Journal of Basic and Applied Engineering Research
Print ISSN: 2350-0077; Online ISSN: 2350-0255; Volume 2, Number 16; April-June, 2015 pp. 1399-1401
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/jbaer.html

Detection and Mitigation of DDOS Attack by Optimizing the HADOOP Scheduler

Savneet Kaur Ahuja[1], Paras Chawla[2] and Sonia Saini[3]

[1]M.Tech, Student, JMIT, Radaur
[2,3]JMIT, Radaur
E-mail: [1]savneetahujaa@gmail.com , [2]paraschawla@jmit.ac.in, [3]soniasaini@jmit.ac.in

Abstract—*A massive volume of internet has increased in the world of communication which increases many obstacles. The main obstacle is DDOS attack. DDOS attack floods hundreds or thousands of requests on the target machine and either make it lethargic or unavailable for coming requests. It damages the database of the machine. To handle the big data, many schemes have been implemented but the most efficient scheme is the Hadoop. Hadoop is the open source tool designed by Google and it supports the distributed computing environment technology. The paper focuses on the different types of DDOS attack and a proposed method is designed to detect and mollify the DDOS attack. This paper compares the different types of DDOS attack and also compares the proposed work with the CAPTCHA technique.*

Keywords*: Big data, Distributed computing, Hadoop, DDOS attack*

1. INTRODUCTION

A massive volume of traffic has increased in the communication world. This increases the flooding in the network. This flooding is called DDOS attack. DDOS attack is the main obstacle which generates catastrophic failure in the machine. There are different types of DDOS attack such as synchronize (SYN) flooding attack, User datagram protocol (UDP) flooding attack, Domain name system amplification (DNS A) flooding attack etc. These attacks follow some protocols to send the infinite number of packets and machine fails to respond the further requests. This paper focuses on the SYN flooding attack, UDP flooding attack and DNS A flooding attack.

In synchronize flooding attack, attackers send the large of packets to the victim machine one after the other and makes the network unavailable for further packets. In User Datagram Protocol, attackers send the requests to the target machine and it is unavailable for the further requests. Spoofed IPs is used to send the requests so that victim does not get any information of the attacker. In Domain Name System Amplification attack, attacker sends the URL requests to the target machine and it is unavailable for the further URL requests. It sends requests 10 times faster than the Domain name system.

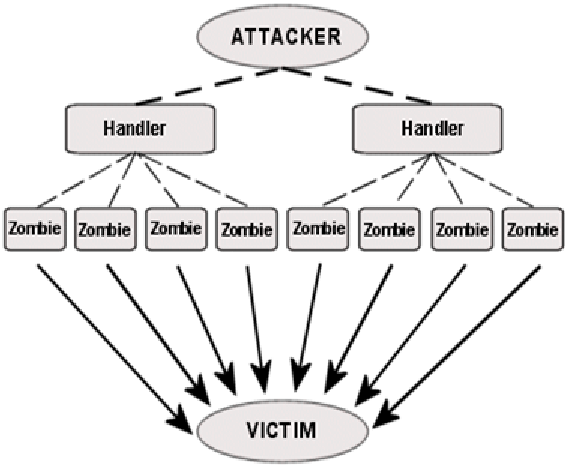

Fig. 1: Architecture of DDOS attack

To handle the large number of requests, hadoop is the efficient method. Hadoop, a open source software which supports distributed computing environment. Hadoop consists of Hadoop distributed Filesystem and Mapreduce. Hadoop distributed Filesystem splits the file into the log files. Mapping consists of Map phase and reduce phase. In map phase, it maps all the files and in reduce phase, It shuffles, sorts and then reduces the files which contains DDOS attack Hadoop scheduler allocates the jobs to the job tracker and then it further assigns to the task tracker.

2. RELATED WORK

IP blacklisting concept is used. Table is formed and then traffic is checked. If the volume of traffic is high then IP is put into the table. It is blacklisting. It checks the bad host files to know the blacklisted IP. Then the access rate is being checked and if it is more than the threshold users then restricts the http count. Then further CAPTCHA technique is used to differentiate between botnet and human users. [9]

Wavelet analysis method is the complex method for detecting the DDOS attack. Modified Wavelet analysis method includes

Isomap algorithm and wavelet analysis. It is used to reduce the network traffic but enhances the analytical network data. This method detects the weak DDOS attack. Its performance is better because it considers the extra step. This method is also used in real time detection. [12]

New challenges have been faced in the cloud computing. It addresses the important problem. This research examines the impact of security particularly in case of DDOS attack. Software defining network technology is used to detect the DDOS attack. Mitigation architecture monitors the attack detection and controls over it. A graphical based model handles dataset shift problem. This is effective in real world network traffic. [13]

It analysis the DDOS attack detection. It tells about the framework which consists of three parts:-

1. It collects the log module which it tells packet and log collection module (PLCM).
2. Then it analysis the packet and creates pattern which it tells PAM (packet analysis module).
3. Finally the third module perceives the DDOS perceives the DDOS attack and this is called DM (detection module).

The model which is used is normal behavior model. Then it tells the detection of DDOS attack and detection are used the network at the normal state and its next step is that it checks for attack. Finally it defines the threshold by using the parameter of normal state. [14]

3. PROPOSED WORK

In the proposed method, Netstress has introduced the different types of DDOS attack and Wireshark captures it. The captured file is copied in the hadoop system and then hadoop scheduler allocates the jobs. Hadoop checks the size of log files. If the size of log files are large then it is blocked otherwise it is processed. In this way, results are collected.

Algorithm is as follows –

```
Flooding = Netstress (SYN, UDP, DNS A)
{
Capturing = Wireshark (Black, Blue, Blue)
{
Hadoop system = Wireshark.txt
{
Scheduler = job assignment
{
Job= Log files (N)
{


If
Size of (log file (1) > threshold value
Then
IP (log file (1) = blocked
Else
IP (log file (1) = processed
}
}
}
}
}
```

4. RESULTS

After the implementation of detecting method, the comparison of following parameters with respect to different types of DDOS attack.

4.1 SLOTS_MILLIS_MAPS–

It considers the time which is executed during the mapping. Fig. 2 shows Slots millis maps versus Job done. It is a time graph. This Fig. shows that The DNS A takes more time as compared to other.

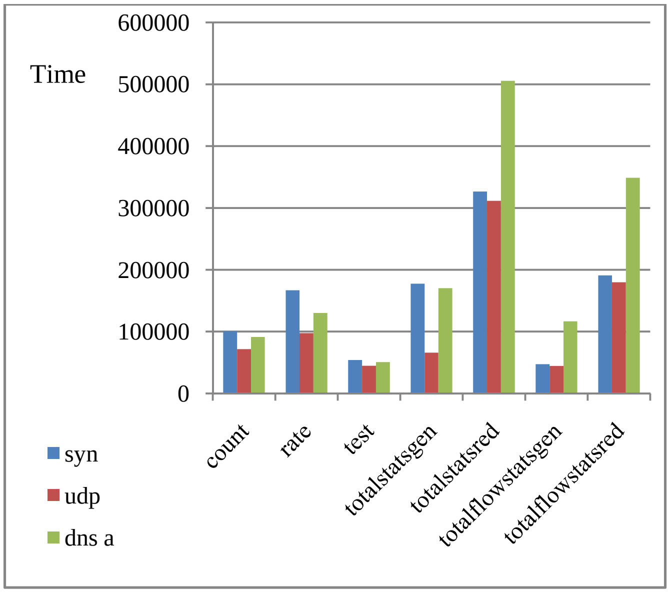

Fig. 2: SLOTS_MILLIS_MAP versus Job done

a. *SLOTS_MILLIS_REDUCE–*

It considers the time which is executed during the reducing. Fig. shows Slots millis reduce versus Job done. It is a time graph. This Fig. shows that The DNS A takes more time as compared to other.

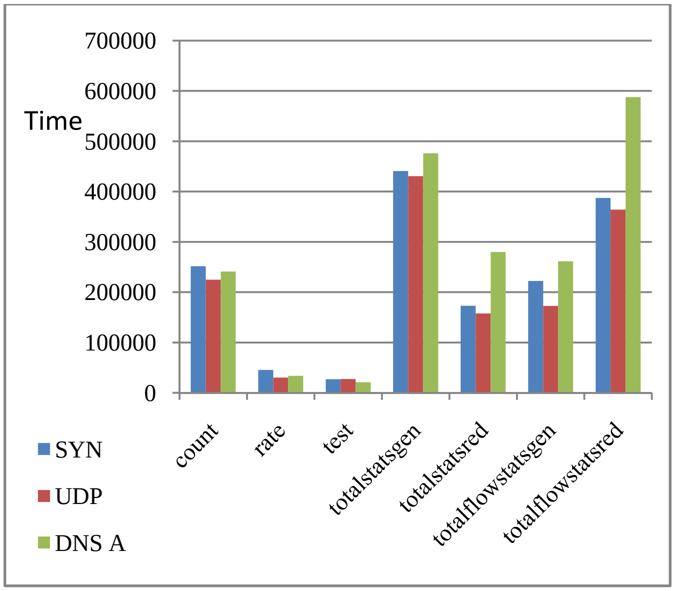

Fig. 3: SLOTS_MILLIS_REDUCE versus Job done

b. Comparison between the Capcha technique and the proposed method

Table 1: Comparison between the Capcha technique and the proposed method

Parameters	CAPTCHA TECHNIQUE	Proposed Method
DDOS attack	HTTP Get	Netstress
Mode	Online	Online/Offline
Monitors	Traffic	Traffic + size of Log files
Technique	Captcha technique	Hadoop
Filter	IPs	IPs + Packets

5. CONCLUSION AND FUTURE PERSPECTIVE

In this paper, we have discussed the Detecting method of DDOS attack in which DDOS attack is introduced by NETSTRESS and captured by Wireshark. The above graphs conclude that the mapping and reducing time is more in DNS A flooding attack. This means the header files of DNS A is more complex than other types of DDOS attack. The table concludes that proposed method is better than the previous method because it is only for connectionless attacks but proposed method is for all types of DDOS attack. Proposed method is also effective for real world network.

In this paper, we are focusing on one node but in future, we will consider the multinodes. We are focusing on only three types of ddos attack but in future, we are trying to consider all the types of ddos attack.

REFRENCES

[1] Hadoop Distributed File System. *http://Hadoop.apache.org/common/docs/current/ hdfsdesign.html*

[2] Fair Scheduler. *http://Hadoop.apache.org/common/docs/r0.20.2/fair scheduler. html*

[3] Mirkivic and Peter Reiher, A Taxonomy of DDOS Attack and DDOS Defense Mechanisms, ACM SIGCOMM CCR, Volume 34, Pages 39-53, 2004

[4] Amey shevtekar, Nirwan ansari, "Is It Congestion or a DDOS Attack?" IEEE COMMUNICATIONS LETTERS, VOL. 13, NO. 7, JULY 2009

[5] B.b.gupta, anupama mishra, r.c.joshi, "A Comparative study of Distributed Denial of Service Attacks, Intrusion Tolerance and mitigation Techniques" 2011 European Intelligence and Security Informatics Conference, ISBN 978-0-7695-4406-9, Page 286–289, 12-14 Sept. 2011, Athens

[6] Owen O'Malley, "TeraByte Sort on Apache Hadoop", Yahoo!, May 2008

[7] Yeonhee Lee and Youngseok Lee "Perceiveing DDOS attacks with Hadoop", Proceedings of The ACM CoNEXT Student Workshop, ISBN: 978-1-4503-1042-0, December 6 2011, Tokyo, Japan

[8] Jiong xie, fanjun meng, hailong wang, hongfang pan, jinhong cheng, xiao qin, Research on Scheduling Scheme for Hadoop clusters, International Conference on Computational Science, ICCS 2013, ISBN 1877-0509, pages 2468–2471, May 2013

[9] Khundrakpam Johnson Singh and Tanmay De, "DDOS Attack Detection and Mitigation Technique Based On Http Count and Verification Using CAPTCHA", 2015 International Conference on Computational Intelligence & Networks, ISBN 2375-5822/15, Pages 196–197, 12-13 Jan. 2015, Bhubaneshwar

[10] S. S. Vernekar, A.R. Buchade, "Mapreduce based Log File Analysis for System Threats and Problem Identification". In the Proceeding of 3rd IEEE International Advance Computing Conference (IACC), ISBN 978-1-4673-4527-9, Pages 831 - 835, Feb 2013

[11] T. White, Hadoop: The Definitive Guide. O'Reilly Media, Inc., USA, 2009.

[12] Bing Wang, Yao Zheng, Wenjing Lou, Y. Thomas Hou, "DDOS attack Protection in the era of cloud computing and Software defined network" Volume 81, Pages 308-319, 22 April 2015

[13] Liang Fu Lu, Mao Lin Huang, Mehmet A. Orgun, Jia Wan Zhang "An Improved Wavelet Analysis Method for Detecting ddos Attacks", Network and System Security (NSS), 2010 4th International Conference, ISBN - 978-0-7695-4159-4/10, pages 318–322, 1-3 Sept 2010, Melbourne, VIC

[14] Junho choi, chang choi, byeongkyu ko, pankoo kim, A method of DDOS attack detection using HTTP packet pattern and rule engine in cloud computing environment, Springer, ISSN 1433-7479, Volume 18, Issue 19, September 2014, Berlin Heidelberg