Sky Shield: A Sketch-Based Defense System against Application Layer Ddos Attacks

Pavithra Pandith[1], Shubha H.D[2], Manasa Manjunatha[3]

[1,2]Final Year B.E Student, ISE, The National Institute of Engineering, Mysore
[3]Assistant Professor, Department of ISE, The National Institute of Engineering Mysore

---

Abstract **-** DDoS stands for distributed denial of service attack. It's basically a DOS attack but simultaneous requests are sent from multiple compromised nodes to one targeted system instead from a single node, to bring it down and stop servicing a normal user. The compromised nodes are botnets which are vulnerable and is under the control of a bot master which sends commands to these systems which triggers sending requests from botnets to target simultaneously. At the application layer as soon as attack is detected we try to reduce it using sky Shield application. Sketch is a data structure where it uses hashing with key being unique IP address of system and value being no of packets sent, bytes etc. For each request we calculate sketch and update it each time. Here we calculate the divergence between two sketches and based on observation flag it as malicious or genuine user.

Keywords: DOS attack, Botnet, Bot master, Sketch, hashing.

1. INTRODUCTION

At the application layer ,DOS attacks are increasing day by day because of which many systems are been compromised and also many organizational servers are been crashing and they stopped servicing normal users which brings huge losses to organization. The main goal of attackers is to bring the system down by exhausting all the resources so that no more it can service any request. These attacks can take place at network or application layer. We concentrate on application layer because here is where web pages are generated and http requests sent. In DoS attack, requests are sent from one single host to target. But in Distributed DoS multiple systems are used to send requests to target. Victims of a Distributed DoS attack is not only the target but also all those compromised nodes which are under control of botmaster. Sky Shield application is designed to detect the source of attack and quickly stop servicing it, so that system can perform as usual like before. Here a sketch is designed for each requests and is updated on each new request. Once it notes of malicious activity that is when large divergence is observed between original and updated sketch it marks as malicious in bloom filter.

A. EXISTING SYSTEM

Static threshold: We set a threshold value on number of requests a node can service. If requests are more than threshold mark as malicious, care should be taken because it might be flash crowd also.

Behavioural analysis: Here we suspect of attacks based on behaviour i.e if a pdf file is downloaded more than usual suspect it.

Challenge response: Using captcha test, since bots does not have image processing capabilities, it cannot type the distorted or tilted letters.

B. PROPOSED SYSTEM

A sketch data structure can effectively distinguish between normal user and attacker .It keeps track each and every nodes activity .Here we use hashing technique called a sketch with the key being IP address of a packet from the receiver and the values are number of packets sent, bytes, requests made for connection, for each packet we design this sketch and update the sketch as new packet arrives and we calculate divergence between original and updated sketch i.e the network flow difference ,here we can also detect spoofed IP addresses also.

2. ARCHITECTURE

The system architecture makes use of Bloom filter, it is basically a data structure here it marks node as either malicious or genuine and it is based on trust value .It helps to identify trusted client and give them access to a system and also mark malicious users and stop servicing them. We calculate trust value based on node's activity .It makes use of Captcha test to hold legitimate IP and also keep track of botnets in network.

Sketch uses two bloom filters one called whitelist which holds legitimate users and granting access based on Captcha test and other one blacklist which holds malicious attacker list. Sketch is calculated for each requests i.e for each packet and

each time it is updated after new packet comes from a same machine .At any point of time if large divergence is observed between two sketches then it is marked as malicious and captcha test is given to those machines, finally it denies access to those attacker machines if it fails test.

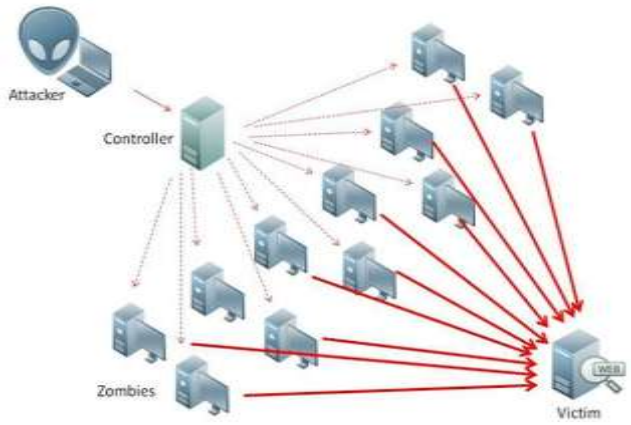

FIG - 1: SYSTEM ARCHITECTURE

3. METHODOLOGIES

A. Sketch Design

For this project we are using a Sketch i.e hash data structure because in a network of huge traffic, hashing is more efficient to store the requests and retrieve it effectively. Because it takes O (n) to retrieve information. Here key must be unique so we choose IP address because network of nodes is identified uniquely by its IP address and the value being records such as no of connection request made, packet sent etc.

B. Bloom filter design

Bloom filter is a data structure where it marks either malicious or genuine. It depends upon trust value. IP addresses are stored on filter which helps in determining trusted clients and give them access. Trust value depends upon node's activity, network's traffic. It makes use of Captcha test to hold legitimate IP and also keep track of botnets in network.

C. Calculation of divergence

For each sketch we calculate the rise in request by comparing its rise in peak level with the previous or the original sketch .When we notice a rapid change in request made or huge change in peak levels. It is marked as malicious.

D. Bot Detection

Bot master detects vulnerable systems in network and keeps it under his control. Bot master continuously sends commands to those affected nodes i.e bots wherein they initiates requests to target to crash it. Challenge Response Captcha test used to detect bots because they fail in image processing because normal humans can recognize image tilts but bots cannot.

E. Detection of Attacker IP Address

In this we try to find out the IP address of attacker so that we can block further requests from those nodes so that we can control further crashing and bring back system to original.

4. CONCLUSION

Network traffic is increasing rapidly nowadays thereby the ones who hacks the internet, so cyber security has become a serious issue. Many and many nodes are having some security issue so that they become vulnerable to threats by hackers and will be controlled by them according to their needs and is triggered to do some malicious acts. So we need to prevent and reduce these attacks as soon as it is detected .Distributed DoS attack are difficult to distinguish between legitimate users and malicious attack ,careful observation should be made and necessary steps should be taken to flag as malicious or intended user. Steps are taken to mitigate it at application layer i.e as soon as it is detected stop servicing the intruder machines. First we calculate divergence and use other technique called as bloom filter and captcha to detect it.

REFERENCES

[1] C. Wang, T. T. Miu, X. Luo, and J. Wang, " Skyshield: A sketch-based defense system against application layer ddos attacks ", IEEE Transactions on Information Forensics and Security, 13(3) : 559–573, 2018

[2] Ripon Patgiri1 , Sabuzima Nayak1 , and Samir Kumar Borgohain , "Preventing DDoS using Bloom Filter " , EAI Endorsed Transactions on Scalable Information Systems ,Volume 5 , Issue 19 , June 2018

[3] S. Simpson, S. N. Shirazi, A. Marnerides, S. Jouet, D. Pezaros, and D. Hutchison. An inter-domain collaboration scheme to remedy ddos attacks in computer networks. IEEE Transactions on Network and Service Management, pages 1–1, 2018

[4] C. Tseung, K. Chow, and X. Zhang. Anti-ddos technique using self-learning bloom filter. In Intelligence and Security Informatics (ISI), 2017 IEEE International Conference on, pages 204–204. IEEE, 2017

[5] P. Xiao, Z. Li, H. Qi, W. Qu, and H. Yu. An efficient ddos detection with bloom filter in sdn. In

Trustcom/BigDataSE/I-SPA, 2016 IEEE, pages 1–6. IEEE, 2016

[6] B. Schneier. Lessons from the dyn ddos attack. https://www.schneier.com/blog/archives/2016/11/lessons_from_th_5.html, Nov 2016.

[7] M. Aldwairi and K. Al-Khamaiseh. Exhaust: Optimizing wu-manber pattern matching for intrusion detection using bloom filters. In Web Applications and Networking (WSWAN), 2015 2nd World Symposium on, pages 1–6. IEEE, 2015.

[8] T. Halagan, T. Kováčik, P. Trúchly, and A. Binder. Syn flood attack detection and type distinguishing mechanism based on counting bloom filter. In Information and Communication Technology, pages 30–39. Springer, 2015

[9] S. D. Jackman, B. P. Vandervalk, H. Mohamadi, J. Chu, S. Yeo, S. A. Hammond, G. Jahesh, H. Khan, L. Coombe, R. L. Warren, and I. Birol. Abyss 2.0: resource-efficient assembly of large genomes using a bloom filter. Genome Research, 27, 05 2017.

[10] P. Kakkar, P. Sharma, and K. Krishan. Security methods against tcp syn flooding ddos attacks in wireless networksa survey. International Journal of Current engineering and scientific research (IJCESR), 2018

[11] L. Kavisankar, C. Chellappan, S. Venkatesan, and P. Sivasankar. Efficient syn spoofing detection and mitigation scheme for ddos attack. In Recent Trends and Challenges in Computational Models (ICRTCCM), 2017 Second International Conference on, pages 269–274. IEEE, 2017

[12] S. S. Kolahi, K. Treseangrat, and B. Sarrafpour. Analysis of udp ddos flood cyber attack and defense mechanisms on web server with linux ubuntu 13. In Communications, Signal Processing, and their Applications (ICCSPA), 2015 International Conference on, pages 1–5. IEEE, 2015.

[13] J. Shu, X. Jia, K. YANG, and H. Wang. Privacy-preserving task recommendation services for crowdsourcing. IEEE Transactions on Services Computing, 2018.

[14] C. Tseung, K. Chow, and X. Zhang. Anti-ddos technique using self-learning bloom filter. In Intelligence and Security Informatics (ISI), 2017 IEEE International Conference on, pages 204–204. IEEE, 2017.

[15] K. Verma and H. Hasbullah. Bloom-filter based ipchock detection scheme for denial of service attacks in vanet. Security and Communication Networks, 8(5):864– 878, 2015.