A Study on Recent Approaches in Managing and Detection of DDoS Attacks

A. Anthony Paul Raj [1†] **and J. K. Kani Mozhi** [2††],
Paulraj_15@yahoo.co.in drjkkanimozhi@gmail.com
[1†] Research Scholar, Periyar University. , [2††] Professor, Dept. of Computer Application,
Sengunthar Arts and Science College

Abstract
In a system we use to share the data over the around the world. While sharing the data is to keep up the information confidentially. Attacker in the system may capture this privately data or distorted. So security is the principle piece of concern. There are a few security attacks in system. A standout among the most critical and modern day dangers is DDoS (Distributed disavowal of administrations) attacks. It gives an opportunity to an attacker to expand access to a huge number of computers by use their vulnerabilities to set up attacks systems or Botnets. The fundamental thought of this paper is to concentrate on modern day approaches managing and Detection of DDoS attacks

Keywords:
DDoS attack; vulnerabilities; Botnets

1. Introduction

To keeping up the computer data is extremely hard to handle in the modern system world. Some interruption may happen on the framework or system based framework. Without security dealings and regulate set up our data may be an attack. This sort of attack is one or more clients, bots attack a solitary target bringing about the framework to back off, along these lines invalidate its clients the capacity to utilize it. The DDos attack is the most popular attack in network. Dos (Denial of Service) and DDoS (Distributed Denial of Service) attacks are attempts to make a server resource unavailable to its intended users [1]. DDoS attacks are typically executed from numerous causes and can result in big traffic flows. The content delivery network (CDN) company found there's been a 125 percent increase in distributed denial of service (DDoS) attacks year over year [2].

There are two types of DDos attack classification based on communication device such as Attacks with direct communication and Attacks with indirect communication

A. Direct Attack Communication:

During direct attack communication, the client and handler machine to identity each other in order to communicate. This is accomplished by hard-coding the IP location of the handler tackles in the attack code that is later installed on the agent. Each client then reports its readiness to the handlers, who store its IP address in a data for later transformation. The noticeable disadvantage of this approach is that discovery of one negotiated machine can representation the whole DDoS network. Additionally, since operators and handlers listen to network associations, they are identifiable by system scanners.

B. Indirect Attack Communication:

Attacks with indirect communication deploy a level of indirection to raise the survivability of a DDoS network. Recent attacks provide the example of using IRC channels [4] for agent/handler communication. The use of IRC services swaps the function of a manager, since the IRC channel offers enoughobscurity to the attacker. Since DDoS users establish outbound connections to a standard service port used by a genuine network service, agent communications to the control point may not be easily distinguished from legitimate network traffic. An attacker controls the agents using IRC communications channels.
In Q1 2019, DDoS activity was distributed more or less evenly, with the exclusion of one peak on 6 February. The peak number of attacks in one day was 1,272, recorded on 31 March [3].

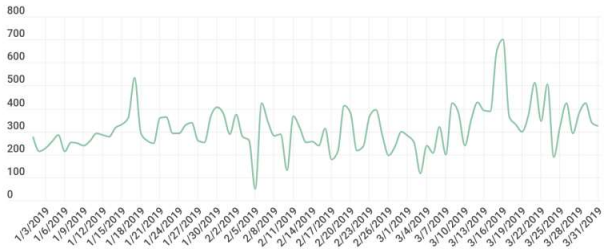

Figure 1. DDoS attacks over time* in Q1 2019
Source - Kaspersky DDoS Intelligence Report for Q1 2019 Securelist [3].

2. DDOS ATTACKS

Denials of service (DoS) attacks have become a most important threat to modern computer networks. This type

Manuscript received October 5, 2024
Manuscript revised October 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.10.19

of attacks could have various forms, but frequently they send thousand and millions of Zombie hosts against a single target. These are innocently recruited from the millions of vulnerable computers accessing the Internet through high bandwidth, all ways requesting to the target. These tackle, hackers can quickly build a mass of zombies, all waiting for to launch a DDoS attack.

The word DDoS attack is an expansion of DoS attack. Normally attackers start attacking the victim with DoS attacks at the same time in synchronization. In DDoS attack there is one master attacker and number of attacking zombies. Master is responsible for problem control commands for zombies, and the zombies are accountable for making actual attack traffic. The Fig. 1 shows the representation diagram of DDoS attack.

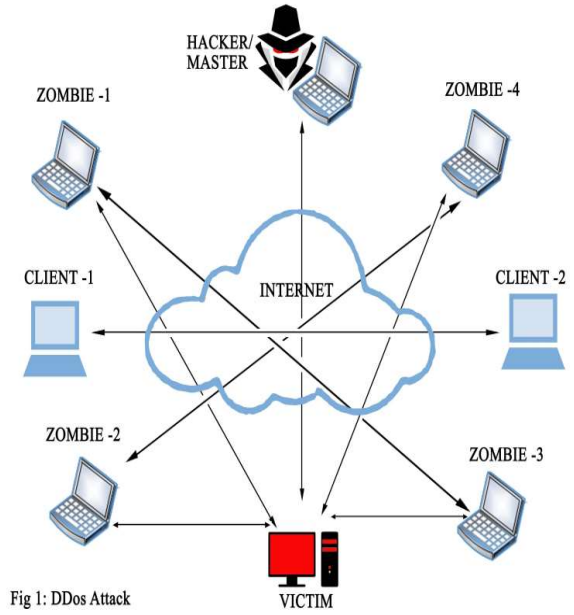

Figure 2 DDOS Attacks

There are different types of DDoS attacks can be classified into the following categories. In this paper we focus on SYN Flooding, UDP Flood, REFLECTED Attack, SLOWLORIS and ZERO –DAY DDOS.

C. Syn Flooding

This is the most vital attack happen through the three-way handshake. In three-way handshake client demand a new linking by transfer SYN packet server ACK sends back to client. Finally client acknowledged with ACK [4].This kind of attack is a run of the mill DDoS that sends fast amount of packets at a machine trying to keep connection from being shut. The sending machine does not close the connection, and in the end that connection times out. On the off chance that the attack is sufficiently solid it will devour all assets on the server and send site disconnected.

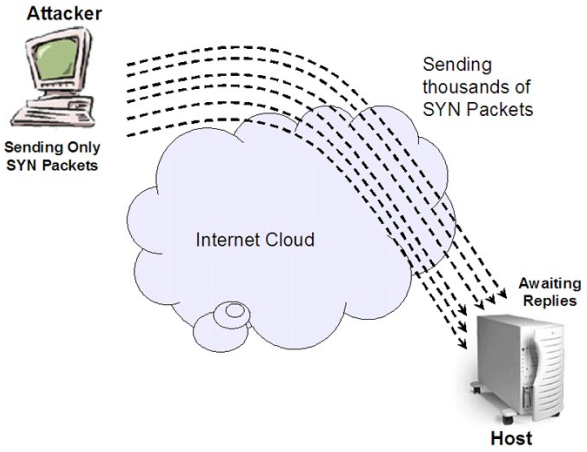

Figure 3 Source: http://zaielacademic.net/ [10]

D. Udp Flood

In UDP Flood attack attacker sends large numeral of UDP packets to a victim system, due to which there is capacity of the network and the reduction of available bandwidth for genuine service needs to the victim system [5]. A UDP flood is a system flood and still a standout amongst the most widely recognized flood today. The attackers send UDP packets, regularly vast ones, to single destination or to arbitrary ports. Much of the time the attackers parody the SRC IP which is anything but difficult to do subsequent to the UDP contract is " low connection" and does not have any sort of handshake component or session. Normally the mechanism of UDP flood attack is each device in the botnet sends UDP packet to all the ports to the server. [9]

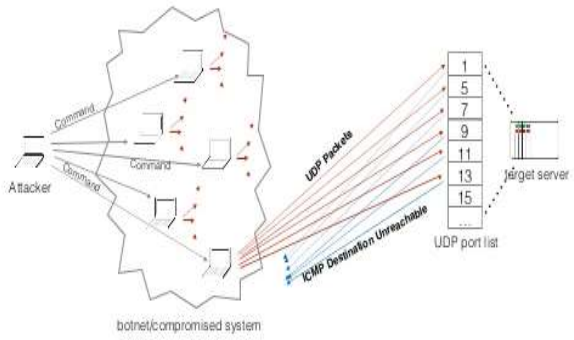

Figure 4 Source: DDoS Attack Detection & Mitigation in SDN [9].

E. Reflected Attack

Reflection attacks are attacks that utilization the same convention in both bearings. The attacker parodies the casualty's IP address and sends a solicitation for data through UDP to servers known not to that kind of solicitation. The server answers the solicitation and sends the reaction to the casualty's IP address. From the servers' point of view, it was the casualty who sent the first demand. Every one of the information from those servers heaps up, blocking the objective's Internet network. With the amplified data transmission, typical activity can't be adjusted and customers can't interface. Any server open to the Internet and running UDP-based administrations can be utilized as a reflector.

F. Slowloris

By sending HTTP headers to the objective site in modest pieces as moderate as could reasonably be expected (holding up to send the following minor lump awaiting just before the server would stage out the request), the server is compelled to keep on waiting for the headers to arrive. On the off chance that enough associations are opened to the server in this style, it is rapidly not able to handle real demands.

G. Zero-Day Ddos

"Zero-day" is an essentially obscure or new attack, abusing vulnerabilities for which no patch has yet been discharged. The term is surely understood amongst the individuals from the programmer group, where the act of exchanging Zero-day vulnerabilities has gotten to be a famous movement.

3. DDOS ATTACK Approaches

In various researchers discuss the concepts of DDos attacks deduction. In [6] the author discusses Intrusion Detection System (IDS).An IDS is a software or hardware that is used to identify unauthorized traffic that is against the policy of the network [6].IDS can be named serving part either for system based or have based or blend of both. In a system based IDS system activity is observed while in host-based IDS working framework log records and application are checked. The host-based is situated in a solitary host and the system construct is situated in light of a machine that is isolated from the host. Network-based IDS, it can be frequently used to detect attacks such as DoS attacks, worms, botnet and scans and other type of attacks [6].

IDS can be named serving part either for system based or have based or blend of both. In a system based IDS system activity is observed while in host-based IDS working framework log records and application are checked. The host-based is situated in a solitary host and the system construct is situated in light of a machine that is isolated from the host. If there is any match, it produces an alarm for the eventual attack [7].Anomaly based IDS are otherwise called conduct situated in which it contrasts the system movement and past ordinary system activity. On the off chance that any deviation happens gives the notice of assault. The ordinary activity can be grouped into two: prepared and standard.

The standard depends on standard Protocols. The trained traffic can be used to control the threshold value that cans be used for upcoming detection. Anomaly-based detection system mainly involves of three phases: parameterization, training and detection [8].The system parameters are characterized in parameterization stage. The typical conduct of activity is characterized in preparing stage. In location stage, the traffic behavior is contrasted and preparing stage. On the off chance that the consequence of the correlation surpasses the edge esteem, an alert is brought on.The test examination of the author inferred that Cumulative Sum is one of the identification algorithms that perform well when contrasted with different procedures less memory assets and calculation. It perform superior to anything different methods since it is non-parametric, it doesn't require preparing and is robust towards attack profile varieties.

The following research authors are used as Statistical based DDoS attack Detection methods. Let as discuss one by one. In [11] the authors Akella.et al introduce the attack Detection by use of source and victim side and the author focus on: A profile is constructed from normal traffic and detects anomalies in the traffic using stream sampling. As a rule this methodology utilized as a part of the network routers. Research paper by Prasad, ARMReddy and KVGRrao[12] presents an introduction to Modeling and Counter measures of Flooding attacks to ITM using Bonnet and Group Testing. In [13] the author Chen introduce the attack Detection in Victim side and the author focus on Detects DDoS attacks using two-sampled-test by integrating the statistics of SYNarrival rate. These are some classification in Statistical based DDoS attack Detection methods.

The authors Bayu Adhi Tama et al [14] attempts to characterize papers concerning DoS/DDoS attack location utilizing information mining methods. Most of papers were chosen and deliberately investigated by creators from two online journal databases. Each of chose paper was considered in light of the volume of information mining, for example, affiliation, classification, clustering, and hybrid techniques. The discoveries of this work demonstrate that arrangement and half and half strategies got a lot of consideration from analysts.

The author Suchita Korad[15] used to deduction the DDos attack by using two components HDFS and MapReduce. Hadoop's focal administration hub otherwise called NameNode parts the information into substantial number of same size pieces and circulates them amongst the group hubs. Hadoop's MapReduce exchanges bundled code for hubs to prepare in parallel, the information every hub is mindful to prepare. The location server for the most part serves as the Hadoop's NameNode, which is the centerpiece of the Hadoop DDoS recognition bunch. On effective exchange of log record/documents, the identification server split the document into same size substantial pieces and begins MapReduce DDoS recognition occupations on bunch hubs. We have talked about MapReduce work analyses what's more, counter based DDoS identification calculation. Once the recognition undertaking is done, the outcomes are spared into HDFS.

In [16] the author Niharika Sharma introduced the concept of machine learning techniques this technique provide production of unknown attacks. There are some techniques for detection of DOS attacks such as Decision Trees: In Decision tree knowledge a decision tree is used as a analytical model in which observations about an item are mapped to conclusions about the item's target value.[16], K-Means Clustering: k-means and naive baye classification techniques are used to classify whether the packet is normal or is DOS attack,[17][18], Genetic Algorithms: This approach uses evolution theory to data evolution in order to filter the traffic data and thus reduce the complexity[16].

4. Conclusion

A DDos attack is a difficult and serious issue and consequently, several approaches have been deducted to DDos. The modern attack and defense mechanisms are difficult to understand the global view of the DDos issue. It is essential to know the current trends in attack technology in order to efficiently and properly evolve defense and response approach. The DDoS attack protection classifications outlined in this paper are useful to the coverage that they explain our thoughts and direct us to extra useful solutions to the problem of DDoS.

5. Acknowledgment

Foremost, my gratitude goes to Dr. J. K. Kani Mozhi, Professor, Department of Computer Application, Sengunthar Arts & Science College, Tiruchengode, who guided me into the fractal realm. Her vision, her enthusiasm and her spirit inspired and enlightened me to carry out this research paper with curiosity and involvement. And I thank my wife Mrs. A. Arockia Vinnarasi my son Master A. Joel Roy and my little angel A. Jessica Mariam who always supported to me. Finally, I thank God who gives me good health, continuous encouragement and support throughout the research work and my life.

REFERENCES

[1] Santhosh Kumar Karre, “Distributed Detection of DDoS Attack,”International Journal of Future Computer and Communication, Vol. 2, No. 6, December 2013.

[2]http://www.zdnet.com/article/ddosattacksincreaseover125percentyearoveryear/.

[3]https://securelist.com/analysis/quarterlymalwarereports/74550/kasperskyddosintelligencereportforq12016/

[4] Divya Kuriakose, V.Praveena "Survey on DDoS Attacks and Defense Approaches "International Journal of Innovative Research in Computer and Communication Engineering,Vol. 1, Issue 8, October 2013.

[5] F. Lau, S. H. Rubin, M. H. Smith and L. Trajkovic, “Distributed Denial of Service Attacks” IEEE International Conference on Systems, Man, and Cybernetics, Nashville, 8-11 October 2000, pp. 2275- 2280.

[6] T. M. Wu, "Intrusion Detection Systems ", Information Assurance Technology Analysis Centre (IATAC), September 2009.

[7]F. Dressler, G. Munz, G. Carle, "Attack detection using cooperating autonomous detection system(CATS),"Wilhelm-Schickard Institute of Computer Science, Computer Networks and Internet, 2004.

[8] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Macia-Fernandez, E. Vazquez, "Anomaly-based network intrusion detection:Techniques, systems and challenges," computers &security, vol.28, pp. 18-28, 2009.

[9] DDoS Attack Detection & Mitigation in SDN FINAL VIVA PRESENTATION 2014-12-08 COMSE-6998 Presented by Chao CHEN (cc3736).

[10] http://zaielacademic.net/security/syn_attacks.htm

[11]A. Akella, , Bharambe, M. Reiter, M., and Seshan, S“Detecting DDoS attacks on ISP networks.”Proceedings of the Workshop on Management andProcessing of Data Streams, San Diego, CA, 8 June, pp. 1–2. ACM. . (2003).

[12] K Munivara Prasad, Dr. A Rama Mohan Reddy ,Modelling and Counter measures of Flooding attacks to ITM using Botnet and

[13] Group Testing, Global journal of Computer Science and Technology (GJCST), Volume11, Issue 21,pp-15- 24,Dec 2011,

[14] C.L. Chen “A new detection method for distributed denial-of-service attack traffic based on statistical test”,. Journal of Universal Computer Science, 15, 488–504. ,(2009).

[15] Bayu Adhi Tama, Kyung-Hyune Rhee,” Data Mining echniques in DoS/DDoS Attack Detection: A Literature Review,” The 3rd International Conference on Computer Applications and Information Processing Technology (CAIPT 2015), Yangon, Myanmar, June 23-24, 2015.

[16] Suchita Korad, Shubhada Kadam, Prajakta Deore3, Madhuri Jadhav, Prof.Rahul Patil, “Detection of Distributed Denial of ServiceAttack with Hadoop on Live Network”,International Journal of Innovative Research in

Computer and Communication Engineering, Vol. 4, Issue 1, January 2016

[17] Niharika Sharma, Amit Mahajan, Vibhakar Mansotra, " Machine Learning Techniques Used in Detection of DOS Attacks: A Literature Review " International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 3, March 2016

[18] Mangesh D. Salunke ,Prof. Ruhi Kabra," Denial-of-Service Attack Detection „International Journal of Innovative Research in Advanced Engineering (IJIRAE) „„Volume 1 Issue 11 (November 2014)

[19] Mangesh Salunke, Ruhi Kabra, Ashish Kumar." Layered architecture for DoS attack detection system by combine approach of Naive bayes and Improved K-means Clustering Algorithm", International Research Journal of Engineering and Technology (IRJET), Volume: 02 Issue: 03 ,June-2015.

BIOGRAPHY

A. ANTHONY PAUL RAJ received his B.Sc., B.Ed degree in Computer Science from Pope John Paul II College of Education under Pondicherry Uinversity. He completed his M.SC in Computer Science from St.Joseph College,Trichy under Bharathidasan University. He is completed M.Phil in Computer Science under Bharathidasan University. He is pursuing her Ph.D in Periyar university, Salem. He has 11 years of Teaching Experience. His area of interest is Network Security.

J. K. Kani Mozhi working as an Professor, in Department of Computer Applications,Sengunthar Arts & Science College,She has 17 years of teaching Experience. Her area of intreset in image processing and Network Security