IJBCS
ISSN: 2147-1428

Original Article

International Journal of Basic and Clinical Studies (IJBCS)
2019; 8(1): 23-36 Veranyurt O.

Usage of Artificial Intelligence in DOS/DDOS Attack Detection

Ozan Veranyurt*

* Bahçeşehir University, Institute of Science, Department of Cyber-Security, Istanbul, Turkey

Abstract

The main objective of a Denial of Service (DOS) attacks is to target a specific entry and create a flood of different type of network packets. If the attack is formed in Distributed Denial of Service than the attacker compiles multiple systems across the internet called as zombies/agents and executes the attack by remotely controlling them. In this paper it is aimed to examine detection of Denial of Service attacks through different Machine Learning Algorithms and Artificial Neural Networks (ANN). The evaluation will be done with the Knowledge Discovery and Data Mining Tools Competition (KDD 99) dataset and the data collected in lab tests. The focus of the study will be the assessment of the Machine Learning and ANN algorithms success in the detection of Network Layer DOS Attacks.

Key words: DOS, Machine Learning, Neural Networks, DOS and AI

Correspondence address: Yıldız Mh., Çırağan Cad., 34349 Beşiktaş/İstanbul; Tel: +905321764977; E-mail: ozan.veranyurt@bahcesehir.edu.tr

Introduction

DOS / DDOS attacks are one of the most fundamental problems of today's internet world. This threat, which cannot be solved since the first day of the Internet, is a serious problem that cannot be solved for a long time with the currently used TCP / IP protocol. The main purpose of DDOS attacks is to make the system dysfunctional. Despite the important evolution of the information security technologies, the attack continues to challenge the existing defense systems. There are four implementation schemes of DOS defense systems: Source-end, intermediate, distributed and victim-end (1). Detection suffers from efficiently differentiating the normal stream and abnormal stream of traffic. Filtering clogs up during heavy traffic whereas trace-back can only be effective under subsidized traffic, so performed mostly after the closing of the attack. Most of the existing detection mechanism have limited success because of the following challenges (i) the attack itself often uses legitimate requests to flood the target and this makes it hard to distinguish an

attack traffic from legitimate traffic (ii) fast real time detection is difficult because of huge amount of data involved in current computer networks (2).

Common DOS/DDOS Attacks

SYN Flood attack

In a SYN flood attack, a malicious client sends a large number of SYN packets, but never sends the final ACK packets to complete the handshakes. In this way the listen queue of that port is overwhelmed and will not be able to respond any further requests after a certain point. In the distributed attack scenario, the target receives SYN requests on an open port from multiple compromised bots with spoofed or real IP addresses.

Ping of Death

A ping of death ("POD") attack involves the attacker sending multiple malformed or malicious pings to a computer. The maximum packet length of an IP packet (including header) is 65,535 bytes. However, the Data Link Layer usually poses limits to the maximum frame size – for example 1500 bytes over an Ethernet network. In this case, a large IP packet is split across multiple IP packets (known as fragments), and the recipient host reassembles the IP fragments into the complete packet. In a Ping of Death scenario, following malicious manipulation of fragment content, the recipient ends up with an IP packet which is larger than 65,535 bytes when reassembled. This can overflow memory buffers allocated for the packet, causing denial of service for legitimate packets (3).

Smurf

A Smurf attack is a form of a distributed denial of service (DDoS) attack that renders computer networks inoperable. The Smurf program accomplishes this by exploiting vulnerabilities of the Internet Protocol (IP) and Internet Control Message Protocols (ICMP).

The steps in a Smurf attack are as follows:

- First, the malware creates a network packet attached to a false IP address — a technique known as "spoofing."
- Inside the packet is an ICMP ping message, asking network nodes that receive the packet to send back a reply
- These replies, or "echoes," are then sent back to network IP addresses again, setting up an infinite loop (4).

Slowloris

Slowloris is a highly-targeted attack, enabling one web server to take down another server, without affecting other services or ports on the target network. Slowloris does this by holding as many connections to the target web server open for as long as possible. It accomplishes this by creating connections to the target server, but sending only a partial request. Slowloris constantly sends more HTTP headers, but never completes a request. The targeted server keeps each of these false connections open. This eventually overflows the maximum concurrent connection pool, and leads to denial of additional connections from legitimate clients (3).

IJBCS
ISSN: 2147-1428

Original Article

International Journal of Basic and Clinical Studies (IJBCS)
2019; 8(1): 23-36 Veranyurt O.

HTTP flood attack

In an HTTP flood DDoS attack, the attacker exploits seemingly-legitimate HTTP GET or POST requests to attack a web server or application. HTTP floods do not use malformed packets, spoofing or reflection techniques, and require less bandwidth than other attacks to bring down the targeted site or server. The attack is most effective when it forces the server or application to allocate the maximum resources possible in response to each single request (3).

Detection of DOS/DDOS Attacks

While forming the attack structure the anonymity is a key point, the challenge for the victim is the detection. Security experts try to build the defenses on the victim-end. The most common solution used for DOS/DOS detection is an Intrusion Detection System (IDS). IDS can be a software or an appliance with the purpose of detection of any thread against the system. IDS systems have two ways of working, signature based and anomaly based detection. In the signature based approach, the IDS system compares the known information of signatures that are stored in a central or cloud database. If the pattern of packets match the known signature then it generates an alarm. In some cases IDS can have IPS features and can decide to block/drop the packets on its own. This technique is a valid approach for known attacks and creates a low rate of false alarms. On the other hand an anomaly based IDS checks network traffic patterns and learns the behavior of normal traffic, thus has the capability to compare normal/abnormal traffic. This gives the anomaly based approach more chance to detect zero- day attacks. In the following chapters of this study we will focus on anomaly detection considering the attacks as datasets and for given datasets we will evaluate different Machine Learning algorithms and ANN success in attack detection at network layer.

Material and Method

For the evaluation purposes 2 datasets were used in this study. First data set for the analysis is the data set used for The Third International Knowledge Discovery and Data Mining Tools Competition, which was held in conjunction with KDD-99, the Fifth International Conference on Knowledge Discovery and Data Mining. The competition task was to build a network intrusion detector, a predictive model capable of distinguishing between ``bad'' connections, called intrusions or attacks, and ``good'' normal connections. This database contains a standard set of data to be audited, which includes a wide variety of intrusions simulated in a military network environment (4).

IJBCS
ISSN: 2147-1428

Original Article

International Journal of Basic and Clinical Studies (IJBCS)
2019; 8(1): 23-36 Veranyurt O.

Dataset Name	Author	Date	Real or Simulated	Features	DDoS attack Types	Dataset Size	Availability	Advantage	Limitation
KDD'99 Cup dataset [8]	MIT Lincoln Labs		Simulated	-two weeks of attack-free encounters and five week attack instance -output divided into 5 categories of ;DOS, Probe, R2L, U2R, and Normal -has 38 total attack types	SYN flood	743 MB	Available	-easily obtainable -many attack type available	-heavily imbalanced dataset with 80% attack traffic.
CAIDA DDoS Attack 2007 dataset [9]	Paul Hick	Aug 4, 2007	Simulated	-consist of data anonymized within one hour - resource consumer	UDP flood	21 GB	Quasi-restricted	-available for public use -effective to handle large DDoS attack above 5 Gb -traces can be read on any software reading tcpdump	-non-attack traffic is unavailable -does not include payload packets
EPA http dataset	Laura Bottomley	Aug 29, 1995	Real	-46,014 GET requests - 1622 POST requests -107 HEAD requests -6 invalid requests -One-second accuracy on timestamp	HTTP flooding	4.4 MB	Available	-smaller dataset size	-cannot determine legitimate and illegitimate HTTP requests -small dataset may limit the extent of attack detection
DARPA_2009_malware-DDoS_attack-20091104	University of Southern California-Information Sciences Institute	Nov 4, 2009	Real	-background traffic and malware attack on compromised hosts of 172.28.0.0/16 IP range. -Attack performed on non-local target of IP 152.162.178.254 at TCP port 499	Malware DDoS attack	346.5 MB	Quasi-Restricted	-contains vectors for attacks from real DDoS attacks	

Table 1. Comparison of Datasets

Table 1 demonstrates the publicly available datasets for further derivation. In this study the KDD dataset was selected, because it presented an imbalanced traffic and all of the attacks were identifiable through abnormalities at network layer.

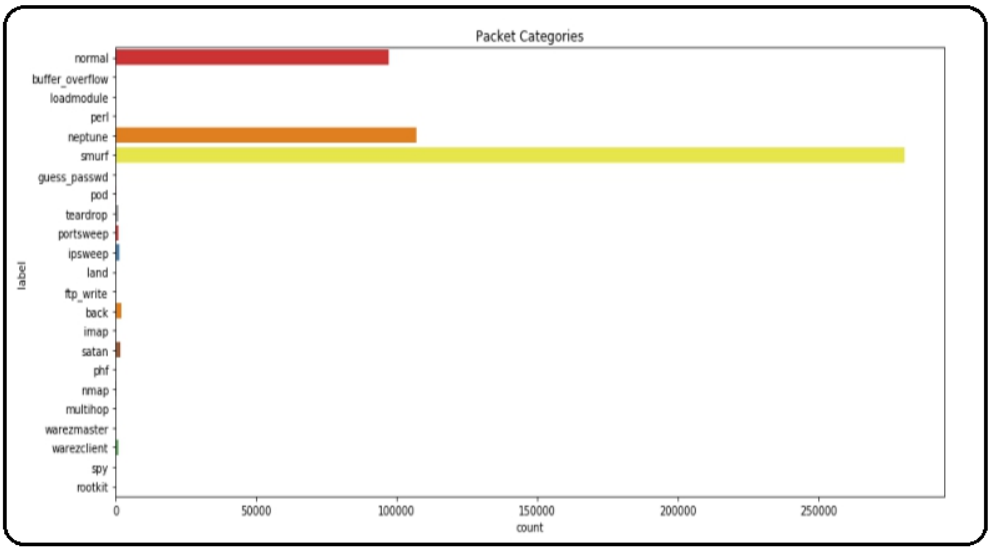

Figure 1. KDD Distribution of Packets

IJBCS
ISSN: 2147-1428

Original Article

International Journal of Basic and Clinical Studies (IJBCS)
2019; 8(1): 23-36 Veranyurt O.

Figure 1 reflects the packet distribution of the KDD dataset and as can be seen, the packet types are distributed in an imbalanced way. While Neptune and Smurf attacks have large scale of data, attacks like IP or port sweeping have much less data which makes the dataset more challenging for the Artificial Intelligence to comprehend.

Compared Machine Learning Algorithms

In this study, Support Vector Machine (SVM), Decision Tree, Random Forest, Naïve Bayes and ANN algorithms were used to process the data and obtain the results. The reason for choosing these algorithms for comparison is the fact that the data we were working on was not linear and particularly random. For this purpose, classification algorithms that were recommended for big datasets were utilized. The study will go through each algorithm's working principles in basics in the next section.

The basic principle of the Support Vector Machine (SVM) is to derive a hyperplane that maximizes the separating margin between the positive and negative classes. The standard SVM algorithm is a supervised learning technique, which requires labeled data to create classification rule. The algorithm can be used for prediction and classification (6).

In the SVM Algorithm it is considered that class distinction can be achieved with a function. By default it is useful for linear classification, however with the kernel trick that alters the core regression function nonlinear data can be classified as well. For this purpose the algorithm uses linear, polynomial, RBF or exponential function methods. A sample distribution of data for regression with these kernel functions are demonstrated in Figure 2.

Support Vector Machine Classification

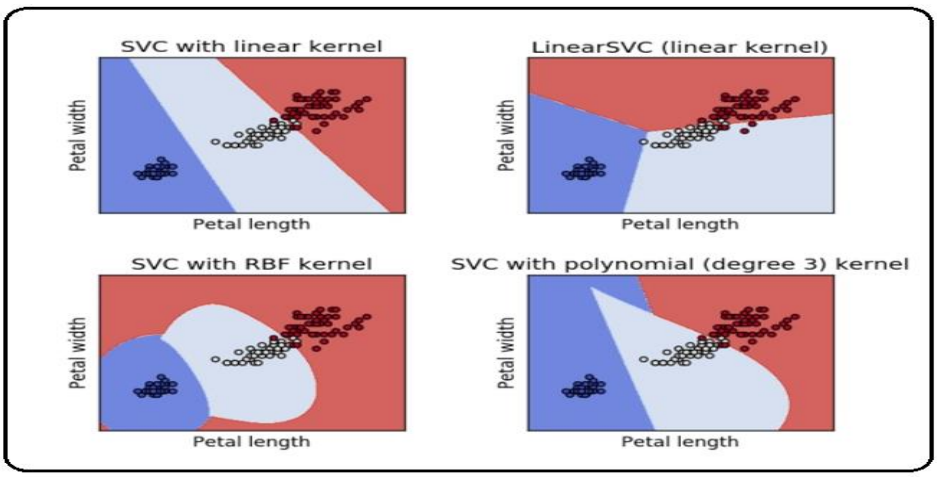

Figure 2. Comparison of SVM Kernels on Iris Dataset

IJBCS
ISSN: 2147-1428

Original Article

International Journal of Basic and Clinical Studies (IJBCS)
2019; 8(1): 23-36 Veranyurt O.

Naive Bayes Classification

In a simpler explanation, Naive Bayes presumes that a specific feature in set or class is independent from any other feature within the same set. For example, to diagnose if a fruit is strawberry, color, size could be key features even though they are dependent on each other. However each feature plays an independent role for making a prediction if the object is a strawberry or not. It is another reason for calling the algorithm Naïve.

Naive Bayes model is easy to build and particularly useful for very large data sets. Along with simplicity, Naive Bayes is known to outperform even highly sophisticated classification methods.

Bayes theorem provides a way of calculating posterior probability P (c | x) from P(c), P(x) and P (x | c). Look at the equation below:

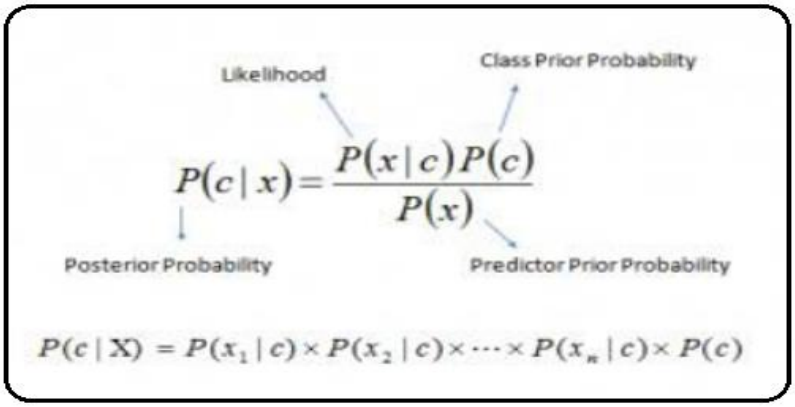

Figure 3. Bayes Theorem

As illustrated in Figure 3:

- $P(c \mid x)$ is the posterior probability of *class* (c, *target*) given *predictor* (x, *attributes*).
- $P(c)$ is the prior probability of *class*.
- $P(x \mid c)$ is the likelihood which is the probability of *predictor* given *class*.
- $P(x)$ is the prior probability of *predictor* (7).

For the classification purpose, the algorithm uses Conditional Probability Table (CPT). The table is used for calculating the probability of a variable for a specific state. While forming the relationships between variables, a parent-child relationship is formed in which the child node's probability is dependent on the parent (6).

Decision Tree Classification

Decision tree learning method is another subcategory machine learning algorithms. There are applications such as classification tree or tree of regression tree which can be considered as sub methods of decision tree learning.

In the decision tree learning, a tree structure is formed and the class labels on the leaf level of the tree and the handles that go to these leaves and with the arms coming from the beginning are expressed.

IJBCS
ISSN: 2147-1428

Original Article

International Journal of Basic and Clinical Studies (IJBCS)
2019; 8(1): 23-36 Veranyurt O.

During the learning of the decision tree, the set on which the training is performed is divided into sub-clusters according to various characteristics, this process is repeated (recursive) and continues until the repetition has no effect on the estimation. This process is called recursive partitioning.

Random Forest Classification

Random Forest is another supervised machine learning algorithm. As the name implies it builds a forest from Decision Trees with the "bagging" method. The concept of bagging method is that a combination of different learning models gives better results.

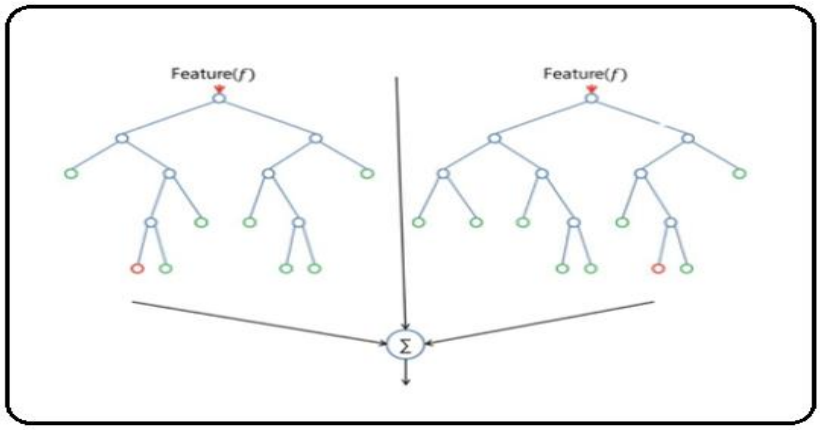

Figure 4. Random Forest Illustration

The algorithm can be used both for regression and classification. In the Figure 4 a sample Random Forest is illustrated based on feature selection.
Classification of the Feature (f) is divided into sub Decision Trees and each probabilistic result is averaged for a better result (8).

The algorithm can be utilized for both linear and nonlinear problems, however it is recommended to use it with large datasets since working with small scale datasets can cause overfitting condition which means memorization of the data.

Artificial Neural Networks

A neural network consists of a collection of processing units called neurons that are highly interconnected according to a given topology. ANN have the ability to learning by example and generalize from limited, noisy, and incomplete data. They have been successfully employed in a broad spectrum of data-intensive applications (9).

The Neural network's foundation shows resemblance to our nervous system and the network is divided into neuron. The structure of neural networks and the structure of neurons which function is shown on Figure 5.

IJBCS
ISSN: 2147-1428

Original Article

International Journal of Basic and Clinical Studies (IJBCS)
2019; 8(1): 23-36 Veranyurt O.

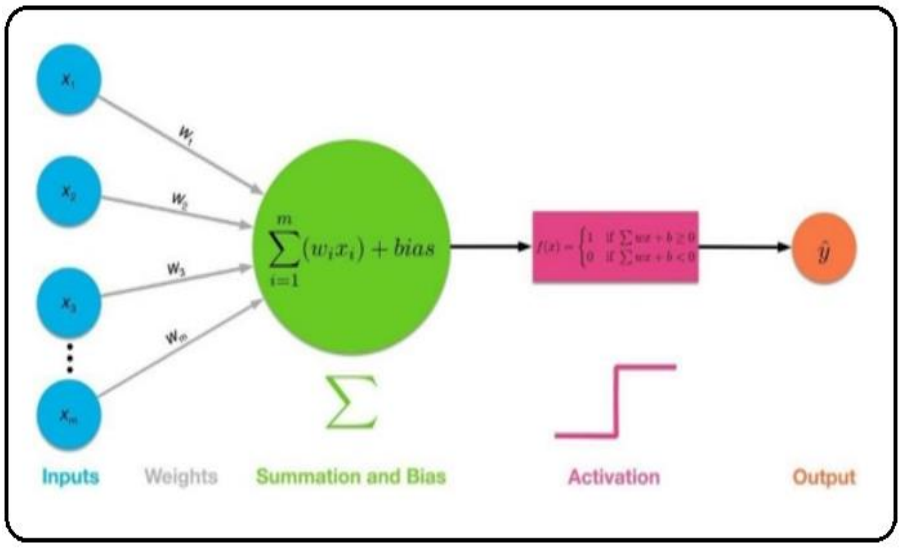

Figure 5. ANN Illustration

Learning in artificial neural networks is achieved by minimizing the value of the weight vector between neurons. The output from each neuron is produced once a threshold is reached
which is confirmed by the activation function. Depending on the complexity of the ANN, it is trained and the aim of the training of the ANN is to find the weight values that will produce the correct outputs for the examples shown to the network. When the network reaches the correct weight values, it means that the samples have the ability to make generalizations about the event they represent. The back-propagation for the network learning can be summarized as the procedure of repeatedly adjusting the weights to minimize the difference between the actual output and the desired output. With multiple iterations the weights are adjusted until maximum accuracy is reached. The complexity of Artificial Neural Networks and layer concepts can be further elaborated, however we will not explore any further on how the ANN works as it is beyond the scope of this study.

Results

Results from KDD 99 Dataset Evaluations

The KDD 99 Dataset was trained and tested with the enlisted algorithms in the comparison scale of execution time and classification accuracy. Below in Figure 6 results are shared.

IJBCS
ISSN: 2147-1428

Original Article

International Journal of Basic and Clinical Studies (IJBCS)
2019; 8(1): 23-36 Veranyurt O.

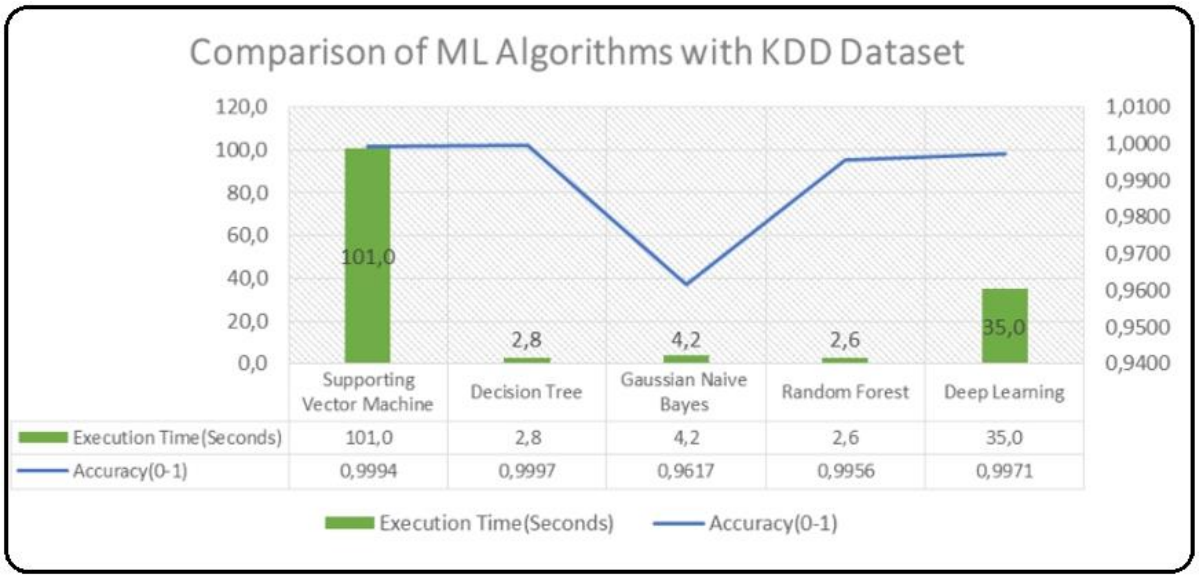

Figure 6. KDD 99 Dataset Execution Results

Support Vector Machine demonstrated a significant delay compared to other tested algorithms despite using different kernels for data division. The reason behind this outcome is that the available kernels for SVM are linear, polynomial and radial basis based. Polynomial and Radial Basis Function (RBF) can be used for extrapolation of non-linear data however if the data is so randomly distributed in multiple-axis in data space classification takes much longer time than any other probabilistic classification. Another reason behind the delay was that the class set in the training contained 22 separate features for classification. On the other hand all algorithms showed probability accuracy over 99%. One of the key factors in the success was the ratio of training and test data distribution. Probabilistic accuracy showed observable increase as the training data was during multiple execution tests from 50% to 77%. Successful results (Over 95% success rate), were obtained once the size of the training set was augmented over 65%. For every test data distribution was randomized for better accuracy.

Final results for the Artificial Neural Networks improved through multiple trials. Firstly the training period was the key delay factor in execution time and it required 15 iterations for
substantial results which required more than 120 seconds execution time. For faster backwards propagation in the neural network we used Rectified Linear Unit (Relu) as the activation function. Being a linear activator, the function saved time in the learning process for the input and hidden layers. Best results were obtained with a 2 layer neural network creating output with a sigmoid activator. With the optimal collection of activators, we were

IJBCS
ISSN: 2147-1428

Original Article

International Journal of Basic and Clinical Studies (IJBCS)
2019; 8(1): 23-36 Veranyurt O.

able to reduce iteration size to 5 for the acceptable probability accuracy. Figure 7 illustrates the confusion matrix for the ANN test results.

Figure 7. ANN Confusion Matrix for KDD 99 Dataset

In Figure 7, packet types were represented as integer labels. The diagonal marked with darker greens reflect the true positives found in the test execution.

While test results on the KDD 99 dataset showed optimistic results, the input features used for clarification raises questions from network security perspective. Firstly, at network layer the determination of the attack vector from source and destination IP addresses were critical for determining if the traffic was an attack or not however in this dataset neither source nor destination addresses were used as classification features. For instance, in order to form a smurf attack broadcast addresses are used and echo replies are sent back to the victim. Without proper destination IP classification, the AI shall not be using right input for classification. Same implies for other network floods using TCP Flags. If AI does not learn to interpret the flags correctly, then the classification done is limited only to the improvised learning dataset. Secondly for a ping of death attack, the payload carried over the ICMP packet is the key identifier and is not listed in the classification dataset. All of these questions conclude to one fact, for realistic anomaly detection input layers provided to AI should be selected based on the possible fingerprints of the attack. Therefore, the tests were repeated with a narrowed down dataset produced in lab environment and assessed the performance of the algorithms once more.

IJBCS
ISSN: 2147-1428

Original Article

International Journal of Basic and Clinical Studies (IJBCS)
2019; 8(1): 23-36 Veranyurt O.

Results from Lab Evaluations

Due to the listed reasons in previous chapter, the enlisted lab traffic was generated. Below in the Figure 8 the distribution of traffic patterns is displayed.

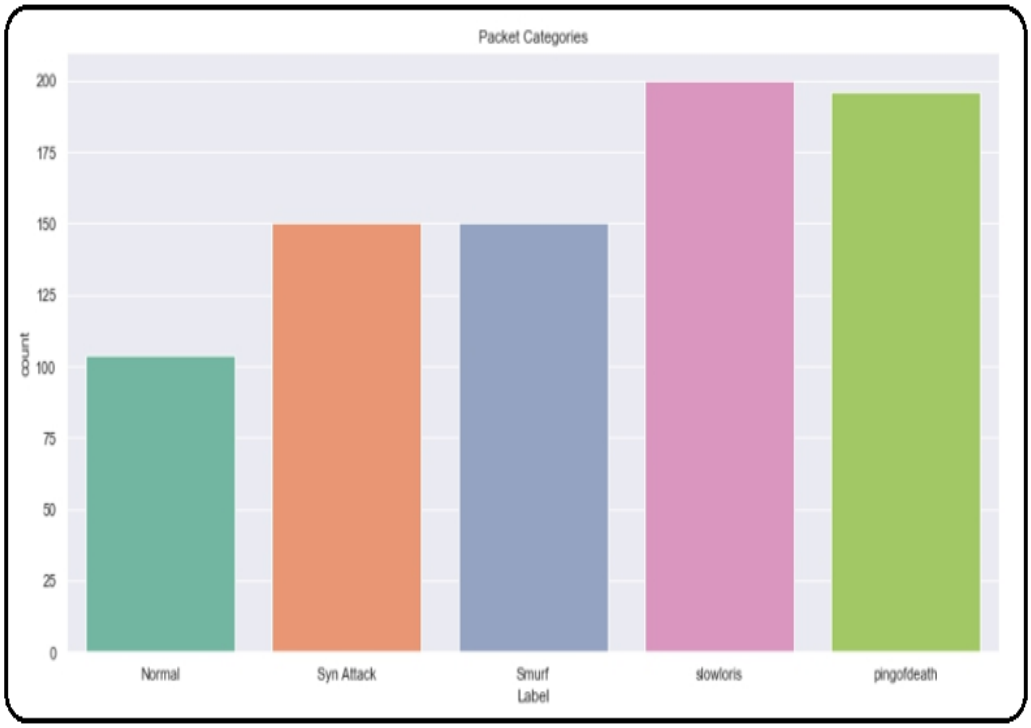

Figure 8. Lab Generated Traffic Packet Distribution

Attacks were simulated in a way that they were targeting same server from random IP addresses and using different source/destination port combinations. For each attack type it was tried to generate relatively close amount of traffic. This was one of the main differences between the KDD dataset. Secondly the input dimension took the core protocol fields like TCP flags, source, destination ports, and fragment size etc. so that classification would occur more likely as in the real world.

IJBCS
ISSN: 2147-1428

Original Article

International Journal of Basic and Clinical Studies (IJBCS)
2019; 8(1): 23-36 Veranyurt O.

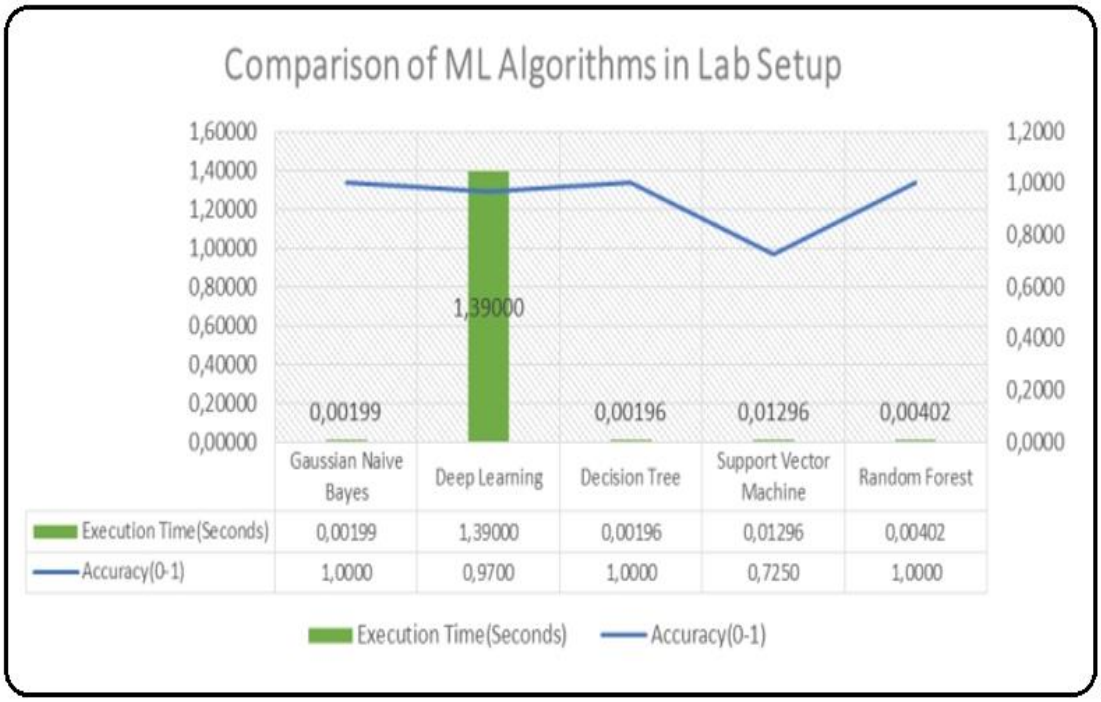

Figure 9. Comparison of ML Algorithms with Lab Generated Dataset

Figure 9 displays the summary of lab dataset execution results. For a smooth comparison same algorithm setup was used for the tests and as can be interpreted from the figure, ANN, Decision Tree and Random Forest showed perfect accuracy. First reason for this result was the data size being much less compared to KDD 99 dataset. Secondly it can be assumed that the even distribution of data made the Decision Tree based algorithms produce better results. In terms of execution time, ANN demonstrated the margin result with a time of 1,39 seconds. SVM execution time was significantly reduced due to lack of data and input dimension which also proved that, it is not a recommended choice for large datasets with multiple nonlinear input dimensions. Deep learning demonstrated higher execution time due the training period, however it shows consistent accuracy results in both tests. For acceptable accuracy results, ANN required 10 iterations to reach best learning rate as can be seen on Figure 10.

IJBCS
ISSN: 2147-1428

Original Article

International Journal of Basic and Clinical Studies (IJBCS)
2019; 8(1): 23-36 Veranyurt O.

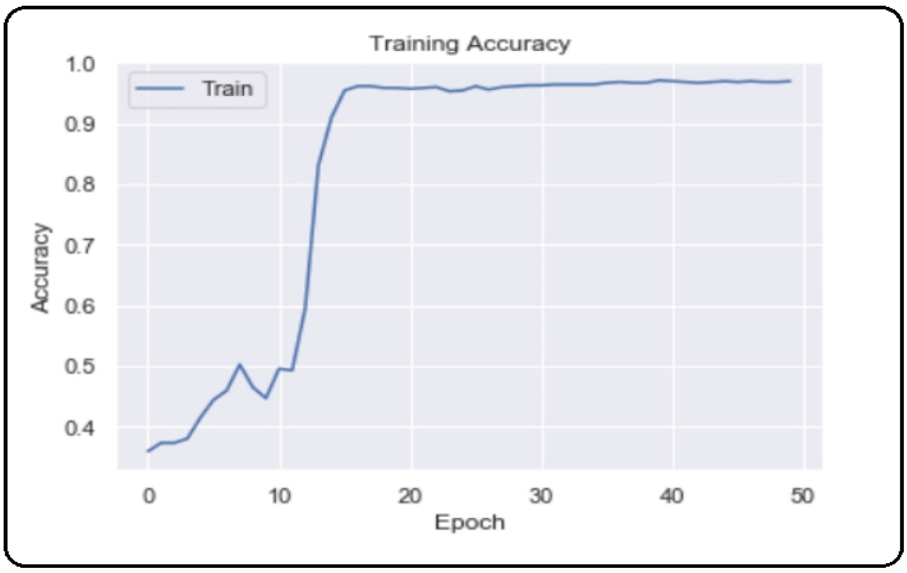

Figure 10. Training Accuracy through Iterations for ANN

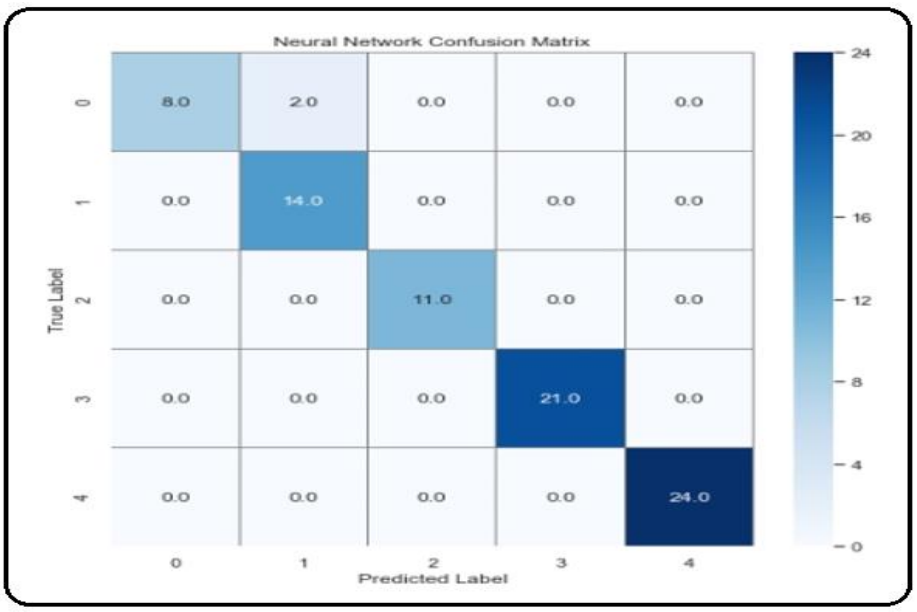

Figure 11. Confusion Matrix for ANN

IJBCS
ISSN: 2147-1428

Original Article

International Journal of Basic and Clinical Studies (IJBCS)
2019; 8(1): 23-36 Veranyurt O.

As can be seen in Figure 11, in both test studies ANN is capable of generating an ignorable number of false positives.

Conclusion

Network layer DOS/DDOS attacks can be simulated in with many different approaches and results can produce debatable results through ML, however with this study we wanted to highlight the achievability of Network layer DOS/DDOS detection through AI. With the results we derived from this study, it can be argued that the success in the attack detection lies in the correct algorithm selection and usage of proper input classes. In Today's security world, the biggest challenge is the zero-day attacks that are not detected through signature based IDS software/appliances. With the usage of AI for traffic anomaly detection, this risk is a challenge that can be mitigated.

References

1. M. Idhammad, K. Afdel and M. Belouch, "DoS Detection Method based on Artificial Neural," *International Journal of Advanced Computer Science and Applications,* pp. 465-471, 2017.
2. M. Suresh and R. Anitha, "Evaluating Machine Learning Algorithms for Detecting DDoS
Attacks," *Springer-Verlag Berlin Heidelberg* , 2011.
3. "DDOS Attack Types," (Online). Available: https://cwatch.comodo.com/ddos-attack-types.php.
4. "What is a Smurf Attack?," (Online). Available: https://usa.kaspersky.com/resource-center/definitions/smurf-attack.
5. K. 9. Dataset, "KDD Cup 1999 Data," (Online). Available: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.
6. M. Ahmed, A. N. Mahmood and J. Hu, "A survey of network anomaly detection techniques," *Journal of Network and Computer Applications,* pp. 20-29, 2016.
7. S. Ray, "6 Easy Steps to Learn Naive Bayes Algorithm," September 2017. (Online). Available: https://www.analyticsvidhya.com/blog/2017/09/naive-bayes-explained/.
8. N. Donges, "The Random Forest Algorithm," 22 February 2018. (Online). Available: https://towardsdatascience.com/the-random-forest-algorithm-d457d499ffcd.
9. M. Zamani and M. Movahedi, *Machine Learning Techniques,* Department of Computer
Science, University of New Mexico, 2015.