



## DETECTION STRATEGIC MECHANISM AGAINST DENIAL OF SERVICE ATTACKS: DOS ATTACKS

Arun Kumar Singh

Ewing Christan Institute of Management and Technology,  
Allahabad, Uttar Pradesh, India

Neda Firoz

Ewing Christan Institute of Management and Technology,  
Allahabad, Uttar Pradesh, India,

Arun K. Misra

Motilal Nehru National Institute of Technology,  
Allahabad, Uttar Pradesh, India

**Abstract:** : DOS or Denial-of-service attacks are found in many forms and they're an explicit attempt to block the genuine access of user to the system via reducing availability of the system just similar to physical Dos attacks where for example intentionally the electrical power is removed. Sometimes the attacker may also play with a computing devices and make it inaccessible by altering the existem specification of the management information system. These physical intrusions are tackled by tough security measures and strategies. Although few software guards against some attacks, yet it flops to defend against DoS flooding attacks and it may further exploit unrestricted forwarding of internet packets. DDoS distributed denial of service attacks are another contiguous type of attack over the availability of Internet resources. The attackers are smart enough to penetrate into comparatively large number of computers exploiting weaknesses of different softwares so as to setup distributed attacks. These computers are unsuspecting in nature so they can be easily invoked for planning and attempting attack over more victim systems. Over the time the counter measures are developed attackers also improve the existing attack tools developing as well as imitating techniques for distributed denial-of-service attacks. So it is imperative develop complete expositions for defending against known attack variants of such kinds. However this procedure needs a complete understanding of techniques, prerequisites and scope used in diverse kinds of attacks. This paper tries to describe the scope of DDoS problem in possible comprehensive capacity. We have tried to propose new methods to categories different techniques used in DDoS attack, also categories attack networks and defining characteristics of different software tools that help to build up such attack networks. With this new approach we attempt to propose different classes' methods the target this problem during, before, and after actual DDoS attacks. This work envisioned to stimulate research into efficient creative an effective ramparts, detection mechanism and methods for such attacks. This intern may help to create broad and ample solutions providing generalized approach towards countering known as well as derived DDoS attacks.

**Keywords:** denial of service, attack, ICMP, Treaceback, Syn flooding, Ip filtering

### I. INTRODUCTION

The major cause of incorrect operation in the Internet is probably denial-of-service attacks and hence the most serious menace that the Internet world faces today [1]. In February 2000, a Canadian teenager attacked some of the most important sites of the Internet which included CNN, Amazon, yahoo, eBay and buy. Ever since, attacks seemed to be on the ascent [2]. Regrettably, users are more concerned in using software that are having new and innovative features rather than software negligible or no flaws. Furthermore the security does come with a price. Modern software disburses a huge number of cycles to draw somewhat 3D window via alpha blending that provides small or no progress at all. Thought security remains the major problem in trade, many are not willing to spend many cycles on the security. There are many users that do not bother for whether the system is secure, protected of can it be used as a target or propelling pass for Mal wares of all kinds. The sense of security is deceitful which is perhaps worse than lack of security.

Nevertheless there are many under skilled system administrators that abandon their systems and leave the door open to various threats by not complying to standard measures. Added the point that, number of directly linked libraries, schools, homes [3], offices, or other entities has risen

exponentially lately and one is now able to begin to see the whole aspect of the phenomenon. Security threats can be characterized as:

- Breaches of confidentiality
- Failure of authenticity
- Unauthorized denial of service

### II. DOS OR DENIAL OF SERVICE ATTACK

Dos or Denial-of-service attacks is a common term that validates a resource depleting attack over a server, internet infrastructure such that the server is not able to provide service with valid authentication services[4]. Denial of Services does not give brief study to view of different ways that are being exploited in such an attack. It is not comply itself what is frequently through whichever by using or manipulating a known weakness which comes under categories of vulnerability of the application, so as to crash the computer machine or by Internet control message Protocol (ICMP) packets with great traffic [5].

This will use up all the accessible communication devices, leaving it powerless of allocation other upcoming requests by legitimate users.

### A. Classical DoS

These attacks contain a merely host, and attacking the victim [6]. Normally attacker host system is not adequate bandwidth to consume, over the networks. Thus a bandwidth depleting Dos attack is normally not achievable. However other forms of resource depleting attacks are possible, such as taking advantage of known susceptibilities on the server's application, in command to crash the sensitive system, or by challenging the memory resource of the system via TCP SYN packets [7].

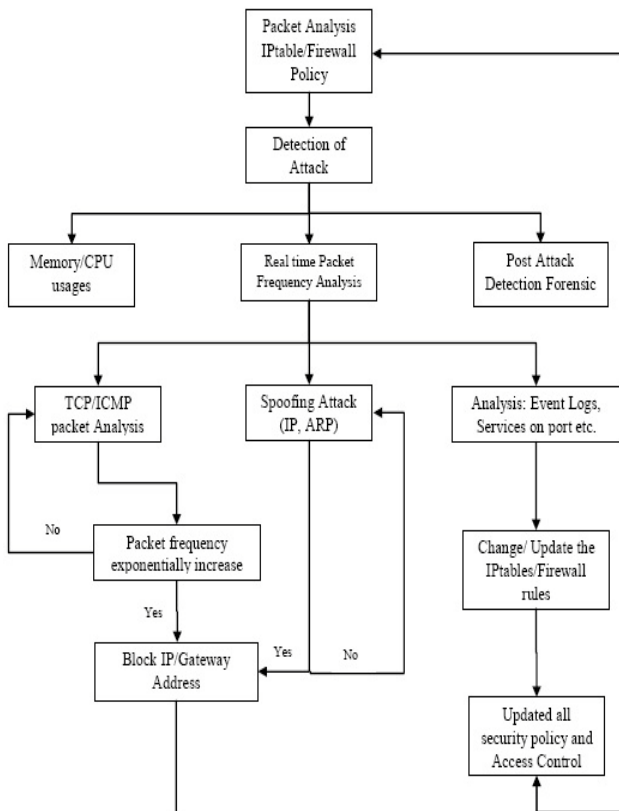


Figure 1. DDoS Attack Classification

While DoS attack use number of computers to direct an attack a single server, DDoS is an acronym used for distributed denial of service attacks. It is a distributed attack in a way that an attacker has to first compromise many intermediate hosts and further using them to attack the victim concurrently. This attack obliges the user to first gain access to large number of computers, before DDoS attack can be done [8]. It is tough to trace the original attacker of a DDoS attack since the attacker himself does not partake in this type of attack, rather he allows the compromised hosts to do this dirty task for him. DDoS attacks are very common these days and are predominantly used for consuming bandwidth resource over the server.

**TCP SYN flooding** is a kind of Dos attack that produces many bad TCP SYN packets concerning a normal connection amid the client and the server using TCP, the connection is initiated by the client using a TCP SYN packet, next the server responds with a SYN ACK packet and finally the client reverts an ACK packet to establish the connection which is commonly known as 3way Handshake. In this TCP SYN attack the attacker initiates 3way Handshake but it is never finished, i.e. an ACK packet is never sent back. This in turn will cause the server to hoard the memory slot for each unfinished

connection. Once the server's memory is occupied with unfinished connections owing to flooding of these packets the server will stop receiving the incoming requests until the memory slots are feed up. Normally this TCP SYN packets use bogus IP addresses to prevent tracing back of the attackers. Missing IP addresses make sure no replies are sent back to the server [9, 10, and 11]. Although TCP SYN flooding may be done using only simple computer yet it's often done via multiple computers. However, in advanced attacks eg. DRDoS (Distributed Reflection DoS) can be attempted using TCP SYN flooding. DRDoS is similar in behavior to SMURF attacks except the fact that TCP SYN packets are used instead of echo requests. We can also say that in DRDoS attack the attacker and large number of TCP SYN packets using victims IP address to intermediary hosts. They are sometimes also known as reflectors and they rely to victim with a large number of SYN /ACK packets. Later if the victim's response is not obtained then it is assumed that the packets are lost [12]. Therefore re-sending of packets is done which further adds on more traffic to the victim side. DRDoS are a new kind of attacks which are difficult to prevent as SYN/ ACK packets are imperative response from reflectors. The reflectors may not be able to tell exactly that either they are participant in DRDoS attack or not, because of the reason that volume of incoming TCP SYN packets are not high such that it becomes flooding.

This is done in a way such that TCP SYN packets are evenly distributed along multiple reflectors and each reflector receives small share of these packets [13]. The basic idea of DDoS attack is to force multiple systems to send large traffic at the same time and place. The congregated traffic that the network machines harvest can painlessly cripple the accessible network infrastructures. Consequently the recipient, the victim of this attack will not be able to have reliable and steadfast network door to access or serve genuine customers, in case if the target machine in a network infrastructure. Today DDoS attacks are simply a small networks systems that are known to be "agents" that regulate a huge amount of system machines called "daemons" or "zombies". These "zombie" systems will finally launch the attack as instructed by the agents [14]. Thus the attacker, to be able to launch an operational DDoS attack, requires huge number of compromised systems acting as "zombies", and may be acquired via any hacking practice. Researchers are yet to sightsee different ways to distinguish factual sources of an incoming attack.

### B. Promising Research

The research in the area of DoS attacks has helped a lot to quantify the frequency and scope of these attacks [15]. While we know backscatter analysis does nothing to stop or mitigate any single DoS attack, and these analysis are based upon certain set of assumptions, one of them is that attacks use random spoofed addresses and hence this analysis does not counts as attacks that do not spoof source addresses [16]. It is hence imperative to take approaches in different directions for analyzing DoS attacks. Although many attacks are characterized at packet level better tools of attack may generate traffic that is not easily identified. The research has helped to enumerate the frequency of DoS attacks [17].

## III. CAUSE OF DoS ATTACKS

One main cause of such TCP SYN attacks seems to be the preliminary communication that takes place before authenticating. The server is unable to distinguish between

legitimate and fake traffics not much can be done here. The requirement that all requests should be first authenticated can be imposed would be an attack of Dos type as the Server spends a lot of time verifying digital signatures to know the authenticity. The new avenue proves to be a dangerous form of attack. Another cause of Dos attacks maybe lack of accounting of resources [18].

All OS implement this kind of framework virtually, and this has not proved adequate in high load environments [19]. The packets incoming are processed in order of highest priority and finally discarded due to the reason that there is no application available for serving them. This kind of scenario is known as Lovelock. Although there is an application to serve incoming packets yet the process priority is not considered [20].

#### A. Counter measures

**Deflect attacks:** Honeypots are systems set up with little security to be an inducement for an attacker such that the attack is targeted at Honeypots and not the real system. Honeypot have great value in deflecting attacks and they even serve as a way to find relevant information about the attackers. This is done storing a record of their activity and further learning of types of attacks.

The latest researches only focus on usage of honeypot systems, which in a way imitate a legitimate network for attracting DDoS attackers. The aim is to attract the attacker and allow him to install agent codes inside the honeypot. This stops few genuine systems from compromising and keeps a track of handler /agents' behavior. This facilitates in better understanding defense mechanism against installation attacks. The central idea is not to stop the attacking packets rather to make sure that users are able to do the normal work in spite of presence of attackers. Hence, a good defense strategy should be able to achieve this goal.

#### B. Post attack forensics

**1 Analysis of traffic pattern:** the traffic pattern data can be analyzed post attack if it is stored during a DDoS attack facilitating a glimpse of characteristics within the traffic. This data further can be used for updating of load balancing and great counter measures for increasing efficiency and protection ability. In addition, these traffic patterns help network administrators in developing new techniques for filtering, preventing entry and exist of DDoS attacks.

**2. Packet trace back:** it is also a kind of strategy that helps in finding identity of attackers using packet traces. The core idea is that the traffic of internet could be traced back the right source rather than that of spoofed addresses. This permits back tracing of the traffic of attackers, while the attacker is busy in sending huge traffics. This method sounds good and assists to provide victim system with relevant information for filtering and blocking the attacks. A model for developing network traffic tracking system has been proposed that may identify and trace the user traffic throughout a network. This kind of system has been successful inside a network eg. Corporate networks-where internal client systems are fully managed by a central network administrator who can trace back individual end user actions. This method breaks down as the Network begins to become widely distributed. Traffic tracing is difficult over large networks [21]. As the control of various sections of Internet is done different network administrator it may be

difficult to find out who may be responsible for monitoring the traffic on the Internet. The unfavorable response is expected from most Internet users because of fear of loss of privacy.

#### C. Event logs

The administrators of networks may keep logs of DDoS attacks and keep up the information so as to perform forensic analysis and thus help to enforce laws in the event of severe financial damage. We may use honeypots, other tools such packet sniffers, firewalls, server logs, etc. to store and find out all the events occurring altogether during execution of an attack. It may help the investigators to find out what kind of attack was done even their combinations could be discovered.

#### D. Detection of the open ports

An open port is like an open door which is left as an invitation for any intruder. Unfortunately there are needs to open up ports such as HTTP or SMTP ports for everyone to see though there are services that are accessible only when required. This is where knocking of Port turns up. Let's assume that services with finite user base need not open their ports all time. SSH is kind of service which only allows password bearing users to come in [22]. Now here the port opens up only from protected and authentic sources which prevent exploitation. The role of IP filters is restricted to control the routes of packets through the TCP /IP stack and also control their flow based on their IP headers. With the help of Port knocking the equivalence of IP address and individual user is not compulsory [23].

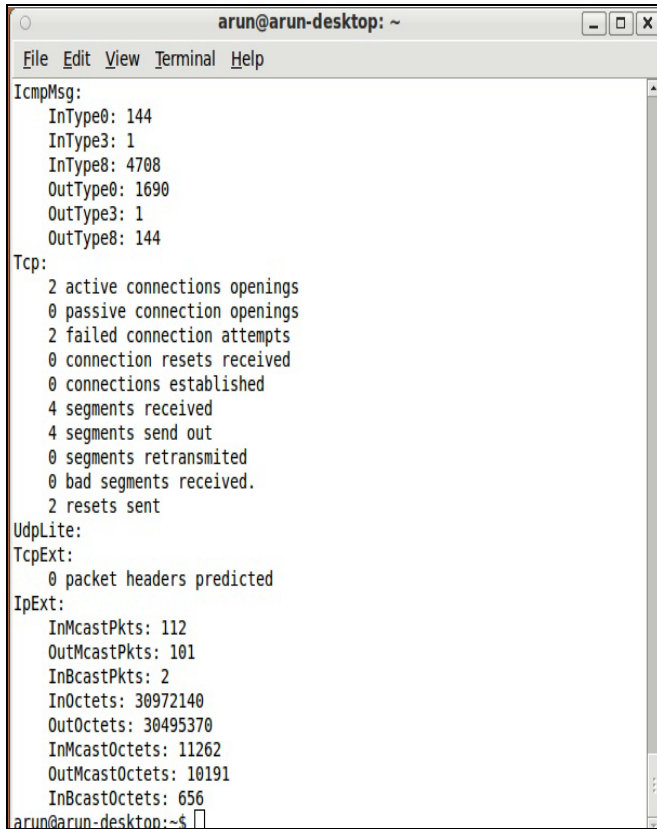
## IV. PROPOSAL WORK

A Denial of Service (DoS) attack aims to end the service made available by a target. It can be launched in two ways. The first way is to exploit software vulnerabilities of a target by distributing deformed or distorted packets and smash the system. The second way is to exploit huge volumes of useless traffic to subjugate all the resources that could service legitimate movements in the network. Though it is possible to protect the first way of attack by repairing known vulnerabilities, the second way of attack cannot be so simply prevented. When the traffic of a DoS attack comes from various sources, we call it a Distributed Denial of Service (DDoS) attack. Through using multiple attack sources, the potential of a DDoS attack is amplified.

#### A. False Positive Rate and Detection Accuracy

We describe a false positive as a normal process that is misdiagnosed by the taxonomic scheme as an attack. The false positive rate is defined as the amount of false positives divided by the total amount of detection decisions made. We express a false negative as an attack that has not been noticed by the detection scheme. The false negative rate is termed as the number of false negatives divided by the total number of detection decisions made. We define the detection accuracy whilst the number of attacks detected divided by the total number of attacks. False positives may cause indirect damage in many cases, but there are other unwelcome methods of high false positive rates. For example, when a reactive system identifies and responds to a DoS attack, it can launch a signal to the system administrator of the targeted system that it is taking

action. In case where most of the signals prove to be false, then the system administrator will ignore them.



```

arun@arun-desktop: ~
File Edit View Terminal Help
IcmpMsg:
InType0: 144
InType3: 1
InType8: 4708
OutType0: 1690
OutType3: 1
OutType8: 144
Tcp:
2 active connections openings
0 passive connection openings
2 failed connection attempts
0 connection resets received
0 connections established
4 segments received
4 segments send out
0 segments retransmitted
0 bad segments received.
2 resets sent
UdpLite:
TcpExt:
0 packet headers predicted
IpExt:
InMcastPkts: 112
OutMcastPkts: 101
InBcastPkts: 2
InOctets: 30972140
OutOctets: 30495370
InMcastOctets: 11262
OutMcastOctets: 10191
InBcastOctets: 656
arun@arun-desktop:~$

```

Figure 2. Detection and countermeasure of Denial of Services

When attack is happening on the victim's system, how the victim knows about attack and verifies as well as analysis all the connection (TCP, ICMP etc.) in and out from the victim's system. Check all the packets either in or out for analysis, if victim block/unblock the all ICMP reply packets, then victim check all the incoming packet and frequency of the packets. After that that analysis of the memory usages, how much memory usages gradually increases as per that frequency after certain time period all the memory has been usages and service has been blocked.

## V. CONCLUSION

The most fundamental tutorial to be learned from distributed denial of service is that all sites on the Internet are interdependent, whether they know about it or not. The impression upon your site and its operations is dictated by the (in) security of other sites and the capability of a remote attacker to implant the tools and, later on, to control and direct more than one system worldwide to launch an attack. Attackers typically exploit well-known vulnerabilities, many of which have readily available fixes. Complicating matters are the intrusion tools that are widely available. Intruders have automated the processes for discovering vulnerable sites, compromising them, installing daemons, and concealing the intrusion. Even security-conscious sites can suffer a denial of service because attackers can control other, more vulnerable computer systems and use them against the more secure site. Thus, although you may be able to "harden" your own systems to help prevent having them used as part of a distributed attack, currently available technology does not enable you to avoid becoming a victim. There is some hope for the future in

technological and other approaches. Handling denial of service is essentially an exercise in risk management. There are sometimes technical solutions to management problems. There are always management solutions to technical problems. We encourage readers to look at denial of service from both points of view.

## VI. ACKNOWLEDGEMENTS

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions.

## VII. ACKNOWLEDGMENT

The preferred spelling of the word "acknowledgment" in America is without an "e" after the "g". Avoid the stilted expression, "One of us (R.B.G.) thanks . . ." Instead, try "R.B.G. thanks". Put applicable sponsor acknowledgments here; DO NOT place them on the first page of your paper or as a footnote.

## VIII. REFERENCES

- [1] K. Stefanidis and D. N. Serpanos, Dept. of Electrical and Computer Engineering, University of Patras, GR-26504 Patras, Greece, Countermeasures Against Distributed Denial of Service Attacks, in IEEE Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications 5-7 September 2005, Sofia, Bulgaria
- [2] A. Belenky and N. Ansari, IP Traceback with deterministic packet marking, in IEEE Communications Letters, Vol. 7, No. 4, , April 2003.
- [3] Lersak Limwivatkul' and Arnon Rungsawangr 'National Electronics and Computer Technology Center, Klong Luang, Pathumthanee, Thailand, Distributed Denial of Service Detection using TCP/IP Header and Traffic Measurement Analysis, Intanational Syinposium on Communications and Information Technologes 2004 ( ISCIT 2004 ) Sappom, Japruui. 2004.
- [4] CERT Coordination Center. "Denial of Service Attacks,"<http://www.ce-.or~t~h-tips/denial-of-serv~ce.html>
- [5] Microsoft Security, "Window 2000 Server Checklist", <http://~.microsoh.comhsecurity>
- [6] A.John1, T Sivakumar, Department of Computer Science, Ramanujam School of Mathematics and Computer Science, Pondichery University, Puduchery, India, DDoS: Survey of Traceback Methods, International Journal of Recent Trends in Engineering, Vol. 1, No. 2, May 2009.
- [7] Workshop on Information Assurance and Security United States Militaly Academy , Proceedings of the 2005 IEEE, West Point, NY Queue-based Analysis of Dos attacks Suraiya Khan, Issa Traore
- [8] D.W. Gresty, Q. Shi, M. Merabti School of Computing and Mathematical Science, Liverpool John Moores University, Byrom Street, UK. Requirements for a General Framework for Response to Distributed Denial-of-Service.
- [9] T. C. Greene, "The Mother of all DDoS attacks looms", 2000. <http://www.theregister.co.uk/000224-000001.html>.
- [10] C. Oakes, "DoS: Defence Is the Best Offence", WIRED online, February 10th 2000. <http://www.wired.com/news/technology/0,1282,34230,00.html>
- [11] Cisco Guard, Cisco Systems. <http://www.cisco.com/en/US/products/ps5888/index.html>
- [12] Cyber Operations. <http://www.cyberoperations.com>
- [13] Lancopet. <http://www.lancopet.com>.
- [14] Mazu Networks. <http://www.mazunetworks.com>.

- [15] Webscreen Technology.  
<http://www.webscreentechnology.com>.
- [16] Survey of Current Network Intrusion Detection Techniques  
[http://www.cse.wustl.edu/~jain/cse571-07/ftp/ids/1\\_of\\_18\\_12/19/2007](http://www.cse.wustl.edu/~jain/cse571-07/ftp/ids/1_of_18_12/19/2007)
- [17] Sailesh Kumar, Bernstein, Dan J. , Survey of Current Network Intrusion Detection Techniques “SYN cookies” from: <http://cr.yt.to/syncookies.html> April 2003.
- [18] Buletinul Stiintific al Universitatii “Politehnica” din Timisoara, ROMANIA, Developments in DoS Research and Mitigating Technologies
- [19] Transactions on AUTOMATIC CONTROL and COMPUTER SCIENCE Vol.49 (63), 2004, ISSN 1224-600X 1
- [20] Computer Emergency Response Team, “CERT advisory CA-2000.01 Denial of service developments”, Jan 2000.(<http://www.cert.org/advisories/CA-2000-01.html>)
- [21] Scott A. Crosby, Dan S. Wallach, “Denial of Service via Algorithmic Complexity Attacks”
- [22] Peter Druschel and Gaurav Banga, “Lazy receiver processing (LRP): a network subsystem architecture for server systems”, In Proceedings of 2nd USENIX Symposium on OSDI, Seattle, Oct 1996.
- [23] Digital Equipment Corporation, “Performance tuning tips for Digital Unix”, June 1996.