DDoS Attack Detection through Flow Analysis and Traffic Modeling

J. Udhayan[1], T. Hamsapriya[2], and N.A. Vasanthi[3]

[1] Dr. NGP Institute of Technology, Kalapatti
[2] Information Technology, PSG College of Technology
[3] Information Technology, Park College of Engineering & Technology
Coimbatore, India
{udhayangodwin,hamsapriya.t,vasanti.au}@gmail.com

Abstract. DDoS attack is the formidable cyber warfare of 20th century. Lot of research has already been taking place to mitigate DDoS attack. However DDoS attack still remains a potential threat. This research work considers the model level solution. Having a proper model of the traffic flow will help the administration unit to closely monitor the unusual behavior of the traffic; it will also help to identify the flash crowd which is the occasional accumulation of legitimate traffic. Hence in this paper, the normal traffic behavior is modeled, with the help of that the abnormal traffic which is evident during the DDoS attack is detected. Then the methodology to do the flow specific detection to segregate attack flow from the normal flow is discussed. Finally the possibility to curb the attack from the various hops is discussed.

Keywords: DDoS, Zombie, Goodput, Throughput, Botnet, Flash Crowd.

1 Introduction

The DDoS attacks over the servers of SCO corporate Website, Estonia service, Blue Frog service, and against several prominent Web sites like Yahoo, eBay, Amazon have caused severe damage to the victim [1]. Apart from this, plenty of victims around the World, from petite commercial sites to government organizations one time or another have faced DDoS attack. The DDoS attack is performed with the intent to deplete the server resources and make it unavailable to the legitimate clients, therefore it involves dumping of chunk data over victim's resources from many compromised computers (zombies) or network of zombies (Botnet)[2]. Attacker performs two things before manipulating a DDoS attack. First the attacker sets up a master component in a networked entity. Once the master component is installed, then the attacker spreads out the agent component which will get itself installed in less or unsecured computers. Once the installation is over the agent component communicates back with the master. Now it is up to the attacker to pass on the command to the zombies through master. The activities that the zombie performs in favor of the attacker are hidden to the owner of that system. Once this has been done the attacker can command a devastating attack over a specific target by passing on the commands through the master component.

V.V. Das, E. Ariwa, and S.B. Rahayu (Eds.): SPIT 2011, LNICST 62, pp. 89–94, 2012.

2 Related Work

Nowadays any DDoS attack is devastating because of its ability to generate mammoth volume of traffic from the millions of zombies [2]. Therefore understanding the rate criterion behind the DDoS attack is essential to model the behavior of the DDoS traffic. Hence various DDoS attack rates are discussed as follows.

2.1 Moderate Rate Attack

Smart DDoS attackers usually masquerades the flood as a normal (legitimate) flow throughout the network to avoid the detection. Moreover the traffic is generated from the millions or billions of zombies, each zombie generates normal or less than normal rate traffic in a way that, it never floods the network bandwidth but when it reaches the victim it overloads it to stalemate condition. This attack cannot be mitigated without eliminating moderate amount of genuine flows, since it always maintains the rate between less than the normal to slightly over normal.

2.2 Other Rate Attack

Constant rate attack [4] usually generates steady traffic with the rate greater than the legitimate traffic. However this attack can be segregated from the normal flow because the rate at which the packets generated was always above the normal rate and it is almost constant. This attack usually floods the network bandwidth, thus gets filtered by various network packet filters. As the result it is rarely used nowadays. Increasing rate attack [4] starts from the lowest possible rate and keep on increasing. This attack aims to cripple the victim server bit slowly than constant rate attack by taking its time. However this mechanism exhibits steady increase in the rate which is unusual and easily detectable.Fluctuating rate attack [4] is hard to predict because it is normally meager rate and lacks continuation therefore it is not a potential threat.

3 Proposed Detection Model

In this section a DDoS defense framework is discussed which focuses on efficient detection and mitigation of various DDoS attacks real-time.

3.1 DDoS Premonition Strategy

Most of the cases backlogs of the traffic are cached in the server for monitoring. Making use of such backlog will always help improving the detection procedure. However a thorough knowledge on the history is necessary to precisely detecting the ongoing attack at its inception stage. For instance, College web server receives enormous hits while the results are published which is called as flash crowd [3]. However if no result is published and if the hits still goes up, then the traffic must be

monitored for DDoS attack. This kind of knowledge on the history helps to adjudge the occasional raise in the legitimate traffic. However attackers still may fool the history based detection through imitating the normal behavior of the traffic and staging it on right occasion.Any server will have a processing limit on the incoming requests. Based on the processing need the administration would have chosen the server. Hence through analyzing the server the amount of traffic that environment generates can be admonished [5]. From our analysis any server will works fine and processes requests quickly and without any struggle until it receives 75% requests out of its processing capability. Hence the proposed DDoS premonition procedure works as follows. Consider the ability of server to process 75% requests out of its maximum processing capability without any juggle as Tolerance factor T_f. Now if the traffic arrives less than the Tolerance factor, it is no harm to the server. If the traffic starts to arrive more than the tolerance factor then it has to be monitored for the potential attack. Hence if the incoming packets/second i.e. throughput $T_i^* > T_f$ then the traffic is analyzed for the DDoS attack through triggering the attack confirmation procedure.

3.2 Attack Confirmation Procedure

Let $T_n(t)$ be the normal traffic, i.e. the total number of flows arriving at Target server in α time interval, Say the time interval $\alpha = \alpha_1, \alpha_2, \alpha_3, \ldots\ldots \alpha_n$number of seconds. Assume that the DDoS attack is set off against the target machine at α_t which is inside the range of α, when the attack starts the normal traffic $T_n(t)$ so for will be increased to $T_n^*(t) > T_f$. The motive behind the attacker is to junk the packets beyond the processing capability of the server. Say the maximum request processing capability of the server is T_m then the attack is considered successful while it reaches $T_n^*(t) > T_m$. This is the point where the victim server collapses. Hence to avoid this, the DDoS monitoring has to be done instantly while $T_n^*(t) > T_f$.

Consider a random process { A(t),t = nΔ, n Є N}, where Δ is a constant time interval, N is the set of positive integers, A(t) is a random variable and it is the aggregate throughput for incoming packets. A(t) is calculated during time interval {t - Δ , t} as follows:

$$A(t) = \sum_{i=1}^{CF} n_i \, , i = 1,2,3 \ldots . CIF. \tag{1}$$

Here n_i represent total number of packet arrivals for a flow I in {t - Δ, t} and CIF represents cumulative incoming flow or total number of incoming flows.

Similarly the aggregate throughput for outgoing packets O(t) is calculated during time interval {t - Δ , t} as follows:

$$O(t) = \sum_{i=1}^{CF} n_i \, , i = 1,2,3 \ldots . COF. \tag{2}$$

Here COF represents cumulative outgoing flow or total number of outgoing flows. However to confirm the attack the following equations are used

$$\frac{O(t)}{A(t)} \leq 0.90 \; then alert \; the \; detection. \tag{3}$$

$$\frac{O(t)}{A(t)} \geq 0.90 \; then it is harmless \; traffic. \tag{4}$$

Once the alert is raised this implies the possibility for attack flows amongst the flow. Following Flow specific detection is then used to segregate the DDoS flows.

3.3 Attack Mitigation Procedure

The goal is to detect the attack flows at various vantage points not only at the perimeter level. Therefore the characteristics of each and every flow are analyzed using goodput. Goodput is the application level throughput, i.e. the number of useful bits per unit of time, forwarded by the network from a certain source address to a certain destination, excluding protocol overhead and retransmitted data packetsGoodput is identified as appropriate method because the valid output or valid data doesn't flow or flows in insignificant proportions from the victim. Therefore the attack flow is detected using the following equation

$$\frac{Outgoing goodput per flow}{Incoming Throughput per flow} \leq \varepsilon. \tag{5}$$

To detect the attack flow the goodput for each and every flow is calculated in shorter time window Δ because genuine flow always maintains healthy goodput rate. Hence if the goodput is low then that flow is decided as attack flow.Once the attack is confirmed not only the victim starts the filtering but it can alert the preceding hops through multicasting or broadcasting the attack flow details [6]. The preceding hop thus can filter the attack flows and also forward the alert to its preceding hop device. This will soothe the influx at victims end.

4 Result Analysis

To perform the analysis the backlog of moderate rate DDoS attack is chosen. Because this kind of attack is difficult to detect and even if it is detected it is even hard to segregate it from the legitimate traffic. Moreover if the mechanism can detect the moderate rate attack it can detect other attacks easily. After analyzing the traffic for more than a week using eqn (3) the normal traffic pattern is studied and the percentage of traffic received is graphed. It is tedious and unnecessary to present the result of various aspects of the analysis. Normally the overall traffic rate is 10000 pps (packets per second) and 20000 pps range. However 30000 pps mark is expected to happen during peak hours in the evening, happened in the afternoon for one day. Hence the graph for that particular day had been plotted and the result is given in fig.1.

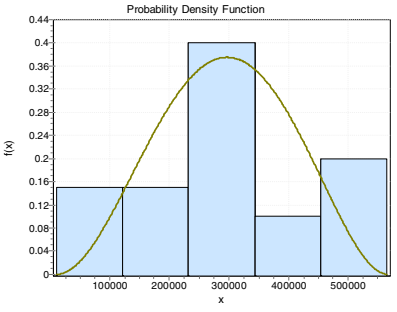

Fig. 1. Attack traffic distribution

According to eqn (4) the above shown traffic pattern has experienced DDoS attack. However the observed server cannot handle packets beyond 50000 pps at that time the drop has occurred tremendously and the packets range is distributed. However the packet range 30000 pps is at the peak which is something unusual. Moreover the flows at that peak region are analyzed for validity using eqn (5), but the result shows the annoying number of invalid flow as in fig.2.

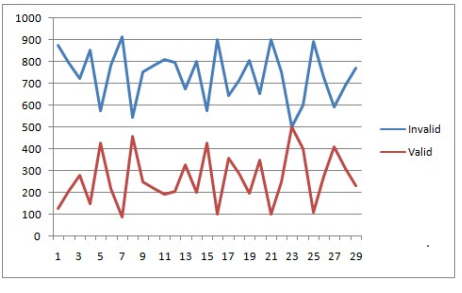

Fig. 2. Legitimate traffic against attack traffic

The traffic peak 30000 pps is analyzed with the step size of 1000 for validity using eqn (5). But majority of them had no valid data.

The simulation tool NS-2 is used to model the behavioral increase and the stability in attack traffic after it reaches 30000 pps range as in fig 3. It is because if the exponential increase in the drop after the 3000 pps.

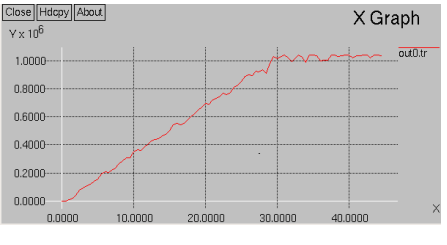

Fig. 3. Moderate Rate Constant slave set DDoS attack. Y axis 1 unit = 1 X 10^3 packets, X axis 1 unit = 1 *60 seconds.

However 20000 pps is 75% percent mark, if the influx traffic stays within this range no packet drop is experienced, if the range goes beyond then the drop intensifies. This result is presented in fig.4.

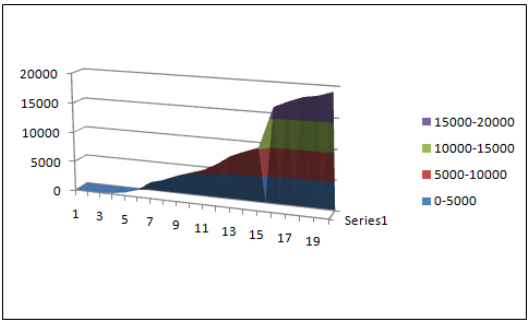

Fig. 4. Observation of packet drop above 75%

In the fig.4 the x-axis 1 is 76%, 2 is 77%, ... 20 is 95%. The drop almost starts at 76% and increases gradually. Hence the DDoS detection should be started at 75%.

5 Conclusion

In this paper various rates of DDoS attack has been discussed, then the method to model the legitimate traffic is presented, using that model the DDoS attack can be detected. The performance jiggle that happens when the packet rate consumes more than 75% of the sever capability has been discussed. Moreover a goodput based procedure to detect and segregate the DDoS attack is presented. Results shows that the DDoS attack confirmation & mitigation procedure handles DDoS effectively.

References

1. Zaroo, P.: A survey of DDoS attacks and some DDoS defense mechanisms. Advanced Information Assurance (CS 626)
2. Udhayan, J., Hamsapriya, T., Anitha, R.: Lightweight C&C based botnet detection using Aho-Corasick NFA. International Journal of Network Security & Its Applications (IJNSA) 2(4) (2010)
3. Cholda, P., Domzal, J., et al.: Performance Evaluation of P2P Caches: Flash-Crowd Case. In: Australian Telecommunication Networks & Applications Conference (2010)
4. Udhayan, J., Hamsapriya: Statistical Segregation Method to minimize the effects of false detection during DDoS attack. International Journal of Network Security 13(3), 152–160 (2011)
5. Best Practices for Performance in ISA Server (2006), `http://technet.microsoft.com/en-us/library/bb794835.aspx`
6. PyungKoo, P., HeeKyoung, Y., SangJin, H., JaeCheul, R.: An effective defense mechanism against DoS/DDoS attacks in flow-based routers. In: ACM International Conference on Advances in Mobile Computing and Multimedia, New York, USA (2010)