The International Journal Of Engineering And Science (IJES)
|| Volume || 4 || Issue || 5 || Pages || PP.50-56 || 2015 ||
ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805

A Trusted Approach Towards DDos Attack

[1]Soma Sundaram.M, [2]Rameya.J , [3]Prof.Thanuja.R
[1,2,3]*School of Computing, SASTRA University*

ABSTRACT

A computer network plays a major part in the development of any industry. Nowadays, in this fast paced networking world each and every industry depends on internet for their progress. As said above this is the fast paced world, the attack to disable the progress are also fast paced. DDoS (Distributed Denial of Service) is one among them. Though it is one of the many attacks, they temporarily disable a service provided by the company. This paper proposes a series of steps which not only checks the possible attack but also tries its best to thwart them. Instead of going for conventional approach of blocking the excess traffic, the proposed approach will prolong the access to the service. In the mean time checking for the possible attack is done. Thus, not only it thwarts the attacks but also gives them reliable user their access with a little bit of delay, resulting in high reliability.

Keywords - DDoS attack, Defense mechanism, Ant based IP trace-back, IP spoofing,Chi-Square test.

Date of Submission: 27-April-2015 Date of Accepted: 25-May-2015

I. INTRODUCTION

A Distributed Denial of Service (DDoS) attack is a malevolent endeavour to make a server or a system asset occupied to clients, ordinarily by briefly intruding on or suspending the services of a host joined with the Internet. These attacks are sent by two or more individuals, or bots. Casualties of a DDoS attack comprise of both the end targeted system and all systems utilized and controlled by the programmer of the attack. In a DDoS attack, the approaching traffic flooding the causality starts from a wide range of sources – conceivably many thousands or more. This adequately makes it difficult to stop the attack essentially by hindering a solitary IP address; ditionally, it is exceptionally hard to recognize true client activity from attack traffic when spread crosswise over such a variety of source. Starting 2014, the recurrence of perceived DDoS attacks had come to a normal rate of 28 every hour. Our work is particularly centred around identification and counteractive action of DDoS attack in the system. DDoS force massive danger to the networks.

Many methods are being introduced to counter-attack these threats. Attackers constantly break into the security system. And researchers try finding new methods to handle the attacks. Our aim is to modify the existing architecture and to develop a defence mechanism that is trusted and reliable against these unwanted security threats or attacks

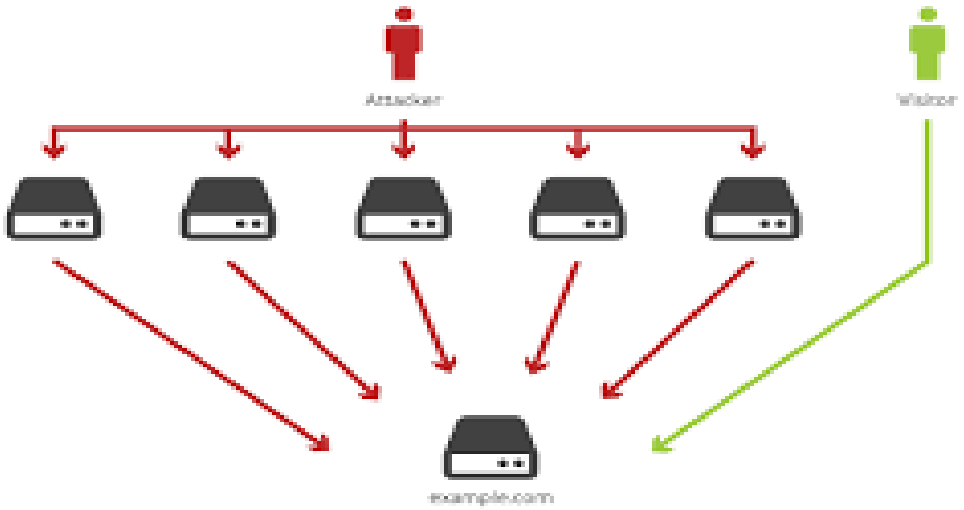

Fig 1.sample DDoS attack

II .LITERATURE SURVEY

DDoS attacks are often accompanied with mislead origin addresses, making them hard to recognize the hacker. Proactive ways to deal with DDoS threats are discovering the first machine that causes the attack, thus attempting to put an end to the excessive packet movement. Most present IP follow back routines are obliged to alter the system base, for example, encoding the switch's data into the corresponding fields of the IP header or putting away an agent measure of the bundle content at the switches for IP follow back reason. A more adaptable arrangement is sought, as altering framework consumes more time and money.And also there are various routing and optimization problems .The trace-back issue is a variety of the routing problem.To overcomes this problem and to provide a flexible solution ant based algorithm is used. Thus the Ant algorithm can be utilized to find the possible path in which the DDoS attack can come. This proposed ant-based trace-back method is helpful in finding the path.

Even this path provides only partial flow of information in the network. The ant based trace-back algorithm use flow level information. Numerous methodologies were acquainted with identify flooding and are taking into account inconsistency recognition, since factual measurements of movement will be changed by flooding. Discovery and stopping must be pushed close to the origin due to the dispersed way of these attacks. The investigation of activity stream is not versatile; likewise the examination intakes more cost.

Actually dissecting extensive measure of movement from system is complex to the core. Identification should be done at the change point where overwhelming difference happens in the result. But these systems do prove to be useful when the technique sums up the entire bundle of activity in a period. These attacks can be easily ignored in the traffic that is running on the background. Along these lines the attack pass undetected. Thus an approach based on Sketch, LMS filter, $\chi 2$ divergence is was proposed for anomaly detection. This identification framework monitors and records various characteristics like packets, SYN, flows, for each discrete period of time. In the starting venture of processing the traffic flow is summed up randomly. Second venture is where the forecasting of the time series with Least Mean Square is done. Then the change is detected with $\chi 2$ divergence. Spoofing the packets can be done by a host. This is carried out by using a random IP addresses that is filled into their IP headers.

Spoofing of IP is generally connected with Distributed Denial of Service (DDoS) attacks. Generally DDoS limits and to an extent blocks the access to the legitimate user. This is carried out by depleting the resources of the server of the victim. In order to hide the flooding IP sources, attackers often spoof the IP address. This is done because it is hard to check the spoofing of IP because of the destination-based directing of the Internet. The destination-based directing does not keep up state info of the system which is sending. In this manner it forwards each bundle toward its destination without checking the source of the packet. Thus IP spoofing makes the DDoS attacks substantially much harder to protect against. There are two methods to protect against these attacks. They are Router-based and victim-based.

Improvements to the routing infrastructure are carried out in router based method. Improving the flexibility of Internet servers against attacks is carried out in the exploited victim based method. Endeavours to find flooding sources after events of DDoS attacks is carried out in the router based method. It additionally serves to locate the areas of flooding sources. To find and reject the spoofed traffic there seems to be a mechanism. They share the same resource standards and code paths as the trusted requests. But TTL value will always differ. The hop-count information is not put away in the IP header directly, but it is to be processed based on the Time To Live field. TTL is an 8-bit field in the IP header, which indicates the maximum lifetime of each packet. Each intermediate router decrements the TTL estimation of an in-transit IP packet by one before forwarding it to the next-hop.

$$\text{The final TTL value} = \text{The initial TTL} - \text{hop count} \quad \ldots\ldots(1)$$

The real test in the hop-count calculation is that only the destination sees the final TTL value.

Ingress Filtering is used to restrict the forged Traffic. It generally revolves around the idea of eliminating the spoofed packets.Working of this filter is generally by restricting downstream network traffic to known, and intentionally.Advertised prefixes through an ingress filter. Ingress filtering helps in further possible capabilities for networking equipment like automatic filtering on remote access servers.It checks every packet on ingress to ensure user is not spoofing the packets.

III. CONCEPTUAL MODELLING

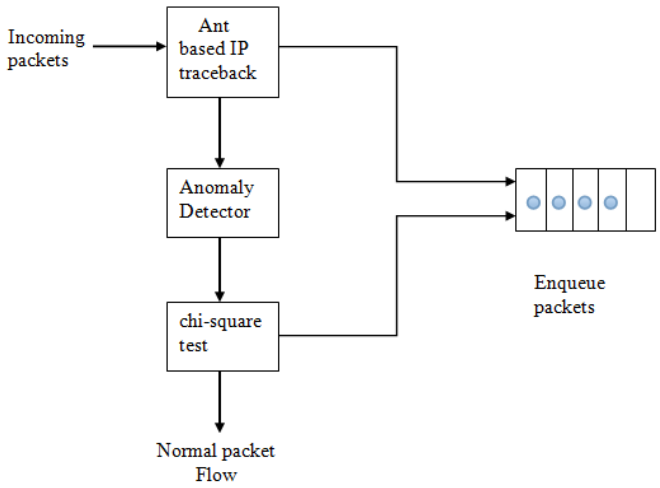

Fig 2.The three tier proposed function

The steps involved in the proposed model are

1. Ant based IP trace-back
2. Anomaly Detector
3. Chi-square based filtering

a. Payload check

b. Header check

3.1 Ant based IP trace-back

All the deceived packets are dropped by the hop count filter. At times, the attack packets are sent with the spoofed header. This hides the attacker's identity. The attacker can spoof the header of the packet, but the hop count value cannot be changed or manipulated. Hence, when a packet arrives, the TTL value is extracted and for all the incoming bundles the number of HOP is calculated. Comparison is done between the value that is stored in the IP2HC (IP to Hop Count) table and the calculated value. If the values that are calculated match with the table value then the packet is accepted and passed on to next filter. But if the values doesn't matches then the packet is a deceived packet, then it is dropped. There is a possibility that a packet may change or deviate from the original path due to a possible node failure or crash. The packet will reach the destination via some other route. When it arrives to the destination via some other route, the hop count value may change. So, taking into account of only the specified hop count value for checking of a possible attack may lead to a legitimate packets getting dropped or denied access. For this purpose the Ant based IP trace-back algorithm is clubbed with hop count filter. This algorithm is helps us in finding the source of the packet. This algorithm utilizes flow level information in order to identify the origin of the bundle. The proposed ant based algorithm has two characteristics, they are heuristics and convergence.

3.2 Anomaly Detector

Basically the anomaly detector functions as a behavior monitor. It check for the possible change in the normal behavior of the packets. Behavior can be of anything like frequency of traffic at a certain time, number of packets from a certain IP, number of requests received from a router etc. It can also even take into account the incoming and outgoing packets to and from a router. Based on one or many of the above mentioned parameters behavior check is done and those packets which seems to be deviating from the normal flow are marked and sent to the next level of filters. Here frequency of traffic is taken as a parameter and checked for the behavior change. It actually helps in detecting the flooding attacks and diverts it to subsequent filters, forcing the attacker into a longer run. The undeceived packets are directly sent to the next layer of filtering without being marked. To test for a possible DDoS attacks the deceived and marked packets needs to be checked. In order to confirm this, the possible attack packets are sent to check for a DDoS attack in the succeeding level of filters.

3.3 Chi-Square based filtering

3.3.1 Payload check

The payload length of the packets differs from one with another. Each packet will have the payload length related to the payload value and the type of request. Not all the payload lengths are same. Here we use the length of the payload to check for the possible attack. We monitor the payload length of the incoming packets for a predefined amount of time and find their usual behavior. This particular behavioral value is checked with all other incoming packets and if there is no change in the value of the incoming packets they are dropped, because if the length of the payload is same for all the packets it indicates a possible attack. It indicates a possible flooding of packets from the same IP. Each requests to the service will be different, hence they will have different payload value ans subsequently different payload length. To find the behavioral change the probability factor is used and cross checked with the Chi-Square distribution. Not only the payload length but also the payload value can be monitored and the check for the possible attack can be done.

3.3.2 Header Check

The header check is similar to that of the payload check except for the fact that the header length is used instead of the payload length. The behavioral change is monitored, probability factor is found and cross checked with chi-square distribution. Again, here the header value can be monitored in the space of header length.

The distance between two discrete probability distributions (p and q) is measured using the X^2 divergence. For two probability sets p = (p'1, p'2, p'3, . . . , p'^{n}) and q = (q'1, q'2, q'3, . . . , q'^{n}).

$$(1)... \quad X^2 = \sum \frac{(E-O)\text{^}2}{O}$$

'E' - expected output

'O' - observed output

The expected output means that incoming packets that were studied for a specific period of time and the anticipated being the current incoming packet

Using the above formula, a goodness of fit test is established.This analysis whether the observed frequency distribution differs from a theoretical distribution or not. There by deciding whether the packets are attack packets or normal packets.

IV. RESULTS

A DDoS attack is being generated by sending external requests from external entities. Well known attack of TCPSYN is generated. The consumers are depicted as attackers to create flooding attack at a time. The behavior of each IP is learnt initially by the defense mechanism of our proposed approach. After learning the behavior of each IP, the defense Mechanism operates to identify a possible attack and will discard the further attack packets

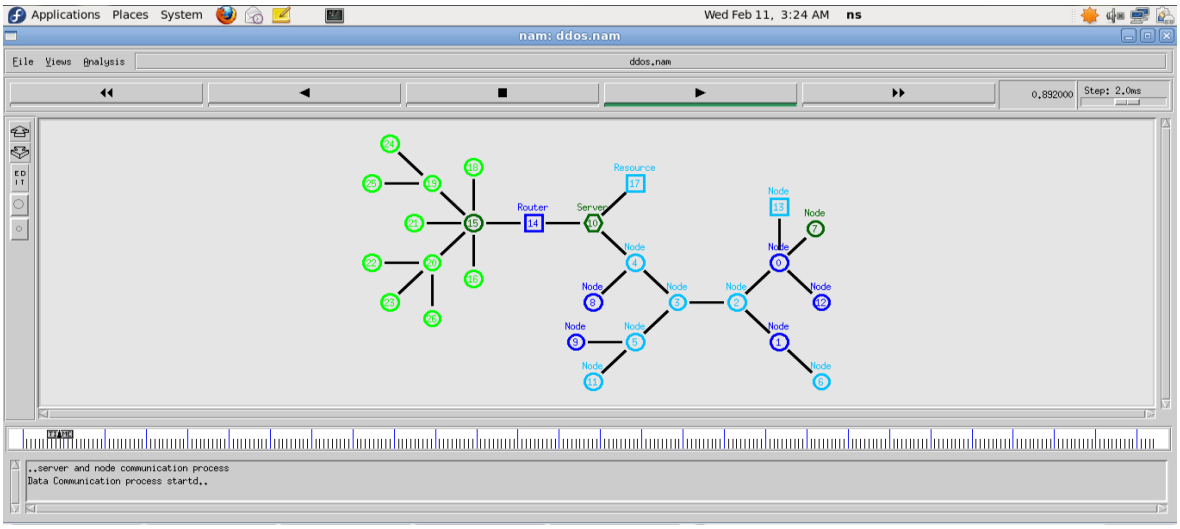

Fig 3. Initial network structure

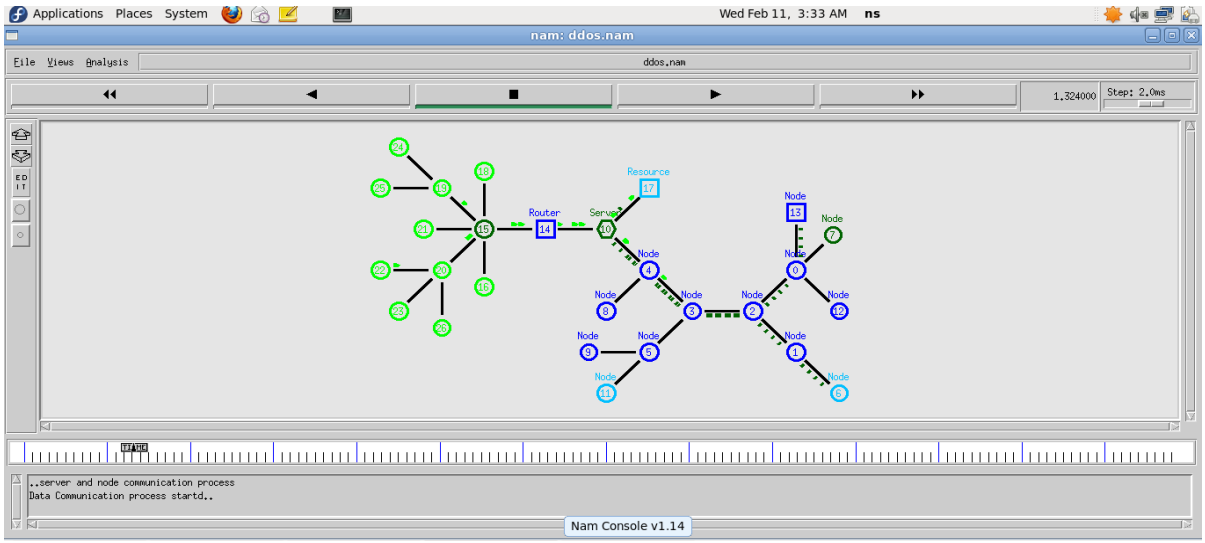

Fig 4 Packet transfer between different nodes

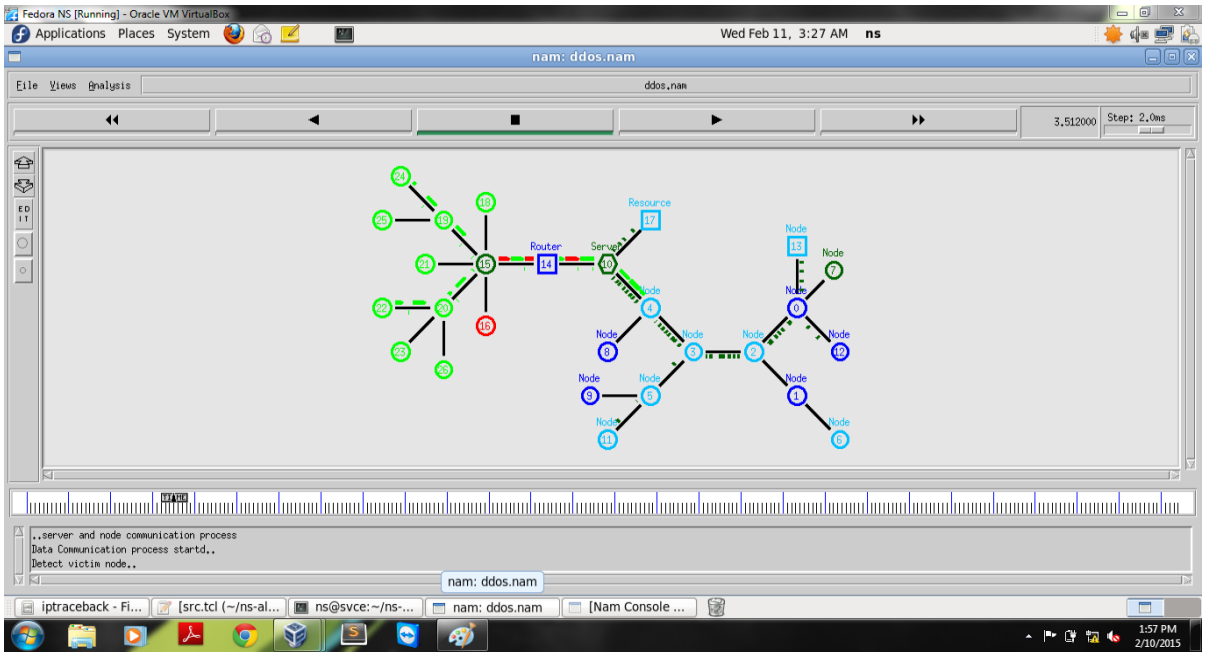

Fig 5 The attack packet being sent

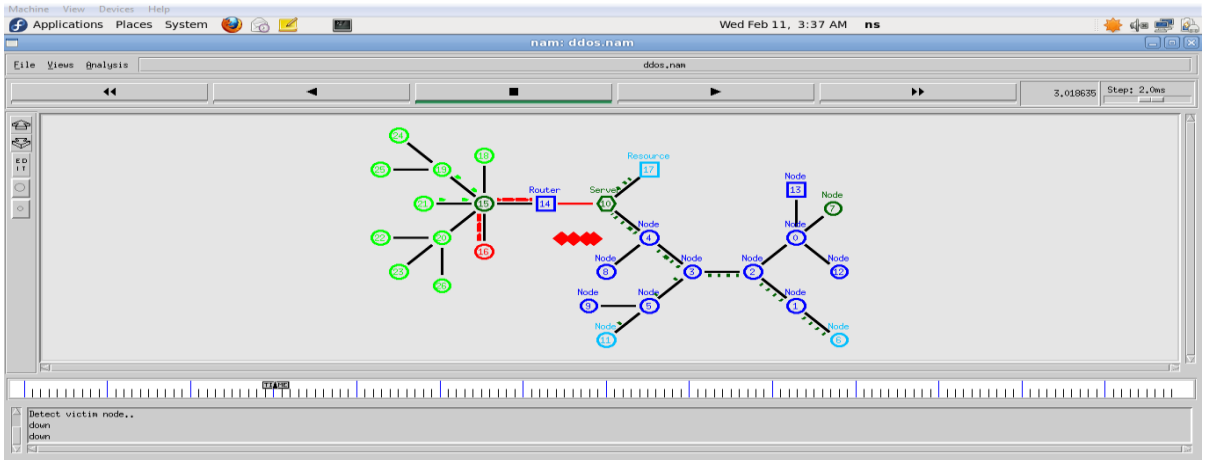

Fig 6 Dropping of attack packets

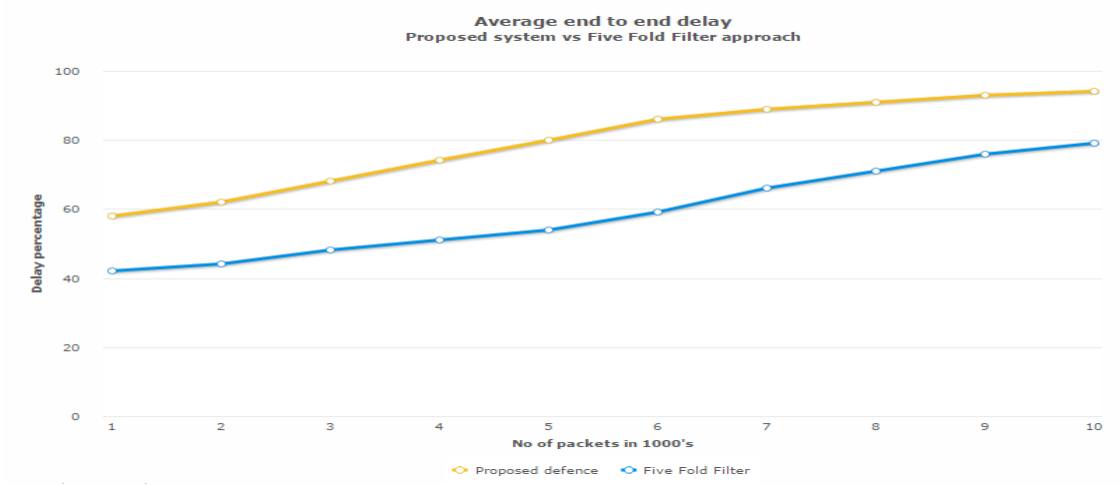

Fig 7 The effectiveness of DDoS mechanism

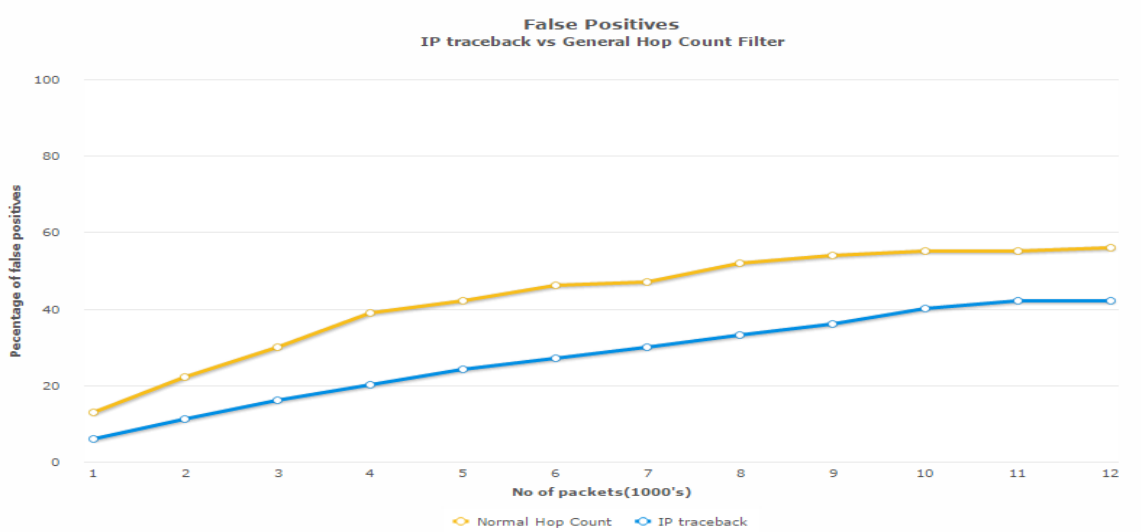

Fig 8 The graph is with the percentage of genuine packets that are present in the test set Vs that detected by the DDoS Defense Mechanism for various time intervals. Also the graph shows improvement of IP based trace-back over Hop count filter with number of false positives Vs the number of packets.

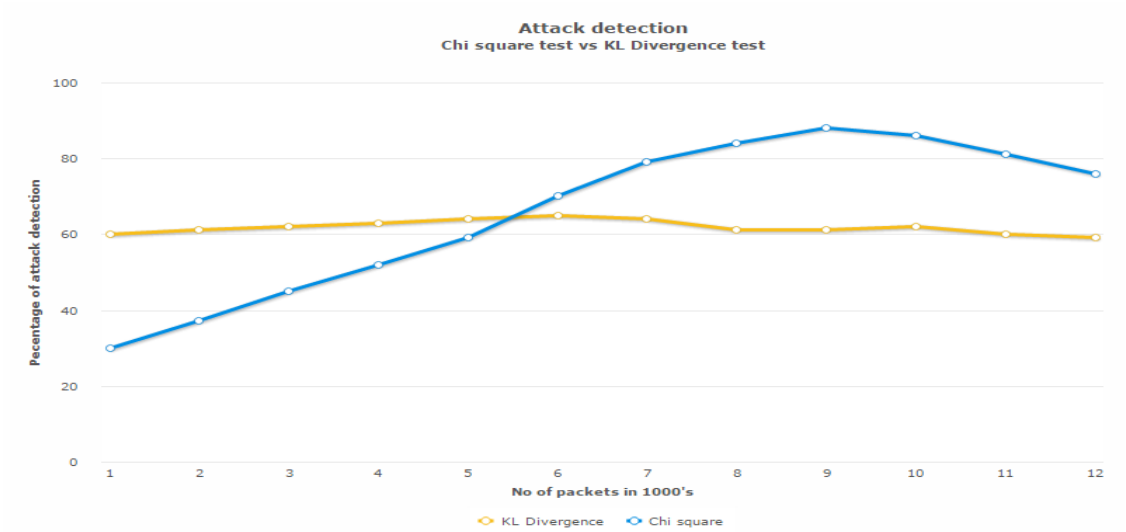

Fig 9 Advantage of using Chi-square over K-L divergence.

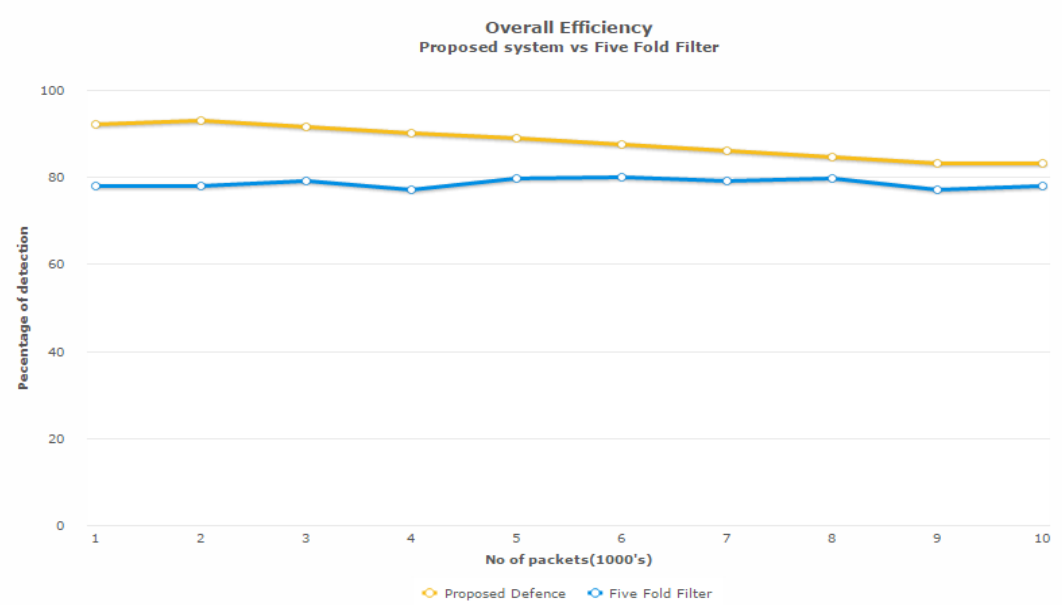

Fig 10 Overall performance graph for depicting the upper hand of the proposed architecture over the five fold architecture

V. RESULTS

The proposed approach results in filtering of the spoofed IP packets and the potential attack packets from the attacker. Here the blocking of the access as a whole is not done, but when there seems to be an excess traffic, the requests are processed with a delay from the normal access time. In the meantime, the check for the possible attack is done. Though the delay seems to be increasing with the incoming packets being flooded, the end result being high reliability of the service offered. Increase in the latency is a tradeoff for this approach. Reducing the delay for the access will result in more efficient and reliable approach towards this attack. However to solve this, parallelization of the entire process can be done, depending upon the traffic flow on a particular day or time, the number of threads to be processed can be setup. This improvisation will help in reducing the overhead of processing the entire of flow of packets by one filter. Again it may create an overhead of giving access to a particular packet, like for which packet, one has to give priority. This can be solved by a simple FIFO queue model. Geography based filter can also be clubbed with this process for more efficient filtering, but attackers can spoof the geography of the packets. So, for this an efficient method of detecting the proxy servers has to be implemented. If done, it will be more appropriate for efficient and reliable packet filtering approach for a possible DDoS attack.

REFERENCES

[1]. Varalakshmi.P, Thamarai Selvi.S, "Thwarting DDoS attacks in grid using information divergence", Volume 29, Issue 1, January 2013, Pages 429–441
[2]. Mohamed M.Abd-Eldayem,"A Proposed HTTP service based IDS", Egyptian Informatics Journal, Vol 15, Issue 1, March 2014
[3]. Broniatowskia.M,Leorato.S,"An estimation method for the Neyman chi-square divergence with application to test of hypotheses", A Journal of Multivariate Analysis, Volume 97, Issue 6, July 2006, Pages 1409–1436
[4]. P. VARALAKSHMI, THAMARAI SELVI.S, A. JAVED ASHRAF, K. KARTHICK, B-TREE BASED TRUST MODEL FOR RESOURCE SELECTION IN GRID, IN: IEEE INTERNATIONAL CONFERENCE ON SIGNAL PROCESSING COMMUNICATIONS AND NETWORKING, 2007, PP. 222–227.
[5]. Daneil S. Yeung, Shuyuan Jin, Xizhao Wang, Covariance matrix modeling and detecting various flooding attacks, IEEE Transactions on Systems, Man, and Cybernetics Part A: Systems and Humans 37 (2) (2007) 157–169.
[6]. Jelena Mirkovic, Peter Reiher, D-WARD: a source-end defense against flooding denial-of-service attacks, IEEE Transactions on Dependable and Secure Computing 2 (3) (2005) 216–232.
[7]. Issariyakul • Ekram Hossain-"Introduction to Network Simulator NS2 "-published in springe
[8]. ns2 Tutorial Exercise Multimedia Networking Group",The Department of Computer Science,UVA Jianping Wang Partly adopted from Nicolas's slides.
[9]. University of texas," Network simulator tutorial" by Austin Dave.
[10]. Cheng Jin,Haining Wang,Kang G. Shin"Hop-Count Filtering: An Effective Defense Against Spoofed DDoS Traffic",IEEE/ACM transcation on Networking,Vol 15,No.1,Feb 2007
[11]. Osman Salem,Ali Makke,Jean Tajer,Ahmed Mehaoua,"Flooding attack detection in Traffic of backbone networks",36th Annual IEEE Conference on local computer Networks.
[12]. Yulong Wand,Rui Sun,"An IP-Traceback-based packet Filtering for Eliminating DDoS Attacks,Journal of Networks,Vol 9,No.4,april 2014 6.1 Web Links
http://csis.bits-pilani.ac.in/faculty/murali/resources/tutorials/ns2.htmTeerawat
http://www.isi.edu/nsnam/ns/tutorial/
http://nile.wpi.edu/NS