Using Machine Learning to Predict Distributed Denial-of-Service (DDoS) Attack

Qozeem Adeniyi Adeshina* and Baidya Nath Saha
Department of Mathematical and Physical Sciences, Concordia University of Edmonton, Alberta, T5B 4E4, Canada

* Corresponding author

doi:https://doi.org/10.21467/proceedings.115.21

ABSTRACT

The IT space is growing in all aspects ranging from bandwidth, storage, processing speed, machine learning and data analysis. This growth has consequently led to more cyber threat and attacks which now requires innovative and predictive security approach that uses cutting-edge technologies in order to fight the menace. The patterns of the cyber threats will be observed so that proper analysis from different sets of data will be used to develop a model that will depend on the available data. Distributed Denial of Service is one of the most common threats and attacks that is ravaging computing devices on the internet. This research talks about the approaches and the development of machine learning classifiers to detect DDoS attacks before it eventually happen. The model is built with seven different selection techniques each using ten machine learning classifiers. The model learns to understand the normal network traffic so that it can detect an ICMP, TCP and UDP DDoS traffic when they arrive. The goal is to build a data-driven, intelligent and decision-making machine learning algorithm model that will use classifiers to categorize normal and DDoS traffic using KDD-99 dataset. Results have shown that some classifiers have very good predictions obtained within a very short time.

Keywords: Cybersecurity, DDoS traffic, KDD-99 dataset.

I. Introduction

Cybersecurity attacks pose a very big threats to businesses and organizations around the world. It is a situation where attackers called cybercriminals use resources at their disposal to take aggressive action against a single computer device or a network of computers devices. A cybersecurity attack can come in several ways - Distributed Denial-of-Service (DDoS) attack where heavy traffic is focused towards the target to bring it down, Ransomware attack where cybercriminals uses malware to encrypt victim's file and demand for ransom, Phishing attack is a situation where the criminals disguise to fool the target into doing harmful activities, Malware attack is using malicious software to damage the target computer, SQL Injection is a situation where an attacker exploits a vulnerability to take over the victim's database. There are different intentions that these criminals have when carrying out the malicious activities. It ranges from stealing data for use, financial gain, competitive advantage etc. In order to defeat these dangerously growing attacks, there is need to learn how to foresee the attacks and the need to know what security measures to put in place to protect the organizational businesses. Distributed Denial of service (DDoS) is one of the most used methods of attacking because it is difficult to defeat. The reason for this difficulty is due to the attack appearing from different IP address locations across the internet concurrently, making identifying the source of the attack more difficult. There are lots of devices on the internet that are vulnerable to DDoS attacks. The DDoS attack can be targeted towards any network devices, but mostly web servers. The attack is achieved by funneling requests that will eventually saturate and overwork the target device's resources like processor utilization, bandwidth, memory etc. such that genuine request will not be processed thus optimal

Proceedings DOI: 10.21467/proceedings.115; Series: AIJR Proceedings; ISSN: 2582-3922; ISBN: 978-81-947843-5-7

operation are hampered. DDoS attacks can be categorized into three groups viz

Volume based attack – The high volume of traffic is directed towards the target using Synchronize (SYN) Flood, User Datagram Protocol (UDP) Flood, Internet Control Message Protocol (ICMP) Flood and other spoofed packet flood to overwhelm the bandwidth of the target computer or network measured in bits per second (bps).

Protocol based attack – This type of DDoS focuses on exploiting server resources by targeting Layer 3 and Layer 4 protocol communications with malicious connection requests measured in Packets per second (Pps)

Application based attack – This attack focuses on web applications and are regarded as the most sophisticated and serious type of attacks. It exploits weakness and flood requests at layer 7 (Application layer) measured in Requests per second (Rps).

II. Literature Review

This section provides a review of Distributed Denial of service attack detection using machine learning techniques. Numerous cyber-attack detection techniques and protection strategies have been proposed in recent years because of the rise in these threats. Studies have revealed that these detection systems come in three major ways; anomaly, signature or hybrid of the two. In the three cases, a set action will be performed if a signature is matched or not in the case of signature-based and if a deviation between the normal set parameter and the current in the case of anomaly-based.

The favorable position of the signature-based approach is the low level of incorrect alarm it triggers. However, the issue is to compile signatures that will cover all possibilities of the attack. Contrarily, the anomaly-based approach has more incorrect alarms but can detect unknown attacks and requires more computational resources. While the hybrid approach makes use of the two strategies [1], [2]. DDoS attacks are specific type of network intrusion that has drawn the attention of a lot as mentioned in recent surveys [3], [4].

Numerous strategies have been adopted in the past regarding approaches adopted for DDoS classification. This classification study has provided a basis for DDoS flooding attack categorization using targeted protocol level [5].

Network/Transport-Level DDoS Flooding Attacks: These attacks are typically launched using User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), Transmission Control Protocol (TCP), and Domain Name System (DNS) protocol packets.

Application-Level DDoS Flooding Attacks: These attacks are focused on disrupting legitimate services by exhausting the target server resources, e.g. Central Processing Unit (CPU), sockets, memory and input/output (I/O) bandwidth. This category of attack is sneakier in operation than volume-related attacks because they are very similar to normal traffic and generally consume less bandwidth.

There are great challenges in dealing with DDoS attacks. These challenges have to do with timing, how early they are detected and preventing the attack. Although the complete solution to this menace has not been accomplished[5], [6]. A summary of some reviews of detection of Distributed Denial of Services using machine learning is summarized in the table below.

Poggi et al. [7] used an online discrete event Simulator to collect data traffic information from each node independently and then trained each node of network with Naive Bayes algorithm to determine DDoS attack impact on network by increasing efficiency of DDoS attack detection time.

Stefan at al. [8] put consideration to utilize features of network data traffic flow and network resources to use most of the genuine user requests.

TABLE I: Literature review of DDoS attack detection techniques using machine learning algorithms.

Author	Year	Learning Method	Dataset
Poggi et al. [7]	2008	Element Wise Learning, Naive Bayes method.	Online OmNET++ simulator-based data.
Stefan at al. [8]	2007	Artificial Neural Networks (ANN), Extended Back-Propagation algorithm	Different levels of network stack data using network emulator
Shon et al. [9]	2005	Genetic Algorithm (GA), Enhanced Support Vector Machine (SVM)	1999 DARPA IDS dataset by MIT Lincoln Lab.
Muhammad et al. [10]	2019	kNN, SVM and RF models	CICIDS2017.
Selvakumar et al. [11]	2011	RBPBoost Classification Algorithm, Back propagation, Weighted Majority Voting.	KDD Cup, DARPA 1999, DARPA 2000 datasets
Wei et al. [12]	2009	Fourier to Time Reconstruction algorithm.	NS2 simulation data
Symeon at al. [13]	2002	Hybrid perception based back-propagation NN, Fuzzy ARTMAP.	DARPA 98, 99 datasets.

Shon et al. [9] utilized Genetic Algorithm (GA) for features selection using maximum available fields of network data traffic and then applied Support Vector Machine (SVM) for classification of genuine and DDoS infected packets.

Muhammad et al. [10] used supervised machine learning techniques as classifiers to classify DDoS attacks. The technique includes Random Forests (RF), K-Nearest neighbors (KNN) and Support Vector Machines (SVM).

Selvakumar et al. [11] utilized multiple backward propagation of errors (back-propagation) models to obtain basic result. Q-statistics techniques along with Weighted Majority Voting and Weighted Product Rule are used for selecting best back-propagation model used initially in order to enhance classification accuracy. However, the technique requires a manual weight setting which may as well not be accurate

Wei et al. [12] used Fourier to time reconstruction algorithm to propose a DDoS attack detection technique where the service source sends pair of probes to service request node and verify the legitimacy of the request using the gap between probes.

Symeon at al. [13] used statistical Klomogrov-Smirnov test to fetch similarities from network data measurements. Further to the first statistical approach, they applied five distinct neural network techniques for classification purposes. Back-propagation and hybrid perception based back-propagation neural network techniques achieve the highest classification accuracy than others.

DDoS attacks are quickly becoming the most prevalent type of cyber threat, growing rapidly in recent years in both number and volume according to recent market research. DDoS attacks may remain on the internet for some time. The solution to this problem includes the adoption of detection and mitigation strategies that are easily adoptable and economically viable. Besides, these approaches should leverage existing provider infrastructure and be implemented considering new scientific and technological trends.

III. Methodology

Detecting the different types of DDoS volumetric attacks (TCP flood, UDP flood, ICMP flood) will be considered in this research. The architecture that attackers use to carry out these types of DDoS attack is shown in Fig1 which is divided into Control and Attack stage [14].

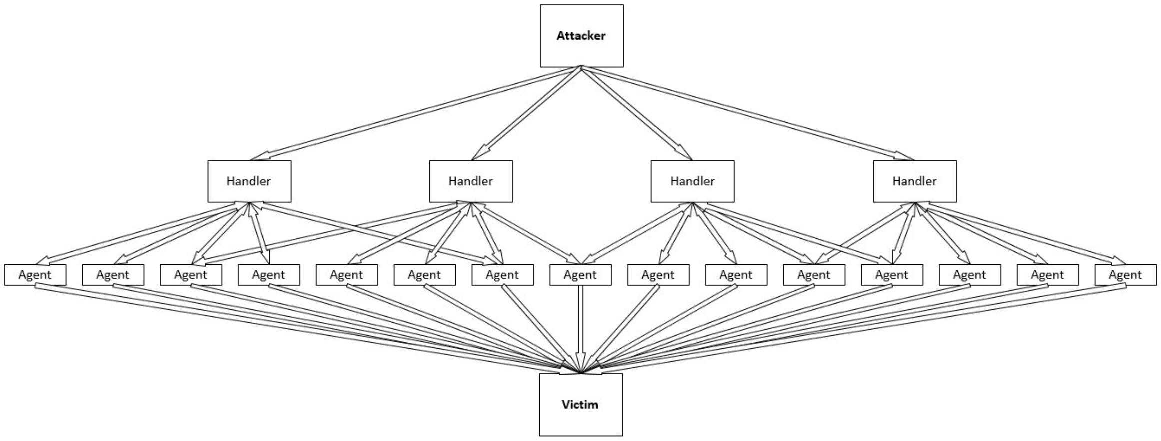


Fig. 1: DDoS Attack Architecture

The nodes under control stage are vulnerable targets (Handlers) that are used to control another set of vulnerable targets (Agents). The attacker being the central controller that is using the handlers and agents to finally launch a distributed attack traffic (attack stage) on the victim. The volumetric attacking traffic can be TCP, UDP or ICMP which will eventually overwhelm the final target (victim).

The dataset used is from The Third International Knowledge Discovery and Data Mining Tools Competition, which was held in conjunction with KDD-99 The Fifth International Conference on Knowledge Discovery and Data Mining. This database contains a standard set of data to be audited, which includes a wide variety of intrusions simulated in a military network environment. The dataset has been split to 70% training set and 30% testing set.

This section describes how data is extracted from the dataset described above, and the feature selection techniques that are used. It describes how different machine learning algorithms and techniques are used to classify traffic into normal or DDoS infected under different feature selection methods. Machine learning is a technique that draws implications from existing data using mathematical and statistical methods. This will then be used to forecast or predict the unknown with the implications. There are 10 machine learning models and 7 feature selection methods that were used in this research paper. Gradient Boosting, Random Forest, Logistic Regression, K-Nearest Neighbor (KNN), Decision Tree, Support Vector Machine (SVM), Neural Network, Naïve Bayes, AdaBoost and Multinomial Naive Bayes will be used to carry out the network traffic classification and their performance will be analyzed.

The ten classifiers adopt the same type of framework structure as shown in Fig 2. The dataset with forty features will be fed into the feature selection algorithm. These different feature selection techniques will produce the most suitable attributes that will help to correctly predict if a DDoS attack is imminent. The relevant features will then be used by the DDoS classifier to appropriately classify into ICMP, TCP, UDP or normal packets.

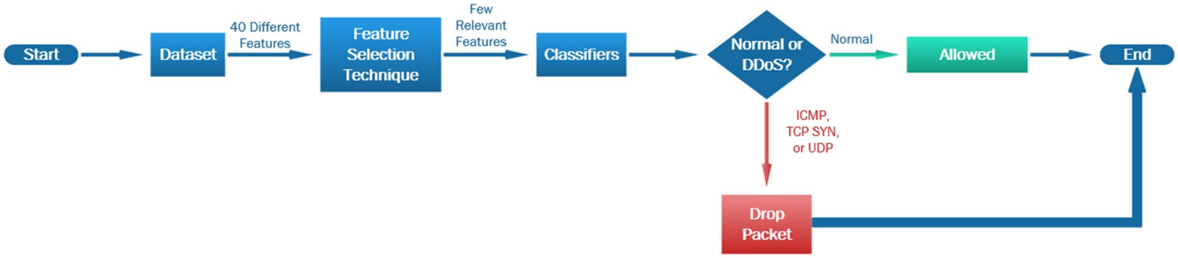


Fig. 2: Feature Selection and Classification System

Feature Selection Methods Used

Various types of DDoS attacks are studied to select the traffic parameters that change unusually during such attacks. There are seven feature selection techniques used to extract relevant attributes for the classification. The seven feature Selection methods used are detailed below.

1. Variance Threshold: Sets a threshold and any feature with a variance lower than this threshold will be removed.
2. Mutual Information: Calculates mutual information value of all independent value with respect to dependent variable.
3. Anova f-Test: Analysis of variance uses f-test to statistically test the equality of means.
4. Selectk Best: Scores the features using a function and then removes all but the highest scoring features.
5. Pearson Correlation: This is a number between -1 and 1 that indicates the extent to which two variables are linearly related.
6. RFE Wrapper: Uses iterative search to narrow down features.
7. Embedded Methods: Forces the model to set a coefficient of non-independent attributes to zero.

Brief Description of the Ten Classifiers Used

1. K-Nearest Neighbor: This is one of the methods for early detection of DDoS attacks. It is a simple and easily applicable supervised machine learning algorithm that can be used for regression and classification. K being a positive integer, KNN uses nearest K neighbors to determine the class of the new data point. It mostly uses Euclidean distance function to compute the nearest neighbor. When a new data comes in, Euclidean function is used to calculate the distance between this new data and data in the training set separately. K smallest distance (neighbors) is then selected to determine the class of the new data.

2. Gradient Boosting: This is a greedy algorithm and can overfit a training dataset quickly. It is a technique that can be used for both regression and classification issues. It produces a prediction model from several weak prediction models.

3. AdaBoost: This machine learning algorithm works by attaching weights to the observations, putting more weight on difficult to classify instances and less weight on those that were already handled well. New weak learners are added serially that focus their training on those more difficult patterns.

4. Support Vector Machine: SVM is also a supervised machine learning algorithm which can be used for both classification and regression problems. It is however, commonly used for classification. It uses hyperplane in an N-dimensional space (N is the number of features) that clearly classifies the data points.

5. Naive Bayes: This is a simple probabilistic classifier based on Bayes' Theorem which is useful for large dataset [15]. Naïve Bayes model is easy to build when the features in the datasets are independent of each other. The classifier is fast and not sensitive to unrelated features. The Naïve Bayes performs very well in binary cases for example when the classification purpose is to discriminate if the incoming packets are DDoS or normal [16]. The model learns by computing the probability of the training data.

6. Neural Network: This algorithm uses a basic building block called neurons. The collections of these connected neurons are called artificial neurons. ANN is a strong classification tool based on the artificial neuron model. Artificial neurons are designed to behave similarly to biological neurons in the biological brain.

7. Decision Tree: This classification algorithm is a simple representation for classifying examples. It is a Supervised Machine Learning technique where the data is continuously splitted according to a certain parameter.

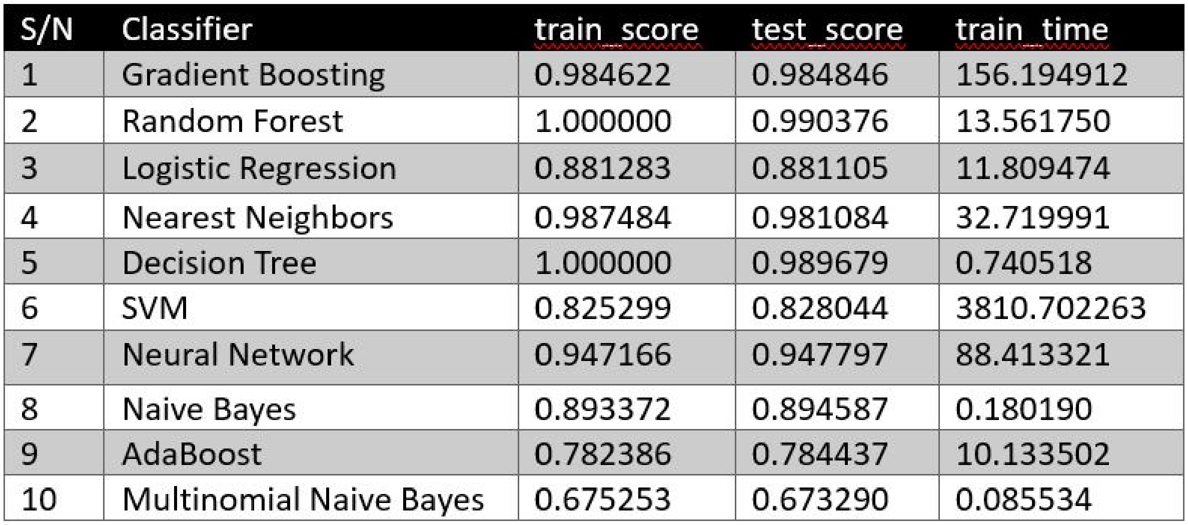
8. Random Forest: This is a tree-based and ensemble learning algorithm also used for classification and other tasks that operate by constructing a lot of decision trees from randomly selected subset of training set. It aggregates the votes from different decision trees to decide the final class of the object.

9. Logistic Regression: This classification algorithm is used when the value of the target variable is categorical in nature. Logistic regression is commonly used when the data at hand has binary output and it belongs to one class or another or is either a 0 or 1.

10. Multinomial Naïve Bayes: This algorithm considers a feature vector where a given term represents the number of times it appears or very often i.e. frequency. It is suitable for classification with discrete features.

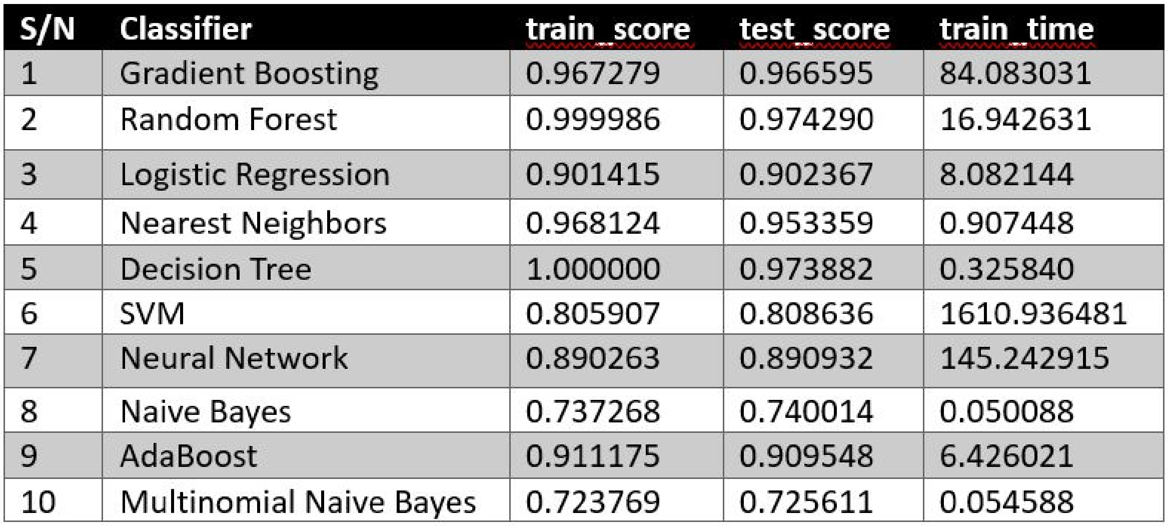
IV. Experimental Results and Discussions

The ten different classifiers produce different results under the seven different feature selection methods. The results are as displayed in the tables below



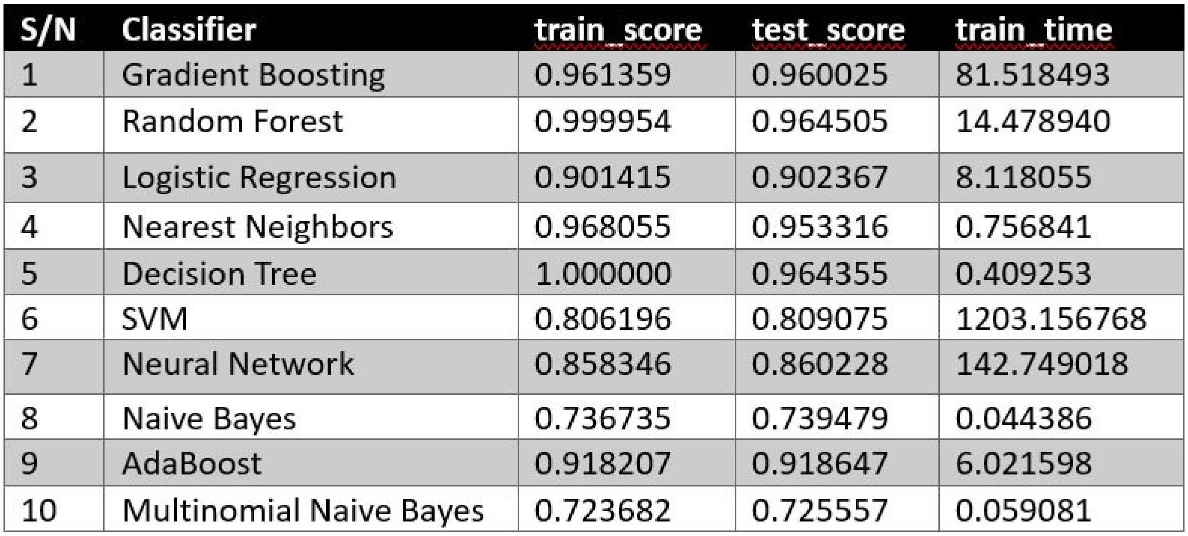
S/N	Classifier	train_score	test_score	train_time
1	Gradient Boosting	0.984622	0.984846	156.194912
2	Random Forest	1.000000	0.990376	13.561750
3	Logistic Regression	0.881283	0.881105	11.809474
4	Nearest Neighbors	0.987484	0.981084	32.719991
5	Decision Tree	1.000000	0.989679	0.740518
6	SVM	0.825299	0.828044	3810.702263
7	Neural Network	0.947166	0.947797	88.413321
8	Naive Bayes	0.893372	0.894587	0.180190
9	AdaBoost	0.782386	0.784437	10.133502
10	Multinomial Naive Bayes	0.675253	0.673290	0.085534

Fig. 3: Variance Threshold Feature Selection Method



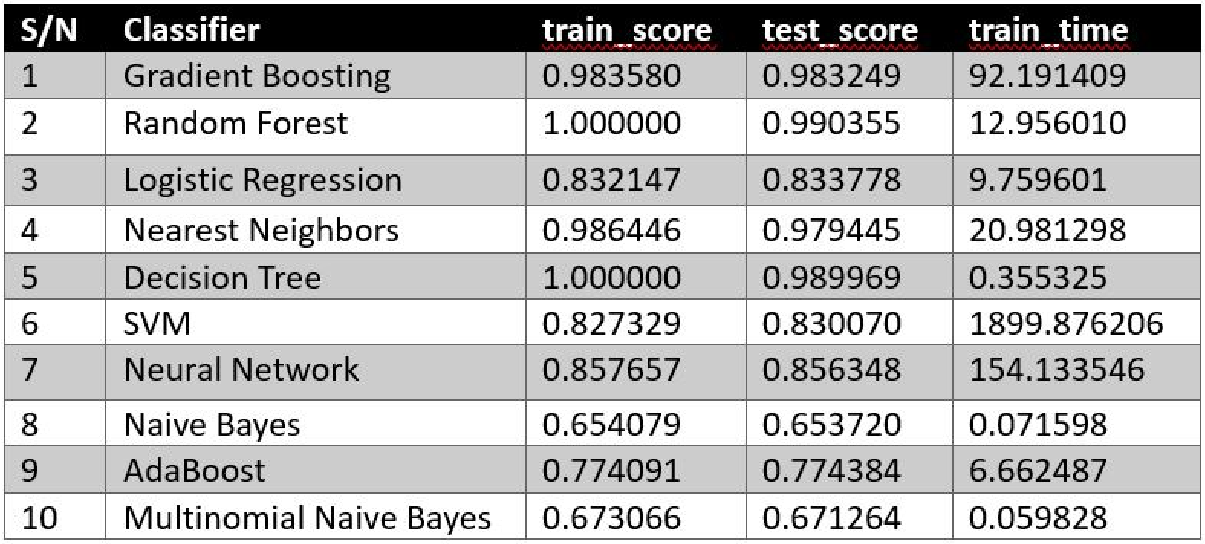
S/N	Classifier	train_score	test_score	train_time
1	Gradient Boosting	0.967279	0.966595	84.083031
2	Random Forest	0.999986	0.974290	16.942631
3	Logistic Regression	0.901415	0.902367	8.082144
4	Nearest Neighbors	0.968124	0.953359	0.907448
5	Decision Tree	1.000000	0.973882	0.325840
6	SVM	0.805907	0.808636	1610.936481
7	Neural Network	0.890263	0.890932	145.242915
8	Naive Bayes	0.737268	0.740014	0.050088
9	AdaBoost	0.911175	0.909548	6.426021
10	Multinomial Naive Bayes	0.723769	0.725611	0.054588

Fig. 4: Mutual Information Feature Selection Method



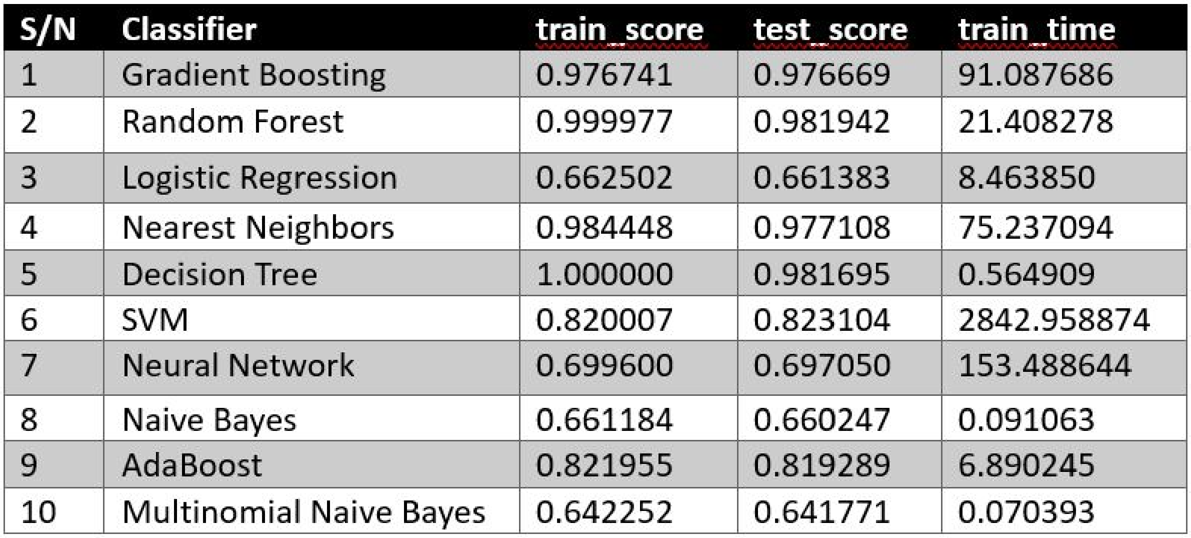
S/N	Classifier	train_score	test_score	train_time
1	Gradient Boosting	0.961359	0.960025	81.518493
2	Random Forest	0.999954	0.964505	14.478940
3	Logistic Regression	0.901415	0.902367	8.118055
4	Nearest Neighbors	0.968055	0.953316	0.756841
5	Decision Tree	1.000000	0.964355	0.409253
6	SVM	0.806196	0.809075	1203.156768
7	Neural Network	0.858346	0.860228	142.749018
8	Naive Bayes	0.736735	0.739479	0.044386
9	AdaBoost	0.918207	0.918647	6.021598
10	Multinomial Naive Bayes	0.723682	0.725557	0.059081

Fig. 5: Anova f-Test Feature Selection Method



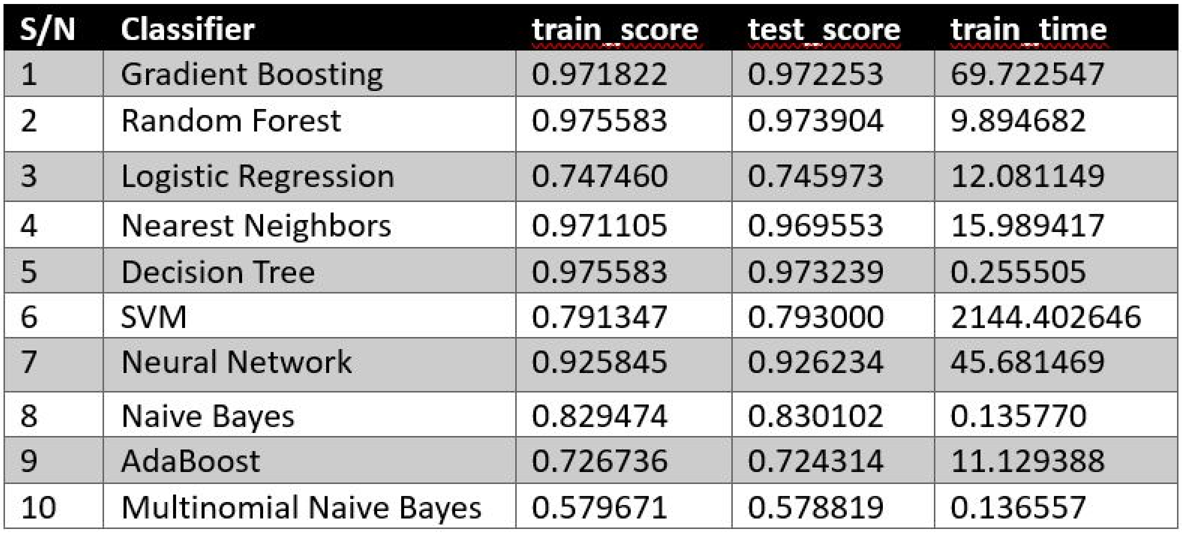
S/N	Classifier	train_score	test_score	train_time
1	Gradient Boosting	0.983580	0.983249	92.191409
2	Random Forest	1.000000	0.990355	12.956010
3	Logistic Regression	0.832147	0.833778	9.759601
4	Nearest Neighbors	0.986446	0.979445	20.981298
5	Decision Tree	1.000000	0.989969	0.355325
6	SVM	0.827329	0.830070	1899.876206
7	Neural Network	0.857657	0.856348	154.133546
8	Naive Bayes	0.654079	0.653720	0.071598
9	AdaBoost	0.774091	0.774384	6.662487
10	Multinomial Naive Bayes	0.673066	0.671264	0.059828

Fig. 6: Selectk Best Feature Selection Method



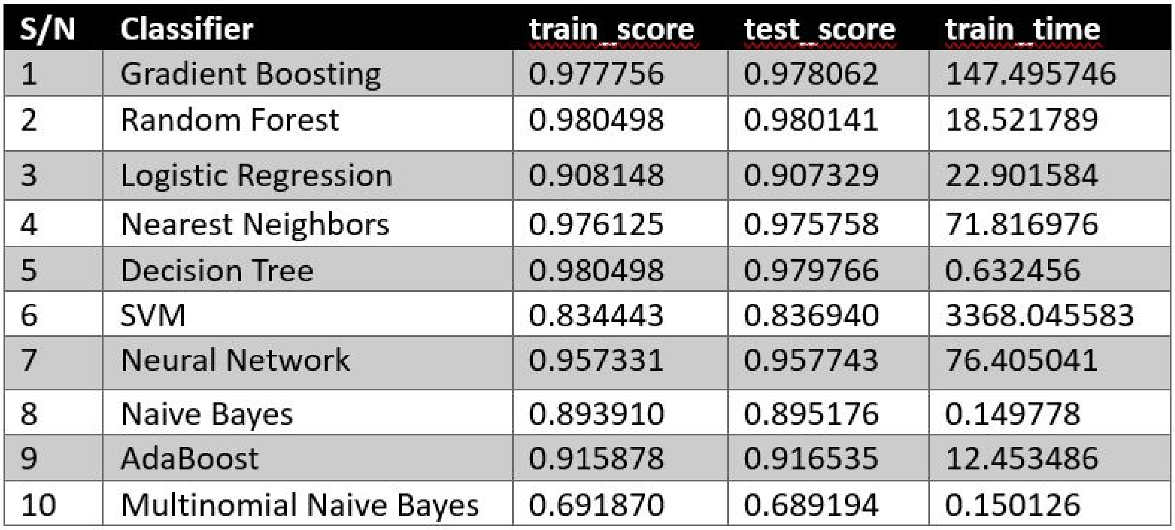
S/N	Classifier	train_score	test_score	train_time
1	Gradient Boosting	0.976741	0.976669	91.087686
2	Random Forest	0.999977	0.981942	21.408278
3	Logistic Regression	0.662502	0.661383	8.463850
4	Nearest Neighbors	0.984448	0.977108	75.237094
5	Decision Tree	1.000000	0.981695	0.564909
6	SVM	0.820007	0.823104	2842.958874
7	Neural Network	0.699600	0.697050	153.488644
8	Naive Bayes	0.661184	0.660247	0.091063
9	AdaBoost	0.821955	0.819289	6.890245
10	Multinomial Naive Bayes	0.642252	0.641771	0.070393

Fig. 7: Pearson Correlation Feature Selection Method



S/N	Classifier	train_score	test_score	train_time
1	Gradient Boosting	0.971822	0.972253	69.722547
2	Random Forest	0.975583	0.973904	9.894682
3	Logistic Regression	0.747460	0.745973	12.081149
4	Nearest Neighbors	0.971105	0.969553	15.989417
5	Decision Tree	0.975583	0.973239	0.255505
6	SVM	0.791347	0.793000	2144.402646
7	Neural Network	0.925845	0.926234	45.681469
8	Naive Bayes	0.829474	0.830102	0.135770
9	AdaBoost	0.726736	0.724314	11.129388
10	Multinomial Naive Bayes	0.579671	0.578819	0.136557

Fig. 8: RFE Wrapper Feature Selection Method



S/N	Classifier	train_score	test_score	train_time
1	Gradient Boosting	0.977756	0.978062	147.495746
2	Random Forest	0.980498	0.980141	18.521789
3	Logistic Regression	0.908148	0.907329	22.901584
4	Nearest Neighbors	0.976125	0.975758	71.816976
5	Decision Tree	0.980498	0.979766	0.632456
6	SVM	0.834443	0.836940	3368.045583
7	Neural Network	0.957331	0.957743	76.405041
8	Naive Bayes	0.893910	0.895176	0.149778
9	AdaBoost	0.915878	0.916535	12.453486
10	Multinomial Naive Bayes	0.691870	0.689194	0.150126

Fig. 9: Embedded Feature Selection Method

V. Conclusion and Future work

Based on the dataset used for this research and the outcome of classifications, some classifiers have shown consistently good results (over 95%) across all the feature selection methods. These include Gradient Boosting, Random Forest, Nearest Neighbors and Decision Tree. However, Multinomial Naive Bayes, when compared to others, has shown poor prediction performance (less than 73%). Gradient Boosting, Random Forest, Nearest Neighbors and Decision Tree machine learning algorithms are therefore recommended during DDoS classification when accuracy is the factor been considered. Similarly, some Classifiers take very long time to run and some very short time. SVM has proven to be the slowest while Multinomial Naive Bayes and Decision Tree were the fastest. Cumulatively, when both speed and accuracy is to be considered, Decision Tree classifier is therefore recommended during DDoS traffic classification. In future, we would like to implement domain knowledge to improve the performance and reduce the execution time of the classifiers.

References

[1] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network anomaly detection: Methods, systems and tools," *IEEE Communications Surveys Tutorials*, vol. 16, no. 1, pp. 303–336, 2014.

[2] W. Meng, W. Li, C. Su, J. Zhou, and R. Lu, "Enhancing trust management for wireless intrusion detection via traffic sampling in the era of big data," *IEEE Access*, vol. PP, pp. 1–1, 11 2017.

[3] M. Masdari and M. Jalali, "A survey and taxonomy of dos attacks in cloud computing: Dos attacks in cloud computing," *Security and Communication Networks*, 07 2016.

[4] R. Zuech, T. Khoshgoftaar, and R. Wald, "Intrusion detection and big heterogeneous data: a survey," *Journal of Big Data*, vol. 2, pp. 1–41, 2015.

[5] S. Taghavi Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks," *IEEE Communications Surveys amp Tutorials*, vol. 15, pp. 2046 – 2069, 11 2013.

[6] R. Chang, "Defending against flooding-based distributed denial-of-service attacks: A tutorial," *Communications Magazine, IEEE*, vol. 40, pp. 42 – 51, 11 2002.

[7] J. Berral, N. Poggi, J. Alonso, R. Gavaldà, J. Torres, and M. Parashar, "Adaptive distributed mechanism againts flooding network attacks based on machine learning," in *ACM Workshop on AISec*. ACM Press, NY, Oct 2008, pp. 43–49. [Online]. Available: http://hdl.handle.net/2117/9989;http://portal.acm.org/citation.cfm?id=1456389

[8] S. Seufert and D. O'Brien, "Machine learning for automatic defence against distributed denial of service attacks," 07 2007, pp. 1217 – 1222.

[9] T. Shon, Y. Kim, C. Lee, and J. Moon, "A machine learning framework for network anomaly detection using svm and ga," vol. 2005, 07 2005, pp. 176 – 183.

[10] M. Aamir and S. Zaidi, "Clustering based semi-supervised machine learning for ddos attack classification," *Journal of King Saud University - Computer and Information Sciences*, 02 2019.

[11] P. Kumar and S. Selvakumar, "Distributed denial of service attack detection using an ensemble of neural classifier," *Computer Communications*, vol. 34, pp. 1328–1341, 07 2011.

[12] W.-Z. Lu, W.-X. Gu, and S.-Z. Yu, "One-way queuing delay measurement and its application on detecting ddos attack," *J. Network and Computer Applications*, vol. 32, pp. 367–376, 03 2009.

[13] C. Manikopoulos and S. Papavassiliou, "Network intrusion and fault detection: A statistical anomaly approach," *Communications Magazine, IEEE*, vol. 40, pp. 76 – 82, 11 2002.

[14] S.-C. Lin and S.-S. Tseng, "Constructing detection knowledge for ddos intrusion tolerance," *Expert Systems with Applications*, vol. 27, pp. 379–390, 10 2004.

[15] A. Goyal and R. Mehta, "Performance comparison of naïve bayes and j 48 classification algorithms," 2012.

[16] R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning ddos detection for consumer internet of things devices," 04 2018.