Journal of Computer Science

Original Research Paper

Correlation Based Approach with a Sliding Window Model to Detect and Mitigate Ddos Attacks

[1]Ayyamuthukumar, D. and [2]S. Karthik

[1]Department of CSE, K.S. Rangasamy College of Technology, Tiruchengode, Namakkal, Tamilnadu, India
[2]Department of CSE, SNS College of Technology, Coimbatore, Tamilnadu, India

Article history
Received: 13-11-2013
Revised: 02-12-2013
Accepted: 22-12-2014

Corresponding Author:
Ayyamuthukumar, D.
Department of CSE, K.S. Rangasamy College of Technology, Tiruchengode, Namakkal, Tamilnadu, India
Email: ukdkumaarcse@gmail.com

Abstract: DDoS attacks have become very popular since the turn of this millennium and has stayed in the headlines due to ever increasing and sometimes devastating attacks on popular web servers. In this study, we deal with DDoS attacks by proposing a correlation based approach with a sliding window model to detect and mitigate DDoS attack. The proposed scheme identifies malicious traffic flow towards a target system based on the volume of traffic flowing towards the victim machine and uses a correlation based approach with a sliding window model to detect and isolate malicious hosts. Rate limiting is applied individually on each malicious flow based on the volume of malicious traffic generated by the attacking hosts rather than a collective rate limiting on the total malicious flow towards victim. The results observed in simulation shows that the proposed approach detects the onset of the attacks very early and reacts to the threat by rate limiting the malicious flow based on the volume of attack traffic generated by each attacking hosts. The approach also adapts quickly to any changes in the rate of flow. The proposed system can be successfully implemented at critical points in the network as autonomous defense systems to limit the volume of malicious packet flow towards the target system.

Keywords: DDoS, Correlation, Sliding Window, Adaptive Rate Limiting

Introduction

The rapid growth of cyberspace into a vital global communication and business network has created a global infrastructure where both the network and its resources are highly vulnerable to Internet security threats. Given the social and economic dependency of the current era on the Internet it is essential to ensure the immunity of the cyberspace against any potential threats/attacks.

Distributed Denial of Service attack is one of the most critical threats to the stability and growth of the Internet. The attack involves denying the availability of a targets resource to legitimate users. The resources of the victim hosts are consumed by malicious attackers such that the victims service are either fully disrupted or is significantly degraded, rendering it virtually useless to legitimate users.

Vulnerable hosts in Internet are identified and compromised to become zombie machines which are then remotely controlled and coordinated to launch an attack on a victim machine. The attack is orchestrated by sending a large volume of malicious packets such that the targets victim's CPU usage is maxed out from processing this useless traffic and thus preventing it from performing any useful work.

The DDoS attack is distributed and coordinated across several hosts and also the behavior of the malicious packets is very similar to the behavior of legitimate packets making it hard to prevent and detect the DDoS attacks.

Related Work

The attack tools that threaten the stability of the Internet are becoming more and more powerful and the average time between the point of detection of vulnerability and its exploitation is rapidly shrinking. This creates a critical need to develop tools and techniques which can prevent/detect an attack and trace the attack to its origin quickly.

Several software for launching a DDoS attacks are available on the Internet. The tools are powerful and

the attack traffic generated by the software mimics the behavior of legitimate traffic. DDoS attacks are very hard to prevent, since the onset of attack occurs very quickly and the resources can be overwhelmed within a very short interval. The effectiveness of any proposed defense system depends on how quickly an attack can be detected and how accurately the malicious traffic can be distinguished from legitimate traffic.

Several defense systems have been proposed by researchers to counter DDoS attacks. The DDoS attack detection system depends on either the packet attributes or the traffic volume. DDoS mitigation strategy is either based on IP traceback or packet filtering or rate limiting.

IP Traceback involves identifying the attack hosts and taking it out of action. Kannan *et al*. (2012) proposed mechanisms for the detection and mitigation of DDoS attacks based on IP Traceback.

Moorthy *et al*. (2012) propsoed the use authentication technique for mitigating DDoS attacks in wireless local area networks. Udhayan *et al*. (2013) proposed the use of penalty scheme to enable zombies to recover from unauthorized use of resources.

Beak *et al*. (2007) proposed a packet marking method to detect DDoS attacks. Bhaya *et al*. (2014) proposed the use of data mining to detect DDoS attacks. Anurekha *et al*. (2012) proposed a dynamic approach to defend against Distributed Denial of Service attacks using an adaptive spin lock rate control mechanism which detects DDoS attacks based on the volume of traffic received at a defense system and applies an adaptive rate limiting strategy to limit the volume of malicious traffic that reaches the target victim.

The rate limiting strategy proposed by researchers in the DDoS defense systems have a major drawback. Irrespective of the volume of malicious flow generated by individual attackers towards a target victim, the rate limit is applied equally on the consolidated flow and does not take the individual strength into consideration. In this study a correlation based approach with a sliding window model is proposed to detect and mitigate DDoS attack by identifying the volume of malicious traffic generated by each attacker and applying an adaptive rate limit based on this value on the individual malicious flow.

Correlation Based Approach with a Sliding Window Model to Detect and Mitigate DDoS Attacks

Correlation based approach with a sliding window model to detect and mitigate DDoS attacks is a reactive autonomous defense system against DDoS flooding attacks, which can be installed at any intermediate node in the network on the path of a malicious DDoS traffic towards the victim machine.

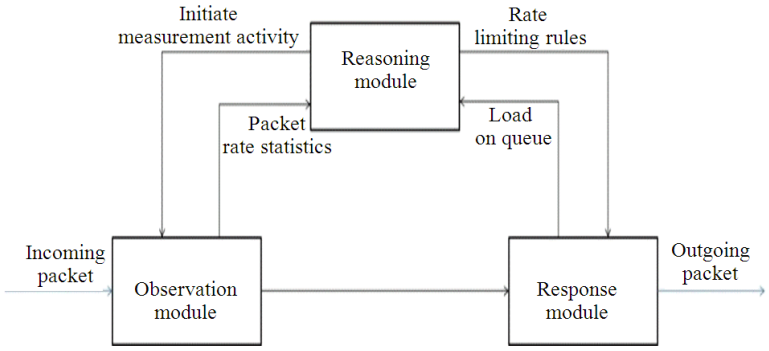

Fig. 1. Architecture of correlation based approach with a sliding window model to detect and mitigate DDoS Attacks

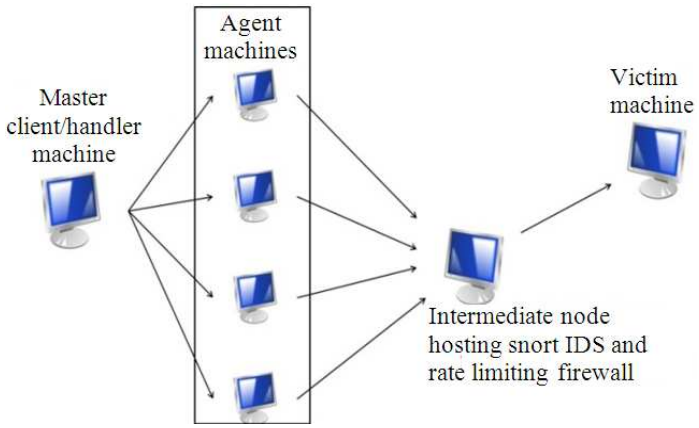

Fig. 2. Topology of simulated network

The proposed scheme identifies malicious traffic flow towards a target system based on the volume of traffic flowing towards the victim machine and responds to the onset of the attack by implementing an adaptive rate limiting on the malicious traffic passing through that system towards the victim.

Assumption and Definition

The proposed defense system assumes the presence of a security mechanism at exit routers of a network to filter all spoofed IP packets. DDoS attack generates a huge volume of traffic without any consideration for the network state and does not decrease its transmission rate even if congestion occurs in the network. Legitimate traffic adapts the transmission rate based on the network state.

Propsoed Architecture

The proposed correlation based approach with a sliding window model to detect and mitigate DDoS attacks consists of three functional units-observation Module, Reasoning Module and Response Module as depicted in Fig. 1. The observation module detects the presence or absence of an attack. The reasoning module determines the volume of malicious traffic contributed by each attacking hosts and determines the rate limit to be applied. The response module implements the rate limit on the outgoing flow at the defense system.

Observation, Reasoning and Response Module

Observation module observes the packet arrival rate at the defense system for successive observation interval given by a time period T sec. Correlation analysis can be used to determine the degree of association of a packet arrival rate with itself over successive observation intervals. DDoS attacks are characterized by a sudden abnormal increase in the traffic and sudden change in the correlation coefficient indicates the presence of a DDoS attack.

The number of previous observation intervals taken into consideration for attack detection and mitigate DDoS attacks is defined as the window size. The proposed sliding window model limits the window size to 5. If X is the total number of packets received during the current observation interval and Y is the total number of packets received during the previous observation interval the correlation coefficient is calculated as:

$$r = \frac{\sum xy}{N\sigma_x\sigma_y}$$

Where:
$X = (X-X_{mean})$ and $Y= (Y-X_{mean})$
N = The window size
σ_x = The standard deviation in X
σ_y = The standard deviation in Y

When a packet is received the hash index is calculated as a function of the source address, destination address and the protocol of the packet and the observation module increments the count value in a Hash data structure. Each index in the hash table consists of five entries in which the total number of packets received from the source address to the destination address per protocol is stored for five successive observation intervals. Applying a sliding window model, at the end of each observation interval the earliest entry is removed and the count for the next interval is stored.

Reasoning module is primarily responsible for identifying the target of DDoS attack, the source machine generating the malicious traffic and packet type of the malicious traffic and classifying a flow as legitimate or malicious flow. The proposed rate of limit to be applied is determined independently for each source machine based on the strength of attack packet generated from that machine towards the target machine.

The rate limit is calculated by determining the total number of packets generated during the observation interval and number of packets generated by each individual machine.

Assuming n numbers of source machines are generating the attack traffic and x1, x2, x3,…xn are the number of packets generated by each source machine. The average number of packets (μ) received during an observation interval at the defense system is given by:

$$\mu = \frac{1}{n}\sum_{i=1}^{n}(x_i$$

The total variation (V) in the volume of attack traffic from all source machines in a given observation interval is determined by:

$$V = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(x_i - \mu)^2}$$

The strength of attack flow (Z_i) from each source machine is calculated as the deviation between the total number of packets generated from that source machine during the given observation interval, the average number of packets received during the observation interval and the total variation in the volume of attack traffic and is given by:

$$Z_i = \frac{x_i - \mu}{V}$$

The Rate of Limit (RL) to be applied to the attack traffic flow is given by:

$$RL = RL_{prev} + (N * Z_i)$$

where, N is the window size and RL_{prev} is the rate of limit applied in the previous observation interval.

The Response Module applies the rate limit on the individual malicious flow upto a maximum threshold beyond which the attack flow is not throttled. When the attack concludes or decreases in strength, the rate of limit decreases until it comes down to zero and normal activity resumes at the defense system.

Materials and Methods

To evaluate the proposed scheme a testbed comprising of a handler machine, four source machines for traffic generation a defense system hosting the Snort IDS and a victim machine was created as illustrated in Fig. 2. To simulate DDoS attack in the test bed, UDP flood, TCP SYN flood and ICMP flood were generated using Stacheldraht tool.

Three of the source machines were used as agent machines to generate attack traffic and one source machine was used to generate legitimate traffic. The attack traffic comprised of UDP, TCP SYN and ICMP flood. The same source port and destination port numbers were used throughout the trace. Size of the attack packets, the rate of packets generated and duration of attacks were varied. The effect of the attack was similar regardless of the protocol used. The data collected using Libpcap at the defense system is presented in Table 1.

The attributes of the attack traffic from three source machines are shown in Table 2. The duration of attack was 600 sec.

Table 1. Test bed environment

Parameters	Attack dynamics
Duration of simulation	600 sec
Observation interval	3 sec
Protocol used	UDP, TCP SYN and ICMP
Attack rate	Constant
Number of legitimate hosts	1
Number of attack hosts	3-(1 host per protocol)
Number of packets	220646
Number of bytes	13475081
Average packet size	61 bytes
Average packet/second	368
Average bytes/second	22459

Table 2. Attack traffic characteristics

Source machines	Attack type	Number of packets	Packet rate (Packets/sec)	Byte rate (Bytes/sec)
Machine 1	UDP Flood	41588	69	4187
Machine 2	TCP SYN flood	51564	86	5099
Machine 3	ICMP flood	36038	60	3632

Results

The simulation of attack traffic generation at all three machines continued for 600 sec. The rate of packet generation was kept constant at all three machines. The observation interval was set at 3 sec. The attacks were detected at 3.001657 sec with a detection delay of 1.038521 sec.

It was observed that the observation interval was a key factor in the detection delay. The longer the duration of observation interval, the detection was more accurate, but the detection delay was higher. A shorter observation interval resulted in smaller detection delay but created more overhead in alert generation.

Rate limiting is applied based on the strength of the attack traffic of each individual attack flow and not as a constant rate of limit on the collective flow. This drastically improves the efficiency of the defense system.

The results clearly show that the proposed scheme can detect DDoS attacks early and the adaptive rate limiting strategy based on individual malicious traffic volume can be successfully deployed to limit the amount of malicious flow towards the target machine.

Discussion

The proposed correlation based approach with a sliding window model to detect and mitigate DDoS attacks, monitors the total volume of packets received at the defense system. It initiates packet rate limiting when the volume of traffic exceeds a threshold value instead of waiting untill the router is fully overwhelmedresulting in quicker attack detection than other schemes. The use of sliding window model ensures faster defense and attack mitigation than other previously proposed systems. Instead of applying a rate limit indiscriminately on the collective malicious flow, the proposed scheme identifies the volume of malicious traffic contributed by each attacking hosts and applies different rate limit on each individual malicious flow. This allows quicker recovery in case of false positives. While authentication technique and penalty schemes are effective in specialized servers catering to registered users it cannot be used in generalised servers such as google or yahoo, where users are not authenticated and all users are assumed to be legitmate. The proposed scheme is highly effective in rate limiting the malicious traffic and also protects the legitimate flows more efficiently.

Conclusion

The proposed correlation based approach with a sliding window model to detect and mitigate DDoS attack is a reactive approach to defend against DDoS

attacks. The scheme is light weight and can be easily deployed at crucial points of the core network for defense against DDoS attacks. The simulation results show that the proposed system identifies a DDoS attack quickly and responds by rate limiting the malicious traffic flow to limit damage to the victim and also allows legitimate flows towards the target system with a higher degree of accuracy.

Author's Contributions

D. Ayyamuthukumar: Organized the study, designed the research plan, participated in all experiments, coordinated the data-analysis and contributed to the writing of the manuscript.

S. Karthik: Improvements and suggestions in research plan executions.

Ethics

This article is original and contains unpublished material. The corresponding author confirms that all of the other authors have read and approved the manuscript and no ethical issues involved.

References

Anurekha, R., K. Duraiswamy, A. Viswanathan, V.P. Arunachalam and K.G. Kumar *et al*., 2012. Dynamic approach to defend against distributed denial of service attacks using an adaptive spin lock rate control mechanism. J. Comput. Sci., 8: 632-636. DOI: 10.3844/jcssp.2012.632.636

Beak, C., J.A. Chaudhry, K. Lee, S. Park and M. Kim, 2007. A novel packet marketing method in ddos attack detection. Am. J. Applied Sci., 4: 741-745. DOI: 10.3844/ajassp.2007.741.745

Bhaya, W. and M.E. Manaa, 2014. Review clustering mechanisms of distributed denial of service attacks. J. Comput. Sci., 10: 2037-2046. DOI: 10.3844/jcssp.2014.2037.2046

Kannan, A.R., K. Duraiswamy and K. Sangeetha, 2009. Three Dimensional Multidirectional Geographical IP Traceback: Direction Ratio Sampling Algorithm. J. Comput. Sci., 5: 136-139. DOI: 10.3844/jcssp.2009.136.139

Moorthy, M. and S. Sathiyabama, 2012. Effective authentication technique for distributed denial of service attacks in wireless local area networks. J. Comput. Sci., 8: 828-834. DOI: 10.3844/jcssp.2012.828.834

Udhayan, J. and M.R. Babu, 2013. Deteriorating distributed denial of service attack by recovering zombies using penalty scheme. J. Comput. Sci., 9: 1618-1625. DOI: 10.3844/jcssp.2013.1618.1625