Journal of Computer Science 8 (5): 632-636, 2012
ISSN 1549-3636

Dynamic Approach to Defend Against Distributed Denial of Service Attacks Using an Adaptive Spin Lock Rate Control Mechanism

[1]Anurekha, R., [2]K. Duraiswamy, [3]A. Viswanathan,
[4]V.P. Arunachalam, [3]K. Ganesh Kumar and [3]A. Rajivkannan
[1]Department of Information Technology,
Institute of Road and Transport Technology, Erode, Tamilnadu, India
[2]Department of CSE, K.S. Rangasamy College of Technology,
[3]Department of CSE, K.S.R. College of Engineering,
Tiruchengode, Namakkal, Tamilnadu, India
[4]SNS College of Technology, Coimbatore, Tamilnadu, India

Abstract: Problem statement: The last decade has seen many prominent Distributed Denial of Service (DDoS) attacks on high profile webservers. In this study, we deal with DDoS attacks by proposing a dynamic reactive defense system using an adaptive Spin Lock Rate control (D3SLR). D3SLR identifies malicious traffic flow towards a target system based on the volume of traffic flowing towards the victim machine. **Approach:** The proposed scheme uses a divide and conquer approach to identify the infected interface via which malicious traffic are received and selectively implements rate limiting based on the source of traffic flow towards victim and type of packet rather than a collective rate limiting on flow towards victim. **Results:** The results observed in simulation shows that D3SLR detects the onset of the attacks very early and reacts to the threat by rate limiting the malicious flow. The spin lock rate control adapts quickly to any changes in the rate of flow. **Conclusion:** D3SLR can be successfully implemented at critical points in the network as autonomous defense systems working independently to limit damage to the victim and also allows legitimate flows towards the target system with a higher degree of accuracy.

Key words: Spin lock rate control, adaptive rate limiting, distributed denial of service

INTRODUCTION

The frequency, severity and sophistication of Distributed Denial of Service (DDoS) attack pose a serious threat to the availability of evolving Internet services. DDoS attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. They are capable of either crashing the host such that it cannot communicate properly with the rest of the network or disrupting/degrading the host's service and rendering it unavailable for legitimate users.

The key feature of DDoS includes distributing the attack across several hosts and coordinating the attack among the hosts. Multiple compromised machines are used to launch/direct a coordinated attack on a target machine, usually one or more servers, by overwhelming the target machine with a large volume of malicious packets that can cause the target machine's CPU usage to max out, preventing any work from occurring. It can trigger errors in the target machine and force it into an unstable state or lock-up. Exploiting errors in the operating system can cause resource starvation and/or thrashing and ultimately crash the operating system itself. The software for launchinga DDoS attack is powerful and the attack traffic mimics the behavior of legitimate users and hence is much harder to detect.

Related works: Since DDoS attacks came to prominent focus in the late 1999, many countermeasures have been proposed by researchers to counter DDoS attacks, the most popular being the IP traceback, use of overlay architecture and rate limiting/filtering at source/victim end routers or gateways.

The most popular approach to DDoS defense is by use of IP traceback-trace the origin of attack and take the host system out of action. This is a slow process during which the victim site can do nothing to restore

Corresponding Author: Anurekha, R., Department of Information Technology, Institute of Road and Transport Technology, Erode, Tamilnadu, India

its service to legitimate clients. Lim and Uddin (2005) and Wang *et al*. (2002) proposed mechanisms for the detection and mitigation of SYN flooding attack.

Secure Overlay architecture proposed by Keromytis *et al*. (2002) and Resilient Overlay architecture proposed by Andersen *et al*. (2001) authenticates all access requests to target machine and authenticated traffic is routed via an overlay network to one of the servlets, which then forward the requests to the target site. Wang *et al*. (2006) later proposed a generalized form of the overlay architecture. Overlay and redirection architectures are designed for effectiveness of emergency services and are not suitable for protecting a general-purpose public server (such as Yahoo or Google), because all users are supposed to be authorized, which makes the authentication itself meaningless.

Filtering techniques, proposed by Ferguson and Senie (2000) and Park and Lee (2001) and Rate Limiting techniques, proposed by Liang and Yau (2002) discard packets that match specific conditions specified at the router. When properly configured and supported by network operators, these approaches can effectively prevent DDoS attack. However this approach is dependent on the cooperation and implementation by network operators and Internet Service Providers (ISP). The ISPs usually do not have strong incentive to implement the filtering mechanisms into their routers since it increases the overhead but has no direct benefit to their own clients.

D-Ward: Mirkovic and Reiher (2004; 2005) proposed a Source-End DDoS Network Attack Recognition and Defense (D-WARD) installed at the source router which uses a novel traffic profiling techniques and adaptive response to achieve autonomous attack detection and accurate response. D-WARD is configured with a set of local addresses whose outgoing traffic it polices-its police address set. This set identifies all machines in the stub network or all customers of an ISP. D-WARD consists of observation, rate-limiting and traffic-policing components.

The Observation Component monitors all packets passing through the source router and gathers aggregate flow and connection granularity statistics on two-way communications between the police address set and the rest of the Internet. The aggregate flow is the traffic between the police address set and one foreign IP address and connection granularity is the aggregate traffic between a pair of IP addresses and port numbers, where one address belongs to the police address set and the other is a foreign address. Periodically, statistics are compared to legitimate traffic models and agflows and connections are classified as attack or legitimate. The observation component passes the information to the rate-limiting component which decides to impose, modify or remove the rate limit based on the agflow's sending rate.

D-WARD's rate-limit strategy applies modified TCP congestion control for fast recovery from false positives. A fast exponential decrease of the sending rate is performed when the attack is detected to quickly relieve the victim of high-volume traffic. Once the attack subsides, D-WARD performs a slow recovery of rate-limited agflows, linearly increasing the sending rate. This is done to probe the state of the receiver and to reevaluate its ability to handle traffic. After a while, if the attack is not repeated, D-WARD performs a fast recovery of rate-limited agflows, increasing the sending rate exponentially.

The traffic-policing component periodically receives rate-limited agflow information from the rate-limiting component and connection classification information from the observation component which are to reach a decision whether to forward or drop each outgoing packet. Packets from nonlimited agflows and good connections are always forwarded. TCP packets from transient connections on limited agflows, whose sequence number matches the predicted value, are forwarded if the Early Packet Rate Limit for the agflow is not exhausted. Other transient-connection packets are forwarded if the agflow's rate limit is not exhausted. Some of the major drawbacks of the above defense system are:

- Requires wide range of deployment for effective defense
- Needs to monitor and log information about every packet. Increases the computational and memory overhead
- Does not take transient traffic into consideration. Only traffic originating from the source network is considered

In order to overcome these limitations a dynamic approach to defend against DDoS attack using an adaptive spin lock rate control mechanism has been proposed.

Dynamic DDoS Defense with Adaptive Rate Limiting (D3ARL): The two key problems faced in the identification of malicious traffic are false positives-alerts that are triggered on normal/legitimate activity where no attack is underway, but the normal activity matches an attack signature and false negatives-alerts triggered when a detection mechanism fails to detect an actual attack, since it did not have the rules to match the attack.

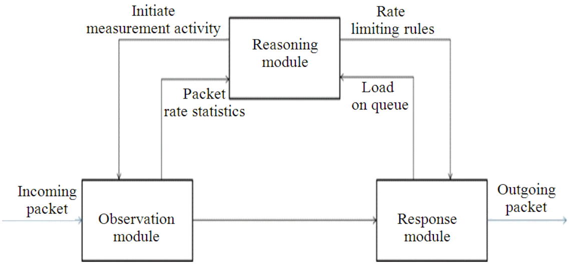

Fig. 1: D3SLR architecture

An ideal defense system should have the ability to correctly identify and differentiate malicious traffic from legitimate traffic, have very low or negligible false positive and false negative rates and fast response handling mechanisms.

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.

D3ARL architecture: The proposed Dynamic DDoS Defense with Adaptive Rate Limiting mechanism consists of Monitoring module, Reasoning module and Response module as depicted in Fig. 1.

Monitoring, reasoning and response module: Monitoring module observes the packet arrival rate at each incoming interface for an observation interval T_{obs}, calculates its collective incoming flow and computes the Ratio of Collective Flow (RCF) at each interface (I_F). 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 type 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 interface (I_F), 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 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, 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 by 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. 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 attack, 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.

Spin lock rate control: D3SLR is a reactive defense system in which rate limiting is applied on outgoing traffic on detection of abnormal activity. D3SLR implements a spin lock rate control mechanism which does not immediately throttle the outgoing flow. Rather it tries to increase the initial Spin Lock Rate Limiting factor (SLR) by small increments (n*δ*SLR) in successive observation periodsT_{obs}, where n is the count of observation period since the onset of attack identification and δ is the current percentage of load at the outgoing queue.On onset of attack the rate limiting is applied in iterative steps. In the first observation intervala Spin Lock Rate Control (SLR) is applied on total volume of traffic at the infected interface. In the second observation interval SLR is incremented and applied to the traffic at infected interface destined for the DA alone. During the next observation interval SLR is again incremented and applied to the traffic from SA to DA. Further rate limiting is applied to the specific packet type on traffic from SA to DA with an increasing SLR factor given by:

$$SLR = SLR + \sum_{n=0}^{\infty} n * \delta * SLR$$

The rate limiting is continued until a minimum volume of flow is achieved at the infected interface beyond which the flow cannot be throttled.When the DDoS attack concludes, Spin Lock Rate Control gradually decrements the SLR in successive observation intervals by SLR, (SLR-δSLR), (SLR-2δSLR), (SLR-3δSLR) and so on until the rate limit spins down to zero and normal activity resumes at the defense system.

MATERIALS AND METHODS

To evaluate D3SLR's ability to control and mitigate the effect of DDoS attacks, DDoS attack is simulated using NS-2 network simulator. The network topology for simulation of DDoS is as shown in Fig. 2.

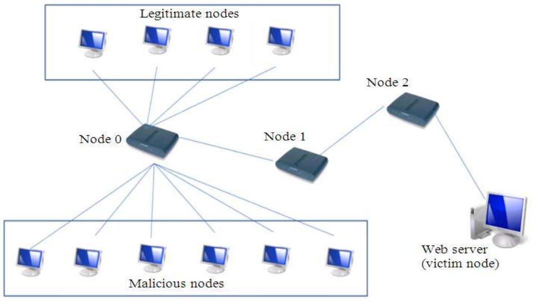

Fig. 2: Topology of simulated network

The topology consists of 10 source machines, a core network and a victim network. Four source machines generate legitimate traffic and six source machines generate attack traffic. For UDP based attacks, legitimate users generate UDP traffic at rate of 0.5 Mbps to web server starting at 1.0-29.0 sec, while malicious clients generate traffic between 8-10 Mbps to web server for 15 sec from at 11.0-25.0 sec.

RESULTS

The simulation is carried out for 30 sec and Fig. 3 shows the volume of legitimate and attack traffic generated during the simulation period.

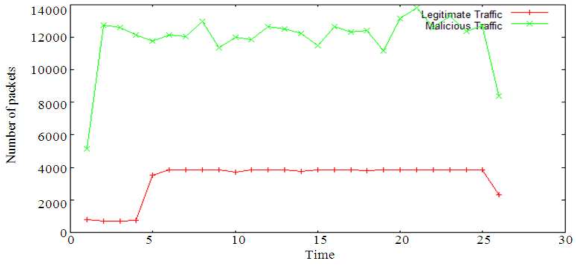

Fig. 3: Volume of legitimate and malicious traffic Generated

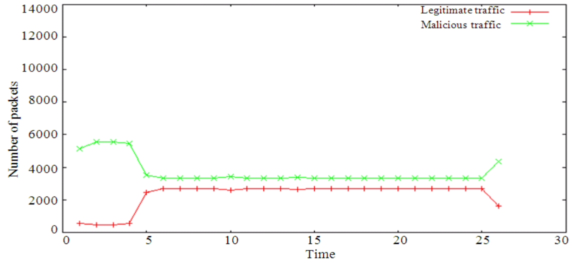

Fig. 4: Legitimate and malicious traffic forwarded from Node 0 when no defense is implemented

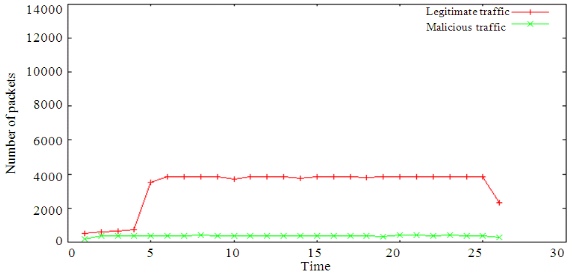

Fig. 5: Legitimate and malicious traffic forwarded from Node 0 when D3SLR defense is implemented

Figure 4 shows the percentage of attack traffic and legitimate traffic forwarded from the Node 1 when no defense scheme has been deployed and Fig. 5 shows the simulation result of D3SLR scheme. The results clearly show that D3SLR can detect DDoS attacks early and rate limiting can be successfully deployed to limit the amount of malicious flow towards the target mcahine. Also the proposed spin lock rate control mechanism responds to changes in the traffic flow quickly.

DISCUSSION

The proposed D3SLR scheme only monitors infected interfaces of a router and individual packet measurement is initiated only on confirmation of an attack. This reduces the 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 in comparison with DWARD systems. The proposed scheme involves lower overhead yet protects legitimate flows more efficiently.

CONCLUSION

D3SLR 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 D3SLR 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.

REFERENCES

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

Ferguson, P. and D. Senie, 2000. Network ingress filtering: defeating denial of service attacks which employ IP source address spoofing. The Internet Society.

Keromytis, A.D., V. Misra and D. Rubenstein, 2002. SOS: Secure overlay services. Proceedings of the 2002 Conference on Applications, Technologies, Architectures and Protocols for Computer Communications, ACM New York, NY, USA., pp: 61-72. DOI: 10.1145/633025.633032

Liang, F. and D. Yau, 2002. Using adaptive router throttles against distributed denial-of-service attacks. J. Softw., 13: 1220-1228.

Lim, B.P. and M.S. Uddin, 2005. Statistical-based SYN-flooding detection using programmable network processor. Proceedings of the 3rd International Conference on Information Technology and Application, Jul. 4-7, IEEE Xplore Press, Sydney, pp: 465-470. DOI: 10.1109/ICITA.2005.262

Mirkovic, J. and P. Reiher, 2004. A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Commun. Rev., 34: 39-53. DOI: 10.1145/997150.997156

Mirkovic, J. and P. Reiher, 2005. D-WARD: A source-end defense against flooding denial-of-service attacks. IEEE Trans. Dependable Secure Comput., 2: 216-232. DOI: 10.1109/TDSC.2005.35

Park, K. and H. Lee, 2001. On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets. Proceedings of the 2001 Conference on Applications, Technologies, Architectures and Protocols for Computer Communications, ACM New York, NY, USA., pp: 15-26. DOI: 10.1145/383059.383061

Wang, H., D. Zhang and K.G. Shin, 2002. Detecting SYN flooding attacks. Proceedings of the 21st Annual Joint Conference of the IEEE Computer and Communications Societies, Jun. 23-27, IEEE Xplore Press, New York, pp: 1530-1539. DOI: 10.1016/j.comcom.2005.09.008

Wang, X., S. Chellappan, P. Boyer and D. Xuan, 2006. On the effectiveness of secure overlay forwarding systems under intelligent distributed DoS attacks. IEEE Trans. Parallel Distributed Syst., 17: 619-632. DOI: 10.1109/TPDS.2006.93