DDOS Attacks Detection using Supervised Learning Methods - An Evaluation of different Machine Learning Algorithms

G. Dayanandam
Research Scholar
ANUCET
ANU, Guntur, AP, India

E. Srinivasa Reddy, PhD
Professor
ANUCET
ANU, Guntur, AP, India

D. Bujji Babu, PhD
Professor
QISCET
Ongole, AP, India

ABSTRACT
Nowadays, there is exponential growth rate in number of users connected to the internet. Due to this, it is possibility to generate huge network traffic. If there is increased in network traffic, then there is a chance of increasing in network attacks. Distributed Denial of Service (DDoS) attack is one of such network attacks which deny the legitimate access to the server. The server is flooded with huge number of requests beyond the server capacity.

Therefore the detection of such attacks is very tedious task. Machine learning algorithms will help to detect such type of attacks effectively as compared to the statistical based detection methods.

In this paper, the researcher calculated Nearby Zero Variance (NZV) variables and eliminated them from the original dataset. It will help the model to detect the attacks with more accuracy. Then the researcher applied PCV method to preprocess the data and traincontrol () function is used to fine tune the variables. The researcher applied four supervised machine learning algorithms i.e., SVM, Decision Tree with C4.5, Naïve Bayes and Neural Networks to evaluate the model. All models performed very well as compared to other existing machine learning algorithms with the average accuracy of above 99%. Out of four supervised machine learning algorithms, decision tree with C4.5 got the average accuracy of 0.997.

Keywords
DDoS attacks, Caret Package, Nearby Zero (NZV) variance, KDD'99 Dataset, PCA, SVM, C4.5, Naïve Bayes, Neural Networks and Supervised machine learning algorithms.

1. INTRODUCTION
Nowadays, all organizations are focusing on cost saving and more flexibility. Cloud technologies [1] are the best choice for cost saving and more convenient. With less infrastructure required and delivery of more services or applications can be done by using cloud technologies. The cloud technology is more benefit to all customers due to resource sharing and fault tolerance. So, customers no need to spend heavily on any softwares, infrastructure and any platform. All these services are provided by cloud technologies.

Infrastructure as a Service (IAAS) is a service provided by the cloud, which is similar to build new house. If anybody want to build new house, need plan, raw material, workers etc… then you can construct new house as per the customer requirements, which liked by everyone. Establishing new Laboratory with high end servers and LAN capabilities are comes under this IAAS.

Cloud technology's another service is Platform as a Service (PAAS), which is similar to purchasing already built house. Here, there is no need of plan, raw material and workers but that house structure may not as good as built new house. But it reduces the overheads of workers and cost. Installation of Softwares such as Server Software, Network Software and Operating System Software are comes under PAAS.

Software as a Service (SAAS) is another service provided by the cloud which is similar to staying in hotel room as pay per use policy. i.e. the customer can pay the rent for the number of days spent in the hotel room. It has advantage of no burdens of built the new house, but the customer cannot get permanent house. So most of the cloud technologies comes under this category i.e. Software as a Service (SAAS). Because, there is no need to build the new house, purchase already built house, but the customers can stay in the hotel room by paying as per stay. Accessing softwares and Services by paying according to usage are the examples of SAAS.

When services provided by the cloud are heavily depend upon the internet, so there is a possibility of cyber-attacks. Hackers are try to focus on weakness of services provided by the cloud and try to take control of the authorized data. During this situation, there is a chance of Distributed Denial of Service (DDoS) attacks. DDoS attack is one form of the Denial of Service (DoS) attack.

DoS attack [2] is one of the cyber-attacks, where one attacker attacked one server. The attacker disrupt the services of the server so that authorized users cannot access their services.

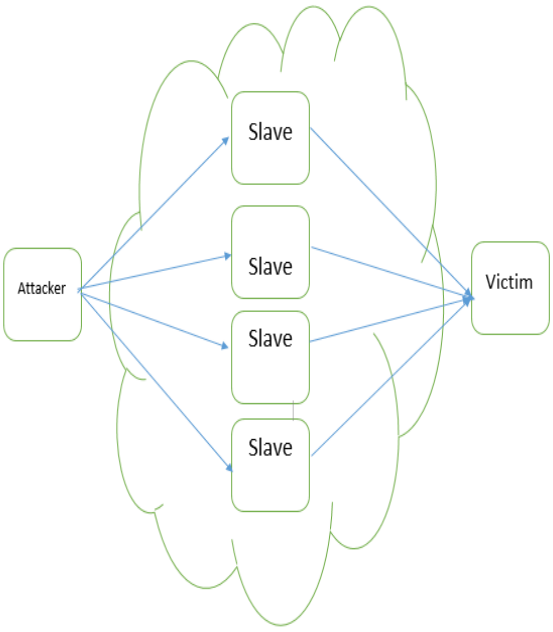

Fig.1 DoS attack

DDoS attack [3] is advancement of DoS attack. In DDoS attacks, the attacker try to take the control of other weak systems in the network, and make them as BOTs and attack the targeted server with the help of BOTs. This network of BOTs is called BOTNET. In this attack, there is possibility of more attacks on one server. It comes under many to one attack whereas DoS treated as one-to-one attack.

Fig.2 DDoS attack

The main aim of DDoS attacks is to take the revenge on particular organization, to damage the reputation of an organization or to perform financial loss to that organization.

Such type of DDoS attacks can be solved in three ways. The researcher can prevent the DDoS attacks before happening (or) the researcher can isolate the network by detecting DDoS attacks (or) need to recover the data and take backup once the attack happened.

Detection of DDoS attacks can be done by using machine learning algorithms.

Artificial Intelligence plays a big role for finding solutions of real world problems.

Machine learning is a past of Artificial Intelligence.

There are 3 types of machine learning algorithms[3]. They are

1. Supervised learning
2. Unsupervised learning
3. Reinforcement learning

1.1. Supervised Learning

This learning is suitable for structured data. Labeled data is used in this supervised learning. Some times labeling is also called a categorizing.

1.2.Unsupervised Learning

This learning is suitable for unstructured data. Unlabeled data is used by this unsupervised learning. In this model, the data is divided into clusters based on their similarities.

1.3.Reinforcement learning

If data is not labeled (or) unlabeled, then this type of learning is suitable. Instead machine tries different actions and will give us signal if that action is correct.

Our focus is on supervised learning, where our data is structured data.

Supervised learning is divided into two types.

1. Classification Algorithms
2. Regression Algorithms

1.1.1. Classification Algorithms

In classification techniques, the dataset is split into different classes based on different parameters. Based on what it learn by the computer, the dataset categorizes into various categories. Classification algorithm based on the following mapping function

$$X \rightarrow Y \qquad \rightarrow (1)$$

Where X is input and Y is desired output.

1.1.2. Regression in machine learning

In regression algorithms, there is correlation between dependent and independent variables. So regression algorithms are used to help in predicting continuous variables.

In this paper, section – 2 describes related work, section – 3 discusses about methodology, section – 4 provides results and discussion, section –5 discusses conclusion and future work.

2. RELATED WORK

In this section, the researcher will focus on recent methods proposed by various researchers. S. Sumathi et al. [4] discussed different ML based algorithms to design the IDS. Their proposed algorithm provide superior results than conventional algorithms. Their proposed model involves SVM and KNN models in combination with c4.5 and got the average accuracy of 0.9604.

Bhosale et al [5] proposed five different classification algorithm and performed better results as compared to statistical methods.

Singhal et al [6] introduced big data technology to address DDoS attacks in application layer. They did review about various machine learning algorithms to detect and mitigate attacks in cloud environment.

Roopak et al [7] developed an algorithm which used multi objective optimization, attained average accuracy of 99%.

Swami et al [8] developed ML techniques to detect DDoS in SDN networks, but intrusion detection was not done.

Dwivedi et al [9] implemented a grasshopper optimizing algorithm to identify the trend features using different classification algorithms.

Hussain et al [10] developed various machine learning algorithms to analyze the performance of the model and confirmed that KNN method outperformed other methods.

Doucette et al [11] used ARMED classification strategy in RPCA to identify the abnormal traffic in DoS. They didn't performed hyper parameter tuning method.

Rathore & Part et al [12] proposed semi supervised ML based models for IDS. The experimental validation takes on NSL-KDD dataset and obtained the average accuracy of 86.53%. They didn't considered false alarm rate.

Ravi & Shalini et al [13] developed a method for classifying and mitigating DDoS attacks in SDN cloud environment. They achieved on average accuracy of 96.28% of DDoS classification.

Nesa et al [14] implemented algorithm for IoT environment based on non-parametric sequence based learning algorithms. They got an average accuracy of 99.65%.

3. METHODOLOGY

The researcher used KDD'99 dataset to detect smurf attack which is one of the DDoS attacks. The proposed methodology outlined in Fig.3 were pursued throughout this experiment.

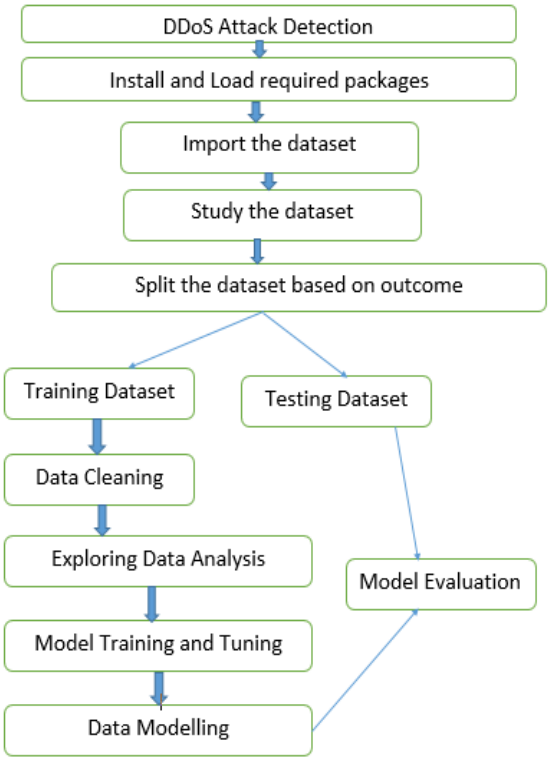

Fig.3. Flow Diagram

Step by Step process:-

Step 1:- Install caret and required packages

Step 2:- Read KDD'99 [15] dataset by importing into 'R' Software.

Step 3:- Study the dataset to identify dependent and independent variable.

Step 4:- Identifying Nearby Zero Variance (NZV) [16] variable. Sometimes, predictions have only single unique values (i.e. Zero Variance Predictor) when using data generating mechanism. Due to this, all machine learning models except tree based models may crash or unstable.

Similarly, predictors may have unique values occur with very low frequencies.

When data is split into cross validation or bootstrap sub samples, there may be some predictors are zero variance predictors or some samples may have less influence on the model.

These NZV predictors may need to be recognized and removed prior to the models.

To identify these type of predictors, the following two metrics can be calculated.

1. Frequency ratio of frequent value would be near one for well-behaved predictors and very high for unbalanced data.
2. As granularity of the data increases, the percent of unique values i.e. the ratio of unique values to total number of samples reaches zero.

Predictor may be consider s NZV predictor, if the frequency ratio is greater than a pre-specified threshold and the unique value percentage is less than a threshold.

The Nearby Zero var function can be used to identify Nearby Zero Variance variables (the saveMetrics argument can be used to show the details and usually default to FALSE)

After identifying NZV variables, eliminate them from the dataset so that the result will be more effective or select non NZV variables for dataset which is effective for models.

Step 5:- Split the dataset based on outcome.

Step 6:- Preprocess the data, i.e. identify missing values which will reduce the performance of models using principal component analysis(PCA) method. In our dataset there is no such missing variables.

Step 7:- Apply Model training and tuning.

Step 8 :- Apply different machine learning models to evaluate the performance of the each model by giving testing dataset to each model.

In our proposed method, the researcher applied SVM, Decision Tree model, Naïve Bayes model and Neural Network model.

4. RESULTS AND DISCUSSIONS

Different machine learning algorithms are applied on KDD'99 dataset, which is used to detect smurf attack which is one of the DDoS attacks. In our model, the researcher applied Nearby Zero Variance(NZV) method to identify the variables. Which are not correlated to the output variable. By detecting and eliminating NZV variables in the dataset, the researcher can improve the performance of the model. By using K-fold cross validation and PCA method. The researcher can performing the model tuning.

In next step, the researcher applied different machine learning algorithms to evaluate the detection of smurf attack in the dataset.

The researcher applied SVM, Decision Tree, Naïve Bayes and Neural Network methods to correct prediction of smurf attacks using following parameters.

True Positive (TP): Correctly identified the attack

False Positive (FP): Incorrectly identified the attack

False Negative (FN): Incorrectly identified the normal traffic.

True Negative (TN): Correctly identified the most traffic or non-attack vectors.

The researcher evaluated model with confusion matrix. Confusion matrix is a square matrix which is described in the following table 1.

Table 1. Confusion Matrix

N=Total Predictions	Actual: Yes	Actual: No
Predicted: Yes	True Positive(TP)	False Positive(FP)
Predicted: No	False Negative(FN)	True Negative(TN)

Performance of the model can be calculated by using following formulas.

Accuracy=$\frac{TP+TN}{TP+FP+TN+FN}$ → (2)

Accuracy provides the ratio of correctly identified attacks with the overall traffic i.e. which contains attacks and normal traffic.

Precision=$\frac{TP}{TP+FP}$ → (3)

Precision will give us fraction of correct predictions.

Sensitivity(or) Recall=$\frac{TP}{TP+FN}$ → (4)

Sensitivity is the fraction of DDoS attacks that are correctly predicted.

Specificity=$\frac{TN}{TN+FP}$ →(5)

Specificity is the likelihood of test without producing False Positive findings.

F1 Score=$\frac{2*recall*precision}{recall+precision}$ →(6)

F1 Score is the weighted average of Recall and Precision.

False Alarm Rate=$\frac{FP+FN}{TP+FP+TN+FN}$ →(7)

Where TP means True Positive, FP means False Positive, FN means False Negative and TN means True Negative.

The researcher compared proposed method with other existing DDoS attacks detection methods.

Table 2. Comparison of proposed model with existing models

S. No	Algorithm	Accuracy	False Alarm Rate	Recall	Specificity
1	SVM with 10 fold cross validation . [Sumathi et al]	0.9604	0.9872	0.9810	0.9810
2	GWABC-SVM [Ghayth almahadh et al]	0.9974	0.986	0.9866	0.9866
3	LVQ with DT [C.Bhagyalakshmi et al]	0.9874	0.998	0.996	0.998
4	SVM with NZV	0.9962	0.9958	0.9958	0.9957
5	Decision Tree with NZV	0.9997	0.9995	0.9995	0.9995
6	Naïve Bayes with NZV	0.9912	0.9907	0.9907	0.9907
7	NN with NZV	0.9989	0.9912	0.9912	0.9912

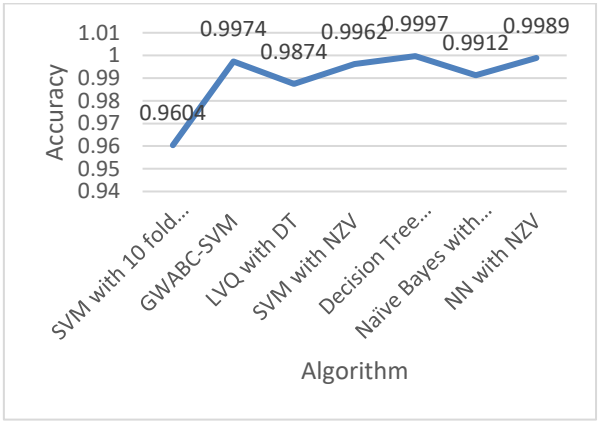

Fig.4. Accuracy Comparison

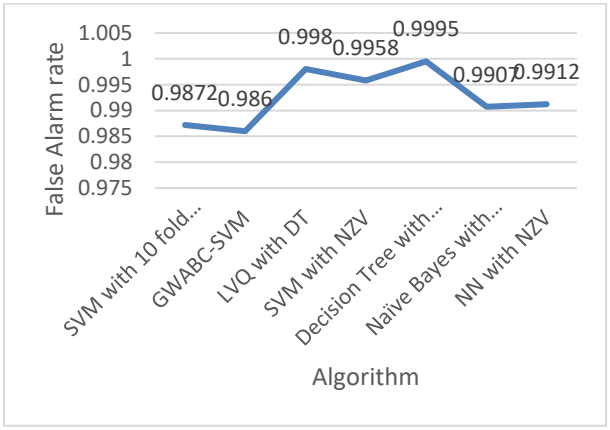

Fig.5. False Alarm rate Comparison

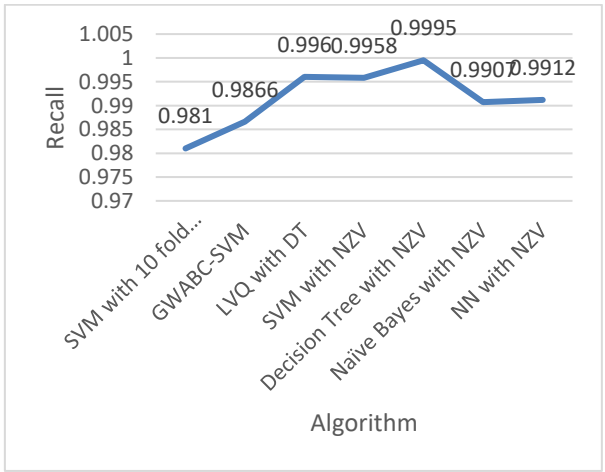

Fig.6. Recall Comparison

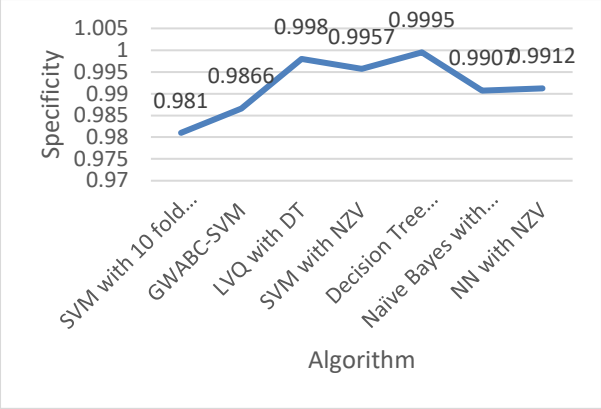

Fig.7. Specificity Comparison

Our proposed method with Nearby Zero Variance (NZV) performed well as compared to all existing methods as given in the table.2. Out of all proposed methods, Decision Tree classifier with NZV got the average accuracy of 0.9997 as compared to other NZV combination methods. Fig.4. to Fig.7. clearly tells the proposed method of Decision Tree classifier with NZV has better results as compared to existing methods.

5. CONCLUSION AND FUTURE WORK

In this paper, the researcher evaluated different machine learning algorithms to detect smurf attack in KDD'99 dataset. First the researcher calculated NZV variables in the dataset, and eliminated from the dataset. Elimination of NZV variables would improve the performance of the model.

By using K-fold cross validation, the researcher trained the dataset. PCA was used to preprocess the dataset and tune the model with traincontrol() function. The researcher applied different supervised learning methods such as SVM, Decision Tree with C4.5, Naïve Bayes and Neural Networks model on testing dataset. The researcher proposed models with NZV combination outperformed all existing methods and got an average accuracy of above 0.99. Out of all methods, Decision Tree with NZV variable and got the highest performance of 0.9997. This research surely useful for future research with an extensive evaluation by considering various datasets or scenarios would enhance the research to fix the addressed issues.

6. REFERENCES

[1] https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

[2] https://www.cloudflare.com/en-gb/learning/ddos/glossary/denial-of-service/

[3] https://www.radware.com/cyberpedia/ddos-attacks/

[4] www.analyticvidhya.com

[5] Bhosale K S, Nenova M & Iliev G, Intrusion detection in communication networks using different classifiers, in Tehno-Societal 2018 (Springer, Cham) 2020, 19-28

[6] Singhal S, Medeira P A, Singhal P & Khorajiya M, Detection of application layer DDoS attacks using big data technologies, J Discret Math Sci, 23(2) (2020) 563-571

[7] Roopak M, Tian G Y & Chambers J, Multi-objective-based feature selection for DDoS attack detection in IoT networks, IET Networks, 9(3) (2020) 120-127

[8] Swami R, Dave M & Ranga V, DDoS attacks and defense mechanisms using machine learning techniques for SDN, in Research Anthology on Combating Denial-of-Service Attacks (IGI Global) 2021, 248-264

[9] Dwivedi S, Vardhan M & Tripathi S, Defense against distributed DoS attack detection by using intelligent evolutionary algorithm, Int J Comput Appl, (2020), DOI: 10.1080/1206212X.2020.1720951.

[10] Hussain Y S, Network Intrusion Detection for Distributed Denial-of-Service (DDoS) Attacks using Machine Learning Classification Techniques (2020), http://hdl.hdandle.net/1828/11679.

[11] Doucette C, Broderick-Sander R, Toll B, Helsinger A, Soule N, Pal P, Zhou C & Paffenroth R, A robust principal component analysis approach to DoS-related network anomaly detection, Proc SPIE 11417, Cyber Sensing 2020, 114170B (27 April 2020); https://doi.org/10.1117/12.2562774.

[12] Rathore S, Park J H, Semi-supervised learning based distributed attack detection framework for IoT, Appl Soft Comput, 72 (2018) 79-89.

[13] Ravi N, Shalinie S M. Learning-driven detection and mitigation of DDoS attack in IoT via SDN-cloud architecture, IEEE Internet of Things Journal, 7(4) (2020), 3559-3570.

[14] Nesa N, Ghosh T & Banerjee I. Non-parametric sequence-based learning approach for outlier detection in IoT, Future Gener Comput Syst, 82 (2018) 412-21.

[15] http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

[16] cran.wustl.edu