International Journal of Research
Available at https://edupediapublications.org/journals

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 13
October 2017

A Comprehensive Survey Report on Distributed Denial of Service(DDoS) Attacks and Possible Defense Mechanisms

Ch. Sandeep & M. Sadanandam

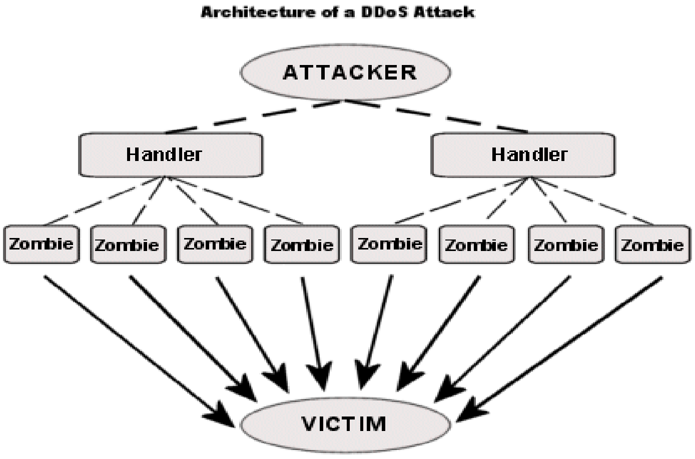
Associate professor Computer Science and Engineering S.R.Engineering college Warangal, Telangana

Assistant professor Computer Science and Engineering KU College of Engineering Warangal, Telangana

Sandeep892@gmail.com ; Sadanb4u@yahoo.co.in

Abstract— *In the last decade of advances in internetwork technology, users are more convenient to obtain online services such as trading, gaming, etc. Due to advancement in internet technology, internet resources and services now can be used in both remotely and in a distributed environment. Attackers make use of above environment and perform various attacks on resources and services of networks. A Denial of Service (DoS) attack denies the access of other legitimate users to shared services or resources where as Distributed Denial of Service (DDoS) attackers usually use multiple distributed computer resources to launch a coordinated DoS attack against one or more targets.*

A distributed denial-of-service (DDoS) attack is an attack in which multiple compromised computer systems attack a target, such as a server, website or other network resource, and cause a denial of service for users of the targeted resource. The flood of incoming messages, connection requests or malformed packets to the target system forces it to slow down or even crash and shut down, thereby denying service to legitimate users or systems. DDoS attacks have been carried out by diverse threat actors, ranging from individual criminal hackers to organized crime rings and government agencies. In certain situations, often ones related to poor coding, missing patches or generally unstable systems, even legitimate requests to target systems can result in DDoS-like results.

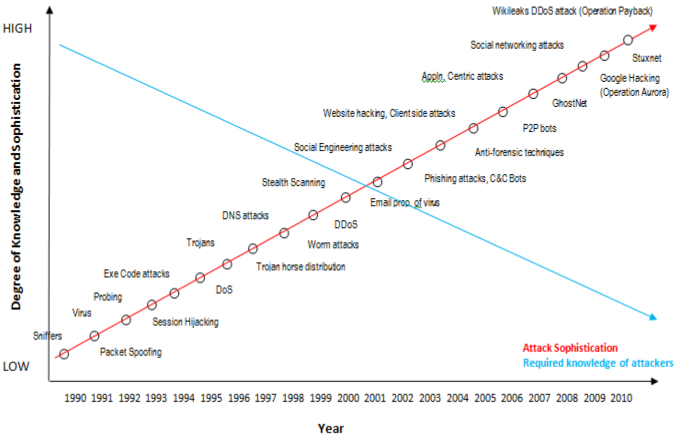


DDoS attacks last for a period of time for exhausting the server resources, such as CPU, memory, and connection capacity by the following types of attacks: Session Flooding Attacks, Request Flooding Attacks, Asymmetric Attacks, Slow Request/Response Attacks, Among the above attacks, DDoS attack is the most prevalent threat in cyberspace. Researchers have been proposing many defence mechanisms to combat the attacks.

Introduction:

A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. They target a wide variety of important resources, from banks to news websites, and present a major challenge to making sure people can publish and access important information.

Distributed Denial of Service (DDoS) attacks constitute one of the major threats and are among the hardest security problem facing in today's websites. With increasing computational complexity in Internet applications as well as larger network bandwidths in the systems hosting the web applications, server resources such as CPU or I/O bandwidth have become the bottleneck much before the network. In cyber space most common attacks on discredited environment include packet spoofing, session hijacking, cross side scripting (XSS), SQL injection, execution of malicious software(Virus, Worms), DNS rebinding and DDoS (Distributed Denial of Service). The following Figure shows the evolution of various attacks on network.



1) *How DDoS attacks work:*

In a typical DDoS attack, the assailant begins by exploiting the vulnerability in one computer system and making it the DDoS master. The attack master system identifies other vulnerable systems and gains control over them by either infecting the systems with malware or through bypassing the authentication controls (i.e., guessing the default password on a widely used system or device).

A computer or networked device under the control of an intruder is known as a zombie, or bot. The attacker creates what is called a command-and-control server to command the network of bots, also called a botnet. The person in control of a botnet is sometimes referred to as the botmaster (that term has also historically been used to refer to the first system "recruited" into a botnet because it is used to control the spread and activity of other systems in the botnet). Botnets can be comprised of almost any number of bots; botnets with tens or hundreds of thousands of nodes have become increasingly common, and there may not be an upper limit to their size. Once the botnet is assembled, the attacker can use the traffic generated by the compromised devices to flood the target domain and knock it offline.

2) *Types of DDoS attacks:*

There are three types of DDoS attacks. Network-centric or volumetric attacks overload a targeted resource by consuming available bandwidth with packet floods. Protocol attacks target network layer or transport layer protocols using flaws in the protocols to overwhelm targeted resources. And application layer attacks overload application services or databases with a high volume of application calls. The inundation of packets at the target causes a denial of service.

3) *Internet of Things (IOT) and DDoS attacks:*

While the things comprising the internet of things (IoT) may be useful to legitimate users, in some cases, they are even more helpful to DDoS attackers. The devices connected to IoT include any appliance into which some computing and networking capacity has been built, and, all too often, these devices are not designed with security in mind.

Devices connected to the IoT expose large attack surfaces and display minimal attention to security best practices. Internet of things botnets are increasingly being used to wage massive DDoS attacks. In 2016, the Mirai botnet was used to attack the domain name service provider Dyn, based in Manchester; attack volumes were measured at over 600 Gbps. Another late 2016 attack unleashed on OVH, the French hosting firm, peaked at more than 1 Tbps. DDoS attacks can create significant business risks with lasting effects. Therefore, it is important for IT and security administrators and managers, as well as their business executives, to understand the threats, vulnerabilities and risks associated with DDoS attacks.

In March 2013, DDoS attack rate reached 300 Gigabits per second, the biggest DDoS attack ever seen in the internet [1, 2]. This attacks mainly targeted on the web infrastructure of the Spamhaus, a non profit organization dedicated to spam. Hence DDoS are the most significant type of attack on cyberspace.

Cybercriminals are increasingly turning to Distributed Denial of Service (DDoS) this year, as 33% of organizations faced such an attack in 2017—up from just 17% in 2016, according to a new report from Kaspersky Lab. These cyber attacks are hitting businesses of all sizes: Of those affected, 20% were very small businesses, 33% were SMBs, and 41% were enterprises. Half of all businesses reported that the frequency and complexity of DDoS attacks targeting organizations like theirs is growing every year, highlighting the need for more awareness and protection against them. According to Kaspersky Lab, of the companies that were hit in 2016, 82% said that they faced more than one DDoS attack. At this point in 2017, 76% of those hit said they had faced at least one attack.

Sample case study: In 1996 the Federal Communications Commission (FCC) issued the E911 First Report and Order which required wireless providers to forward 911 calls to a PSAP regardless of caller validation: "The basic 911 rules require wireless carriers to transmit all 911 calls to a Public Safety Answering Point (PSAP) without regard to validation procedures intended to identify and intercept calls from non-subscribers. Under the rules, therefore, both subscribers and non-subscribers can dial 911 and reach emergency assistance providers without having to prove their subscription status."

A DDoS attack launched from a mobile smart phone device can exploit this ruling in order to make its attack more difficult to mitigate. If a bot randomizes the device's cellular identifiers, it becomes impossible to blacklist its 911 calls. In this paper we expose and analyze this new threat by proving its feasibility and by measuring its potential impact via simulations. We found that only 6,000 infected devices are enough to severely harm the availability of the 911 services of a US state. We also found that some device-level and network-level countermeasures can help in mitigating this threat.

DDoS Attacks and Possible Counter Measures:

In several existing mechanisms that are deployed at network layer the DDoS attacks are detected by analyzing the protocol header information, packet arrival rate and plenty of a lot of parameters. Detection depends on the distinction within the main informatics parameters, like supply informatics address, supply destination try, hop count, next protocol field and combination of multiple attributes. A science technique that allows the tracing of attack supply in provided within the intelligent router based mostly hardened network that is projected in.

DDoS Attacks and Possible Counter Measures:

In several existing mechanisms that are deployed at network layer the DDoS attacks are detected by analyzing the protocol header information, packet arrival rate and plenty of a lot of parameters. Detection depends on the distinction within the main informatics parameters, like supply informatics address, supply destination try, hop count, next protocol field and combination of multiple attributes. A science technique that allows the tracing of attack supply in provided within the intelligent router based mostly hardened network is projected in.

Mostly, a hop count based technique, In which, whenver an informatics packet is received, it is plunged if immense distinction exists between its hop count & amplitude of hops; the calculable values are projected in. Probabilistic suggests that networks may not notice malicious packets in Differential Packet Filtering against DDoS Flood Attacks. Overlay network is projected by Keromytis, through that the approved traffic is shipped. Secure Overlay Service (SOS) network changes its topology perpetually to forestall DDoS and may survive although few key nodes are attacked.

Another possible counter measure is the design of open, scalable and independent security on the Internet exploits the vulnerability to DDoS attack. Host's resources and network bandwidth are two main targets of DDoS attacks. Most attacks aim at the defect of protocols and applications: SYN flood, UDP flood, ICMP flood, SIP flood, etc. Some attacks like UDP flood, ICMP flood deplete the network bandwidth. Others like SYN flood, SIP flood exhaust a victim's system resource (e.g., CPU, memory) as well. In a UDP flood attack, an attacker sends the packets to some random or specified ports to attack these ports and saturating the network resources. DDoS attacks also take advantage of techniques like IP spoofing, network amplifier/reflector, the combination of attack methods to avoid detection and prompt their influence.

For that purpose, we elaborate on two dichotomies: one focusing on which elements they rely on (network elements vs. flows) and another focusing on their defense functionalities. Solutions in the literature can be classified according to whether they are intrinsic or extrinsic. A property that is inherited and essential is named intrinsic, whereas a property that varies depending on exterior factors is called extrinsic. In our case, some solutions are related to structural attributes of the SDN environment, whereas others are mostly related to the properties of network flows. For this reason, we propose to classify identified mechanisms as intrinsic vs. extrinsic solutions.

Intrinsic solutions can be further categorized as table-entry-based, scheduling-based, and architectural. Table-entry-based models propose solutions related to the limited table size of switches. Each unknown flow needs a new entry in switch memory. This becomes a bottleneck during a DDoS attack, which contains packets with different IP addresses. In fig.1 the impact of a DDoS attack in SDN is presented. Their results highlight the importance of managing the flow tables. They conclude that table entry replacement policies should use multiple parameters such as number of packets, generation date, and utilization properties of a flow entry, rather than using just one parameter such as earliest expiration time. Besides, a controller should have an intermediate buffer module, which stores the flow entries temporarily and manages the replacement of flow entries. These suggestions can also be utilized as DDoS mitigation methods. Similarly, Katta et al. presents a solution for a general attack scenario related to the memory of switches. Switches can allow a limited number of entries in their tables due to resource constraints on memory capacity. Proper update policy of these entries is essential against DDoS attacks since attack packets are also dropped or forwarded according to these entries. Their work proposes a rule update mechanism for switch tables. Although their idea is not specifically proposed targeting DDoS attacks, it is beneficial for DDoS mitigation. Scheduling-based solutions are implemented on the controller.

These models suggest that it is essential to protect the controller since it is the core of the system in SDN. In order to provide this capability, such models deal with scheduling assignment of tasks from switches. The approach proposed by Hsu et.al. provides scalability, Hsu et al. proposed a hash-based mechanism that operates in the controller to increase scalability of the network. Their work performs hash-based round-robin scheduling for assigning the incoming packets from a crowded switch to several queues in the controller. In this model, the controller can still serve the switch even if it has a high amount of traffic due to flash crowd or DDoS attack.

This model does not have a detection mechanism and acts in the same way for flash crowd. This situation results in unproductive service for DDoS attack packets in the controller. Lim et al. suggest that the most essential aim of a defense mechanism is to provide the controller's work continuity in case of an attack since the controller's failure leads to the entire SDN being unavailable. They leverage a scheduling-based scheme that contains most of the attack traffic at attack ingress switches so that the SDN as a whole can continue normal operation. If one switch is infected by DDoS, normally the controller cannot serve other users. In order to prevent this problem, they create different queues for each switch. Actually, this model realizes the opposite of the attacks in SDN.

Intrinsic solutions:

Solutions against DDOS attacks in SDN environment, which are focused on network entities and their functionalities/ elements.

Extrinsic solutions:

Focused on network flows and their characteristics are Statistical Machine learning based.

In our case, some solutions are related to structural attributes of SDN environment, whereas others are mostly related to the properties of network flows. For this reason, we propose to classify identified mechanisms as intrinsic vs. extrinsic solutions.

Conclusion:

A loss availability of resources, internet services and network performance degradation in important times has motivated us to do research on DDoS attacks and possible measures to identify DDoS attacks and find counter measures to safeguard the networks performance from such attacks.

The survey paper is aimed to make a comprehensive analysis on several DDoS attacks in order to meet the following objectives:

1. Prevention of unauthorized users
2. Protection of availability of services and resources
3. A deep learning based DDoS attack detection approach (called Deep Defense). Deep learning approach can automatically extract high-level features from low-level ones and gain powerful representation and inference.

References:

1. http://newindianexpress.com/world/article1520116.ece,
2. http://www.cyberintelligentsecurity.net/corero/dds_overview.php
3. Lin, Y.H., Kuo, J.J., Yang, D.N. and Chen, W.T., 2017, May. A cost-effective shuffling-based defense against HTTP DDoS attacks with SDN/NFV. In *Communications (ICC), 2017 IEEE International Conference on* (pp. 1-7). IEEE.
4. Guri, M., Mirsky, Y. and Elovici, Y., 2017, April. 9-1-1 DDoS: Attacks, Analysis and Mitigation. In *Security and Privacy (EuroS&P), 2017 IEEE European Symposium on* (pp. 218-232). IEEE.
5. Kalkan, K., Gur, G. and Alagoz, F., 2017. Defense Mechanisms against DDoS Attacks in SDN Environment. *IEEE Communications Magazine*, *55*(9), pp.175-179.
6. Yuan, X., Li, C. and Li, X., 2017, May. DeepDefense: Identifying DDoS Attack via Deep Learning. In *Smart Computing (SMARTCOMP), 2017 IEEE International Conference on* (pp. 1-8). IEEE.
7. Hoque, N., Bhattacharyya, D.K. and Kalita, J.K., 2015. Botnet in DDoS attacks: trends and challenges. *IEEE Communications Surveys & Tutorials*, *17*(4), pp.2242-227