Network Protection Against Flooding DDOS Attack

Rashida Farsath.k
Computer science & Engg.

Abstract

To detect Distributed Denial Of Service attack, this paper proposes an algorithm which provides network security. The proposed system is composed of intrusion prevention systems (IPSs) located at the Internet service providers(ISPs) level and IPSs act as a virtual protection rings around the hosts to defend DDOS attack.

1. Introduction

Disruption from service caused by DDoS attacks is an immense threat to Internet today. These attacks can disrupt the availability of Internet services completely, by eating either computational or communication resources through sheer volume of packets sent from distributed locations in a coordinated manner or graceful degradation of network performance by sending attack traffic at low rate. DDoS (Distributed Denial of Service) attacks are amplified form of DoS attacks where attackers direct hundred or even more zombie machines against a single target. DDoS attacks are becoming an increasingly significant problem. According to the latest Quarterly Global DDoS Attack Report commissioned by DDoS mitigation company Prolexic, there's been a 22 percent increase in the number of DDoS attacks carried out over the last 12 months.On March 22, 2013 the largest DDoS attack yet seen in the history of the Internet hit the CloudFlare network.

Network security breaches represent a growing threat to businesses and institutions, costing them billions of dollars every year. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are assaults on a network that flood it with so many additional requests that regular traffic is either slowed or completely interrupted. Unlike single bullet intrusion attacks (such as a worm or Trojan) which cause information damage or leakage, DoS attacks disrupt the availability of network resources and can interrupt network service for a long period of time.

Typical victims for DoS attacks are online businesses, carriers and service providers. DoS attacks target revenue-generating organizations by overtaxing link capacity. This costs them both direct and indirect damages. Direct damages include revenue loss or increased network costs. Indirect damages are related to business reputation and increased operational expenses. The main challenge in mitigating DoS and DDoS attacks shown in Fig.1 is to detect traffic anomalies and filter out only the attack traffic while maintaining the uninterrupted flow of legitimate traffic. Filtering out malicious traffic must be performed with caution, particularly since false positives may occur which could block real user traffic.

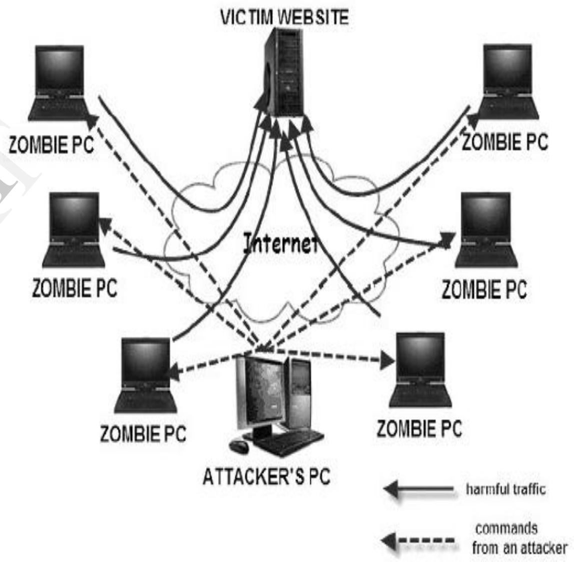

Figure:1 DDOS attack

A basic denial of service attack involves bombarding an IP address with large amounts of traffic. If the IP address points to a Web server, then it may be overwhelmed. Legitimate traffic heading for the Web server will be unable to contact it, the site becomes unavailable and Service is denied. If you run your own servers, then you need to be able to identify when you are under attack. That's because the sooner you can establish that problems with your website are due to a DDoS attack, the sooner you can start to do something about it.To be in a position to do this, it's a good idea to familiarize yourself with your typical inbound traffic profile; the more you know about what your normal traffic looks like, the easier it is to spot when its profile changes. Most DDoS attacks start as sharp spikes in traffic, and it's helpful to be able to tell the difference between a sudden surge of legitimate visitors and the start of a DDoS attack.

These days, online computers, especially those with a high-bandwidth connection, have become a desirable target for attackers. Attackers can gain control of these computers via direct or indirect attacks. Direct attacks refer to sending packets containing a malicious payload that exploits a vulnerable computer, for example, an unpatched Windows home PC. Generally, these attacks are conducted via automated software so that the number of compromised computers can be maximized in a short period. The requirement for launching direct attacks is that publicly available services on the targeted computers contain software vulnerabilities. For example, the Blaster Worm spread by exploiting a vulnerability in the Remote Procedure Call (RPC) service [CERT 2003], which allowed malicious code to be executed in the remote host. Unfortunately, this kind of vulnerability occurs frequently and has been increasing. According to CERT[2006] statistics as shown in Figure 2, the number of vulnerabilities reported in 2005 was 5,990, which is 35 times the number in 1995.

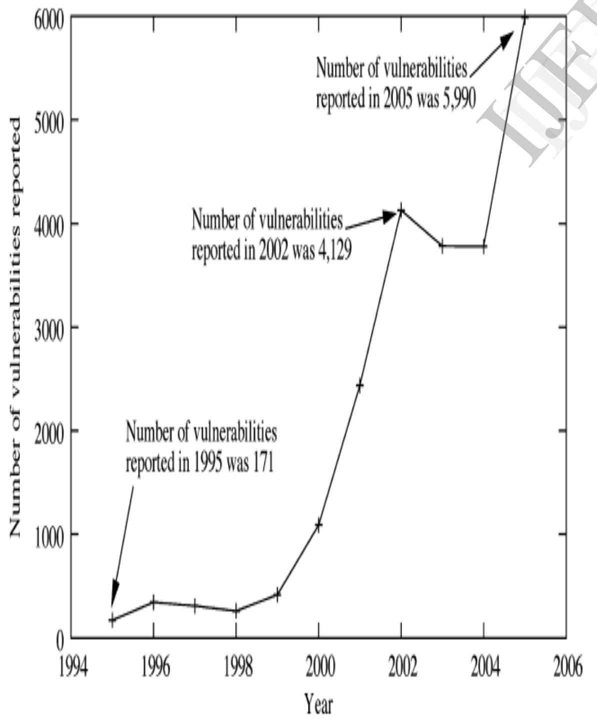

Fig. 2 The number of vulnerabilities reported each year according to CERT.

This paper presents a new system that detects flooding DDoS attacks as far as possible from the victim host and as close as possible to the attack source(s) at the Internet service provider (ISP) level. It relies on adistributed architecture composed of multiple IPSs forming overlay networks of protection rings around subscribed customers. it act as a service to which customers can subscribe.

The IPSs form virtual protection rings around the host they protect. The virtual rings use horizontal communication when the degree of a potential attack is high. In this way, the threat is measured based on the overall traffic bandwidth directed to the customer compared to the maximum bandwidth it supports.

2. System Components

The system is composed of several IPSs each with the following components

1) Packet Processor- When a rule is matched it examines the traffic and update the traffic information in the detection window.

2) Metrics Manager- It computes the frequency and entropy with the specified rule as follows,

Frequency- The frequency is the proportion of packets matching rule within a detection window

Entropy- The entropy measures the uniformity of distribution of rule frequencies.

3) Selection Manager- Traffic can be calculated during elapsed time based on traffic profile.

4) Score Manager- It assigns the score to each rule depending on their frequencies and the entropies.

High entropy and High rule frequency-It is to detect the attack by using the traffic and setting the rule for each one by using the high frequency and high entropy.

Low entropy and High rule frequency-It uses the high frequency which represents the direct threats with low entropy.

High entropy and Low rule frequency-It represents the potential threats by using the low frequency value.

Low entropy and Low rule frequency-This includes both high and low frequencies because of the low entropy.

5) Collaboration Manager- It will confirm the potential attack when the customer capacity is higher than the current traffic.

A key problem to tackle when solving bandwidth attacks is attack detection.There are two challenges for detecting bandwidth attacks. The first challenge how to detect malicious traffic close to its source. This is particularly difficult when the attack is highly distributed, since the attack traffic from each source may be small compared to the normal background traffic. The second challenge is to detect the bandwidth attack as soon as possible without raising a false alarm, so that the victim has more time to take action against the attacker.

Previous approaches rely on monitoring the volume of traffic that is received by the victim . Due to the bursty nature of Internet traffic, a sudden increase in traffic may be mistaken as an attack. If we delay our response in order to ensure that the traffic increase is not just a burst, then we risk allowing the victim to be overwhelmed by a real attack. We need to distinguish between these events.

A better approach is to monitor the number of new IP addresses, rather than the local traffic volume.It provides a system of adding legitimate IP addresses into an IP Address Database (IAD) and keeps the IAD updated adding new legitimate IP addresses and deleting expired IP addresses. This is done off-line to make sure the traffic data used for training does not contain any bandwidth attacks. A simple rule can be used to decide whether a new IP address is legitimate or not. For example, a TCP connection with less than 3 packet is considered to be an abnormal IP flow. During detection period, we collect several statistics of incoming traffic for the current time interval Δn, by analyzing the number of new IP addresses, we can detect whether a DDoS attack is occurring.

Algorithm

An alternative algorithm can be used as an enhancement to the system which can detect the burst nature of traffic in the network against DDos.

Let Xn represent the fraction of new IP addresses during time interval Δn. For the random sequence {Xn},there is a step change of the mean value at m from α to α + h. We require an algorithm to detect changes of at least step size h and estimate m in a sequential manner so that the detection delay and false positive rate are both minimized. Here we use the non parametric CUSUM (Cumulative Sum) method in our detection algorithm.

The main idea behind the non-parametric CUSUM algorithm is that we accumulate values of Xn that are significantly higher than the mean level under normal operation. One of the advantages of this algorithm is that it monitors the input random variables in a sequential manner so that real-time detection is achieved.

As we mentioned before, Xn represents the fraction of new IP addresses in the measurement interval Δn. In normal operation, this fraction will be close to 0,

E(Xn) = α ≪ 1 since there is only a small proportion of IP addresses that are new to the network under normal condition.

However, one of the assumptions for the nonparametric CUSUM algorithm is that mean value of the random sequence is negative during normal conditions, and becomes positive when a change occurs. Thus, without loss of any statistical feature, {Xn} is transformed into another random sequence {Zn} with negative mean

$$Zn = Xn - \beta, \text{ where } a = \alpha - \beta .$$

Parameter β is a constant value for a given network condition, and it helps to produce a random sequence {Zn} with a negative mean so that all the negative values of {Zn} will not accumulate according to time. When an attack happens, Zn will suddenly become large and positive,

i.e. h + a > 0, where h can be viewed as a lower bound of the increase in Zn during an attack. Hence, Zn with a positive value (h + a > 0) is accumulated to indicate whether an attack happens or not.

The attack detection threshold N is used for the yn, accumulated positive values of Zn,

Our change detection is based on the observation of h ≫ β.

For efficiency, we use the recursive version of algorithm which is shown as follows:

$$yn = (yn-1 + Zn)+,$$

$$y0 = 0$$

where x+ is equal to x if x > 0 and 0 otherwise. A large yn is a strong indication of an attack.yn represents the cumulative positive values of Zn. We consider the change to have occurred at time τN if yτN ≥ N. The decision function can be described as follows

$$dN\,(yn) = 0 \text{ if } yn \le N;$$

$$= 1 \text{ if } yn > N.$$

N is the threshold for attack detection and dN (yn) represents the decision at time n,'1' if the test statistic yn is larger than N, which indicates an attack, and '0' otherwise, which indicates the normal operation.

Why do people perpetrate DDoS attacks?

The main goal is to inflict damage on the victim. Frequently the ulterior motives are personal reasons
(a significant number of DDoS attacks are perpetrated against home computers, presumably for purposes of revenge), or prestige (successful attacks on popular Web servers gain the respect of the hacker community). However, some DDoS attacks are performed for material gain (damaging a competitor's resources or blackmailing companies) or for political reasons (a country at war could perpetrate attacks against its enemy's critical resources, potentially enlisting a significant portion of the entire country's computing power for this action).

3. Conclusion

This paper proposed, an algorithm as a solution for the detection of flooding DDoS attacks. It provides protection to subscribed customers against DDOS attack and saving valuable network resources.

4. References

1. T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of network-based defense mechanisms countering the DoS and DDoS problems," Comput. Surv., vol. 39, Apr. 2007, Article 3.
2. A. Networks, Arbor, Lexington, MA, "Worldwide ISP security report," Tech. Rep., 2010.
3. R. N. Smith and S. Bhattacharya, "A protocol and simulation for distributed communicating firewalls," in Proc. COMPSAC, 1999, pp.74–79.
4. R. Janakiraman, M. Waldvogel, and Q. Zhang, "Indra: A peer-to-peer approach to network intrusion detection and prevention," in Proc. IEEE WETICE, Jun. 2003, pp. 226–231.
5. J. L. Berral, N. Poggi, J. Alonso, R. Gavaldà,, J. Torres, and M. Parashar, "Adaptive distributed mechanism against flooding network.
6. Anirban Chakrabarti and G. Manimaran. Internet infrastructure security-A taxonomy. IEEE Network, 16:13– 21, 2002.
7. M. Basseville and I. V. Nikiforov. Detection of Abrupt Changes: Theory and Application. Prentice Hall, 1993.