# Denial of Service(DoS) attack incidents and defense mechanisms

Venkat Jamadar[1],Jabiulla B[2],Rakesh S[3],Pradeep Sadanand[4]
Student[1], Student[2], Student[3],Assistant Professor[4]
Computer science and Engineering,
BMS College of Engineering,Bangalore,India

**Abstract:A DoS attack is a dangerous malicious attempt by a single person or a group of people to cause the victim, site, or node to deny services to its users. As in another case it is also possible that a lot of malicious hosts coordinate to flood the victim with an abundance of unnecessary threat packets, so that the attack occurs simultaneously from multiple points. This type of attacks are called Distributed DoS, or DDoS attacks. the improvements in the technology leads different types of attacks. The tools which are available now are not able to identify the different type of attacks**.

**Index term:Introduction,incidents,classification of denial of service mechanism,types of attacks, ddos detection approaches,ddos defense mechanism.**

## I.INTRODUCTION:-

Denial of Service(DoS) attacks have become a major threat to current computer networks.To have a better understanding on DoS attacks. This survey involves an overview on existing DoS, DDOS attacks and major defense techniques are in the wireless networks and internet. in this survey we describe host based and networks based DoS attack methods. DoS attacks are classified according to the major attack types. Current available technologies are also reviewed, including different defense products in deployment and representative defense approaches in research survey. the different DoS attacks and defenses in 802.11 protocol based wireless networks are explored physical ,network layers and MAC. Some of the major attack names keywords are Denial of Service (DoS), Distributed Denial of Service (DDoS), Internet Security, Wireless Security, Scanner, Spoofing.

DOS attack history and incidents:-

• DoS attacks started at around early ’90s.

• At the first stage they were quite "primitive", involving only one attacker exploiting maximum bandwidth from the victim, denying others the ability to be served. This was done by using different flooding attack methods.

• These attacks had to be "manually" synchronized by a lot of attackers in order to cause an effective damage.

• The shift to automating this synchronization, coordination and generating a parallel massive attack became public in 1997, with the release of the first publicly available DDoS attack tool is Trinoo.

• In the following years, few more tools were published – TFN, sTFN2K, and Stacheldraht ("Barbed wire" in German).

• The subject came to public awareness only after a massive attack on public sites on February 2000. in a period of three days the sites of cnn.com Yahoo.com, amazon.com, buy.com,& eBay.com were under attack.

• Analysts estimated that Yahoo! Corporation has Lost in e-commerce business and in advertising revenue when it was knocked offline for three hours.

• There were about fifty computers at Stanford University, many computers at the University of California at Santa Barbara has crashed.

• A study during a period of three weeks in February 2001 showed that there were about 4000 DoS attacks each week. Most DoS attacks are neglected by the news media nor are they prosecuted in courts.

## II.CLASSIFICATION DDOS ATTACK MECHANISMS:-

DoS attacks can be classify into 2 category:

1)Flooding Attacks.

2)Logical Attacks.

***Types of flooding attacks:-***

i) TCP SYN flood Attack:- In this type of attacks the attacker uses spoofed IP addresses to send requests to a server. The server will responds by sending the SYN/ACK signal back and server waits for the ACK signal from its client. But no reply comes from client because the IP is spoofed and the real client is unaware of the ACK signal that the server is expecting. This leaves the half open connections on the server side thus consuming its resources. So sending thousands of requests this can force the server to crash.

ii).ICMP attack: An attacker sends forged ICMP echo packets to broadcast addresses of vulnerable networks. All the systems on this network reply to the victim with ICMP ECHO replies. This rapidly blocks bandwidth to the target and prevents its from providing services to legitimate users .

iii). UDP Flood Attack: A UDP flood attack is possible when an attacker sends a UDP packet to a random port on the victim system. The victim system will wait on port for the application. When it realizes that there is no application that is waiting on the port, flood attack generates an ICMP packets of target unreachable to the forged source address. If flood of UDP packets are send to the victim machine, the system will surely go down.

***Types of Logic Attacks:-***

i) Ping of Death:-By using the ping command to exploit the fact that the maximum packet size that TCP/IP allows for being transmitted over the Internet is restricted to 65,536 octets. In this attack, the target system is pinged with a data packet that exceeds the maximum bytes allowed by TCP/IP.

ii) Teardrop Attack: An attacker sends multiple fragments that cannot be able to reassembled properly making use of a bug in the TCP/IP fragmentation re-assembly code of various operating systems by manipulating the offset value of packet and cause reboot or halt the victim system.

iii) Land Attack: An attacker sends a forged packet with the same source and destination IP address. Whenever victim system replies to that packet it actually sends that packet to itself, it will create an infinite loop between the target system and target system itself thus causing the system to crash.

## III.CLASSIFICATION OF SOME DDOS DEFENSE MECHANISMS:-

DDoS defense mechanisms can be classified as follows:

1. DDoS Attack Prevention: Attack prevention methods try to stop all well-known broadcast based and signature based DDoS attacks from being launched in the first place. Prevention techniques allow to keep all the machines over Internet update with patches and security holes. Signature of the packets is matched with the existing database consisting of known attack patterns at each edge router.

To prevent the DDoS attack the following approaches are useful:-

i) Filtering all packets entering and leaving the network helps protect the network from attacks conducted from neighboring networks, and prevents the network itself from being an unaware attacker.

ii) Firewall can allow or block protocols, ports or IP addresses but other complex attack like on port 80 cannot be handled by it because it is unable to distinguish between legitimate traffic and DDoS attack traffic. Only those attacks can be identified whose signatures are already there in the database. A slight variation from the original attack pattern can leave the attack undetected. Also new attacks cannot be detected.

2. DDoS Detection: Attack detection aims to detect an ongoing attack as soon as possible without misclassifying and disrupting legitimate traffic.

## IV.DDOS DETECTION APPROACHES DIVIDED INTO TWO TYPES:-

i) Signature based detection: Signature based approach employs a priori knowledge of attack signatures. The signatures are manually constructed by security experts analyzing previous attack patterns and used to match with incoming traffic to detect intrusions.

ii) Anomaly based detection: Anomaly-based system uses a different method to detect the attack. It identifies any kind of network connection violating the normal connection as a threat.

**V.DDOS DEFENSE MECHANISMS:-**

[1].DENIAL-OF-SERVICE (DoS) attacks are one type of aggressive and menacing intrusive behavior to online servers. DoS attacks vastly focus on degrading the availability of a victim, which can either be host, router, or an entire network. Interconnected systems, cloud computing servers, web servers, so on, are under threads from the network attackers. Denial-of-service (DoS) attacks cause serious impaction these computing systems. In this paper, a DoS attack detection system that uses multivariate correlation analysis (MCA) for accurate network traffic characterization by extracting the geometrical correlations between network traffic features. The MCA-based DoS attack detection system employs the principle of anomaly based detection in attack recognition. This makes solution capable of detecting known and unknown DoS attacks effectively by learning only the patterns of legitimate network traffic. Furthermore, a triangle-area-based technique is proposed to enhance and to speed up the process of MCA the influences of both non-normalized data and normalized data on the performance of the proposed detection system are examined. The results show that this system outperforms two other previously developed state-of-the-art approaches in terms of detection. A MCA based analysis DoS attack detection system which is powered by the triangle-area based MCA technique and the anomaly-based detection technique. The former existing technique captures the geometrical correlations hidden in individual pairs of two distinct features within each network traffic record, and allows space for more accurate characterization for network traffic behaviors. The latter technique facilitates to be able to distinguish both known and unknown DoS attacks from legitimate network traffic.

[2].The Internet is vulnerable to bandwidth distributed denial-of-service (BW-DDoS) attacks, wherein many hosts will send a large number of packets to cause congestion and disrupt legitimate traffic. These attacks can cause loss or severe degradation of connectivity between the Internet and victim networks or even whole autonomous systems (ASs), possibly disconnecting entire regions of the Internet. In this paper proposed a detection system, attacking agent, attack mechanism, protocol mechanism, network level defense mechanism, mechanism location.

Attacking Agent:- three types of attacking agents: puppets, zombies, and root zombies. Acquiring puppets is relatively easy and can be done by fooling users into browsing to an attacker's website. Zombies are more difficult they require attackers to install malware on zombie machines by exploiting some vulnerability or tricking users into installing the malware. Root zombies require either zombies that were initially installed with high privileges or a privilege escalation exploit that can maliciously gain such privileges.

***Attack Mechanisms:-***
Three types of attack mechanisms:
Direct flooding, amplification, and reflection. In a naïve kind of attack, attack traffic is limited by the compromised machines 'bandwidth capacity, and the victim's entire load is due to the direct flooding induced by packets the zombies send. Amplification attacks use the attacking agents' bandwidth more effectively, such that, on average, every packet a zombie sends causes non compromised machines to transmit multiple or larger packets to the victim.

***Protocol Manipulation:-***
Attackers use two types of protocol manipulations. The first step is to avoid detection, and the second attempt is to exploit legitimate protocol behavior and cause legitimate clients and servers to excessively misuse their bandwidth against the victim. Typically, protocol manipulation for bandwidth attacks requires a strong zombie with administrative privileges, because the manipulation is commonly done at the low protocol layers handled by the OS, usually IP and TCP. Note that not all BW-DDoS attacks use manipulation.

***Response Mechanism:-***
There are four different kind of defense mechanisms are available: filtering, rate limiting, detouring and absorbing, and break through.
***Filtering:-*** Assuming the offending flows are identified, they can be filtered out. Filtering can take place in various network locations: close to the destination or close to the source.

***Rate limiting:-*** In contrast to completely blocking the attacking flows, rate-limiting schemes let the offending flows transmit their typical rate or obey some other limit.

***Detouring and absorbing:-***Additional schemes use overlay networks and cloud computing. Overlays mitigating BW-DDoS attacks can be divided into detouring and absorption.
Breakthrough: - The final categories of BW-DDoS mechanisms are those that use aggressive clients to break through the congestion. Aggressive clients use TCP friendly protocols as long as they can sustain enough good put.

***Defense Mechanism Location:-***
The various defense mechanisms can be deployed at different network locations. Some are deployed close to the destination, that is, near the victim.
[4]. In Distributed Reflection (DRDoS), attackers fool innocent servers (reflectors) into flushing packets to the victim. But many of present DRDoS detection mechanisms are associated with specific protocols and cannot be used for unknown protocols. the packet rate of one converged responsive flow may have linear relationship with another.. The preliminary simulations indicate that RCD can differentiate reflection flows from legitimate ones efficiently, thus can be used as a useable indicator for DRDoS.
The focus is on two typical scenarios involving one attacker and multiple reflectors:

a) One attacker spoofs requests to reflectors randomly with uniform distribution, at a constant rate, e.g., the outgoing bandwidth.
b) One attacker spoofs requests to reflectors randomly with uniform distribution, at a low level but variable rate.

The letter concentrates on detecting DRDoS independent of specific protocols, and introduces the Rank Correlation based Detection (RCD) algorithm. RCD will start calculate the rank correlation when the suspicious flows found, between flow pairs and give final alert according to preset thresholds. The preliminary simulations demonstrate that it could be a helpful indicator for DRDoS detection. The result could also be used to pick out and discard malicious flows. There are a lot of interesting works in the future, including:
1) The Other correlation-like comparison and measurement of their effectiveness.
2) Extensive effective experiment opposes to real DRDoS in the Internet.
3) Using RCD in many scenarios.
4) What the attackers can do to escape from countermeasures and detection.

[5].This presents a sophisticated strategy to stealthy attack patterns against applications running in the cloud. Instead of aiming at making the service unavailable, the proposed strategy aims at exploiting the cloud flexibility, forcing the application to consume more resources than needed, affecting the cloud customer more on financial aspects than on the service availability. The attack pattern is orchestrated in order to face, or however, highly delay the techniques proposed in the literature to detect low-rate attacks. It does not exhibit a periodic waveform typical of low-rate exhausting attacks. In contrast with them, it is an iterative and incremental process. In particular, the attack potency (in terms of service requests rate and concurrent attack sources) is slowly enhanced by a patient attacker, in order to inflict significant financial losses, even if the attack pattern is performed in accordance to the maximum job size and arrival rate of the service requests allowed in the system. Using a simplified model empirically designed, we derive an expression for gradually increasing the potency of the attack, as a task of the reached service degradation (without knowing in advance the target system capability). The proposed attack strategy, namely SIPDAS (Slowly-Increasing-Polymorphic DDoS Attack Strategy) can be applied to several kind of attacks, that leverage known application vulnerabilities, in order to reduce the service given by the target application server running in the cloud. The term polymorphic is inspired to polymorphic attacks which change message sequence at every successive infection in order to evade signature detection mechanisms. Even if the victim detects the SIPDAS attack, the attack strategy can be re-initiate by using a different application vulnerability, or a different timing.

[6].In this DoS attack detection system which is equipped with previously developed MCA technique and the EMD-L1. The existing technique helps to extract the correlations between individual pairs of two distinct features within each network traffic record and offers more accurate characterization for network traffic behaviors. The latter technique facilitates this system to be able to effectively distinguish both known and unknown DoS attacks from legitimate network traffic. Evaluation has been conducted using the KDD Cup 99 data set and ISCX 2012 IDS evaluation data set to verify the effectiveness and performance of the proposed DoS attack detection system. The results have announce that the detection system achieves maximum 99.95% detection accuracy on KDD Cup 99 data set and 90.12% detection accuracy on ISCX 2012 IDS evaluation data set. It outperforms three state-of-the art approaches on KDD Cup 99 data set and shows advantages over the four NB-based detection approaches on ISCX 2012 IDS evaluation data set. Moreover, the analyses computational complexity of the proposed detection system, which achieves comparable performance in comparison with state-of-the-art approaches. The time cost analysis shows that the proposed detection system is able to cope with high speed network segments. As future research focus, a new CIDS will be invented based on the detection approach proposed in this article. The new CIDS will contribute an enhancement to the security of the increasingly important Cloud computing environments with its capability of handling sophisticated cooperative intrusions.

[8].One of the fundamental security elements in cellular networks is the authentication procedure performed by means of the Subscriber Identity Module that is required to grant access to network services and hence protect the network from unauthorized users. a new kind of denial of service attack based on properly crafted SIM-less devices that, without any type of authentication and by exploiting some specific features and performance bottlenecks of the UMTS network attachment process, are capable of introducing new significant service degradation up to disrupting large sections of the cellular network coverage range. The knowledge of this type of attack can be exploited by many applications both in security and in network equipment manufacturing sectors.

[12] DoS attacks on stream-ing video servers were investigated in partial. In this paper, we investigate DoS resilience of Real Time Streaming Protocol (RTSP). We show that by using a simple command line tool that opens a large number of RTSP connections, we able to launch DoS attacks on the proxy and the server.

• We show that by using a simple tool, it is possible to open hundreds of RTSP connections from a single client to streaming servers.
• We investigate the effect of large number of connections from a single client on the resources of streaming servers and proxies.
• We show that streaming servers allow multimedia players to send some sort of heartbeat messages to keep connections alive.

[13]In this section we present anti-jamming techniques that are built entirely at the PHY layer
1) Simple PHY Layer Techniques: The jamming-to-signal ratio, captured by Equation 3, provides various insights on possible ways to fight against jammers. For instance a legitimate transmitter can increase its transmission power. As another example the distance between the transmitter and the receiver, i.e., the length of the link can be reduced, thus boosting the received signal strength. Both of these approaches are brute force techniques. They result in a decreased jamming-to-signal ratio and hence, can be expected to

improve performance. However, such strategies might not provide significant benefits in CSMA/CA networks (e.g. 802.11, sensor networks, etc.); decreasing the jamming-to-signal ratio will potentially help in cases where only the receiver is affected by the jammer. If the transmitter is able to sense the jammer, packets will not be transmitted at all, causing a severe performance degradation.

## V.CONCLUSION:-

To the best of our knowledge, our survey study is the first of its kind to study and compare DDoS tools and defense mechanisms evolved over the period of time. With the evolution of attacks, it is informed that various counter-measures are proposed and are implemented. Survey study will helps to security professionals to analyze the attack strategies and to come up with robust security solutions. Some of the major challenges in the particular domain and the future work has to be takes place.

## VI.ACKNOWLEDGMENT

The work reported in this paper is supported by the college through the TECHNICAL EDUCATION QUALITY IMPROVEMENT PROGRAMME [TEQIP-II] of the MHRD, Government of India.

## VII.REFERENCES:-

[1]. Zhiyuan Tan, ArunaJamdagni, Xiangjian He, Senior Member, IEEE, Priyadarsi Nanda, Member, IEEE, and Ren Ping Liu, Member, IEEE "A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis". IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS VOL. 25, NO. 2, FEBRUARY 2014.

[2]. MotiGeva, Amir Herzberg, and YehoshuaGev "Bandwidth Distributed Denial of Service: Attacks and Defenses".IEEE FLOODING ATTACKS,JANUARY 2014.

[3]. Jonny Milliken, Member, IEEE,"Impact of Metric Selection on Wireless DeAuthenticationDoS Attack Performance". IEEE WIRELESS COMMUNICATIONS LETTERS, VOL. 2, NO. 5, OCTOBER 2013.

[4]. Wei Wei, Feng Chen, Yingjie Xia, and GuangJin,"A Rank Correlation Based Detection against Distributed Reflection DoS Attacks". IEEE COMMUNICATIONS LETTERS, VOL. 17, NO. 1, JANUARY 2013.

[5]. Massimo Ficco and MassimilianoRak,"Stealthy Denial of Service Strategy in Cloud Computing". IEEE Transactions on Cloud Computing.

[6]. Zhiyuan Tan, Member, IEEE, ArunaJamdagni, XiangjianHe,"Detection of Denial-of-Service Attacks Based on Computer Vision Techniques".IEEE Transactions on Computers.

[7]. Massimo Ficco,"dos attacks against cloud applications". IEEE Transactions on Cloud Computing.

[8]. Alessio Merlo, Mauro Migliardi, Nicola Gobbo, Francesco Palmieri, and Aniello Castiglione, Member, IEEE,"A Denial of Service Attack to UMTS Networks Using SIM-Less Devices". IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 11, NO. 3, MAY-JUNE 2014.

[9]. Yajuan Tang, Xiapu Luo, Qing Hui, and Rocky K. C. Chang,"Modeling the Vulnerability of Feedback-Control Based Internet Services to Low-Rate DoSAttacks".IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO.3, MARCH 2014.

[10]. Nikita Lyamin, Alexey Vinel, Magnus Jonsson, and Jonathan Loo,"Real-Time Detection of Denial-of-Service Attacks in IEEE 802.11p Vehicular Networks". IEEE COMMUNICATIONS LETTERS, VOL. 18, NO. 1, JANUARY 2014.