Ranking of Machine learning Algorithms Based on the Performance in Classifying DDoS Attacks

Rejimol Robinson R R
Dept. Electronics and Communication Engineering
College of Engineering, Trivadrum

Ciza Thomas
Dept. Electronics and Communication Engineering
College of Engineering, Trivadrum

***Abstract*— Network Security has become one of the most important factors to consider as the Internet evolves. The most important attack which affects the availability of service is Distributed Denial of Service. The service disruption may cause substantial financial loss as well as damage to the concerned network system. The traffic patterns exhibited by the DDoS affected traffic can be effectively captured by machine learning algorithms. This paper gives an evaluation and ranking of some of the supervised machine learning algorithms with the aim of reducing type I and type II errors, increasing precision and recall while maintaining detection accuracy. The performance evaluation is done using Multi Criteria Decision Aid software called Visual PROMETHEE. This work demonstrates the effectiveness of ensemble based classifiers especially the ensemble algorithm of Adaboost with Random Forest as the base classifier. Publicly available datasets such as DARPA scenario specific dataset, CAIDA DDoS Attack 2007 and CAIDA Conficker are used to evaluate the algorithms.**

Keywords—DDoS; MCDA; Visual PROMETHEE; IDS;

I. INTRODUCTION

The world of Internet is under the shadow of cyber warfare and the catastrophe it brings is a single click away. The golden principle of security namely Confidentiality, Integrity and Availability cannot be maintained since the influence of Internet is remarkably high in industrial, political as well as in defense fields. Machine to machine communication via Internet is not at all secure because of the increasing number of vulnerabilities exploited in each layer of the TCP/IP protocol suite. Establishing new security policies, updating the signature database of Intrusion Detection Systems(IDS) with latest attack signatures, analyzing and being aware of new security flaws and threats are some of the steps that one can take to mitigate the severe impact of network attacks.

Companies, operating critical online business including those that providing electronic banking and e-commerce services depend on their services to be always up for business success. But the massive destruction capability, annoyance and the financial impacts of Distributed Denial of Service attack (DDoS) has made it a major challenge to the network security. Most of the Corporate and other industries depend access control list, intrusion detection systems, intrusion prevention systems and other available security measures among which intrusion detection system is a primary tool. Anomaly based and signature or misuse based IDSs are the two broad categories of IDSs. Anomaly based detection technique models the behavior of normal traffic to distinguish attack traffic from normal while the signature based detection uses pattern matching to compare the data instances with the signatures already stored in the database. Most of the well-known IDSs such as Snort, Bro etc. are signature based detection systems with high false alarm rate as the main challenge.

DDoS detection systems necessitates processing of large amounts of network traffic data and the detection systems must be capable of searching this traffic data for harmful packets or packet flows. Machine learning based classifiers are experts in finding out patterns in the dataset with the help of features used to describe the data. Machine learning techniques can provide decision aids for the analysts and can automatically generate rules to be used for network intrusion detection system.

Reducing false alarm rate and maintaining detection accuracy are very crucial criteria in the performance of machine learning algorithms. The primary objective of this paper is to evaluate and rank a few commonly used machine learning algorithms with the aim of giving preference to reduce the type I and type II errors of classification algorithms. This work gives more importance to precision and recall of the algorithms as they are the crucial factors for better performance in classifying skewed dataset. There is a tradeoff existing among the precision and recall, so the algorithms are analyzed and ranked using Multicriteria Decision Aid (MCDA) software called Visual PROMETHEE. The algorithms considered mainly falls in the category of individual, hybrid and ensemble classifiers. Publicly available datasets such as DARPA scenario specific dataset, CAIDA DDoS Attack 2007 and CAIDA Conficker are used to evaluate the algorithms.

The organization of the remaining part of the paper is as follows. Section II discusses the background of machine learning algorithm in detecting DDoS attacks and the datasets used for evaluation. Section III presents the experimental setup and section IV presents the ranking of algorithms. The conclusion and future work are given in section V.

978-1-4673-6670-0/15/$31.00 ©2015 IEEE

II. BACKGROUND

A. Machine learning algorithms in detecting DDoS attacks

Classifiers are tools that classify data based on specified features or patterns present in that data. Some of the worth noticing works in the field of DDoS detection includes the work of Gil and Poletto, in which they assume that packet rates between two hosts are proportional during normal operation [1]. This work make use of a dynamic tree structure known as Multi Level Tree for Online Packet Statistics (MULTOPS) structure for monitoring packet rates for each IP address. Wang et al. proposed a method solely for detecting SYN flood by monitoring statistical changes in the ratio of SYN packets to FIN and RST packets [2]. Kulkarni et al. trace the source IP addresses and construct Kolmogorov Complexity Metrics for identifying their randomness. In fact the randomness of source IP addresses is very low without any DDoS attack; otherwise, it is very high under DDoS attacks with randomly distributed source IP addresses [3]. Mirkovic and Reiher put forward the method known as D-WARD, which behaves as a firewall in which it monitors the statistical changes of parameters of incoming and outgoing traffic models [4]. Attackers can carefully mix different types of traffic to ensure the proportion of each trace is same as it is in normal. Hence, this scenario will affect the initial assumption made in building the models in the above said algorithms.

The research works in the field of machine learning algorithms suggests wide variety of supervised machine learning algorithms can be used for their efficient characterization of evolving attack vectors which in turn helps the detection of DDoS [5],[6]. Bouzida et al., in their work, extend the definition of anomaly detection to consider known attacks and normal profiles to explore supervised machine learning techniques. They explore the effectiveness of neural networks and decision trees for intrusion detection [5]. Decision tree induction algorithm has proven its efficiency in predicting the different classes of the unlabeled data in the test data set for the KDD 99 intrusion detection contest. Experimental results demonstrate that while neural networks are highly successful in detecting known attacks, Decision trees are more capable of detecting new attacks [5]. Li et al. demonstrate a DDoS detection system that use LVQ neural network for host anomaly detection and through this method they could improve the recognition rate of detection system [7]. Gumus et al. present an adaptive implementation of Naive Bayes algorithm with exponential weights for moving average and standard deviation [8]. They also compare adaptations of several machine learning algorithms on KDD'99 intrusion detection dataset.

Researchers have also used ensemble classifiers since single classifiers makes error on different training samples. So the total error in classification can be reduced by creating an ensemble of classifiers and combining their outputs. The ensemble of neural classifiers is used to detect flooding attacks based on the performance regarding the detection accuracy on KDD cup dataset [9]. The work of Arun Raj Kumar and Selvakumar focuses on the identification of high rate flooding attack with high detection accuracy and fewer false alarms using adaptive and hybrid neuro-fuzzy systems with Adaptive Neuro-Fuzzy Systems (ANFIS) as a base classifier [10]. It is also worth noticing the improved performance of hybrid GA and ANN over GA and SVM [11], [12] and fusion IDS [13], [14] over individual IDSs.

The comparative study of machine learning algorithms in relation to network intrusion detection done in [15] gives a detailed study of machine learning algorithms and its evaluation using Weka. This study highlights Random Forest and BayesNet as the suitable candidates for intrusion detection based on NSL-KDD dataset.

B. Datasets and features

One of the main hurdles while doing research in DDoS detection system is the lack of proper dataset because of the difficulty to create a real world scenario including all possible attacks and normal traffic. The well-known datasets available today are DARPA/Lincoln labs packet traces, the KDD Cup dataset derived from DARPA traces and Cooperative Association for Internet Data Analysis (CAIDA) dataset 2007 etc.

The DARPA/MIT Lincoln evaluation (IDEVAL) dataset has been used as a bench marking dataset in various research works as well as in many intrusion detection systems [16]. The data is useful for testing both host based and network based systems as well as both signature and anomaly based systems [17]. McHugh criticizes the DARPA dataset about collected traffic data, attack taxonomy and evaluation criteria [19]. Mahoney and Chan studied the DARPA dataset well and point out some irregularities in the attributes [20]. They discovered that many attributes that have small fixed range in simulation while they have large and growing range in real traffic, particularly in attributes like remote client addresses, TTL, TCP options and TCP window size. But the work of Thomas and Balakrishnan, evaluated the DARPA dataset in two signature based IDSs and two anomaly based IDSs and justifies the usefulness of DARPA dataset for IDS evaluation [18]. They list out some details for the poor performance of the dataset which states that the training and testing datasets are not correlated for R2L and U2R attacks and hence most of the pattern recognition and machine learning algorithms except for the anomaly detectors that learn from the normal data will perform very badly in detecting U2R and R2L attacks. The real world network traffic is mostly normal with relatively small fraction of attack traffic. This attack traffic itself contains rarer attacks namely R2L and U2R. This literature discusses the two problems faced by Intrusion detection system due to the inherent skewness in network traffic. The base rate fallacy and the accuracy paradox apart from the lack of representative data set are the main drawbacks of these kind of security systems [17].

The CAIDA dataset contains approximately one hour of anonymized traffic traces from a DDoS attack on August 4, 2007 (20:50:08 UTC to 21:56:16 UTC). This type of denial-of-service attack attempts to block access to the targeted server by consuming computing resources on the server and

by consuming all of the bandwidth of network connecting the server to the Internet [21]. Bhattia et al. used this dataset to distinguish DDoS attack from flash crowds [22]. The ensemble algorithms analyzed in [23] divide this dataset into three separate sets of SYN flood, UDP flood and HTTP flood each having their own attributes for attack detection.

The Conficker dataset contains data from the UCSD Network Telescope for three days between November 2008 and January 2009 [24]. The packets seen by the network telescope result from a wide range of events include misconfiguration, scanning of address space by attackers, malware looking for vulnerable targets, backscatter from randomly spoofed source DoS attacks and the automated spread of malware.

The DARPA 2000 Intrusion Detection Scenario-Specific datasets, LLS-DDOS 1.0-Scenario One is specifically for DDoS. This is the first attack scenario example data set to be created for DARPA. It includes a distributed denial of service attack run by a novice attacker. This attack scenario is carried out over multiple network and audit sessions. These sessions have been grouped into 5 attack phases over the course of which the adversary probes, breaks-in, installs Trojan mstream DDoS software, and launches a DDoS attack against an off-site server [25].

III. Experimental Setup

In this work, we intended to rank ten different supervised machine learning algorithms based on the metrics to evaluate their performance in classification. False positive rate, False negative rate, Precision, Recall and Detection accuracy are the metrics taken and there exists a tradeoff among these metrics. The organization of experimental setup is shown in Fig.1. The experiment is divided into the following phases.

a) Packet header parsing of network traces.
b) Feature extraction.
c) Normalization.
d) Classification and evaluation of metrics
e) Ranking of algorithms

The input to the feature extraction module is the parsed packet header information of traffic traces. We have selected LLS-DDOS 1.0-Scenario One dataset from 2000 DARPA Intrusion Detection Scenario-Specific datasets, CAIDA 2007 traces and CAIDA Conficker as attack traces. The normal traffic is selected from DARPA. Three independent training and test datasets are formed from these attack traces mixed with the normal traffic. The data in its raw form need to be pre-processed to make it ready to use for Weka, a popular suite of machine learning software which supports several standard data mining tasks [26].

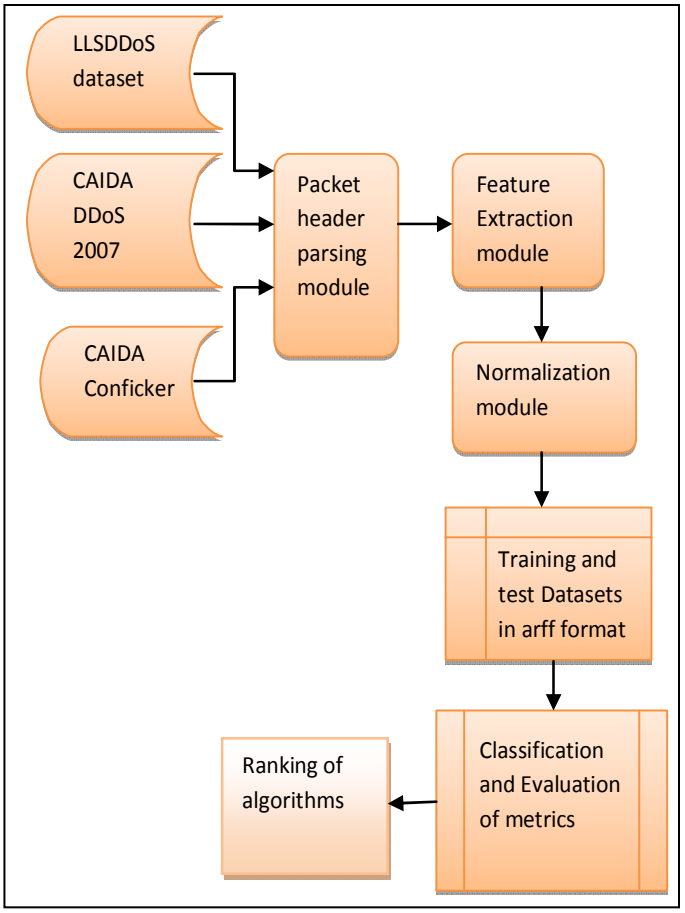

Fig. 1. Organization of work elements for the evaluation of machine learning algorithms in the detection of DDoS

The packets are analysed using Wireshark and the selected header fields are exported to a file in CSV (Comma Separated Values) format. The header parsing module implemented in Python extracts the fields present in the packet header and converts the stream of packets into flows. A traffic flow is defined as a sequence of packets sent from a particular source to a particular unicast, anycast, multicast destination that the source desires to label as a flow, according to RFC 3697. This is followed by feature extraction module and normalization module. Feature extraction module does the process of extracting the seven features present in the traffic flows. The output of this module is a set of feature vectors of dimensionality seven, such that $X=(x_0,x_1,x_2,x_3,x_4,x_5,x_6)$, where x_i is the i^{th} feature extracted from traffic flow.

The work of Karimazad and Faraahi discussed the seven features which contain sufficient information related to the presence of a DDoS attack [27]. These features are very prominent and clear so it is comparatively easy to distinguish flooding attacks from normal traffic. The features considered in their work are Average Packet Size, Number of Packets, and Time Interval Variance, Packet size Variance, Number of Bytes, Packet Rate and Bitrate. The traffic traces considered in our work mainly contains flooding attack and hence these features are selected to model the traffic. Normalization or scaling of data is necessary to make the data values fall between same ranges. This step is used to make sure that the

machine learning algorithms that we are going to evaluate is not biased to some features present in the data. So the values are scaled between [0,1] using minmax normalization according to (1).

$$x_i = \frac{(x_i - x_{\max})}{(x_{\max} - x_{\min})} \quad (1)$$

where x_i is the i^{th} feature value, x_{max} is the maximum value of i^{th} feature in the dataset and x_{min} is the minimum value of i^{th} feature in the dataset. This normalized data is properly labeled and shuffled to distribute the instances evenly across the sample space. This dataset is converted to arff format to provide it as an input to the Weka 3.6 software for further processing. The results obtained are the classification output and the performance metrics of ten different machine learning algorithms.

The metrics selected for ranking are Flase positive (FP), False negative (FN), Precision (P), Recall (R) and Detection-accuracy. The classification is done with respect to attack class. So the True Positive (TP) is the number of attacks that are correctly classified as attack, True negative (TN) is the number of normal traffic correctly classified as normal, False negative (FN) is the number of attacks incorrectly classified as normal and False positive (FP) is the number of normal traffic incorrectly classified as attack.The Precision is the measure of what fraction of test data that are classified as attacks are actually from attack class (2)and Recall is the measure of what fraction of attacks are correctly classified as attack (3).

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

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

Detection accuracy can be calculated using (4)

$$Detection - accuracy = \frac{TP + TN}{TP + FP + TN + FN} \quad (4)$$

We would like to analyze algorithms by the minimization of Type I error (FN) and type II (FP) errors and maximization of Precision and Recall. These parameters are given to the MCDA software called Visual PROMETHEE which evaluates the actions based on given criteria [28]. In mathematical terms the problem can be defined as following:

$$\max\{f_1(a), f_2(a) \mid a \in A\} \wedge \min\{f_3(a), f_4(a) \mid a \in A\} \quad (5)$$

where A is the finite set of ten algorithms called actions in Visual PROMETHEE and the criteria are Precision, Recall FN, and FP, which are represented as f_1, f_2, f_3, f_4 respectively.

The decision maker wants to identify an action that is the best on all the criteria at the same time. We have ten actions and four criteria and the criteria are more or less conflicting with each other. The objective of the MCDA is to identify the best compromise decisions. Inorder to achieve this objective, it is necessary to have some information about the preference and the priorities of the decision maker. In Visuasl PROMETHEE non negative weights which represent the relative importance of the criteria can be defined. PROMETHEE ranking is based on preference flows, which are computed to consolidate the results of the pair wise comparisons of actions and rank all the actions from the best to the worst one. Three different preference flows are computed and is given in (6), (7) and (8).

- *Phi +(Φ^+):the positive or leaving flow*
- *Phi-(Φ^-) :the negative or entering flow*
- *Phi(Φ) :the net flow*

The positive preference flow (Φ^+) measures how much an algorithm *a* is preferred to the other *n-1* ones. It is the global measurement of the strengths of an algorithm *a*. The negative preference flow Φ^- measures how much the other *n-1* algorithms are preferred to *a*. The net preference flow is the balance between the positive and negative preference flows [26].

$$\Phi^+(a) = \frac{1}{n-1}\sum_{b \neq a} \Pi(a,b) \quad (6)$$

$$\Phi^-(a) = \frac{1}{n-1}\sum_{b \neq a} \Pi(b,a) \quad (7)$$

$$\Phi(a) = \Phi^+(a) - \Phi^-(a) \quad (8)$$

$$\Pi(a,b) = \sum_{j=1}^{k} w_j * P_j(a,b) \quad (9)$$

The function $\Pi(a,b)$ given in (9) is the multicriteria preference index and $w_j > 0$ is the normalized weight allocated to criterion f_j. $P_j(a,b)$ is the value of the preference function for criterion f_j when action *a* is compared to action *b*.

PROMETTHEE II complete ranking is used because all the algorithms are compared and the ranking include no incomparabilities even when comparison is difficult. It is based on net preference flow. The algorithm *a* is preferred to algorithm *b* in this ranking if and only if it is preferred to algorithm *b* according to the net preference flow. That is:

$$a\ P^{\Pi}\ b \quad \text{if anf only if } \Phi(a) > \Phi(b) \quad (10)$$

where $a\ P^{\Pi}\ b$ is the relation "*a* is preferred to *b*"

IV. RANKING OF ALGORITHMS

Table I shows the detection accuracy and the Table II shows the performance metrics selected as criteria for ranking. This table is given as input to Visual PROMETHEE. In PROMETHEE II complete ranking method, the net effect of two preference flows are taken and it combines the positive and negative preference flows in one single score. PROMETHEE II ranking windows are shown in Fig. 2, 3, 4

where the green color portion of vertical axis shows the positive preference flows and the red color shows the negative preference flows.

TABLE I. DETECTION ACCURACY OF MACHINE LEARNING ALGORITHMS ON THREE DIFFERENT DATASETS

Algorithm	LLS-DDOS1.0	CAIDA 2007	CAIDA Conficker
	Accuracy (%)	*Accuracy (%)*	*Accuracy (%)*
Naïve Bayes	76.05	50.1	94.51
RBF network	80.68	79.83	96.03
Multi Layer Perceptron	83.2	94.43	99.36
Bayesnet	91.13	96.42	99.75
IBK	95.76	98.21	99.92
J48	96.69	99.26	99.96
Voting	97.35	98.84	99.96
Bagging+Random Forest	98.14	99.26	99.96
Random Forest	97.75	99.26	100
Adaboost+Random Forest	99.47	99.89	99.96

In all the three scenarios, Adaboost with Random forest as the base classifier ranks first and Naïve Bayes towards bottom of the red color portion shows its negative preference. Among the single classifier category Random Forest is much better than the near competitors like IBK, BayesNet, and J48 as shown in Fig.2, 3, 4.

Rule based learning algorithms exhibit slightly inferior performance in the case of CAIDA conficker dataset. The performance degradation is mainly due to the less variance of data compared to the other two datasets. The CAIDA confiicker dataset contains DDoS attack generated using a larger botnet where the flooding attack-vectors are clearly distinguishable with a larger bias. The Naïve Bayes jumps to higher position and Bayes net jumps much towards lower position in the red region only because of the lower variance and larger bias of this dataset. Hence in this dataset, all the algorithms give detection accuracy above 99% as given in Table I**.**

V. CONCLUSION

The main objective of this work is to evaluate the performance of Machine learning algorithms in detecting DDoS attack and rank them according to the preferences given by the decision maker. As we are using skewed dataset which contains more normal traffic and less number of DDoS attack, Type I and Type II errors are crucial in evaluating the algorithms. Moreover the importance is also given to maximize precision and recall of classification algorithms. Ranking of algorithms using these conflicting criteria is given to Visual PROMETHEE, MCDA software. The PROMETHEE II ranking highlights Adaboost with Random forest base classifier as the first choice compared with other single, hybrid and ensemble machine learning algorithms. As a future work it is proposed to classify DDoS flooding attacks using machine learning algorithms which are optimized to decrease the misclassification cost incurred due to Type I and Type II errors.

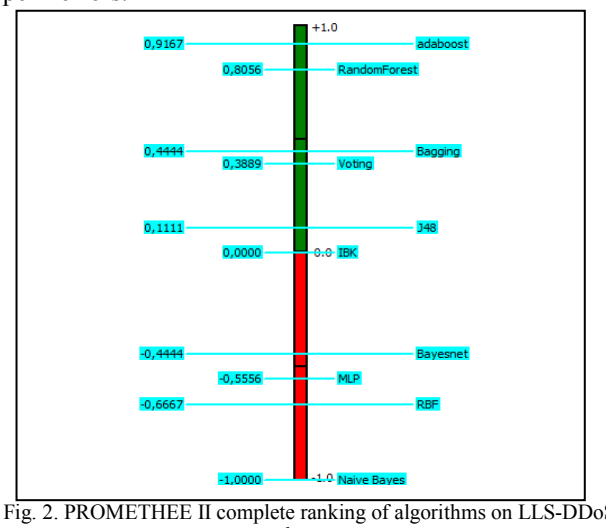

Fig. 2. PROMETHEE II complete ranking of algorithms on LLS-DDoS dataset

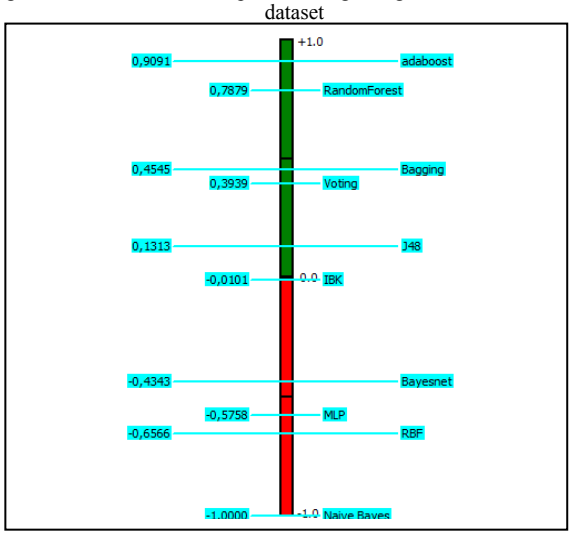

Fig. 3. PROMETHEE II complete ranking of algorithms on CAIDA dataset

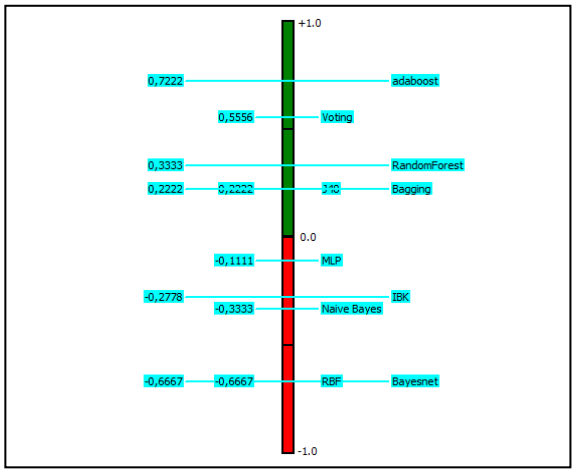

Fig. 4. PROMETHEE II complete ranking of algorithms on CONFICKER dataset

TABLE II. EVALUATION METRICS FOR ALGORITHMS

Algorithm	LLS-DDOS1.0				CAIDA 2007				CAIDA Conficker			
	FN rate	*FP rate*	*Precision*	*Recall*	*FN rate*	*FP rate*	*Precision*	*Recall*	*FN rate*	*FP rate*	*Precision*	*Recall*
Naïve Bayes	0.577	0.57	0.8	0.423	0.068	0.534	0.27	0.932	0.023	0.144	0.583	0.977
RBF network	0.423	0.069	0.818	0.577	0.773	0.002	0.952	0.227	0.093	0.062	0.75	0.907
Multi Layer Perceptron	0.434	0.024	0.926	0.566	0.284	0	1	0.716	0	0.22	0.905	1
Bayesnet	0.136	0.063	0.881	0.864	0.136	0.019	0.905	0.864	0.023	0	1	0.977
IBK	0.087	0.018	0.964	0.913	0.102	0.005	0.975	0.898	0.012	0	1	0.988
J48	0.057	0.02	0.962	0.943	0.045	0.01	0.955	0.955	0	0	1	1
Voting	0.064	0.006	0.988	0.936	0.057	0	1	0.943	0	0	1	1
Bagging+Random Forest	0.015	0.012	0.978	0.985	0.091	0	1	0.909	0	0	1	1
Random Forest	0.011	0.006	0.989	0.989	0.08	0	1	0.92	0	0	1	1
Adaboost+Random Forest	0.008	0.006	0.989	0.992	0.045	0	1	0.955	0	0	1	1

REFERENCES

[1] T. M. Gil, M. Poletto, "MULTOPS: A datastructure for bandwidth attack detection". In USENIX, editor, Proceedings of the 10th USENIX Security Symposium, August1317, Washington, vc DC, USA, 2001.

[2] H. Wang, D. Zhang and K. G. Shin, "Detecting Syn Flooding attacks".In Proceedings of IEEE INFOCOMM,2002, 1530-1539.

[3] A. Kulkarni, S.Bush, and S. Evans, "Detecting Distributed Denial of Service Attack using Kolmogorov complexity metrics", Tech. Rep 2001 crd176 GE research and Development Centre Schectades , NY.

[4] J. Mirkovic, P Reiher," D-WARD,a source end defence against flooding denial of service attacks", IEEE transaction on Dependable Secure Computing, vol. 2(3), pp. 216-232, 2005.

[5] Y. Bouzida and F. Cuppens."Neural networks vs. decision trees for intrusion detection". IEEE / IST Workshop on Monitoring, Attack Detection and Mitigation (MonAM2006) Tuebingen, Germany, September, 2006.

[6] M. Sammany, M. Sharawi, M. El-Beltagy,.and I. Saroit, "Artificial neural networks architecture for intrusion detection systems and classification of attacks", Publication in the 5th international conference INFO2007, Cairo University, 2007.

[7] J. Li Yong, L. Lin Gu, "DDoS Attack Detection Based On Neural Network", Aware Computing (ISAC), 2010 2nd International Symposium 196 – 199, IEEE 2010.

[8] F. Gumus, C. OkanSakar, Z. Erdem, O. Kursun, "Online Naive Bayes classification for Network Intrusion Detection", 2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), 2014.

[9] P. Arun Raj Kumar, S.Selvakumar, "Detection of distributed denial of service attack detection using an ensemble of neural classifier", Computer Communication 34, Elsevier, pp. 1328-1341, 2011.

[10] P.Arun Raj Kumar, S.Selvakumar, "Detection of distributed denial of service attacks using an ensemble of adaptive and hybrid neuro-fuzzy systems", Elsevier, Computer Communications 36(2013), pp. 303-319, 2012.

[11] A. Dastanpour, S. Ibrahim, R. Mashinchi, A. Selamat, "Comparison of genetic algorithm optimization on artificial neural network and support vector machine in intrusion detection system", IEEE conference on Open Systems(ICOS), pp. 72-77, 2014.

[12] M. Barati, A. Abdullah, N I Udzir, R. Mahmod, N. Mustapha, " Distributed Denial of Service Detection using hybrid machine learning techniques", International Symposium on Biometrics and Security Technologies, pp. 268-273, IEEE, 2014.

[13] C. Thomas, N. Balakrishnan, Improvement in intrusion detection with advances in sensor fusion, Information Forensics and Security, IEEE Transactions on, vol. 4, no. 3, pp. 542-551, 2009.

[14] C. Thomas, Improving intrusion detection for imbalanced network traffic, John Wiley Security and Communication Networks, vol. 6 (3), pp. 309-324, 2013.

[15] S. Choudhury and A. Bhowal, "Comparative analysis of machine learning algorithms along with classifiers for network intrusion detection, International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials(ICSTM), pp. 89-95, IEEE 2015.

[16] http://www.ll.mit.edu/ideval/data/

[17] C. Thomas and N. Balakrishnan, "Improvement in minority attack detection with skewness in network traffic", Proceedings of SPIE, vol. 6973, pp. 69730N-12, 2008.

[18] C. Thomas, V. Sharma, N. Balakrishnan, "Usefulness of DARPA dataset for Intrusion Detection System evaluation", Proceedings of SPIE, vol. 6973, pp. 69730G-8, 2008.

[19] J. McHugh, "Testing Intrusion Detection Systems: A critique of the 1998 and 1999 DARPA IDS evaluations", as performed by Lincoln Laboratory, ACM Transactions on Information and System Security, vol.3, No.4, Nov. 2000.

[20] M. V. Mahoney, P. K. Chan, "An analysis of the 1999 DARPA /Lincoln Laboratory evaluation data for network anomaly detection", Technical Report CS-2003-02.

[21] http://www.caida.org/data/passive/ddos-20070804_dataset.xml (about attack 2007)

[22] S. Bhatia, G. Mohay, A. Tickle, E. Ahmed, "Parametric differences between a real-world Distributed Denial-of-Service attack and a Flash Event" Sixth International Conference on Avilabilty, Reliability and Security, IEEE, 2011.

[23] P. Arun Raj Kumar and S. Selvakumar, " M2KMIX: Identifying the type of high rate flooding attacks using a mixture of expert systems ", I. J. Computer Network and Information Security, pp. 1-16, 2012.

[24] http://www.caida.org/data/passive/telescope-3day. conficker_dataset.xml.

[25] www.ll.mit.edu/ideval/data/2000/LLS_DDOS_1.0.html.

[26] www.cs.waikato.ac.nz/ml/weka/

[27] R. Karimazad, A. Faraahi, "An anomaly-based method for DDoS attacks detection using RBF Neural Networks", International Conference on Network and Electronics Engineering IPCSIT, vol.11, IACSIT Press, Singapore, 2011.

[28] www.promethee-gaia.net/software.html.