Secured Network from Distributed DOS through HADOOP

R.S.Dayama
Department of
Computer Engineering
N.B.N.Sinhgad College
of Engineering, Solapur

Aakanksh Bhandare
BE Student
N.B.N.Sinhgad College
of Engineering

Bhagayshri Ganji
BE Student
N.B.N.Sinhgad College
of Engineering

Vijaya Narayankar
BE Student
N.B.N.Sinhgad College
of Engineering

ABSTRACT

The purpose of this paper is to study the characteristics of DDOS attack, various models involved in attacks and to provide alternative. To defences mechanism with their improvements to combat DDOs attack.

Recent DDOS attack has demonstrated horrible destructive power by paralyzing web servers within short time. DDOs detection method based on hadoop that implements an Http Get Flooding detection algorithm in mapreduce on the distributed computing platform.

An assout on a network that floods it will so many requests that regular traffic is either solved or completely interrupted. Hackers use distributed DDOS attack & leaves hundreds and thousands of bots to overwhelm in terms of bandwidth & reduce the services that are rendering to the user.

Keywords

HADOOP, DDOS,

1. INTRODUCTION

Now a day's large organization that depends on the internet for their business which provides services such as online gaming, e-commerce & financial services etc. Where such organizations requires response and internet connectivity to serve customer request

As these services are completely depend on internet and internet are always prone to failure may be accenditial or intentional where success in the attack are DOS and DDOS.As the whole request and response due to the popularity of organization the traffic on the network increases. The traffic on the network can be made by legitimate user or it may be from the attacker so as to stop the use of resources and slow down the network.

Once such type of attack is DOS attack .A Dos is an attempt to make machine or network resources unavailable to its intended user, resources like bandwidth, memory, computing power etc. DOS Attack is send by one person or single system. DDOS is distributed. DDOS is forwarded version of DOS attack and it is

sent to two or more person which is large scale coordinator of flooding the network with large amount of packet which does victim server unable to handle large no of request so the server becomes slow or sometimes may be crashed whose resources are attacked is knows as primary victim.

Considering DDOS is just like a master slave relation where master is an attacker where it creates zombies with the bot program and act like a slave where zombie does not know they are under an attack and on producing false request. The system whose services are attacked is called as primary victim and zombie is the secondary victim.

This attack can be characterized into two

- Bandwidth flooding and
- Resource flooding

In the bandwidth flooding the hacker flood the network with unwanted request and traffic increases which prevent the user request to reach the server. In the second category the victim resources are engaged by the attacker in order to make resources unavailable.

2. EXISTING SYSTEM

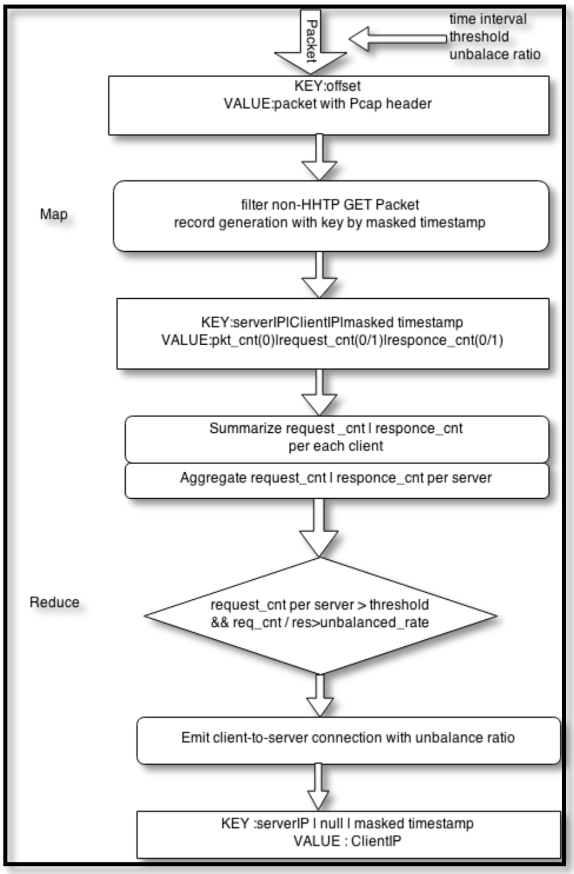
In recent several approaches user proposed ,such as PCA and Sketch based analysis where there disadvantage like in PCA the computing cycles usually requires large amount of computing cycles where as in sketch based study the main focus is on memory utilization ,in which hash tables were used to reduce memory consumption and searching complexity. Still this technique requires sufficient memory and complex completion.

Detecting DDOS attack detection system and characterized into two parts

- Software based system
- Hardware based system.

The hardware based approach implemented by Jinghe Jin and team, the advantage is that, its packet processing speed but problem is high false positive rate. To overcome this high false positive rate and big data traffic software based system we solve problem of high traffic. To overcome the problem of big data in DOS attack Hadoop framework is used. In this paper, counter based algorithm is used to solve the problem of high false positive rate and access pattern method for detecting DOS attack using behaviour of attacker.

3. COUNTER BASED METHOD


Packet
time interval
threshold
unbalace ratio
KEY:offset
VALUE:packet with Pcap header
Map
filter non-HHTP GET Packet
record generation with key by masked timestamp
KEY:serverIPlClientIPlmasked timestamp
VALUE:pkt_cnt(0)lrequest_cnt(0/1)lresponce_cnt(0/1)
Summarize request _cnt l responce_cnt
per each client
Aggregate request_cnt l responce_cnt per server
Reduce
request_cnt per server > threshold
&& req_cnt / res>unbalanced_rate
Emit client-to-server connection with unbalance ratio
KEY :serverIP l null l masked timestamp
VALUE : ClientIP

In counter based Method, It counts the total number of traffic volume or the number of web-pages request.DDos attack with low volume of traffic such as HTTP GET. Map reduce algorithm to detect with DDOS with URL Counting. To lower the false positive rate, we adopted response rate against page request as secondary regulation as well as traffic volume.

As seen in figure this algorithm need three input parameter of time interval, threshold and unbalance ratio, which can be loaded through the distribute cache mechanism of map reduce.

- Time interval limits monitoring duration page request.
- Threshold indicates permitted frequency of the page request to the server against previous normal status, which determine whether the server should be alarm or not.
- The unbalance ration variable denotes the anomaly ratio of response per page request between a specific client and server. This value is used for picking out the attacks from the client.

In map reduce algorithm the map function filters the non HTTP GET packet and generate key value of server IP address, masked time stamp and client IP address.

- The masked time stamp with time interval is used for the specific URL within the same time duration.

The reduce function summarizes the number of URL request, page request and server responses between a client and server. Finally, the algorithm aggregates values per server. When the total request for a specific server exceeds the threshold, the Map Reduce Job emits records whose response ratio, marking them as attackers.

4. ACCESS PATTERN BASED METHOD

To overcome the efficiency of counter based method the output of the counter based method is forwarded to the access pattern based method. In this method it is assume that the server is affected by the same bot program which conducts the same behaviour and the attacker could be differentiated from the normal user. There are two jobs in access pattern method, first is to access sequence and second is to hunt the infected hosts.

In the first job access sequence is obtained of the web page that is requested by the client to the server. This also calculates the spending time and number of bytes required by the each URL.

The second job hunt out infected host by comparing the access sequence by comparing the spending time and the bytes requested by each client that access the same server.

5. PERFORMANCE ANALYSIS

For counter based algorithm, configured a small hadoop tested which consist of one proxy server and 10 slaves nodes. Each node consist of quad core 2.93 GHz Intel i7 CPU ,16 GB memory,1 TB hard disk & 1 Gbps Ethernet Cards, by verifying clusters nodes measuring of DDOS attack is performed .

As the server is running at the backend ie. Http server and soon as the bot program runs it to create large number of false request that can be seen on the server in figure 1 and 2, log records at the server .The ddos attack code is executed in the figure 3 where the actual MapReduce code is executed. It will stop the attacker from sending false request and save the server from crashing as it could be seen in figure 4 error to bot program. As the bot will have error it will stop functioning.

As the first diagram is bot program which is named as sn5.After that database result and the dos attack ,next what error it give to error to the bot program .i.e. try to stop.

6. CONCLUSION

A framework is prepared for determining the abnormal behaviour of the user in order to find the DDOS attack. In this paper we proposed system which consist of implementation counter and access pattern algorithm by using map reduce in hadoop.

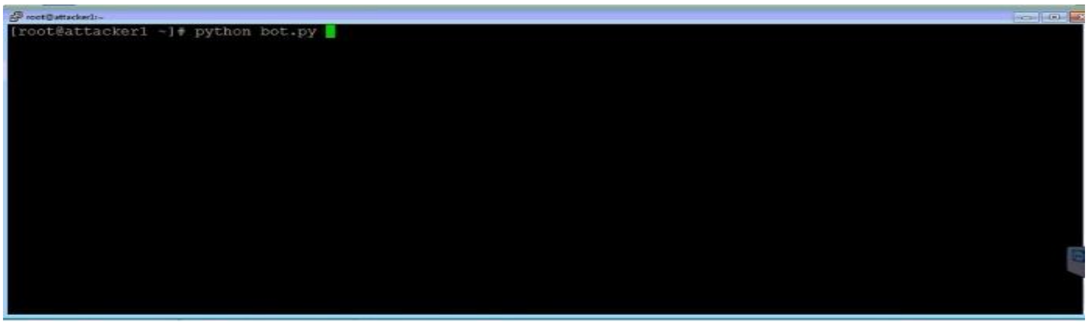
7. REFERENCES

[1] J. Mirkivic and P. Reiher, A Taxonomy of DDoS Attack and DDoS Defense Mechanisms, ACM SIGCOMM CCR, 2004

[2] H. Sun, Y Zhaung, and H. Chao, A Principal Components Analysis-based Robust DDoS Defence System, IEEE ICC, 2008

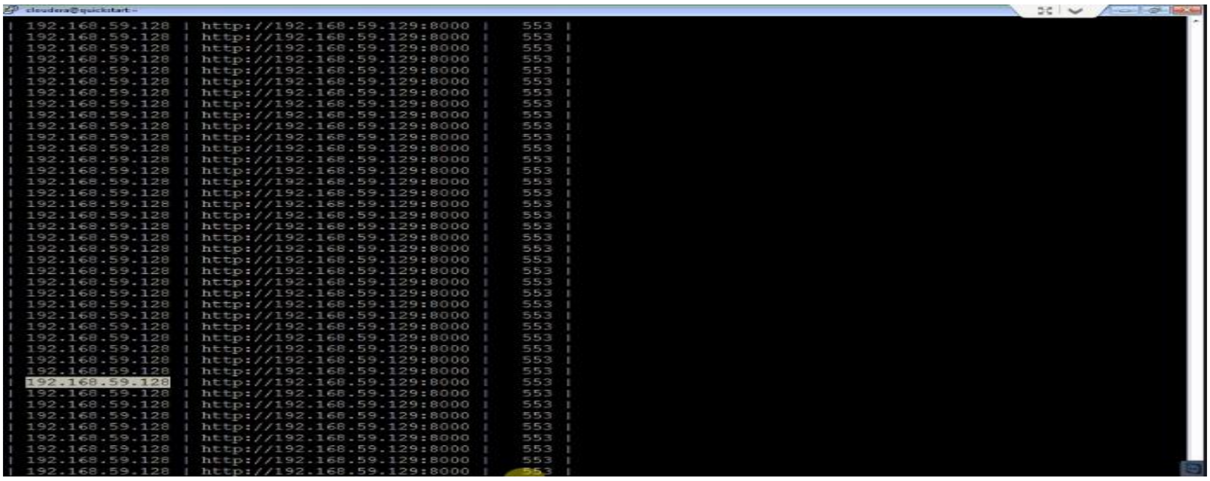
[3] H. Liu, Y Sun, and M. Kim, Fine-Grained DDoS Detection Scheme Based on Bidirectional Count Sketch, IEEE ICCCN, August 2011

[4] Y. Lee, W. Kang, and Y. Lee, A Hadoop-based Packet Trace Processing Tool, TMA, April 2011



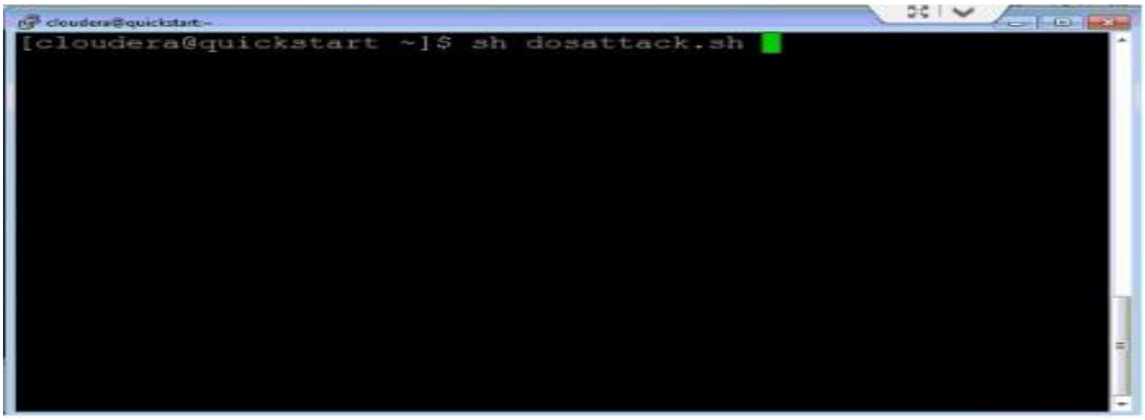
```
[root@attacker1 ~]# python bot.py
```

Figure 1 Execution of BOT program



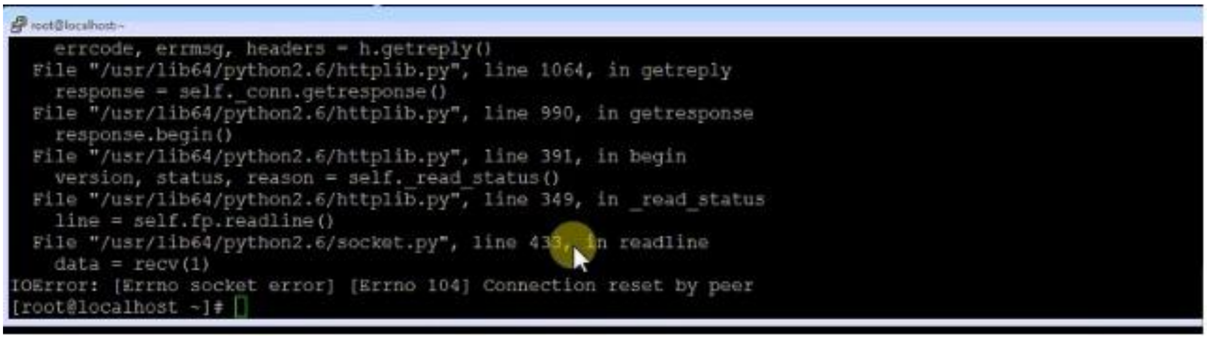
```
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
| 192.168.59.128 | http://192.168.59.129:8000 |    553 |
```

Figure 2 Attack entry on Sever Side



```
[cloudera@quickstart ~]$ sh dosattack.sh
```

Figure 3 Execution of Anti BOT program



```
    errcode, errmsg, headers = h.getreply()
  File "/usr/lib64/python2.6/httplib.py", line 1064, in getreply
    response = self._conn.getresponse()
  File "/usr/lib64/python2.6/httplib.py", line 990, in getresponse
    response.begin()
  File "/usr/lib64/python2.6/httplib.py", line 391, in begin
    version, status, reason = self._read_status()
  File "/usr/lib64/python2.6/httplib.py", line 349, in _read_status
    line = self.fp.readline()
  File "/usr/lib64/python2.6/socket.py", line 433, in readline
    data = recv(1)
IOError: [Errno socket error] [Errno 104] Connection reset by peer
[root@localhost ~]#
```

Figure 4 Automatically termination of BOT program