Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 03, March-2020

Denial of Service Attacks: Tools and Categories

Hadeel S. Obaid
College of Engineering
University of Information Technology and Communications
Baghdad, Iraq

***Abstract*—DoS attacks cause severe damage to services available online. This kind of attacks try to prevent legitimate users from using their rights to online services by bringing down servers. Issues in Internet security provide the hackers with ways to attack network systems. These attacks can be performed using many tools and techniques. This paper gives an overview on DoS attacks categories and tools. Also, it defines the most known Dos attack incidents and explains the IP Spoofing.**

Keywords— DoS Attack; RDoS Attack; IP Spoofing.

I. INTRODUCTION

DoS attacks try to prevent legitimate users from accessing a system by decreasing availability of the system [1]. They enforce heavy computation functions to the target through abusing the weakness of the system or overwhelming it by a massive volume of worthless requests. The target server is sent offline for minutes or for days resulting in a severe damage to the system services. Therefore, efficient DoS attacks detection is important in order to protect online services [2]. Even though software patching protects against some attacks, it fails to defend against DoS flooding attacks [1]. A secondary protection, which contains both detections of the attack and defenses, is essential. Observing the traffic of the network, including using intelligent routers and firewalls configuration, may help to stop DoS/DDoS attacks to some degree [3].

DoS attacks represent the main security issues that threatened internet services and result in senior income losses [4]. Even though DoS attacks happened during the1980s and early 1990s, the attacks were not common security occurrences [5]. However, this changed when the Internet started to become a common medium. The backscatter study was used to evaluate the period and the number of DoS attacks over the Internet [6]. The results showed that more than 5,000 distinct targets were the victims of more than 12,000 attacks during a period of 3 weeks checked in February 2001. the Internet of Things (IoT) has recently been presented as the next revolution and a part of the internet of the future [26] [27]. DoS can be also used to pull down any IoT network as well [28].

The rest of the paper is ordered as following: in section 2 includes the related work. Section 3 explains RDoS attacks. Section 4 presents IP Spoofing. DoS Categories and DoS tools are in Section 5 Section 6 respectively. Section 7 contains DoS defense mechanisms. Finally, the Conclusion in section 8.

II. RELATED WORK

Many researchers have proposed different techniques to detect and prevent DoS and DDoS attacks. Most of the DoS attack are detection mechanisms based on the Intrusion Detection System (IDS), machine learning algorithms and data mining techniques. Machine learning (ML) is a known area of computer science that mainly deals with the discovery of data patterns and data-related irregularities [29]. Researchers have tried to develop new techniques to defend against DoS attacks or combine more than one mechanism to make attack execution more sophisticated. However, attackers often find ways to compromise Internet systems and launch DoS attacks.

Subramani Rao [7] has used Access Control Lists (ACL) to Mitigate DoS attack. ACL are rules applied to a machine to control permissions. His project aims to apply ACL on the Cisco routers to block particular set of IP packets. This list offers a defense to a network because it controls incoming and outgoing traffic from a single point. He used ACL rules to block traffic from the attacking network. These rules are applied to the command line interface of the router. The results showed that the traffic is completely blocked from the attacking network.

Subramanian and others have proposed a technique using Hop Count Filtering (HCF) system and the Support Vector Machine (SVM) algorithm to filter the majority of the spoofed traffic on the network layer [8]. DDoS attackers using genuine IP addresses are subjected to traffic limits at the initiating application layer. The two-layer defense method defends legitimate packets from being denied, thus mitigating DDoS efficiently. Hop Count Filtering (HCF) system recognizes packet with spoofed source IP address. The source IP address and corresponding hops from a server (victim) are recorded in a record table. The incoming packet could then be checked against the table for authenticity. The design of the table of an IP2HC decreases the amount of storage space by IP address clustering.

III. REFLECTOR DENIAL OF SERVICE (RDOS) ATTACK

Staying anonymous or hiding the source of traffic is an important aim for an attacker [9]. Attackers have found an innovative approach to attack, which is called Reflector Denial of Service (RDoS) shown in Fig. 1.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 03, March-2020

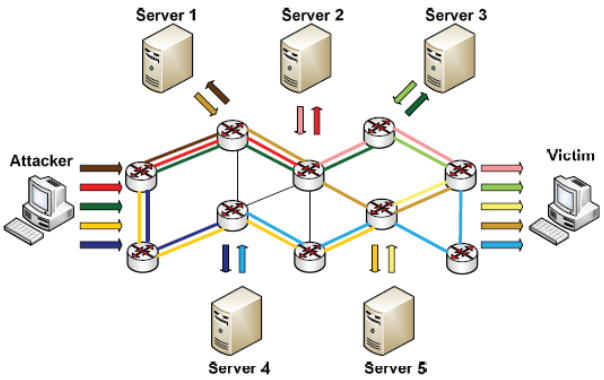

Fig. 1. RDoS Principle

The purpose of a bandwidth attack is to hide the attack traffic source using innocent web servers or routers called reflectors to send malicious packets to the target [9]. A system can be a potential reflector if it replies to an incoming packet. Conceptually, attackers send packets where the source addresses are made up; the victims address surrounding web servers or routers. The devices in the network reply to the incoming packets, where they then appoint them to the relevant address, which is obtained as a victim source address. Thus, the target server receives a large volume of requests which means it is under DoS attack. RDoS attack can be implemented in a straightforward way or in a distributed way. The Distributed Reflective Denial of Service attack (DRDoS) contains three stages. Stage one is identical to a regular DDoS attack, where the attacker is connected to a number of agents. However, at the second stage, there is a slight difference when the attacker agents control zombies. Rather than ordering zombies to direct malicious packets to the target straightway, the zombies are instructed to direct traffic forged source third party IP addresses using the victims' IP addresses. At the third level, the reflectors will direct the response traffic to the target, which results in a DRDoS attack. As compared to typical DDoS attack, DRDoS attacks are more scattered with third parties and it is hard to find the origin of the attack. Additionally, the attack traffic source IP addresses come from innocent machines that make tracing back the original attack highly difficult [9].

IV. IP SPOOFING

In IT world, spoofing means deceiving other computer systems or computer clients. This is normally done by concealing one's identity over the internet. It can be done through an IP address or email, among other methods. We are interested in spoofing through IP addresses [10].

Internet Protocol (IP) is the main protocol to send and receive data over the Internet [11]. The IP packet header includes beside
other things the packet source address and the destination address. Typically, the source address represents the address from which the packet is sent. By tampering with the header of the packet so it includes different addresses, the attacker is able to make the packet appear to be sent from another machine. When the machine receives a spoofed packet, it will reply to the tampered source address. The attacker uses such a technique if he is less interested in the response or the attacker can potentially guess the response.

IP spoofing represents the most common type of online disguise [11]. The term IP spoofing aims to conceal the sender identity or to impersonate another machine. In spoofed attack, an attacker directs packets to the victim showing that the packet comes from a confidential user. To succeed; First, the attacker has to define the IP address of a confidential machine, modifying the packet header so that it seems like a packet comes from a reliable system. In theory, the attacker is tricking the victim to believe that it is an authentic machine in the network. This enables the attacker to establish a connection and gain entrance to the victim, permitting the formation of a backdoor entrance to the victim machine. Fig. 2 illustrates the valid source IP address. Fig.2 explains a typical communication between computers have legal source IP addresses, asking the web server for web pages [11]. The request includes the IP address of the workstation (192.168.0.5), which represents the source IP address and the IP address (10.0.0.23) is for the web server and represents the destination IP address. The response of the web server contains a web page with source IP address (10.0.0.23) and (192.168.0.5) as the destination IP address.

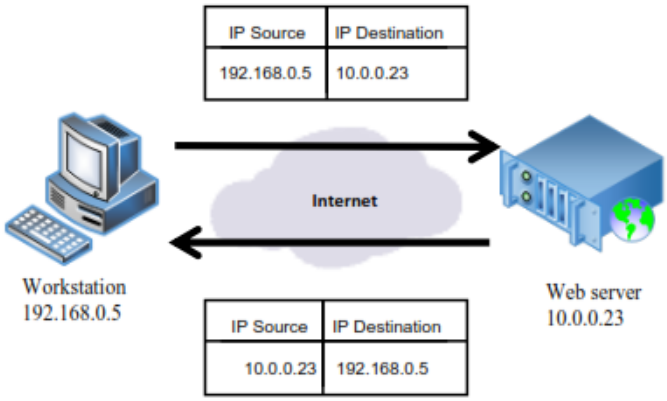

Fig. 2. Valid Source IP Address

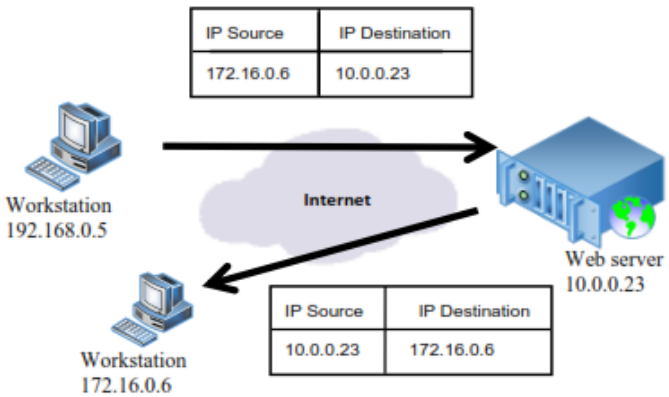

Fig. 3. Spoofed Source IP Address

Fig. 3 shows the communication of requesting web pages between a computer with spoofed source IP and a web server [11]. The workstation uses the spoofed source IP (172.16.0.6). The web server replies to the request and sends data to the actual workstation that have the IP (172.16.0.6). The spoofed IP address system then receives unwelcome connection tries from the web server, where they are merely discarded.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 03, March-2020

IP Spoofing is Easy because: -

- Authentication only depends on Source addresses.
- IP routing is hop after hop. Each packet is routed individually. All the routers that the packet goes through determining the route for an IP packet.
- Only the Destination addresses are looked by the Routers.
- Changing the source address filed in the packet header is easy.

IP spoofing is a main technique in all DoS attacks is to conceal the attacker identity by sending packets have a fake source IP addresses [6]. Also, for some DoS attacks, a particular value in the field of the source IP address is a requirement. By using the victim's address as a source IP address of the packet, the packet is sent from the victim. So in this case, the victim is enforced to contact a non-existing host.

V. DENIAL OF SERVICE ATTACKS CATEGORIES

To understand DoS attacks, we need to know how researchers classify different types of these attacks. Based on my study, I would like to classify DoS attacks into two classes as in Fig. 4:

Weaknesses-based Attacks: - This kind of attack misuses any flaws or weaknesses in the internet protocols or the internet system to perform the denial of service attacks. For example, the abuse of the ICMP, HTTP and TCP protocols.

Flooding Attacks: - The Attacker sends an enormous amount of traffic to exhaust the victim resources, thereby the traffic from legitimate users are dropped. The term resources refer to memory, CPU cycles, bandwidth, buffers, descriptors, etc.

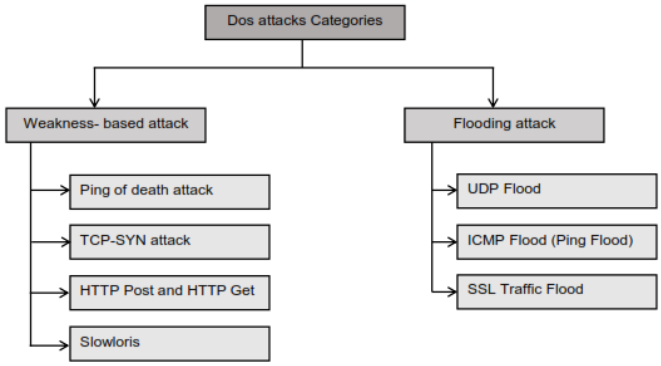

Fig. 4. DoS Attacks Categories

Several kinds of literature classified DoS attacks, for example, that can be categorized into a Bandwidth Attack or called Volume Based Attack [12]. This attack overloads the network traffic by sending huge broadcast traffic. The attacker particularly spoofs the source IP addresses to make the attack untraceable from the victim's network. Report describes the Bandwidth DoS attacks as the increasing of the network traffic to the target victim servers so that the bandwidth becomes overloaded [13]. A network is flooded with requests, whereby it is difficult for legitimate network requests from typical users to reach the website whereby the infrastructure is jammed and cannot serve the requests that come from users.

Loukas in his thesis mentioned that the target of this attack is the bandwidth of the network with either flood attacks, for example ICMP floods or UDP floods [5].

Alvaro Garcia declared that high data volume attacks are able to exhaust all the bandwidth existing between a target and an (Internet Service Provider) ISP [14]. The ISP networks require having a high bandwidth because they are obliged to route from several resources to several ends. Typically, the victim is connected with the ISP with bandwidth amount smaller than the connections inside the ISP networks. Therefore, once large traffic volume comes from the ISP and goes over these connections, it will cause links overfilling and traffic slowing down. Bandwidth can be consumed by the attacker through sending any traffic to the network connections such as sending large amount of simple ICMP packets to cause bandwidth exhaustion.

Haiqin Liu classified DDoS attacks into a bandwidth attacks based on the target of DDoS attacks [15]. He stated that for bandwidth DDoS attacks there are two types: denial of network service attacks and denial of edge service. The former type, the attacker typically tries to saturate the entry bandwidth of the victim side. However, he was not clear in defining what exactly denial of network service attacks and denial of edge services are.

Other researchers have classified DoS attacks into protocol attacks. For example, Albiz classifies DoS attacks into various groups depending on targeted protocols of the layer in the TCP/IP stack [16]. It divided Protocol DoS attacks into DoS at the application layer and the DoS at the network and transport layers. Regarding DoS at the application layer, protocols like Telnet, HTTP, IMAP, FTP, SSH, IRC, SMTP/POP, XMPP, BOOTP/DHCP, SNMP, DNS, NTP, RTP, TLS/SSL, SIP can become an object to launch a DoS attack. While in DoS at the network and transport layers, protocols like TCP, UDP, and ICMP are used to perform DoS attacks.

Another category of DoS attacks is the Resource attack, which is stated by researches [15] and [13]. This type of attack consumes the computing resources which are assigned to an application. For example, a file-processing server or an email server have limitations or constraints in resources where it can handle a certain number of user sessions in each time. As Muharish stated, the resource attack happened when an attacker attempts to send a huge number of virtual connections to consume memory and CPU resources of the victim server [13]. As the resource of the victim is limited, a huge number of broken connections will make the server unable to reply to legitimate clients.

VI. DOS AND DDOS COMMON TOOLS

Denial of service tools, at least at the beginning, were proof-of-concept code examples that demonstrated insecurities in common operating systems, including Windows, Linux, Solaris and UNIX [17]. Today, many DoS and DDoS tools are available online. Table 1 list the most common DoS and DDoS tools and description:

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 03, March-2020

TABLE I. COMMON DOS AND DDOS TOOLS

DoS Tools	Description
Low Orbit Ion Canon (LOIC)	A simple tool for flooding TCP, HTTP or UDP traffic, can also be used to perform DDoS
High Orbit Ion Cannon (HOIC)	High speed attack tool and can flood up to 256 websites at one go, send GET and HTTP POST requests
Hping or hping3	Transmit an ICMP echo request, also can send massive volumes of TCP traffic
Slowloris	Attack the web server by generating slow HTTP request
Trinity	Generate SYN, UDP, RST, fragment, random, null flood and flags requests
Trinoo	Efficient DDoS attacks tool, send UDP packets

A. *Low Orbit Ion Canon (LOIC)*

Today, many DoS and DDoS tools are available online such as Low Orbit Ion Canon (LOIC), which is a very common DoS attacks tools and it is existing freely over the Internet. The famous hackers group (Anonymous) used this tool to attack many networks of large enterprises they even using IRC to invite Internet clients to involve them in their DDoS attack. LOIC was developed by Praetox Technologies and was intended to be used by developers who needed to make their servers to be under a heavy traffic load for experimental purposes [18]. However, the hackers Anonymous took the open-source tool and used it to execute organised DDoS attacks. Later, LOIC was amended and given its “Hivemind” characteristic to allow any LOIC user to obtain a LOIC’s copy at an IRC server, where control is transferred to a master user who can then send commands using IRC to LOIC clients simultaneously. A single user can apply this tool to launch a DoS attack against small servers by sending HTTP, UDP, or TCP packets to the victim. Only the URL or IP address of the server are needed to obtain by the user and the LOIC will perform the attack.

B. *Hping*

Hping or hping3 is a tool that is able to deal with the size of a random packet and its fragmentations [19]. Hping implements the testing of the firewall rule, the testing of the protocol based-network performance and port scanning. It presents more employment than just transmitting an ICMP echo request, which is the traditional use of ping. It can be used to send massive volumes of TCP traffic to a victim and spoofing the source IP addresses to make it look to be random or initiate from a user source

C. *Slowloris*

Slowloris is a software that enables a machine to attack the web server of another machine with limited bandwidth and side effects on not related ports and services. This program is written by Robert "RSnake" Hansen [12]. This tool can generate denial-of-service traffic on a target server using a very slow HTTP request. It sends HTTP headers to the victim server in small parts and slowly so as to make the server wait for the next small part until a time out on the request is finished (i.e., the server is enforced to carry on waiting for the headers to reach). Slowloris also attempts to keep many connections of the web server open and keep them opened as long as possible.

D. *Trinity*

Trinity is a DoS tool that can be controlled using IRC or ICQ [5] This tool is able to generate SYN, UDP, RST, fragment, random, null flood and flag requests that cause exhaustion and link congestion to endpoint resource.

E. *Trinoo*

Trinoo is an efficient DDoS attacks tool that uses a master node and many broadcast nodes. In this case, a master host commands several broadcast hosts to perform the attack [19]. Mirkovic and Loukas describe this tool as a tool used to organise distributed UDP flood attacks, where the attacker is connected to a (handler) or Trinoo master and orders it through a TCP connection in order to execute a DoS attack [5]. Then, the handler is connected to the Trinoo agents through UDP and instructs them to launch the DoS attack for a period through directing UDP packets with a specified size to random ports of victims IP addresses.

VII. REVIEW ON DETECTION AND DEFENSE MECHANISMS OF DOS ATTACKS

DoS attacks try to prevent legitimate users from accessing a system by decreasing availability of the system [1]. They enforce heavy computation functions to the target through abusing the weakness of the system or overwhelming it by a massive volume of worthless requests. The target server is sent offline for minutes or for days resulting in a severe damage to the system services. Therefore, efficient DoS attacks detection is important in order to protect online services. Even though software patching protects against some attacks, it fails to defend against DoS flooding attacks. A secondary protection, which contains both detections of the attack and defences, is essential. Observing the traffic of the network, including using intelligent routers and firewalls configuration, may help to stop DoS/DDoS attacks to some degree.

Koc and Carswelll have implemented experiments using Naïve Bayesian (NB), KDD99 dataset, and its variables; Tree (NBTree), Averaged One-Dependence Estimators (AODE), Weightily AODE (WAODE), Tree-Augmented Naïve Bayesian (TAN), Decision DTNB, and Hidden Naïve Bayesian (HNBNB). The results of their experiments indicate that Proportion K-Interval discretization techniques, along with HNB, offer high accuracy to detect DDoS attack [20].

Lohit Barki et al. have proposed an IDS to detect DDoS attack in Software Defined Network (SDN) using machine learning algorithms such as K-Nearest neighbour, Naive Bayes, K-medoids and K-means to categorise incoming traffic into regular and irregular categories [21]. The detection rate and efficiency parameters are used to measure these algorithms. The algorithm has more accuracy in choosing to implement Signature IDS; its results are then processed by Advanced IDS, where the intent is to detect anomalous behaviour using open connections. This helps to provide accurate results of the hosts involved in the DDOS attack.

Katkar and Bhatia have performed an experiment for intrusion detection using REPTree classifier and assess the variation in its performance when it is combined with different

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 03, March-2020

data pre-processing and feature selection techniques [3]. Experiment results show that the accuracy of REPTree classifier in detecting intrusion is better when used with Numeric to Binary pre-processing technique on the data set of KDD99.

Zhiyuan Tan et al. have presented detection system to detect DoS attack using multivariate correlation analysis (MCA). By extracting geometrical correlations between different features of network traffic, MCA can be used for network characterization. Such a detection system uses anomaly based detection in its attack recognition [2]. The advantage is it makes the solution able to detect identified and unidentified DoS attacks through learning normal patterns of the network traffic. Additionally, to improve and to accelerate MCA processes, a triangle-area-based method is suggested. The efficiency of this suggested detection system is assessed using the data set of the KDD Cup 99. The effects of both regulated and non-regulated data on the performance of the proposed detection system are tested.

Detection methods such as Client Puzzle Protocol (CPP) and Ingress filtering are used to detect DoS and DDoS attacks at the Application layer [9]. In internet communication, CPP algorithm is used and aims to stop misuse of server resources. CPP requires that all clients that want to connect to the server to resolve a mathematical puzzle before the connection is to be established. When the puzzle is solved, the client passes the solution of the puzzle to the server. If the client failed to solve the puzzle, the server refuses the connection. The puzzle is not hard to solve but the attacker attempt to establish a huge number of connections with the target and this will be difficult because of the time delay. The Ingress filtering technique is used to ensure that the arrival packets do not have fake source IP addresses in their header. Every packet is sent with the IP source address in the header. If this IP address is fake, this is considered as an attack. In Ingress filtering, packets are examined based on the information from the past so that the server will not be allowed to respond to packets from possible attacking IP addresses.

Xiuzhen Chen et al. proposed a model to assess DoS attacks threats on some attributes of network security such as availability of service in real time, observing security threat evolution of the attacked system and enhancing valuation precision [22]. The technique depends on using a sensor on chosen servers to constantly observe pre-identified network parameters performance. The threat index value (TI) is obtained using the DS evidence reasoning algorithm to merge suitable metrics of network rendering in order to make decisions concerning operational states of observed systems. As soon as the evolution of the security menace is obtained, suitable reply policies is accepted to limit DDoS attack occurrence in the network systems. To try the suggested model of threat evaluation, real network situation tests are designed. This method compared with other methods averts the one-sided result acquired from a single sensor. Additionally, it assists administrators to define the state of security threat and gives threat evolution of service obtainability over time. The experiment of real network displays that the technique enhances the precision of threat evaluation. Also, it proves the effect of DoS attacks on the security of the network at the beginning of the attack is different from the end of denial of service attacks. It supplys administrators with a macroscopically picture of threat evolution. Additionally, it provides administrators with the basis to take on security reply rules in a real environment for the dependable network.

Regarding the defence mechanisms against DoS attacks, Jarmo Mölsä claimed in his report that there is no single defence against DoS attacks that is enough [6]. A complete set of defences have to be applied to provide depth. In case of one layer fails, other layers can detect, prevent, or minimise an attack. A successful intrusion needs all defensive layers to be failed.

Subramani Rao has used Access Control Lists (ACL) to Mitigate DoS attack [7]. ACL are rules applied to a machine to control permissions. His project aims to apply ACL on the Cisco routers to block particular set of IP packets. This list offers a defence to a network because it controls incoming and outgoing traffic from a single point. He used ACL rules to block traffic from the attacking network. These rules are applied to the command line interface of the router. The results showed that the traffic is completely blocked from the attacking network.

A H M Jakaria and his colleagues have proposed a mechanism called VFence to prevent DDoS attacks that influence the architecture ability of the Network Function Virtualization (NFV) [23]. To allow flexible and dynamic network function implementation, NFV is virtualizing network functions within virtual machines on servers. In this technique, network agents are used to interrupt packets where there is a potential attack to confirm validity and to protect the server through the removal of illegitimate packets. Because the intensity of the attack is often changed, the framework of NFV-based defence dynamically organises agents to balance the load of the attack. The results of the simulation prove that the technique is able to successfully fail the DDoS attacks by making all the requests from legitimate users served; the increase in the response time of the server is unimportant in comparison to one from a successful DDoS attack.

Weiler has presented a scheme that assistances in depth defence in a network against DDoS attacks [25]. This system lures attackers into the confidence that DDoS attack is successful and convinces the malicious user that the salves are compromised effectively. The scheme is a sort of a honeypot that lures the attacker to believe that. By this means, the honeypot operator can study the attacker strategies and can perform effective defences in the rest of his network.

Bellaïche and Grégoire have presented a mechanism to allocate and find an appropriate time-out value for connection-establishment to situations [24]. The experiments have proved the effectiveness of the proposed scheme in controlling backlog queue size by quickly eliminating failed or fake connection tries. The technique is able to decrease the size of the backlog queue to 50% with maintaining normal connections. This mechanism is easy to perform with no change in the TCP protocol.

Luo et al. have constructed a defence technique for DDoS in Software-Defined Networks (SDN) by analysing the specific characteristics of SDN and determining if it is beneficial to defend against DDoS attack [25]. SDN is a communication network architecture that decouples network

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 03, March-2020

forwarding and control. In SDN, specific characteristics like programmability and central control are used to defend against DDoS attack. They illustrate how such a technique could resist DDoS attacks using spoofed UDP flood attacks as an example.

Subramanian and others have proposed a technique using Hop Count Filtering (HCF) system and the Support Vector Machine (SVM) algorithm to filter the majority of the spoofed traffic on the network layer [8]. DDoS attackers using genuine IP addresses are subjected to traffic limits at the initiating application layer. The two-layer defence method defends legitimate packets from being denied, thus mitigating DDoS efficiently. Hop Count Filtering (HCF) system recognises packet with spoofed source IP address. The source IP address and corresponding hops from a server (victim) are recorded in a record table. The incoming packet could then be checked against the table for authenticity. The design of the table of an IP2HC decreases the amount of storage space by IP address clustering. HCF-SVM runs on the side of the possible victim at the network layer, which has a strong motivation to perform the filtering function. There is no need for collaboration with routers. It uses narrow information such as source IP addresses and (Time-to-Live) TTL values to filter the attack packets, facilitating the need for execution. The scheme of IP2HC tables decrease the storage space amount. Additionally, a rate limiter at the application layer penalises attack flows and offers bandwidth for legitimate users with no denial of services. HCF-SVM scheme proves 98.99% accurate and reduces the false positive (FP) rate.

VIII. CONCLUSION

In conclusion, an attacker may use single machines to perform DoS attacks, or he/she may employ many zombie botnets to increase the attack's intensity. In this case, DoS attacks are called DDoS attacks. DDoS attacks are one of the most serious security threats to internet systems. Staying unknown is an important desire for the attacker. The attacker always finds new ways to hide his identity. Therefore, the attacker uses reflectors to make the DDoS attack more complicated. Spoofing techniques are also used to conceal the identity of the attacker and make it difficult for anyone to know his IP address. Many researchers try to classify DoS and DDoS attacks into dissimilar categories. Most of them are classified DoS and DDoS attacks into bandwidth DoS attacks and protocol DoS attacks. In bandwidth DoS attacks, the attacker floods the network traffic by sending a huge amount of traffic. DoS attacks take advantage of weaknesses in the Internet protocol system to perform the attack. The attackers can execute DoS and DDoS attacks manually, but there are many free tools available and online that perform diverse types of DoS attacks. They are very simple to use, where attackers only need to know the IP address or the URL of the target server.

REFERENCES

[1] Carl, G., Kesidis, G., Brooks, R.R., and Rai, S.: 'Denial-of-service attack-detection techniques', IEEE Internet computing, 2006, 10, (1), pp. 82-89.
[2] Tan, Z., Jamdagni, A., He, X., Nanda, P., and Liu, R.P.: 'A system for denial-of-service attack detection based on multivariate correlation analysis', IEEE transactions on parallel and distributed systems, 2013, 25, (2), pp. 447-456
[3] Katkar, V.D., and Bhatia, D.S.: 'Experiments on detection of Denial of Service attacks using REPTree', (IEEE, 2013), pp. 713-718
[4] Shah, M., Soni, V., Shah, H., and Desai, M.: 'TCP/IP network protocols—security threats, flaws and defense methods' (IEEE, 2016), pp. 2693-2699
[5] Loukas, G.: 'Defence against denial of service in self-aware networks', 2006
[6] Mölsä, J.: 'Mitigating denial of service attacks in computer networks' (Helsinki University of Technology, 2006. 2006)
[7] Rao, S., and Rao, S.: 'Denial of Service attacks and mitigation techniques: Real time implementation with detailed analysis', This paper is from the SANS Institute Reading Room site, 2011
[8] Subramanian, K., Gunasekaran, P., and Selvaraj, M.: 'Two Layer Defending Mechanism against DDoS Attacks', International Arab Journal of Information Technology (IAJIT), 2015, 12, (4)
[9] Durcekova, V., Schwartz, L., and Shahmehri, N.: 'Sophisticated denial of service attacks aimed at application layer', (IEEE, 2012), pp. 55-60
[10] Sandeep, R.: 'A study of DoS & DDoS-smurf attack and preventive measures', International Journal of Computer Science and Information Technology Research, 2014, 2, pp. 1-6
[11] Rashid, S., and Paul, S.P.: 'Proposed Methods of IP Spoofing Detection & Prevention', International Journal of Science and Research, 2013, 2, (8), pp. 438-444
[12] Shaker, K.: 'Analyzing DoS and DDos Attacks to Identify Effective Mitigation Techniques', American International University-Bangladesh (AIUB), 2014
[13] Muharish, E.Y.M.: 'Packet filter approach to detect denial of service attacks', 2016
[14] de la Villa, A.G.: 'Distributed Denial of Service Attacks defenses and OpenFlow: Implementing denial-of-service defense mechanisms with software-defined networking': 'Core. ac. uk' (2017)
[15] Liu, H.: 'A collaborative defense framework against DDoS attacks in networks', 2013
[16] Abliz, M.: 'Internet denial of service attacks and defense mechanisms', University of Pittsburgh, Department of Computer Science, Technical Report, 2011, pp. 1-50
[17] Farraposo, S., Boudaoud, K., Gallon, L., and Owezarski, P.: 'Some issues raised by DoS attacks and the TCP/IP suite', (2005), pp.
[18] Myers, L.: 'Guide to DDoS attacks, integrated intelligence center technical white paper', Center for Internet Security, 2014
[19] Kaur, H., Behal, S., and Kumar, K.: 'Characterization and comparison of distributed denial of service attack tools' (IEEE, 2015), pp. 1139-1145
[20] Koc, L., and Carswell, A.D.: 'Network intrusion detection using a hnb binary classifier', (IEEE, 2015), pp. 81-85
[21] Barki, L., Shidling, A., Meti, N., Narayan, D., and Mulla, M.M.: 'Detection of distributed denial of service attacks in software defined networks', (IEEE, 2016), pp. 2576-2581
[22] Chen, X., Li, S., Ma, J., and Li, J.: 'Quantitative threat assessment of denial of service attacks on service availability', (IEEE, 2011), pp. 220-224
[23] Jakaria, A., Yang, W., Rashidi, B., Fung, C., and Rahman, M.A.: 'Vfence: A defense against distributed denial of service attacks using network function virtualization', (IEEE, 2016), pp. 431-436
[24] Weiler, N.: 'Honeypots for distributed denial-of-service attacks', (IEEE, 2002), pp. 109-114
[25] Luo, S., Wu, J., Li, J., and Pei, B.: 'A defense mechanism for distributed denial of service attack in software-defined networks' (IEEE, 2015), pp. 325-329
[26] Sabry, S.S., Qarabash, N.A., and Obaid, H.S.: _The Road to the Internet
of Things: a Survey', (IEEE, 2019), pp. 290-296.
[27] Obaid, H.S., Al-Shareefi, N.A., and Abbas, S.A.: 'Internet of Things and Wireless Sensor Networks for Environmental Noise Sensing: Issues and Challenges', Journal of Southwest Jiaotong University, 2019, 54, (6)
[28] Anirudh, M., Thileeban, S.A., and Nallathambi, D.J.: _Use of honeypots
for mitigating DoS attacks targeted on IoT networks', pp. 1-4.
[29] Obaid, H.S., Dheyab, S.A., and Sabry, S.S.: _The Impact of Data Pre-Processing Techniques and Dimensionality Reduction on the Accuracy of Machine Learning', (IEEE, 2019), pp. 279-283.