International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-4, Issue-1)

Research Article | **January 2015**

Mitigating Application DDoS Attacks using Random Port Hopping Technique

R Praveen Kumar[1], Jagdish Babu[2], T. Guna Sekhar[3], S. Bharath Bhushan[4]
[1,2]Assistant Professor, Dept. of CSE, VEMU Institute of Technology, P. Kothakota, India
[3]Research Scholar, Dept. of CSE, KL University, Vijayawada, India
[4]Research Scholar, School of IT, VIT University, Vellore, India

Abstract—

Distributed denial of service attacks are growing rapidly with the help of internet to target the network resources. Every year, 76% of distributed denial of Service attacks are happened towards customers only. End users are losing their services due to application layer distributed denial of service attacks. Detecting the Application layer attacks are more complex compare to other attacks. In this paper proposed a technique to avoid application layer denial of service attacks. In this technique server is dynamically changing their port number with function of time based on the random number generator.

Keywords— Application DOS attacks, Port hopping, NAT, Port numbers, Random number generator.

I. INTRODUCTION

Presently, Internet plays a major role in our everyday scenario. For example, online trading, bank transactions, hospital data maintenance, automated vehicles, and so on. Also many internet dependent electronic devices are rapidly growing with reducing human effort, particularly by means of communication, where, internet is a good interface between the remote applications to exchange the information.

Internet is affected by various threads like SQL Injection, XSS (Cross Site Scripting) attacks, DDOS attacks, etc [4]. Each thread focuses with specific effect on particular type of network. One of the top threads in the network is DDoS (Distributed Denial of Service) attacks. The main aim of the DDoS attack is, to unavailable the network resources, or compromise the web servers [3]. DDoS attacks are classified into three categories that is network layer (or layer 3) attacks, transport layer (or layer 4) attacks, and application layer (or layer 7) attacks.

Table 1: 2012 Q2 to 2013 Q3 DDOS attack metrics

	2012 Q2	2013 Q1	2013 Q2
Layer 3 and 4 attacks	80.95%	76.54%	74.71%
Layer 7 attacks	19.05%	23.46%	25.29%

The above table 1 [1] shows percentage of DDoS attacks occurred in various quarters from 2012 to 2013. Layer 3 and 4 attacks are decreased 6.24% from Q2 2012 to Q2 2013. Layer 7 attacks are increased 6.24% from Q2 2012 to Q2 2013. At present online applications (like Commercial applications / open source applications) are increasing due to people are fascinated towards smart trend. Customers are purchasing commercial applications for fulfilling their dedicated and custom purpose. But commercial application vendors are trying to avoid the internet attacks like DDoS attacks for their premium users.

Now, conventional enterprise security mechanisms such as firewalls, and Intrusion Detection System or Intrusion Prevention System are utilized to manage enterprise security services or ISP framework [5]. The current wireless security measures are not well to protect the sensitive information over internet. Most of the wireless devices need enhanced security techniques to provide the sensitive information. Every time, intruders changing their behaviour to target the sensitive/ dedicated system. Always intruders are trying to break the system logically rather physically. With against to intruder, we need to update security mechanisms to protect the systems over internet, periodically. In this paper we proposed an efficient mechanism to mitigate application denial of service attacks.

The rest of the paper is organized as follows: In section 2, we introduce the application DDoS attacks. In section 3, we introduce port hopping technique. In section 4, we introduce proposed method for mitigating application dos attacks. In section 5, results and analysis. We conclude this paper in section 6.

II. APPLICATION DDOS ATTACKS

Application DDoS attacks are growing rapidly and harder to trace. These attacks are targeting the application layer design and implementation to prevent authorized access to the victim services and diverting the application access controls. The attacks are not detectable by existing enterprise security monitoring, because attacks does not consume more bandwidth and indistinguishable from normal traffic. They use HTTP or HTTPS as their communication and they maintain own proxy servers for obfuscate the true origin of the attacker. A small survey on application layer DDoS attacks are shown in figure 1 [2].

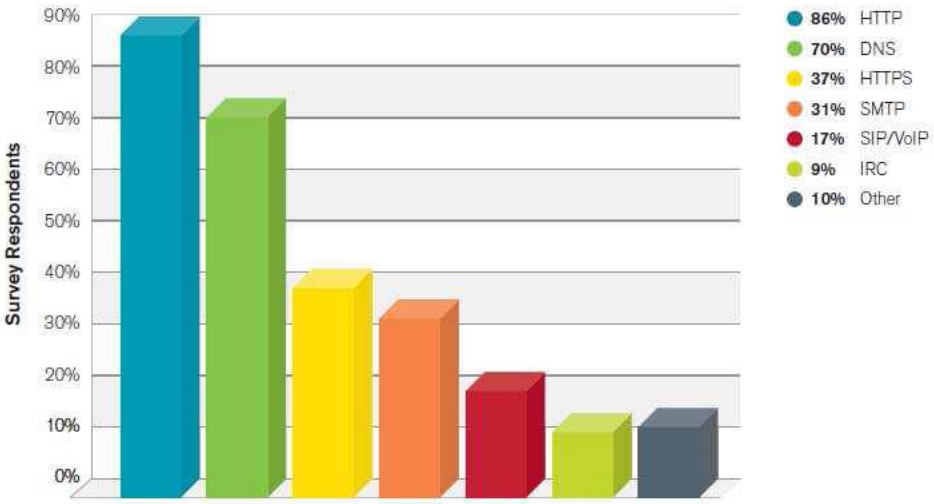

Figure 1: Targets of Application-Layer Attacks

2.1 Volumetric DDoS attacks

These attacks targeting web servers with high bandwidth consuming such as ICMP or UDP flooding attacks [8]. Attack trace backing and detection is easy with enterprise security devices.

2.2 Application layer DDoS attacks

These attacks consume low bandwidth to target specific well known applications like [8, 3] HTTP, DNS, VOIP, and SMTP etc. Trace backing and detection of the attack is harder.

III. PORT HOPPING TECHNIQUE

Port hopping is efficient technique for mitigating application layer denial of service attacks. Before that we need to know about; what is network address translation (NAT)? And what is port number and where we can use the port numbers?

3.1. NAT

When the system is connected to internet, each system having private address and global address. Private address for internal communication and global address for communication with rest of the world. NAT provides mapping between private address and global address. All incoming/outgoing packets go through the NAT router, which replaces the destination/source address in the packet with the appropriate private address/global address shown in below figure 2 [6].

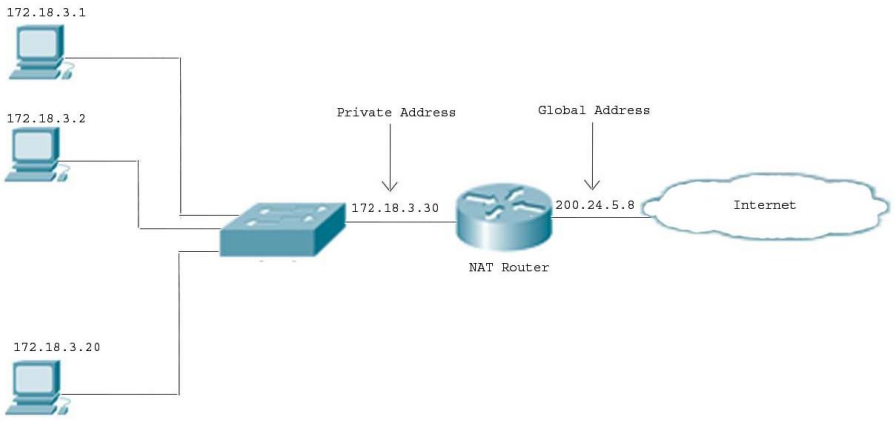

Figure 2: Network Address Translation

Translating private/global address are stored in the translation table. Translation table is deployed in NAT router. The translation table consists of five fields those are private address, private port number, external address, external port number, transport protocol. The translation table has shown in below table 2 [4].

Table 2: NAT Translation Table

Private Address	Private Port Number	External Address	External Port Number	Transport Protocol
172.18.3.1	1400	25.8.3.2	80	TCP
172.18.3.2	1401	25.8.3.2	80	TCP
-----	-----	-----	-----	-----

The above table having two different hosts inside private network with addresses 172.18.3.1 and 172.18.3.2. They need to access HTTP server on external host 25.8.3.2. When the response from 25.8.3.2 to NAT. NAT will divide the packets based on the private port number and then forward to the appropriate private address. These attacks consume low bandwidth to target specific well known applications like [8, 3] HTTP, DNS, VOIP, and SMTP etc. Trace backing and detection of the attack is harder.

3.2. Port Number

The network layer is responsible for host to host communication. Network layer protocol is capable for delivering the message to the destination node. Transport layer is responsible for delivery the message from process to process communication [6]. Figure 3 shows process to process communication.

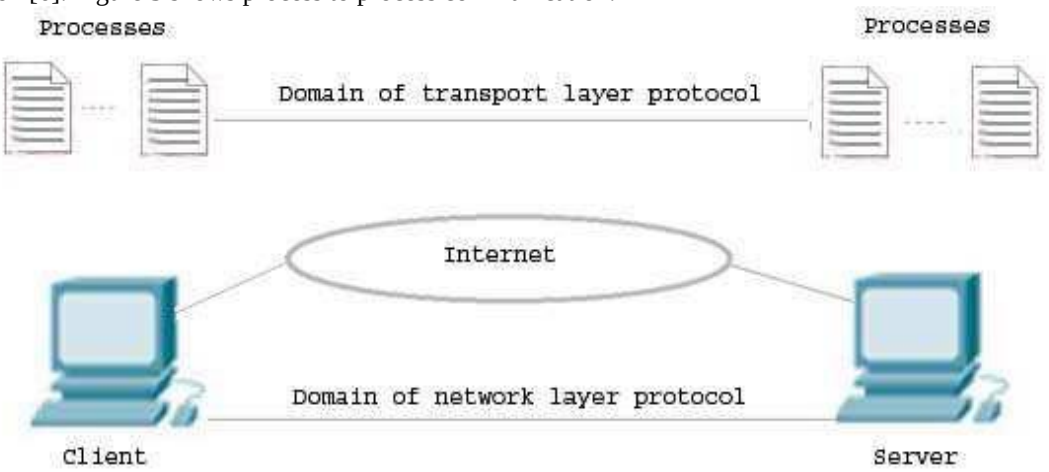

Figure 3: Process to Process Communication

Hosts (local host/remote host) are defined using IP addresses. Processes are defined using port numbers. The range of the port numbers 0 to 65535. ICANN, 65536 port numbers are classified into 3 categories that is well known ports, registered ports, and dynamic ports [6]. First, well known ports ranging from 0 to 1023. These are reserved for unique identification purpose and controlled under ICANN. Second, registered ports ranging from 1024 to 49,151 are registered, but not controlled under ICANN. Third, dynamic ports ranging from 49,152 to 65535; not controlled under ICANN. These port numbers are used for temporary process to process communication.

In port hopping technique, client and server they establish a connection. At the time of data transmission server port numbers are changing randomly as a function of time slots. In this scenario complete time is divided into discrete slots *TSi*, where *i*=0, 1, 2,…, let each time slot duration *t* [5]. In UDP/TCP, the port numbers are unchanged for particular communication interval. In port hopping technique, different port numbers are used in different time slots for the same service. Let *Pi* represents the port number used by the server in time slot *TSi*. *Pi* is determined by equation (1), where *k* is a shared cryptographic key between the server and the client and f is a pseudo-random number generator [5].

$$Pi=f(i,k) \quad \rightarrow \quad (1)$$

Client wants to communicate with the desired server, then it will find the servers present port number *Pi* using the shared secret key *k* and the time slot number *i*. When the server receives packets from client, If packet having invalid port numbers, then they can be easily found and filtered off and no need to examine the contents of the packets. Finally, server reduces the malicious packets. Packet may reach near the boundary of time slots. Time synchronization errors between server and client, two ports are used at the boundaries of time slots [5].

IV. PROPOSED TECHNIQUE

Attackers are targeting high profile web servers to degrade server resources. Where attacker means, either botnet or zombies. They unnecessary to generate traffic to forward specific web servers. To unavailable network resources. By using this proposed method we can avoid such type of attacks.

In server and client communication first they will establish a connection through either 3 way handshake protocol/ 4 way hand shake protocol. After establishing the connection; they ready to transfer the information/ data from client to server or server to client vice versa. Now the complete information is subdivide into packets. Each packet having source address and source port number, destination address and destination port number, and protocol. In this proposed technique the port numbers are dynamically changing at various time intervals. By using this scenario it will avoid the botnet attacks or application layer denial of service attacks.

After establishing the connection, server will shares two non negative prime numbers. Assume *a* and *b* are two public keys. Client will generate secret keys *(n, m)*. Where $n = ab$; $m = (a-1)(b-1)$. Randomly choose *P* value in the range of $1<P<m$. Where *P* should be co-prime of *m*. Compute *Q* value by using below formula,

$$P * Q = 1 \bmod n$$

Server port numbers are dynamically changing based on the PRNG technique that is linear congruential generator [7] to generate random numbers.

$$Xn+1 = (PXn + Q) \bmod M$$

Client received and regenerated two secret non negative prime numbers that is *P* and *Q*. Now client can able to generate random port numbers based on the secret keys. Here *X*n is called seed. Let *Xn* is always constant (that is 1024). Where *M* indicates maximum range of port number(that is 65535). Client uses above mathematical notations to generate random port numbers. Through this technique client will actively communicate with the server and to mitigate the application layer distributed denial of service attacks.

V. RESULTS AND ANALYSIS

In quarter 2 2012, application denial of service attacks are increased to 19.05%. In quarter 2 2013, application layer denial of service attacks are increased to 25.29%. Every year application dos attacks are growing rapidly to target high profile web servers and network resources. In this paper proposed a novel technique that is port hopping to avoid application denial of service attacks. In this proposed technique server port numbers are dynamically changing as a function of time and share the cryptographic keys. Authorized clients can easy to determine the server port numbers and access the authorized information. This technique is more secure and efficient than other techniques. This technique has implemented and tested the randomness of the port numbers for exchanging the information.

VI. CONCLUSION

A In client server communication, they are using IP address and port number. But attackers gain this information to target the high profile web servers to degrade their performance. Control measures are also unable to detect the application layer denial of service attacks. In this paper we implemented a port hopping technique to avoid application layer denial of service attacks. In this proposed technique, initially server share cryptographic key to client for generating random port numbers. Client can use the random port numbers for exchanging their information with the server. This proposed port hopping technique is more secure and efficient than others to mitigate the application layer attacks.

REFERENCES

[1] Prolexic, “Prolexic Quarterly Global DDoS Attack Report," 2013.
[2] Arbor Networks, “Arbor Special Report: Worldwide Infrastructure Security Report”, Arbor Special Report, Vol. 8, 2012.
[3] Zhang Fu, Marina Papatriantafilou, and Philippas Tsigas, “Mitigating Distributed Denial of Service Attacks in Multiparty Applications in the Presence of Clock Drifts,” *IEEE Transactions on Dependable And Secure Computing*, vol. 9, May/June 2012.
[4] Yash Pravinkumar Raithatha, Chirag Suryakant Thaker, “Various Methods used for the Protection, Detection and Prevention of Application Layer DDOS Attacks,” in IJCSMR, Vol. 2, May 2013.
[5] H. Lee and V. Thing, “Port Hopping for Resilient Networks," in Proc. IEEE 60th Vehicular Technology Conf, Vol.5, pp. 3291-3295, 2004.
[6] Behrouz A. Forouzan, “TCP/IP Protocol Suite," in Tata McGraw-Hill Edition, 2011, pp-147-379.
[7] http://www.math.utah.edu/pa/Random/Random.html
[8] Christos Douligeris, Aikaterini Mitrokotsa, “DDoS attacks and defense mechanisms: classification and state-of-the-art," in Elsevier, pp. 645-666, 2004.

