Applying Machine Learning for Recognition of DDoS Attacks using NSL- KDD

OPEN ACCESS

Volume: 12

Special Issue: 1

Month: June

Year: 2025

P-ISSN: 2321-788X

E-ISSN: 2582-0397

Citation:
Rajeev, Haritha. "Applying Machine Learning for Recognition of DDoS Attacks Using NSL-KDD." *Shanlax International Journal of Arts, Science and Humanities*, vol. 12, no. S1, 2025, pp. 101–08.

DOI:
https://doi.org/10.34293/sijash.v12iS1-June.9124

Dr. Haritha Rajeev
Assistant Professor, Department of BCA
Bharata Mata College (Autonomous), Thrikkakara, Edappally, Kochi, Kerala

Abstract
DDoS (Distributed Denial of Service) attacks are significantly dangerous. Spotting them is very essential for system availability and performance. DDoS detection is noticing a growing attempt in network traffic and reducing its effects. To identify or detect DDoS attacks, many methods have been developed including Statistical analysis, Machine learning and anomaly detection. To distinguish between legitimate and malicious data the features rely on packet rates, flow patterns and network behavior. The fineness of the DDoS detection depends on the classification methods and the accuracy of the classification algorithm. Attackers continue to create new strategies to avoid detection in DDoS. Therefore, it is very necessary to increase the accuracy and effectiveness of DDoS detection algorithms.
Keywords: K-Nearest Neighbor, Logistic Regression, Random Forest

1. Introduction

DDoS attacks are considered as dangerous as it attempts to overload a targeted system or network with a flood of traffic from several sources to disrupt the service. When the attempt is launched from several devices, it is difficult to stop because it will be widely spread across the device. The hackers can demand money from the users or larger industries in order to end the attack. Larger companies have been shut down due to the DDoS attacks, and even many nations have used these attacks as a tactics in cyber warfare. The attackers mainly use Bots that can be infected with the virus and allows the attackers to take complete control of the system. The bots or Botnets includes computers, IoT devices, mobile phones etc. The user may not be aware that their system had been compromised. The users may not be able to access to the devices they have been using, services such as emails, websites and banking and all other services will not be able to function properly. The flood of traffic will make the system totally unresponsive until the target responds to the attacker's demand.

Most important step to get rid of DDoS attack is to strengthen the security level of all the internet connected devices. Then install an antivirus software, also enable the firewall and configure it to restrict incoming traffic coming into the system. Ensure that the system is performing as usual. We need to make sure that difficulties caused by DDoS attack is crucial or not. A model for DDoS attack is proposed.

Several algorithms are been used in this. The algorithms will be trained and tested using dataset as well as they will be compared with to check the accuracy.

2. Related Work

DDoS have been a cause for financial losses and security. In this article a study has been conducted for detecting various methods and in different platforms. Three primary sections of the work include review of targeted attack on SDN platforms, statistical based platforms, machine-learning based detection.[1]. DDoS attacks can be considered as an oldest and dangerous attack. They tend to perform mass disruption and pose cybersecurity risk to all kinds of business. IDC predicted that attacks will be increased up to 18% in 2023, to improve detection prediction, we need to utilize the correlations between missing packets. In order for that we need to guarantee that these correlations are computed accurately.[2]. This article explains about DDoS attacks using SDN concept. For that we need to gather table entries to deploy flow collector module. DNN model is also being used for detecting the attacks. The DNN model is been preprocessed using trained data, and then the prediction is being made. DNN models are good in detecting errors as well as accurate than machine learning methods, which also sets the foundation for DDoS attack's defense mechanism.[3]. More network attacks are been increasingly day by day the expansion of IoT devices are developed. DoS and DDoS attacks are considered to be more intense and frequent. During the recent times deep model learning models achieve high significance due to their exceptional performance in the field of image processing. CNN models help in an effective manner, as their capability is being utilized in DoS and DDoS attacks. By using binary classification, we got almost 99% accuracy at an average precision of 87%.[4]. In the recent times cloud computing era has been emerged as one of the most crucial infrastructures. DDoS attack is one of the main important issues when it comes to data security. DDoS attack use TCP traffic which can be hard to spot. We also provide real time TCP based

DDoS detection method that extracts useful features from TCP data and uses two decision tree classifier to separate malicious traffic from legitimate traffics.[5]. This article introduces to SDN (Software Defined Network) as it is the network paradigm of the future. SDN is very sensitive to DDoS attacks because it controls control plane from data plane. There are mainly two approaches used here. The first phase id clustering and classification approach and the next is detecting validation method in SDN using Mininet emulator.[6]. Network vulnerabilities or attacks are common in our daily life, the vulnerabilities on networks are also on the rise. Several measurements have been taken in-order to prevent attacks. Majority of DoS/DDoS defense systems produce high volumes of false alarms which creates people to mistrust them. It is essential to identify right alerts to determine attack techniques used during launch of attacks, it is necessary to study them, alert correlation is a process for determining multi-step attacks such as DoS/DDoS attacks. Effectiveness of this method is evaluated on DARPA 2000 datasets.[7]. It has been proved that strengthening the foundation of cyber protection is very important. In fact, to identify a DDoS attack can be found using spline functions. The spline extrapolation technique makes it possible to predict DDoS cyberattacks with accuracy.[8]. The two-stage DDoS attack detection algorithm combined with machine learning is proposed in this research. By starting with a time series-based multidimensional sketch and employing CNN attack detection findings. Using RNN flow data taken from the sketch, we build flow-level DDoS attack detection for drawings that incorporate portable DDoS attacks in the second stage[9]. As the DDoS attack has been considered as one of the most expensive attacks for corporate companies. These attacks are more frequent and are intense as they disturb the victim, causing a considerable financial loss. There is new method

for detecting DDoS attacks by analyzing traffics arriving to the server from BOTNET that uses machine learning algorithms. The DDoS attack is examined using simulation's findings.[10].

3. Data Collection and Pre-processing

The dataset called NSL-KDD is used in this, it is basically a network intrusion detection dataset and it contains more data and realistic network attacks, with larger records and more training and test sets. A collection of pre-processed network traffic data features, including source and destination IP addresses, protocol types, port numbers, and labels indicating if a network connection is normal, are included in the NSL-KDD dataset. The dataset is taken from Kaggle repository. There are 22543 rows in the dataset and 43 columns.

3.1Data Pre-processing

Data pre-processing in NSL-KDD Dataset is an important step as it deals with a huge amount of data. It is very important to note that missing values, removing duplicates and all can affect the entire data. So, margin of error should be avoided. There are several steps to be ensured and to be taken care to pre-process NSL-KDD dataset:

1. Remove Duplicates - Removing duplicate values is so important as it creates duplicate values. The duplicate values can be identified by comparing all the attributes in the record. They can be harmful as they produce results irrelevant in the models.
2. Remove Irrelevant Records - NSL-KDD dataset contains record contains data for both normal network and traffic. Some data might be irrelevant as it contains attacks that have no relevance at all. Removing such data can reduce the size and complexity of the dataset and it will simplify the analysis.
3. Remove Missing Values – If any missing values are found, they must be handled appropriately.
4. Normalize Dataset – Normalizing the dataset means to convert them to a common scale and it can improve the performance of the models. Techniques such as min-max scaling or z-score normalization can be used.
5. Imbalance Correction – NSL-KDD dataset is heavily imbalanced towards attack. Sampling method can be used to solve this problem.

The above mentioned are the main pre-processing steps in the NSL-KDD dataset. As it can be applicable for all the other cases also. Label Encoding is a pre-processing technique in which it uses categorical or nominal values into numerical data. Label Encoding is a simple and efficient way to handle categorical data and is commonly used in data science and machine learning. Label Encoding works by assigning a unique number label to each category in a categorical feature. The next step is Train-Test split, in that we use 0.3 percent of data the dataset is divided into a training set and a testing set using the train_test_split function. This indicates that 30% of the data will be utilised for testing and 70% for training. Then, using the fit technique to train the model on the training set, we build an instance of the logistic regression model. Finally, using the predict method to predict the target variable on the testing set, we assess the model's performance. A crucial pre-processing method in machine learning, train-test splitting aids in assessing the model's performance on untried data. However, in order to create a machine learning model that is reliable and accurate, it is crucial to use Train-Test Split sparingly and in conjunction with other pre-processing methods. Next step is Cross validation, The input characteristics and the target variable are divided after loading the iris dataset. The evaluation metric (accuracy) is then defined and a logistic regression model instance is created. To calculate the accuracy score and carry out 5-fold cross-validation on the logistic regression model, we utilise the cross_val_ score function. Finally, we output the accuracy's mean score and standard deviation. In machine

learning, the cross_val_score function is a helpful pre-processing method for assessing the model's performance on a small dataset. However, in order to create a machine learning model that is reliable and accurate, cross-validation must be used carefully and in conjunction with other pre-processing methods. Next step is mean absolute error, in that the input characteristics and the target variable are separated when we load the Boston housing dataset. The linear regression model is then created, fitted to the data, and trained before being used to forecast the target variable. The mean_absolute_error function is then used to determine the mean absolute error between the predicted and actual numbers, and the outcome is reported. The mean_absolute_error function is a useful pre-processing technique for evaluating the performance of regression models. To create a reliable and accurate machine learning model, it should be combined with additional assessment metrics and pre-processing methods. The last pre-processing step is accuracy score, in that the characteristics of the input and the target variable are divided after loading the iris dataset. Using the train_test_split function, we divided the dataset into training and testing sets, created a random forest classifier model instance, fitted the model to the training data, then predicted the classes of the testing data using the trained model. We next use the accuracy_score function to compute the accuracy score between the predicted and actual classes and display the result. An effective pre-processing method for assessing the effectiveness of classification models is the accuracy_score function. To create a reliable and accurate machine learning model, it should be combined with additional assessment metrics and pre-processing methods.

4. Methodology

The Algorithms used here are Random Forest, Logistic Regression, K-Nearest Neighbor.

Then split data into testing and training. For training purpose 70% of data is used and for testing 30% of data is used. NSL-KDD is the dataset that will be used, it helps to compare between different intrusion detection methods. For collecting analytical information on the predictions provided by a model, a helper function is used. 'data_set', 'predictions', and 'y' are the three arguments required by the function. Predictions is a list or array of the predicted values, data set is a Pandas Data Frame holding the input characteristics required to construct predictions, and y is a Pandas Series having the actual target variable values. The function initially generates a Pandas Series of anticipated values with the same index as the 'y' Series. The 'data_set', predictions', and 'y' Series are then combined into a single DataFrame referred to as 'predicted_vs_actual'. The predicted and actual class distributions are summarised in this matrix, which may also be used to determine assessment measures like accuracy. By comparing the projected and actual values, the function then collects rows with incorrect predictions and stores them to a new DataFrame named "base_errors."

The 'actual' and 'predicted' columns are examined by the function to determine the type of mistake. False positives are saved in a DataFrame named "false_positives," false negatives are saved in "false_negatives," and the entire collection is saved in an object called "prediction_data." This function is helpful for gaining insights into a classification model's performance and identifying the sorts of errors the model makes. It is a post-processing phase that aids in model analysis and assessment rather than a pre-processing step.

4.1 Applying Machine Learning Algorithms

Random Forests

Random Forest comes under ensemble techniques. This can be considered as the most sophisticated and adaptable method and is frequently used for regression and classification. A number of decision trees are built by the algorithm using randomly chosen samples from the

training set of features and data. Each tree is constructed using a random selection of features, and the best feature and split point are used to divide the data in a way that maximizes information gain. The combination of all the individual decision trees' predictions is what the random forest algorithm produces as its output. The majority vote of the different trees' forecasts is used to determine the final prediction.

Random forest algorithm is known for its high accuracy and robustness to noise and overfitting. It is widely used in various fields for prediction purposes, that is finance, medical, image processing. Due to its ability to handle high-dimensional data and non-linear, it can be considered as a choice for problems that involves complex datasets.

Logistic Regression

The supervised machine learning algorithm of choice for classification tasks is logistic regression. Using a logical function that converts input data into a range of values between 0 and 1, it calculates the likelihood of an event depending on input features. Based on the threshold value, this function converts any input value to a probability between 0 and 1, which may then be used to categorise the events as positive or negative. For jobs requiring binary classification, logistic regression is popular and effective. It has applications in a number of industries, including marketing, finance, and healthcare.

K-Nearest Neighbor

A popular machine learning technique that may is been used for classification and regression problems in K-Nearest Neighbor's (KNN). Being non-parametric, it makes no assumptions regarding the distribution of the data. The k-nearest neighbor's to a particular data point in the feature space are determined by the method. A distance metric, such as the Euclidean or Manhattan distance, is used to determine the separation between the data points. The data point is then given the class label of the k-nearest neighbor's to establish its class label. KNN is a simple-to-use method that is frequently applied in anomaly detection, picture classification, and recommendation systems. KNN, however, can be computationally costly, particularly when dealing with data that has a high degree of dimension.

In the figures given below, Figure 1 and Figure 2 are two pie charts that displays the distribution of values in the dataset for normal traffic and attack traffic. The flag in time of attack shows the status of the TCP connection. In this each wedge corresponds to the proportion of connections that has flag values. Legend on the side of chart shows which color corresponds to which flag value. They both are separated by two data frames, we can clearly see the difference between them.

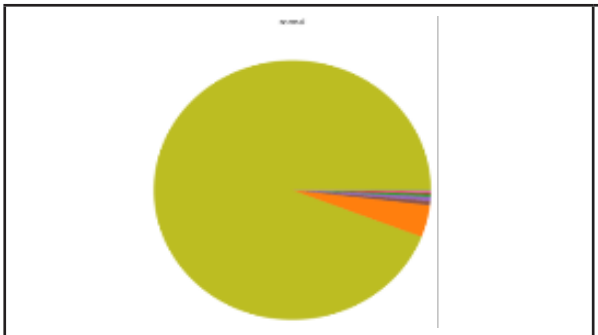

Figure 1 Normal Traffic

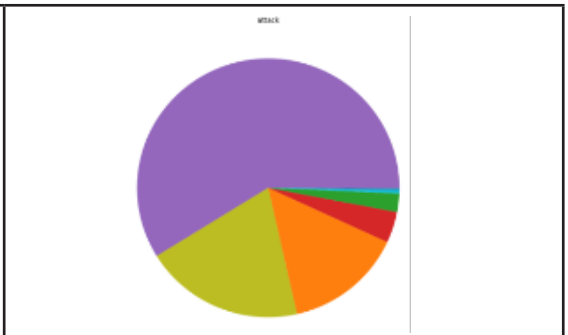

Figure 2 Attack Traffic

5. Experimental Results and Discussions

For predicting DDoS detection, we used random forest, logistic regression and KNN algorithm. The ratio used for testing and training the data is 70:30. The results of the algorithms are as follows. Random forest with an accuracy of 99.27, Logistic regression with an accuracy of 82.24 and KNN with an accuracy of 99.00. Out of these 3 algorithms Random Forest has the most accuracy compared to other algorithms. The different model's overall performances and accuracy variations can be visualized by creating a boxplot. Figure 3 represents the boxplot of different models used in this study. A confusion Matrix is used to visualize the summary of the model's performance in predicting classes and highlighting patterns or discrepancies in the prediction, this is represented in Figure 4.

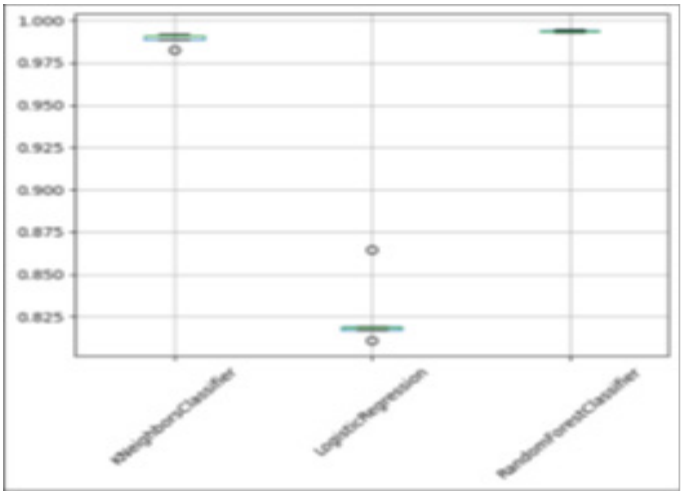

Figure 3 Boxplot of Different Algorithms

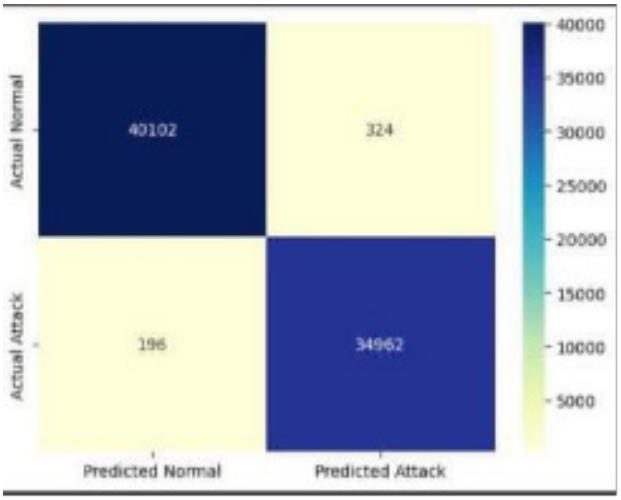

Figure 4 Confusion Matrix

6. Conclusion

Distributed Denial of Service (DDoS) attacks has always been dangerous to many services. The development of effective DDoS attack detection techniques has become a critical research area in the cybersecurity field. An approach is to propose a machine learning algorithm or framework that can accurately detect DDoS attacks without relying on traditional signature- based approaches. A solution is to use supervised learning techniques, such as clustering or anomaly detection, to identify abnormal traffic patterns that may be indicative of a DDoS attack. By training the algorithm on normal traffic data, it can learn to identify deviations from expected behavior, thereby alerting security teams to potential attacks.

Another approach could be to use deep learning techniques, such as (CNNs) or (RNNs), to analyze network traffic and identify patterns that are consistent with DDoS attacks. Furthermore, it may be possible to combine multiple detection techniques, such as using both unsupervised learning and deep learning, to improve accuracy and reliability of DDoS attack detection. This hybrid approach could potentially leverage the strengths of each technique while minimizing their weaknesses.

In conclusion, detecting DDoS attacks is an essential aspect of cybersecurity, and the development of effective techniques remains a critical research area. Approaching the topic from a unique perspective, such as proposing a machine learning algorithm or framework. By leveraging supervised learning, deep learning, or a combination of both, it may be possible to accurately detect DDoS attacks and mitigate their impact on online systems and services.

References

1. J. Chen, L. Yang and Z. Qiu, "Survey of DDoS Attack Detection Technology for Traceability," 2022 IEEE 4th Eurasia Conference on IOT, Communication and Engineering (ECICE), Yunlin, Taiwan, 2022, pp. 112-115.
2. R. S. Pavan Kumar, K. G. Chand, M. V. Krishna, B. G. Nithin, A. Roshini and K. Swetha, "Enhanced DDOS Attack Detection Algorithm to Increase Network Lifetime in Cloud Environment," 2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2022, pp. 1783-1787.
3. W. Zhao, H. Sun and D. Zhang, "Research on DDoS Attack Detection Method Based on Deep Neural Network Model inSDN," 2022 International Conference on Networking and Network Applications (NaNA), Urumqi, China, 2022, pp. 184-188.
4. F. Hussain, S. G. Abbas, M. Husnain, U. U. Fayyaz, F. Shahzad and G. A. Shah, "IoT DoS and DDoS Attack Detection using ResNet," 2020 IEEE 23rd International Multitopic Conference (INMIC), Bahawalpur, Pakistan, 2020, pp. 1-6.
5. J. Jiao et al., "Detecting TCP-Based DDoS Attacks in Baidu Cloud Computing Data Centers," 2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS), Hong Kong, China, 2017, pp. 256-258.
6. D. Firdaus, R. Munadi and Y. Purwanto, "DDoS Attack Detection in Software Defined Network using Ensemble K-means++ and Random Forest," 2020 3rd International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), Yogyakarta, Indonesia, 2020, pp. 164-169.
7. N. Hoque, D. K. Bhattacharyya and J. K. Kalita, "An alert analysis approach to DDoS attack detection," 2016 International Conference on Accessibility to Digital World (ICADW), Guwahati, India, 2016, pp. 33-38.
8. S. Kivalov and I. Strelkovskaya, "Detection and prediction of DDoS cyber-attacks using spline functions," 2022 IEEE 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Lviv- Slavske, Ukraine, 2022, pp. 710-713.

9. Y. Sun, Y. Han, Y. Zhang, M. Chen, S. Yu and Y. Xu, "DDoS Attack Detection Combining Time Series-based Multi-dimensional Sketch and Machine Learning," 2022 23rd Asia-Pacific Network Operations and Management Symposium (APNOMS), Takamatsu, Japan, 2022, pp. 01-06.
10. D. Satyanarayana and A. S. Alasmi, "Detection and Mitigation of DDOS based Attacks using Machine Learning Algorithm," 2022 International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates, 2022, pp. 1-5.