ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 19, April 2017

SUPERLATIVE METHOD TO PRECLUDE DDOS ATTACK BY DHCF

Mr.K.Saravanan
Associative Professor
Kings Engineering College
Chennai-602117
Email-kgs.saran@gmail.com

A.Bright Ganth, P.Mari Muthu
UG Students
Computer Science and Engineering
Kings Engineering College
chennai-602117

Abstract— *Distributed Denial-of-Service attack (DDOS) is a major threat for cloud environment. Because cloud environment has a week security. DDOS attack forces cloud network node or computer that reduces, restricts the accessibility of system resources to legitimate user. Attacker flood the non-legitimate service request (or) traffic to overload its resources and cloud network becomes unavailable. Also slowdown the network performance. The impact of DDOS attack provides Loss of goodwill, Disabled Network, Financial Loss, Disabled Organization. DDOS attack are possible through layers example: Network layers, Session layers, Application layers. Some DDOS attack SYN floods, slowloris, phlashing, UDP flood, ICMP flood and etc. The Existing paper used as Confidence Based Filter (CBF) to detect the DDOS attack in cloud environment. CBF is the first module to sniff the packets. This method deployed by two periods, i.e., non-attack period and attack period. Moreover especially, scoring speed is high &small storage size it is less efficient to detect the packets accurately. In this paper, the detection & prevention techniques like Spoofing Prevention Method (SPM) (arbitrary Ip address detecting), Hop Count Filter (uses packet header information), and Distributed packet filtering (uses router packet information) .These methodology are used to detect & cease potential attacks in cloud.*

Keyword- **DDOS attack, Cloud Network, Spoofing prevention method (SPM), Distributed Hop Count Filter (DHCF)**

1. INTRODUCTION

The goal of this project have been the following Our goal of this project is to create a new set of rules during run time. The main intention of my project to prevent DDOS attack from the attacker (hacker). Network Packet Sniffer is a piece of software that monitors all network traffic. So the intruder cannot be able to attack the system with virus. It is an important detection technology and is used as a countermeasure to preserve system availability while processing. It should be more helpful for identification of network anomalous behaviors. Providing unbreakable security against DDOS. Network monitor will discard the spoofed IP my matching the organization standard unique id.so Spoofed IP can be denied by server. Denying &neutralize the botnet connection.

DDOS ATTACK MODES

Different modes through which DDOS attacks are commonly launched was studied by Mirkovic and Reiher (2004). Attacks could be launched manually or in automated way. With the sophisticated set of attack tools springing up, the launching becomes easier and rapid. The attacks are direct attacks when launched from a single source or indirect when launched via some agents or reflector nodes that multiply the attack received and uses differ rent paths to instigate the attack and to hide the identity of the source. Distributed denial of service attack is perpetrated by a collection of nodes called zombies or bots that are compromised by a master node so that the magnitude of the impact is larger. Attackers normally use BotNet using internet relay channel to carry out DDoS attacks because of which the identity of the true attacker becomes harder to trace.

Based on the vulnerability exploited to make the service denial, attacks can be categorized into two basic types namely brute force attacks or semantic attacks. Brute force attacks are activated by simply flooding seemingly legitimate or legitimate requests at high rates or at heavy volume with the intention of consuming the network resources rapidly. On the other hand, semantic attacks exploit vulnerabilities in networks, protocols or operating systems to exhaust the victim resources. Brute force attacks such as DNS request attack, Smurf attack and SYN flooding attack (Eddy 2007) are launched by exploiting the protocol vulnerabilities

Ingress filter makes a check on the incoming packets address to see if it matches with its sub network while egress filter does the same on outgoing packets from its sub network. But both are preventive methods and incentive for deploying them at ISPs is low. Bremler Barr and Levy (2005) proposed a defensive spoof prevention mechanism that can be deployed at the victim end routers. Haining Wang et al (2007) and Jin et al (2003) dealt with IP spoofing near victim servers b Defense y checking Time to Live (TTL) value of packets

Prevention Mechanisms

Mechanism aim at preventing the likelihood of attacks to happen, through scanning and eliminating the vulnerabilities in the entities prone to attacks, which is a cumbersome activity. Another strategy presented by researchers includes source authentication and access control mechanisms to prevent anonymous attackers to peep in. Access control lists (ACL) are designed to filter inbound and outbound traffic from unaccountable sources. Various client authentication mechanisms are found in the literature to eliminate unauthorized users from making requests to the servers, like solving client puzzles (Aura et al 2000).

Patric and Sean (2008) suggested a trusted puzzler to construct puzzles to be solved by clients. Yang et al (2004) introduced a method called stateless Internet flow filter to authenticate clients by capability handshaking with server. Yang et al (2005) introduced a traffic validation architecture using the concept of capabilities that enable destinations to authorize senders, in combination with routers that preferentially forward authorized traffic. The next best strategy is to stop attacks well before they reach the target. The literature contains preventive solutions that address attack prevention in this context and most of the methods mentioned filtering spoofed packets at the source end as the viable solution. Since DoS attackers by and large employ spoofed source address to hide their identity, filtering spoofed traffic may reduce the attack flow into the network.

II.LITERATURE SURVEY

A. Aaqib Iqbal Wani and Janaki Raman, " Identification and Avoidance of DDOS Attack for Secured Data Communication in Cloud" *,IEEE Trans. Inf . forenscis Security,vol. 3,no2, pp.232-245 jun.2012*

We point out that DDOS attacks do possess a security risk for individual cloud customers. DDOS attacks can be prevented.The project propose a dynamic resource allocation mechanism to automatically deal with the available resources of a cloud to diminish DDOS attacks on individual cloud clients .We intend to clone multiple parallel IPS"s to accomplish the task.

Block Diagram for Identification of Attacks

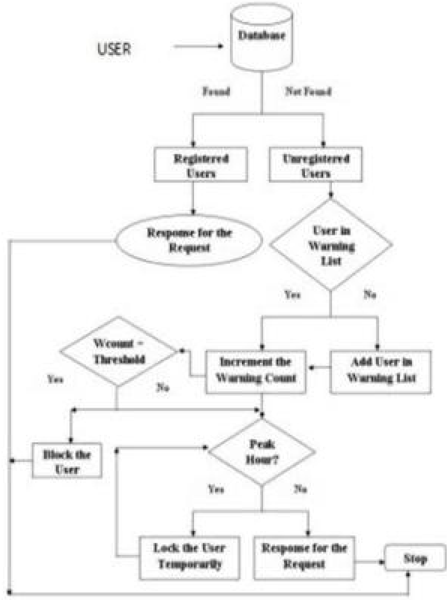


Fig. Identification of attacks under DDoS

B. YiZhang and QiangLiu "Real Time DDOS Attack Detection and Prevention System Based on per-IP Traffic Behavioral Analysis" *proc.IEEE INT.conf.Cloud Security, Nov.2009, pp.685-699*

The DDOS detection algorithm proposed here consists of two parts: Recognition and Decision.When it detects the negative behavior of the suspicious IP record, the alarming counter related to corresponding attack type will be automaticallyaccumulated.After differentiate the attacker, the system will block its traffic and forward the normal user packets. Moreover, our system can quickly filter the attack traffics and forward the normal traffics simultaneously by means of the fast identification technology

C. Waqar Ali and Jun Sang "WINDOWS AUTHENTICATION BASED PACKET CAPTURING SCHEME TO PREVENT DDOS SECURITY ISSUES",*IEEE Trans. Cloud Security*., vol.20,no.9 2546-2562,Sep.2013

Flood attack: Flood attack are well known from DDOs attack.The producer of a flood attack is basic where intruders send traffic beyond a server can manage

Teardrop attack: It is an attack taking advantage of a weak point in the restore of IP packet and potentially confuses the receiving system.

Syn attack: Syn flooding is an attack taking advantage of the three way hand Shaking of TCP, when a hacker is flooding the receiving packet with syn message.

D. Shane marsh and T.Gerves "A CONFIDENCE-BASED FILTERING METHOD FOR DDOS ATTACK DEFENSE IN CLOUD ENVIRONMENT", *seminar security protocol application pp10-25,*apr.2009

Construction of the *nominal profile* is divided into small time intervals, which are called windows.CBF calculates the confidence values of every attribute value pair and stores them in a certain data structure.

III.SYSTEM ANALYSIS

"System analysis is the dissection of a system into its component pieces to study how those component pieces interact and work." System analysis is a survey and planning of the system and project, the study and analysis of the existing business and information system, and the definition of business, requirements and priorities for a new or improved system

EXISTING SYSTEM

As a network administrator who needs to identify, diagnose, and solve network problems while DDOS attack happen its more crucial for company.It is difficult to identify the DDOS attack, if the network traffic is not tracked, it give big trouble.Confidence-Based Filtering method, named CBF, is investigated for cloud computing environment. This method is deployed by two periods, i.e., non-attack period and attack period. Legitimate packets are collected in the non-attack period, for extracting attribute pairs to generate a nominal profile.to determine whether to discard it or not.

DISADVANTAGES

- CBF has a small storage size
- acceptable filtering accuracy
- generating nominal profile &confidence value takes time

IV. PROPOSED SYSTEM

In this project a network analyzer (as a. packet sniffer), this system make it easy for us to monitor and analyze network traffic. We can quickly identify network bottleneck and detect network abnormities like (DDOS, worm, XSS, cross side scripting) we can monitor network traffic information of each node, both local and remote. We are enhance the hop count filter as Distributed Hop Count Filter to preclude attack by its parameter.DHCF can accomplish two tasks namely, protecting servers and dredging network bandwidth simultaneously. We originating the traced to its true source.by using ip matching to detect spoofed ip(arbitrary ip).We can easily find out which host is generating or has generated the largest traffic (request).

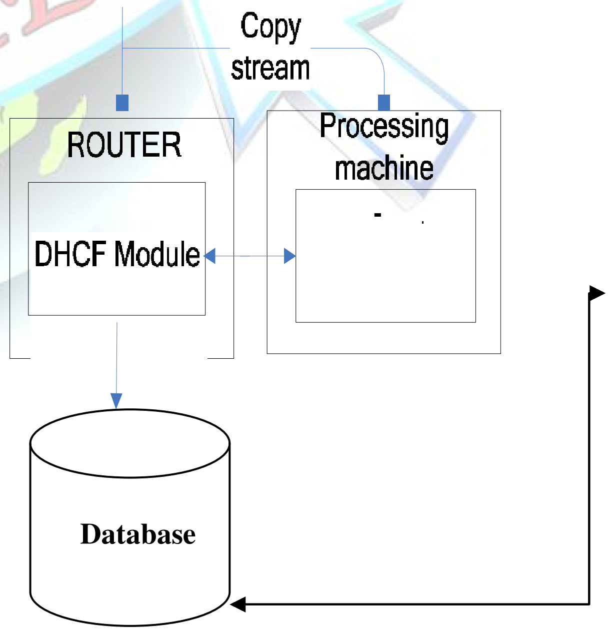


Fig3.1.1 scenario of confidence based filtering

Technology used

- DHCP(Computing Hop)
- Ip Filter(Spoofed in detection

Advantage

- Effective filtering
- Spoofing can be detected easily
- High Speed computing
- Spoofing Data Service can be protected

V. ARCHITECTURE DIAGRAM

The server can monitor the traffic and capture the packet, router has the hop computation and update in database parallel in user interface monitor, IP filter can reject and allow the packet as legitimate or unauthorized. Server gives permission to access the information.

It provides all the Graphical Interfaces components required by the server to interact with the system. It shows all the incoming packets into the desktop, and upon proper identification and clarification. As a network analyzer (as a. packet sniffer. With this system network traffic monitor feature, we can quickly identify network bottleneck and detect network abnormities traffic.

SERVER INTERFACE MODULE

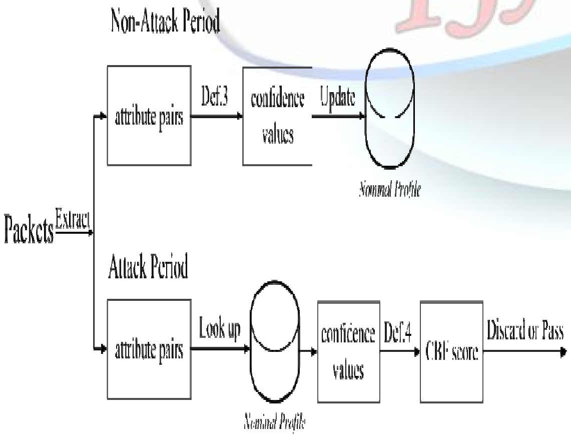


Fig 5.1: DDOS detection

We can monitor network traffic with this network traffic monitor feature to detect abnormal traffic. It allows you to get a clear view of the complex network, conduct packet level analysis.

Network Flow monitoring informs the administrators where their bandwidth is used, the person using it and the reason as to why the person is using it. This is important in that it shows you how the usage may affect you network. If it is potentially harmful then you can take the necessary corrective precautions depending on the nature of the danger. Its configuration involves setting a Network Flow in LAN and creating a new Network Flow for each IP. Packet sniffing is used in a network to capture and record data flow. It allows for discerning every single packet and carrying out analysis on its predefined parameters. It is an addition to regular bandwidth capabilities. [5] proposed a novel scheme for mobile Television services over WiMAX network, called the Wireless Switched Digital Video (WSDV) scheme, is proposed. Compared with the conventional broadcast or unicast schemes, the hybrid approach introduced in the proposed WSDV approach exploits the merits of two conventional schemes and mitigates their demerits, which enables it to increase wireless capacity for mobile Television services.

DHCP COMPUTATION

Distributed Hop-Count Filtering (DHCF) builds an accurate IP02HC (IP to hop-count) mapping table, while using a moderate amount of storage, by clustering address prefixes based on hop-count. To capture hop-count changes under dynamic network conditions, we also devise a "safe" update procedure for the IP2HC mapping table that prevents pollution by HCF aware attackers.

Two running states, *alert* and *action*, within HCF use this mapping to inspect the IP header of each IP packet. Under normal condition, HCF resides in *alert* state, watching for abnormal TTL behaviors without discarding packets.

Besides the IP2HC inspection, several efficient mechanisms are available to detect DDOS attacks. Through analysis using network measurement data, we show that the HCF can recognize close to 90% of spoofed IP packets. Then since our hop count based clustering significantly reduces the percentage of false positive we can discard spoofed IP packets with little collateral damage.

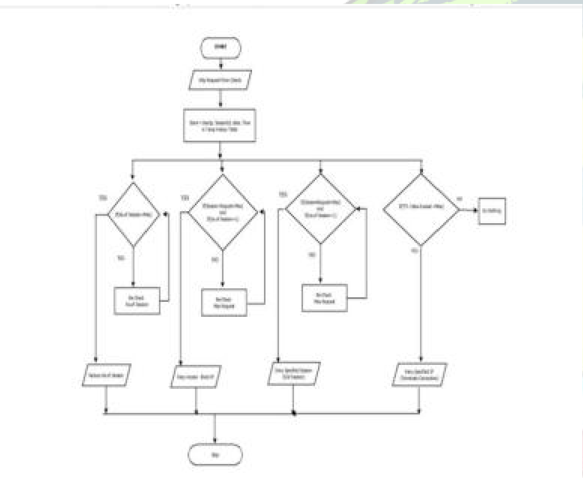
DATABASE

SQLyog is the RDBMS it is the backend

process .it store the information in tables as tubles. Initially the organization IP are stored in the database. The input packets are extracted and header information are stored in db then client ip are matched and give the alert to sever monitor to allow this request as legitimate request if the Ip is spoofed the header information detail are stored in IP then the server screen pop up notification as allow/discard .

SYSTEM MODELLING

A system model is the conceptual model that describes and represents a system. A system comprises multiple views such as planning, requirement, design, implementation, deployment, structure, behavior, input data, and output data views. A system model is required to describe and represent all these multiple views



DDOS DIVIDE-AND-CONQUER ALGORITHM

STEP 1: GET HTTP Request from Clients
STEP 2: PARSE [HTTPHEADER]
STEP 3: STORE database entries details in the list IP Addr, SessionID, Date, Time, S.no -> Temp
Track Table
STEP 4: Use Divide-and-Conquer Search Method (TempTrack, S.no.First, S.no.Last) IP is found
STEP 5: **If Number of Session value is equivalent to Maximum value**
STEP 6: Matched value of step 5 is true then Reduce Number of Session
STEP 7: Matched value of step 5 is false then Recheck Number of Session GOTO ->STEP 8
STEP 8: **If (Number of Session = 1 AND SessionRequest =High)**
STEP 9: Matched value of step 8 is true then Deny Accessibility permissions to IP address
STEP 10: Matched value of step 8 is false Recheck maximum Request GOTO ->STEP 10
STEP 11: **If (Number of Session >1 AND SessionRequest = High)**
STEP 12: Matched value of step 11 is true then End specified session
STEP 13: Matched value of step 11 is false then Recheck maximum request GOTO ->STEP 14 STEP 14: **If (TTL>=MAX)**
STEP 15: Matched value of step 14 is true then the TTL value is exceeded and terminate the connection
STEP 16: Matched value of step 14 is false then do nothing
STEP 17: END

// If the list has 2 or more items
Step 4.1: if (S.no.First < S.no.Last)

// See "Choice of pivot" section below for possible choices

Step 4.2: Choose any pivotIndex such that S.no.First ≤ pivotIndex ≤ S.no.Last
// Get lists of bigger and smaller items and final position of pivot

Step 4.3: pivotNewIndex:=partition(TempTrack, S.no.First, S.no.Last,pivotIndex)

// Recursively sort elements smaller than the pivot

Step 4.4: DDOS(TempTrack, S.no.First, pivotNewIndex - 1)

// Recursively sort elements at least as big as the pivot

Step 4.5: DDOS(TempTrack, pivotNewIndex + 1, S.no.Last)
Step 4.6: function partition(TempTrack, S.no.First, S.no.Last,pivotIndex)
Step 4.7: pivotValue := TempTrack [pivotIndex] Step 4.8:swap TempTrack [pivotIndex] and TempTrack [S.no.Last]

// Move pivot to end

Step 4.9: storeIndex := S.no.First
Step 4.10: for i from S.no.First to S.no.Last - 1 // S.no.First ≤ i < S.no.Last
Step 4.11: if TempTrack[i] < pivotValue
Step 4.12: swap TempTrack[i] and TempTrack[storeIndex]
Step 4.13: storeIndex := storeIndex + 1
Step 4.14: swap TempTrack[storeIndex] and TempTrack [S.no.Last]

```
        // Move pivot to its final place
Step 4.15:  return storeIndex
```

Algorithm Explanation

First step of the algorithm is to get request from the user. In order to detect the intruders, the entry of all users and their activities are maintained as history in the database. The history also contains the information about the users with their corresponding IP address, session id, entry time, date, serial no, and their accessing site. Based on the history, can easily identify all the users accessing the server. Each user entering the internet is assigned a unique IP address. This IP address is also stored in the database along with the users' entry details. The particular user can be identified by this IP address.

This all entry details are stored as history list, if the list is contains n number of items, then implement a technique called DDoS Divide-and-Conquer algorithm. The list has to be partitioned by using D&C Search method and the divided result will be stored in the Temporary track table. By the use of user entry details, check with the number of session value is maximum. If the match returns true value, then reduce number of session. Otherwise, rechecked with maximum number of session. If the details are not matched, then check whether the number of session value is one, which is equivalent to maximum session request value. If the details are matched, then the user is treated as blocked user and the access is denied.

Otherwise, rechecked with maximum session request value. If both the matched result returns false then it is compared with, more than one number of session value is equivalent to the maximum session request value, If this is true end that particular or specified session. Otherwise, the user is rechecked with maximum number of session request. Finally, the initial TTL (Time-To-Live) value is compared with the maximum assigned value. If the matched result is true then terminates the connection and end the process. Otherwise, their request is accepted and the response is provided to the user efficiently. Thus this algorithm provides a better method to block and prevent from the intruders from accessing the web page.

CONCLUSION

The aim of this paper is to study and devise efficient and practical algorithms to tackle the Websites based distributed denial-of-service attacks, and it focuses to identify and prevent the attack carried out by the hackers and block them from using the site and it also provides how best the degradation of the performance can be prevented by using N factor DDoS Divide-and-Conquer algori-thm proposed in the methodology to improve server performance and deny the accessibility permissions to the hackers.

In this work the blocking is done using a different mechanism based on the user categorization. To improve tracing back the attackers on a global scale is always a difficult and tedious task. For increasing the accuracy of finding attackers, it uses categorizat-ion and Divide-and-Conquer method. To invoke this method by monitoring sever load and network traffic when attains maximal value. Hence there will be no traffic congestion for web users to access the web server with minimal storage overhead and it is effective. Thus the proposed algorithm is suitable for satisfying the organizat- ion's requirements. Thus this paper makes an attempt to provide an efficient and well suitable algorithm to identify the attack or threat made by the user on server performance and prevent the server from that kind of attack. In future, this algorithm can be enhanced with proper steps to satisfy large number of requests.

REFERENCES

[1] Dr. K. Kuppusamy and S. Malathi, "An Effective Prevention of Attacks using GI Time Frequency Algorithm under DDoS", IJNSA journal, Vol. 3, No. 6, November 2011, PP.249-257.

[2] WONG, Tsz Yeung., On Tracing Attackers of Distributed Denial-of-Service through Distributed Approaches, Ph.D. thesis, The Chinese University of Hong, September, 2007.

[3] M. Muthuprasanna.,"Distributed divide-and- conquer techniques for effective DDoS attack defense", G. Manimaran Iowa State University Ames.

[4] K. Park and H. Lee. "On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets". In Proc. ACM SIGCOMM, San Diego, CA, August 2001.

[5] Christo Ananth, M. Suresh Chinnathampy, S. Allwin Devaraj, S. Esakki Rajavel, V. Kulandai Selvan, P. Kannan, "CAPACITY BEHAVIOUR USING WSDV SCHEME OVER WIMAX", ABHIYANTRIKI-An International Journal of Engineering & Technology (AIJET), Vol. 1, No. 2,December 2014,pp:18-27

[6] F. Baker, Requirements for IP version 4 routers. RFC 1812, June 1995.

[7] C. Jin, H. Wang, and K. Shin, Hop-count filtering: An Effective Defense Against Spoofed DDoS traffic. In Proceedings of the 10th ACM conference on Computer and Communications Security,October 2003.

[8] Kihong Park, Heejo Lee, "On the Effectiveness of Probabilistic Packet Marking for IP Traceback under Denial of Service Attack", Network Systems Lab, Department of Computer Sciences, Purdue University, West Lafayette.

[9] Junaid Israr, Mouhcine Guennoun, and Hussein T. Mouftah, "Mitigating IP Spoofing by Validating BGP Routes Updates" , IJCSNS, VOL.9 No.5, May 2009, PP 71-76.

[10] Internet Attack Methods and Internet Security Technology, Second Asia International Conference on Modelling & Simulation, 2008.

[11] Cliff C. Zou, Nick Duffield, Don Towsley, Weibo Gong, “Adaptive Defense Against Various Network Attacks “ , University of Massachusetts, AT&T Labs Research, Florham Park, NJ, 2006.

[12] Guangsen Zhang, Decentralized Information Sharing for Detection and Protection against Network Attacks, Ph.D. thesis, january 2006.

[13] Shigeyuki Matsuda, Tatsuya Baba, Akihiro Hayakawa, and Taichi Nakamura, Design and Implementation of Unauthorized Access Tracing System, Proceedings of the 2002 Symposium on Applications and the Internet (SAINT.02), 2002 IEEE.

[14] William Stallings, Network security Essentials Applications and standards, Fourth Edition, Pearson Education.

[15] Larry Rogers, "What Is a Distributed Denial of Service (DDoS) Attack and What Can I Do About It?" February 2004, http://www.cert.org/homeusers/ddos.html

[16] Chirala Lokesh, B. Raveendra Naick, G. Nagalakshmi, “ ETM: a novel Efficient Traceback Method for DDoS Attacks”. International Journal of Computer Science and Management Research , Vol 1. Issue 3, October 2012.