A Review Paper on DDoS Detection Using Machine Learning

Diksha Sharma
Computer Science Department
Chandigarh University
Chandigrah,Punjab
dikshagaur036@gmail.com

***Abstract* - There is almost no place in the world today that is not connected to the internet. One of the most widely used technologies is the IOT, which allows millions of devices to be connected through the internet. As this technology grows, DoS/DDoS attacks are the most common and dangerous threats. DDoS attacks are becoming more complex and they are becoming almost impossible to detect. Distributed denial of service is a subclass of denial of service. In the order to prevent DDoS attacks, many types of research have been conducted. Machine learning and deep learning are commonly used to prevent DDoS attacks. This paper describes different attack types, such as layer attacks. In this paper, we carried out a comparative analysis of machine learning algorithms to discover and classify DDoS attacks. A study of the effectiveness of detecting DoS/DDoS attacks in networks has been conducted.**

Keywords : DDOS , ML , SVM

I. INTRODUCTION

DDoS is a server attack whose primary objective is to stop authorised users from accessing the source. In this case the security of linked devices increases. Hackers may target personal information and data that protects users from unauthorised changes [1]. Attacks and distributed denial of service attacks, hardware tempering and message suspension. DDoS attacks are a unique malware that the attacker installs to locate tools with vulnerabilities in the network. The impact of the assault in large part depends on the duration through which service is suspended and the scale of the assault. A massive amount of bots offer pc the energy to increase high equipment to carry out malicious activities just as the spread of spam emails, viruses, click-on fraud and so on. It is essential to make a smart detection of this assault through the usage of machine learning techniques. Machine learning has made an incredible development in current years in detecting DDoS attacks. Machine learning techniques that can detect the maliciousness of the packets are used to combat various sorts of DDoS attacks detection has been demonstrated using machine learning approaches such as knn, decision trees and random forests.

These machines contain infected computers and other devices that can be remotely controlled by an attacker. An individual bot is called a bot or a zombie, while a group of bots is called a botnet. An attacker can set up a botnet and then send remote instructions to each bot to direct an attack. Bots send requests to the IP address of a victim's server or network when they are targeted by the botnet, resulting in an overload of the servers or networks, resulting in an interruption in normal traffic.

A. Denial of service attacks.

Denial of service is an attempt to make a website or application unusable by users, for example by flooding it with too much network traffic. Attackers interfere with legitimate user access using various techniques that consume a lot of network bandwidth or other resources. In the simplest form an attacker uses someone to perform a DOS attack on a target as shown in the following figure.

B. Distributed denial of service attacks.

In a Distributed Denial of Service (DDOS) attack, an attacker uses multiple resources to lunch an attack on a target. These resources can include distributed clusters of infected computers ,routers IOT devices and other endpoints . the image below shown the host network participating in the attack , creating a flood of packets or requests to bypass the target.

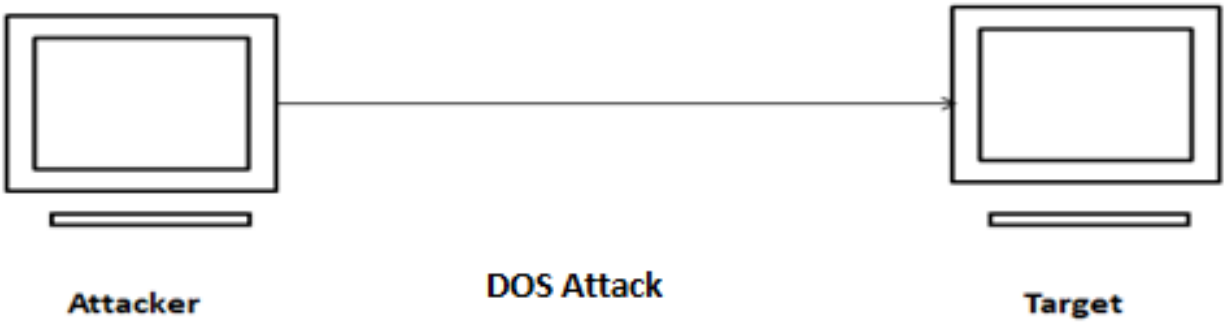

Fig. 1. Denial of service attacks

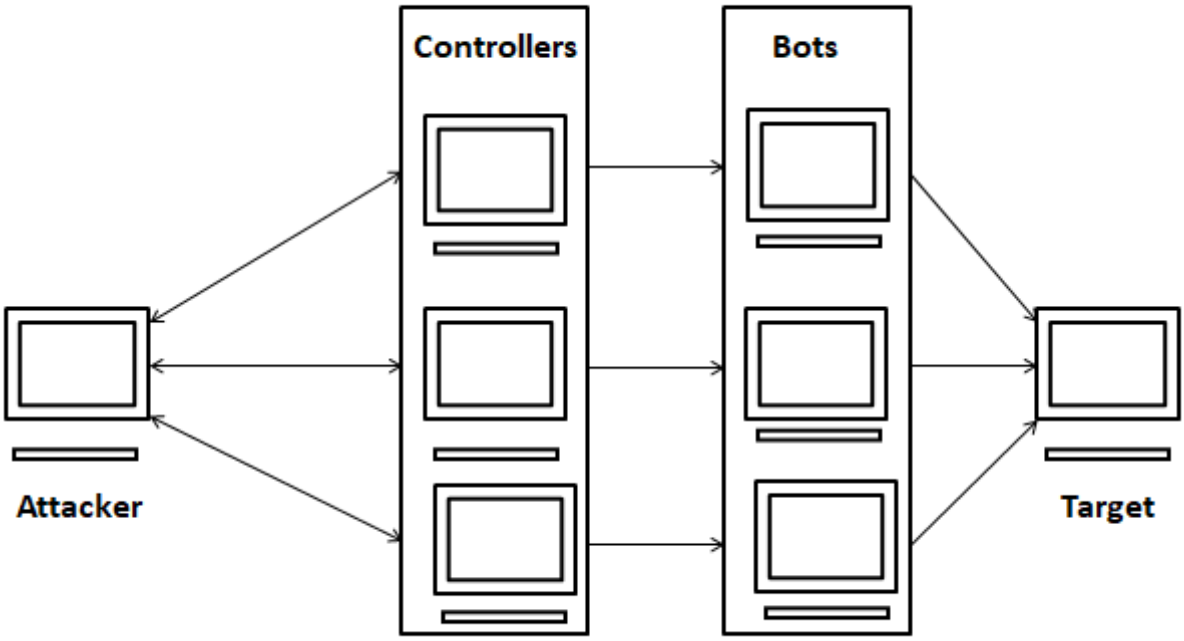

Fig. 2. Distributed denial of service attacks

There are seven layers in the open system interconnection OSI model. DDoS attacks are most common at layers there, four, six and seven.

Layer 3 and 4 attacks correspond to the network and transport layers of the OSI model. These collectively as infrastructure layer attacks.

Layers 6 and 7 correspond to the presentation and application layers of the OSI model. These layers together as an application layer attack.

DOS and DDOS attacks can be divided into three types:

1) Application layer attacks

The attacker's goal in these attacks is to undermine the target server, causing a denial of service. As the server often loads multiple files and runs database queries to create a web page, a single HTTP request can be computationally cheap on the client side but costly for the server to respond to.

2) Protocol attacks

Protocol attacks, also known as state exhaustion attacks, overuse server resources and network equipment like firewalls and load balancers, causing service disruptions.

3) Volumetric attacks

This category of attack attempts to create congestion by consuming all available bandwidth between the target and the larger internet. Large amounts of data are sent to a target by using a form of amplification or another means of creating massive traffic, such as requests from a botnet.

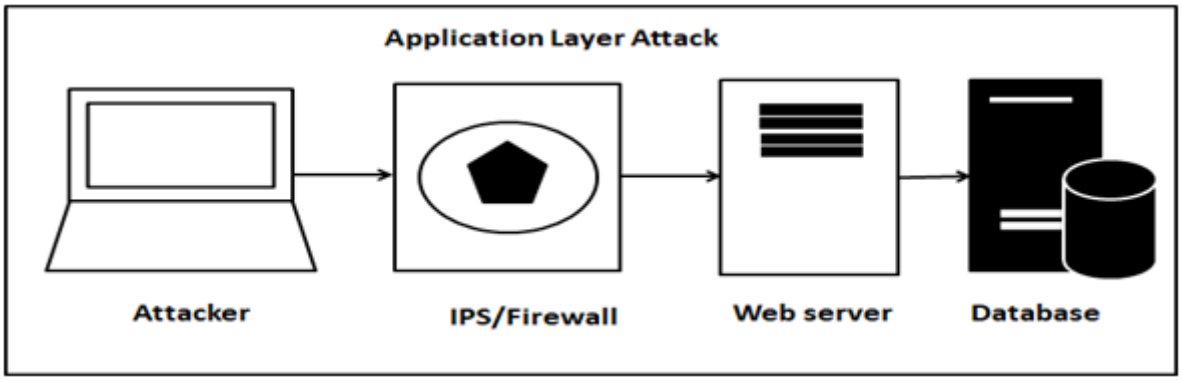

Fig. 3. Application layer attacks

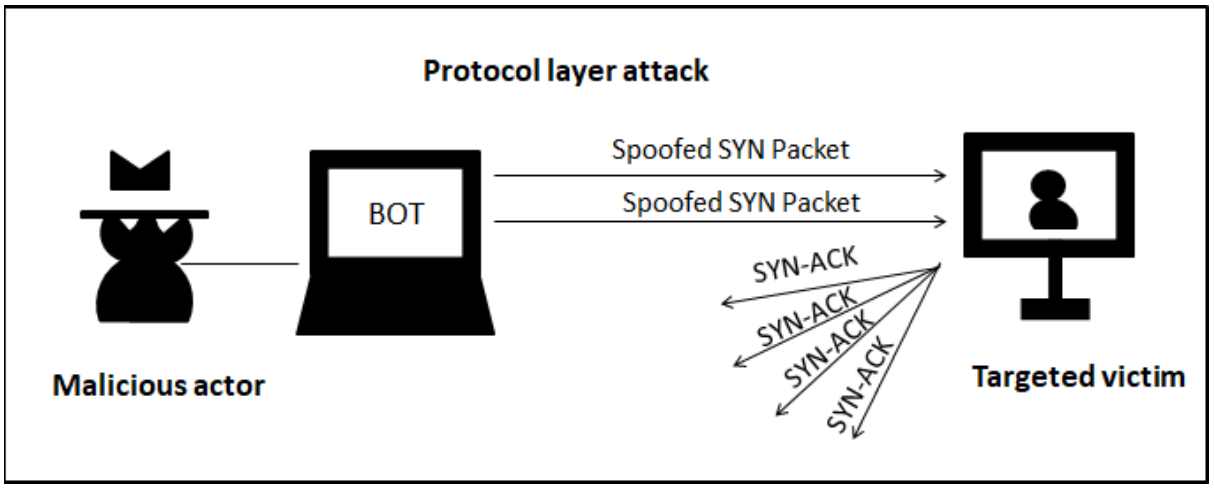

Fig. 4. Protocol attacks

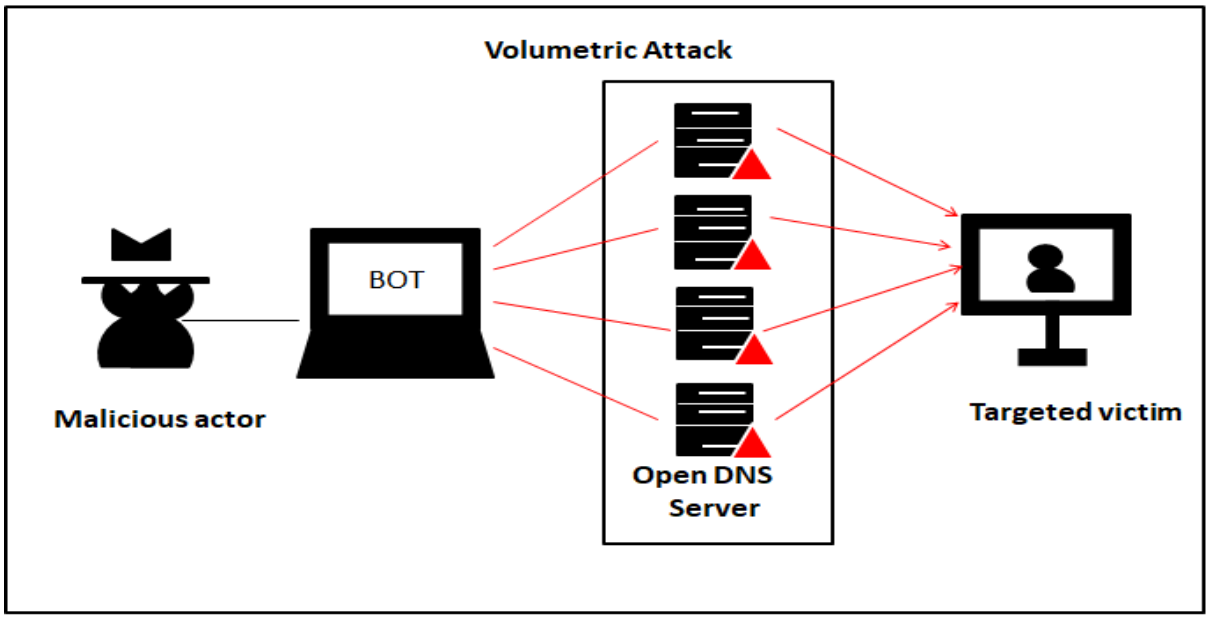

Fig. 5. Volumetric attacks

II. LITERATURE REVIEW

Ancy Sherin Jose et al.[2]it is assumed that open flow will allow sdn to collect flow data from which derived features can be obtained. Additionally, they declared that a dataset of simulated networks was used to accomplish DDoS categorization. Experimental characteristics are used for assessment to better understand and categorise DDoS. They used 7 properties from group 3 and attained a 99.999% total accuracy. They identified the top two characteristics that help us identify DDoS attacks. The attributes utilized can be used to build a simple multistage classification model.

Nisha Ahuja and colleagues.[7] The management, centralization and direction of traffic between hosts are referred to as software-defined networking (sdn). The model and mininet emulator is created using the sdn dataset. In these research works, the author combined random forest and support vector machine (SVM) to classify traffic using svc findings and random forest filtering. The class is accurate in many situations as seen by the model's 98.8 per cent accuracy and 98.27 percent precision. According to the accuracy, the detection was carried out without traffic control.

Sara abdalelah abbas.[10] reduce the number of features used in training. They also use a lot of machine learning to train models. They got 99 points. 97% accurate using the best machine learning techniques.

Jiangtao Pei et al. [5] they carried out local attacks in their study using a DDoS attack program. The packet capture tool analyses the capture attack in comparison to regular packets finds the data attack laws and then transforms it into data attack attributes. To identify the DDoS attack machine learning used the random forest approach. To conduct the characteristics on a large scale, it first extracts the feature and converts the format. The random forest algorithm which recognizes the DDoS attack receives these collected features.

III. IDENTIFICATION OF DDOS ATTACKS

As DDOS can cause a service to become slow suddenly, further investigation may be necessary. This is because other factors such as a legitimate spike in traffic can create similar

performance problems. DDOS attacks can be detected using tools that analyse traffic.

.Malicious traffic from a single IP address or range.

The vulnerability results from shared user behaviour such as device type ,location or browser version.

A request that rapidly advances to one page to the end of

An event that causes an abnormal result, such as a butt.

Follow these four simple steps to scan your network for IP addresses in use

simple ip scaning: operating systems like windows and linux come with simple communication protocols.

Commonds such as “ipconfig” , “arp –a” or “ping” provide easy scaning and troubleshooting.

Ipconfig – This commond displays all network settings assigned to one or more adapters on the computer. You can view information such as IP subnets and gateways.

Arp –a –When you issue the “arp –a” command,ypu gets the Mac identification and IP address type for all devices on the network.

Ping – it helps to identify the connection between two devices and find the ip address of the hostname.

IV. COMMON TYPES OF DDOS ATTACKS

In a network connection on the internet, there are many different layers or components. Each layer has its purpose, just like how a house is built from the ground up.

TCP flood: Attacks that use TCP flooding exploit a flaw in its three-way handshake to drain the target's resources.

Syn Flood: When an attacker sends a series of syn packets to each target's port while pretending to be that target's IP address, they are considered a syn flood.

UDP flood: The attacker attacks a target with packets using the user datagram protocol in an attempt to denial of service. As part of the assault, a random port will be overloaded on a nearby machine. This will cause the host to frequently check if there is an active programme listening on that port. If not, it will send an ICMP "destination unreachable" message.

ICMP flood: Ping flood is a type of denial-of-service attack where the attacker floods the target with echo requests through the Internet control message protocol.

HTTP flood: An HTTP flood occurs when an attacker sends a large number of requests to the targeted server.

DNS flood: A DDOS attack that involves flooding the DNS servers for a domain so that the domain's resource records cannot be resolved is known as a "DNS flood".

V. MITIGATING A DDOS ATTACK

1. Detection- to stop a distributed attack, a website needs to be able to distinguish an attack from a high volume of normal traffic. If a product announcement has a website swamped with legitimate new visitors, the last thing the site wants to do is stop them from viewing the content of the website.
2. Response- in this step, the DDOS protection network responds to an incoming identified threat by intelligently dropping malicious bot traffic and absorbing the rest of the traffic.
3. Routing- by intelligently routing traffic, an effective DDOS mitigation solution will break the reaming traffic into manageable chunks preventing denial of service.
4. Adaption- good network analyses traffic for patterns such as repeating offending IP blocks, and particular protocols being used improperly.

VI. CONCLUSION

Distributed denial of service attacks will continue to represent the greatest threat to many large and small enterprises since they harm internet users in a variety of ways. the sectors that might require human interference, complex calculations and a lack of free-to-access data. To detect a DDoS assault, however, many areas need attention. To detect DDOS attacks a variety of algorithms like liner regression, random forest, support vector machine and naïve bayes classifier are utilised. Convolution neural networks are used in DDoS attack detection and deep learning also plays a significant role in this process. So, we have reviewed the many methods of identifying DDoS attacks.

REFERENCES:

[1] Tejaswini Ulemale, Review on Detection of DDOS Attack using Machine Learning, 2022

[2] Dutta Sai Eswari1, P.V.Lakshmi, A Survey On Detection Of DDoS Attacks Using Machine Learning Approaches, Turkish Journal of Computer and Mathematics Education, 2021.

[3] Ancy Sherin Jose, Latha R Nair2, Varghese Paul. Towards Detecting Flooding DDOS Attacks over Software Defined Networks Using Machine Learning Techniques published in Genetic 2021

[4] Pande, S., Khamparia, A. & Gupta, D. Feature selection and comparison of classification algorithms for wireless sensor networks. J Ambient Intel Human Compute (2021).

[5] Parvinder Singh Saini, Sajal Bhatia, Sunny Behal. Detection of DDoS attack using machine learning algorithms published in research gate in March 2020.

[6] Jiangtao Pei, Yunli Chen, Wei Ji." A DDoS Attack Detection Method Based on Machine Learning" published in ICSP 2019.

[7] Chin-Shiuh Shieh, Wan-Wei Lin, Thanh-Tuan Nguyen, Chi-Hong Chen, Mong-Fong Horng and Denis Miu. Detection of Unknown DDoS Attacks with Deep Learning and Gaussian Mixture Model, IEEE ICICT 2021.

[8] Nisha Ahuja, Gaurav Singal, Debajyoti Mukhopadhyay, Neeraj Kumar. Automated DDOS attack detection in software-defined networking published in Science Direct 2021.

[9] Alzahrani, R.J.; Alzahrani, A. Security Analysis of DDoS Attacks Using Machine Learning Algorithms in Networks Traffic.

[10] Pheeha Machaka, Olasupo Ajayi, Hloniphani Maluleke, Ferdinand Kahenga, Antoine Bagula, Kyandoghere Kyamakya, Modelling DDoS Attacks in iot Networks using Machine Learning,2021.

[11] Sara Abdalelah Abbas, Mahdi S. Almhanna, Distributed Denial of Service attacks detection System by Machine Learning Based on Dimensionality Reduction, Icmaict 2020.

[12] Swathi Sambangi and Lakshmeeswari Gondi."A Machine Learning Approach for DDoS (Distributed Denial of Service) Attack Detection Using Multiple Linear Regression" published on 25 December 2020.

[13] Alzahrani, R.J.; Alzahrani, A. Security Analysis of DDoS Attacks Using Machine Learning Algorithms in Networks Traffic. Electronics 2021, 10, 2919.https://doi.org/10.3390/electronics10232919.