# DDOS ATTACK USING MACHINE LEARNING TECHNIQUES

## DOMAIN:MACHINE LEARNING AND NETWORK SECURITY


Mentor:Arun N(H.O.D )

NAME: Utpal Balse
BRANCH:Information Science *and Engineering* USN:18BTRIS051

NAME: Purvasha Padhy
BRANCH: Information *Science and Engineering* USN:18BTRIS031

NAME: Rakesh C S
BRANCH: Information Science *and Engineering* USN:18BTRIS033



***Abstract*** *- The definition of a Distributed Denial Of Service(DDoS) are requests sent to many computer systems or servers computer systems or servers over multiple targets, causing a flood of incoming requests which corrupts the system, causing it to shut down or become inactive. DDoS challenges the CIA triad(Confidentiality, Integrity, Availability).*

*We want to create a system which uses a machine learning based implementation to detect and classify common types of network traffic flows. We will be examining multiple different sources of datasets which have a mixture of various modern types of attacks. We will be using machine learning tools to train the model to classify DDoS attacks and apply algorithms to produce our desired results. In this project , we put up with a DDoS attack detection system on the source of the operating system, based on machine learning techniques. This system comes up with statistical data from the Operating system environment to the virtual machines, to prevent different network routes from withdrawing out from the network. We evaluate diverse machine learning algorithms and carefully compare their performance.*


## INTRODUCTION

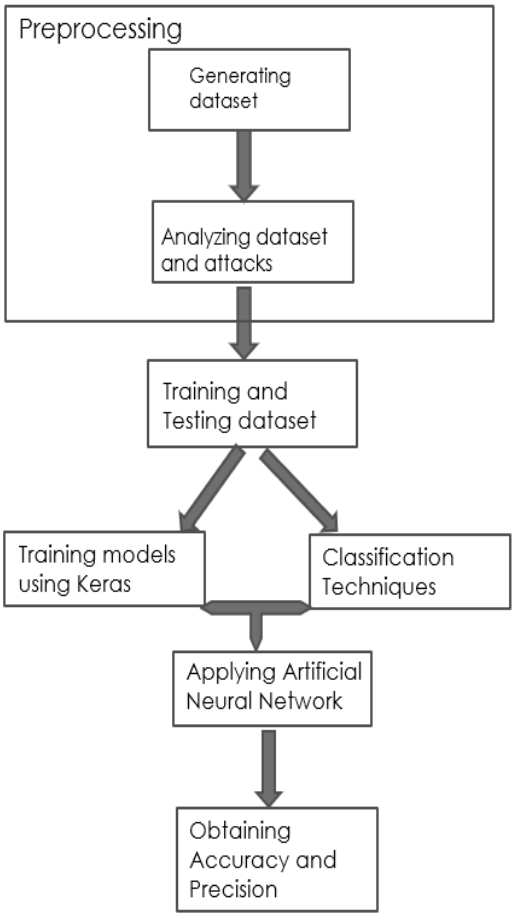
DoS and DDoS assaults are currently a big danger to the Internet. This threat, in the form of Internet availability, is a major issue that is impeding the growth of online businesses, which rely on their websites being accessible to users.In this paper we analyze some of the major Dos/DDos attacks using the traffic analyser, wireshark and discuss the efficient machine learning algorithms to find the patterns. We use these patterns to identify if certain network traffic is a DDoS attack or not. The definition of a Distributed Denial Of Service(DDoS) attack is where many attacks are targeted by a malicious hacker who intends to compromise systems by sending multiple requests to the server causing a server to be entirely unresponsive or shutdown.

A Denial of Service (DoS) assault, on the other hand, often entails a significantly lower volume of traffic, coming from a single source one device DDoS puts the CIA (Confidentiality, Integrity, and Availability) triad to the test.We want to create a system which uses a machine learning based approach on determining and to find out what type of an attack has occurred to a particular system. We will be examining multiple different sources of datasets which have a mixture of various modern types of attacks. We will be using machine learning tools to train the model to classify DDoS attacks and apply algorithms to produce our desired results.

## Methodology

Our research is mainly composed of DDoS detection using machine learning by implementation of ANN(Artificial Neural Network). Problem: Context of the problem is finding multiple methods in order to reduce large amounts of multi data and to determine common attacks. Solution: literature survey provided us with many machine learning techniques in order to Dimensionally reduce data. Most promising results were registered by an algorithm called ANN. The expansion of ANN is Artificial Neural Networks which will include systematic steps in order to train, test and find data accuracy

DATASET GENERATION




New dataset is generated because there is no providing data sets that contain a modern Attack such as (SIDDOS, HTTP Flood), other data sets may include a high amount of duplicate and differential records, and that may bring out negative results .some of the few attacks generated via traffic control are (UDP,SYN,DNS,FIN) floods.

Analyze the current state of existing intrusion detection datasets, including characteristics and smal results. Collect and process open DDoS datasets from reliable sources and review them based on their qualities and features. Use suitable machine learning algorithms to guide the datasets and build appropriate training models by labeling training purposes according to the type of network traffic, maliciou..In this paper we Train, authenticate, test almost every dataset using machine learning algorithms and generate results.Analyze the intrusion detection performance of each dataset based on their respective results.

## Volume and Class Distribution

Each data set represents multiple data inside it so it can be in form of information of binary values it holds in the status of records each particular attack has a large portion of records data to be used in order to apply the machine learning algorithms the distribution of records of the data are given below in a volume of records.

DATASETS NO OF RECORDS

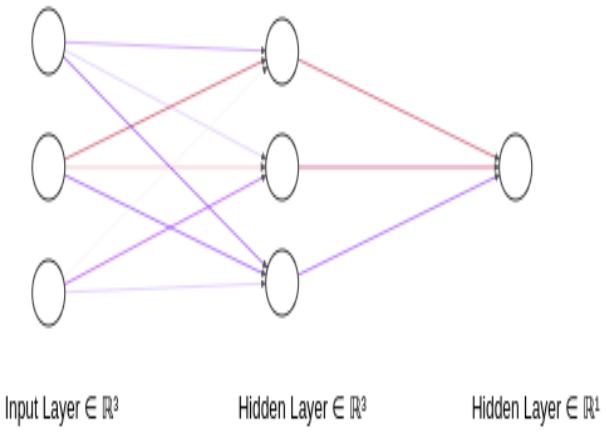
| | |
|---|---|
| Wednesday_0600 | 10,000 |
| Wednesday_0601 | 10,000 |
| Wednesday_0602 | 10,000 |
| Wednesday_0603 | 10,000 |

## Classification/Modeling

To carry out analyzing the dataset we can use different types of machine learning algorithms to train our and implicate our dataset and also to test the precision and accuracy of the data set using tools Machine learning techniques to analyze and detect attacks like Random Forest, ANN ,Logistic Regression, Na¨ıve Bayes, SVM, Perceptron) can be used but since ur approach is to imitate human intelligence data we use a modeling called Artificial Neural network to identify train and test data.

## USECASE

(ANN) generally known as an artificial neural network.Which is general subset of machine learning algorithms which will constitute under Deep Learning.The process involves mainly Extract info from pcap files.Preprocess data for machine learning model.Rigorous training and testing of models on a regular time interval use trained models to identify attacks over a cluster of supported nodes across a network



**H/W & S/W COMPONENTS USED**

Hardware used for creating dataset:A workstation laptop with 16GB Ram, 3gb graphic card

I7 10th gen

Good Network Connection

Software used:

VMware to run multiple virtual machines.

2 kali linux vm's, where one was an attacker machine and one was a victim machine which was used to capture the packets.In the kali attacking machine, we used hping3, which is a packet generation program which was used to simulate attacks and send the network requests to the victim machine.Tshark and wireshark to capture incoming and outgoing packets inthe victim vm and convert it into csv so that it can be processed and worked on as a dataset.Python ide is used to process the captured dataset to implement theANN algorithm Hardware used for creating dataset. A workstation laptop with 16GB Ram, 2gb graphic cardI7 10th processor

Software used:

VMware to run multiple virtual machines.2 kali linux vm's, where one was an attacker machine and one was a victim machine which was used to capture the packets. In the kali attacking machine, we used hping3, which is a packet generation program which was used to simulate attacks and send the network requests to the victim machine.Tshark and wireshark to capture incoming and outgoing packets in the victim vm and convert it into csv so that it can be processed and worked on as a dataset.Python ide is used to process the captured dataset to implement the ANN algorithm.

# Conclusion

This project represents a way of handling DDOS attacks using Machine Learning Algorithm using Intrusion System.We bring out to use ANN to improve the accuracy and establish a way identifying attacks using regression methods still more work is to be done a sample description of providing a general systematic way of evaluating ddos attack is described here. In the future we tend to establish more research for this dedicated project and bring out more effective results and Accuracy in Detecting DDOS attacks.

# References


1]Aggarwal, P., & Sharma, S. K. (2015).Analysis of KDD dataset attributes: Class wis for intrusion detection. In the 3rd *international conference on recent trends in computing 2015 (ICRTC-2015), procedia computer science* (vol. 57, pp. 842–851).

2. handola, V., Banerjee, A., & Kumar, V. (2009a). Anomaly detection: A survey. *ACM Computing Surveys, 41*(3), 1–72.

3. Dickerson, J. E., & Dickerson, J. A. (2000). Fuzzy Network profiling for intrusion detection. In *PeachFuzz 2000. 19th international conference of the North American fuzzy information processing society— NAFIPS (cat. no. 00TH8500), Atlanta, GA* (pp. 301–306). https://doi.org/10.1109/ nafips.2000.877441.

4. MouhammdAlkasassbeh et al, Detecting Distributed Denial of Service Attacks Using Data Mining Techniques, )international Journal of Advanced Computer Science and application, Vol. 7,Issue 1, pp. 436-445, January 2016.

5. Niharika Sharma, Amit Mahajan, Vibhakar Mansotra, )identification and analysis of DoS attackUsing DataAnalysis tools, )international Journal of
)innovative Research in Computer and Communication Engineering, Vol. , )ssue ,pp. -11375, June 2016.

6. D. Anstee, C. F. Chui, P. Bowen, and G. Sockrider, Worldwide Infrastructure Security Report,Arbor Networks Inc., Westford,

MA, USA, 2017.

7. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: a survey on enabling technologies, protocols, and applications,"IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347–2376, 2015e

8. Prajakta Solankar1, Prof. Subhash Pingale2, Prof. Ranjeetsingh Parihar¸,dzDenial of Service Attack andClassification Techniques for Attack Detection,dz (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (2) , pp 1096-1099, 2015.