ijecs open access www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 10 October, 2014 Page No.8772-8776

Adaptive Rate Limiting Strategy To Defend Against Distributed Denial Of Service Attacks

Mrs.C.krishnaveni

ckrveni@gmail.com
Department of CSE,SKR Engineering College,
Chennai,Tamilnadu,India

Abstract

Problem statement: **Distributed Denial of Service (DDoS) attacks is one of the more serious threats currently faced by Internet based companies. In this study, we deal with DDoS attacks by proposing a dynamic reactive defense system to detect and prioritize the malicious traffic flow towards a target system. Approach: The proposed scheme identifies the most critical flaw in the attack traffic based on the strength of malicious flow and the duration of attack persistence and applies an adaptive rate limiting on each individual flow instead of a fixed rate limit on the collective attack flow. The results: The scheme reacts very quickly to any changes in the network state. The results observed on the dataset shows that the proposed scheme detects the onset of the attacks very early and reacts to the threat by rate limiting the malicious flow. Conclusion: The proposed system can be successfully implemented as an autonomous defense system to limit damage to the victim by limiting the malicious flows towards the target system with a higher degree of accuracy.**

Keywords **:** Distributed Denial of Service, Rate Limiting, Flood Detection, Correlation, Flow Priority

I. INTRODUCTION

Internet connected systems face a consistent and real threat of Distributed Denial of Service (DDoS) attacks. DDoS attack is an explicit attempt by an attacker to overload the server(s) or network(s) with useless traffic that result in loss or interruption of all network connectivity and services and renders it unavailable to legitimate users. The primary resources targeted in a DDoS attack are bandwidth, processing capacity and storage capacity of victim machine and costs in terms of money and time.

A successful DDoS attack requires many susceptible and compromised machines to generate an extremely large volume of malicious traffic capable of overwhelming the target system for a duration long enough to cause sufficient damage to the target system in terms of availability to its legitimate users. Even for hardened internet based companies the loss of revenue due to

unavailability caused by a DDoS attack can be devastating.

❖ Related Works

The DDoSdefense mechanisms proposed by researchers are categorized based on DDoS detection, response and traceback. The detection techniques mainly include IP attributes-based DDoS detection or traffic volume-based DDoS detection. Response techniques involve either packet filtering or rate limiting.

Anurekha et al, proposed a scheme which uses a divide and conquer approach to identify the infected interface via which malicious traffic are received and identifies malicious traffic flow towards a target system based on the volume of traffic flowing towards the victim machine. It selectively implements rate limiting based on the

source of traffic flow towards victim and type of packet protocol rather than a collective rate limiting on flow towards the victim.

Beak, C., Proposed a Novel Packet Marketing Method to detect DDoS Attack using Link-ID's (information about the path between the Border Gateway Protocol (BGP) routers in the Autonomic Systems (AS) and each BGP router's connection to the outside of the AS) instead of IP addresses or routers to construct the path information of each packet and response included packet filtering methods.

Karthik, S., Et al proposed a Multi Directional Geographical Traceback with and Directions Generalization using Segment Direction Ratios (SDR). And Kannan, A. R., Proposed a Three Dimensional Multidirectional Geographical IP Traceback using Direction Ratio Sampling Algorithm and random sampling methods to reconstruct the path of the attack packets and trace the attack source.

Viswanathan, A., Et al proposed a Geographical Division Traceback for detecting DDoS attacks and utilizes the geographical information for identifying the source machines.Filtering techniques discard packets that do not match specific conditions specified in the router. However this approach is dependent on the cooperation and implementation by network operators and Internet Service Providers. Dropping all packets from a suspicious source(s), while effective in creating an immediate relief at the victim may also cause a great deal of legitimate traffic to be dropped. Hence this thesis proposes rate limiting as a more effective alternative to packet filtering approach. Here instead of dropping all malicious packets, the number of identifying malicious packets allowed to pass through a router is limited to a certain threshold.

Geographical traceback schemes while responding well in test beds and simulation environments do not work well in real situations. Hence this paper proposes a novel detection and response strategy to detect and mitigate DDoS attacks.

- **Priority Based Defense Against Distributed Denial of Service Attacks With an Adaptive Rate Limiting Strategy**

Priority Based Defense Against Distributed Denial of Service Attacks With an Adaptive Rate Limiting Strategy 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.

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 on 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..

II. ARCHITECTURE

The proposed Priority Based DefenseAgainst Distributed Denial of Service Attacks With an Adaptive Rate Limiting
Strategy consists of three functional units – Observation Module, Reasoning Module and Response Module as depicted in Fig. 1

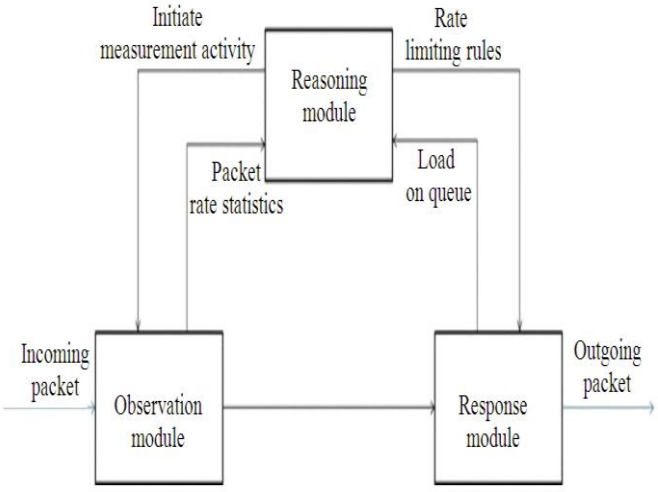

Fig. 1: Architecture of Priority Based DefenseAgainstDDoS Attacks With an Adaptive Rate Limiting Strategy

- ***Observation, reasoning and response module***

Monitoring module observes the packet arrival rate at each incoming interface for an observation interval Tobs, calculates its collective incoming flow and computes the Ratio of Collective Flow (RCF) at each interface (IF). This information is forwarded to the reason module. It is also responsible for monitoring the incoming packets and updating the Destination Based Table (DBT), Source Based Table (SBT) and Packet-type Based Table (PBT) when measurement activities are initiated by the reasoning module. All tables use a Time Stamp (TS) field to monitor when a record was last modified. When a table overflows the record with the oldest TS (Least Recently Used) is replaced. DBT contains the Destination Address (DA) of all packets arriving at infected interface and the number of packets for each DA. SBT records the Source Address (SA) of machines generating the packets for the DA from the DBT. For a specific SA-DA pair the PBT records the count of various packet types of traffic.

Reasoning module is primarily responsible for classifying a flow as legitimate, suspicious or attack flow based on packet information obtained from the monitoring module and the current load on outgoing queue. If the Ratio of Collective Flow (RCF) for the interface (IF), is less than a predefined threshold and load on the outgoing queue is below the maximum queue threshold (QMAX_T), reasoning module classifies the incoming flow as a normal / legitimate flow. If the RCF is above the threshold value and load at the queue is less than QMAX_T, flow is classified as suspicious flow and if both RCF and load exceeds the threshold, the flow is confirmed as malicious and the interface is tagged as infected. The reasoning module then activates individual packet monitoring and measurement activities at the infected interface of the monitoring module. It then defines the rules for rate limiting and initiates spin lock rate control to perform rate limiting on the malicious flow which is executed by the response module. The load on the queue is continuously monitored by the reasoning module to observe the effect of the rate limit rules and the rules are modified based on the above observation.

The success of the DDoS attack against a defense system and in turn the victim is defined by the volume of false negatives and false positives at the defense system

- ***Packet monitoring and measurement***

Packet monitoring is applied with a Divide and Conquer cum iterative approach. All incoming packets at router are not monitored. Rather the incoming flow at infected interface alone is monitored. Iterative refinement is used to determine the target of DDoS attacks, identify the source machine generating the malicious traffic and packet type of the malicious traffic and rate limiting is performed on malicious traffic while legitimate/normal traffic from the infected interface is left relatively undisturbed.

When measurement activity is first initiated for an infected interface, during the next observation interval the DBT is updated to determine the target machine for which the maximum volume of traffic was targeted. At the next observation interval the SBT is updated for the specific target address from DBT to isolate the source machine generating the malicious traffic towards the victim.

During the next consecutive interval the type of protocol used by the source machine from SBT for generating the malicious traffic is determined. Rate limiting is performed only on packets of that type from the source to target machine. At the end of each observation interval, all entries in the tables are removed and the values are recalibrated.

- ***Adaptive Rate Limiting Strategy***

This paper proposes the use of an adaptive rate limiting strategy instead of a fixed rate limiting value. Also the proposed rate of a limit to be applied is determined independently for each source machine based on the strength of the attack packet generated from that machine towards the target machine.

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

Assuming an N number of source machines are generating the attack traffic and x1, x2, x3,…Xian are the number of packets generated by each source machine.

The average number of packets 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 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 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 a limit to be applied to the attack traffic flow is given by

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

Where n is the number of successive intervals during which the attack continues and RL is the rate of limit applied in the previous observation interval. The rate limiting continues up to a maximum threshold beyond which the 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 in the defense system.

III.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. To simulate DDoS attack in the test bed, UDP flood, TCP SYN flood and ICMP flood were generated using Stacheldraht tool.

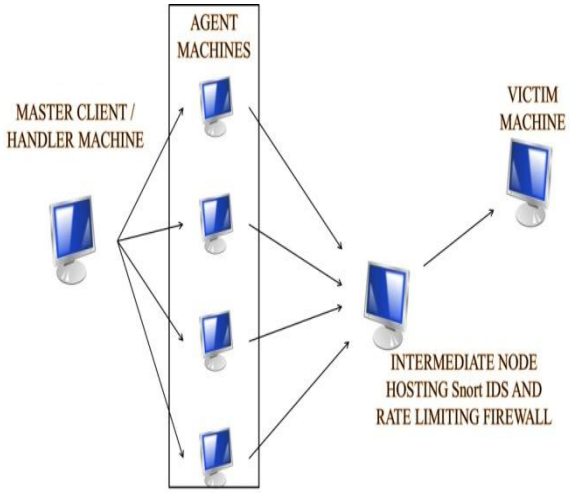

Fig. 2: Topology ofsimulated network

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. The size of the attack packets, the rate of packets generated and duration of attacks was 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.

Table 1: Test Bed Environment

Parameters	Attack dynamics
Duration of simulation	600 seconds
Observation Interval	3 seconds
The 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

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

Table 2: Attack Traffic Characteristics

Source Machines	Attack Type	Number of packets	Packet Rate (packets/Sec)	Bit 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

IV .RESULTS

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

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.

The adaptive rate limit strategy initially applied a small rate limiting factor and increased it gradually up to a maximum threshold value. 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 rate limiting can be successfully deployed to limit the amount of malicious flow towards the target machine.

V .DISCUSSION

The proposed scheme quickly detects the presence of DDoS attacks and has lower computational and memory overhead. It can be implemented at crucial checkpoints in the network to protect a target system. This drastically reduces the number of deployment points required to successfully combat DDoS attacks when compared to source end and victim end defense systems. The adaptive rate limiting strategy responds quickly to any changes in the traffic flow. The proposed scheme involveslower overhead yet protects legitimate flows more efficiently.

VI.CONCLUSION

Priority Based Defense Against Distributed Denial of Service Attacks With an Adaptive Rate Limiting Strategy is a reactive approach to defend against DDoS attacks. The scheme is light weight and can also be minimally deployed at crucial points of the core network for efficient results. The simulation results show that the proposed system responds quickly to malicious flows. Once detected, the attack flow can be throttled to limit damage to the victim and also allows legitimate flows towards the target system with a higher degree of accuracy.

VII .REFERENCES

[1] Andersen, D., H. Balakrishnan, M. Kaashoek and R. Morris 2001. Resilient overlay networks. Proceedings of the 18th ACM Symposium on Operating Systems Principles (SOSP' 01), ACM, New York, pp: 131-145. DOI: 10.1145/502034.502048

[2] 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

[3] Beak, C., Chaudhry, J. A., Lee, K., Park, S., And Kim, M., 2007, A Novel Packet Marketing Method in DDoS Attack Detection, American Journal of Applied Sciences, pp: 741-745, DOI: 10.3844/ajassp. 2007.741.745

[4] Ferguson, P. And D. Scene, 2000. Network ingress filtering: defeating denial of service attacks which employ IP source address spoofing. The Internet Society. http://rfc-ref.org/RFC-TEXTS/2827/index.html

[5] Ghazali, K. W. M., AndHassan, R., 2011, Flooding Distributed Denial of Service Attacks - A Review, Journal of Computer Science. Pp: 1218-1223. DOI: 10.3844/jcssp. 2011.1218.1223

Karthik, S., Arunachalam, V. P., And Ravichandran, T., 2011. Multi Directional Geographical Traceback with and Directions Generalization. Journal of