International Journal of Engineering & Technology, 7 (4.36) (2018) 390-393

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Anomaly Detection in Distributed Denial of Service Attack using Map Reduce Improvised counter-based algorithm in Hadoop

Y.S.Kalai vani[1], Dr.P.Ranjana[2]

[1]Sindhi College, Bangalore,India.
[2]Hindustan Institute of Technology and science,Chennai, India.
**Corresponding author E-mail: kalaiys@rediffmail.com*

Abstract

A Distributed Denial of Service (DDOS) is one of the major threats in the cyber network and it causes the computers flooded with the Users Datagram Packet (UDP).This type of attack crashes the victim with large volume of traffic and the victim is not capable of performing normal communication and crashes it completely. To handle this DDOS attack the normal Intrusion Detection System is not suitable to hold and find the amount of the data in the network. Hadoop is a frame work that allows huge amount of data and it is used to processes the huge amount of data. A Map reduce program comprises of a Map task that performs filtering and sorting and a Reduce task that performs summary operation. The propose work focuses on the detection algorithm based on Map Reduce platform which uses the Improvised counter based (MRICB) algorithm to detect the DDOS flooding attacks. The MRICB algorithm is implemented with Map Reduce functionalities at the stage of verifying the Network IPS. This proposed algorithm also focuses on the UDP flooding attack using anomaly based intrusion detection technique that identifies the kind of packets and the flow of packet in the node is more that the set threshold and also identifies the source code causing UDP Flood attack . Thus it ensures the normal communication with large volume of traffic.

Keywords: *Anomaly detection, Denial of service, Hadoop, Map Reduce.*

1.Introduction

DDOS attack is a distributed, huge scale coordinated attempt of flooding the cyber net with an enormous amount of packets which is difficult for victim network to handle so the victim is unable to provide the services to its users and the network performance is greatly reduced. DDOS has two formats of attacking system. In first approach the malicious (Chaitanya Buragohain, Nov 2015) packets injected with virus, worms as running application and it is called vulnerability attack. In second approach is to weaken the victim's system by exhausting the resources such as input-output bandwidth, database bandwidth, CPU, memory.etc. DDOS attacks are classified into different types such as HTTP flood attack, UDP flood attack, ping of death attack

In this research paper we have taken a type of attack UDP flooding attack which comes under the classification of distributed of denial of service. UDP flooding attack can be detected by a improvised counter based algorithm in Hadoop. Threshold value is set for the UDP Packets, if UDP packets are exceeds the Threshold values then the UDP attack will be detected. In a UDP flood, the attackers send highly-hoaxed UDP(user datagram protocol) packet at a very high packet rate using a large Source IP range. Because of the UDP attack the victims network such as routers, firewalls, severs are exhausted by a large number of incoming UDP packets. This attack normally consumes network resources and available bandwidth, exhausting the network until it goes offline. UDP flooding attacks are very difficult to detect and blocking the network and it block the resources of the victim.

Classificaton Of DDoS Attack

A. Infrastructure attack

Infrastructure attack consists of Network bandwidth, routing equipment and computing resources. In this type of attack the attacker to overwhelm the resource capacity of node in a network by sending a large number of fake requests. Examples for this Infrastructure attacks are TCP/SYN flood (Alkasassbeh, 2016)UDP flood, ICMP Flood etc.

TCP SYN flood:

This attack is caused by an attacker sends a lot of ordinary SYN segments to fill up resources causing a service to be denied for its connections.

UDP flood

In this attack huge amount of UDP packets are sent to random ports on the victims side . Sometimes port are open without knowledge of administrator causing server to respond. A respond to a UDP Packet with an ICMP unreachable reply to the spoofed source IP address[3] makes the situation worse by overwhelming network environment of the victimized IP address.

ICMP flood:

This attack is referred as a Smurf attack or ping of flood, is a ping based Dos attack that ends large numbers of ICMP packets to a server and attempts to crash TCP/IP Server.

B .Application level attack :

This type of attack which attacks the resources of the server by sending the HTTP request through the network. It has two categories which are given below

Common application layer attack:

In this attack the attacker sends the normal request which consumes large amount of server resources or high work load requests across many TCP sessions are sent to the server,so it will cause common application layer attack.

HTTP flood attacks:

Some applications level DDoS are caused by HTTP GET flood . HTTP GET flood attack caused by an attacker who sends the large amount of request in which it consumes a large amount of resources of a server because of HTTP GET packets are flooded and it consumes a resources of a server which server not able to process the requests because of HTTP Flooding attack.

2.Intrusion Detection Approaches:

An Intrusion detection system(IDS) is tool which is used to monitor the network for malicious activities in the network and it detects the attacks from the anomalous packets. Intrusion detection system is classified in to three types are:

Host based Intrusion detection System:

It is an IDS which monitors the internal part of the computer system and monitors the network packets in the network interface.

Hybrid Intrusion detection System:

It is an IDS which monitors the computer's internal activities and network activities.

Network Intrusion Detection System:

It is an IDS that attempts to discover the unauthorized access to a computer network and detect the cyber threats in the network. It is classified into two types

i)Anomaly Detection system.

This type of approach[2] analyses the network activities and looks for an unusual behavior in the network, if an anomaly found in the system then alarm is triggered.

ii)Misuse detection system

This approach is used to detect the known patterns of attacks. If the pattern is matched there Is possibility of an attack that alarm will be triggered. It is used to detect the attacks which are in the variations in known attacks.

To detect DDoS attack in the network sophisticated approach is needed which resolves the problem of finding the attack in huge volume of data. To handle this situation and solve the problem pervious model in DDoS attack is improvised. Hadoop [(Shweta Tripathi1, 2013)is a platform which handles a huge volume of data and it is used to store the data in the form of zetabyte. Existing System not able to solve the problem of finding UDP flooding attack in a efficient manner. In this research paper the Map Reduce Improvised Counter Based algorithm is used to detect the UDP flooding attack.

3.Haddop - Proposed System Framework

Hadoop is a proposed system frame work which handles huge volume of data with efficiency. Traditional approach is not suitable to handle the UDP (Riaz Ahamed, Dec 2017) packets because it can hold very less volume of data. Map Reduce is a programming model in Hadoop which is used to process distributed data. It consists of many cluster of machines in the distributed form. It consists of two phases such as Map phase and Reduce phase. In map phase packets coming from different clusters and it are separated as a UDP Packets. It has the key as <source IP, UDP packets> in the map phase. In Reduce phase the filtered UDP packets are entered based on the Threshold value. These splits are then parallel processed by the mappers. In the Reduce Phase the intermediate results provided by the map phase are summarized and associated records are processed by single reducer.

The data set DARPA which is used for the experiment to detect the UDP flooding attack. The master distributes different sets of data among different mappers and the intermediate results are stored at the Mappers. The master then assigns the task of extracting information regarding the attack data to the reducers.

In Reduce phase has detection algorithm which is used to detect (Alkasassbeh, 2016)[6] the UDP Flooding attack based on the threshold value. If UDP packets are exceeding the Threshold value then the attack will be detected in the network and stores the IP address of the attackers also.

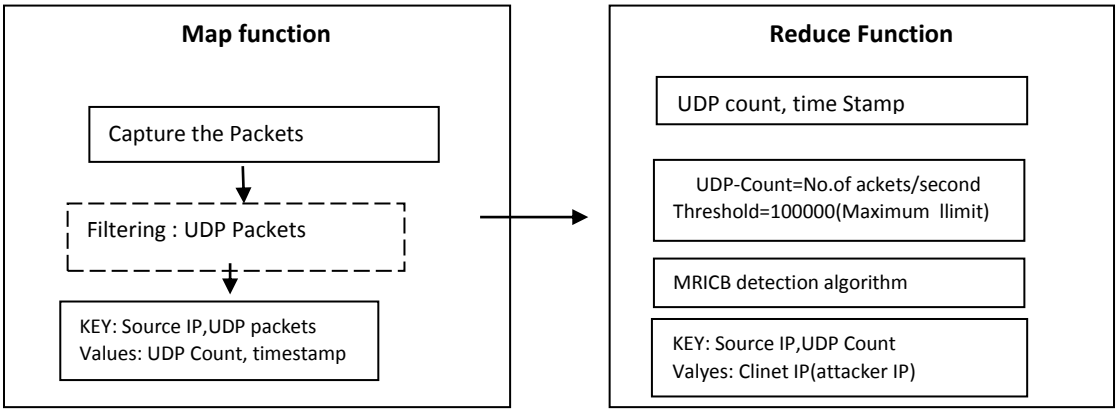


Fig: 3.1 Map Reduce function to detect UDP Flood attack

4.Implementation

The following algorithm which is improvised by Map Reduce in Hadoop. Hadoop is a platform which accepts huge number of data from the node and this algorithm is used to detect the unusual behavior of the packet in the network. We set the Hadoop [7]environment which has Map (Shweta Tripathi1, 2013) Reduce programming model which has two stages. In first stage this algorithm which separates the UDP packets from the network. In second stage this algorithm detects the UDP flood attack which contains Threshold value as 1000000 for UDP packets and if the UDP exceeds the Threshold value then UDP flood is detected along with the source IP address.

4.2. Algorithm to Detect UDP Flood Attack(MRCIB)

STEP 1: Start[map function]
STEP 2: Identify nodes in network.
STEP 3: If nodes in range(belongs to the same network)
STEP 4: Set THRESHOLD=1000000
THRESHOLD=UDP-PACKETS/SECOND
MINIMUM=500
MAXIMUM=1000000
DEFAULT=10000
STEP 5: CAPTURE packets.
STEP 6: If packet not of standard type[Reduce function]

Notify Malformed_ packet.
STEP 7: Identify UDP_PACKET.
STEP 8: If UDP_PACKET > THRESHOLD
Notify UDP_FLOOD_ATTACK
STEP 9: Stop

4.1. Algorithm implementation in Java

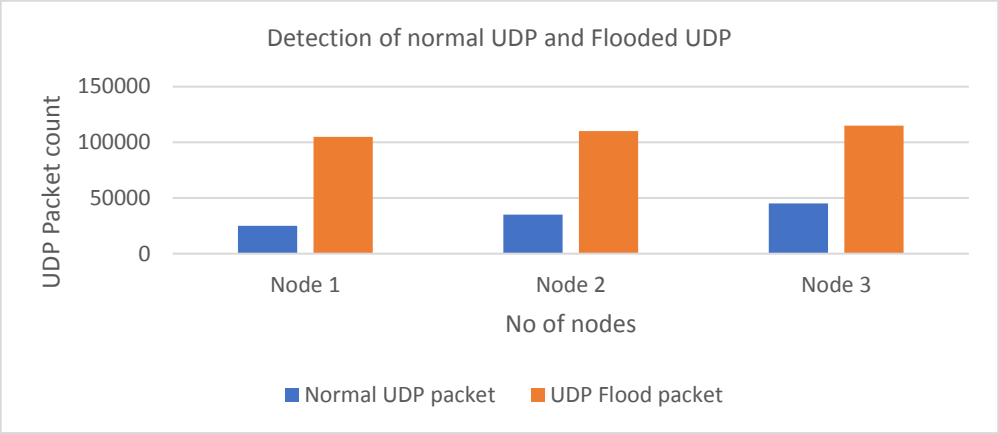
The MRICB algorithm is implemented in java. Hadoop is Java based platform which needs to face the challenges like efficiency, accuracy, security. Since Java meets all the challenges because of its enhanced features. Java has a set of packages which will solve all requirements from the user side. The package Remote method invocation is used to make the establishment between the nodes in the network. There are different types of nodes are available in the network which want to communicate with server. It has the interface which has the method detection which has the implementation part of UDP (S.Navale, 2012)]flood detection. It accepts the inputs as UDP packet from the port 80 and checks the condition that it should not exceed the threshold 100000 as the maximum. If it exceeds the exception will throw as UDP Flood attack detection.

Code for MRICB algorithm in java

```
import java.rmi.*;
public interface DDOSservice extends Remote
{
//Interface of RMI service that will actually attack on a target machine
public String attackdetection()
{
 throw RemoteException;
}
}

Server program
Public class DDOSServer extends UniCastRemoteObject implmenets Runnable DDOSservice
{
   Final String Target = “xyz”;
 Static DDOSServiceServer_instance;
Public DDOSServiceServer() throws RemoteException
{

super();
}

Public void run()
{
//fix the Threshold value as 100000

/if it exceeds the Threshold identify the UDP flood exception
//Accepting the packets from the client
 For(int UDP=0;UDP<=1000000;i++)
{
try{
   Socket net = new Socket(Target,80);
sendRawLine(“GET/HTTP/1.1”,net);
sendRawline(“Host:”+Target,net);
System.out.println(“Attacking the”+Target”+” with connection”+UDP);
}catch(Exception e)
{
System.out.println(“UDP flood attack);
}
}
```

5.Results

Results of the MRICB(Map Reduce Improvised Counter Based) algorithmhas as a graph which consists of two ranges of UDP packet such less than the Threshold value and more than the Threshold value. If it exceeds the threshold value UDP flood is detected other wise the nodes will communicate normally. The map and reduce function has the methodology which has the two phases of separating the UDP (Hadoop Distributed File System, 2013) packets and testing the threshold value.



6.Conclusion & Future work

This paper proposed a Hadoop based robust and efficient DDoS Detection model which has the mechanism to detect the UDP flooding attack by measuring the Threshold values for the nodes. MRICB algorithm implementation values are plotted in the graph shows the difference between normal UDP packet and flooded UDP. For the future work we plan to optimize the Map Reduce jobs, to enhance the model high end speed links and to enhance pattern matching algorithm for detecting the packets.

References

[1] Chaitanya Buragohain, M. J. (Nov 2015). Anomaly based DDoS Attack Detection . *International journal of computer Applications* , 0975-8887.

[2] *Hadoop*. (2011, june). Retrieved from www.wiki/apache.org/hadoop.

[3] *Hadoop Distributed File System*. (2013, june). Retrieved from httP://hadoop.apache.org.

[4] Riaz Ahamed, H. G. (Dec 2017). Studey on Analysis of Hadoop Based Metwork Intrusion Detection System. *International Journal of Engineering Science Invention* , 01-04.

[5] S.Navale. (2012). Detecting And Analyzing Ddos Attack Using Map Reduce In Hadoop ., (pp. 1,2,3,4).

[6] Shewetha tripathi, B. A. (2013). "Hadoop Baed defence solution to handle distributed network system. *journal of information Security* , 4,150-164.

[7] Shweta Tripathi1, B. G. (2013). Hadoop Based Defense Solution to Handle Distributed. *Journal of Information Security, 2013, 4, 150-164* , 4,150-164.

[8] Hadoop Wiki", June 2011, [online] Available: wiki.apache.org/hadoop.

[9] Hadoop Distributed File System. http://hadoop.apache.org/ common/docs/current/hdfs design.html.