Detection of DDoS Attacks using Machine Learning Algorithms

Parvinder Singh Saini
Research Scholar
Shaheed Bhagat Singh State Technical Campus
Ferozepur, Punjab, INDIA
prvinder.saini@gmail.com

Sunny Behal
Associate Professor
Shaheed Bhagat Singh State Technical Campus
Ferozepur, Punjab, INDIA
sunnybehal@sbsstc.ac.in

Sajal Bhatia
Associate Professor
School of Computer Science & Engg
Sacred Heart University
Connecticut, USA
sajalbhatia@gmail.com

***Abstract*— Distributed Denial of Service attack (DDoS) is the most dangerous attack in the field of network security. DDoS attack halts normal functionality of critical services of various online applications. Systems under DDoS attacks remain busy with false requests (Bots) rather than providing services to legitimate users. These attacks are increasing day by day and have become more and more sophisticated. So, it has become difficult to detect these attacks and secure online services from these attacks. In this paper, we have used machine learning based approach to detect and classify different types of network traffic flows. The proposed approach is validated using a new dataset which is having mixture of various modern types of attacks such as HTTP flood, SID DoS and normal traffic. A machine learning tool called WEKA is used to classify various types of attacks. It has been observed that J48 algorithm produced best results as compared to Random Forest and Naïve Bayes algorithms.**

Keywords—DDoS attack, HTTP-Flood, UDP-Flood, smurf, SIDDoS, WEKA, IDS, HIDS, NIDS.

I. INTRODUCTION

Internet services have become utmost important now days for business organizations and individuals. With the increase in demand of network-based services networks intruders have also increased their attacks on these services to halt the response of services to the legitimate users. The attacks which halts or slows down the services of network applications are known as DDoS attacks. A DDoS attack is achieved by attackers by controlling millions of freely available computer systems on the internet [1]. Thus, causing servers to deny response to legitimate users and keeping busy with the requests generated by the attacks. Prominent websites like banking, social networking sites, universities etc are more targeted by these attacks. Therefore, one or more security tools like antivirus software, firewall and intrusion detection system (IDS) should be used in computer network to protect important data and services from the intruders.

One of the most used solutions to deal with the DDoS attacks is an intrusion detection system (IDS). An IDS preserves integrity, confidentiality and availability of computer network resources and web services. Machine learning techniques are used in IDS system to detect and classify various DDoS attacks and eliminate intrusion. However, it is hard to achieve hundred percent performance accuracy in classifying and detecting attacks.

Currently, there are various type of DDoS attacks are active in networks like Smurf attack, HTTP POST/GET and SQL Injection DoS (SIDDoS). All of them causes denial of service to network services by sending huge volume of useless traffic to web server. Various publically available datasets are obsolete and don't have newer and latest type of attack traffic such as SIDDOS, Smurf and HTTP flood in them. Therefore, there was a need of a dataset which includes various new attacks in it. So, we used dataset [2] created by Mouhammd Alkasassbeh, Ahmad B.A Hassant, Ghazi Al-Naymat and Mohammd Almseidin which includes four type of harmful attacks namely: UDP-flood, SIDDoS, HTTP-flood and Smurf.

Classification of network traffic in done using machine learning techniques. Classification is done on the basis of some features like average packet size, bit rate, packet size, inter arrival time etc. These features are used to decide the class of network traffic i.e. normal or DDoS attack. Mostly DDoS attacks have same average packet size. So, by analyzing dataset machine learning techniques makes decision about the traffic type in the network either as attack traffic or as a normal traffic. We have used WEKA [3] tool as machine learning technique in our research to detect attacks in the network traffic.

II. BACKGROUND AND RELATED WORK

DDoS attacks are very common nowadays. These attacks cause a severe damage to network resources and cause denial of service to legitimate users. In recent time, Behal et al. [4] compared various publicly available datasets and found that all publicly available datasets are obsolete and not appropriate, also all these datasets lacks required features of networks traffic.

Behal et al. [5] 40 research articles and found 45% of researchers have used information entropy-based techniques, around 10% have used information divergence-based techniques and about 38% have used correlation-based techniques. Further he pointed out that majority of the techniques have used the flow similarity concept to determine the DDoS attacks.

978-93-80544-38-0 /20/$31.00 ©2020 IEEE

P Sangkatsanee et al. [6] generated a new real-time instruction detection mechanism applicable to machine learning techniques. He proposed 12 essential network traffic features on the basis of which differentiation between normal, DDoS and probe data is done.

Sofi et al. [7] crested new dataset of 27 features and five various traffic classes. Four machine learning algorithms namely Naïve Bayes, SVM, Decision Tree and MLP were applied by them to identify DDoS attacks. Out of four algorithms MLP gave best results.

Mahadev et al. [8] used Naïve Bayes classifier in weka tool to analyze the networks traffic stream and found out that it gives 99% accuracy in detecting DDoS attacks.

Behal et al. [9] investigated generalized entropy (GE) and generalized information divergence (GID) metrics based on information theory collectively for detecting HR-DDoS attacks, LR-DDoS Attacks and FEs. Both GE and GID metrics are found highly efficient in detecting DDoS Attacks.

Behal et al. [10] used a novel set of information theory based ϕ-Entropy and ϕ-Divergence metrics for detection of DDoS attacks from FEs and found that these metrics are highly efficient than the earlier used GE and GID metrices.

Alkasassbeh et al. [2] created a new dataset that contains new types of attack. They used the attacks type that were not used in previous research. Dataset is having 27 features and 5 classes. They applied three machine learning algorithms Naïve Bayes, random Forest and MLP to classify the attack and found out that MLP classifier achieved highest accuracy.

Kaur et al. [11] used weka tool to detect anomaly in the networks traffic and concluded that an efficient detection algorithm is required to detect the DDoS attack.

S Duque et al. [12] found that k-means clustering showed increase in efficiency with usage of correct number of clusters. Further it was noted that with the increase of number of clusters above the number of data types, false negative rate, the detection rate and efficiency decreases, but the false positive rate increases.

Pan et al. [13] used a hybrid Neural Network technique. They proposed a self-organizing map (SOM) of hybrid Neural Network and functions on the basis of radial to classify and detect DDoS attacks. The technique they proposed achieved very good accuracy rate results for detecting and classifying DDoS attacks.

Norouzian et al. [14] proposed very effective classification technique for detection and classification of network traffic into two classes normal and attack. The new IDS approach proposed by them was a based on Multilayer Perceptron Neural Network for the detection and classification of data into 6 classes. MLP design with two hidden layers of neurons was implemented by them and they achieved accuracy rate 90.78 %.

Berezinski et al. [15] calculated entropy using various methods and found out that Renyi and Tsallis entropy performed best. They found out that Shannon entropy was worst in calculation of false positive rate, accuracy as well as weighted ROC curves. Approach based on volume performed very poor. They also concluded that WEKA gave best results with Simple Logistic classifier.

III. Intrusion Detection System

An intrusion detection system is a system designed for detecting intrusion or anomaly in the system. It classifies networks traffic into various categories based on characteristics of the network traffic and detects anomaly in the traffic. Intrusion detection system can detect as well as remove the anomalies in the network without even consulting the network engineer. An intrusion detection system is of two types *host based* and *network based*.

A. Host intrusion Detection System (HIDS)

Host intrusion detection system is applied on computers or network devices to prevent DDoS attacks on that particular device. This type of IDS provides no support for monitoring of full network.

Fig.1 shows networks architecture of HIDS. In the figure it is clear that IDS is applied on each and every host or node in the network. So, intrusion detection is done at every node rather than for full network. So, a system with HIDS applies IDS protocols on each and every node and not on the whole of the network.

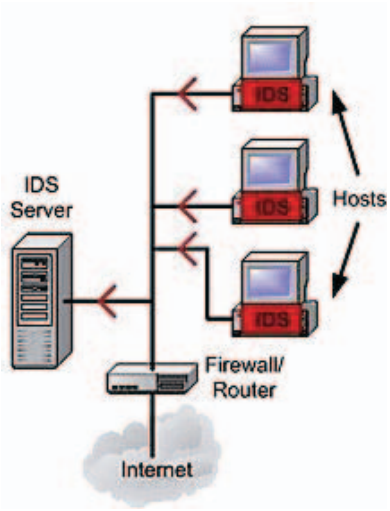

Fig. 1. Host intrusion detection system (HIDS)

B. Network intrusion detection system (NIDS)

Network intrusion detection system (NIDS) is an IDS which covers whole network. When NIDS is used each and every system in that particular network is secured for the DDoS attacks and this system detect anomalies from whole networks not the single device.

Fig.2 shows network architecture of a NIDS system. In a NIDS the intrusion detection mechanisms are attached to the whole of the network rather than on each and every node of the

network. Here from Fig.2 it is clear that an IDS system is attached to the full network and it performs all work related to intrusion detection and removal from the whole of the network. So, in NIDS there is no need to apply IDS mechanism to all the hosts or the nodes of the network and a single standalone IDS mechanism is attached to whole network and it detects and removes attacks from whole network.

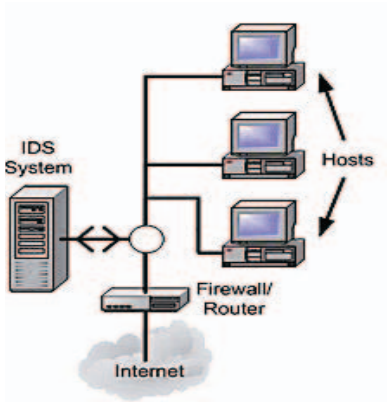

Fig. 2. Network intrusion detection system (NIDS)

IV. CLASSIRIERS USED

A classifier is an algorithm or a technique used to group or classify available data into varies categories depending upon some characteristics. In machine learning, a classifier is used to learn pattern in available data and then the classifier is used to classify data into various groups according to the patterns. In this paper, we have used three classifiers *Naïve Bayes, Random Forest, MLP* and *J48*.

A. Naïve Bayes

Naïve Bayes classifiers are set of classification algorithms based on Bayes' theorem. Naïve Bayes is not a single algorithm but it is a collection of multiple algorithms, which shares a common principal.

B. Random Forest

Random forest is collection of a number of individual decision trees that works together. Class prediction is done by each and every individual tree in the random forest. And the class which gets most number of votes is the prediction of our model.

C. MLP

Multi-layer Perceptron (MLP) classifier relies on underlying Neural Network to perform the task of classification.

D. J48 (C4.5)

J48 (C4.5) is a classification algorithm used to develop decision tree. It was developed by Ross Quinlan. J48 is an extension of Quinlan's earlier ID3 algorithm. Decision trees generated by J48 algorithms can be used for classifications. J48 is also referred as statistical classifier

V. EXPERIMENT AND RESULTS

In our work, we carried out the experiments on Ubuntu 19.04 platform, Intel(R) Core™ 2 Duo CPU T6600 @ 2.20 GHz x 2, 3GB RAM. WEKA (a machine learning tool) version 3.8.3 was used. To test the efficiency of algorithms ten-fold validation was used.

Rest of this section is organized as Dataset used, Evaluation Matrices and Results Discussion.

A. Dataset used

We used dataset collected by Mouhammd Alkasassbeh, Ahmad B.A Hassant, Ghazi Al-Naymat and Mohammd Almseidin, which includes four harmful type of attacks: UDP flood, HTTP flood, Smurf and SIDDoS. Distribution of varies attacks in this dataset are listed in Table:1. The dataset we have used in our experiment has 27 features which are shown in Table:2.

TABLE I. DISTRIBUTION OF ATTACKS

Attack Name	No. of Records
Smurf	361
UDP Flood	5843
SIDDOS	189
HTTP Flood	134

TABLE II. DATASET FEATURES

Variable No	Description	Type
1	SRC ADD	Continuous
2	DES ADD	Continuous
3	PKT ID	Continuous
4	FROM NODE	Continuous
5	TO NODE	Continuous
6	PKT TYPE	Continuous
7	PKT SIZE	Continuous
8	FLAGS	Symbolic
9	FID	Continuous
10	SEQ NUMBER	Continuous
11	NUMBER OF PKT	Continuous
12	NUMBER OF BYTE	Continuous
13	NODE NAME FROM	Symbolic
14	NODE NAME TO	Symbolic
15	PKT IN	Continuous
16	PKT OUT	Continuous
17	PKTR	Continuous
18	PKT DELAY NODE	Continuous
19	PKTRATE	Continuous
20	BYTE RATE	Continuous
21	PKT AVG SIZE	Continuous
22	UTILIZASION	Continuous
23	PKT DELAY	Continuous
24	PKT SEND TIME	Continuous
25	PKT RESERVED TIME	Continuous
26	FIRST PKT SENT	Continuous
27	LAST PKT RESERVED	Continuous

B. Evaluation Matrices

The evaluation of performance of these kinds of systems is usually done by using the information provided by this matrix shown in Table 3 [16].

TABLE III. CONFUSION MATRIX

		Predicted	
		Positive	Negative
True	Positive	TP	FN
	Negative	FP	TN

Accuracy – Rate of instances correctly classified by a classifier.

$$Accuracy = \frac{TP+TN}{TP+FN+FP+TN} \quad (1)$$

Precision – Total predicted true instances of DDoS attacks divided by the total number of predicted true and false DDoS attacks.

$$Precision = \frac{TP}{TP+FP} \quad (2)$$

Recall – Total predicted number of DDoS attacks divided by the total number of actual DDoS attacks.

$$Recall = \frac{TP}{TP+FN} \quad (3)$$

C. Result Discussion

For the detection of various attacks from the datasets we used WEKA and applied various classifiers. For the evaluation of results both the explorer and knowledge flow environment of WEKA was used. Fig.3, Fig.4, Fig.5, Fig.6 and Fig.7 depicts results generated from WEKA showing class Normal, Smurf, UDP Flood, HTTP Flood and SIDDOS

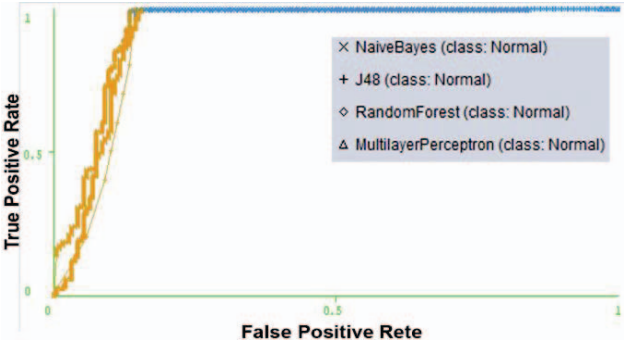

Fig. 3. Threshold curve of normal class using all four classifiers

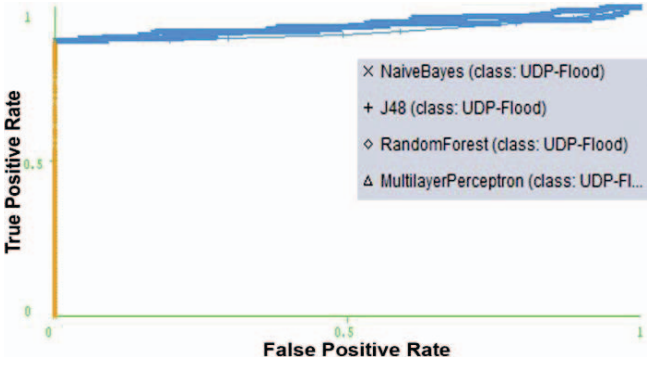

Fig. 4. Fhreshold curve of UDP-Flood class using all four classifiers

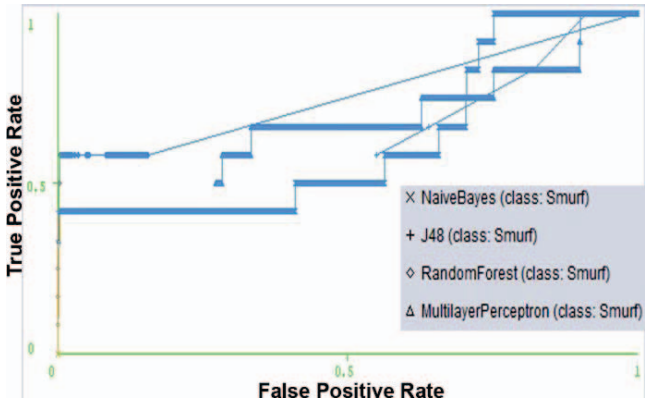

Fig. 5. hreshold curve of Smurf class using all four classifiers

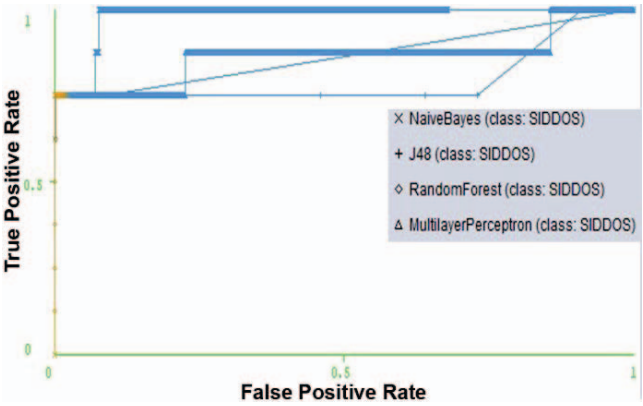

Fig. 6. Threshold curve of SIDDOS Class using all four classifiers

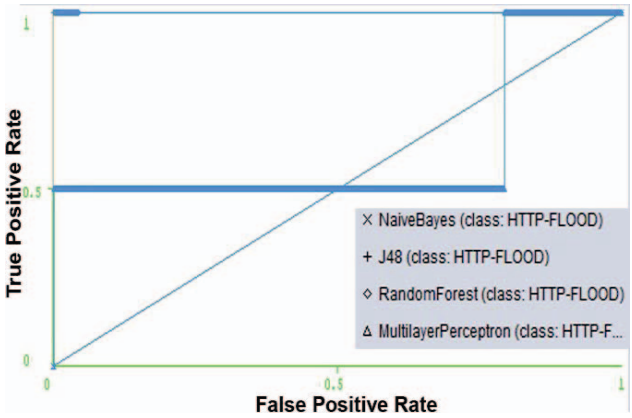

Fig. 7. hreshold curve of HTTP-Flood class using all four classifiers

Further, for evaluating performance of the classifiers used we used confusion matrix based on evaluation matrices discussed in section 5.2. The final confusion matrices of J48, MLP, Random Forest and Naïve Bayes are showed in Table 4, Table 5, Table 6 and Table 7 respectively. From the confusion matrices the precision, accuracy and recall for all four classifiers was calculated. The accuracy for J48, MLP, Random

Forest and Naïve Bayes was calculated as 98.64%, 98.63% 98.10% and 96.93% respectively

TABLE IV. CONFUSION MATRIX OF J48 CLASSIFIER.

	Normal	UDP-Flood	Smurf	SIDDOS	HTTP-Flood
Normal	56393	0	2	7	2
UDP-Flood	576	5267	0	0	0
Smurf	228	0	121	10	2
SIDDOS	13	0	0	176	0
HTTP-Flood	2	0	2	11	119

TABLE V. CONFUSION MATRIX OF MLP CLASSIFIER.

	Normal	UDP-Flood	Smurf	SIDDOS	HTTP-Flood
Normal	56392	2	1	7	2
UDP-Flood	576	5267	0	0	0
Smurf	228	0	121	10	2
SIDDOS	13	0	0	176	0
HTTP-Flood	4	0	1	11	118

TABLE VI. CONFUSION MATRIX OF RANDOM FOREST CLASSIFIER.

	Normal	UDP-Flood	Smurf	SIDDOS	HTTP-Flood
Normal	56071	219	102	10	2
UDP-Flood	569	5272	2	0	0
Smurf	226	2	121	9	3
SIDDOS	19	0	7	153	10
HTTP-Flood	1	0	1	10	122

TABLE VII. CONFUSION MATRIX OF NAÏVE BAYES CLASSIFIER.

	Normal	UDP-Flood	Smurf	SIDDOS	HTTP-Flood
Normal	55426	0	933	41	4
UDP-Flood	572	5267	4	0	0
Smurf	219	0	9	10	123
SIDDOS	13	0	0	175	1
HTTP-Flood	0	0	0	11	123

However, calculating only accuracy is not enough for evaluation of performance of a classifier. So, calculation of precision and recall was also dene. It was required as the data was imbalanced. Number of normal class instances were much higher as compared to the number of other class instances. Therefore, for each class (Normal, HTTP-flood, SIDDOS, UDP-flood and Smurf) we calculated recall and precision.

Fig.8 and Fig.9 depicts comparison of predicted precision values and recall values of all classes for each classifier used. From the figures it is clear that each classifier predicted normal class with high values of recall rate and precision rate. However, for the rest of four classes the performance of each and every classifier varies.

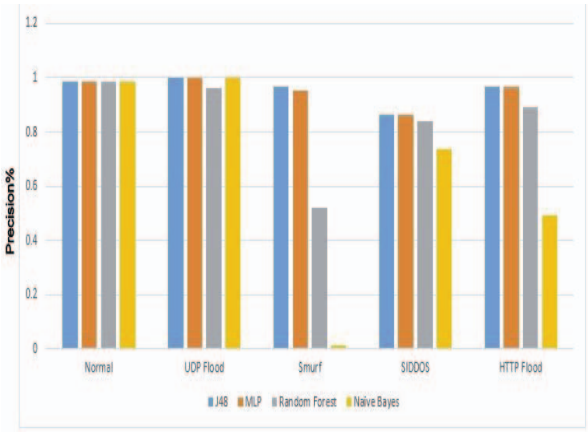

Fig. 8. Precision Results

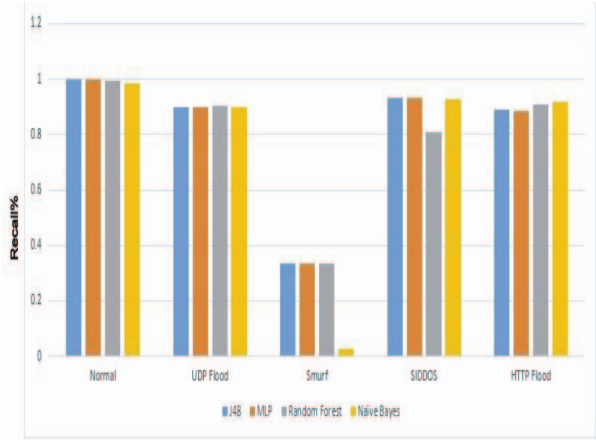

Fig. 9. Recall Results

From the Fig.8 and Fig.9 it is clear that J48 outperformed in all four classifiers for calculating various classes and Naïve Bayes gave out the worst results

So, the proposed classifier as compared with the previous research MLP classifier outperformed in all aspects. J48 gave higher accuracy as compared to MLP. Also outperformed in precision and recall values as shown in Fig.8 and Fig.9. Moreover, J48 shown less time complexity as compared to MLP classifier.

VI. CONCLUSION AND FUTURE WORK

Distributed denial of service (DDoS) attacks are severe threat to network security. They cause halt of services of online applications and network services and resources. During DDoS attack legitimate users kept waiting for the services while system remains busy resolving the false requests of bots. In this paper we used machine learning tool WEKA for detecting and defining DDoS attacks. We used a dataset of 27 features and 5 different classes. Four different classifiers J48, MLP, Random Forest and Naïve Bayes were used to classify the attacks from the dataset. From the investigation of results provided by three classifiers it was noted that the J48 classifier outperformed the rest two classifiers. J48 gave 98.64% accuracy while the rest

three algorithms MLP, Random Forest and Naïve Bayes gave 98.63%, 98.10% and 96.93% accuracy respectively.

The future work is to create a dataset with more modern types of attacks, as this dataset includes only four type of attacks.

REFERENCES

[1] DDoS Attack Report, Computer Emergency Response Team. http://www.cert.org, 2015

[2] M Alkasassbeh, Ahmad B.A Hassant, G Al-Naymat and M Almseidin, Detecting Distributed Denial of Service Attacks Using Data Mining Techniques, International Journal of Advanced Computer Science and Applications, Vol.7, No. 1,2016.

[3] Weka 3.8.3 tools [online]. <https://www.cs.waikato.ac.nz/ml/weka/>

[4] S Behal and K Kumar , Trends in Validation of DDoS Research, Procedia Computer Science 85 (2016) 7-15.

[5] S Behal, K Kumar and M Sachdeva, Characterizing DDoS attacks and flash events: Review, research gaps and future directions, ELSEVIER Computer Science Review 25 (2017) 101-114.

[6] P Sangkatsanee, N Wattanapongsakorn and C Charnsripinyo, Practical real-time intrusion detection using machine learning approaches, ELSEVIER Computer Communications 34(2011) 2227-2235.

[7] I Sofi, A Mahajan and V Mansotra, Machine Learning Techniques used for the Detection and Analysis of Modern Types of DDoS Attacks, International Research Journal of Engineering and Technology (IRJET), Volume:04 Issue:06 June-2007

[8] Mahadev, V Kumar and H Sharma, Detection And Analysis of DDoS Attack At Application Layer Using Naïve Bayes Classifier, International Journal of Computer Engineering & Technology (IJCET), Volume 9, Issue 3, May-June 2018, pp. 208-217,Article IJCET_09_03_025.

[9] S Behal and K Kumar, Detection of DDoS attacks and flash events using information theory metrics-An empirical investigation, ELSEVIER Computer Communications 103(2017) 18-28.

[10] S Behal and K Kumar, Detection of DDoS attacks and flash events using novel information theory metrics, ELSEVIER Computer Networks 116 (2017) 96-110.

[11] S Kaur, S Behal and G Kumar, Detection of DDoS Attacks using Weka Tool: A Case Study, National Conference on Computing, Communication & Electrical Systems (IJCSN), December 2017 – Proceedings.

[12] S Duque, M Nizam bin Omar, Using Data Mining Algorithms for developing a Model for Intrusion Detection System (IDS), ELSEVIER Procedia Computer Science 61 (2015) 46-51.

[13] W pan and W Li, A hybrid neural network approach to the classification of novel attacks for intrusion detection, Parallel and Distributed Processing and Applications, pp 564-575, Springer, 2005.

[14] M R Norouzian and S Merati, Classifying attacks in a network intrusion detection system based on artificial neural networks, Advanced Communication Technology (ICACT), 2011 13th International Conference on, pp 868-873, IEEE, 2011.

[15] P Berezinski, B Jasiul and M Szpyrka, An Entropy-Based Network Anomaly Detection Method, Open Access Entropy 2015, 17,2367-2408; doi:10.3390/e17042367.

[16] V. M. Patro and M. R. Patra, "Augmenting weighted average with confusion matrix to enhance classification accuracy", Transactions on Machine Learning and Artificial Intelligence, Vol 2, no. 4, pp 77-91, 2014.