DDoS Detection Technique by Using Various Methods

Mr. Ranjit R. Mane[1] Prof. B. W. Balkhande[2]
[2]Professor
[1,2]Departement of Computer Engineering
[1,2]BVCOE, Navi Mumbai, India

Abstract— There are a many network attacks on the Internet, and they are increasing each year. The condition of internet attacks is on the increase toward a distributed, collaborative direction. Internet attacks exhaust a lot of resources, take up a lot of bandwidth, making the victim host cannot accept normal network requests, resulting in substantial economic losses. In this paper explain three different methods to detect DDoS attack. This paper is based on the analysis of the distribution of network traffic, using detection method based on the analysis of the correlation of IP addresses. Next method of DDoS attacks called stealthy DDoS attacks, which can be launched by complicated attackers. Such attacks are different from traditional DDoS attacks in that they cannot be detected by previous detection methods effectively. In response to this type of DDoS attacks, in this paper a detection approach based on time-series decomposition, which divides the original time series into trend and random components. It then applies a double autocorrelation method and an superior cumulative sum technique to the trend and random components, respectively, to detect anomalies in both components.

Key words: DDoS Attack, IP asddress

I. INTRODUCTION

People have been provided many convenient, because generalized computer network infra building and increasing the number of internet users could make easy access to computer data. However, the opposition of convenience, every year, the internet crime has been raised such as hacking and invasion of privacy. The crime occurs economical spoil by flooding traffic to network or illegal access to computer system which could stop the right service. Distributed Denial of Service (DDoS) is attack type since long before, but it is the most serious attack type because it has simple attack technique and the tool which is easy to find anywhere. Also, it happens frequently and is not easy to block out effectively [1]. Recently, the main purpose of DDoS is political or commercial demanding to the target by occurring disable web site or server. The target for an attack has been diversified for example, game business site, stock site, or internet portal site. Since late 1990, it started to happen. DDoS attack is a major threat to the network at present. It does great harm to the world's economic and society. Almost all major portals have suffered from the attacks, resulting in countless economic losses. DDoS attack is a devastating attack in which an attacker using multiple attack vectors being controlled to send a large number of attack packets to the target host to take up and consume a lot of resources of target host and network, making the target host to its knees, and unable to provide services to normal requests. DDoS attacks have characteristics of distributed and large strength, and can make the victim suffer from great damage in a very short time. It is a major threat of network security at present. How to detect and defense DDoS attacks have become an important research topic. DDoS attack detection is a hot research topic in the network security domain. The core issue of DDoS attack detection is to distinguish between normal traffic and attack traffic. Normal burst traffic is caused by a large number of normal access in a short time, such as large enterprises working hours will result in the sudden increase in traffic, important news browsing and so on.

A. Types Of Ddos Attack :

1) Ping of Death:

POD is an old denial of service attack that was quite effective back in the day, but is not really much of a threat anymore. Ping of Death has also been called Teardrop, and a few other names. Within the IP protocol there are maximum byte allowances for packets (information) sent between two machines. The max allowance under IPv4 is 65,535 bytes. When a large packet is sent it is separated across multiple IP packets, and when reassembled creates a packet so big it will cause the receiving server to crash.

2) SYN Flood:

This type of attack is a classic DDoS that sends rapid amounts of packets at a machine in an attempt to keep connections from being closed. The sending machine does not close the connection, and eventually that connection times out. If the attack is strong enough it will consume all resources on the server and send the website offline.

3) UDP Flood:

A User Datagram Protocol Flood works by flooding ports on a target machine with packets that make the machine listen for applications on those ports and send back an ICMP packet.

4) Reflected Attack:

Forged packets are sent out to as many computers as possible. When the packets are received the computers reply, but because the packets are spoofed, instead of responding to the real sender, the machines will all attempt to communicate with the machine at the spoofed address. Eventually, if the attack is strong enough the server will shut down.

5) Nuke:

This is an old distributed denial of service attack that uses corrupted ICMP packets with a modified ping utility to delivers bad packets to the target server. With enough volume the attack can be successful.

6) Slowloris:

These types of DDoS attacks like these are way more complex than some of the other DDoS attacks we've talked about. Slowloris is a DDos toolkit that sends out partial requests to a target server in an effort to keep the connections open as long as possible. At the same time it does this, it sends out HTTP headers at certain intervals, which ramps up the requests, but never makes any connections. It doesn't take long for this type of DDoS attack to take down a website.

7) Peer-To-Peer Attacks:

These types of attacks exploit peer-to-peer networks by maliciously redirecting legitimate visitors to the site or server they want to attack. If the attacker is able to pull it off with enough people, the resulting DDOS shuts down the site.

II. DDOS ATTACK DETECTION METHODS

A. Detecion Algorithm Based On The Correlation Of Ip Address Analysis:

1) The Basic Idea Of The Algorithm:

Sample the data packets on the network edge router close to the target host. Analyze the network traffic using correlation coefficient. First record the amount of data packets of different IP addresses in each unit of time. And statistic the amount of data packets of different IP addresses in several adjacent time intervals. That is, the amount of data packets in a sliding window time interval. Move the sliding window one unit time interval rightward and statistic the amount of data packet in the next sliding window time interval. At this time, calculate the correlation coefficient of data packets in adjacent slide window time interval. In the same way, move the sliding window time interval one unit time interval rightward successively. Calculate the correlation coefficient of data packets in adjacent slide window time interval. Then we can get the network traffic changes with time, and to determine whether there is a network attack. Under normal circumstances, the IP address access to the target network will be in a relatively stable range, the change of the correlation coefficient of IP packets is also relatively stable. In the event of network attacks, the attacker controls a large number of attack sources to attack the target host. And the IP addresses access to the target host will be dispersed and become erratic. By analyzing correlation coefficients of the amount of network packets in each time period, we can analyze the abnormal conditions in the network, and to detect network attacks.

B. Related Definition:

1) Covariance of random variables:

Let X, Y be random variables, and the covariance of X, Y is

$$p_{(XY)}=\frac{Cov(X,Y)}{\sqrt{D(X)}\sqrt{D(Y)}}=\frac{E\{[X-E(X)][Y-E(Y)]\}}{\sqrt{D(X)}\sqrt{D(Y)}}$$

2) he correlation coefficient of Random variables and Let X,Y be random variables, and the correlation coefficient of X,Y is

$$p_{(XY)}=\frac{\sum_{i=1}^{n}\left(x_i-\overline{X}\right)\left(y_i-Y^{-}\right)}{\sqrt{\sum_{i=1}^{n}\left(x_i-\overline{X}\right)^2}\sqrt{\sum_{i=1}^{n}\left(y_i-\overline{Y}\right)^2}}$$

3) The correlation coefficient of two random vectors[1]

Let random vector X=(x1,x2,………xn)

Y= (y1,y2,…….yn)

Then the correlation coefficient of X,Y is defined as

$$Cov(X,Y)=E\{[X-E(X)]-[Y-E(Y)]\}$$

4) Slide window time interval: A large time interval consisted of several adjacent unit time intervals.

C. The description of the algorithm:

Sample the network traffic on edge routers of the target host. Xi(nk) show the number of data packets of the i-th IP address in the k-th time interval. X(nk) shows the total amount of data packets of all IP addresses in the k-th time interval. Take every adjacent three time intervals as a large time interval, that is, a sliding window interval. Statistic the number of data packets of every IP address in a sliding window time interval. Xi(n) indicates the amount of data packets sent by the ith IP address in the n-th sliding window time interval.

$$X_i(n)=\sum_{k=1}^{3}X_i(n_k)$$

X(n) indicates the total amount of data packets sent by all

IP addresses in the n-th slide window time interval.

$$X_n=\sum_{i=1}^{M}X_i(n)$$

Then move the slide window one unit time interval rightward, statistic the number of data packets sent by every IP address in the next slide window time interval Xi(n+1) and the total amount of data packets sent by all IP addresses X(n+1)

$$X_i(n)=\sum_{k=n}^{3+n}X_i(n_k)$$

Calculate the mathematical expectation of the number of data packets of every IP address in a slide window time interval.

$$E(x(n))=\sum_{i=1}^{M}X_i(n)\frac{X_i(n)}{X(n)}$$

Calculate the correlation coefficient of IP packets in

adjacent slide window time intervals using the correlation coefficient formula.

$$p_{xy}=\frac{\sum_{i=1}^{M}(x_i(n)-E(x(n)))(x_i(n+1)-E(x(n+1)))}{\sqrt{\sum_{i=1}^{M}(x_i(n)-E(x(n)))^2}\cdot\sqrt{\sum_{i=1}^{M}(x_i(n+1)-E(x(n+1)))^2}}$$

During the normal network traffic circumstances, the source IP address access to the target network will be in relatively stable range.

D. Multi-Core Based DDos Detection System:

By Multi-core methodology we mean the separation of the process of IFDDS and placing them on one or more cores. In this section, we show the structure of IFDDS, analyze which part of IFDDS is suitable to a single core of execution and decide the structure of multi-core based detection system.

1) IFDDS:

IP flow based DDoS detection system IFDDS works. Traffic pre-processing model provide two kinds of data: the 5 features and general characteristics of ongoing attack.

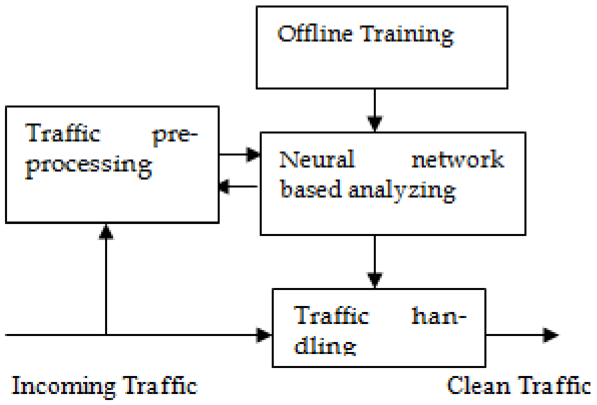

Fig 1: Structure of IFDDS

The 5 features will be calculated every certain time (depends on real network environment and system's processing ability). If an attack is detected, the neural network analyzer will notify the pre-processing model by sending it an interrupt. Then the pre-processing model will send the general characteristics of the ongoing attack to the traffic handling model. The neural network analyzer is composed of the offline training part and the online analyzer. The online analyzer activates the preprocessing model's characteristic sending function and the traffic handling model separately when an attack occurs. The traffic handling model is not a part of the IFDDS. It can be a common firewall, which will be activated by the analyzer model while DDoS occurs to do a simple filtering.

2) *Multi-Core Based DDos Detection System:*

Considering the 2 main parts of IFDDS and the framework in Figure 1, we use a "divide and conquer" approach [12]. Non-DDoS related applications are assigned to some certain cores named common cores. IFDDS is assigned to other cores named DDoS related cores. Further more, the process of IFDDS will be separated and assigned to two DDoS related cores: which means traffic preprocessing model and neural analyzer will run in parallel 116 with each other, and exchange message when necessary (Figure 1). As is shown in figure 2, the traffic handling model is pictured with transparent line, and also involved in non-DDoS related applications, these are because: to IFDDS the traffic handling model will be in a state of hibernation while no DDoS happens; traffic handling model is expected to be a common firewall who can filter packets with certain characteristics (general characteristics of the ongoing attack provided by the traffic pre-processing model), and there must be some other communication between the firewall and other non-DDoS related applications.

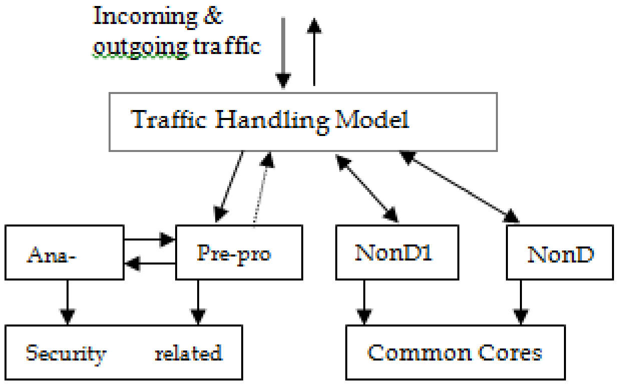

Fig 2: The Structure of Multi-core based IFDDS

E. *Stealthy DDos Attacks:*

1) *DDos Detection Algorithm:*

The important performance metrics of DDoS detection include detection accuracy and detection latency. However, it is impossible to reduce both at the same time; we need to find out an appropriate trade-off between the two metrics.

- *Self-Adaptive CUSUM Technique For Random Component:*

In order to accurately and timely detect the mutation point of random series *R*, we adopt the CUSUM technique in our approach. The basic idea of CUSUM is to accumulate those small offsets during the process to amplify the varying statistical feature and thus improve the detection sensitivity. CUSUM can detect a small deviation of the mean effectively.

It is generally defined as:

$$\begin{cases} yi = (yi-1 + xi)+ \\ y0 = 0 \end{cases} \qquad (7)$$

where *xi* is the observed original value and Δ+ is Δ if

Δ > 0 and 0 otherwise. When *xi* becomes positive from a negative value, *yi* becomes larger, and its exceeding a threshold *TH*CUSUM indicates the change point of the original series. In our implementation, we use *R˜i = Ri − RH* as the original series, where *RH* is the upper bound of *Ri* series during normal process.

Although the original CUSUM algorithm can quickly and efficiently detect attacks, after an attack period ends, the alarm will remain active. To stop the alarm, we consider the attack is over if *yi* does not grow for *C*AttackEndΔ*t*. When the alarm stops, we reset *yi* to 0.

- Double Autocorrelation Technique For Trend Component:

As shown in Fig., the double autocorrelation coefficient can be used as an indicator of the existence of SIDA in network traffic; the injected SIDA traffic increases the double autocorrelation coefficient. It results from the high internal dependency of SIDA traffic. The FCE series obtained from the same traffic also exhibit this property. Based on these observations, we can detect the anomaly in the trend component using the following condition:

$$p'_k(i) > TH_{DA,} 2 \le k \le K_{max} \qquad (8)$$

where *ρ_k*(*i*) is the double autocorrelation coefficient series at phase *i*. If all the first *K*max elements of the double autocorrelation coefficient series (except the very first element which always equals to 1) exceed the threshold *TH*DA, then we conclude that there is SIDA traffic embedded in the traffic. Considering the fact the SIDA traffic is injected to the normal traffic in a very slow pace, another condition should be introduced in order to detect the SIDA traffic at an early stage. During $\theta\Delta t$ period, if the sum of the first *Kmax* element (except the very first one) keeps growing _CDAθ_ times, then we consider a SIDA attack is initialized by attackers asfollows:

$$\sum_{j=i-\theta+1}^{i} 1 * \left\{ \sum_{k=2}^{K_{\max}} p_k^{'}(j) > \sum_{k=2}^{K_{\max}} p_k^{'}(j-1) \right\} \geq [C_{DA}\theta]$$

where *C*DA is an empirically-determined constant. The above condition can be checked by the following way. We firstly compare the sum of the first *Kmax* element of the double autocorrelation coefficient series at phase $i-\theta+1$ with that at phase $i-\theta+2$. If the former is greater than latter, then 1 will.

III. Conclusion

In this paper, we introduce various types of DDoS attack detection methods, Based on the dispersion of IP addresses of DDoS attacks, in this paper we use a detection method based on correlation analysis. First we find the amount of IP data packets in each time interval, and then calculate the amount of data packets in a slide window time interval. Finally, calculate the amount of IP addresses in each slide window time interval according to the correlation coefficient formula and to analyze the network flow condition. The formal approach is to get the correlation of IP addresses by calculating the correlation coefficient of IP addresses in two adjacent time interval. A multi-core based DDoS detection system was proposed in this paper. We redesigned IFDDS to be MIFDDS using multi-core methodology. The goal of doing so was to take the advantages of multi-core to reduce the time for IFDDS processing large scale DDoS attack and to assign security or non-security applications to proper cores. Experimental results showed that, the using of multi-core didn't lower IFDDS' detecting precision but also increased the speed of detection in certain range. MIFDDS consumed more RAM but not too much. It also improved CPU's efficiency.

In stealthy attack this type of DDoS attacks, we propose a detection approach based on the decomposition of time series, which divides the time series into trend and steady random components. We then analyze different components to detect the anomaly in both long-term and short-term changes of the traffic. By analyzing each component separately and evaluating results synthetically, the approach can greatly reduce both false negatives and false positives.

References

[1] Zhongmin Wang, Xinsheng Wang "DDoS Attack Detection Algorithm Based on the Correlation of IP Address Analysis"

[2] Dongqi Wang, Zhu yufu and lia lie "A Multi-core Based DDoS Detection Method"

[3] Haiqin Liu and Min Sik Kim, "Real-Time Detection of Stealthy DDoS Attacks Using Time-Series Decomposition"

[4] Yun Liu, Jian ping Yin. "A distributed denial of service attack detection based on K-Means algorithm".Computer Engineering and science.2008.

[5] Chang wang Zhang, Jian ping Yin. "Low-rate DoS attack detecting and filtering method based on distributed congestion participation", Computer Engineering and Science,2010,

[6] Jie ren Cheng, Jian ping Yin, "DDoS attacks detection based on ARMA prediction model", Computer Engineering and Science,2010,

[7] Jie ren Cheng, Jian ping Yin, "Distributed denial of service attack detection method based on address correlation", Computer Research and Development,2009,

[8] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," *ACM SIGCOMM Computer Communication Review*,vol. 34, no. 2, pp. 39–53, Apr 2004.

[9] Chang and R.K.C., "Defending against flooding-based distributed denialof- service attacks: a tutorial," *IEEE Communications Magazine*, vol. 40,no. 10, pp. 42–51, Oct 2002.

[10] D. Moore, G. M. Voelker, and S. Savage, "Inferring internet denial-ofservice activity," in *Proceedings of USENIX Security*, 2001.

[11] T. Aura, P. Nikander, and J. Leiwo, "DoS-resistant authentication with client puzzles," *Lecture Notes In Computer Science*, vol. 2133,