2020 IEEE Third International Conference on Artificial Intelligence and Knowledge Engineering (AIKE) | 978-1-7281-8708-2/20/$31.00 ©2020 IEEE | DOI: 10.1109/AIKE48582.2020.00028

Evaluation of Classification algorithms for Distributed Denial of Service Attack Detection

Maulik Gohil
Electrical Engineering and Computer Science Department
Cleveland State University
Cleveland, Ohio, United States
m.r.gohil@vikes.csuohio.edu

Sathish Kumar Ph.D.
Electrical Engineering and Computer Science Department
Cleveland State University
Cleveland, Ohio, United States
s.kumar13@csuohio.edu

***Abstract*—Distributed Denial of Service (DDoS) attacks aims exhausting the target network with malicious traffic, which is a threat to the availability of the service. Many detection systems, specifically Intrusion Detection System (IDS) have been proposed throughout the last two decades as the Internet evolved, although users and organizations find it continuously challenging and defeated while dealing with DDoS. Though, IDS is the first point of defense for protecting critical networks against ever evolving issues of intrusive activities, however it should be up to date all the time to detect any anomalous behavior so that integrity, confidentiality and availability of the service can be preserved. But, the accuracy of new detection methods, techniques, algorithms heavily rely on the existence of well-designed datasets for training purposes and evaluation by creating the classifier model. In this work, experimentation has been carried out using major supervised classification algorithms to classify the DDoS attack accurately from the legitimate flows. Among all the classifier, tree-based classifiers and distance-based classifiers performed the best.**

Keywords - Machine Learning, DDoS, Logistic Regression, Naïve Bayes, SVM, Decision Tree, Random Forest, K-NN.

I. INTRODUCTION

DDoS attack have emerged as one of the most severe network intrusive behaviors and have posed serious threats to infrastructure of computer networks and various network-based services [1]. They are very prominent because it can be easily launched, and causes a catastrophic loss to the organization, moreover it is difficult to trace back and find out the true attackers. DDoS attack targets the availability of network by exhausting its resources which results in denial of the service and it has been increasing rapidly since past couple of years in terms of numbers as well as volume. The trend of shorter attack duration with bigger data volume is becoming more prevalent [6]. Most of the existing work have used dataset such as KDD Cup '99 dataset [2] or DARPA dataset [3] for detecting DDoS attacks. However, as the time passes, the cybercrimes and attacks have taken place in an artful way to intrude the target environment. So, training the classifiers using recent dataset which has all the variety of novel attack signatures, will improve the performance of classifier. We are using the CICDDoS2019 dataset for our analysis [4].

The objective of our work is to implement multiple supervised classifiers to detect DDoS attacks by training models using CICDDoS2019 dataset. Our focus is to reduce the false positives with higher accuracy that eventually helps to improve uptime of the production systems, as well as the reputation of the organization.

II. BACKGROUD AND RELATED WORK

Based on the features captured by the web server logs such as average packet size, incoming bit rate vs outgoing bit rate, Source IP vs Destination IP with their ports etc. [5] it can be detected whether network traffic is abnormal or not. Majorly there are two types of Denial of Service attack. First one is Network level DoS attack, which exhaust the network resource and hence disable the connectivity of actual users whereas another type of attack is application level DoS attack, in which server resource gets exhausted and legitimate user request gets denied. In DDoS attack, attacker gets control over multiple machines called Zombies, from where attacker runs scripts called as bot code and hit the victim server.

There are two major categories. The first one is Reflection Attacks, and another is Exploitation attacks. In Reflection attack, the identity of the attacker remains unrevealed whereas in the Exploitation attacks, this is not the case. Both Reflective attacks and Exploitation attacks, can be implemented through application protocol as well as transport layer protocol or by the combination of both. TCP-based reflective attacks include MSSQL, SSDP whereas UDP based reflective attacks include CharGen, NTP, TFTP.

Kurniabudi in [7] have analyzed relevant and significant features of huge network traffic. Ring et al., have identified 15 different properties to access the suitability of individual dataset [8]. Idhammad described semi-supervised ML approach for DDoS detection based on network Entropy estimation, Clustering, Information Gain Ratio and Trees algorithm [9]. The researchers in [10] proposed the INDB (Intrusion Detection using Naïve Bayes) mechanism to detect intrusion packet. Reason behind using naïve bayes algorithms is its predictability feature. A broad classification of IDS had been presented by Alenezi and Reed in [11]. The difficulties and characteristics of DoS/DDoS attacks had been discussed and data has been analyzed using three different classification methods. Alpna and Malhotra has developed architecture to detect the DDoS attack with the help of KNN and Random Forest [12]. Singh et al., has developed an improved SVM algorithm is used to detect the cyber-attacks [13]. There exist many related works involving DDoS attack detection. However, most of these research evaluate the dataset with a

978-1-7281-8708-2/20/$31.00 ©2020 IEEE
DOI 10.1109/AIKE48582.2020.00028

specific classification algorithm and tries to focus on optimization for better performance [14-16] using older datasets such as KDDCup'99 [2] or DARPA [3]. Here in this paper we are doing comparative analysis between six different classification algorithms using the recent dataset CICDDoS2019 [5].

III. Dataset and Methodology

The dataset has seven csv files having more than 10GB of data. We applied feature extraction algorithms to find out the most important features and performed data preprocessing techniques such as data cleaning, normalization, removal of infinity values. Once model is ready, it is accessed using test-set via measuring the accuracy, precision, recall, f1-score, true positive, and true negatives. If the accuracy is not acceptable than it has been optimized for each classification algorithms. In addition, train test spilt ratio is also analyzed.

DDoS attacks usually takes place via a botnet or multiple bots. So, there are multiple IP addresses or MAC addresses while receiving data packets at target server, but the attributes like length of packets, flow duration, total packets in forward direction, that lead us recognized it as genuine request or malicious one. To compare data packets, data mining technology can be applied to measure the probability or the occurrences to classify data packets. Here, we are doing classification of abnormal traffic using following six machine learning algorithms: Logistic Regression, Support Vector Machine, Naïve Bayes, K-Nearest Neighbor, Decision Tree and Random forest.

For our experimentations, we used dataset with 88 features created by University of New Brunswick. The dataset is publicly available on the Canadian Institute of Cyber security website [5]. The data has been collected for different types of attacks such as Portmap, LDAP, MSSQL, UDP, UDPLag etc. If request is from a legitimate user then it is marked 'Benign', else marked as specific attack name. The dataset has been explicitly created for the analysis purpose and it has been organized per day. For each day, CIC has recorded the raw data including network traffic and event logs from each server machine. Actual dataset had more than 88 features but CIC itself have done dimensionality reduction for which they have used CICFlowmeter-V3 [17] and generated most important 88 features for the analysis and provided csv files. They have also shared PCAP files if someone wants to extract feature by their own.

We have done two types of experiments on the dataset. Initially we sampled the dataset, choosing randomly 30,000 rows from each csv file which adds up to 200,000 rows for our data analysis sample, that is our unbalanced dataset, where for second experiments we derived same amount of benign vs. attack data tuples from each csv files dataset, resulting a fully balanced training and test dataset.

Table 1 shows total number of records each file contains in total vs normal class e.g. Label = 'BENIGN'. More details about dataset can be found at [18]. IP addresses in the dataset were converted to numeric integers before training the model.

CSV File Name	Total Rows	Benign Rows
LDAP	2113234	5124
MSSQL	5775786	2794
NetBIOS	3455899	1321
Syn	4320541	35790
UDP	3782206	3134
UDPLag	725165	4068
Portmap	191694	4734
Total	**20364525**	**56965**

Table 1. Distribution of labeled data

We chose univariate selection technique. It is a statistical test that can be used to select those features that have the strongest relationship with the output label. The scikit-learn library provides the SelectKBest class that helps us to implement the algorithm and gives the result of most correlated features with our class label. We have used top 25 features for training our model. To obtain the importance of each feature of dataset, we used Feature Importance inbuild class that comes with Tree based Classifiers. Figure 1 explains top 15 most important features.

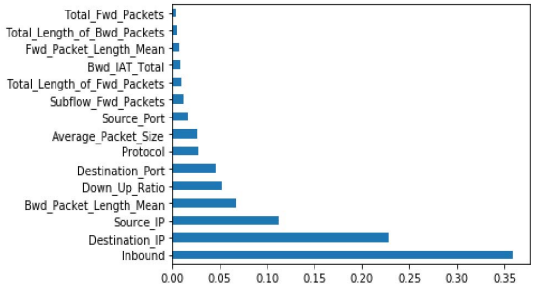

Fig. 1 Variable Importance

IV. Experimental Results and Discussion

A. *Evaluation metrics*

To evaluate the performance of the classifiers, we have used primary performance indicators based on confusion matrix. This matrix contains information about real and predicted classifications which has been carried out by the ML models. To be on fair side, we have also included TP, TN, FP, and FN values in the result table. As mentioned in the previous section, we implemented six different Machine Learning classification algorithm on unbalanced data set as well as on balanced dataset. We have implemented both techniques in python using scikit-learn library.

B. *Experiments*

We did random sampling on each of the individual 7 csv data files choosing 30K, 40K and 50K tuples from each of the

						macro avg		
Unbalanced Dataset	**TP**	**TN**	**FN**	**FP**	**Accuracy**	**Precession**	**Recall**	**F1 Score**
Decision Tree	62599	398	3	0	99.99523	1	1	1
Naive Bayes	61199	370	31	1400	97.72857	0.6	0.95	0.66
Logistic Regression	62619	213	164	4	99.73333	0.99	0.78	0.86
Support Vector Machine	62663	0	337	0	99.46507	0.5	0.5	0.5
K Nearest Neighbor	62598	401	0	1	99.99841	1	1	1
Random Forest	62602	397	0	1	99.99841	1	1	1

Table 3. Results of unbalanced dataset

						macro avg		
Balanced Dataset	**TP**	**TN**	**FN**	**FP**	**Accuracy**	**Precession**	**Recall**	**F1 Score**
Decision Tree	31577	31449	0	0	100	1	1	1
Naive Bayes	31387	29278	2290	71	96.25392	0.96	0.96	0.96
Logistic Regression	31276	8730	12819	201	79.34185	0.85	0.79	0.78
Support Vector Machine	31577	0	31449	0	50.10154	0.25	0.5	0.33
K Nearest Neighbor	31477	31549	0	0	100	1	1	1
Random Forest	31477	31549	0	0	100	1	1	1

Table 4. Results of balanced dataset

file just to measure the ratio of benign traffic to attack traffic. The actual dataset has a smaller number of benign traffic, while it is sampled, that itself is biased. On an average there is 0.5% to 0.7% of the benign traffic compared to Attack label when model was trained using unbalanced data. Table 2 shows class distribution.

Sample	**Attack (1)**	**Benign (0)**
30K	208710	1263
40K	278302	1698
50K	347780	2220

Table 2. Distribution of Class Label when dataset randomly chosen

To avoid bias issues on the accuracy of the classification model, we also created balanced dataset, where we chose all the benign traffic from each of the 7-csv files and the same amount of tuples were randomly sampled from attack traffic. We ended up gathering 105042 rows from all files with equal amount of attack and benign data. As this was very small number, we appended the same data another time in the existing data frame to increase the size of training set beyond 200K rows, which is comparable with the unbalanced data set.

C. Results

Each classifier has been evaluated and assessed using the Accuracy score and other evaluation metrics such as Precision, Recall and f1-score. The overall accuracy for each of the classification algorithm is shown in Table 3 for unbalanced dataset and Table 4, shows output results for the balanced dataset. The data is chosen based on best values from five rounds of observations taken.

As unbalanced dataset is biased towards attack class, the accuracy of all the classification algorithms are extremely high. But that does not help us to make decision for choosing the best performing algorithm for DDoS attack detection. Here all the algorithm except Naïve Bayes performs extremely well for unbalanced data. On the contrary, we noticed little variation in accuracy for balanced dataset. As seen in the Table 4, tree-based algorithms like Decision Tree, Random Forest, and the distance-based classification algorithm K-NN performs the best, whereas Naïve bayes gives good accuracy but the rest of the classification techniques - SVM and Logistic Regression performs poor. Figure 2. shows the Accuracy score comparison between Unbalanced dataset and balanced one for each of the classification algorithm. Moreover Figures 3, 4 and 5 shows the comparison for Precision, Recall and F-1 score between unbalanced and balanced dataset, respectively.

After analyzing the outputs, tree-based classification algorithms like Decision tree & Random forest, and distanced based classification algorithm performed best on both type of datasets and gives almost 100% accuracy. Even when other metrics are considered, these three classifiers performs the best. However, a little performance variation can be noticed when the parameter for each classifier gets changed. Here we tried to come up with best performance for each of the algorithms.

V. FUTURE WORK RECOMMENDATIONS

While our preliminary experimental results are promising, this work can be extended in multiple directions: a) In our experiments, we used just a little more than 200,000 rows, due to hardware limitations. In the future, we can plan to choose dataset with more than 1 million rows. That will give us much better accurate trained model for prediction. b) We can do data mining based on each different type of DDoS attack because it might be possible that Portmap can be detected with good efficiency by K-NN, but for UDPlag, Naïve Bayes could be better. If that is proved, then we can merge all separate models together in a single model to get accuracy nearest to 100% for all types of DDoS Attack. c) We can try different feature selection techniques.

VI. CONCLUSION

In this paper, we have used CICDDoS2019 dataset which is fairly a recent dataset that includes most recent attack signatures for DDoS. The experimentation has been carried out using major supervised classification algorithms to classify

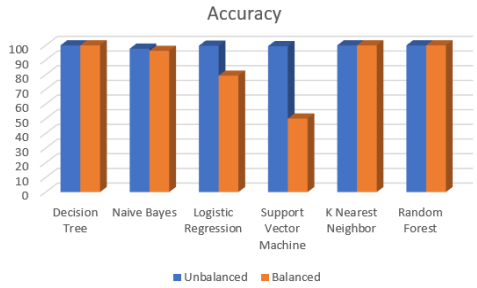

Fig 2. Accuracy scores for Classification Algorithms

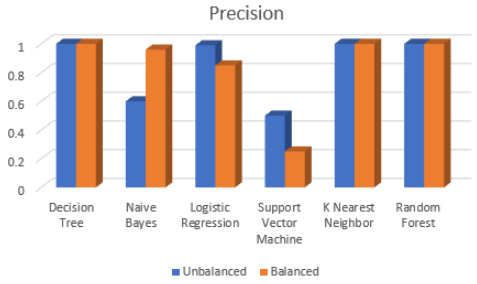

Fig 3. Precision scores for Classification Algorithms

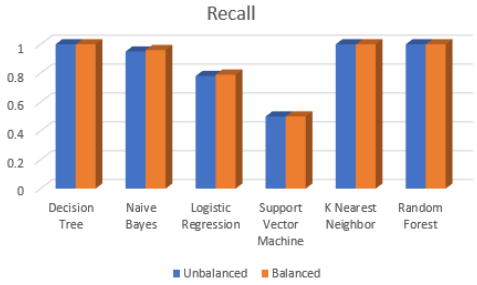

Fig 4. Recall scores for Classification Algorithms

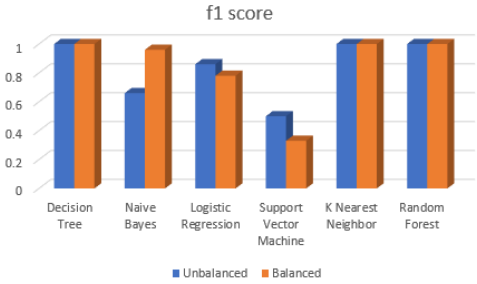

Fig 5. F1-score for Classification Algorithms

the attack accurately from the legitimate flows. When the results are compared with other algorithms among all classifiers, decision tree, random forest & K-NN performed the best. While the preliminary results are promising, we plan to extend the work with expanded dataset and targeting different types of DDoS attacks. We will focus our future work in these directions.

REFERENCES

[1] Neustar. (2014). 2014 - Neustar Annual DDoS Attacks and Impact Report [Online]. Available: http://neustar.biz/resources/whitepapers/ddos-protection/2014-annual-ddos-attacks-andimpact-report.pdf

[2] KDDCUP'99 - http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

[3] DARPA Dataset [Online]. Available: https://www.ll.mit.edu/r-d/datasets

[4] I. Sharafaldin, A.Habibi L.Saqib Hakak, and A. Ghorbani, "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy", IEEE 53rd International Carnahan Conference on Security Technology, Chennai, India, 2019.

[5] CICDDoS2019 - https://www.unb.ca/cic/datasets/ddos-2019.html Last accessed August 2020.

[6] L Buczak, and E.Guven. "A survey of data mining and machine learning methods for cyber security intrusion detection." IEEE Communications surveys & tutorials 18, no. 2 (2015): 1153-1176.

[7] Kurniabudi, D. Stiawan, Darmawijoyo, M. Y. Bin Idris, A. M. Bamhdi and R. Budiarto, "CICIDS-2017 Dataset Feature Analysis With Information Gain for Anomaly Detection," in *IEEE Access*, vol. 8, pp. 132911-132921, 2020, doi: 10.1109/ACCESS.2020.3009843.

[8] M. Ring, S. Wunderlich, D. Scheuring, D. Landes, and A. Hotho. "A survey of network-based intrusion detection data sets." Computers & Security 86 (2019):147-167.

[9] M. Idhammad, K. Afdel, and M. Belouch. "Semi-supervised machine learning approach for DDoS detection." Applied Intelligence 48, no. 10 (2018): 3193-3208.

[10] V. Hema and C. E. Shin. "DoS Attack Detection Based on Naive Bayes Classifier." Middle-East Journal of Scientific Research 23 (2015): 398-405.

[11] M. Alenezi and M. J. Reed, "Methodologies for detecting dos/ddos attacks against network servers," in 7th Intl Conference on Systems and Networks Communications, ICSNC SemiMarkov models, 2012.

[12] Alpna and S. Malhotra, "DDoS Attack Detection and Prevention Using Ensemble Classifier (RF)", IJARCSSE, 2016.

[13] S. Singh, S. Agrawal, M. A. Rizvi, and R.S. Thakur. "Improved Support Vector Machine for Cyber Attack Detection." In Proceedings of the World Congress on Engineering and Computer Science, vol. 1. 2011.

[14] Wankhede, S., & Kshirsagar, D. (2018). DoS Attack Detection Using Machine Learning and Neural Network. 2018 Fourth International Conference on Computing Communication Control and Automation.

[15] Shuyuan Jin and D. S. Yeung, "A covariance analysis model for DDoS attack detection," 2004 IEEE International Conference on Communications (IEEE Cat. No.04CH37577), Paris, France, 2004, pp. 1882-1886 Vol.4, doi: 10.1109/ICC.2004.1312847.

[16] P. Khuphiran, et al.,. (2018). Performance Comparison of Machine Learning Models for DDoS Attacks Detection. 2018 22nd International Computer Science and Engineering Conference

[17] CICFlowMeter-v3 codebase can be accessed using this link - https://github.com/ahlashkari/CICFlowMeter

[18] Iman Sharafaldin, Arash Habibi Lashkari, Saqib Hakak, and Ali A. Ghorbani, "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy", IEEE 53rd International Carnahan Conference on Security Technology, Chennai, India, 2019.

[19] S. Kumar and B. Xu. "A Machine Learning Based Approach to Detect Malicious Fast Flux Networks." In 2018 IEEE Symposium Series on Comp. Intelligence, pp. 1676-1683.

[20] J. Chelladhurai, P. Chelliah, and S. Kumar. "Securing docker containers from denial of service (dos) attacks."2016 IEEE Intl Conference on Services Computing (SCC), pp. 856-859.

[21] C. Chrane and S. Kumar. "An Examination of Tor Technology Based Anonymous Internet." In I n SITE 2015: Informing Science+ IT Education Conferences: USA, pp. 145-153. 2015.

[22] S. Srinivasan, S, and S. P. Alampalayam. "Intrusion Detection Algorithm for MANET." International Journal of Information Security and Privacy (IJISP) 5, no. 3 (2011): 36-49.

[23] S. Kumar, "Classification and review of security schemes in mobile computing." Wireless Sensor Network 2, no. 06 (2010): 41

[24] S. Alampalayam, and A. Kumar. "Predictive security model using data mining." In IEEE GLOBECOM'04, vol. 4, pp. 2208-2212.

[25] S. Alampalayam, and A. Kumar. "An adaptive and predictive security model for mobile ad hoc networks." Wireless Personal Communications 29, no. 3-4 (2004): 263-281.