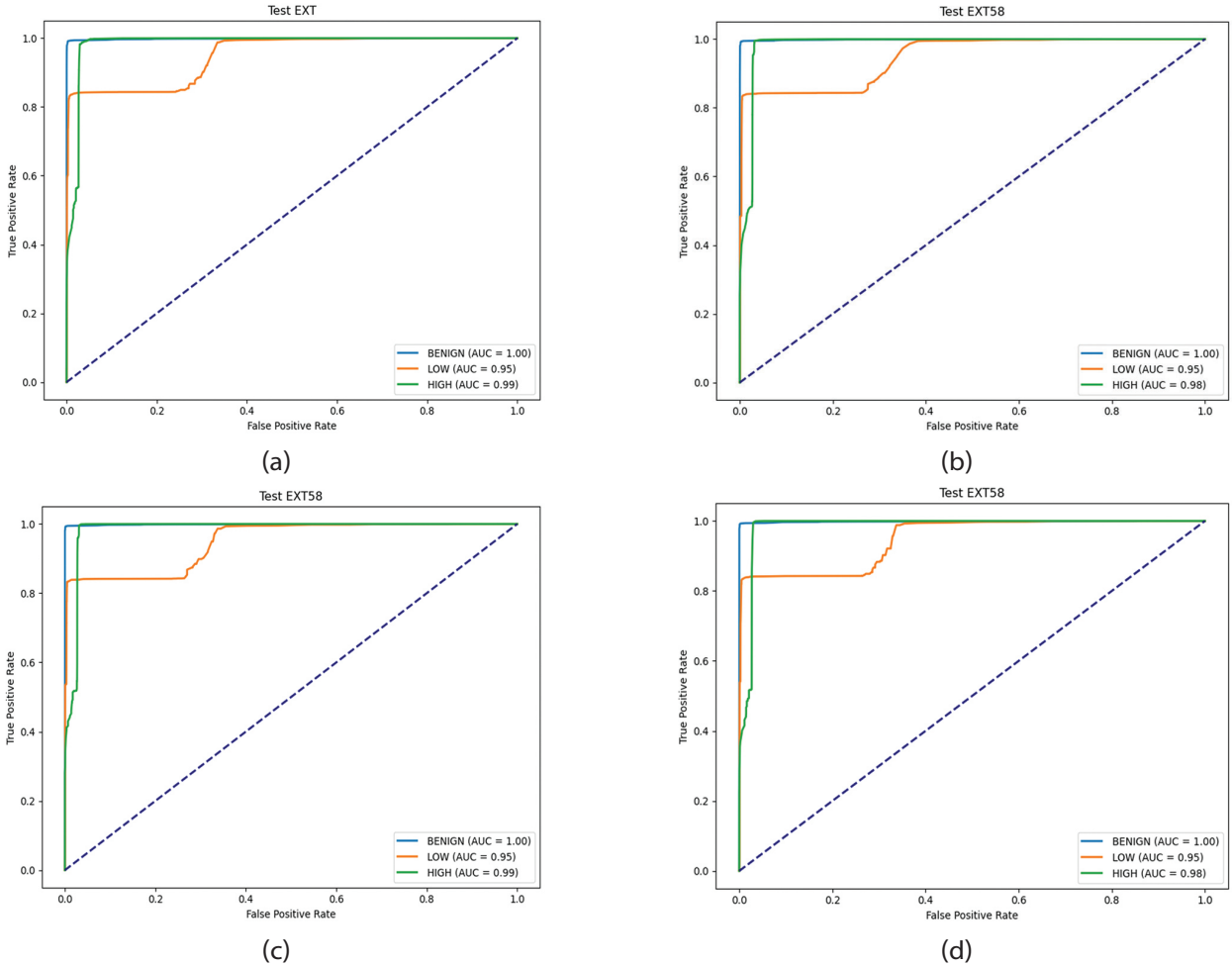



**Fig. 2.** (**a**) ROC curve of EXT model for test dataset D1 (**b**) ROC curve of EXT model for test dataset D2 (**c**) ROC curve of EXT model for test dataset D3 (**d**) ROC curve of EXT model for test dataset D4

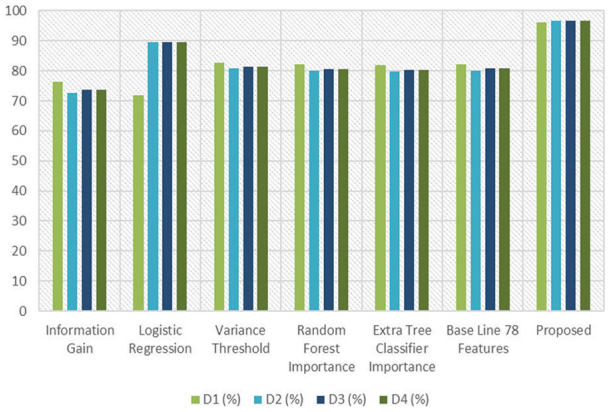


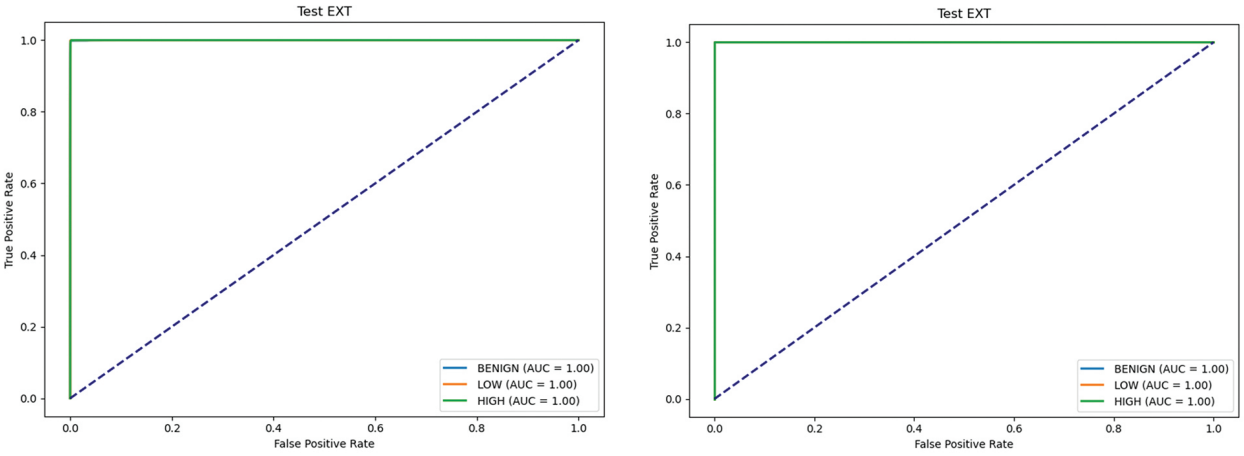

**Fig. 3.** Comparison of proposed feature selection vs. Conventional methods using EXT model

## STATE-OF-THE-ART COMPARISON WITH EXISTING WORKS:

Table 11 compares the proposed method with state-of-the-art existing systems over the four test datasets (D1, D2, D3, and D4). The existing system [27] showed the balanced accuracy (97.16%) is higher than the proposed method over the D4 test dataset. However, this method demonstrated inconsistent performance over the four test datasets. When compared to [27], the proposed system showed consistent performance with 96.50% balanced accuracy on average. Though existing system's feature dimensions are lower compared to the proposed method, the low-rate and high-rate DDoS attack detection performance of the proposed method is superior to the existing methods and systems.

## EVALUATION ON CICIDS2017 AND CICIDS2018:

The 58 features obtained using the proposed feature selection method are projected on CICIDS2017 and CICIDS2018 datasets and normalized using min-max scalar. The normalized training dataset is then used to train the EXT classifier and is validated using validation dataset. Then the proposed method is evaluated w.r.t testing dataset using the trained and validated EXT model. The performance of EXT model, over the CICIDS2017 and CICIDS2018 datasets are depicted in Table 12. The experiment results proved that the proposed method showed better balanced accuracies (an average of 99.81% and 99.99%) over the two datasets.




(a) (b)

**Fig 4.** (**a**) ROC curve of EXT model for CICIDS2017, (**b**) ROC curve of EXT model for CICIDS2018.

**Table 11.** Comparison of proposed method to existing research studies on DDoS attack detection w.r.t balanced accuracy metric metric over the CICDDoS2019 dataset

| SN | Author & Year | FC | Model | Balanced accuracy of testing datasets | | | |
|---|---|---|---|---|---|---|---|
| | | | | D1 (%) | D2 (%) | D3 (%) | D4 (%) |
| 1 | [6] & 2019 | 24 | EXT | 84.93 | 83.53 | 83.88 | 83.98 |
| 2 | [9] & 2020 | 10 | EXT | 64.13 | 59.52 | 62.73 | 62.81 |
| 3 | [13] & 2021 | 10 | EXT | 72.81 | 86.96 | 86.50 | 90.91 |
| 4 | [14] & 2021 | 68 | EXT | 93.15 | 78.80 | 78.54 | 93.32 |
| 5 | [27] & 2022 | 40 | EXT | 96.66 | 91.40 | 92.42 | 97.16 |
| 6 | [10] & 2022 | 20 | EXT | 82.87 | 82.84 | 82.50 | 83.12 |
| 7 | [28] & 2023 | 6 | EXT | 77.27 | 76.85 | 76.05 | 76.12 |
| 8 | [18] & 2024 | 14 | EXT | 64.40 | 61.59 | 61.74 | 61.74 |
| 9 | [11] & 2024 | 22 | EXT | 73.69 | 71.42 | 72.38 | 72.36 |
| 10 | [15] & 2024 | 43 | EXT | 80.25 | 75.85 | 77.61 | 78.07 |
| 11 | [29] & 2024 | 10 | EXT | 73.55 | 74.72 | 73.35 | 73.25 |
| 12 | Base line | 78 | EXT | 82.19 | 80.06 | 80.79 | 80.72 |
| 13 | Proposed | 58 | EXT | 96.12 | 96.56 | 96.67 | 96.66 |

**Table 12.** Performance metrics of EXT model using CICIDS2017 and CICIDS2018 datasets

| Dataset | Class Label | Sns. or Recall (%) | Spe. (%) | Pre. (%) | Acc. (%) | F-Score (%) | BA (%) |
|---|---|---|---|---|---|---|---|
| CICIDS2017 | BENIGN | 99.53 | 99.94 | 99.85 | 99.85 | 99.69 | 99.74 |
| | LOW | 99.88 | 99.97 | 99.83 | 99.96 | 99.85 | 99.92 |
| | HIGH | 99.93 | 99.69 | 99.78 | 99.83 | 99.86 | 99.81 |
| CICIDS2018 | BENIGN | 100 | 99.99 | 99.99 | 99.99 | 99.99 | 99.99 |
| | LOW | 100 | 100 | 100 | 100 | 100 | 100 |
| | HIGH | 99.99 | 100 | 100 | 99.99 | 99.99 | 99.99 |

The ROC curves of EXT model over the CICIDS2017 and CICIDS2018 datasets is depicted in Fig. 4

Results proved that our proposed method also performed better on the other two popular datasets (CICIDS2017 and CICIDS2018). The EXT model performance on the CICIDS2017 dataset in terms of accuracy, precision, recall, and f-score was 99.81%, while on the CICIDS2018 dataset, it was 99.99%. This indicates that our proposed model achieved generalizability.

Here is a summary of the results and key observations:

- Authors & Years: The studies range from 2019 to 2024, with each study offering performance scores for four different datasets (D1, D2, D3, and D4).
- Performance (FC): The number of features selected (FC) varies across studies, from as low as 6 to as high as 78.
- Performance Scores (D1 to D4): The accuracy scores (D1, D2, D3, and D4) vary across various IDS studies, with values generally falling within a range from 59.52% to 97.16%. The highest performance scores tend to appear in more recent studies (2022-2024).
- Baseline: The baseline performance, with 77 features selected, shows moderate accuracy (ranging from 80.06% to 82.19%).
- Proposed Model: The proposed model, with 58 features, achieves very high performance, with accuracy scores of 96.12%, 96.56%, 96.67%, and 96.66% w.r.t D1, D2, D3, and D4 datasets respectively, outperforming the baseline and other state-of-the-art studies.

**Key Observations**

i. The proposed model demonstrates significant improvement over previous research studies on DDoS attack detection, with higher accuracy across all datasets.

ii. The proposed feature selection method reduced 33.33% of the feature space.

iii. The computational cost of the EXT model using 78 features (baseline features) is 25.5 seconds, whereas using 58 features obtained by proposed method it is just 14.99 sec.

iv. The baseline and earlier studies (2019-2020) generally show lower performance, indicating that newer models, including the proposed one, offer enhanced results.

v. Studies with fewer features (e.g., [6] in 2019 and [9] in 2020) typically show lower accuracy, while more recent studies (especially from 2022 and 2023) exhibit better accuracy, possibly due to improved methodologies or optimizations in feature selection and model performance.

Thus, this summary highlights the significant advantage of the proposed method in comparison to previous work, both in terms of accuracy and feature selection.

## 6. CONCLUSION

Distributed Denial of Service (DDoS) attacks can severely impact IT services by rendering systems inaccessible to legitimate users. Despite the challenge involved in detection of DDoS attacks, a much more critical challenge is to differentiate LRDDoS traffic from legitimate traffic. In this paper, we propose a feature selection method that leverages the statistical t-Test to improve the IDS ability to predict LRDDoS and HRDDoS attack traffic more accurately and precisely.

The features obtained using the proposed feature selection method aids the machine learning model to detect LRDDoS and HRDDoS attacks at a 95% confidence level. We evaluated the proposed method on CICIDS2017, CICIDS2018, and CICDDoS2019 datasets. To generalize the learning model for intrusion detection, we evaluated the performance of the trained model using four distinct testing datasets obtained using CICDDoS2019 dataset which contains network traffic flows unseen during training and validation phase. For evaluation, we have considered twelve machine learning classifiers. Among all learning models, the Extra Tree (EXT) model has performed better. When these four testing day datasets are used for experimental study, the EXT model has achieved an average accuracy of 96.50%, a precision of 96.58%, and an F-Score of 96.50%. Overall, the EXT model showed an average accuracy of 99.81% and 99.99% on CICIDS2017 and CICIDS2018 datasets respectively. These results indicate that feature set obtained using the proposed feature selection with extra tree learning machine addressed generalizability.

It is also observed that the computational time for finding the feature subset is much lower compared to the conventional methods and that the proposed method shows comparatively better performance in discriminating low-rate DDoS attack, high-rate DDoS attack and benign network traffic.

In this paper, the research work is limited to finding an optimal feature subset based on feature selection using t-Test and integrating t-Test feature selection with

EXT classifier for machine learning. Future research work could focus on improving the accuracy of LRDDoS attacks detection using new feature extraction methods.

## 7. REFERENCES:


[1] S. Rajagopal, P. P. Kundapur, Hareesha K. S., "Towards Effective Network Intrusion Detection: From Concept to Creation on Azure Cloud", IEEE Access, Vol. 9, 2021, pp. 19723-19742.

[2] U. S. Chanu, K. J. Singh, Y. J. Chanu, "A dynamic feature selection technique to detect DDoS attack", Journal of Information Security and Applications, Vol. 74, 2023, p. 103445.

[3] N. Singh, A. Kaur, "Feature selection for artificial neural network based intrusion detection system", International Journal For Technological Research In Engineering, Vol. 2, No. 11, 2015, pp. 2681-2683.

[4] S. Das, S. Saha, A. T. Priyoti, E. K. Roy, F. T. Sheldon, A. Haque, "Network Intrusion Detection and Comparative Analysis Using Ensemble Machine Learning and Feature Selection", IEEE Transactions on Network and Service Management, Vol. 19, No. 4, 2023, pp. 4821-4833.

[5] Kurniabudi, D. Stiawan, Darmawijoyos, M. Y. Bin Idris, A. M. Bamhdi, R. Budiarto, "CICIDS-2017 Dataset Feature Analysis With Information Gain for Anomaly Detection", IEEE Access, Vol. 8, 2020, pp. 132911-132921.

[6] I. Sharafaldin, A. H. Lashkari, S. Hakak, A. A. Ghorbani, "Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy", Proceedings of the International Carnahan conference on Security Technology, Chennai, India, 1-3 October 2019, pp. 1-8.

[7] S. Li, J. Xu, P. Liu, X. Li, P. Wang, X. Jin, "Truncated Lanczos-TSVD: An Effective Dimensionality Reduction Algorithm for Detecting DDoS Attacks in Large-Scale Networks", IEEE Transactions on Network Science and Engineering, Vol. 11, No. 5, 2024, pp. 4689-4703.

[8] M. Hajimaghsoodi, R. Jalili, "RAD: A Statistical Mechanism Based on Behavioral Analysis for DDoS Attack Countermeasure", IEEE Transactions on Information Forensics and Security, Vol. 17, 2022, pp. 2732-2745.

[9] Y. Jia, F. Zhong, A. Alrawais, B. Gong, X. Cheng, "FlowGuard: An Intelligent Edge Defense Mechanism Against IoT DDoS Attacks", IEEE Internet of Things Journal, Vol. 7, No. 10, 2022, pp. 9552-9562.

[10] A. Maheshwari, B. Mehraj, M. S. Khan, M. S. Idrisi, "An optimized weighted voting based ensemble model for DDoS attack detection and mitigation in SDN environment", Microprocessors and Microsystems, Vol. 89, 2022, p. 104412.

[11] S. Mahdavifar, A. A. Ghorbani, "CapsRule: Explainable Deep Learning for Classifying Network Attacks", IEEE Transactions on Neural Networks and Learning Systems, Vol. 35, No. 9, 2024, pp. 12434-12448.

[12] E. Q. Effah, E. O. Osei, M. Dorgbefu Jnr, A. Tetteh, "Hybrid Approach to Classification of DDoS Attacks on a Computer Network Infrastructure", Asian Journal of Research in Computer Science, Vol. 17, No. 4, 2024, pp. 19-43.

[13] G. C. Amaizu, C.I. Nwakanma, S. Bhardwaj, J. M. Lee, D. S. Kim, "Composite and efficient DDoS attack detection framework for B5G networks", Computer Networks, Vol. 188. 2021, p. 107871.

[14] A. E. Cil, K. Yildiz, A. Buldu, "Detection of DDoS attacks with feed-forward based deep neural network model", Expert Systems with Applications Vol. 169, 2021, p. 114520.

[15] A. A. Najar, S. M. Naik, "A Robust DDoS Intrusion Detection System Using Convolutional Neural Network", Computers and Electrical Engineering, Vol. 117, 2024, pp. 1-19.

[16] Y. Wei, J. Jang-Jaccard, F. Sabrina, A. Singh, W. Xu, S. Camtepe, "AE-MLP: A Hybrid Deep Learning Approach for DDoS Detection and Classification", IEEE Access, Vol. 9, 2021, pp. 146810-146821.

[17] M. A. Ferrag, L. Shu, H. Djallel, K. R. Choo, "Deep learning-based intrusion detection for distributed denial of service attack in agriculture 4.0", Electronics, Vol. 10, No. 11, 2021, p. 1257.

[18] A. A. Alashhab, M. S. Zahid, B. Isyaku, A. A. Elnour, W. Nagmeldin, A. Abdelmaboud, T. A. A. Abdullah, U. D. Maiwada, "Enhancing DDoS Attack Detection and Mitigation in SDN Using an Ensemble Online Machine Learning Model", IEEE Access, Vol. 12, 2024, pp. 51630-51649.

[19] O. Barut, Y. Luo, P. Li, T. Zhang, "R1DIT: Privacy-Preserving Malware Traffic Classification with Attention-Based Neural Networks", IEEE Transactions on Network and Service Management, Vol. 20, No. 2, 2023, pp. 2071-2085.

[20] Z. Li, H. Jin, D. Zou, B. Yuan, "Exploring New Opportunities to Defeat LRDDoS Attack in Container-Based Cloud Environment", IEEE Transactions on Parallel and Distributed Systems, Vol. 31, No. 3, 2020, pp. 695-706.

[21] M. F. Saiyed, I. Al-Anbagi, "Flow and unified information-based DDoS attack detection system for multi-topology IoT networks", Internet of Things, Vol. 24, 2023, p. 100976.

[22] R. Manthena, R. Vangipuram, "Integrating Machine Learning and T-tests to Optimize Distributed Denial of Service Attacks Detection", International Journal of Intelligent and Engineering Systems, Vol. 17, No. 6, 2024, pp. 1023-1043.

[23] M. F. Saiyed, I. Al-Anbagi, "A Genetic Algorithm-and t-Test-Based System for DDoS Attack Detection in IoT Networks", IEEE Access, Vol. 12, 2024, pp. 25623-25641.

[24] I. Sharafaldin, A. Gharib, A. H. Lashkari, A. A. Ghorbani, "Towards a reliable intrusion detection benchmark dataset", Software Networking, Vol. 1, 2018, pp. 177-200.

[25] I. Sharafaldin, A. H. Lashkari, A. A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization", Proceedings of the 4th International Conference on Information Systems Security and Privacy, Portugal, 22-24 January 2018, pp. 108-116.

[26] A. Gharib, I. Sharafaldin, A. H. Lashkari, A. A. Ghorbani, "An evaluation framework for intrusion detection dataset", Proceedings of the International Conference on Information Science and Security, Pattaya, Thailand, 19-22 December 2026, pp. 1-6.

[27] D. Akgun, S. Hizal, U. Cavusoglu, "A new DDoS attacks intrusion detection model based on deep learning for cybersecurity", Computers and Security, Vol. 118, 2022, p. 102748.

[28] R. K. Batchu, H. Seetha, "On improving the performance of DDoS attack detection system", Microprocessors and Microsystems, Vol. 93, 2022, p. 104571.

[29] D. M. Sharif, H. Beitollahi, "Detection of application-layer DDoS attacks using machine learning and genetic algorithms", Computers and Security, Vol. 135, 2023, p. 103511.

**Abbreviations:**

| | |
|---|---|
| IG | Information Gain |
| LR | Logistic Regression |
| RFFI | Random Forest Feature Importance |
| EXT | Extra Tree Classifier |
| VT | Variance Threshold |
| FC | Feature Count |
| SN | Serial Number |

**Appendix:**
List of 58 features selected using proposed feature selection

| SN | Feature Name | SN | Feature Name | SN | Feature Name | SN | Feature Name |
|---|---|---|---|---|---|---|---|
| 1 | Total Fwd Packets | 16 | Flow IAT Max | 31 | Packet Length Std | 46 | Active Mean |
| 2 | Total Backward Packets | 17 | Fwd IAT Mean | 32 | Packet Length Variance | 47 | Active Std |
| 3 | Total Length of Fwd Packets | 18 | Fwd IAT Max | 33 | SYN Flag Count | 48 | Active Max |
| 4 | Fwd Packet Length Max | 19 | Bwd IAT Total | 34 | RST Flag Count | 49 | Active Min |
| 5 | Fwd Packet Length Min | 20 | Bwd IAT Mean | 35 | ACK Flag Count | 50 | Idle Mean |
| 6 | Fwd Packet Length Mean | 21 | Bwd IAT Std | 36 | URG Flag Count | 51 | Idle Std |
| 7 | Fwd Packet Length Std | 22 | Bwd IAT Max | 37 | CWE Flag Count | 52 | Idle Min |
| 8 | Bwd Packet Length Max | 23 | Bwd IAT Min | 38 | Down/Up Ratio | 53 | Inbound |
| 9 | Bwd Packet Length Min | 24 | Fwd PSH Flags | 39 | Average Packet Size | 54 | Flow Duration |
| 10 | Bwd Packet Length Mean | 25 | Bwd Header Length | 40 | Avg Fwd Segment Size | 55 | Fwd IAT Total |
| 11 | Bwd Packet Length Std | 26 | Fwd Packets/s | 41 | Avg Bwd Segment Size | 56 | Fwd IAT Std |
| 12 | Flow Bytes/s | 27 | Bwd Packets/s | 42 | Init_Win_bytes_forward | 57 | Fwd Header Length |
| 13 | Flow Packets/s | 28 | Min Packet Length | 43 | Init_Win_bytes_backward | 58 | Idle Max |
| 14 | Flow IAT Mean | 29 | Max Packet Length | 44 | act_data_pkt_fwd | | |
| 15 | Flow IAT Std | 30 | Packet Length Mean | 45 | min_seg_size_forward | | |