Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

*IJCSMC, Vol. 2, Issue. 7, July 2013, pg.207 – 213*

SURVEY ARTICLE

# OVERVIEW OF DDOS ALGORITHMS: A SURVEY

**S. Chithra[1], Dr. E. George Dharma Prakash Raj[2]**
[1]Computer Science & Bharathidasan University, India
[2]Computer Science & Bharathidasan University, India

[1] *chithra.shona@gmail.com;* [2] *georgeprakashraj@yahoo.com*

***Abstract— The significance of the DDOS problem and the increased occurrence, sophistication and strength of attacks has led to the dawn of numerous prevention algorithms. Each proposed prevention algorithms has some unique advantages and dis advantages over the others. In this paper, we present a classification of available algorithms that are proposed in literature on preventing internet services from possible DDOS attacks and discuss the strengths and weaknesses of each algorithm. This paper provides better understanding of the problem and enables a security administrator to effectively equip his arsenal with proper prevention algorithms for fighting against DDOS threat.***

***Key Terms: - DDOS; Types; Algorithms; Tools***

## I. INTRODUCTION

A Distributed denial of service (DDOS) attack is a DOS attack utilizing multiple distributed attack sources. Typically, the attackers use a large number of controlled bots distributed in different locations to launch a large number of DOS attacks against a single target or multiple targets. With the rapid development of bot nets in recent years, the attack traffic scale caused by DDOS attacks has been increasing, with the targets including not only business servers, but also internet infrastructures such as firewalls, routers and DNS system as well as network bandwidth, the attack influence sphere has also become broader. The remainder of this paper is organized as follows. Section II contains types of DDOS attacks. Section III describes variety of available DDOS algorithms. Section IV describes variety of available DDOS attack tools in the details. Finally, section V conclusion the paper and presents further research.

 

## II. DISTRIBUTED DENIAL OF SERVICE

Most common DOS attacks use thousands of computers sometimes hundreds of thousands. Various types of DDOS attacks are given in fig.1

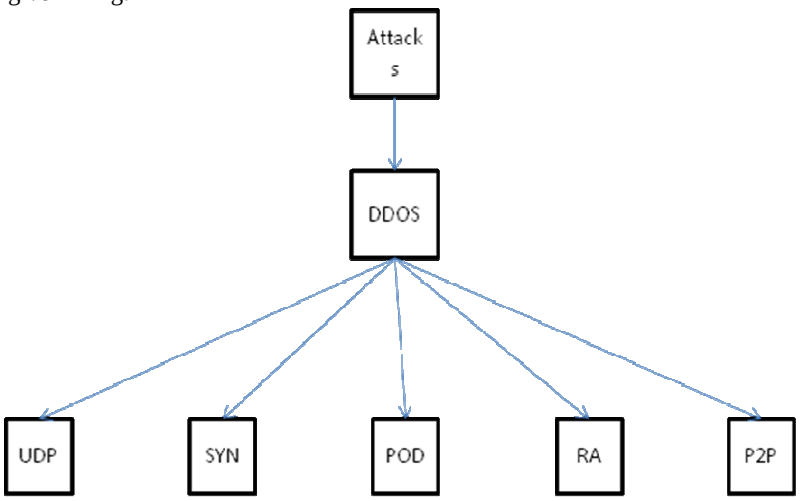


Figure: 1-Types of DDOS attacks

**1. UDP Flood**

User Datagram Protocol is a session less networking protocol. One common DDOS attack method is referred to as a UDP flood. Random ports on the target machine are flooded with packets that cause it to listen for applications on that those ports and report back with a ICMP packet.

**2. SYN Flood**

A "three-way handshake", which is a reference to how TCP connections work, is the basis for this form of attack. The SYN-ACK communication process works like this:

- First, a "synchronize", or SYN message, is sent to the host machine to start the conversation.
- Next, the request is "acknowledged" by the server. It sends an ACK flag to the machine that started the "handshake" process and a waits for the connection to be closed.
- The connection is completed when the requesting machine closes the connection.

A SYN flood attack will send repeated spoofed requests from a variety of sources at a target server. The server will respond with an ACK packet to complete the TCP connection, but instead of closing the connection the connection is allowed to timeout. Eventually, and with a strong enough attack, the host resources will be exhausted and the server will go offline.

**3. Ping of Death**

Ping of death ("POD") is a denial of service attack that manipulates IP protocol by sending packets larger than the maximum byte allowance, which under IPv4 is 65,535 bytes. Large packets are divided across multiple IP packets – called fragments – and once reassembled create a packet larger than 65,535 bytes. The resulting behemoth packet causes servers to reboot or crash.

**4. Reflected Attack**

A reflected attack is where an attacker creates forged packets that will be sent out to as many computers as possible. When these computers receive the packets they will reply, but the reply will be a spoofed address that actually routes to the target. All of the computers will attempt to communicate at once and this will cause the site to be bogged down with requests until the server resources are exhausted.

**5. Peer-to-Peer Attacks**

Peer-to-Peer servers present an opportunity for attackers. What happens is instead of using a botnet to siphon traffic towards the target, a peer-to-peer server is exploited to route traffic to the target website. When done successfully, people using the file-sharing hub are instead sent to the target website until the website is overwhelmed and sent offline.

 

| DDOS | Advantages | Disadvantages |
|---|---|---|
| UDP | Broadcast and multicast connection available | There are no guaranties with UDP It is possible that a packet may not be delivered or delivered twice or delivered in time |
| SYN | Repeated server | Can't repeated server |
| POD | Maximum byte | Minimum byte |
| RA | Possible | Is not possible |
| P2P | P2P networks client provide resources. Like bandwidth, storage space, and computing power | P2P networks related to the topic of data backup recovery and availability |

Figure: 2-Advantages and Disadvantages of DDOS types

## III. DISTRIBUTED DENIAL OF SERVICE ALGORITHMS

The following are the various types of DDOS Algorithms available.

**1) ASA:**

It is hypothesized that mimicking natures principles, and is not its epiphenomena, leads to better algorithms. The so called adaptive sampling framework is used for analyzing the 3-SAT problem, which led to one neural method and five mixed methods, that mix elements of EC and of NC in different ways. These methods have been tested against the best currently know incomplete 3-SAT algorithm. The basic principle behind these algorithms is to sample isolated features from the problem and from candidate solutions, which are adapted iteratively. Evolutionary and neural computations are the two main subfields of this class. This class of algorithms has been dubbed adaptive sampling, and it is described by the adaptive sampling framework.

**2) CA:**

Cluster algorithm or clustering is the task of grouping a set of objects in such a way that objects in the same group called cluster are more similar in some sense or another to each other than to those in other groups clusters. The appropriate clustering algorithm and parameter settings including values such as the distance function to use, a density threshold or the number of expected clusters depend on the individual data set and intended use of the results. Clustering algorithms can be categorized based on their cluster model, there is no objectively "correct" clustering algorithm, but as it was noted, "clustering is in the eye of the beholder". The most appropriate clustering algorithm for a particular problem often needs to be chosen experimentally, unless there is a mathematical reason to prefer one cluster model over another. It should be noted that an algorithm that is designed for one kind of models has no chance on a data set that contains a radically different kind of models. Example: k-means cannot find non-convex clusters [2].

**3) TCM-KNN:**

Transductive confidence machines for K-Nearest Neighbors algorithm to fulfill DDOS attacks detection task towards ensuring the Qos of wed server. The method is good at detecting network anomalies with high detection rate, high confidence and low false positives than traditional methods, because it combines "strangeness" with "p-values" measures to evaluate the network traffic compared to the conventional ad-hoc thresholds based detection and particular definition based detection. The input feature spaces of TCM-KNN to effectively detect DDOS attack against web server. Finally, we introduce genetic algorithm(GA) based instance selection method to boost the real time detection performance of TCM-KNN and thus make it be an effective and lightweight mechanism for DDOS detection for web servers[3].

**4) CA:**

Congestion algorithms to detect upsurges in traffic that can give rise to DOS but this approach may apply only simplistic signatures and also requires state information to be held on the nodes which is not a feasible solution in sensors because of limited memory [4].

 

**5) DSA:**

In computer science, streaming algorithms are algorithms for processing data streams in which. The input is presented as a sequence of items and can be examined in only a few passes typically just one. These algorithms have limited memory available to them much less than the input size and also limited processing time per item. These constraints may mean that an algorithm produces an approximate answer based on a summary or "sketch" of the data stream in memory. Streaming algorithms have several applications in networking such as monitoring network links for elephant flows, counting the number of distinct flows, estimating the distribution of flow sizes [5].

**6) MLA:**

A branch of artificial intelligence is about the construction and study of systems that can learn from data. For example, a machine learning system could be trained on email messages to learn to distinguish between spam and non-spam messages. After learning, it can then be used to classify new email messages into spam and non-spam folders. The core of machine learning deals with representation and generalization. Representation of data instances and functions evaluated on these instances are part of all machine learning systems. Generalization is the property that the system will perform well on unseen data instances; the conditions under which this can be guaranteed are a key object of study in the subfield of computational learning theory. There is a wide variety of machine learning tasks and successful applications. Optical character recognition, in which printed characters are recognized automatically based on previous examples, is a classic example of machine learning.

**7) RA:**

As mentioned above, the shortest paths are calculated using suitable algorithms on the graph representations of the networks. Let the network be represented by graph G (V, E) and let the number of nodes be 'N'. For all the algorithms discussed below, the costs associated with the links are assumed to be positive. A node has zero cost itself. Further, all the links are assumed to be symmetric, i.e. if $d_{i,j}$ = cost of link from node i to node j, then $d_{i,j} = d_{j,i.}$ The graph is assumed to be complete. If there exists no edge between two nodes, then a link of infinite cost is assumed. The algorithms given below find costs of the paths from all nodes to a particular node. The problem is equivalent to finding the cost of paths from a source to all destinations.

**8) RSA:**

A node will initiate a distributed lookup according to the specific p2p routing substrate algorithm. A query message or object key lookup takes O (log N) application layer hops from source to destination. Each node has a routing table with O (log N) entries where each node entry maps a node identifier to an IP address and port number. Using routing table, each intermediate node along the routing path will forward the message to the best node in its routing table among all the candidate nodes stored as routing table entries. Here the best node in the routing table is specific to the particular routing algorithm [6].

**9) TTA:**

To trace back the source of the DDOS attacks in the internet is extremely hard. It is one of the extraordinary challenge to trackback the DDOS attacks, that attackers generate huge amount of requests to victims through compromised computers zombies in order to denying normal services or degrading the quality of services. IP trace back means the capability of identifying the actual source of any packet across the internet; with the help of IP trace back schemes identify the zombies from which the DDOS attack packets entered the internet.

**10) NCA:**

Due to increase in number of users on internet, many people want to attack other system resources. Competitors also want to make their web site more popular than others. So they want to attack the service of other's web site. They keep on logon to a particular web site more times, and then service provided by the web server performance keeps degraded. To avoid that one, this application maintains a status table. In that it keeps the IP addresses of current users and their status. If the particular IP address has been signed on for a first time, it makes the status as genuine user. For 2, 3, 4 it marks as Normal user. For the fifth time it makes the particular IP address status as Attacker. In the time calculations we are only consider 5 times. User wish to server increase the time depends up on the application. After that, the user cannot allow get the service of that particular web site. The service is denied to that particular IP address.

 

| **Algorithms** | **Command Used** | **Types of attack generate** | **Advantage** | **Disadvantage** |
|---|---|---|---|---|
| ASA | Static encryption | TCP SYN,TCP ACK,ICMP-ECHO | That is reduce bandwidth end storage requirement | Can't storage requirement |
| CA-PAA | Static encryption | SYN Flood,Trinoo,TFN2K | Detect DDOS attack in real time | Detect DDOS attack in real time |
| TCM-KNN | Anomaly detection | UDP BOMBING, TCPSYN FLOODING | Instance selection optimization the TP(true positive rate)for TCM-KNN keeps high | Instance selection optimization the FP(false positive rate)for TCM-KNN keeps low |
| CA | Stateless & state full signatures | public key cryptography | A cost effective design and more effective implementation of overall application | Implementation can't effective |
| DSA | Insertions & deletion | TCP TCP- SYN-Flooding | large distinct frequencies in small space and small update/query time | large distinct frequencies in large space and large update/query time |
| MLA | Intrusion, detection security, sensor networks | Black holes, Flooding | Nodes spend 90% of their time successfully | Nodes spend 10% can't successfully |
| RA | No encryption | SYN Flood, UDP Flood | A successful intrusion requires all defense level | During the transient period valid packets can be dropped |

| | | | | |
|---|---|---|---|---|
| RSA | Database, audio, Video | Object key | Set of sending Peers based on query result | Reducing the number of request granted to attackers |
| TTA | Dataset, Conventional comparison | Fast entropy scheme | Reduced 90% detection accuracy | Only for false error type |
| NCA | MAC generator | TCP SYN packet | We are only consider for five times | Packet cannot match the function drop silently discard |

Figure: 3-Advantages and Disadvantages of DDOS Algorithms

 

## IV. DDOS ATTACK TOOLS

There are a variety of different DDOS attack tools. On the internet that allow attackers to execute attacks on the target system. Some of the most common tools are

1. Trinoo [8, 9] can be used to launch a coordinated UDP flooding attack against target system. That used to master/slave architecture and attacker controls a number of trinoo master machines. Communication between attacker and master.
2. Ten [9] communication between the attacker and the control master program but no encryption. Communication between the control masters and slaves is done ICMP echo reply packet. It can implement SYN Flood, UDP Flood, and ICMP Flood attacks.
3. Ten 2k [10] we can use encrypted and ICMP flooding and TCP is flooding and UDP flooding smurf Mix flood. Master to slave can be mixture of encrypted TCP UDP and ICMP slave to master.
4. Stacheldraht[11] communication between the attacker and the control master but encryption. It is used to ICMP flooding and TCP flooding and UDP flooding smurf to attacker to master encrypted TCP master to slave-TCP and ICMP slave to master.
5. Shaft [12] Not encrypted it is used to ICMP flooding and TCP flooding and UDP flooding to attacker to master –unencrypted TCP master to slave –unencrypted UDP.
6. Mstream [13] Not encrypted it is used to TCP flooding that can be attacker to master –unencrypted TCP master to slave –Unencrypted UDP slave to master –Unencrypted UDP.
7. Knight [14] Not encrypted it is used to TCP flooding and UDP flooding an urgent pointer flooder. Uses IRC as its communication method.
8. Trinity [15, 16] not encrypted used to TCP flooding and UDP flooding it is IRC as its communication method.

## V. CONCLUSION

In this paper, we covered an overview of the DDOS problem, available DDOS attack tools, defense challenges and principles, and a classification of available DDOS prevention algorithms. This provides better understanding of the problem and enables a security administrator to effectively equip his arsenal with proper prevention algorithms for fighting against threat. The current prevention algorithms reviewed in this paper are clearly far from adequate to protect internet from DDOS attack. The main problem is that there are still many insecure algorithms over the internet that can be compromised to launch large scale coordinated DDOS attack.

## REFERENCES

[1] K.Kumar, R.C.Joshi and K.Singh,"An Integrated Approach for Defending against Distributed Denial-of-Service (DDOS) Attacks", iriss, 2006, ITT Madras.
[2] SUN Ji-Gui,and LIU jie."Clustering Algorithms Research,"Journal of software, vol.19, pp.48-61, 2008.
[3] Y.Li, B.X.Fang, L.Guo, and Y.Chen,"Network Anomaly Detection Based on TCM-KNN Algorithm,"pp.13-19, 2007.
[4] C.Wan,S.Eisenman, and A.Campbell. "CODA: Congestion Detection and Avoidance In Sensor Networks",In ACM SASN'03,2003,pp.266-279.
[5] S.Ganguly,M.Garofalakis,R.Rastogi,and K.Sabnani."StreamingAlgorithmsfor Robust,Real-Time Detection of DDOS Attacks".
[6] K.Park and H.Lee."On the effectiveness of route-based packet filtering for distributed DOS attack prevention in power-law Internets."
[7] An effective prevention of attacks using giTime frequency algorithm under DDOS by Dr.K.Kuppusamy,s.Malathi,International journal of network security & its Applications (IJNSA),vol.3,no.6,November 2011.
[8] J.Mirkovic,P.Reiher,"A Taxonomy of DDOS Attack and DDOS defense Mechanisms,"ACM SIGCOMM Computer Communications Review, Volume 34, Issue 2,pp. 39-53,April 2004.
[9] D.Dittrich,"The DOS project's Trinoo Distributed Denial of Service attack tool, "University of Washington, October 21, 1999.Available at:http://staff.washington.edu/dittrich/misc/trinoo.analysis.txt.
[10] J.Barlow, W.Thrower,"TFN2K-An Analysis,"Axent Security Team. February 10, 2000. Available at: http://security.royans.net/info/posts/bugtraq_ddos2.shtml.
[11] D.Dittrich,"The Stacheldraht Distributed Denial of Service attack tool, "University of Washington, December 1999.Available.
[12] S.Dietrich, N.Long, D.Dittrich,"Analyzing Distributed Denial of Service tools: The Shaft Case, "in Proceedings of the 14th Systems Administration Conference (LISA 2000), New Orleans, LA, USA, pp.329-339, December 3-8, 2000.

 

[13] D. Dittrich, G. Weaver, s.Dietrich, and N. Long, "The "Mstream" distributed denial of service attack too, "May 2000.
[14] Bysin,"Knight.c sourcecode,"PacketStormSecurity.nl, July 11, 2001.
[15] B.Hancock,"Trinity v3, a DDOS tool, "hits the streets, computer Security 19(7), pp.574, 2000.
[16] M.Marchesseau,"Trinity-Distributed Denial of Service Attack Tool," 11 Sept, 2000. Available at : http://WWW.giac.org/

 