A Survey On Detection Of Ddos Attacks Using Machine Learning Approaches

Dutta Sai Eswari[1], P.V.Lakshmi[2]
[1]Assistant Professor,Department of Computer Science & Engineering Keshav Memorial Institute of Technology, Narayanaguda,Hyderabad. TelanganaIndia
[2]Senior Professor,Department of Computer Science & Engineering GITAM University, Visakhapatnam Andhra PradeshIndia
[1]saieswari3@gmail.com, [2]vpanga@gitam.edu

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 10 May 2021

Abstract: Distributed Denial of service (DDoS) attack is also referred as Distributed Network attack. In network security, This attack is very dangerous. DDoS attack stops the all essential services of different online applications. The traditional Internet services of architecture is unsafe to DDoS attacks and the collection of internet connected devices affected by the malwares, then it allows the intruders to control all the internet connected devices is a Botnet or attacked networks. In Botnet, one disadvantage is that if the Botnet is set up then the intruder creates the large scale networks to attack against one or more victims. In this paper, We have surveyed discrete types of machine learning approaches used to detect the DDoS attacks. These attacks are increasing everyday and have become more complicated. Hence it has become difficult to detect these attacks and secure online services from these attacks. So, it is very arduous to spot DDoS attack. Finally, this review paper describes the classification methods for DDoS attacks using machine learning approaches.

Keywords: Machine Learning, Distributed Denial of Service (DDoS) Attack, Botnet, Naïve Bayes, Fuzzy logic.

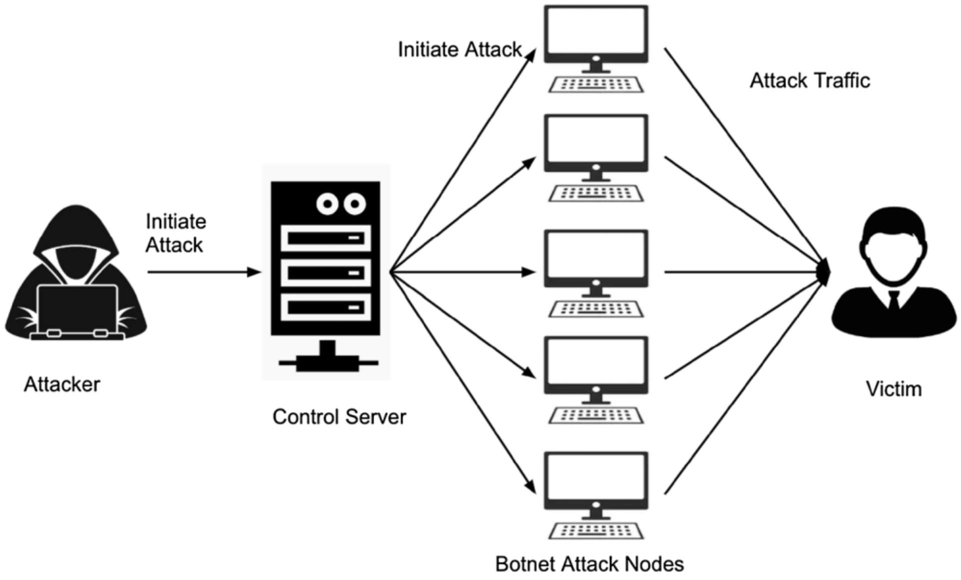
1. Introduction

Recently, Distributed Denial of Service (DDoS) attacks have acquired enormous money related adversities to trade and governance all over the world, as appeared in Worldwide Infrastructure Security Report [1]. In most Internet conditions, gadgets help out applications that run by thought on the affiliation, which interfaces with hazardous experts to see responsibility concerning contraptions. Appropriately, it is reachable to have the impedance of affiliations or the utilization of contraptions as a starting inspiration driving attacks for different region, similar to the event of the DDoS attacks [2], which has been accumulated for various considerations, for example, (I) straightforwardness and office of execution, not needing enormous unequivocal data on the aggressor side, and (ii) arrangement of stages and operations for related attack union. Possibly the most hazardous malevolent traffic on the web is the DDoS volumetric attack, which is in hazard for over 65% of aforesaid attacks [3]. In a volumetric DDoS, a couple of aggressors arrange the sending of a high speed of pointless information attempting to over-bother the disasters figuring resources or the close by association joins. As shown by one perspective, the high achievement rates for such an attack happen pondering when the distracted Internet switches reliably utilize the FIFO (First-In-First-Out) and DROP-TAIL lining areas. Solid traffic is besides destroyed [3]. Intensely hot clear domain and control of DDoS attacks has gotten earnestly testing as aggressors keep utilizing novel techniques to dispatch DDoS attacks [4]. The ever-increasing number of DDoS attacks, concurred with making gathering in their sorts, generating bad effect, has undertaken DDoS attack Detection, disavowal, and help the foremost need.

A Distributed Denial of Service (DDoS) attack [5,6] is a huge growth, associated with attack on the strategy of relationship of a maddening turn of events or network resources, dispatched by suggestion through unlimited coordinated PCs on the web. Going prior to implementing an attack the assailant undertakes command over giant uncountable PC machines over the web and these PCs are frail machines. The assailant abuses these PCs deficiencies by embedding harmful code or other different hacking strategy so that he could easily overpower them. These delicate or bargained machines conceivably scands in numbers and these are expectedly named as 'zombies.' The gathering of zombies when in doubt spread out the 'Botnet.' The scale of the attack relies upon the size of the Botnet, for clearer Botnet, attack is ensured greater and shocking. DDoS attacks within the Internet may be dispatched with the usage of two huge strategies. In the key strategy the attacker ship a few risky packs to the trouble to stupefy a show or a software strolling on it. The Second method from an overall perspective joins the network/transport-level/application-level flooding attacks [7], wherein an assailant do each going with: (i) interfere with an authentic customer's straightforwardness by exhausting exchange speed, network resources or switch supervising cutoff or (ii) upset relationship of an ensured clients by obliterating the master assets, as an example, CPU, memory, plate/database record transmission and I/O move pace. Nowadays, DDoS attacks are reliably dispatched through competent, by suggestion controlled, and all around included Zombies or Botnet PCs of an network, which are never-endingly or concurrently sending a massive degree of traffic or association alluding to the goal plan. The attack consequences the goal configuration either react powerfully or abend absolutely [7], [8], [9]. Zombies of a Botnet are normally picked utilizing Trojan horses, worms, or discretionary segments [10], [11].

It is exceptionally hard for the protect portion to see the genuine attacker considering the utilization of sign IP addresses by zombies immensely influenced by the attacker with Botnet [12].

In Figure 1, depicted as, the attacker assistants with control server to make the control and dominate the design. The control server has stacks of resources and which is an amazing trained server, the control cut off may contains the different form like memory, bandwidth and processing power. Regardless of taking the commands from the attacker, the middle people, furthermore referred to as Agents are liable for looking through Botnets. They send instructions identified with models and amend the same to the Botnets. In this, the owner makes the undermined frameworks for the malwares introduced on their PCs on the off chance that they are one of the parts in the Botnets. Always attackers utilize the specialists as work locale leaps to begins the attacks against the target systems (victims) [13]. Therefore, this is required to locate the Botnet DDoS attacks to intrude with the designs of several assets from being crushed. Machine Learning methods when presented to information are in shape for adjusting autonomously and gaining from prior calculations to decipher the accessible information for recognizing hidden patterns.



2. Literature survey

This part gives the literature survey of Machine Learning approaches used especially in detection of DDoS attacks such as Naïve Bayes, Artificial Neural Networks, Fuzzy Logic, Decision tree and Support Vector Machine are made with their interrelated works have been covered.

1. Naïve Bayes:

The Machine Learning approach belongs to a basic probabilistic classifier [14]. This is [15] used to detect the authority and to manage IRC traffic based on Botnets. So this approach identifies IRC and non-IRC traffic by differentiating the presentation of J48, Bayesian network and Naïve Bayes. In this paper[15],author identify the features that gives enhanced accuracy. This classifier obtains mutually false positive (15.04%) and low false negative (2.49%) for real time low false negative (7.89%) rates and IRC/non-IRC flows used for Botnets experienced on IRC flows proves Naïve Bayes to be an professional classifier. In [16] the proposed approach is hierarchical layered used to attacks of detection rate.

2. Fuzzy Logic:

Fuzzy Logic techniques are primarily used by Anomaly detection. A prediction and detection approach was planned [17] against DDoS attacks using Fuzzy logic in IEEE 802.15.4. Fuzzy Logic based prediction and detection approach helped in DDoS attack detection by contrasting the consumption of energy used for sensor nodes. These nodes are recognized as a malicious attacker by considering the abnormal energy consumption.

3. Support Vector Machine:

Which is the most popular and frequent approach. In this approach[18] using RTS and SVM organized an research to detect DDoS attacks. Preprocessing of the packet data that was obtained primarily from the network was done by the RST. SVM model is fed with the quality set preferred by the RST to study and analysis correspondingly. RST and SMV could decrease false positives rates when outcomes are compared with PCA(Principal component analysis),therefore increasing the accuracy.

4. Artificial Neural Networks:

Artificial Neural Networks are used processing elements to exchange a set of input to a set of outputs whose functionality is similar to the biological nervous systems like a human brain. In this approach [19] “RBF-NN detector” used 9 packet parameter with the relevant parameters are calculated by these frequencies. Which were expected depending on the frequencies, classifies the RBF-NN traffic as normal class otherwise whether it is an attack class**.** Distributed Time Delay Neural Network (DTDNN)[20] has huge chances of detecting attacks with improved accuracy. Classification of data with fast exchange rates and also with high speeds completed by DTDNN.

5. Decision Tree:

Many investigates were completed on decision tree analytical advance to identify the DDoS attack. In this method [21], the decision tree traces back the attacker's position after an attack is detected using a traffic-flow model matching technique. For detection of DDOS attacks a C.45 classifier is used. Author in [22] finds out a technique in which the DDoS attack could be professionally detected. Several Machine Learning techniques takes more time to detect the attack or generates low accuracy. In [22] C4.5 algorithm is used and it shows low accuracy and takes greater time to construct the decision tree while algorithm C5.0 is capable as it requires low time and compared memory to the C4.5. A further work is carried out using C4.5, C5.0 and ID3 which makes an better decision tree with reduced error pruning and feature selection[23].Based on the results obtained C5.0 has performed better with accuracy and usage of memory.

3. The classification methods for ddos attacks

The DDoS attacks, being dispersed in nature makes them incredibly unbelievable to fight or trace back mechanism. Knowing and seeing all the properties of [24],[25] DDoS attacks is one of the significant steps towards the progress of historic and skilled DDoS defensive mechanism that described the essential for understanding DDoS attack and their impact in cloud environment. Figure 2 illustrates the classification methods for DDoS attacks dependent on the mode, stream, impact and consumption of the attack.

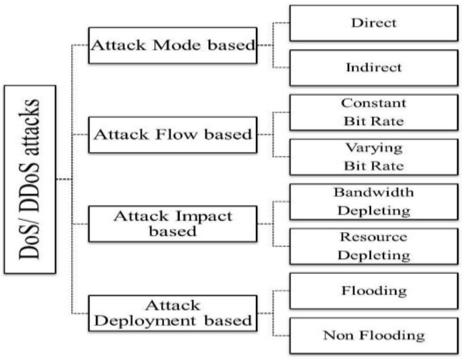


Figure 2: The Classification methods for DDoS Attacks

DDoS have different appearances, but flooding attack, the most outstanding form of DDoS is the guideline purpose of assembly of this research work. The Flooding attack is an attack wherein it covers the network with unnecessary packets, for example either the node may send different packets or the middle point may send the entrancing gatherings which beat its rate limit. A DDoS attack has been mentioned here into two, considering the show level that it attacks and dependent on botnets. Considering the flooding attacks, protocol level could be classified into two categories. 1) Transport/Network level or 2) Application level. In Transport/Network layer, ICMP, DNS, TCP and UDP protocol packets are usually used to launch the attacks. Thinking about the Botnets, DDoS attacks can be classified into attacks because of IRC based botnets and attacks considering internet based Botnets. The following with Figure 3 obviously depicts the classification methods of DDoS flooding attacks.

1. Network /Transport Level Flooding DDoS Attacks

Such forms of attacks are launched utilizing DNS, ICMP, TCP and UDP protocol packets. Here we've got four kinds of attacks on this group.

a. Normal flooding attacks

The association of the legitimate users is the major point of the flooding attacks. Attackers mainly attempt to tire out the victim’s network bandwidth. Illustrations of flooding attacks are VoIP flood, DNS flood, ICMP flood, UDP flood and so on all these flooding can be accomplished either by spoofed or non-spoofed IP addresses.

b. Protocol exploitation flooding attacks

The utilization bugs of a touch of the victim's protocols are the primary agenda here. Attackers use some particular features to consume majority of the victim's resources. Instances of protocol exploitation flooding attacks are RST/FIN flood, ACK& PUSH ACK flood and TCP SYN flood and so on.

c. Reflection-based flooding attacks

Rather than sending direct requirements to the reflectors, attackers traditionally send conveyed ICMP repeat request. Considering that the reflectors will send their reactions to the individual being victim. In this manner, the reflectors exhaust the requirements of the individual being victims. The Models are Smurf and Fragile attacks.

d. Amplification-based flooding attacks

For each message they get, attackers misuse services to make more prominent and different messages to build the traffic towards the individual being victims. Reflection and improvement techniques are consistently utilized by the assistance of Botnets. For instance attackers send spoofed requests to vast number of reflectors in smurf attack, which is the reflection and this is finished by mauling IP broadcast feature of the groups and that is the expansion. The entire of the above kinds of attack were introduced in [26], [27], [28].

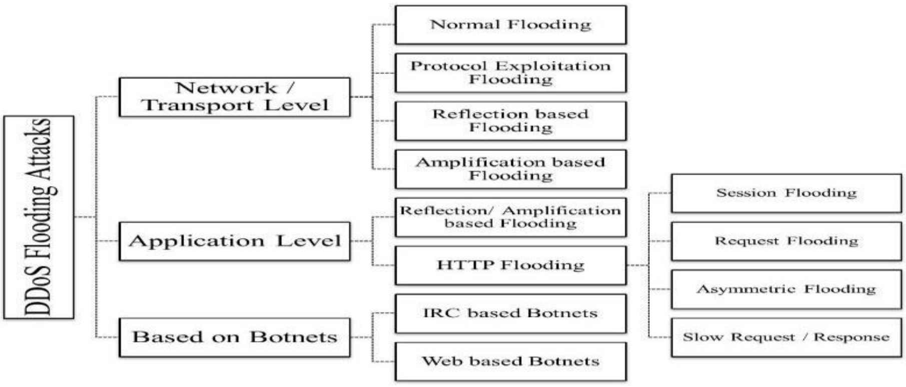


Figure 3. Classification of DDoS Flooding Attacks

2. Application Level DDoS Flooding Attacks

Upsetting valid user's facilities with killing the server services includes CPU, memory, I/O bandwidth, Sockets and disk bandwidth is the center of application level DDoS attacks. Being like to legitimate traffic, they are stealthier than numerous attacks. Due to the fact that the application layer attacks target the Hypertext Transfer Protocol (HTTP) or Session Initiation Protocol (SIP), DNS they typically contains the same collision to the resources. Now, SIP flooding attacks and DNS amplification flooding attacks are briefly described like the two well-known application level flooding attacks in this group exploiting DNS as well as SIP protocols.

a. Reflection/Amplification based flooding attacks

These types of attacks used to send fake application-level protocol requests. DNS amplification attack used to rent both reflection and amplification techniques. With respect to DNS, reply messages are constantly significantly better than the uncertainty messages. So, the attackers who make a huge amount of network traffic use fake source IP addresses to produce small DNS queries. This generated large quantity of data traffic is goes to the sufferer system to make it partially or completely incapable.

VoIP flooding attack, a new example that uses reflection technique is a difference of UDP flooding. In this, attacks send VoIP packets from fake source IP addresses through SIP at a extremely high rate. The array of the source IP address will also be extremely large. The fake connections use large amount of resources. The victim VoIP server should be able to distinguish authentic and fake VoIP connections. The VoIP flooding will destroy a network with packets from random source IP addresses or even permanent.

b. HTTP flooding attacks

In this category, the subsequent are the four types of attacks.

i. Session flooding attacks

Attackers meeting correlation request rates are higher than the genuine users requests in this kind of attack. This consumes a lot of the server resources and causes flooding attack. In this group, HTTP get/post flooding attack plays most vital role in this category in which a huge number of legal HTTP requests are generated by the attackers in the structure of get/post, to a victim web server. Such an attack is likewise called as extreme VERB and uses non-spoofed IP addresses.

ii. Request flooding attacks

In this group, sessions that include several requests than normal are sent by the attackers. Single-session HTTP get/post flooding attack (also known as excessive VERB Single session) is the famous attack in this category. This is different from the earlier attack and permits different requests in a particular HTTP session using the quality of HTTP 1.1. Therefore attackers can bound the HTTP attack session rate and may keep away from the session rate constraint method of different defense mechanisms.

iii. Asymmetric attacks

Sessions that include high volume requests are sent by attackers.

3. Botnet-Based DDoS Attacks

The most essential mechanisms that enhance DDoS flooding attacks are Botnets. Present days application layer attacks have almost utilized Botnets. A complete introduction of Botnets and tools made utilizing botnets near to the central focuses and preventions are related with the survey [33]. A short study of the planning of Botnet near to tools used to dispatch DDoS flooding attacks is introduced in this part. Progress of a efficient and effective defense mechanism winds up being all the additional testing when attackers use zombies or Botnets.

A Botnet is formed by group of zombies or bots that are managed by means of an attacker. The bots or zombies are called as the Agents and the attacker is also called as the Master of the Botnet. Alongside master and agents, there are controllers in the botnet through which the masters analyze by recommendation with their representatives to ask for and control the network. Figure 4 illustrates the elements of a Botnet during a DDoS attack.

Botnets are developed in different ways. Botnets can be categorized into three major categories like P2P, Web and IRC depends on how bots are restricted by the masters [34], [35].

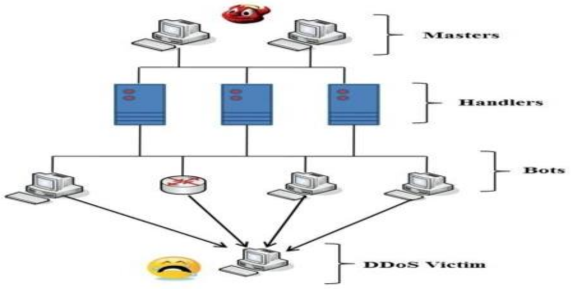


Figure 4: Botnet based DDoS Attack

a. IRC-based Botnets

Internet pass on Chat is a instant online messaging protocol dependent on text. It has customer server design and can interface innumerable customers through different expert servers. Attackers can utilize authentic IRC ports by manhandling IRC channels as controllers to send commands to the bots. For the explanation that IRC servers consistently have huge volume of traffic, an attacker can easily cover his quality and pass on the harmful code through file sharing.

Instead of retaining up the list regionally at their site, attackers can take a look at the rundown of every open bot, by checking into the IRC server. Centralized command and control (C&C) structure restraints the IRC based Botnets and their basic drawbacks is that, servers are the essential issues of dissatisfaction.

b. Web-based Botnets

To launch commands to the bots, Botnets have begun utilizing HTTP as a communication protocol and in this manner it is commonly called HTTP based Botnets. Correspondence through HTTP makes the course towards following back to the command and control structure additionally testing. Not at all like IRC-based Botnets, web based Botnets don't keep up relationship with a command and control server and rather than that each web Bot downloads the principles which sometimes utilizes web demands. Complex PHP scripts are utilized to organize and control web based bots and for correspondence in addition, they use encryption over HTTPS (port 443) or HTTP (port 80) protocol. Web based Botnets are likewise stealthier than IRC based Botnets in nature since they can cover themselves inside legitimate HTTP traffic. Low-Orbit Ion Cannon (LOIC) 4, Dull Energy and Aldi are the three conspicuous and broadly utilized Web-based Botnet tools. The hazardous tool can destroy the attacked hosts, at whatever point needed by affecting the conventionality of all the information on the hard drive.

4. Evolution and Analysis of Various Traceback Methods

In this part, evaluation of various traceback methods is finished on the sources of metrics described in earlier sector and shown in the Table 1 and Table 2. Every scheme is evaluated with the new classification of traceback methods such as Packet logging input debugging, DPM, link testing, PPM, ICMP trackback, reposition and Entropy difference. Its Advantages and Drawbacks has been show in the Table 3.

Category	Link Testing	Control Flooding	ICMP Traceback	Packet Logging
ISP involvement	High	None	Low	Moderate
Range of attack packets wanted for traceback	N-A	Huge	Very large	1
Processing overhead	Low	None	Low	Low
Storage requirement	Low	Low	Low	Fair
Ease of implementation	Yes	Yes	Yes	Yes
Scalability	High	N-A	High	Fair
Bandwidth overhead	High	Huge	Low	None
Number of functions had to enforce the scheme	None	1	2	3
Ability to address most important DDOS attack	Yes	No (only DDoS attack)	Yes	Yes
Classification	IDS based	IDS based	Proactive	IDS assisted

Table 1: Evaluation of Traceback Methods

Category	Traceback using IP-Sec	PPM	Pushback	Traceback using Entropy variation
ISP involvement	High	None	No	No
Range of attack packets wanted for traceback	Fair	Very large	Large	Very large
Processing overhead	High	Low	High	High
Storage requirement	No	High	N-A	Fair
Ease of implementation	Yes	No	Yes	No
Scalability	Poor	High	High	Highest
Bandwidth overhead	High	None	Very Low	High
Number of functions had to enforce the scheme	None	2	2	2
Ability to address most important DDOS attack	No	Poor	Yes	Yes
Classification	IDS assisted	Proactive	Proactive	Proactive

Table 2: Evaluation of Traceback Methods

S.NO	Traceback Methods	Benefits	Drawbacks

1.	Input debugging/ Controlled Flooding with Link Testing [3][14][21][22]	✓ Suitable with accessible protocols ✓ It accepts the incremental execution ✓ Convenient to available routers and network communications ✓ Examination of post packet study is allowed ✓ ISP assistance isn't always essential.	✓ This approach is used for DOS Attacks no longer for DDOS Attacks ✓ This method isn't always feasible for broad operation. ✓ It can’t sketch the attack when it's far ended i.e. attack should wait dynamic til the trace back is concluded. ✓ Bandwidth slide could be very high whilst tracing the attack source. ✓ It obtains regenerated plan of the internet topology.
2.	Traceback for ICMP [12]	✓ Suitable with accessible protocols ✓ This helps the incremental execution. ✓ Permits previous packet study ✓ Not required ISP support ✓ Suitable with network infrastructure and existing routers	✓ It produces additional network traffic by the Bandwidth overhead. ✓ Low defensive as there may be no encryption approach carried out with key allocation.
3.	Detection method DPM/PPM [4][6][7]	✓ This is simply to execute ✓ This has no bandwidth overhead and less processing ✓ It is compatible for a array of attacks not now(D) DoS ✓ It doesn’t have the intrinsic security defects. ✓ It cannot tell internal topologies of the ISPs ✓ This is measurable	✓ Some packets will leave the router without being marked, Since every router marks packets probabilistically ✓ This is also costly to execute this method on behalf of memory overhead ✓ However this supposition is not valid when attack is extremely distributed for example in reflector attacks. One vital supposition for PPM to work is that DOS attack traffic could have larger volume than general standard traffic.
4.	Logging Hashbased Scheme [8]	✓ Suitable with presented protocols ✓ maintain for incremental execution ✓ Permits previous packet study ✓ irrelevant network traffic is suspended ✓ Suitable with network infrastructure and existing routers	✓ Storage requirements and Resource motivation in terms of processing ✓ Allocation of classification information between various ISPs leads to legal issues and logistic ✓ Low appropriate for distributed denial of service attacks
5.	IP Traceback Using IP-Sec [16]	✓ Suitable with accessible protocol ✓ Permits previous packet study ✓ It is secured highly	✓ ISP connection is necessary ✓ Low measurable
6.	Pushback [9][10]	✓ This is simple to execute ✓ It makes use of collective based congestion control algorithm which has been formerly carried out. ✓ Appropriate with network communications and current routers.	✓ Precisely whilst a switch receives a pushback signal, it is going to check and control the aggregate showing up rate from the various links and discover the links which provides to the plug up. Anyhow, this technique is not suitable if the attack traffic is dependably spread throughout the inbound links. ✓ Due to the fact that arriving aggregate rate is comparative in every link, switch can't see the virulent traffic and basic traffic which prompts the problem of fake negative and fake positive in this regard.

7.	Traceback with Disorder form [11]	✓ It executes functions which can be far-flung of intruders to perform IP traceback. ✓ This scheme is measurable ✓ It will not sicken from the packet pollution wrangle ✓ The router level isn't always a trouble at Storage space requirement ✓ This scheme can process as a free software program module with the current routing software which performs satisfactory execution.	✓ The separation of DDOS Attacks and flash crowds are not taken into account in this method, it would see flash crowd as DDOS Attack engaging false positive

Table 3: Benefits and drawbacks of various Traceback Methods

5. Conclusion

In this survey paper, we have surveyed distinct types of machine learning approaches that are used to hit upon the DDoS attacks. We have presented classification methods of different DDoS attacks. We have represented different types of detection and machine learning methods with their benefits and drawbacks primarily based up on when and where they detect and react to DDoS attacks. Lastly, We have represented an evaluation and analysis of various traceback methods such as DPM, input debugging, Packet logging, link testing, PPM, ICMP trackback, reposition and Randomness difference. Basically it is extremely difficult to plan and execute Detection of DDoS. Hence, in real time networks various execution parameters are required to be evaluated against each other smoothly and properly in order to fulfill all the requirements for DDoS detection.

References

1. D. Anstee, C. F. Chui, P. Bowen, and G. Sockrider, Worldwide Infrastructure Security Report, Arbor Networks Inc., Westford, MA, USA, 2017.
2. S. T. Zargar, J. Joshi, and D. Tipper, “A survey of defense mechanisms against distributed denial of service (DDOS) flooding attacks,” IEEE Communications Surveys and Tutorials, vol. 15, no. 4, pp. 2046–2069, 2013.
3. Y. Cao, Y. Gao, R. Tan, Q. Han, and Z. Liu, “Understanding internet DDoS mitigation from academic and industrial perspectives,” IEEE Access, vol. 6, pp. 66641–66648, 2018.
4. Hoque, N., Bhattacharyya, D., Kalita, J.: Botnet in DDoS attacks: trends and challenges. IEEE Commun. Surv. Tutor. 99, 1–1 (2015).
5. P. J. Criscuolo, “Distributed Denial of Service, Tribe Flood Network 2000, and Stacheldraht CIAC-2319,”, Department of Energy Computer Incident Advisory Capability (CIAC), UCRL-ID-136939, Rev. 1., Lawrence Livermore National Laboratory, February 14, 2000.
6. Todd B., “Distributed Denial of Service Attacks,” Feb. 18, 2000, [online] http://www.linuxsecurity. com/resource files/intrusion detection/ ddos–whitepaper.html.
7. J. Mirkovic and P. Reiher, “A taxonomy of DDoS attack and DDoS defense mechanisms,” ACM SIGCOMM Computer Communications Review, vol.34, no. 2, pp. 39-53, April 2004.
8. Ranjan. S, Swaminathan. R, Uysal. M, and Knightly.E, “DDoS-Resilient Scheduling to Counter Application Layer Attacks under Imperfect Detection”, IEEE INFOCOM’06, 2006.
9. Chang R. K. C., “Defending against flooding-based distributed denial of service attacks: A tutorial,”, Computer Journal. IEEE Communication Magazine,Vol. 40, no. 10, pp. 42-51, 2002.
10. Puri. R, “Bots and Botnet – an overview”, Aug. 08, 2003, [online] http://www.giac.org/practical/GSEC/ Ramneek Puri GSEC.eps
11. CERT, “Denial of Service Attacks,” June 4, 2001, [online] http://www.cert.org/tech tips/denial of service.html
12. Liu. J, Xiao. Y, Ghaboosi. K, Deng. H, and J. Zhang, “Botnet: Classification, Attacks, Detection, Tracing, and Preventive Measures,”, EURASIP Journal. Wireless Communications and Networking, vol. 2009, Article ID 692654, 11 pages, 2009.
13. Rodríguez-Gómez RA, Maciá-Fernández G, García-Teodoro P (2013) Survey and taxonomy of Botnet research through life- cycle. ACM Comput Surv (CSUR) 45(4):45.

14. Mouhammd Alkasassbeh IT Department ,Ghazi Al-Naymat ,Ahmad B.A Hassanat ,Mohammad Almseidin,‟ Detecting Distributed Denial of Service Attacks Using Data Mining Techniques,‟ (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 1, 2016.
15. Irfan Sofi, Amit Mahajan, Vibhakar Mansotra ,Machine Learning Techniques used for the Detection and Analysis of Modern Types of DDoS Attacks (IRJET), Vol.04,Issue,06,June2017.
16. Jasreena Kaur Bains ,Kiran Kumar Kaki ,Kapil Sharma,‟ Intrusion Detection System with Multi Layer using Bayesian Networks‟,International Journal of Computer Applications (0975 – 8887) Volume 67– No.5, April 2013.
17. C Balsrengadurali and Dr.S Saraswathi,‟ Fuzzy Based Detection and Prediction of DDoS Attacks in IEEE 802.15.4 Low Rate Wireless Personal Area Network,‟ IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 6, No 1, November 2013.
18. Vipin Das , Vijaya Pathak, Sattvik Sharma, Sreevathsan, MVVNS.Srikanth,Gireesh Kumar T,‟ NETWORK INTRUSION DETECTION SYSTEM BASED ON MACHINE LEARNING ALGORITHMS‟, International Journal of Computer Science & Information Technology (IJCSIT), Vol 2, No 6, December 2010.
19. Gavrilis, Dimitris & Dermatas, Evangelos. (2005). Real-time detection of distributed denial-of-service attacks using RBF networks and statistical features.Computer Networks.48.235-245.10.1016/j.comnet.2004.08.014.
20. L. M. Ibrahim, “Anomaly network intrusion detection system based on distributed time-delay neural network (dtdnn),” Journal of Engineering Science and Technology, vol. 5, no. 4, pp. 457–471, 2010.
21. Yi-Chi Wu, Huei-Ru Tseng, Wuu Yang and Rong-Hong Jan‟ DDoS detection and traceback with decision tree and grey relational analysis‟ Int. J. Ad Hoc and Ubiquitous Computing, Vol. 7, No. 2, 2011
22. Zekri, M., El Kafhali, S., Aboutabit, N., & Saadi, Y. (2017, October). DDoS attack detection using machine learning techniques in cloud computing environments. In Cloud Computing Technologies and Applications (CloudTech), 2017 3rd International Conference of (pp. 1-7). IEEE.
23. Rutvija Pandya and Jayati Pandya. Article: C5.0 Algorithm to Improved Decision Tree with Feature Selection and Reduced Error Pruning. International Journal of Computer Applications 117(16):18-21, May 2015.
24. V. Jean Shilpa, P. K. Jawahar (2019)”Advanced Optimization by Profiling of Acoustics Software Applications for Interoperability in HCF Systems”, Journal of Green Engineering, Alpha publishers,9(3),pp.462-474.
25. P.Radha, B.MeenaPreethi, ”Machine Learning Approaches For Disease Prediction From Radiology And Pathology Reports”, Journal of Green Engineering, Alpha publishers,9(2),pp. 149-166
26. ://www.darkreading.com/vulnerability-management/167901026/security/attacks-reaches/228000532/index.html
27. A.Suresh Kumar, 2018, ‘Obfuscating Software puzzle for Denial of Service attack mitigation’, International Journal of Pure and Applied Mathematics.
28. M. Kowsigan and S. Priyadharshini, 2018, ‘Security in Data & Dissemination of Distributed Data in Wireless Sensor Network’, International Journal of Pure & Applied Mathematics, Volume 118.
29. Higgins, K.J 2010, ‘Researchers to Demonstrate New Attack That Exploits HTTP, [online] http://www.darkreading.com/vulnerability-management/167901026/security/attacks-reaches/228000532/index.html
30. Shekyan, S 2012, 'Are you ready for slow reading?’ Retrieved from https://community.qualys.com/blogs/security labs/2012/01/05/slow-read
31. Bhuvaneswari K., and Rauf H.A., 2009, ‘Edgelet based human detection and tracking by combined segmentation and soft decision’, International Conference on Control Automation, Communication and Energy Conservation, Issue 5204487.
32. Poornaselvan K.J., Gireesh Kumar T., and Vijayan V.P., 2008, ‘Agent based ground flight control using type-2 fuzzy logic and hybrid ant colony optimization to a dynamic environment’, Proceedings - 1st International Conference on Emerging Trends in Engineering and Technology, ICETET, Issue 4579922, PP: 343 - 348.
33. Hoque, N, Bhattacharyya D.K &Kalita, J.K 2015, 'Botnet in DDoS Attacks: Trends and Challenges', IEEE Communications Surveys & Tutorials, Vol. 17, no. 4, pp. 2242-2270.
34. Alomari, E, Manickam, S, Gupta, B.B, Karuppayah, S &Alfaris, R 2012, 'Botnet- based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art', International Journal of Computer Applications, Vol. 49, no. 7, pp. 24-32.
35. R.Kanmani and A. Jameer Basha, 2016, ‘Performance analysis of wireless OCDMA system using OOC, PC and EPC codes’, Asian Journal of Technology, Vol-15(12), PP: 2083-2089.