IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 8, Issue 8, August 2020

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

9940 572 462 | 6381 907 438 | ijircce@gmail.com | www.ijircce.com

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 8, August 2020 ||

Semi-Supervised Machine Learning Approach for Ddos Detection

Nikhil Kumar Rajpoot[1], Arun Mittal[2]

M. Tech Student, Department of CSE, Greater Noida Institute of Technology, Greater Noida, Dr. APJ Abdul Kalam Technical University, Lucknow, India[1]

Asst. Professor, Department of CSE Greater Noida Institute of Technology, Greater Noida, Dr. APJ Abdul Kalam Technical University, Lucknow, India[2]

ABSTRACT: Distributed Denial of Service (DDoS) is a cyber-attack on network with an intended purpose of disrupting the normal operation of a targeted server. Even though advanced Machine Learning (ML) techniques have been adopted for DDoS detection, the attack remains amajor threat of the Internet. Most of the existing ML-based DDoS detection approaches are under two categories: Supervised and Unsupervised. Supervised ML approaches for DDoS detection rely on availability of labeled network traffic datasets. Whereas, unsupervised ML approaches detect attacks by analyzing the incoming network traffic. Both approaches are challenged by large amount of network traffic data, low detection accuracy and high false positive rates. This work presents Semi-supervised ML approach for DDoS detection based on network Entropy estimation, Co-clustering, Information gain ratio and Random Forest algorithm. The Unsupervised part of the approach allows reducing the irrelevant normal traffic data for DDoS detection which allows reducing false positive rates and increasing accuracy. Whereas, the supervised part allows reducing the false positive rates of the unsupervised part and to accurately classify theDDoS traffic

KEYWORDS: DDoS attacks,Machine learning,Semi-supervised

I.INTRODUCTION

Despite the important evolution of the information security technologies in recent years, the DDoS attack remains a major threat of Internet.A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.The attack aims mainly to deprive legitimate users from Internet resources. The impact of the attack relies on the speed and the amount of the network traffic sent to the victim.

Machine Learning (ML) is the science of making computers learn and act like humans by feeding data and information without being explicitly programmed. The machine receives data as input, use an algorithm to formulate answers. DDoS detection approaches based on Machine Learning can be classified into 3 groups i.e., Supervised, Unsupervised and Semi-supervised. In this work Semi-supervised ML approach is used which is the combination of Supervised and Unsupervised approaches, which works on both labeled and unlabeled datasets, that allows increasing the accuracy and decreases the false positive rate. In Semi-supervised ML approach, entropy is estimated for header features of the network traffic data. The Unsupervised co-clustering algorithm splits the incoming network traffic data into 3 clusters. Then, the information-gain ratio is estimated for each cluster by usingaverage entropy of feature header between the traffic data and cluster. The data cluster that provides the high information-gain ratio is considered as anomalous and they are selected for preprocessing and classification using ensemble ML classifiers i.e., Random Forest algorithm. To better evaluate the performance of this approach NSL-KDD network traffic dataset is used.

A.PROBLEM STATEMENT

For DDoS detection, the presence of large amount of irrelevant data in the incoming network traffic data reduces the performance of supervised approach. Due to high dimensional network traffic data 'the curse of dimensionality' problem occurs which prevents the unsupervised approach to detect the attacks accurately.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 8, August 2020 ||

1.2.1 Existing System

In existing ML based DDoS detection approaches, Supervised ML approach uses generated labeled network traffic datasets to build the detection model.Unlike the first category, in the unsupervised approachesno labeled dataset is needed to build the detection model.The DDoS and the normal traffics are distinguished basedon the analysis of their underlying distribution characteristics.

Disadvantages:

- Supervised ML approaches are unable to predict the new legitimate and attack behaviors. Presence of noisy data reduces the performances of the classifiers.
- The main drawback of Unsupervised ML approach is high false positive rates.

1.2.2 Proposed System

Semi-supervised approach is taking the advantage of both Supervised and Unsupervised methods, which is capable to work on both labeled and unlabeled datasets. Unsupervised part includes entropy estimation, co-clustering and info-gain ratio. The supervised part is the Random forest ensemble classifier.

Advantages:

- The Unsupervised part of our approach to reduce the irrelevant and noisy normal traffic data, which reduces the false positive rates and increases the accuracy of supervised part.
- Supervised part reduces the false positive rate of unsupervised part and classifies the DDoS traffic accurately.

II.LITERATURE SURVEY

Empirical evaluation of several major information metrics namely, Hartley entropy, Shannon entropy, Renyi's entropy, generalised entropy, Kullback-Leibler divergence and generalised information distance measure in their ability to detect both low-rate and high-rate DDoS attacks is Bhuyan MH, Bhattacharyya DK, Kalita JK [1].

Akilandeswari V. et al. have used a Probabilistic Neural Network to discriminate flash crowd events fromDDoS attacks. The method achieves high DDoS detection accuracy with lower false positives rates [2].

Alan S. et al. have proposed a DDoS Detection Mechanism based on ANN (DDMA). The authors used three different topologies of the MLP for detecting three types of DDoS attacks based on the background protocol used to perform each attack namely TCP, UDP and ICMP. The mechanism detects accurately known and unknown, zero day, DDoSattacks[3].

Lui T, Wang Z, Wang H, Lu K[4] proposed an entropy based method to analyze the numerous IDS alerts and detect real networks attacks. Shannon entropy is used to examine distribution of the source IP address, destination IP address, source threat and destination threat and datagram length of IDS alerts; employ Reyni cross entropy to fuse the Shannon entropy vector to detect network attack.

Boro D. et al. [5] have presented adefense system referred to as DyProSD that combinesboth the merits of feature-based and statistical approachto handle DDoS flooding attack. The statistical modulemarks the suspicious traffic and forwards to an ensembleof classifiers for ascertaining the traffic as malicious ornormal.

Mohamed I. et al. [6]have proposed a supervised DoS detection method basedon a feed-forward neural network. This method consists ofthree major steps: (1) Collection of the incoming networktraffic, (2) selection of relevant features for DoS detectionusing an unsupervised Correlation-based Feature Selection(CFS) method, (3) classification of the incoming networktraffic into DoS traffic or normal traffic.

Mustapha B. et al. [7] have presenteda two-stage classifier based on RepTree algorithm andprotocols subset for network intrusion detection system.The first phase of their approach consists of dividing theincoming network traffic into three types of protocols TCP,UDP or Other, then classifying it into normal or anomalytraffic. In the second stage a multi-class algorithm classifythe anomaly detected in the first phase to identify theattacks class in order to choose the appropriate intervention.Two public datasets are used for experiments in this papernamely the UNSW-NB15 and the NSL-KDD.

Ali S. B. et al. [8] have proposed an innovative ensemble of Sugeno type adaptive neuro-fuzzy classifiers for DDoS detection using an effective boosting technique named Marliboost. The proposed technique was tested on the NSL-KDD dataset and has achieved good performance.

Mohiuddin A. and AbdunNaser M. [9] have proposedan unsupervised approach for DDoS detection based onthe co-clustering algorithm. The authors have extendedthe co-clustering algorithm to handle categorical attributes. The approach was tested on the KDD cup 99 datasetand achieved good performance.

Van Loi C. [10] proposed a novel oneclasslearning approach for network anomaly detectionbased on combining auto-encoders and density estimation.Authors have tested their method on the NSL-KDD dataset, and obtained satisfactory results.

V. Jaiganesh, Dr. P. Sumathi, S. Mangayarkarasi [11], have classified attacks into four classes DoS, Probe, U2R, R2L using Machine learning and BPN techniques. They have worked on detection rates for four attacks. For DoS attack the detection rate is 78.15% using BPN.

Changjun Han, Yi Lv and Dan Yang, Yu Hao in [12],trained data using BPN model with 8 attack types. Where,1325 connections used for training and 1245 for testing. Their obtained results are: detection rate 80.5%, false alarm rate7.4% and omission rate 11.3%. Sufyan T. Faraj and et al. in [13], first trained data to detect and classify normal andabnormal events using BPN. Then abnormal events are further classified into five categories. Detection rate and false positiverate is calculated in different scenarios. For detection of normal and abnormal events detection rate for test set is about90% and for classification into DoS, U2R, R2L, Probe is approximately 60-85%.

Mukhopadhyay and etl al [15], trained BPN Neural Network Model for DoS, U2R, Probe, U2L and normal attack classes. The system gets success rate 73.9% for new test set and 95.6 % for level 1 test set. Hua TANG and Zhuolin CAO in used SVM and MLP neural network for anomaly detection. They compared accuracy for DoS, U2R, Probe, U2L attack classes and found that accuracy of neural network is better than SVM. Vladimir Bukhtoyarovf and Eugene Semenkin, used neural network ensemble approach. Their work was focused on classifying probe attacks using joint usage of trained neural network. They found 99.87% detection rate for probe attacks but large amount of training time required which was one of the IDS issue.

The performances of network intrusion detection approaches, in general, rely on the distribution characteristics of the underlying network traffic data used for assessment. The DDoS detection approaches in the literature are under two main categories unsupervised approaches and supervised approaches. Depending on the benchmark datasets used, unsupervised approaches often suffer from high false positive rate and supervised approach cannot handle large amount of network traffic data and their performances are often limitedby noisy and irrelevant network data. Therefore, the need of combining both, supervised and unsupervised approaches arises to overcome DDoS detection issues.

III.SYSTEM ARCHITECTURE

System Architecture is a conceptual model that defines the structure, behavior and more views of a system. An architecture description is the formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviors of the system.

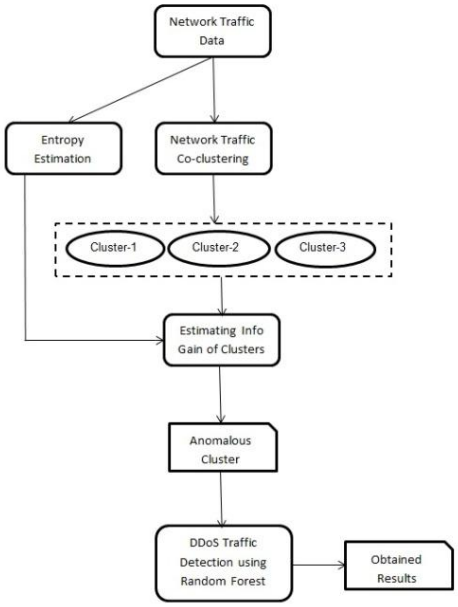

Fig. 4.1.1 System Architecture

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 8, August 2020 ||

Fig 4.1.1 represents the system architecture of the proposed approach. It is a comprisedof some components that are related to each other and work together to implement the system.

Network Traffic Data

In proposed work, NSL-KDD[18] network traffic data is used. NSL-KDD is a data set suggested to solve some of the inherent problems of the KDD'99 data set. Although, this new version of the KDD data set still suffers from some of the problems and may not be a perfect representative of existing real networks, because of the lack of public data sets for network-based IDSs, we believe it still can be applied as an effective benchmark data set to help researchers compare different intrusion detection methods.

The NSL-KDD dataset contains the attack data. It has 42 features divided into three groups: Basic features, content features and traffic features. This dataset contains a total number of 125973 records in training set and 22554 records in testing set.

The NSL-KDD data set has the following advantages over the original KDD data set:

- It does not include redundant records in the train set, so the classifiers will not be biased towards more frequent records.
- There are no duplicate records in the proposed test sets; therefore, the performance of the learners is not biased by the methods which have better detection rates on the frequent records.
- The number of selected records from each difficultylevel group is inversely proportional to the percentage of records in the original KDD data set. As a result, the classification rates of distinct machine learning methods vary in a wider range, which makes it more efficient to have an accurate evaluation of different learning techniques.
- The number of records in the train and test sets is reasonable, which makes it affordable to run the experiments on the complete set without the need to randomly select a small portion. Consequently, evaluation results of different research works will be consistent and comparable.

Entropy Estimation

Initially, the entropy is estimated for FSD features of traffic data. The flow size distribution (FSD) features, the source/destination packets count and the source/destination bytes count, are used to estimate the entropy. As in the case of NSL-KDD dataset, it consists of two FSD features: source bytes and destination bytes. The reason for using the FSD features is that during a DDoS attack the zombie hosts send a large number of packets to the victim which generates a large amount of network flow data.

Network Traffic Co-clustering

Next step is to split the network traffic data into three clusters using a co-clustering algorithm i.e., Spectral co-clustering algorithm. The aim of splitting the network traffic is to reduce the amount of data to be classified by excluding the normal cluster for the classification.Mostof the time, the new unseen normal traffic instances causethe increase of the false positive rate and the decreaseof the classification accuracy. Hence, excluding somenoisy normal instances of the network traffic data forclassification is beneficial in terms of low false positive ratesand classification accuracy.

Estimating Info Gain of Clusters

Estimation of information gain ratio based on the FSD features allows identifying the two cluster that preserve more information about the DDoS attack and the cluster that contains only normal traffic. Therefore, the cluster that produce lower information gain ratio is considered as normal and the remaining clusters are considered as anomalous.

DDoS Traffic Detection using Random Forest

The data present in the anomalous cluster is preprocessed for classification by taking care of missing data, encoding categorical data and feature scaling.

Ensemble-based trees such as Random Forest are used to overcome the representational problem of the unvaried decision tree and to accurately classify the attack data. Hence, ensemble-based trees are widely used for classification.

V. RESULTS AND DISCUSSION

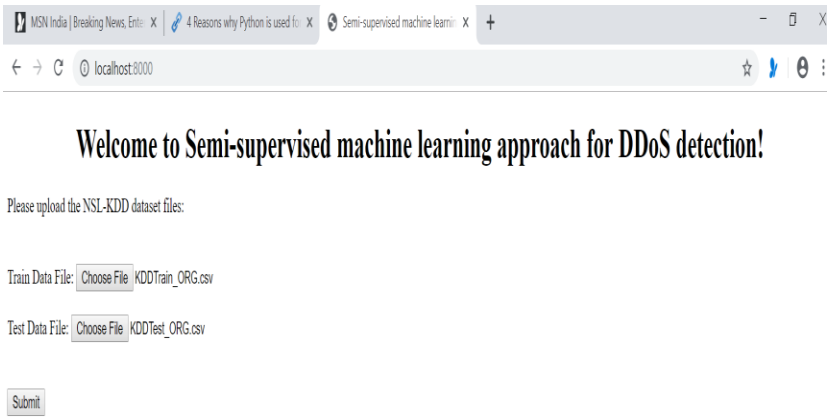

Fig.5.1.1 Screenshot of web page to upload Train and Test dataset

Fig 5.1.1 represents the web page where we upload our NSL-KDD training and testing dataset. Submit button is provided, on clicking which the dataset will be uploaded and the further computations takes place.

Fig 5.1.2 represents the data size of each cluster after clustering. After this information gain is calculated for each cluster which helps to remove the irrelevant normal traffic data.

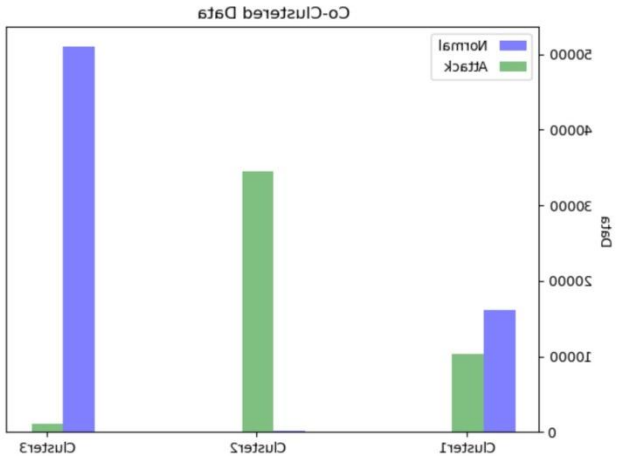

Fig.5.1.2 Screenshot of web page to upload Train and Test dataset

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 8, August 2020 ||

```
Average Entropy:0.492034015598514

+-----------+--------------------+---------------------+
|     X     |  shannon_entropy   |  normalized_entropy |
+-----------+--------------------+---------------------+
| src_bytes | 6.1434157820153334 |  0.5248062578263939 |
| dst_bytes | 6.056304622502039  | 0.45926177337063406 |
+-----------+--------------------+---------------------+
Average Entropy:0.46945053754513505

+-----------+--------------------+---------------------+
|     X     |  shannon_entropy   |  normalized_entropy |
+-----------+--------------------+---------------------+
| src_bytes | 5.193116096657044  |  0.493659283632879  |
| dst_bytes | 4.162444471237995  |  0.4452417914573911 |
+-----------+--------------------+---------------------+
Average Entropy:0.006201544992091686

+-----------+---------------------+----------------------+
|     X     |   shannon_entropy   |  normalized_entropy  |
+-----------+---------------------+----------------------+
| src_bytes | 0.04174545855797314 | 0.00670198646521364  |
| dst_bytes | 0.03381174750526495 | 0.005701103518969732 |
+-----------+---------------------+----------------------+
Average Entropy:0.7765967650261083

+-----------+-------------------+--------------------+
|     X     |  shannon_entropy  |  normalized_entropy |
+-----------+-------------------+--------------------+
| src_bytes |  8.76464699816996 |  0.7591748808924171 |
| dst_bytes | 10.43786249240959 |  0.7940186491597994 |
```

Fig.5.1.3 Screenshot of text file having entropy values

Fig 5.1.3 shows the Shannon entropy, normalized entropy and average entropy values of the whole dataset and the three clusters respectively. These values are stored in a text file.

```
+------------+----------------------+
| Cluster ID |      Info Gain       |
+------------+----------------------+
|     1      |  0.3823283942617106  |
|     2      |  0.4901388405309652  |
|     3      | 0.13424552629960462  |
+------------+----------------------+
```

Fig.5.1.4 Screenshot of text file having info-gain values of clusters

Fig 8.1.4 represents the calculated information gain ratio value of each cluster which is stored in a text file.

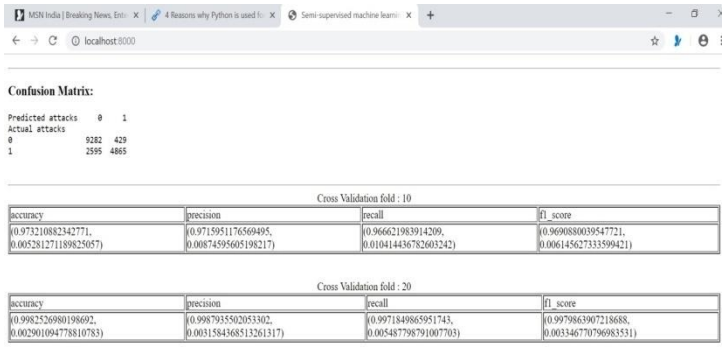

Fig.5.1.5 Screenshot of result page

Fig 5.1.5 shows the result page in which confusion matrix and k-fold cross validation result is generated. A confusion matrix is a table that is often used to describe the performance model on a set of test data for which the true values are known. It shows the four basic terms: true positives, true negatives, false positives, and false negatives.

Cross validation is a statistical method used to estimate the skill of machine learning models. k-fold cross validation is a procedure used to estimate the skill of the model on new data. We have estimated four performance metrics: accuracy, precision, recall and f1-score in each fold as shown in the Fig 5.1.5.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 8, August 2020 ||

- **Accuracy** - Accuracy is the most intuitive performance measure and it is simply a ratio of correctly predicted observation to the total observations.
  Accuracy = TP+TN/TP+FP+FN+TN
- **Precision** - Precision is the ratio of correctly predicted positive observations to the total predicted positive observations.
  Precision = TP/TP+FP
- **Recall** (Sensitivity) - Recall is the ratio of correctly predicted positive observations to the all observations in actual class - yes.
  Recall = TP/TP+FN
- **F1 score** - F1 Score is the weighted average of Precision and Recall.
  F1 Score = 2*(Recall * Precision) / (Recall + Precision)

Classification Report

	precision	recall	f1-score	support
Normal Data	0.78	0.96	0.86	9711
Attack Data	0.92	0.65	0.76	7460
micro avg	0.82	0.82	0.82	17171
macro avg	0.85	0.80	0.81	17171
weighted avg	0.84	0.82	0.82	17171

Fig.5.1.6Classification report

Fig 5.1.6 represents the Classification report of the proposed approach.

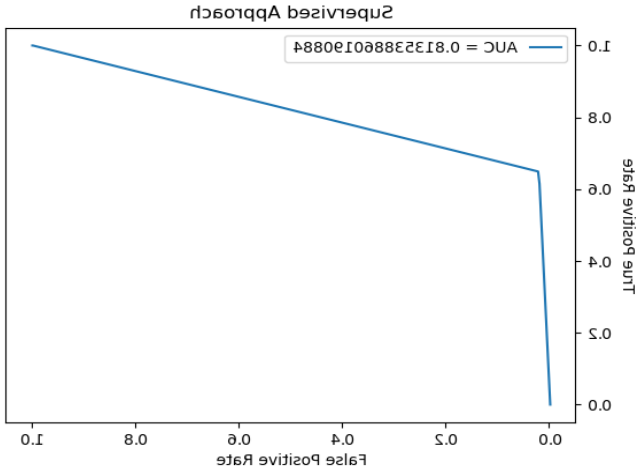

Fig.5.1.7 Graph of Supervised approach

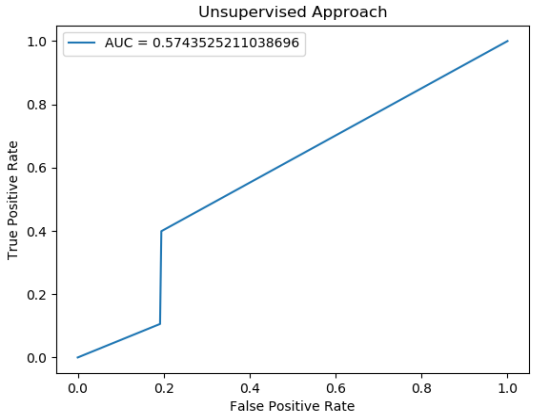

Fig5.1.8 Graph of Unsupervised approach

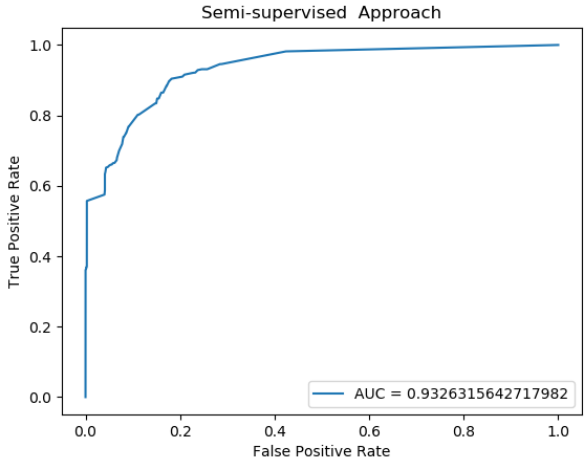

Fig.5.1.9 Graph of Semi-supervised approach

Fig 5.1.9 shows the graph with increased accuracy and decreased false positive rate of proposed approach as compared to the supervised and unsupervised approach shown in the Fig 8.1.7 and 8.1.8 respectively.

VI.CONCLUSION

The main purpose of this project is to adopt Semi-supervised ML technique for DDoS detection. The entropy estimator estimates and analyses thenetwork traffic data entropy. The co-clustering algorithm splits the network traffic data into three clusters. Then,an information gain ratio is computed based on theaverage entropy of the network header features between thecurrent dataset and each one of the obtainedclusters. The network traffic data clusters that producehigh information gain ratio are considered as anomalousand selected for pre-processing and classification using ensemble classifiers based on the Random Forest algorithm. The results, in terms of accuracy and false positive rate, are satisfactory when compared with the state-of-the-art DDoS detection methods. Despite, that the proposed approach shows good performances with the public benchmark datasets, it is important to evaluate its performances in real world scenarios. For future work, we need to perform real world deployment of the proposed approach and evaluate it against several DDoS tools.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 8, August 2020 ||

REFERENCES

[1]Bhuyan MH, Bhattacharyya DK, Kalita JK (2015) An empirical evaluation of information metrics for low-rate and high-rate ddosattack detection. Pattern RecognLett 51:1–7

[2] Akilandeswari V, Shalinie SM (2012) Probabilistic neuralnetwork based attack traffic classification. In: 2012 fourthinternational conference on advanced computing (ICoAC). IEEE, pp 1–8

[3] Saied A, Overill RE, Radzik T (2016) Detection of knownand unknown ddos attacks using artificial neural networks.Neurocomputing 172:385–393

[4] Liu T, Wang Z, Wang H, Lu K (2014) An entropy-based method for attack detection in large scale network. Int J ComputCommunControl 7(3):509–517

[5] Boro D, Bhattacharyya DK (2016) Dyprosd: a dynamic protocol specific defense for high-rate ddos flooding attacks. MicrosystTechnol 23:1–19

[6] Idhammad M, Afdel K, Belouch M (2017) Dos detection methodbased on artificial neural networks. Int J AdvComputSciAppl(ijacsa) 8(4):465–471

[7] Mustapha B, Salah EH, Mohamed I (2017) A two-stage classifierapproach using reptree algorithm for network intrusion detection.Int J AdvComputSciAppl (ijacsa) 8(6):389–394

[8] Boroujerdi AS, Ayat S (2013) A robust ensemble of neurofuzzyclassifiers for ddosattack detection. In: 2013 3rdinternational conference on computer science and networktechnology (ICCSNT). IEEE, pp 484–487

[9] Ahmed M, Mahmood AN (2015) Novel approach for networktraffic pattern analysis using clustering-based collective anomalydetection. Ann Data Sci 2(1):111–130

[10] Nicolau M, McDermott J et al (2016) A hybrid autoencoder anddensity estimation model for anomaly detection. In: Internationalconference on parallel problem solving from nature. Springer, pp717–726

[11] Jaiganesh V., Sumathi P. and MangayarkarasiS.,"An Analysis of Intrusion Detection System using Back Propagation NeuralNetwork",IEEE 2013 publication

[12] Han C., Yi Lv, Yang D., Hao Y., "An Intrusion Detection SystemBased on Neural Network",2011 International Conference onMechatronic Science, Electric Engineering and Computer, August 19-22, 2011, Jilin, China,IEEE Publication

[13] Faraj S, Al-Janabi and Saeed H, "A Neural Network Based AnomalyIntrusion Detection System",2011 Developments in E-systemsEngineering,DOI 10.1109/DeSE.2011.19,IEEE publication

[14] Mukhopadhyay I, Chakraborty M, Chakrabarti S, Chatterjee T, "BackPropagation Neural Network Approach to Intrusion DetectionSystem",2011 International Conference on Recent Trends inInformation Systems, IEEE publication

[15] https://en.wikipedia.org/wiki/Information_gain_ratio

[16] https://www.iiht.com/blog/4-reasons-why-python-is-used-for-machine-learning/

[17] https://en.wikipedia.org/wiki/Random_forest

[18] https://www.unb.ca/cic/datasets/index.html

INNO SPACE

SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details