Denial of Services Attack Detection using Random Forest Classifier with Information Gain

[1]Dr. Sanjay Agrawal, [2]Reena Singh Rajput
[1] Professor, [2]Student,
[1]Department of Computer Technology and application
[1]National Institute of Technical Teacher Training & Research, Bhopal, India

***Abstract*—Denial of service attacks (DoS) are a common threat to many online services. These attacks aim to overcome the availability of an online service with massive traffic from multiple sources. Denial of Service (DoS) is a prevalent threat in today's networks. Denial of service attacks are very common problem in the present scenario. To get rid of DoS attack we have the intrusion detection systems but we need to maintain the performance of the intrusion detection systems. Therefore, we propose a novel model for intrusion detection system using random forest classifier and information Gain (IG) model. Random Forest (RF) is an ensemble classifier and performs well compared to other traditional classifiers for effective classification of attacks. Intrusion detection system is made fast and efficient by use of optimal feature subset selection using IG. In this model we have tried to find out an optimal feature subset that gives performance greater than or equal to the performance given by the set of 41 features and time taken to build the model by the selected feature set is less than the time taken by the set of 41 features. This makes the intrusion detection systems faster and efficient. To evaluate the performance of our model, we conducted experiments on NSL-KDD data set. Empirical result show that proposed model is efficient, fast and robust and can get the high accuracy in detection DoS attack using WEKA tool.**

Key words — Denial of Service (DoS), NSL-KDD dataset, Random Forest, Information Gain.

I. INTRODUCTION

Network security is getting more importance because of the use of network based technologies and the sensitive information in the network. Many security technologies are developed like Intrusion prevention, information encryption and access control to protect the network based system but still they are not enough to detect many intrusions [7]. To detect the network attacks automatic monitoring of network activities, play a vital rule in network security.

There is a serious problem for computer scientists and practitioners for detection and prevention attacks and it have become a major focus of as computer attacks have become an increasing threat to commercial business as well as our daily lives. Intrusion detection system is intending to monitor the events in a system or network by determining whether is an intrusion or not. It also monitors the network traffic for suspicious activity and alert the network or system administrator about those attacks when occurred. The objective of this system intends to cover the availability, confidentiality and integrity of critical networked information system.

The Intrusion Detection systems can also be classified into two categories depending on where they look for intrusions. A host-based Intrusion detection system monitors activities associated with a particular host, and a network based IDS listens to network traffic. We construct a model which not only reducing feature for fast and but also increasing detection accuracy on detection known and unknown attacks. In our experiments, we use the data which originates from MIT's Lincoln Lab; a benchmark datasets. It was developed for Intrusion Detection System evaluations by DARPA. During the experiment, we examine the DoS attack.

II. RELATED WORK

In this section we describe different DoS and DDoS attack detection and prevention techniques proposed by different authors are discussed

V. Hema et.al [5] the author has proposed a traffic classification scheme to improve classification performance when few training data are available is used. The traffic flows are described using the discretized statistical features and traffic flow information is extracted. A traffic classification method is proposed to aggregate the Naïve Bayes predictions of the traffic flows. Since classification scheme is based on the posterior conditional probabilities, it can identify attacks occurring in an uncertain situation. The proposed system is able to improve the detection rate and reduce the occurrence of false positive alarms in the system for detecting denial of service attack using Naïve Bayes classification. The system can detect DOS attack occurring in the Local Area Network (LAN).The proposed system is able to produce minor improvement in these detection rates compared to the existing system. Accuracy in detecting the DOS attacks are also increased. But the detection rate and accuracy decreases with increase in traffic. The experimental results show that the proposed scheme can efficiently classify packets than existing traffic classification methods and achieved 92.34% accuracy.

S. Revathi et.al[6] The author proposed a system uses a statistical method called principal component analysis to filter the attributes and random forest classifier is used to detect various attack present in Denial of Service using NSL-KDD dataset. The proposed system described the nature of various attacks in DoS, using Principal Component Analysis of using it for detecting intrusions. The author used PCA to reduce attribute to avoid dimensionality problem and random forest classifier is used to split data

and to classify accuracy of the proposed system. The results obtained using a proposed criterion for detecting intrusion and leads to approximately 98 % detection rate.

Dimitris Gavrilis and Evangelos Dermatas et.al [7] presented and evaluated a Radial-basis-function (RFB) Neural Network for DDoS attacks dependent on statistical vectors through short-time window analysis. The proposed method was tested and evaluated in a controlled environment with an accuracy rate of 98% of DDoS detection.

Kejie, D.Wu, et al. [8] proposed a framework to detect DDoS attacks and identify attack packets efficiently. The purpose of the framework is to exploit spatial and temporal correlation of DDoS attack traffic. Such techniques can accurately detect DDoS attacks and identify attack packets without modifying existing IP forwarding mechanisms at the routers. This work achieved 97% for detection probability using the proposed framework.

E.Anitha et al. [9] author has proposed a new technique for detection of DDoS attack employing a packet marking approach. In this technique HX-DoS attacks square measure checked against cloud web services to discriminate between the legitimate and illegitimate messages. This can be through with the assistance of rule set based detection, known as CLASSIE. The author is employed modulo marking technique for avoiding the spoof attack. Reconstruct and Drop technique is employed on the victim aspect to drop the packets and take decision. The proposed technique improves the reduction of false positive rate, detection and filtering of DDoS attacks.

Wesam K. AL-Rashdan et.al. [10] The author proposed an intrusion detection model based on hybrid neural network and SVM. The key idea is to aim at taking advantage of classification abilities of neural network for unknown attacks and the expert based system for the known attacks. The author employed data from the third international knowledge discovery and data mining tools competition (KDDcup'99) to train and test the feasibility of proposed neural network component. The author proposed an integrated neural network and SVM for intrusion detection Model. This Model consists of three phases: Phase-1 clustering and Selecting, they used some classification and clustering methods such as KMedoid. Phase-2 Training, they built the Hybrid NN system to generate a new set for each type of attacks. The author used Hopfield network to detect known intrusions, and Kohonen SOM to detect Unknown intrusions and then create new vectors similar to original ones. This will expand number of vectors that will be used by SVM in Phase-3 learning and detecting phase. Therefore, their integrated model improves the performance to detect most intrusions. The experiment results demonstrate efficiency and accuracy of the detector According to the results of the experiment, the proposed model achieves 97.2% detection rate for DoS and Probing intrusions, and less than 0.04% false alarm rate.

Abu-Nimeh et al. [11] proposed a CBART method which is modified Bayesian Additive Regression Trees (BART) to make it applicable to classification. BART is primarily designed to predict quantitative (continuous) outcomes from observations via regression. They modified the current BART model and applied it to spam detection. They conducted parameters optimization which they used different numbers of trees ranging from 30 to 500 and also applied different power parameters for the tree prior, to specify the depth of the tree, ranging from 0.1 to 2.5. They found the optimal number of trees and power parameter. In their experimental results, CBART outperformed all the other classifiers and achieved the minimum average error rates. However, they did not apply feature selection.

S.Mercyshalinie et.al. [12] Author has proposed the framework to detect and mitigate TCPSYN flood attack. For this purpose, it developed the defense problem as an optimization problem that tries to reduce numbers of rejected connection requests and to reduce share of attack half-open connections from the TCP memory space. This solution led to a self-securing server that frequently monitors some performance metrics then tries to increase the security degree by dynamically setting of the desired parameters. Theoretical analysis show that the proposed solution gives an optimal value .The proposed defense mechanism improves performance of the under attack server. This defense mechanism show that h and m are effective control points to safe the TCP servers against SYN flood attack.

Dawei Wang et.al [13] the author has proposed a flow-based DOS detection system based on Artificial Immune systems. It adopts a tree structure to store flow info such that we are able to effectively extract useful features from flow info for higher detecting DoS attacks. Author employs Neighborhood Negative selection (NNS) as the detection rules to detect unknown DoS attacks, and determine attack flows from large traffic. As a result of the robust tolerance of NNS, the proposed solution is able to quickly get attack dynamics. The experimental results show that this solution is able to effectively find unknown DoS attack flows and determine attack flows from background traffic. The weakness of this paper it doesn't find all form of dos attack.

Jamal Esmaily et.al. [15] The author proposed, a method based on the combination of Decision Tree (DT) algorithm and Multi-Layer Perceptron (MLP) ANN is proposed which is able to identify attacks with high accuracy and reliability. The proposed method based on Artificial Neural Network and Decision Trees is proposed to design accurate Intrusion Detection System with high detection rate and low false alarm rate. This method is consisted of two different phases. The first phase is to create a new dataset by feeding the classification results of the DT and MLP on the random dataset. In the second phase, the MLP Network is used again to classify the data in the new dataset and then the results are evaluated. By using this hybrid method, identify attacks with 99.7% accuracy.

Vijay Katkar et.al. [16] The author proposed offline Signature based Network Intrusion Detection System for detection of Denial/Distributed Denial of Service attacks against HTTP servers using distributed processing and Naïve Bayesian classifier. Performance of Naïve Bayesian classifier with different pre-processing methods is evaluate using the test bed. Naïve Bayesian classifier when used with PKI discretization method it classifies normal behavior with 96.61% accuracy and Slow Loris with 97.15% accuracy.

Haddadi, F, Sara Khanchi et.al.[17] The author proposed a NIDS using a 2-layered, feed-forward neural network The proposed system classified normal connections and attacks. Different types of attacks were determined, and they focused on using training function, data validation and a preprocess dataset that caused less memory usage, minimum resource consumption and faster training. After implementing the proposed system on a KDD dataset, the result was very satisfactory, both on accuracy rate and performance.

Lee et.al. [18]The author proposed Quantitative Intrusion Intensity Assessment (QIIA). It provides intrusion (or normal) quantitative intensity value. It is capable of representing how an instance of audit data is proximal to intrusion (DoS attacks) or normal in a numerical value such as "0.95" proximity to intrusion. It can be interpreted as the instance has a probability of 0.95 to be classified as an intrusion. This approach is very novel and refreshing paradigm. It can overcome the drawback of current binary detection and classify intrusions in more detail. For example, DoS attacks can be classified as Smurf, Neptune, Teardrop, etc.

Sivatha Sindhu et al. [19] the author proposed a neuro tree model for a classification engine and wrapper based feature selection algorithm for Minimizing the computational complexity of the classifier were employed by the author. Then, they found optimal weight values to reduce the total error. However, the detection rates were not competent.

III. DATASET DESCRIPTION

In earlier days DARPA 98 [20] and later KDDcup99 [33] dataset has been used for analysis intrusion behavior, but there is various statistical degradation in the dataset which result in poor evaluation of anomaly detection. The inherent problem of KDD dataset leads to new version of NSL-KDD dataset that are mentioned in [21]. It is very difficult to signify existing original networks, but still it can be applied as an effective benchmark data set for researchers to compare different intrusion detection methods [22]. The statistical examination exposed that there are essential issues in the data set which highly affects the performance of the systems, and results in a very poor estimation of anomaly detection approaches. To solve these issues, a new data set as, NSL-KDD [23] is proposed, which consists of selected records of the complete KDD data set.

Advantage of NSL KDD dataset

The NSL KDD dataset has following advantages:

- No redundant records in the train set, so the classifier will not produce any biased result.
- No duplicate record in the test set which have better reduction rates.
- The number of selected records from each difficult level group is inversely proportional to the Percentage of records in the original KDD data set.

NSL-KDD training dataset consists of approximately 4,900,000 single connection vectors each of which contains 41 features and is labelled as either normal or an attack, with exactly one specific attack type

IV. PROPOSED WORK

Before In this section, we describe the methods employed in the proposed work, and illustrate how to apply these methods to build detection patterns with the high performance for intrusion detection.

Overview of the framework

At first in this section we discussed "Random forest" algorithm that is used in our proposed system. The figure 3.2 contains the flowchart of implementation of our framework, showing the steps needed to be performed from NSL-KDD dataset [33] that divided into two part training and testing to classify all types of attacks, using the proposed approach.

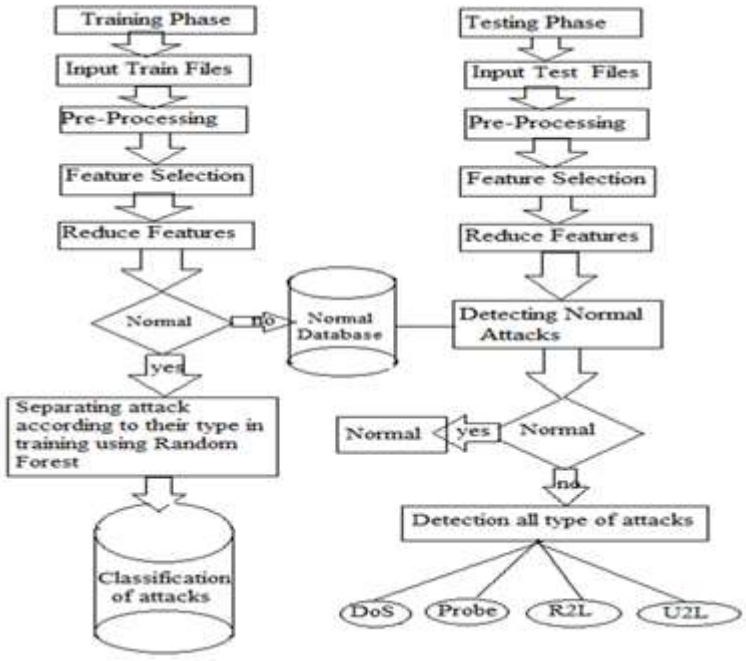

Figure 1 Proposed Framework

Our proposed framework is a new method for detecting all types of attacks especially Denial of service attack. This framework has two phases. The first phase is the training phase where a mathematical model is built using the available data (training dataset). Next phase is detection phase where we use the built model to detect all type of attack. The data for both normal and attack types are extracted from the NSL-KDD Intrusion Detection Evaluation data sets [33]. The features of the data set are analysed using Information Gain (IG) model that generated various statistics to detect intrusion. The information Gain model is used for selection of proper subset of attribute to reduce the dimensionality of the feature set to enable better visualization and analysis of the data. Once proper feature set (attributes) are selected, Random Forest algorithm is applied to classify the all types of attacks. Finally, result is analysed and compared with other classification algorithms. In first we describe detailed study of NSL-KDD dataset is explained for training and testing followed by feature selection, proposed architecture, Information Gain and Random Forest algorithm.

Data Pre-Processing and Feature Selection

Feature selection (FSS) is a pre-processing step commonly used in data mining. It is effective in dimensionality reduction and removes irrelevant features thus increases accuracy. Initially, we have used all features. Here we have selected 41attributes in order to detect the dos attacks. There are 41 features in the NSL-KDD dataset numbered from 1 to 41. They cover all three types of features in NIDSs: intrinsic features, traffic features, and content features. We have defined in our technique 41 feature vectors which will be used to evaluate the performance. Describe blow.

Table 1. List of the Features (Attributes)

S.No.	Feature Name	S.No.	Feature Name
1	Duration	22	Num_file_creations
2	Protocol-type	23	Num_shells
3	Service	24	Num_access_files
4	Flag	25	Num_output_cmds
5	Src_bytes	26	Is_hot_login
6	Dst_bytes	27	Is_guset_login
7	Land	28	Count
8	Wrong_fragment	29	Srv_cout
9	Urgent	30	Serror_rate
10	Hot	31	Srv_serror_rate
11	Num_failed_login	32	Rerror_rate
12	Num_compromised	33	Srv_rerror_rate
13	Root_shell	34	Diff_srv_rate
14	Su_attempted	35	Srv_diff_host_rate
15	Num_root	36	Dst_host_count
16	Dst_host_srv_count	37	Dst_host_same_srv_rate
17	Dst_host_diff_srv_rate	38	Dst_host_same_src_port_rate
18	Dst_host_srv_diff_host_rate	39	Dst_host_serror_rate
19	Dst_host_srv_serror_rate	40	Dst_host_rerror_rate
20	Dst_host_srv_rerror_rate	41	Logged_in
21	Same_srv_rate		

We employ the feature selection algorithm i.e. Information Gain for attribute select the optimal feature set. In this way we proposed to find out a subset out of 41 features, whose performance is equal to or greater than the performance given by the 41 features. For this purpose, we used the IGSA (Information Gain Selection Attribute) algorithm of Weka tool to rank the features with the help of the Ranker Search Method. We get ranking stage employs Information Gain algorithm (IG) that uses a filtering approach. The stage aims at ranking subsets of features based on high information gain entropy in decreasing order. We divided the NSL-KDD dataset into different size of sample datasets. After that we got Reduce dataset files by using IFSA. We saved these file in ARFF format. Then we used the random forest classifier of weka [20] tool to classify the feature set and check their performance.

Random Forest Classifier

Random Forest (RF) is a moderately new algorithm for classification developed by Leo Breiman [28] that uses an ensemble of unpruned classification or regression trees. The random forests generates many classification trees. Each tree is constructed by a different bootstrap sample from the original data using a tree classification algorithm. After the forest is formed, a new object that needs to be classified is put down each of the tree in the forest for classification. Each tree gives a vote that indicates the tree's decision about the class of the object. The forest chooses the class with the most votes for the object. Thus, random forest uses both bagging and boosting as successful approach [12], and random variable selection for tree building. Here blow define the definition of Random Forest algorithm-

The main features of the random forests algorithm are listed as follows: [28] [29]

- It is unsurpassable in accuracy among the current data mining algorithms.
- It runs efficiently on large data sets with many features and it can give the estimates of what features are important.
- It has no nominal data problem and does not over-fit and it can handle unbalanced data sets.
- It generates an internal unbiased estimate of the generalization error as the forest building progresses.

PROPOSED ARCHITECTURE

The random forest is an ensemble classifier. Many current intrusion detection systems are developed for classifying the attacks. However, the methods produce less accuracy in detecting intrusion. Therefore, we propose DoS detection system using Random forest. In this paper we proposed a new model that apply random forest algorithm for network intrusion detection that Classify various type of attacks and improve accuracy of classifier in different type of attacks especially DoS attacks. In fig.4.1 gives the Sequence of implementation Steps for Proposed Approach.

.

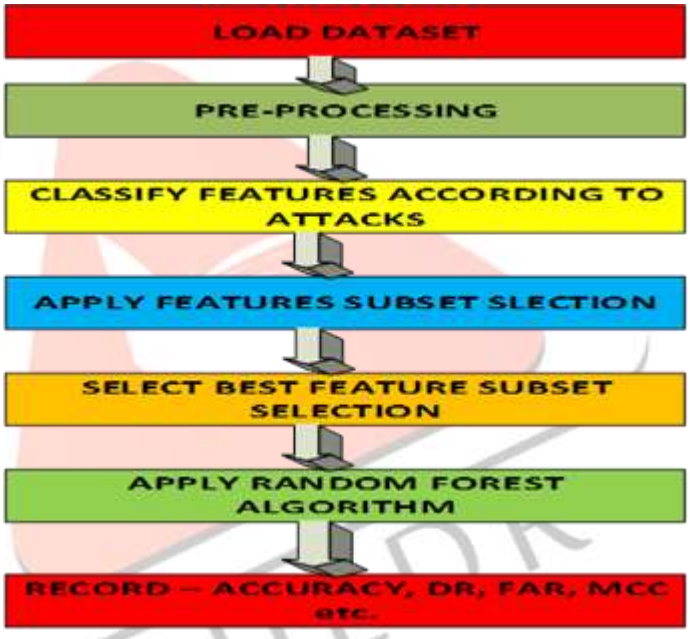

Figure 2: Architecture of implementation

Here we describe the step by step process of proposed approach.to Detect DoS attack by using Random forest algorithm. Random forest model for network to detect Denial of service attack.

Input: NSL-KDD dataset
Output: Classification of different type of attacks
Step 1: Load the dataset
Step 2: Apply pre-processing
Step 3: Cluster the dataset into different-different size datasets.
Step 4: Partition the data set into training and test
Step 5: Select the best set features using feature subset selection measure information gain

InfoGain (Class, Attribute) = H (Class) – H (Class | Attribute)

Step 6: Data set is given to Random forest for training
Step 7: The test data set is then fed to random forest for classification
Step 8: Calculate accuracy, F-Measure, Mathew correlation coefficient etc.

For our experimental analysis, we downloaded the NSL-KDD dataset and save it in CSV format. We adopted the following preprocessing techniques to run the experiment.

- Replace missing values:

In weka, we have used replace missing values filter to replace all missing feature values in NSL-KDD dataset. This filter replaces all missing values with the mean and mode from the training data.

V. Experimental Results

All experiments were carried using weka tool. We used NSL-KDD dataset for our analysis. NSL-KDD dataset consists of 42 attributes; last attribute consists of class label. We tested for various number of Random forest trees. Following performance measures are used to evaluate the classifier.

1. **Accuracy** – Defined as the ratio of correctly classified samples to total number of samples

$$Accuracy = \frac{Sample\ correctly\ classified\ in\ test\ data}{Number\ of\ samples\ in\ test\ data}$$

2. **Precision-** Precision means how many relevant items are selected. It is the ratio of the number of relevant attacks retrieved to the total number of irrelevant and relevant attacks retrieved.

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

3. **F –measure-** It is combination of recall and precision. It measure the accuracy using the precision and recall.

$$F1 = \frac{2TP}{2TP + FP + FN}$$

4. **Mathews correlation coefficient (MCC)-** This is defined as ratio between the observed and predicted binary classifications. MCC is given by:

$$MCC = \frac{TN \times TP - FN \times FP}{\sqrt{(FP + TP)(FN + TP)(TN + FP)(TN + FN)}}$$

Where, F1 = F- (or F1-Measure)
TP =True Positives
FN= False Negatives
FP= False Positives

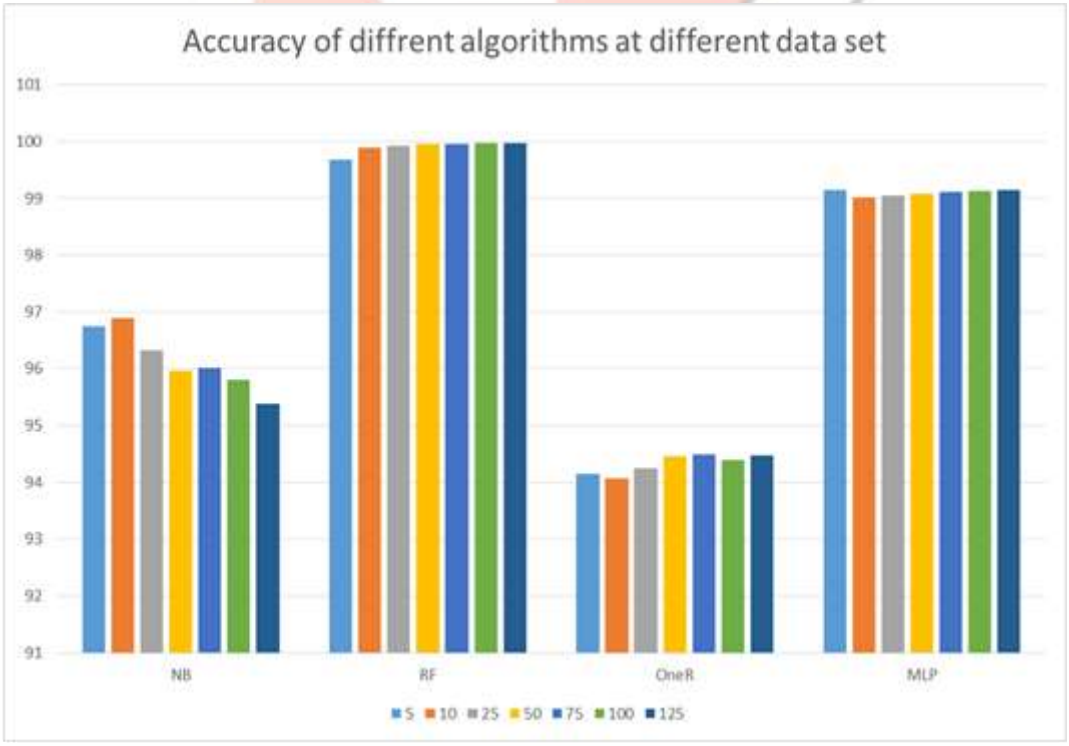

Fig 5.1 Comparison of accuracy results between Machine Learning Algorithm RF, NB, One R, and MLP.

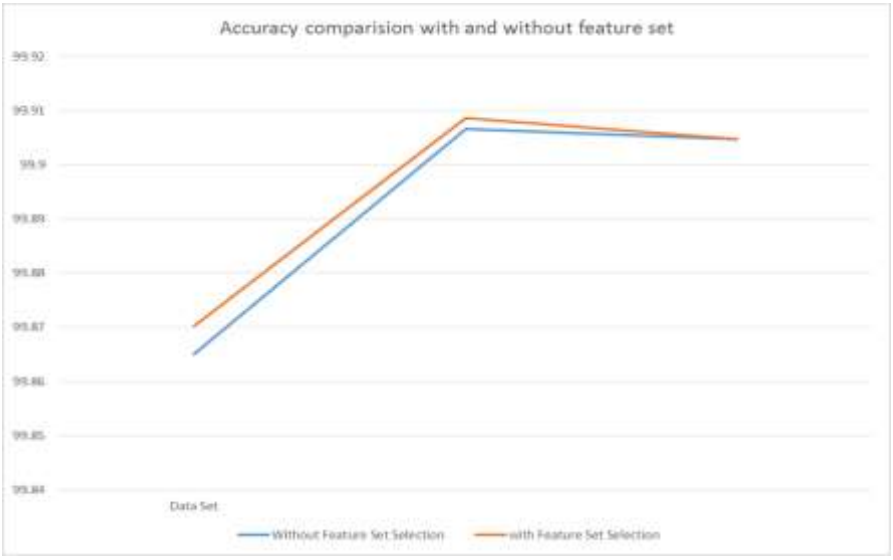

Fig. 5.2 Accuracy comparison of Random forest with and without feature set selection.

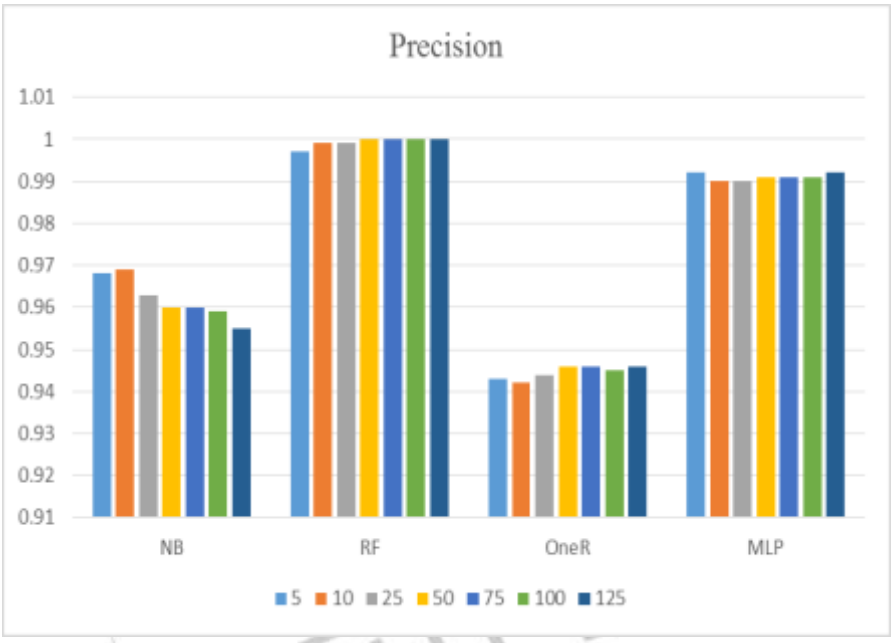

Fig. 5.3 Comparative Precision values of the Proposed, NB, One R, MLP and approaches

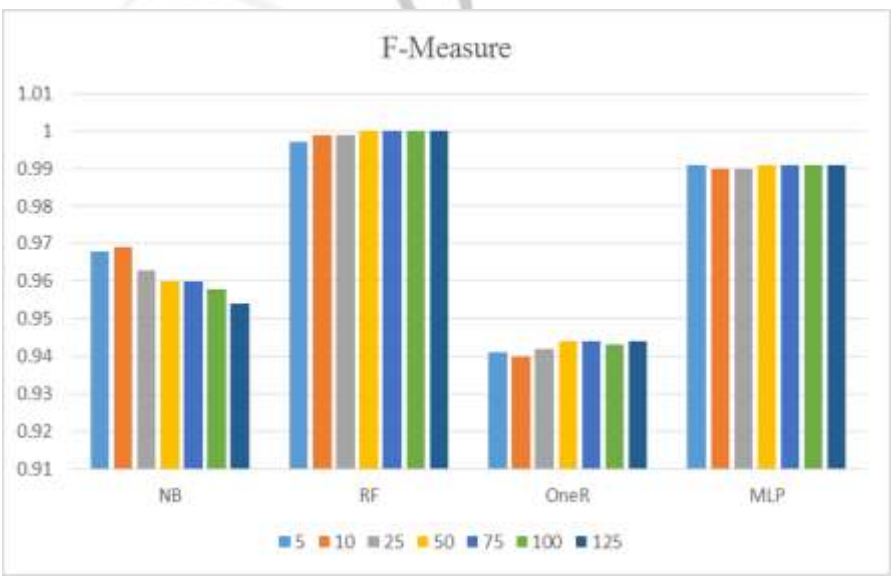

Fig. 5.4 Comparative F-Measure of the Proposed, NB, One R, and MLP approaches

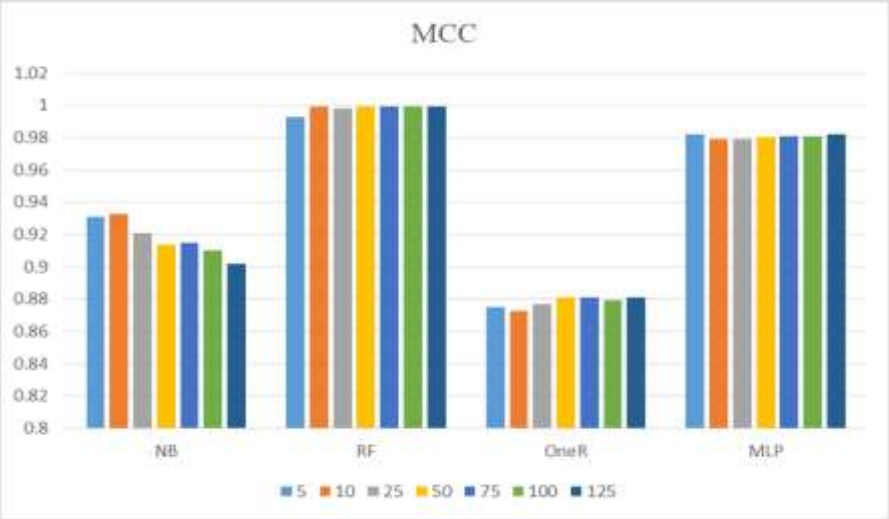

Fig. 5.5 Comparative MCC of the Proposed, NB, One R, and MLP approaches

In the above fig5.1, Y dimension indicate accuracy having dataset size 5000, 10000, 25000, 50000, 75000, 100000,125000 accordingly. X dimension indicate Training performance of different Machine learning algorithms. The results show training performance with respect to no. of samples with all relevant features. It shows that how training performance of network increases when number of samples having relevant features increases.

In experiments, system use 100 iteration and reduced features to classify. To reduce the features from the dataset, we have used the information gain method with ranker features in WEKA. Thus, it could be observed that the parameters which are most important like accuracy, F-Measure are highest with our proposed model as compared to other algorithms.

In our proposed work we carries out our experiments with NSL-KDD dataset. We divided the NSL-KDD dataset into 5000 or 5K, 10,000 or 10K, 25000 or 25K, 50,000 or 50K, 75000 or 75K, 100000 or 100K data samples for finding the accuracy to detect the attacks. After feature selection we get reduced dataset files in ARFF format. The Selected features(reduced one) gives performance greater than or equal to the performance given by the set of 41 features and time taken to build the model by the selected feature set is less than the time taken by the set of 41 features. We spited these dataset files into training and testing into 20%, 40%, 60%, and 80% on different data samples. We used these file in Weka tool for classification using Random Forest Classifier. In Weka the Random Forest Bagging with 100 iterations and base learner with these parameter values -K 0 -M 1.0 -V 0.001 -S 1.

We have used MLP, One R, and Navies biases Classifiers are also for calculating the accuracy of dos detection. These Classifier detect DoS attacks. The results obtained shows that proposed system is efficient enough to do the same. In the research we have compared the efficiency of our proposed system with the existing system.

Using the proposed 'Random Forest' approach, it was found that our approach provides high accuracy, it means our proposed model most accurately identify the DoS attack even with and without feature selection. We analyzed the efficiency of our DoS detection system. In our work, main aim is to improve the efficiency of system to detect DoS.

IV.CONCLUSION AND FUTUREWORK

In this paper we have proposed an architecture to detect the DOS attack using random forest algorithm for classification and IG feature set selection. Feature selection is applied on the data set to reduce dimensionality and to remove redundant and irrelevant features. We applied Information Gain of attributes which reduced the irrelevant features and give the feature set which gives performance greater than or equal to the performance of set of 41 features and in less time. The proposed approach is evaluated using NSL- KDD dataset. It is shown in this paper that proposed approach of 'Random Forest' has a major effect on the overall accuracy of the analysis. This approach has an accuracy of around 99.97% for classification and F-Measure and MCC is recorded 99.9%. Comparison between different algorithms and proposed approach shows that proposed approach is superior in critical evaluation parameters of accuracy and F-Measure etc. We find that proposed system is efficient with the higher accuracy and less error to detect denial of service attack. The propose system is effective and robust to detect denial of service attack. The simulation of the presented technique was provided in 'Weka'.

For future work, we will apply evolutionary computation as a feature selection measure to further improve accuracy of the classifier and apply and test the model using the clustering algorithm in combination with classifier approach and using this model in the cloud for DoS detection

REFERENCES

[1] Tamas Abraham, "IDDM: Intrusion Detection Using Data Mining Techniques", Technical Report DSTO-GD-0286, DSTO Electronics and Surveillance Research Laboratory, 2001.

[2] Jiong Zhang et.al "Network Intrusion Detection using Random Forests" IEEE Transactions on Systems, Man, and Cybernetics, Volume: 38, Issue: 5, Sept. 2008

[3] Daniel Barbarra et.al "ADAM: Detecting Intrusions by Data Mining" 2001 IEEE, Assurance and Security, NY, USA, June 2001

[4] Meiko Jensen et.al "On technical issues in cloud computing", IEEE International Conference on cloud computing, CLOUD 2009, Bangalore, India, 21-25 September, 2009.

[5] V. Hema and C. Emilin Shyni "DoS attack detection based on Naive Bayes Classifier" Middle-East Journal of Scientific Research 23 (Sensing, Signal Processing and Security): 398-405, 2015 ISSN 1990-9233 © IDOSI Publications, 2015

[6] S. Revathi et.al" Detecting Denial of Service Attack Using Principal Component Analysis with Random Forest Classifier" International Journal of Computer Science & Engineering Technology (IJCSET) Vol. 5 No. 03 Mar 2014

[7] D. Gavrilis and E. Dermatas, "Real-time detection of distributed denial of-service attacks using rbf networks and statistical features," Computer Networks, vol. 48, no. 2, pp. 235–245, 2005.

[8] K. Lu, D. Wu et.al "Robust and efficient detection of ddos attacks for large-scale internet," Computer Networks, vol. 51, no. 18, pp. 5036–5056, 2007J.

[9] Anitha, E., and S. Malliga.et.al "A packet marking approach to protect cloud environment against DDoS attacks." International Conference on. IEEE, 2013 Information Communication and Embedded Systems (ICICES), 21-22 Feb. 2013, Page(s):367 – 370Print ISBN: 978-1-4673-5786-9 Chennai.

[10] Wesam K. AL-Rashdan et.al. "Novel Network Intrusion Detection System using Hybrid Neural Network (Hopfield and Kohonen SOM with Conscience Function)" in International Journal of Computer Science and Network Security, VOL.10 No.11, November 2010

[11] Abu-Nimeh, D. Nappa, X. Wang, and S. Nair. Bayesian Additive Regression Trees-Based Spam Detection for Enhanced Email Privacy". In Proc. of the 3rd Int. Conf. on Availability, Reliability and Security (ARES 2008), Barcelona, Spain, pages 1044–1051, IEEE, March 2008.

[12] S.Mercyshalinie et.al. "Defense against DoS Attack: PSO Approach in Virtualization" 2014 ICOAC, 17-19 Dec. 2014, Page(s):199 – 204, Chennai, ISSN: 2377-6927.

[13] Dawei Wang et.al. "Exploiting Artificial Immune System to Detect Unknown DoS Attack in Real Time" Cloud Computing and Intelligent Systems (CCIS), 2012 IEEE 2nd International Conference vol.2, Hangzhou 10.1109/CCIS.2012.6664254.

[14] Y. Xie. An Introduction to Support Vector Machine and Implementation in R. May 2007. Available at http://yihui.name/cv/images/SVM_Report_Yihui.pdf.

[15] Jamal Esmaily et.al. "Intrusion Detection System Based on Multi-Layer Perceptron Neural Networks and Decision Tree" IKT2015 7th International Conference on Information and Knowledge Technology 2015 IEEE.

[16] Vijay Katkar et.al. "Detection of DoS/DDoS attack against HTTP Servers using Naïve Bayesian" 2015 International Conference on Computing Communication Control and Automation 2015 IEEE DOI 10.1109/ICCUBEA.2015.60

[17] F. Haddadi, et.al "Intrusion detection and attack classification using feed-forward neural network," in Computer and Network Technology (ICCNT), 2010 Second International Conference on, pp. 262–266, IEEE, 2010(detecting 59 DDO).

[18] S.Lee, et.al "Quantitative Intrusion Intensity Assessment using Important Feature Selection and Proximity Metrics". In Proc. of the 15th IEEE Pacific Rim Int. Symp. On Dependable Computing (PRDC'09), Shanghai, China, pages 127–134, IEEE, November 2009.

[19] S. Sivatha Sindhu, et,al "Decision Tree Based Light Weight Intrusion Detection Using a Wrapper Approach". Expert Systems with Applications, 39:129–141 2012.

[20] MIT Lincoln Labs, 1998 DARPA Intrusion Detection Evaluation. Available on: http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/index.html, February 2008.

[21] Mahbod Tavallae et.al "A Detailed Analysis of the KDD CUP 99 Data Set", In the Proc Of the IEEE Symposium on Computational Intelligence in Security and Defense Applications (CISDA 2009), pp. 1-6, 2009

[22] J. McHugh, "Testing intrusion detection systems: a critique of the 1998 and 1999 darpa intrusion detection system evaluations as performed by lincoln laboratory," ACM Transactions on Information and System Security, vol. 3, no. 4, pp. 262–294, 2000

[23] J. Mirkovic and P. Reiher et.al. "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms" ACM Sigcomm Computer Communications Review; Vol. 34, No. 2, Apr. 200

[24] Swati Paliwal et.al" Denial-of-Service, Probing & Remote to User (R2L) Attack Detection using Genetic Algorithm" International Journal of Computer Applications (0975 – 8887) Volume 60– No.19, December 2012.

[25] Sabhnani M.et.al "Application of Machine Learning Algorithms to KDD Intrusion Detection Dataset within Misuse Detection Context" ,International Conference on Machine Learning ,Models, Technologies andApplications,2003

[26] Wenke Lee et.al "A Framework for Constructing Features and Models for Intrusion Detection Systems", ACM Transactions on Information and System Security (TISSEC), Volume 3, Issue 4,November 2000.

[27] Taqwa Ahmed Alhaj , Maheyzah Md Siraj,et.al" Feature Selection Using Information Gain for Improved Structural-Based Alert Correlation" Feature Selection Using Information Gain for Improved Structural-Based Alert Correlation

[28] Breiman" Random Forest" Statistics Department University of California Berkeley, CA94720January 2001 pdf.

[29] Mohammed Zakariah et.al " Classification of large datasets using Random Forest Algorithm in various applications: Survey" International journal of Engineering and Innovative Technology (IJEIT) Volume 4, Issue 3, September 2014.

[30] http://weka.sourceforge.net/doc.dev/weka/attributeSelection/InfoGainAttributeEval.html

[31] http://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-30/dos-attacks.html

[32] http://www.cs.waikato.ac.nz/ml/weka/index.html

[33] https://github.com/defcom17/NSL_KDD