Threshold based detection and prevention mechanism for DDos TCP flood attack in heterogeneous setup

PRASANNA V BALAJI
BENIEL DENNYSON
SRM UNIVERSITY

Abstract

Because of exponential growth of the users using Internet applications, providing services to them is prominent requirement of internet. The node providing service to them is to be available anytime and anywhere. But the denial-of-service attacker attempts to exhaust the victim's resources such as bandwidth, processing capacity, storage etc by sending huge unwanted traffic to victim node. By doing so, the attacker makes the victim node to prevent the legitimate nodes from accessing the resources or degrade the services provided by victim node. Hence the network/servers become greater risk. A distributed denial-of-service attack is a large scale attack which launches the many DoS attacks directly or indirectly in the distributed manner. The DDoS attack takes large number of compromised nodes in a network to flood the victim nodes simultaneously from multiple places. This kind of attacks is unpredictable and leads to deadly consequences. Therefore in this paper, we explore the scope of the DDoS TCP Flood attack and the possible ways of prevention of the attacks. We propose a prevention mechanism against the DDoS TCP Flood attack that uses a threshold based attack detection and prevention mechanism. The proposed mechanism is set on a virtual machine of a victim node ie server so that the service requests generated by the attackers are not allowed to the server. The experimental results show that the proposed mechanism performs well as compared with other mechanisms.

Introduction

The drastic growth and success of internet changes the life style of human by the way of getting various services such as banking, transportation, medicine, education etc through internet. Therefore the service providers are able to give service to all, anytime and anywhere. It is accomplished by providing adequate resources such bandwidth, processing capacity, storage etc to the service provider. Therefore the providing high degree of availability of such resource to users is very critical in the internet. Besides it, the attacker also attempts to exhaust the service provider's resource which leads to degrade the availability of resources and services. The attack which exhausts the resources of victims by sending flood of requests/messages, resulting denial of service by the service provider to its legitimate users is called denial-of-service attack (DoS). Syn-flood, teardrop, smurf, ping-of-death, finger bomb, black hole, octopus, snork and ARP cache poisoning are some examples of DoS attack.

On the other hand, Distributed denial-of-service attack (DDoS) uses multiple malicious nodes distributed globally that generate more HTTP traffic to overwhelm victim resources. It is very difficult to distinguish the attack HTTP traffic from normal traffic [17]. To defend against DDoS attack, traffic control mechanism such as ingress filtering, route-based packet filtering and rate limiter are used. Ingress filtering and packet filtering mechanism detect the packets with spoofed source IP addresses and drop them. But the effectiveness of these mechanisms depends on global deployment of filtering in the internet which is difficult. Rate limiter controls the traffic in the link of victim when it is overwhelmed by the attacker by sending the unwanted traffic. It is suitable for the attacks having high data rate on a link but not suitable for the attacks with low data rate [5]. The rate limiting techniques are very simple and easy to understand also but it is hard to set up proper threshold values for detecting the attacks [15].

In this paper, we propose a threshold based DDoS detection and prevention mechanism which uses a virtual machine set on the victim node. The virtual machine allows only the service requests from the legitimate nodes to the server and other requests are not allowed to the server. Therefore the severity due to the DDoS attack is reduced. When the number of service requests generated by a node exceeds the threshold, then the IP address of the node is assumed as suspicious attacker and marked as blacklist node for a limited period and the service requests from blacklist node are not allowed to the victim.

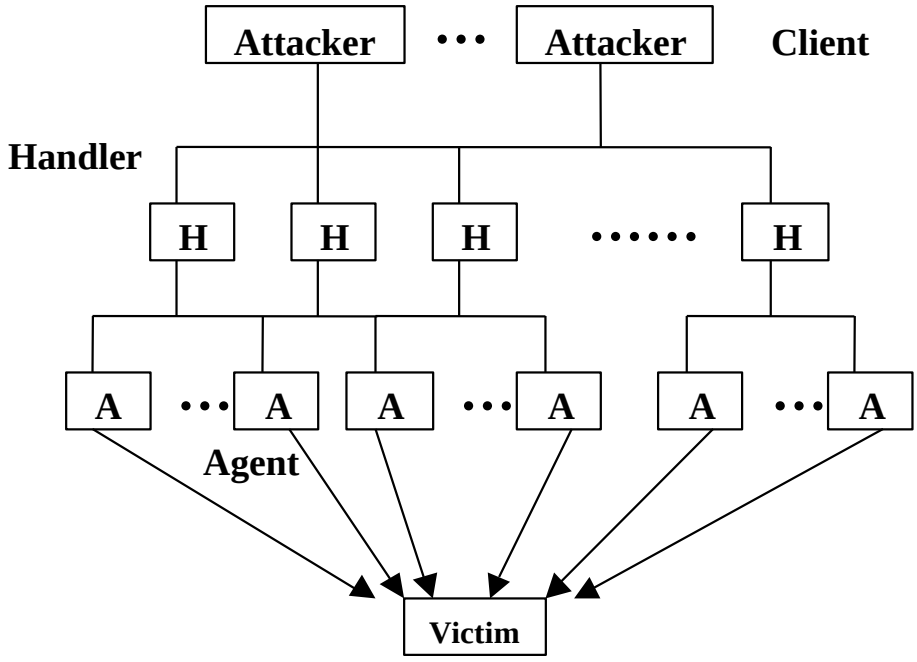


Figure 1 overview of the DDos Attack.

Overview of proposed system

The overview of the proposed mechanism is shown in Fig.2. A virtual node is created on a server to prevent the DDoS attack. Any interactions with the server have to pass through virtual node. The attack detection mechanism is plugged in the virtual node to detect the incoming DDoS attack depending upon the threshold limit allotted to each user. In this paper we consider three different way of spamming the service requests that are,

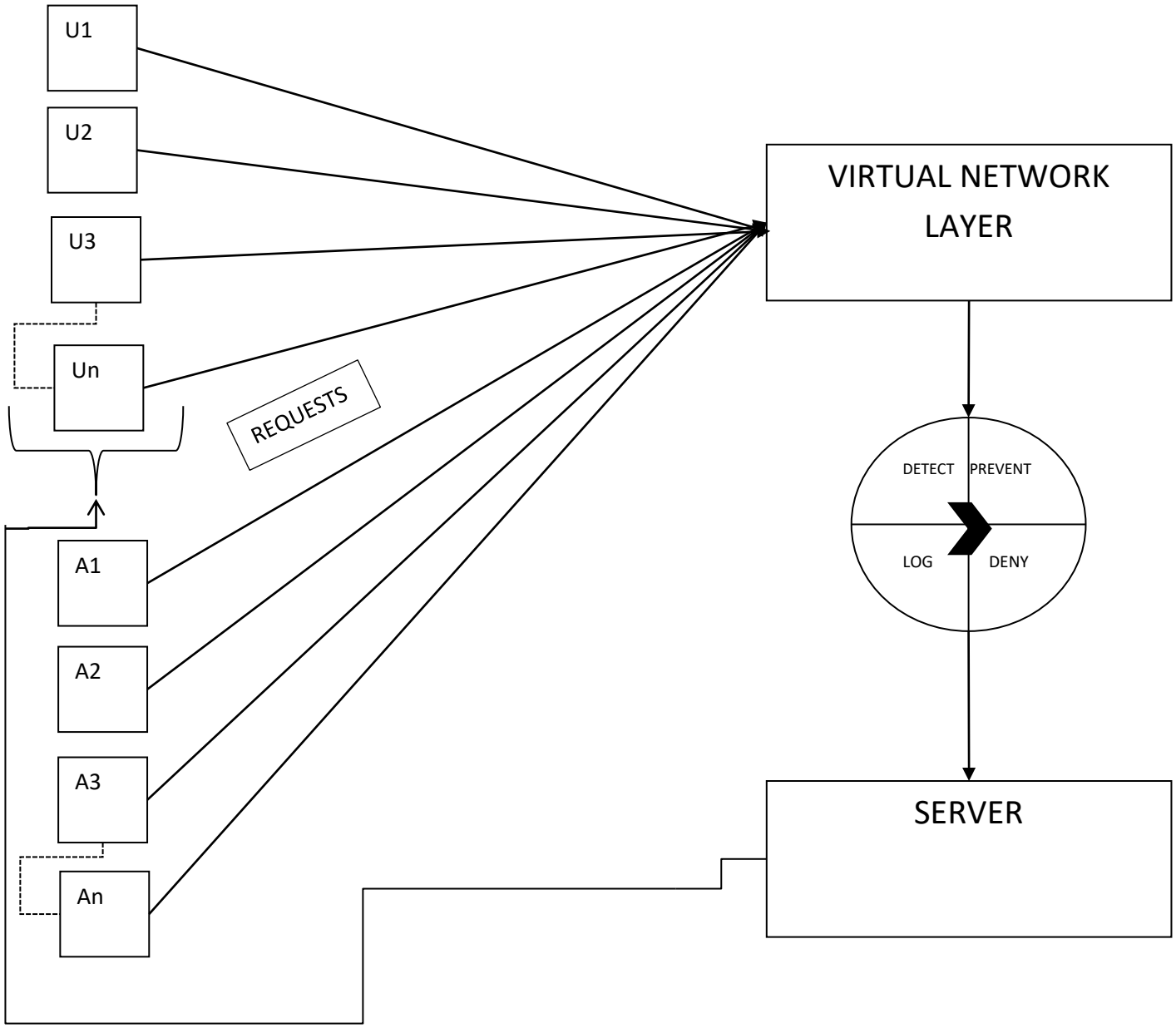


Figure 2 overview of the proposed system.

1) Attacker uses its own bots/machines to spam service requests

2) Attacker uses a fake IP addresses generated by multiple bots to spam the service requests

3) Attacker steals the IP address of a legitimate user to spam the service requests. Similar to detection mechanism, the prevention mechanism is also integrated with the virtual node.

The prevention mechanism cuts the connection between the virtual node and server to prevent any data being stolen or lost or any resource being exhausted. The connection is temporarily terminated and the connection is refreshed after a time period. Even the connection is refreshed after a time period, the IP address is marked in blacklist node.

RELATED WORK

Flood Attacks:

In a DDoS flood attack the victim is flooded the with IP traffic by the attacker [16]. A huge volume of packets sent by the Attacker to the victim system slows it down, crashes the system or saturates the network bandwidth which prevents any legitimate users from accessing the victim's network or system.

UDP Flood Attacks:

User Datagram Protocol (UDP) is a connectionless protocol. When data packets are sent via UDP, there is no handshaking required between sender and receiver, and the receiving system will just receive packets it must process. Sending A large number of UDP packets to a particular system will saturate the network which eventually depletes the bandwidth available for legitimate service requests to the victim network/system [10].

In a DDoS UDP Flood attack, the UDP packets are sent to either random or specified ports on the victim system. UDP flood attacks are designed to attack random victim ports. This causes the victim system to process the incoming data to try to determine which applications have requested data. If the victim system is not running any applications on the targeted port, then the victim system will send out an ICMP packet to the sending system indicating a "destination port unreachable" message.

There are several other DDos Attacks which shuts down an entire network, such as

1. Smurf Attacks
2. Fraggle Attacks
3. Protocol Exploit Attacks
4. TCP SYN AttacksPUSH + ACK Attacks
5. Malformed Packet Attacks

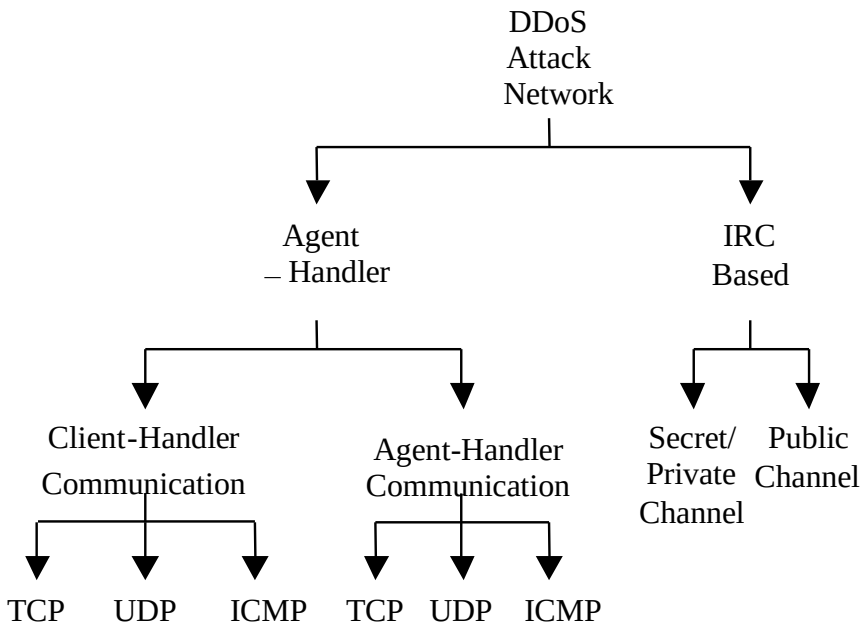


Figure 3 Different types of DDos Attacks.

DDoS countermeasures:

There are a lot of proposed ideas and partial solutions available for mitigating the effects of a DDoS attack. Many of those solutions and ideas assist in preventing only limited aspects of a DDoS attack. However, there is no comprehensive solution to protect against all known forms of DDoS attacks. Also, many derivative DDoS attacks are constantly being developed by attackers to bypass every new countermeasure employed until today. More research is needed to develop more effective and encompassing countermeasures and solutions.

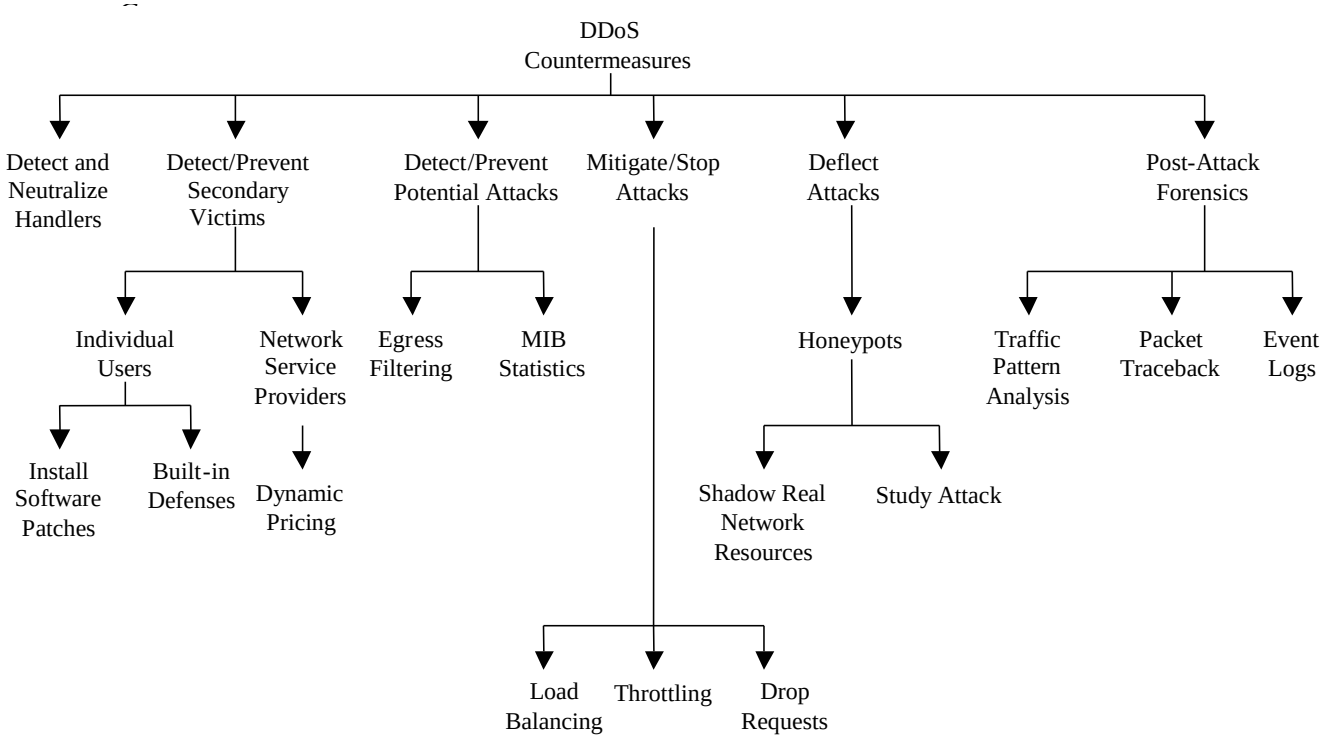


Figure 4 DDos Countermeasures.

Honeypots:

Honeypots are systems that are set up with limited security to be an enticement for an attacker so that the attacker will attack the Honeypot and not the actual system. Honeypots typically have values both in deflecting attacks from hitting the systems they are protecting and serving as a means for gaining information about attackers by storing a record of their activity and learning the types of attacks and software tools used by the attacker. A number of current researches discuss the use of honeypots that mimic all aspects of a legitimate network, in order to attract potential DDoS attackers. This prevents a lot of legitimate systems from getting compromised and allows the honeypot owner to track the handler or agent behavior and better understand how to defend against future DDoS installation attacks [8].

Applying a genetic algorithm to find the feature set of each attack, there has been a solution proposed y the SOM for the classification problem. An optimal solution could only be assured with a brute force approach and a significant time commitment (applying soft computing technique to intrusion detection).The distributed nature of DDos attacks make them extremely difficult to combat or trace back, Attackers normally use three methods to spam service requests which are as follows; Spoof (fake IP), Bots to generate service requests, Morph a legitimate users IP address to spam service requests. Various classifications of DDos attacks have been proposed in literature over the past decade. In this paper, we mainly focus on DDos flood attacks as one of the most common forms and provide a solution to the existing drawbacks.

SYSTEM MODEL

TO BE ADDED

PROPOSED SYSTEM

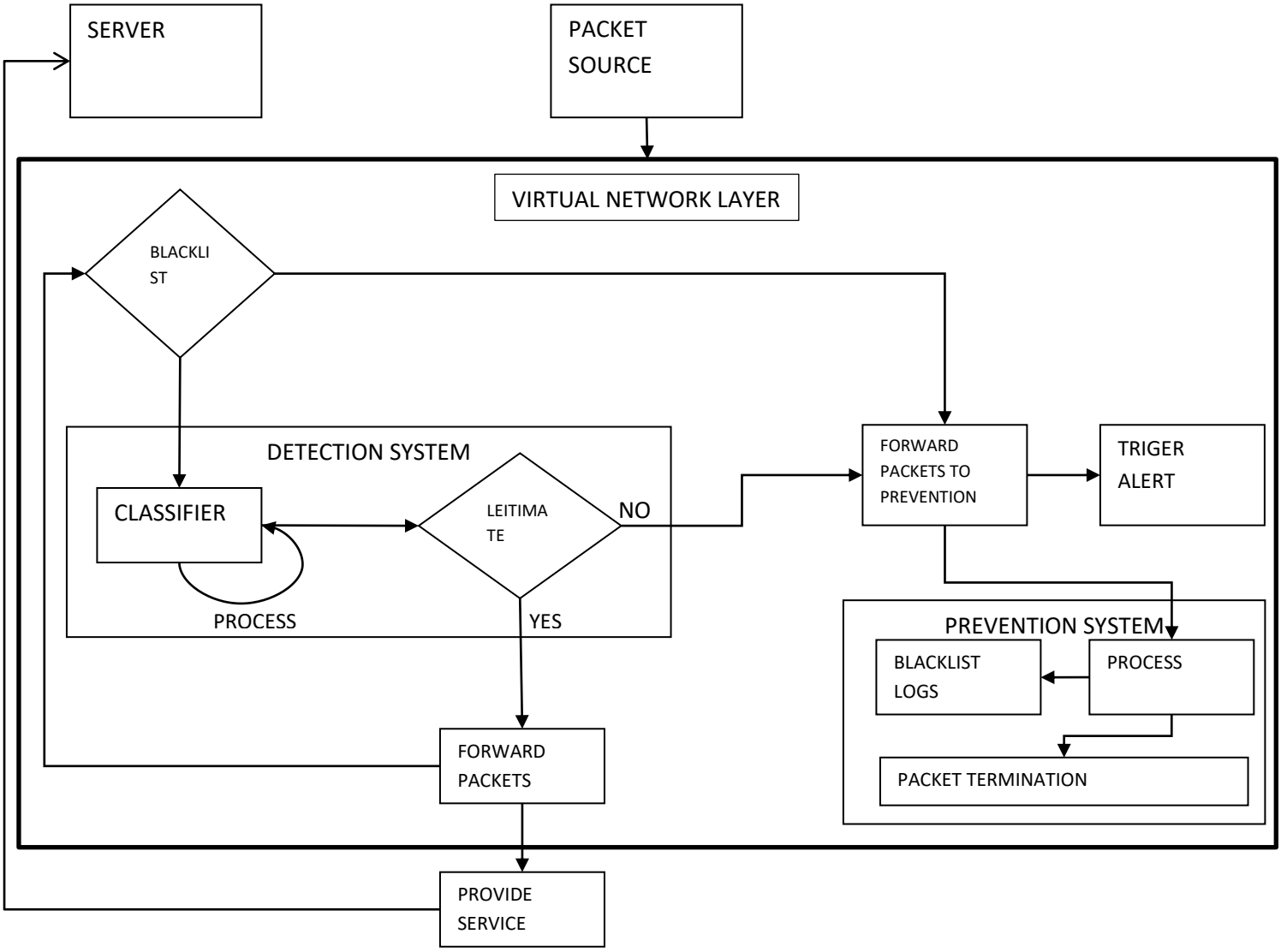


Figure 5 PROPOSED DETECTION & PREENTION SYSTEM

The above diagram shows the architecture of the proposed system in which detection and the prevention process are included. The major process of the proposed system is Detection, Prevention and Recovery phase.

In the phase, we propose a system which could help prevent the damage caused by the DDos TCP FLOOD attacks. Considering all possible scenarios of an attacker that would attempt an attack on a particular server, we put forth our solution.

THEORY :

Considering all different cases, we have come up with a solution.

1. We don't know in whick of these three cases the attacker spams the service requests from .
2. We simply cannot ignore an IP address that beongs to legitimate user.
3. We cannot affort our network being attacked.
4. Banning an IP address that belong to a legitimate user for a limited time would not be a noticable issue.

STEP 1 :

Create a virtual network layer.

Hear we are creating a virtual network layer that would eventually act as a decoy to prevent the DDos attacks.

Any interactions with the real system will have to pass through the virtual layer, which would give us an instinct when the actual system would come under attack.

STEP 2 :

Intergrate a DDos Detection mechanism with the virtual network.

In this stage, we plug in a Detection mechanism in the virtual network the was created. This part of the network is responsible to detect the incoming attacks depending upon the threshold limit alloted to each user. This would further allow the system to take preventive measures.

STEP 3 :

Taking a preventive measure against the DDos attacks.

Once the attack have been detected by the virtual network, immediately the preventive measures are toggled by the system. There are more than one way in which this could work since there are 3 different cases that an attacker might spam requests.

The three different cases are explained earlier, however a quick recap on them would be as follows.

1. Attacker uses his own bots/machines to spam service requests
2. The attacker uses a fake IP addresses, generated by multiple bots to spam service requests.
3. Attackre steals a legitimate users addressto spam service requests.

Similar to the detection mechanism, this is also intergrated with the virtual network.Since we would not be able to predict on which one of the above mentioned cases the attacker would initiate, we would block any requests that exceeds a threshold limits.

Considering the possiblity that the attacker uses a legitimate users IP address, it would be impossible to block a address permanently. This leads us to set a ban time on a pirticular set of IP addresses, later sending an notification that such suspecious activity was found from their respective IP addresses.

This would enable the user to tighten their security and possible give a good insight on the attacker of further invistigation was processed.

STEP 4 :

On this point, the connection between the virtual network and the Actual netowrk is cut preventing any data being stolen or data loss.

However, this is a case that is highly unlikely to happen and in case this happens the priority of keeping the data safe than that of running the service without an interruption comes first.

Here, we realise that there might be cases that the attack is going out of hands and the prevention mechanish set in the virtual network can no longer with hold the pressure.

Thus the connection between the virtual and the Actual network would eventually be cut until the virtual network is refreshed.

Advantages :

1) Prevention of the DDos
2) Usage of a Virtual network
3) Preventing premanent ban on an address
4) Log of data for further invistigation
5) Preventing Data loss or steal.

Disadvantages :

1) Short time ban on legitimate user
2) Sometimes, the system have to be taken down offline from the virtual network.

The major disadvantage would be that the legitimate user incase bets a ban time out, will not be able to use the service ustil the ban have been lifted. But considering the priority of any large

serviec provider its okay to ben an user if found suspesious and later making up to it justifying the reason for ban.

Detection phase:

During the detection phase, the detection sub-system collects the incoming packets within a time frame, for example 60 seconds. The collected packets are subjected to a blacklist check to test whether their sources are blacklisted as attackers of the cloud system. If the packet source is listed in the attacker blacklist, the detection system will send the packets directly to the prevention sub-system without further processing. If the packet source is not blacklisted, the incoming packet will be passed to the classier to decide whether the packets are normal (originating from a client) or abnormal (originating from an attacker). A packet is considered to be an attacking one if the source requests connections to the same destination more frequently than an assumed threshold. The threshold can be manually adjusted by the system administrator to cater for the varying requirements of a particular network. If a packet is considered to be normal, the detection system will send it to its destination (the cloud service provider). Otherwise, the detection sub-system will send the packet to the prevention sub-system.

Algorithm used to detect and remove duplicate requests:

1. Store N records in a temporary file. N is determined based on the number of attacks detected in the previous stage if any.
2. Start Stage 1 at victim server or it can be placed at edge router. Generate Qualifiers $Q=\{Q_1,Q_2\}$ for each flow identified based on Source IP address and Destination IP address.
3. Use Qualifiers to qualify as suspicious records for those records which satisfy the Qualifier Condition QC where [p (1/H)].
4. Calculate feature components $fc_1,\ldots..,\ fc_n$ where n=12 of suspicious flows .
5. Generate Feature Vector $FV=\{fc_1,fc_2,\ldots\ldots\ldots fc_n\}$ for each suspicious flow.
6. Calculate the similarity measure E using Normalized Absolute Distance between the GAV and FV using Eqn(1):

   $$E=[(GAV)-(FV)]/FV$$

7. If E > T_GAV, then it is an Attack. Else it is not an attack
8. If E > T_GAV, then determine the similarity measure S between FV and different attack signatures $A_1,\ldots..A_n$ stored in DCAP using formula in Eqn (2):

$S = [(A_n)-(FV)]/ FV$

9. If Sn of FV matches Threshold T_S partially or completely, then the attacker is A_n.
10. Else FV is a new pattern of DDoS attacker from a new attacker.
11. Hence identify FV as A_{n+1} and store it in updated DCAP.
12. Remove the duplicate requests from attackers and drop any other incoming requests from that ip address.
13. Next, use the source IP address from the above generated feature vector After second attempt of DDoS attack from the same source IP address, then block that particular address. It can be used to determine its binder detection used to identify its previous history of attacks, if any.
14. Request for a Virus Scan.
15. Follow step 6 again.

Prevention phase:

When the packets reach the prevention system, they are considered to be attacking packets by the detection sub-system. The prevention subsystem alerts the system administrator of the attacks. Then, the prevention sub-system will add the attacking source address to the attacker blacklist used by the detection sub-system, if it is not already on the list. Finally, the attacking packet will be dropped. By the detection sub-system, if it is not already on the list. Finally, the attacking packet will be dropped.

The following Algorithm is used for further purpose:

- **1:LOAD DATA**
- **2: FOR I=1: N**
- **3: P=DATA (I, 2)**
- **4: P2=(I, 1)**
- **5: FOR J=1: N**
- **6: N=fiND (DATA (J, 1)==P2) & (DATA (J, 2)==P) 7: IF N>=K**
- **8: NEW_DATA (I, 1)=DATA (I, 1)**
- **9: NEW_DATA (I, 2)=−1**
- **10: ELSE**

- **11: NEW_DATA (I, 1)=DATA (I, 1)**
- **12: NEW_DATA (I, 2)=1**
- **13: END**

Where:

N is the number of packets

P is the destination IP address

P2 is the source IP address

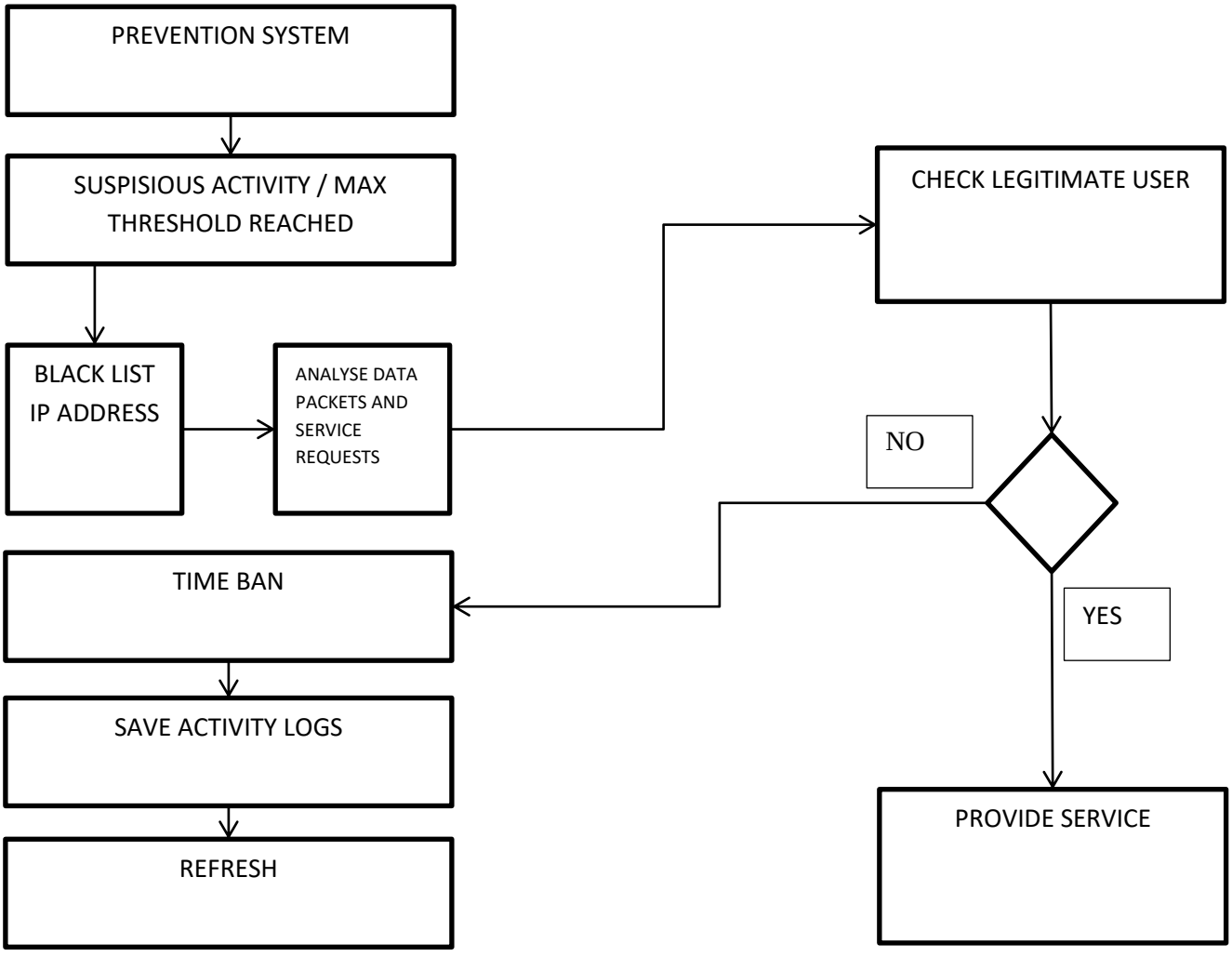
N is the number of packets from the same source to the same destination within 60 seconds

K is the threshold for a packet to be considered an attacking packet

1 indicates abnormal packets (blacklist array)

1 indicates normal packets

New data () is a new entry list with tag ``1" or `` 1'.

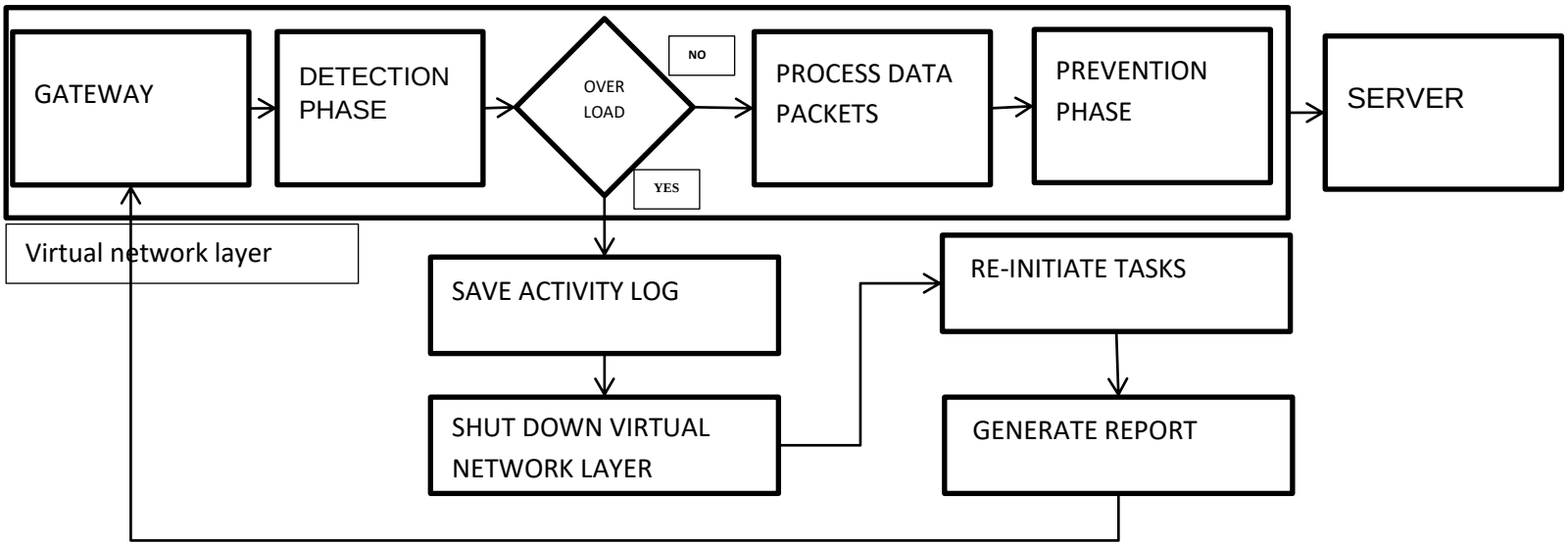


Recovery phase:

The connection between the virtual network and the Actual netowrk is terminated preventing any data being stolen or data loss, which also prevents any damage to the hardware caused by the Attack.However, this is a case that is highly unlikely to happen and in case this happens the priority of keeping the data safe than that of running the service without an interruption comes first.

The termination of connection between the server and the virtual layer occurs only when the attack is going out of hands and the prevention mechanish set in the virtual network can no longer with hold the pressure and protect the system.

Thus the connection between the virtual and the Actual network would eventually be cut until the virtual network is refreshed. This would result in a temperory delay in service but the hardware and data are safe and enough time is bought to counter further incoming attacks.



EXPERIMENTAL SETUP

Different DDos Attack generating bots are required either virtually programmed or a physical setup i.e. Raspberry pi that could generate a number of service requests from different IP addresses. Then the Virtual network layer have to be configured which acts as a mediator between the actual server and the data packets. This virtual network layer could be setup using a Linux operating system and various networking tools. An network tool have to be assigned to monitor and log the data files.

Performance analysis

TO BE ADDED.

Conclusion

This paper proposes a mechanism that prevents the DDoS attack and increases the availability of services and resources to the legitimate nodes. Since all the requests generated by the legitimate nodes and the attackers are analyzed by the virtual machine set on the victim node and the only the service requests from the legitimate nodes are allowed to pass to the victim node, the damages caused by DDoS attack is reduced.

References

1. AQEEL SAHI, DAVID LAI, YAN LI AND MOHAMMED, An Efficient DDoS TCP Flood Attack Detection and Prevention System in a Cloud Environment (DIYKH)

2. B. Wang, Y. Zheng, W. Lou, and Y. T. Hou, ``DDoS attack protection in the era of cloud computing and software-de ned networking," Comput. Netw., vol. 81, pp. 308 319, Apr. 2015.

3. (DEFCON, The SHMOO Group, 2011. (http://cctf. shmoo.com/)

4. K. Kendall, A Database of Computer Attacks for the Evaluation of Intrusion Detection Systems, Master's The-sis, MIT, 1999.

5. Kejie Lu, Dapeng Wu, Jieyan Fan, Sinisa Todorovic, Antonio Nucci, "Robust and efficient detection of DDoS attacks for large-scale internet", Computer Networks, Vol. 51 (2007), pp. 5036–5056.

6. LORI L. DELOOZE, Applying soft computing techniques to intrusion detection, Applying soft computing techniques to intrusion detection, University of Colorado at Colorado Springs Colorado Springs, CO, USA ©2005

7. Monowar H. Bhuyan, Dhruba K. Bhattacharyya, and Jugal K. Kalita,Towards generating real life Datasets for network intrusion detection May 9, 2015 (International Journal of Network Security

8. Nathalie Weiler. "Honeypots for Distributed Denial of Service", Enabling Technologies: Infrastructure for Collaborative Enterprises, 2002. WET ICE 2002. Proceedings. Eleventh IEEE International Workshops, 2002. pp. 109-114. 2002.

9. Neeta sharma , Mayank singh , Anuranjan Mirsha, Prevention against DDos attack using triple pass filter 2016 (International Conference on Computing for Sustainable Global Development)

10. Paul J. Criscuolo. "Distributed Denial of Service Trin00, Tribe Flood Network, Tribe Flood Network 2000, And Stacheldraht CIAC-2319". Department of Energy Computer Incident Advisory Capability (CIAC), UCRL-ID-136939, Rev. 1., Lawrence Livermore National Laboratory, February 14, 2000

11. P. E. Ayres, H. Sun, H. J. Chao, and W. C. Lau, ``ALPi: A DDoS defense system for high-speed networks," IEEE J. Sel. Areas Commun., vol. 24, no. 10, pp. 1864 1876, Oct. 2006.

12. Sunny Behal, Krishan Kumar,Trends in Validations of Ddos Research, International Conference on Computational Modeling and Security (CMS 2016)

13. Saman Taghavi Zargar, Member, IEEE, James Joshi, Member, IEEE, and David Tipper, Senior Member, IEEE, A Survey of Defense Mechanisms Against Distributed Denial of Service (Ddos) Flooding attacks.

14. Sang Min Lee a , Dong Seong Kimb,c,∗ , Je Hak Lee a , Jong Sou Park,Detection of Ddos attacks using optimized traffic matrix (science direct 2012)

15. Sang Min Lee, Dong Seong Kimb, Je Hak Lee, Jong Sou Park, "Detection of DDoS attacks using optimized traffic matrix", Computers and Mathematics with Applications, Vol. 63 (2012), pp. 501–510

16. Stephen Specht. Ruby Lee sspecht@princeton.edu rblee@princeton.edu. Department of Electrical Engineering. Taxonomies of Distributed Denial of Service. Networks, Attacks, Tools, and Countermeasures. Princeton Architecture Laboratory for Multimedia and Security. Technical Report CE-L2003-03.

17. V. Jacobson, C. Leres, and S. McCanne, "The tcpdump manual page," Lawrence Berkeley Laboratory, Berkeley, CA, 1989.

18. Wei Zhou, Weijia Jia, Sheng Wen, Yang Xiang, Wanlei Zhou, "Detection and defense of application-layer DDoS attacks in backbone web traffic", Future generation computer system, Vol. 38(2014), pp. 36-46.