A Review of DDOS Attack and its Countermeasures in TCP Based Networks

Akash Mittal[1], Prof. Ajit Kumar Shrivastava[2], Dr. Manish Manoria[3]

[123]Department of Computer Science & Engineering, TRUBA Institute of Engineering & Information Technology, Bhopal, M.P, India
[1]akash_mitt87@yahoo.co.in , [2]ajitshrivastava@rediffmail.com , [3]manishmanoria@rediffmail.com

ABSTRACT

Today, Internet is the primary medium for communication which is used by number of users across the Network. At the same time, its commercial nature is causing increase vulnerability to enhance cyber crimes and there has been an enormous increase in the number of DDOS (distributed denial of service attack) attacks on the internet over the past decade. Network resources such as network bandwidth, web servers and network switches are mostly the victims of DDoS attacks.

In this paper basically summarizing different techniques of DDoS and its countermeasures by different methods such as Bloom Filter, Trace Back method, Independent Component Analysis and TCP Flow Analysis.

Keywords

Bloom Filter, DDOS attack, Independent Component Analysis, Trace Back Method, TCP Flow Analysis

1. INTRODUCTION

Secure communication has some desirable security aspects such as confidentiality, authentication, message integrity and non repudiation. Besides, recently more people are aware that availability and access control are also urgent requirements of secure communication because of the notorious Denial of Service (DoS) attacks that render by the illegitimate users into a network, host, or other piece of network infrastructure to harm them, especially it is done against the frequently visited websites of a number of high-profile companies or government websites. DDoS (Distributed Denial of Service) attack utilizes adequate puppet computers to create amount of data packets**,** the attacks become coordinated and come from multiple puppets at the same time thus are even devastating.

A typical DDoS attack contains two stages, the first stage is to compromise susceptible systems that are accessible in the Internet and install attack tools in these compromised systems. This is known as turning the computers into "zombies." In the second stage, the attacker sends an *attack command to the "zombies"* through a secure channel to launch a bandwidth attack against the targeted victim(s).

The current attacks on trendy web sites like Amazon, Yahoo, e-Bay and Microsoft and their resultant disruption of services have uncovered the weakness of the Internet to Distributed Denial of Service (DDoS) attacks. It has been observed through reports that more than 85% of

DOI : 10.5121/ijcses.2011.2413

the DoS attacks use TCP [19]. The TCP SYN flooding is the most commonly-used attack. It consists of a stream of spoofed TCP SYN packets directed to a listening TCP port of the victim. Not only the Web servers but also any systems connected to the Internet providing TCP-based network services, such as FTP servers or Mail servers, are susceptible to the TCP SYN flooding attacks.

This paper is organized in such a manner that section 2. is illustrating Type of DDOS Attacks followed by Attack analyzing tools in section 3. In section 4 counter measures against DDOS attacks define with The TCP-Based DDOS Attack and Bloom Filter. In Section 5 independent component analysis has defined with methods and conclusion of the paper describe in section 6.

2. Types of DDoS Attack

Before classification of DDoS attacks, we describe a typical DDoS attack scenario. Then we introduce why it is so prevalent, and its intrinsic reasons why it is so easy to launch. Figure (1) shows a hierarchical model of a DDoS attack. DDoS attack divide into 2 types. One is bandwidth depletion. This method is to congest the network, massive use of the bandwidth then lead the network breakdown. The other type is resource depletion. Attacker depletes the key resources such as CPU, memory and so on. Then break the server [1]. The attack usually starts from numerous sources to aim at a single target. Multiple target attacks are less common; however, there is the possibility for attackers to launch such type of attack Spoofed, altered, or replayed routing information

2.1 *SYN flood attack*

Any system providing TCP-based network services is potentially subject to this attack. The attackers use half-open connections to cause the server exhaust its resource to keep the information describing all pending connections. The result would be system crash or system inoperative [9].

2.2 *TCP Reset Attack*

TCP reset also utilize the characteristics of TCP protocol. By listening the TCP connections to the victim, the attacker sends a fake TCP RESET packet to the victim. Then it causes the victim to inadvertently terminate its TCP connection [2].

2.3 *ICMP attack*

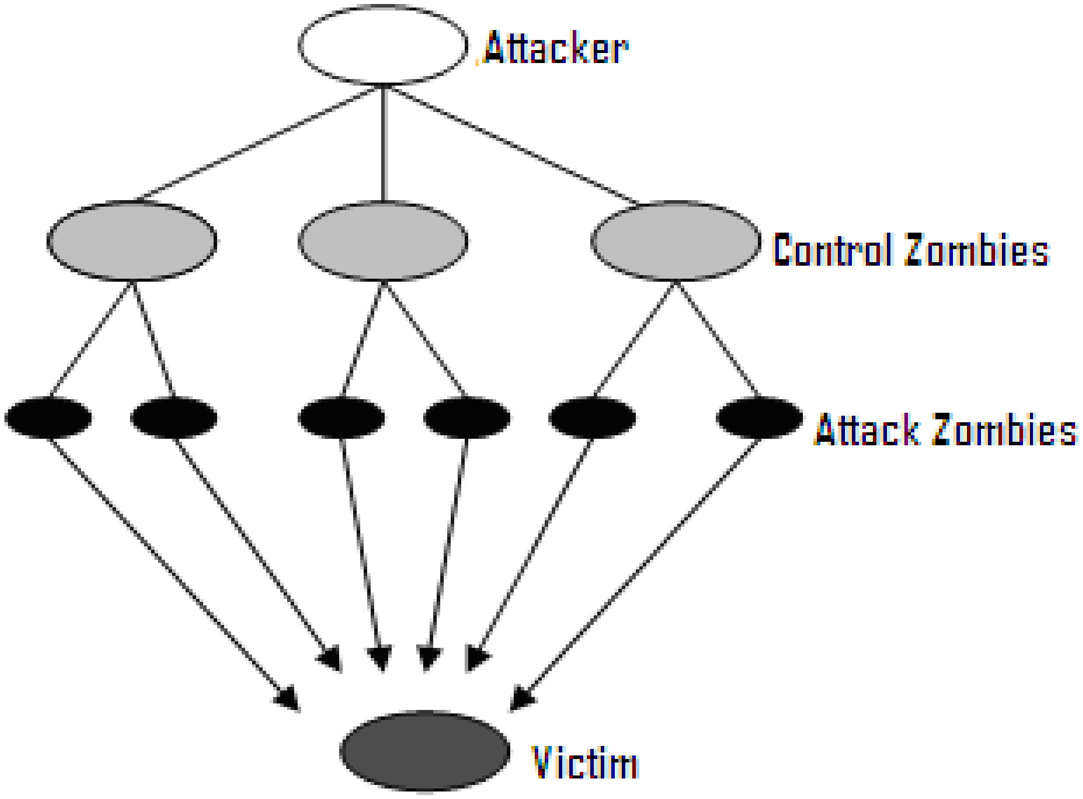
Smurf attack sends forged ICMP echo request packets to IP broadcast addresses. These attacks lead large amounts of ICMP echo reply packets being sent from an intermediary site to a victim, accordingly cause network congestion or outages [CER98]. ICMP datagram can also be used to start an attack via ping. Attackers use the ping Command to construct oversized ICMP datagram to launch the attack [6].

2.4 *UDP storm attack*

This kind of attack can not only impair the hosts. Services, but also congest or slow down the prevailing network. When a connection is established between two UDP services, each of which produces a very huge number of packets, thus cause an attack.

2.5 *DNS request attack*

In this attack scenario, the attack sends a large number of UDP-based DNS requests to a name server using a spoofed source IP address. Then the name server, acting as an intermediate party in the attack, responds by sending back to the spoofed IP address as the victim destination. Because of the amplification effect of DNS response, it can cause serious bandwidth attack [10].



2.6 *CGI request attack*

By simply sending multiple CGI request to the target server, the attacker consumes the CPU resource of the victim. Then the server is forced to terminate its services.

2.7 *Mail bomb attack*

A mail bomb is the sending of a enormous amount of e-mail to a specific person or system. A huge amount of mail may simply fill up the recipient's disk space on the server or, in some cases, may be too much for a server to handle and may cause the server to stop working. This attack is also a kind of flood attack [3].

2.8 *ARP storm attack*

During a DDoS attack, the ARP request volume can become very massive, and then the victim system can be negatively affected

2.9 Algorithmic complexity attack

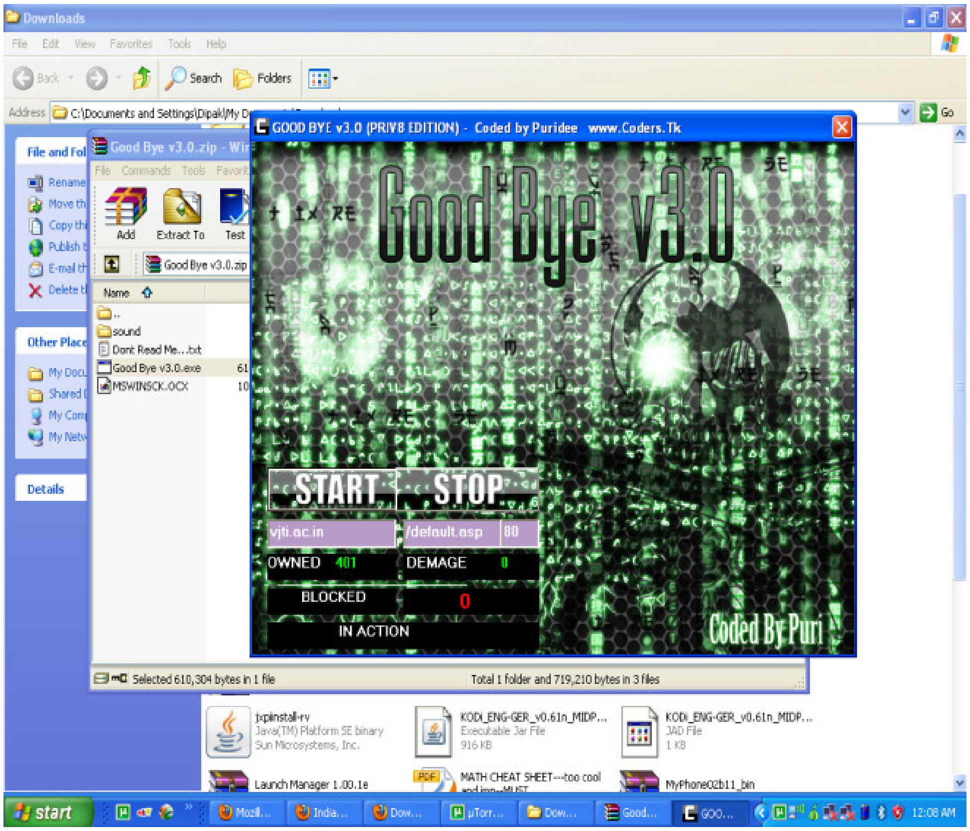
It's a class of low-bandwidth DDoS attacks that exploit algorithmic deficiencies in the worst case performance of algorithms used in many mainstream applications. For example, both binary trees and hash tables with carefully chosen input can be the attack targets to consume system resources greatly [3].

2.10 Spam Attack

This type of attack is used for targeting the various mail services of corporate as well as public users. DDoS attack through spam has increased and disturbed the mail services of various organizations. Spam penetrate through all the filters to create DDoS attacks, which causes serious trouble to users and the data. But these mail services are frequent target of hackers and spammers.[25]

3. TOOLS TO DO ATTACKS

By meeting information such as Firewall, operating system, IP Address, number of open ports and number of alive systems in a network we can make attack with the help of tools. It can carry out DDOS attack [23] with the help of tool Good Bye V3.0 and to perform IP spoofing, we take help of TOR software with add on tor-button. With IP address we identify the target system.



GOOD BYE v3.0 (PRIV8 EDITION) - Coded by Puridee www.Coders.Tk

vjti.ac.in /default.asp 80

OWNED 401 DEMAGE 0

BLOCKED 0

IN ACTION

Selected 610,304 bytes in 1 file

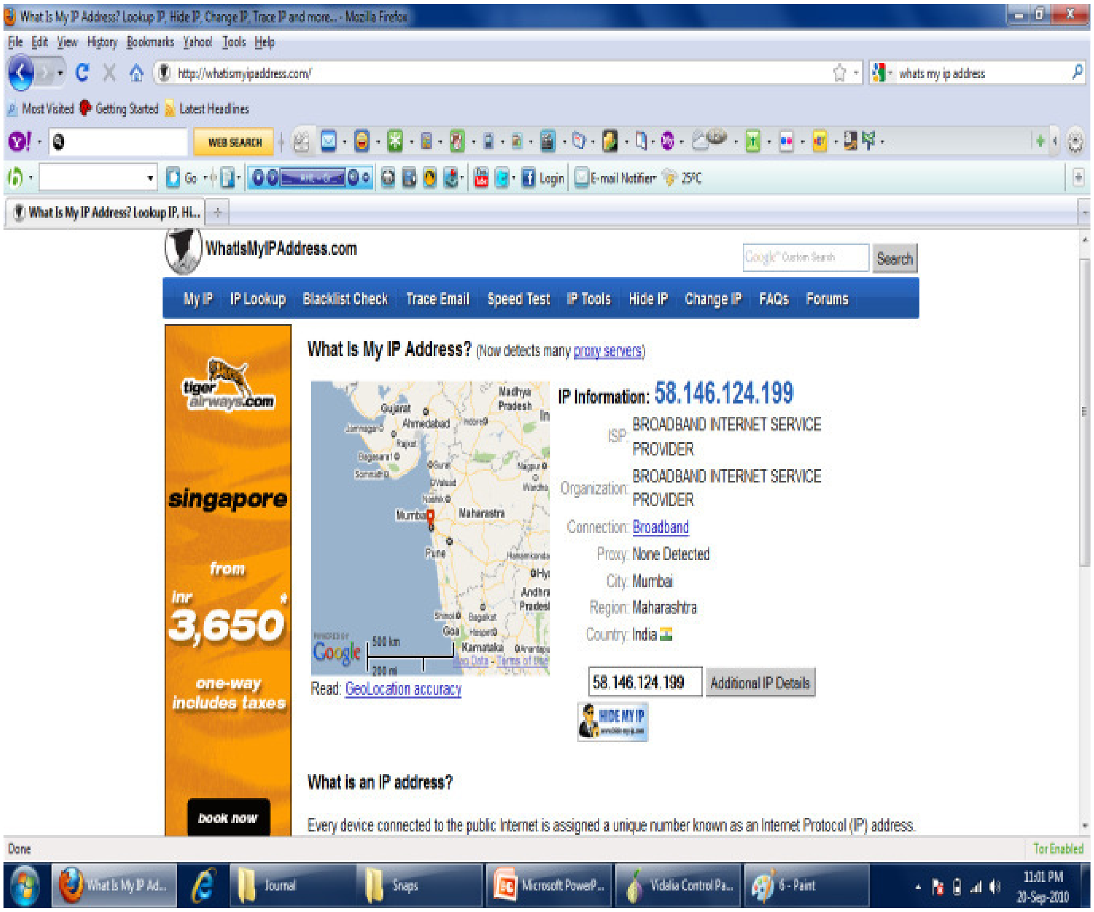
Total 1 folder and 719,210 bytes in 3 files

Figure 2: Write Web site and Click on start

It is a outlook of software (Figure 2) [23].

It have to write down web site address (such as www.trubainstitute.ac.in) with a page (such as /default.asp), so your full address is www.trubainstitute.ac.in/default.asp.

For **IP spoofing** we have to download TOR software with add on tor-button. First time tor button (at the bottom right corner) is disabled. After this we will enable that button. This time information of our system is (Figure 3)



What Is My IP Address? Lookup IP, Hide IP, Change IP, Trace IP and more... - Mozilla Firefox

http://whatismyipaddress.com/

whats my ip address

WhatIsMyIPAddress.com

What Is My IP Address? (Now detects many proxy servers)

IP Information: 58.146.124.199

ISP: BROADBAND INTERNET SERVICE PROVIDER

Organization: BROADBAND INTERNET SERVICE PROVIDER

Connection: Broadband

Proxy: None Detected

City: Mumbai

Region: Maharashtra

Country: India

Read: GeoLocation accuracy

58.146.124.199

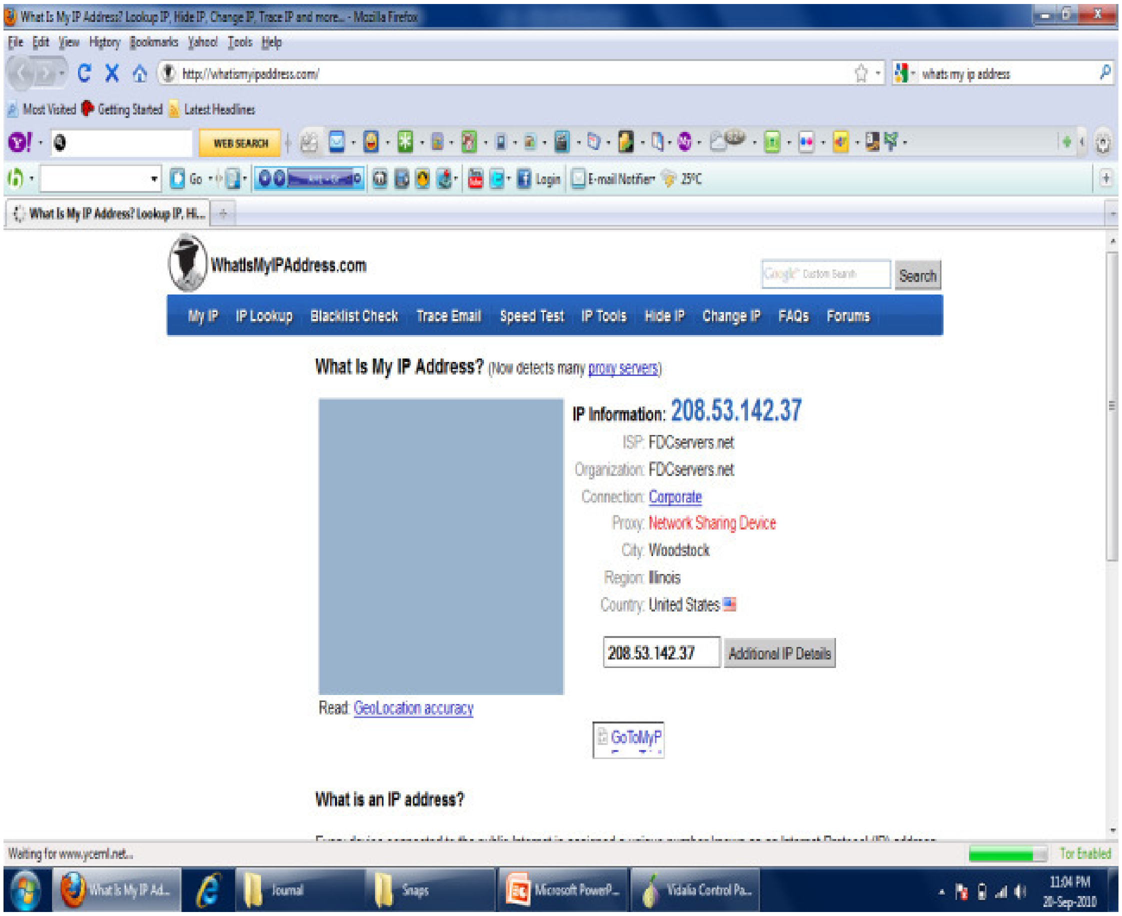
What is an IP address?

Every device connected to the public Internet is assigned a unique number known as an Internet Protocol (IP) address.

Figure 3: IP Information (Tor Disabled)

IP address: 58.146.124.199
ISP: Broadband Internet Service provider
City: Bhopal
Region: M.P
Country: India

This time we enable the tor button and color will change to green. And open Vidalia control panel. Click on new identity button.



What Is My IP Address? (Now detects many proxy servers)

IP Information: 208.53.142.37

ISP: FDCservers.net
Organization: FDCservers.net
Connection: Corporate
Proxy: Network Sharing Device
City: Woodstock
Region: Illinois
Country: United States

208.53.142.37

Read: GeoLocation accuracy

What is an IP address?

Figure 4: IP Information (Tor Enabled)

Now this time information of our system is (Figure 4)

IP address: 208.53.142.37
ISP: FDCsevers.net
City: Woodstock
Region: Illinois
Country: United State

For every time it give different information

4. COUNTERMEASURES AGAINST DDOS ATTACK

Most current DDoS attack detection and prevention schemes are deployed either at the victim server, at the attack source side, or between the two. In the following, we describe schemes representative of each of these three deployments and describe associated problems. Victim server side detection of DDoS attacks has received the bulk of past research attention, doubtless because the main goal of researchers has been to protect the victim server.

Wang et al. [4], detected SYN flooding attacks at leaf routers that connect end hosts to the Internet. They observed that the SYN-FIN packets pair each other in the normal network traffic and proposed a non-parameter CUSUM method to accumulate these pairs. Cheng [5] utilized the TTL (Time-To-Live) value in the IP header to estimate the Hop-Count of each packet. The spoofed packets could be distinguished from normal ones by the Hop- Count deviation. Lemon [6] incorporated SYN cache and cookies to prevent DDoS attacks, using cache or cookies to evaluate the security status of a connection before establishing the real connection with a protected server.

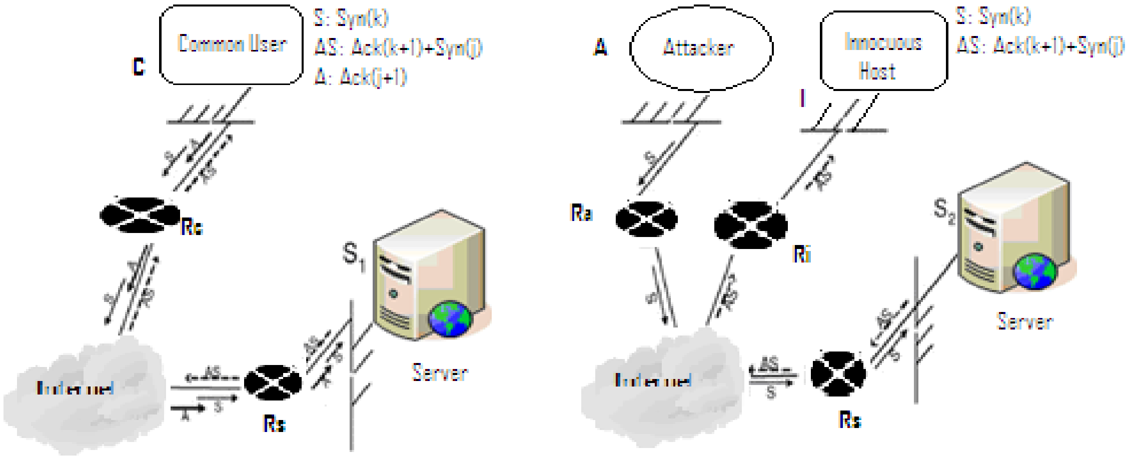
Hussein et al. [6] proposed a framework for classifying DoS attacks based on the header content and the transient ramp-up behaviour. Keromytis et al. employed the secure overlay service (SOS) [7, 8] to proactively prevent DDoS. SOS architecture is composed of SOAP, overlay nodes, beacon, secret servlet and filtered region, which makes it difficult for an attacker to target nodes along the path to a specific SOS-protected destination. Based on SOS, researchers from Columbia University continued their proactive defence research. MOVE [9] and WebSOS [10] are modified forms of the SOS architecture but with different emphasis. Puzzle based methods [11, 12] impose heavily overhead to zombies, which can mitigate attacking rate and make zombies exposed to host owners. Each of these must minimize resource usage while promptly responding and recording the states of numerous connections. At the same time, the method itself must be immune to DDoS attacks. Source side mechanism for detecting and preventing of DDoS attacks can be difficult to deploy. Source-end deployed methods have some advantages but are difficult to deploy. For reasons related to performance, however, ISPs are disinclined to deploy source-end defences in their domains. Mirkovic and Prier [13] introduced a DDoS defence system at the source-end in which attacks were detected by constantly monitoring two-way traffic flows and comparing them with normal flow models. The RFC2827 [14], for example, is designed to filter out spoofed packets with spoofed IP addresses at each ingress router and can drop a suspicious packet that does not belong to its routing domain. However, the fact that it may degrade routing performance makes ISPs reluctant to participate in this defence system. After an attack is detected, it is possible to find the attacking source using trace back [15] and pushback techniques.

Traceback attempts to identify the real location of the attacker. Source IPs used during a DDoS attack are often forged and cannot be used to identify the real location of the attack source. Most traceback schemes respond to this by either marking some packets along their routing paths or by sending special packets [18]. By tracking these special marks, it is possible to reconstruct the real routing path reconstructed and locate the true source IP. After the real path of the spoofed packets has been identified, the pushback technique can perform advanced filtering and work at the last few routers before the malicious traffic reaches the target victim.

A. The TCP-Based DDoS Attack

Most DDoS attacks exploit TCP control packets by spoofing the three-way handshake between the source and the destination server [24]. In this section we analyse the behaviour of TCP control packets first in a normal three-way handshake and then in a spoofed three-way handshake. Figure 5(a) shows a normal three-way handshake. First client *C* sends a *Syn*(*k*) request to the server *S*1, which replies with a packet containing both the acknowledgement *Ack*(*k* + 1) and the synchronization request *Syn*(*j*) and waits with a half-open connection in its memory space for the acknowledgement from the client *C*. Upon receiving both *Ack* (*k* + 1) and *Syn* (j*)* client *C* will finish building the connection by sending *Ack* (j + 1). When server *S*1 gets *Ack* (j + 1), it removes previously stored half-open connections in its memory space. The released memory space on server S1 makes it possible to handle further connection requests from clients and a network can run smoothly. *k* and *j* are respectively sequence numbers produced randomly by the server and the client during the three-way handshake.

In the remainder of this paper, *SY N* means a request sent to a server *S* inside the TCP control packet during the first round of the three-way handshake protocol; *ACK/SY N* will indicate a packet containing both *Ack* (*k* + 1) and *Syn* (j*)* that is delivered back from the server S in the second round; and *ACK* will denote a control package representing *Ack* (j + 1) in the third round. During the normal three-way handshake procedure, *SYN*, *ACK/SYN* and *ACK* all appear at both the edge router *Rc* near the client and at the edge router *Rs* near the server, as shown in Fig. 5. Figure 5(b) shows a spoofed three-way handshake and the implementation of a DoS attack. The packet at the first round of a valid authentication process is a malicious one with a spoofed IP address. The edge router *Ra* in the attacker domain forwards the SYN packet with the spoofed address *PI,* the IP address of the innocent host *I* , to the server *S*2. The server *S*2 replies with an *ACK/SYN* packet and a half-open connection are pending. This *ACK/SYN* will be sent to the innocent host *I* because the server *S*2 regards the *SY N* packet from *I* according to the spoofed source IP *PI.* The edge router *RI* on the innocent host side will receive the *ACK/SY N* packet but as no previous *SY N* request had been forwarded by the client detector at *RI,* the *ACK/SY N* packet is dropped. The pending half-open connection on the server *S*2 is maintained for a long time. More accumulated half-open connections will quickly consume all the memory space reserved for handling TCP requests and the server *S*2 will deny any new requests. It is difficult to trace back the attackers true address because the innocent host *I* , whose IP is used as the spoofed source IP, is usually not in the same domain s the attacker, sender *A*.



(a) Normal three-way handshake (b)Spoofed three-way handshake

B. Bloom Filter

The Bloom filter is first described by Burton Bloom [20] and originally used to reduce the disk access times to different files and other applications, e.g., spell checkers. Now it has been extended to defend against DDoS attacks [17, 21, and 22]. The Bloom filter is composed of a vector *v* of *m* bits, initially all set to 0. We have *k* independent hash functions, *h*1*, h*2*, and hk,* each with a range {0 . . . *m* − 1}. The vector *v* can show the existence of an element in *A*. Given an element *a* □ *A*, the bits at positions *h*1 (*a*)*, h*2 (*a*)*. . . hk* (*a*) in *v* are set to 1 . Note that a particular bit might be set to 1 multiple times which may cause potential false results. Given a query of the existence of *b* in *A*, we check the bits at positions *h*1 (*b*)*, h*2 (*b*)*. . . hk* (*b*). If any one of them is 0, then certainly *b* is not in the set *A*. Otherwise we conjecture that *b* is in it. Otherwise we presume that *b* is a member of that set. There is, however, a certain probability that the Bloom filter will give a false result, a "false positive". The parameters *k* and *m* should be chosen such that the probability of a false positive is small.

5. INDEPENDENT COMPONENT ANALYSISE

Conventional tracing methods be likely to be influenced by traffic not taking part in the attack included in each pattern. And, it is considered that tracing accuracy decreases because the influence grows as the number of attack confluences increases. In this section, a method of resolving traffic pattern to plural independent patterns by using Independent component Analysis, and judging relation between each pattern and attack from analysis of the result is proposed. A better accuracy can be expected from the proposed method than conventional methods for judging the relation to the attack by comparing patterns directly.

Independent Component Analysis

Independent Component Analysis [22] is a method for separating observation signals formed by linear mixing of plural source signals to plural independent signals. Now, n independent source signals are shown as s = (s1, s2, Sn). And, Observed Signal x = (x1, x2, · · ·, xn) is the mixture of Source Signal s mixed by Mixing Matrix A = aij (i = 1, 2… n, j = 1, 2… n), as follows

$$x = As \,\ldots\ldots\ldots\ldots\ldots\ldots \,(1)$$

Then, Independent Component Analysis presumes Mixing Matrix A and Source Signal s. In the case of a model like (1), the problem is to lead Separating Matrix W which makes

Each element of ˆs independent mutually based on Observed Signal x (2).

$$\hat{}s = Wx \,\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \,(2)$$

In (2), ˆs is n dimension vector and a presumption value of s, and W is n * n matrix. In (2), ˆs is n dimension vector and a presumption value of s, and W is n * n matrix. In An ideal case, A−1 = W holds true. But, because A is an unknown, W and A−1 are brought close by learning during actual calculations. Each row vector of Mixing Matrix A obtained by ICA is mutually orthogonal, when observation signals are mutually independent. Then, the independence of the DoS attack traffic pattern and the normal pattern is examined by using this character. The independence between DoS attack traffic pattern and normal traffic pattern is investigated with simple models of DoS attack traffic patterns and normal traffic patterns., SD is a scale of the DoS attack traffic, SN is the mean of the amount of normal traffic, TD is the length of the DoS attack traffic pattern, and TA is the total length of the normal traffic pattern. From the traffic pattern of TCP packets distributed by “The Internet Traffic Archive”[18], the pattern at a time duration TA is randomly selected, and assigned as the normal traffic pattern. To examine the independence between the DoS attack pattern and the normal traffic pattern of the above-mentioned model, the angle between each row vectors of Mixing Matrix A is investigated. TR (= TD/ TA), and SR (= SD/SN) are parameters. When the DoS attack traffic pattern and the normal traffic pattern of the abovementioned model are analysed with ICA, Mixing Matrix A becomes 2*2 matrixes. Each value is a mean value of 100 different pairs of the normal traffic pattern and the DoS attack traffic pattern it is considered that the DoS attack traffic pattern is a pattern with a strong independence in ICA. However, when DoS attacks occur, the pattern actually observed is a mixture of DoS traffic and normal traffic. Hence, if SR is small, the shape of the DoS attack traffic pattern of the model like the above-mentioned is not observed. Then, the independence of the normal traffic pattern including the DoS attack traffic pattern and the original normal traffic pattern is investigated. Therefore, it is considered that a large scale DoS attack traffic pattern has strong independence from the normal traffic pattern. Therefore, it can be regarded that there is a relation between DoS attack and input traffic pattens of each link, by evaluating the inclusion of the independent pattern, which is not included in past normal traffic patterns in input and output patterns.

6. CONCLUSIONS

Efficiency and scalability are the key requirements in design of defence against DDoS Attacks. In this paper illustrate study of various DDOS attack techniques and prevention techniques. All these method based on filtration mechanism and pattern matching based on the different normal or abnormal packet pattern. One great advantage of the development of DDoS attack and defence classifications is that effective communication and cooperation between researchers can be achieved so that additional weaknesses of the DDoS field can be identified DDoS attacks are not only a serious threat for wired networks but also for wireless infrastructures.

On the basis of all these review, a Counter bloom filter Mechanism using the Independent component analysis has been proposed for the future work which will not only detect the DDOS traffic but also help in filtering that unwanted traffic.

7. REFERENCES

[1] Liang Hu, Xiaoming Bi, “Research of DDoS Attack Mechanism and Its Defense Frame,” Computer Research and Development (ICCRD), 3rd International Conference, pp. 440–442, March 2011.

[2] Robert Vamosi, “Study: DDoS attacks threaten ISP infrastructure,” Online at http://news.cnet.com/8301-1009_3-10093699-83.html, CNET News, Nov. 2008.

[3] Elinor Mills, “Radio Free Europe DDOS attack latest by hactivists,” Online at http://news.cnet.com/8301-10784_3-9933746-7.html, CNET News, May. 2008.

[4] Christos Douligeris and Aikaterini Mitrokotsa, “DDoS Attacks And Defence mechanisms: A Classification,” in Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology, (ISSPIT’03), pp. 190-193, Dec 2003.

[5] IEEE Communications Magazine, pp. 42-51, Oct. 2002 Rocky K. C. Chang,” Defending against Flooding-based Distributed Denial-of-service Attacks: A Tutorial,”.

[6] Internet World Stats, Internet User Statistics – The Big Picture: World Internet Users and Population Stats, http://www.internetworldstats.com/stats.htm

[7] L.D. Stein, J.N. Stewart, The World Wide Web Security FAQ, version 3.1.2, February 4, 2002, Available from http://www.w3.org/Security/Faq.

[8] <http://cisco.com> viewed on 15 may 2010.

[9] S. M. Khattab, C. Sangpachatanaruk, R. Melhem, D. Mosse, and T. Znati, "Proactive Server Roaming for Mitigating Denial-of-Service Attacks," in Proceedings of the 1st International Conference on International Technology: Research and Education (ITRE'03), pp. 286-290, Aug. 2003.

[10] A. Yaar, A. Perrig, and D. Song, "PI: A path identification mechanism to defend against DDoS attacks," in proceedings of the IEEE symposium on Security and Privacy, pp. 93-109, May 2003.

[11] P. Feruson and D. Seine, "Network Ingress Filtering: Defeating Denial Of Service Attacks Which Employ IP Source Address Spoofing," RFC2827, May 2000.

[12] A. C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, B. Schwartz, S. T. Kent, and W. T. Strayer, "Single-Packet IP Traceback," IEEE/ACM Transactions on Networking, Vol. 10, No. 6, pp. 721-734, Dec. 2002.

[13] J.Ioannidis and S. M. Bellovin, "Implementing Pushback: Router-Based Defense Against DDoS Attacks," in Proceedings of the Network and Distributed System Security Symposium (NDSS'02), pp. 6-8, Feb. 2002.

[14] Yao Chen1, Shantanu Das, Pulak Dhar, Abdul-motaleb El Saddik, and Amiya Nayak, "Detecting and Preventing IP-spoofed Distributed DoS Attacks," International Journal of Network Security, Vol.7, No.1, pp.70–81, Jul. 2008.

[15] B. Bloom, "Space/Time Trade-Offs in Hash Coding with Allowable Errors," Comm. ACM, vol. 13, no. 7, pp. 422-426, 1970.

[16] Wang H, Zhang D, Shin KG (2002) Detecting SYN flooding attacks. In: Proceedings of Annual Joint Conference of the IEEE Computer and Communications Societies(INFOCOM), vol. 3, pp 1530–1539.

[17] Jin C,Wang HN, Shin KG (2003) Hop-count filtering: An effective defense against spoofed DDoS traffic. In: Proceedings of the 10th ACM Conference on Computer and Communication Security (CCS), ACM Press, pp 30–41.

[18] J.Lemon, "Resisting SYN Flooding Dos Attacks with A SYN Cache", Proceeding of USENIX BSDCon'2002,February, 2002.

[19] Keromytis A, MisraV, RubensteinD(2002) SOS: Secure overlay services. In:ACMSIGCOMMComputer Communication Review, Proceedings of the 2002 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, Pittsburgh, PA, vol. 32, pp 61–72.

[20] Keromytis A, Misra V, Rubenstein, D (2004) SOS: An architecture for mitigating DDoS attacks. IEEE Journal on Selected Areas in Communications 22:176–188.

[21] A. C. Snoeren. Hash-based IP traceback. In Proceedings of the ACM SIGCOMM Conference, pages 3–14. ACM Press, August 2001.

[22] Yuji Waizumi , Tohru Sato and Yoshiaki Nemoto: A new Traffic Pattern Matchinng for DDoS trace back Using Independent Component Analysis in Procedding of World Academy of science ,Engineering and Technology 2009.

[23] Anand Bisen, Shrinivas Karwa, B.B.Meshram, "Countermeasure tool-Carapace for Network Security". In International journal of Network Security & its Applications (IJNSA), VOL.3, NO.3, pp.16-28, May 2011.

[24] Bin Xiao, Wei Chen, Yanxiang He, "A Novel approach to detecting DDoS attacks at an early Stage". In Springer Science + Business Media LLC 2006.

[25] Dhinaharan Nagamalai, Cynthia Dhinakaran, Jae Kwang Lee. "Multi Layer Approach to Defend DDoS Attacks Caused by Spam". In aaXiv.org (Cornell university Library), arXiv: 1010.1583v1 [cs.CR]