Smurf attack using hybrid machine learning technique

Cite as: AIP Conference Proceedings **2463**, 020015 (2022); https://doi.org/10.1063/5.0080211
Published Online: 02 May 2022

G. Revathy, V. Rajendran, P. Sathish Kumar, et al.

Smurf Attack Using Hybrid Machine Learning Technique

Revathy G [a], Rajendran.V [b] Sathish Kumar P [c], Vinuharini S, Roopa G.N

Department of Electronics & Communication Engineering, School of Engineering,
Vels Institute of Science, Technology & Advanced Studies (VISTAS),Chennai, India.

[a] Corresponding author: grevathy19@gmail.com
[b] director.ece@velsuniv.ac.in
[c] sathish.se@velsuniv.ac.in

Abstract. Several techniques have been constructed to make the network environment and also better communication very safe and secure in cyber security domain. Intrusion detection system tool plays very important role in finding malevolent aligned with cyber security systems. Also, finding one of the kinds of Denial of Service attack which is Smurf attack is a major protection challenges facing in network equipment. Smurf attack is a kind of Denial of Service attack or malicious which should be find out for keeping the information (data) very safe and secure in Cyber security. So, in this paper we introduced machine learning hybrid algorithm in which Nearest Centroid Algorithm attains least prediction time as 0.01% and accuracy measure as 99.6% in detection of the network attacks mainly detecting Smurf attack for preventing the information very secure.

Keywords: Intrusion Detection System (IDS), Smurf attack, Denial of Service (DoS) attack and hybrid algorithm.

INTRODUCTION

Nowadays IDS plays a very immense responsibility in preventing various data (information) available in system or network environment. Artificial Intelligence especially machine learning techniques being incorporated with IDS systems because of less protection for information in the network system and also capability to keep on with most recent attacks. On owing to fast increase in growth of AI, there is necessitate to enhance the system sturdiness have been ignored as well as up-to-date investigation looks into various technique of enhancing Intrusion Detection System.

While performing type of DoS attack as Smurf, the hackers utilize their protocol address being similar to sufferer protocol address. This leads to greater mystification on sufferer system, also the enormous overflow of network transfer will send to sufferer system/ device if done exactly. Many firewalls prevent besides this kind of DoS attack mainly Smurf. Figure 1 described how the Smurf attack is being prevented.

FIGURE 1. How Smurf is being prevented

International Conference on Recent Innovations in Science and Technology (RIST 2021)
AIP Conf. Proc. 2463, 020015-1–020015-8; https://doi.org/10.1063/5.0080211
Published by AIP Publishing. 978-0-7354-4192-7/$30.00

This technique uses data from traffic monitors to detect unusual patterns. Typically the anomaly detection algorithm characterizes baseline traffic (i.e., legitimate traffic) in order to be able to detect deviations that indicate anomalies. If an anomaly is detected, an operator is notified to intervene manually.

The main objective of this proposed work is as follows

- To find the attackers who enters into the system for stealing data.
- To detect the Smurf attack if any found in the network environment
- To develop the hybrid machine learning algorithms to detect the intruders who are entering into the network or system environment.
- To evaluate the model performance by finding metrics such as precision, recall, accuracy and prediction time.

Bouyeddou et. al [1] analyzed three kinds of attack datasets for effective detection of cyber attacks namely Denial of Service attack and also DDoS attack. Bouyeddou et. al [2] utilized novel deviation approach to identify Internet Control Message Protocol based DDoS and Dos attacks. Now, 3-Σ (three-sigma) law is tried on that deviation approach for abnormality recognition. Benamar Dhairya Lunkad et. al [3] objective is to identify the DDos attacks using svm algorithm that confine any traffics in the network, sort out the headers on HTTP, standardize the data bases on outfitted features. Soodeh Hosseini et. al [4] initially gathered data, extracting features and finally deviations trial were investigated to find the network attacks by fixing threshold limit in sender side. If the deviations greater than threshold limit, the attacks were found otherwise the data is being processed. S. Indraneel et. al [5] realized high-speed as well as recognition of attacks untimely using BAT approach which depends on bio-inspired attacker based application layer DDoS attack by means of Hyper Text Transfer Protocol. Le et. al [6] had done assessment among several ML techniques such as RF, DT, SVM, MLP, NB and KNN for finding DoS attacks in the system. Mainly, this research work focused on attributes like flow in time, source IP address, and total quantity of bytes which detect the abnormal behavior in the network. Mahmudul Hasan et. al [7] proposed various machine learning algorithms like Neural Network, Logistic regression, support vector classifier to classify the network into malicious and standard along with Internet of Things devices. Also, various metrics were evaluated to predict the overall performance in detecting and categorizing attack from normal. Muraleedharan et. al [8] performed deep learning based classification algorithm to identify sluggish DoS attack occurs on Hyper Text Transfer protocol network environment which attains higher accuracy measures as 99.6%. N.Ugtakhbayar et. al [9] applied Intrusion Detection System approach to detect the intruders especially Smurf attack in the network region. Sagar Pande et. al [10] utilized KDD data source to detect the Distributed DoS attack via machine learning especially Random Forest algorithm and also ping of death approach. Also, this paper analyzes the dataset to categorize the normal from malicious. Saikat Das et. al [11,18] finding already existing attacks and also latest Distributed DoS attack in which ensembling machine learning methods were applied to restrict newly entering malicious attackers that achieves accuracy around 99% in discovering DDoS attacks profitably.

Parvinder Singh Saini et. al [12] applied random forest, Naïve Bayes, and J48 machine learning algorithm to identify and distinguish the network passage flow as malicious and standard on novel datasets consists of flood attack, normal and DoS SID. Among these three algorithms, J48 decision tree based algorithm generates 98.64% accuracy along with better performance. Reddy Sai Sindhu Theja et. al [13] afforded malicious exposure procedure which occurs in network system mainly deep belief method consists of bias, activation function were adjusted by means of optimization algorithm (medium Fitness oriented sea lion). [19] If any malicious attackers found by network, the control is transmitted to trivial bias method which can easily detect the attacks in any junction exclusive of troublemaking usual links will be organized regularly reaches the throughput as 89%.

Divyasree T.H et. al [14] introduced novel approach that is ensemble core vector machine works on the base of least enclosing ball theory for identifying attack like probe, R2L, DoS and U2R very effective and efficient. Moreover, this investigator focused on Chi-square analysis for choosing appropriate attributes for every malicious attack as well as biased function were useful to those attributes for reducing dimensions.

WankLede et. al [15] proposed AI based technique namely machine learning as well as Neural network approach for finding DoS attack in the network. Also, this paper paying attention to layers in the network especially application layers other than network layer and transport layer for finding DoS attack. For detecting such type of attacks, this

investigator utilized machine learning algorithms such as multilayer Perceptron and Random Forest that produced better accuracy.

METHODS ON DETECTING AND CLASSIFYING ATTACKS

The proposed algorithm used for detecting attacks in the networks along with further classification had performed by distinguishing normal and malicious is depicted in figure 2.

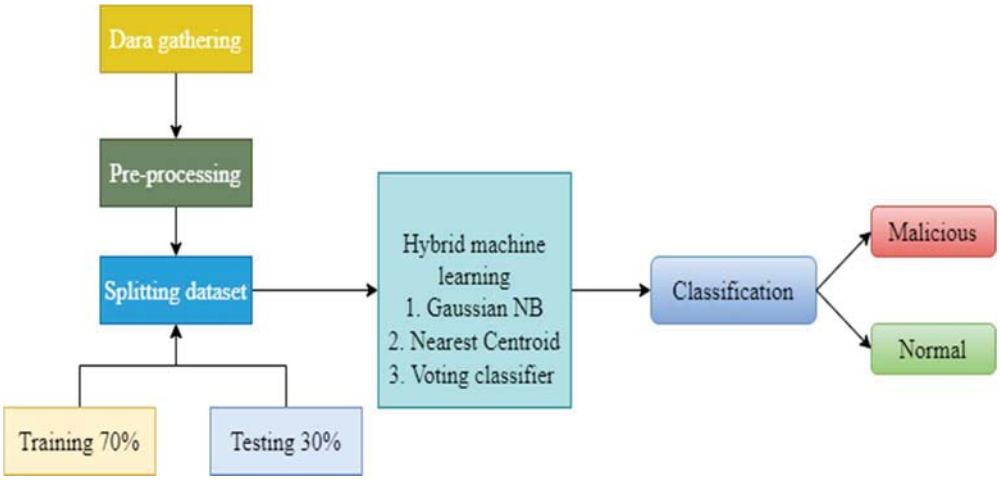

FIGURE 2. Flow of work- Proposed Framework

Data Gathering

The datasets have been gathered from KDD Cup99 and Lincoln laboratory attack datasets for finding attackers if any found in the network and then categorizing the dataset as benign and malignant. The datasets comprises of 22544 samples along with 38 features for detecting attacks.

Pre-processing

The features such as protocol type, service, flags, and port rate are irrelevant features which were removed by pre-processing technique. Therefore, we are having 34 features for further implementation of finding network attacks.

Splitting Dataset

Subsequently attaining most favorable datasets, we are splitting into two phases namely training phase as 70% which undergoes training and testing phase as 30% undergoes testing data and finally validating datasets.

Ihybrid Machine Learning Method

In this work, we proposed machine learning algorithm especially hybrid method which comprises of Gaussian Naïve Bayes, Nearest Centroid, and Voting classifier for preventing our information.

Gaussian Naïve Bayes

GNB is a kind of classification algorithm applied to classify the input data into good or bad. (i. e) This classifier categorize the input data into either yes or no which concepts comes under conditional probability. The formula for conditional probability is shown in equation 1.

$$P(c|x) = \frac{P(x|c)\,P(c)}{P(x)} \quad (1)$$

Where P(c|x) represents the subsequent possibility of attributes in dataset,
P (c) represents class likelihood
P (x|c) represents possibility in which is the likelihood of analyst, P (x) specifies preceding likelihood of forecaster.

Nearest Centroid Algorithm

The concept behind nearest Centroid algorithm is combining the data into k number of clusters in which the task of each cluster based on similar or dissimilar data or space measure to Centroid. The steps for nearest Centroid algorithm is as follows

Step 1: Initialise 'k' number of Centroid arbitrarily. Every data is allocated to adjacent Centroid.

Step 2: Then the Centroids are calculated as the average of every data position allocated to relevant groups.

Step 3: Repeat step 1 and 2 till we allocate all data points in particular cluster.

To perform this kind of clustering, we have to calculate squared Euclidean distance which is more accurate in prediction. The formula to estimate Euclidean distance is defined in equation 2

$$D=\Sigma_{n=1}^{N}\Sigma_{k=1}^{K} r_{nk}\left\|x_n-\mu_k\right\|^2 \quad (2)$$

The above function is known as k-means cost function where D represents summation of squaring the distances on every data to their allocated groups. Here, r=1 while data spot is allocated to the group (k) or else r=0.

Voting Classifier

Voting classifier is also one of the most classification algorithms which make use of various classifiers to formulate further forecasting. Wherever data science experts got confusion, they used this type of classification algorithm to resolve their issues. Hence, several classifiers were utilized for classification, among those classifiers, this voting classifier forecast the outcome depends on the most repetitive data. Moreover, voting classifier is utilized to fix the self-sufficient features to reliant feature during training phase.

Classification

The classification technique is used for categorizing the data into two partitions via specific classifiers. For categorizing the dataset as normal and malignant in the system environment, we applied classification method which helps for distinguishing the same easily.

METRICS ESTIMATION

Finding metrics like recall, precision and prediction time along with accuracy measure in machine learning techniques is to evaluate the overall performance of whatever models used to detect the malicious behaviors if any found in the network. Hence, we are finding those metrics using the formula mentioned in table 1.

In addition to that some other measures like standard deviation, mean, min and max were evaluated for predicting the better outcome during statistical analysis.

TABLE 1. Used metrics with formula description

Metrics	Rule used
Accuracy	$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$
Recall	$\text{Re}\,call = \frac{TP}{TP + FN}$
Precision	$\text{Pr}\,ecision = \frac{TP}{TP + FP}$
F-score	$F\text{-}Score = 2 \times \frac{Precision \times Recall}{Precision + Recall}$
Prediction time	The time taken to forecast the outcome like detection of attacks in the network

Mean: Finding the average of all the samples given in whole datasets. The mean is calculated using the formula

$$\text{Mean} = \frac{\text{Sum of all samples}}{\text{Total number of samples in finding attacks}} \tag{3}$$

Standard deviation (SD): By using standard deviation measure, we can able to estimate the inconsistency of attack dataset samples which is a critical analysis of accuracy calculation in ML based approach. Additionally, this metrics may be utilized to determine self-assurance in algorithm mathematical termination. SD can be measured using the formula

$$\sigma = \frac{\Sigma(X-\mu)^2}{n} \tag{4}$$

Where σ is SD, x is data value, μ is mean value, n is the total number of samples.

Moreover, t-score and p-value have been estimated during statistical analysis to identify the difference, with the intention of making decision whether accepting or rejecting the NULL hypothesis.

P-value and t-score: P-Value denotes "whole likelihood" decided from the right portion of area under curve as soon as the data values are selected arbitrarily from overall attack dataset samples. If the P-value is less, then we can discard the NULL hypothesis and finalize that there will be some noteworthy difference statistically. And also if t-value is greater with lesser p-value, the indication is aligned with NULL hypothesis. We are fixing the alpha value which is specified as threshold value in which the investigations were performed prior to managing test of z-score or a t-value.

RESULTS AND DISCUSSION

Effective Analysis for Gaussian Naïve Bayes

The analysis had done using Gaussian Naïve Bayes for training samples as 1%, 10%, 100%. The GNB trained 157 samples as initial percentage, then trained on 1578 samples as 10, and finally trained on 15780 samples with 100%. Hence, all samples datasets were trained to predict the better measuring parameters such as training time, predicting time, accuracy on both training and testing, F-score, and finally False Negative Rate. The experimental analysis on detection of attacks using GNB is described in table 2.

TABLE 2. Effective Analysis for Gaussian NB

	Training samples		
	1%	10 %	100 %
Training time	0.009009	0.039020	0.167943
Prediction time	0.094800	0.095057	0.081660
Training accuracy	1.000000	1.000000	1.000000
Testing accuracy	0.997930	0.997191	0.998669
F score training	1.000000	1.000000	1.000000
F score testing	0.963918	0.948787	0.976501
FNR for Training	0.000000	0.000000	0.000000
FNR for Testing	0.000000	0.058824	0.000000

Effective Analysis for Nearest Centroid

The analysis had done using NC for training samples as 1%, 10%, 100%. The NC trained 157 samples as initial percentage, then trained on 1578 samples as 10, and finally trained on 15780 samples with 100%. Hence, all samples datasets were trained to predict the better measuring parameters such as training time, predicting time, accuracy on both training and testing, F-score, and finally False Negative Rate. The experimental analysis on detection of attacks and also classification of data as normal and malicious using NC is specified as values in table 3.

TABLE 3. Effective Analysis for Nearest Centroid

	Training samples		
	1%	10 %	100 %
Training time	0.009531	0.010009	0.066014
Prediction time	0.020003	0.019005	**0.019010**
Training accuracy	0.996667	1.000000	1.000000
Testing accuracy	0.980928	0.996008	**0.996008**
F score training	0.952381	1.000000	1.000000
F score testing	0.743539	0.932668	0.932668
FNR for Training	0.000000	0.000000	0.000000
FNR for Testing	0.000000	0.000000	0.000000

Effective Analysis for Voting classifier

The examination had completed using voting classifiers to make decision by most frequently occurring data in specific cluster and also training data samples as 1%, 10%, 100%. The VC trained 157 samples as initial percentage, then trained on 1578 samples as 10, and finally trained on 15780 samples with 100%. Hence, all samples datasets were trained to predict the better measuring parameters such as training time, predicting time, accuracy on both training and testing, F-score, and finally False Negative Rate. The experimental analysis on detection of attacks along with classification algorithm to distinguish attack from malignant using VC is described in table 4.

TABLE 4. Effective Analysis for voting classifier

	Training samples		
	1%	10 %	100 %
Training time	0.015229	0.031255	0.185028
Prediction time	0.384834	0.351032	0.373949
Training accuracy	1.000000	1.000000	1.000000
Testing accuracy	0.997930	0.997191	0.998669
F score training	1.000000	1.000000	1.000000
F score testing	0.963918	0.948787	0.976501
FNR for Training	0.000000	0.000000	0.000000
FNR for Testing	0.000000	0.058824	0.000000

Basically in machine learning concepts, less prediction time leads to greater performance to the model. Hence, we are comparing three machine learning algorithms which were implemented in attack detection as well as classifying attacks. Among these three classifiers, Nearest Centroid method attains lesser prediction time as 0.01 seconds along with greater accuracy as 99.6% that enhances the model performance in both predicting attacks in the network and classification. Figure 3 illustrates that evaluation of metrics to predict the overall performance of hybrid model in detection of network attacks along with classification of attacks.

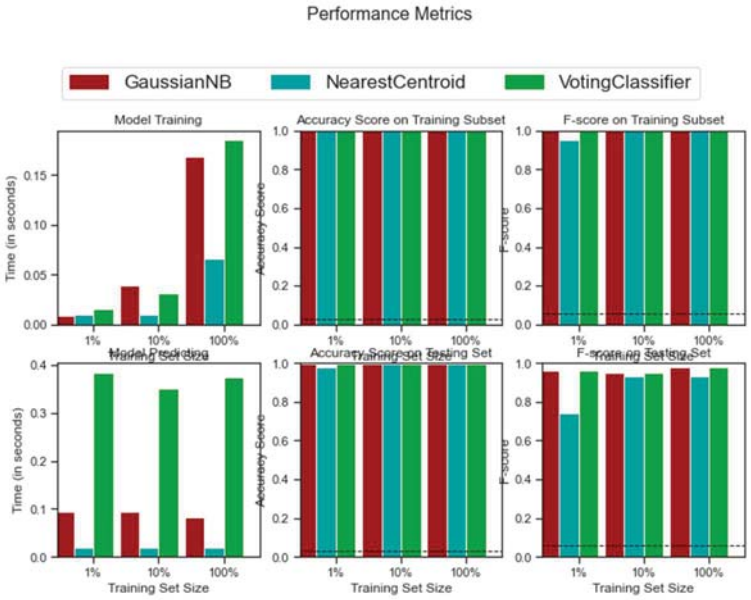

FIGURE 3. Performance evaluation for hybrid approach

CONCLUSIONS

In this proposed work, we conducted experiments on datasets of KDD Cup99 and Lincoln laboratory for distinguishing attack data from normal data. Hence, we introduced hybrid algorithm comprises of Gaussian Naïve Bayes, Nearest Centroid and Voting classifier for finding DoS attack in the network environment. Among these algorithms, Nearest Centroid reveals better outcomes by evaluating metrics like accuracy, prediction time, FNR, and F-score for classifying datasets as regular and DoS attack. Nearest Centroid algorithm achieves less in prediction time as 0.019%, with 99.6% accuracy which enhances the performance of this model in distinguishing attack from normal.

REFERENCES

1. Bouyeddou B, Harrou F, Sun Y, Kadri B, "Detection of smurf flooding attacks using Kullback-Leibler-based scheme," 4th International Conference on Computer and Technology Applications (ICCTA), 11-15 (2018).
2. Bouyeddou, B., Kadri, B., Harrou, F., & Sun, Y, "DDOS-attacks detection using an efficient measurement-based statistical mechanism," Engineering Science and Technology, an International Journal, **1(4)**, 870-878 (2020).
3. Dhairya Lunkad, Govind Singh, "DDOS Attack Detection Using Machine Learning for Network Performance Improvement", **8(9)**, 2320-2882 (2020).
4. Hosseini, S., & Azizi, M., "The Hybrid Technique for DDoS Detection with Supervised Learning Algorithms," Computer Networks, **158**, 35-45 (2019).
5. Indraneel Sreeram, Venkata Praveen Kumar Vuppala, "HTTP flood attack detection in application layer using machine learning metrics and bio inspired bat algorithm," Applied Computing and Informatics, **15(1)**, 59-66 (2019).
6. Le D. T., Dao M. H., Nguyen Q. L. T., "Comparison of machine learning algorithms for DDoS attack detection in SDN," Information and Control Systems, **3**, 59–70 (2020).
7. Mahmudul Hasan, Md. Milon Islam, Md Ishrak Islam Zarif, M.M.A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," Internet of Things, **7**, 100059 (2019).
8. N., M., & B., J, "A deep learning based HTTP slow DoS classification approach using flow data," ICT Express, **7(2)**, 210-214 (2021).
9. N.Ugtakhbayar, D.Battulga and Sh.Sodbileg "Classification of Artificial Intelligence Ids fsor Smurf Attack," International Journal of Artificial Intelligence & Applications (IJAIA), **3(1)**, (2012).
10. Sagar Pande, Aditya Khamparia, Deepak Gupta, and Dang N. H. Thanh "DDOS Detection Using Machine Learning Technique," Recent Studies on Computational Intelligence, Studies in Computational Intelligence **921**, 59-68 (2021).
11. Prabhakaran, A., Krishnan, K. S., Dhinakaran, R., Baskar, S., & Shaisundaram, V. S., "Analysis of the efficiency of an automotive alternator by replacing mild steel into aluminum as a material for rotor," Materials Today: Proceedings, **37**, 1269-1273 (2021).
12. Saikat Das, Ahmed M. Mahfouz, Deepak Venugopal, Sajjan Shiva, "DDoS Intrusion Detection through Machine Learning Ensemble," IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C), 471-477 (2019).
13. Saini, P. S., Behal, S., & Bhatia, S., "Detection of DDoS Attacks using Machine Learning Algorithms," 7th International Conference on Computing for Sustainable Global Development (INDIACom), 16-21 (2020).
14. SaiSindhuTheja Reddy, Gopal K. Shyam, "A machine learning based attack detection and mitigation using a secure SaaS framework," Journal of King Saud University - Computer and Information Sciences, (2020).
15. Saravanakumar, S., Chandramohan, N. K., Prabakaran, S. T., Muniyappan, M., Shanmugam, M., and Shaisundaram, V. S., "The static structural analysis of torque converter material for better performance by changing the stator angle," Materials Today: Proceedings, **37**, 1963-1972 (2021).
16. T.H. Divyasree, K.K. Sherly, "A Network Intrusion Detection System Based On Ensemble CVM Using Efficient Feature Selection Approach," Procedia Computer Science, **143**, 442-449 (2018).
17. Wankhede, S. and Kshirsagar, D, "DoS Attack Detection Using Machine Learning and Neural Network," Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), 1-5 (2018).
18. D.Ravikumar, V.Devi, Arun Raaza, "Development of Brain Computer Interface using Neural Networks," Research Journal of Pharmacy and Technology, **11(10)**, 4397-4400 (2018).
19. V. Devi, D.Ravikumar, M.Meena, E.N.Ganesh, V.Janakiraman "Distributed Denial of Service Detection and Mitigation Solutions in Software Defined Radio Networks," Journal of Xidian University, **14(6)**, 1536-1541 (2020).