

## DESIGN AND ANALYSIS OF A NOVEL GROUP TESTING APPROACH (NGTA) ON A WSN FOR MINIMIZING THE DOS ATTACKS

Ms. D. SRIJA <sup>#1</sup> , Dr. K.VENKATA RAO <sup>#2</sup>

<sup>#1</sup> M.SC Scholar, Master of Computer Science,  
College of Engineering, Andhra University, Visakhapatnam, AP, India.

<sup>#2</sup> Professor, Department of Computer Science and Systems Engineering,  
College of Engineering, Andhra University, Visakhapatnam, AP, India.

### ABSTRACT

In the recent scenario, security domain have attracted a lot of users attention towards it as in current day's security plays a very important role in each and every domain like medical, schools, shopping, financial banks, banking sector, insurance and so on. As the security plays a very important role intruders or attackers also try to hack the sensible information in any of the hacking forms. As the data is transferred mainly through interconnected systems like web servers, local database servers or through an overlay servers like those which are stored on remote hardware not on the local servers, there were a lot of security threads from these network attackers. One among the best hacking technique is Denial of Service Attack (DOS) which comes under non-physical attack. So in this paper we have implemented a Novel Group Testing Algorithm (NGTA) which mainly used for analyzing the accurate network traffic by extracting the geometrical values between the intermediate nodes. Also as an extension for this current application we implemented the modes of delay like if a data be affected by DOS attacker during the data transmission, then the server can identify automatically which type of request or response it has received. This principle is identified in two ways like if the server receives the data within the time period which is specified by client during data transmission then it is treated as normal and termed as Normal Mode. If the same request or response is received more than the stipulated time specified by the server for that request or response, then it is treated as Danger Mode. By conducting various experiments on our proposed system we finally came to a conclusion that a network administrator who has such ability can identify whether the current network is attacker prone or free from attackers.

**Key Words:** Attacker, Group Testing Approach, Denial of Service Attack, Correlation Analysis, Attack Modes.

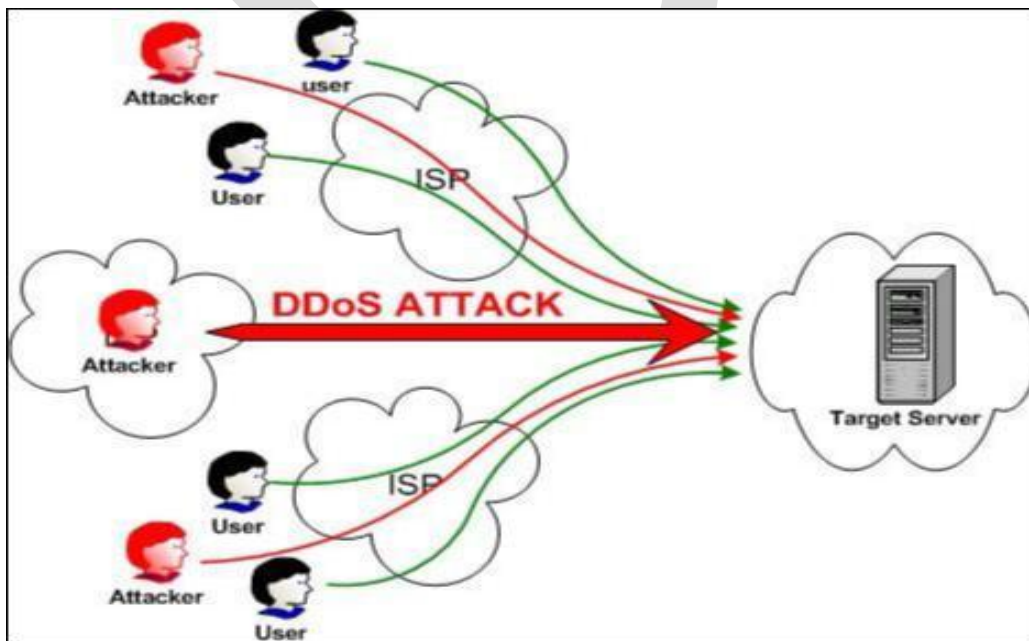
## I. INTRODUCTION

Currently almost all parts of the world are concentrating more and more on their security levels. As there was a tremendous increase of electronic devices almost each and every user try to store, retrieve, access the data to and fro via electronic devices. As the security plays a very important role even though there was a lot of hackers or intruders who try to hack or attack the sensitive data of others during data transmission. In recent days security plays a very vital role in each and every organization like banking, hotels, shopping malls, Hospitals, Schools and so on. As security plays a very prominent role a lot of users try to access the contents illegally and they want to misuse the content during transmission [1].

Generally attacks are classified into two types based on their functionality

1. Physical Attack
2. Non-Physical Attack

The attack which is been attempted by an intruder and in turn misuse the content or damage the content physically from its original content is known as physical attack. In this physical attack the data will not be transferred from valid source to valid destination, even some times with an attacked content [2]. On the other side if an attack occurs just in order to make delay during data transfer, without changing the original content is known as non-physical attacks. In this category the data will not be changed or damaged but just the data will be sending or received to and from the source and destination with some delay. Generally identifying the non-physical attack is very difficult for the network admin as the hacker can create delay either from source node or destination node or at router level. Hence it is very crucial task for the network admin to identify the non physical attacker [3].



**FIG 1. REPRESENTS THE TYPICAL ARCHITECTURE OF A DENIAL OF SERVICE ATTACK ON A TARGET SERVER**

From the above figure 1, we can clearly identify that the dos attack which is created on a distributed network is termed as a distributed denial of service attack and in turn they will try to deny the access of valid user from the target server. These DDOS attackers always try to deny the access of authorized users from the target server. As we all know that more delay always leads to loss, so if a DOS attacker who wish to create some disturbance in transmission of data to and from the target server, then it will be leads to data loss.

Distributed Denial of Service is one form of attack where a lot of zombie computers (infected computers that are under the control of the attacker) are used to either directly or indirectly to flood the targeted server(s), victim, with a huge amount of information and choke it in order to prevent legitimate users from accessing them (mostly web servers that host websites). In most cases, the owners of the zombie computers may not know that they are being utilized by attackers. In some cases, there is only a periodic flooding of web servers with huge traffic in order to degrade the service, instead of taking it down completely which is clearly seen from above figure.

Generally hacker(s) sit at a remote terminal connected to a Botnet Control Centre, which in turn commands individual user machines, collectively called Botnet. These machines are compromised prior to the attack with special software that allows the hacker to exploit them. Subscribing to our service, you are protected from DDoS attacks, due to the fact that Bad/Attack traffic is directed to our protected network. It consists of a number of Points of Presence (PoP) that we have around the world to ensure better connectivity with your visitors, allowing us to receive and balance malicious traffic globally. See diagram below for schematics of one of our PoP's. When bad traffic reaches one of our PoP's it is being filtered and cleaned, then sent out to you as clean traffic. Thus, your site's accessibility is ensured throughout the duration of any type of DDoS Attack [4].

## **II. BACKGROUND WORK**

In this section we mainly discuss the background work that was carried out in identifying the denial of service attacks on a network having multiple clients and one service provider. In this current thesis we will discuss about Unique Multivariate Correlation Analysis algorithm in order to point out the exact location where the denial of service (DOS) attack occurred in the network.

### **DOS ATTACK DETECTION ON A NETWORK**

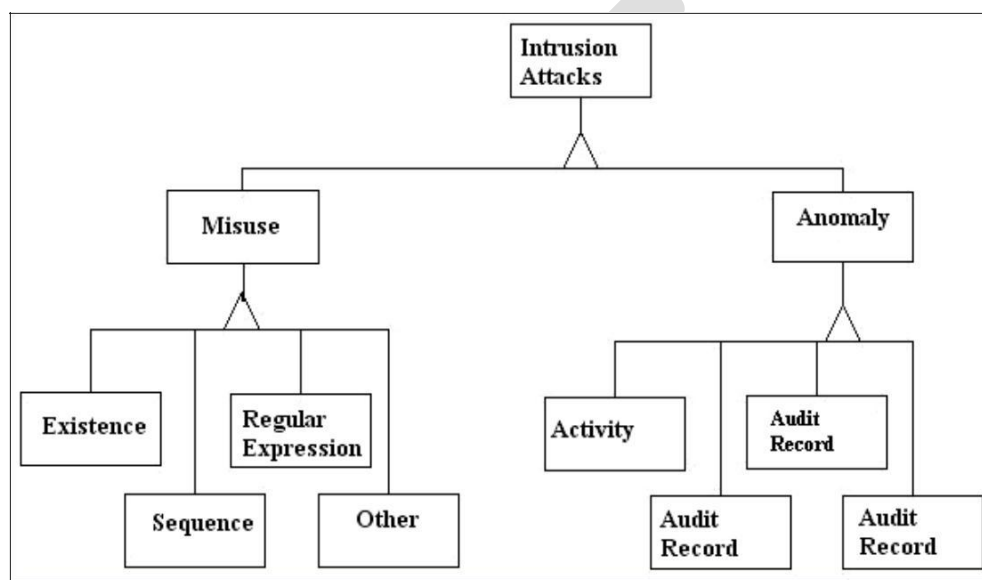
Generally the DOS attack can be occurred either at network end or either at host end. So the system should identify the attack accurately from any level [4], [5]. Generally when coming to the network based attacks detection, it is again classified into 2 main sub categories like:

- i. Misuse Based Detection System
- ii. Anomaly Based Detection System

Generally the misuse-based detection systems will identify the network attacks by monitoring all the network activities and it looks for any matches that found with existing attacks

that occur in the same system. In spite of having high detection rates to known attacks and low false positive rates, misuse-based detection systems are easily known and hacked by any new attacks and even variants of the existing attacks. Along with this it is also a complicated task to maintain the signatures database updated in the network.

On the other hand the anomaly based detection systems are proposed in which the network is monitored continuously and if it found any node significantly deviate from the legitimate traffic as a suspicious objects, anomaly based detection system try to identify the attacks. By doing this the user can able to detect zero-day intrusions that exploits previous unknown system vulnerabilities [6], [7].



**FIG 2. REPRESENTS THE ARCHITECTURE OF A NETWORK BASED DETECTION SYSTEMS**

From the above figure 2, we can clearly get an idea about the architecture of network based detection systems. Generally the network based detection systems is classified into two categories like misuse based and anomaly based and which in turn sub-divided into various other types based on the type of functionality.

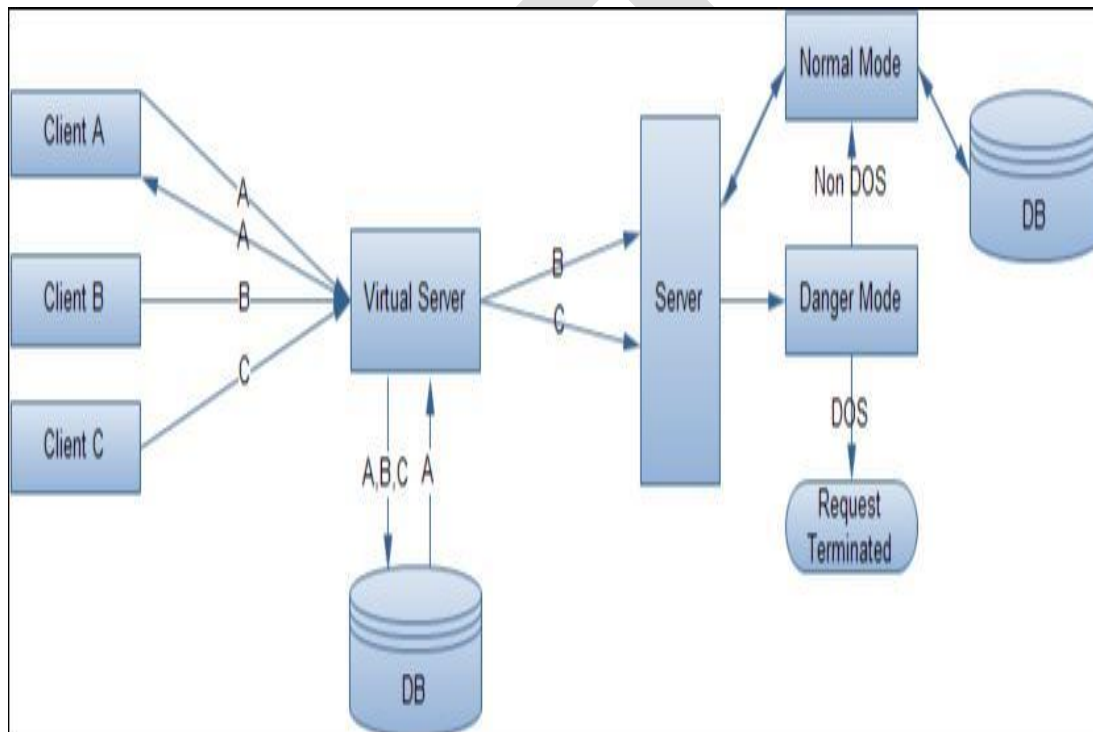
### III. PROCEDURE FOR NOVEL GROUP TESTING ALGORITHM

In this section we will mainly discuss about the proposed procedure for detecting the dos attacker who tries to create delay in sending packets from valid client node to server node and in turn response from server node to requested client node. This NGTA method is mainly used to balance the loan when traffic occurs during data transmission at the intermediate nodes.

The proposed Group Testing Approach consists of  $t$  pools and  $n$  items (including at most  $d$  positive ones). This model can be represented by a  $t \times n$  binary matrix  $M$  where rows represent the pools and columns represent the items. An entry  $M[I, j] = 1$  if and only if the  $I$ th pool contains the  $j$ th item; otherwise,  $M[I, j] = 0$ . The  $t$ -dimensional binary column vector  $V$  denotes

the test outcomes of these  $t$  pools, where 1-entry represents a positive outcome and 0-entry represents a negative one. Note that a positive outcome indicates that at least one positive item exists within this pool; whereas negative one means that all the items in the current pool are negative.

A detection model based on GT can be assumed that there are  $t$  virtual servers and  $n$  clients, among which  $d$  clients are. Binary testing matrix  $M$  and testing outcome vector  $V$ . Attackers. Consider the matrix  $M_{t \times n}$  in Fig. 1, the clients can be mapped into the columns and virtual servers into rows in  $M$ , where  $M[i, j] = 1$  if and only if the requests from client  $j$  are distributed to virtual server  $i$ . With regard to the test outcome column  $V$ , we have  $V[i] = 1$  if and only if virtual server  $i$  has received malicious requests from at least one attacker, but we cannot identify the attackers at once unless this virtual server is handling only one client. Otherwise, if  $V(i) = 0$ , all the clients assigned to server  $i$  are legitimate. The  $d$  attackers can then be captured by decoding the test outcome vector  $V$  and the matrix  $M$ .



**FIG 3. REPRESENTS THE PROPOSED GROUP TESTING APPROACH TO IDENTIFY DOS ATTACK**

From the figure 3, we can clearly get an idea that our proposed GT approach is best suited for identifying the DOS attackers in a distributed environment along with the different types of modes. In this paper we have implemented this GT approach in order to identify the attack which occurred during the network and also we have identified the mode of request and response. Here we can find the request mode as well as response mode[8]-[11].

Initially the sender will choose a data which is to be sending to the receiver and he will estimate the bandwidth based on the system RAM availability and which in turn gives the

approximate time taken to send the data. If the request receives the receiver within the expected time then the data request have received in normal mode. If the request is received more than the expected time with delay, then we can get an idea that request have been received in danger mode. Hence in this way the GT based approach is used for identifying the DOS attacks which is available in the network.

## IV. SYSTEM IMPLEMENTATION PHASE

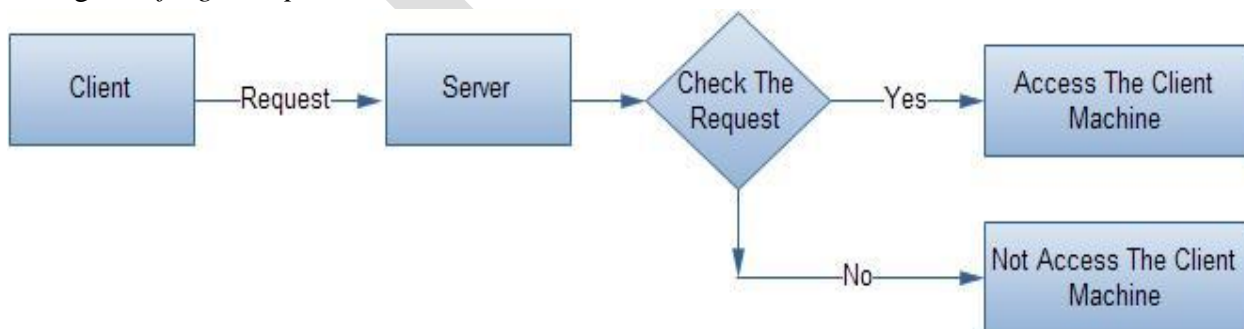
Implementation is a stage where the theoretical design is converted into programmatically manner. Generally in this phase all the whole application is divided into number of modules, where each and every module has individual methodology. Now let us discuss about the modules in detail as follows:

1. Login Module
2. Group Attacker Module
3. Group Testing Module
4. Victim/Detection Module

Now let us discuss about each and every module in detail with a flow-chart for each and every individual module.

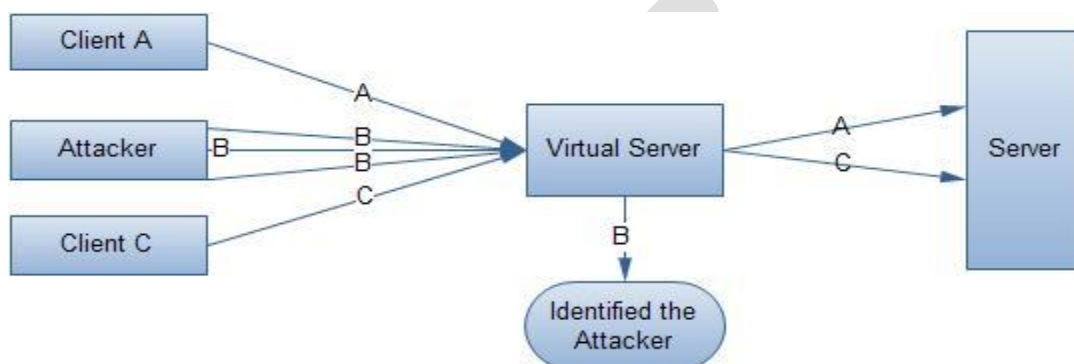
### 1. LOGIN MODULE

In this module the client has the facility to login into the system with a valid user id and password. If the user enters a valid details he can enter into the system if not he will get a invalid authentication. Here the login will be available for only client and for proxy, router and main server there will be no login available. Here each and every task was monitored by the main server. If the application explicitly states which component of the username/password pair was incorrect then an attacker can automate the process of trying common usernames from a dictionary file in an attempt to enumerate the users of the application. Whilst applications may handle authentication failure messages correctly, many still allow attackers to enumerate users through the *forgotten password* feature.



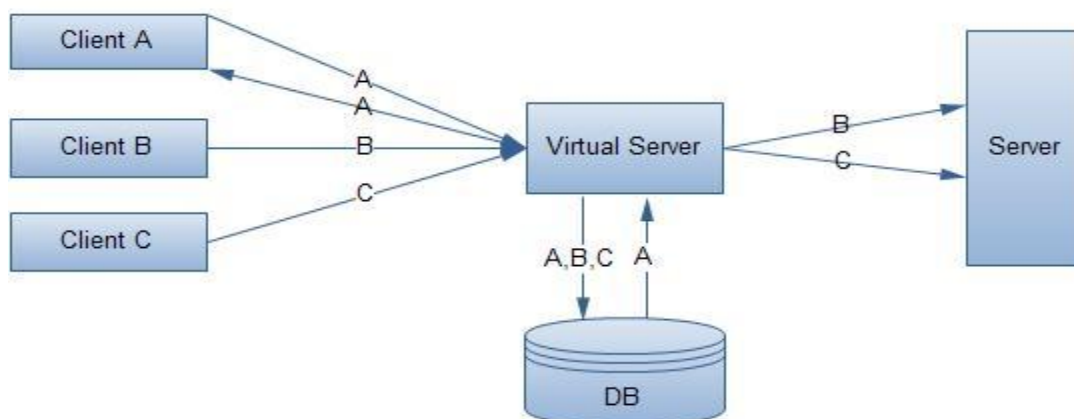
## 2. GROUP ATTACKER MODULE

This is the module in which the group attacker who tries to create the Denial of service attack is monitored and identified in the network. In this module the group attacker is the main person who has the ability to identify the attacker within the network in any of the intermediate level. If the attack was occurred within the client level or proxy level or router level or main level this can be easily identified by the group attacker module. Hence this module is mainly used for monitoring the attack that was caused in the network during data communication. Here virtual server plays a vital role in identifying the attacker that occurs within the network.



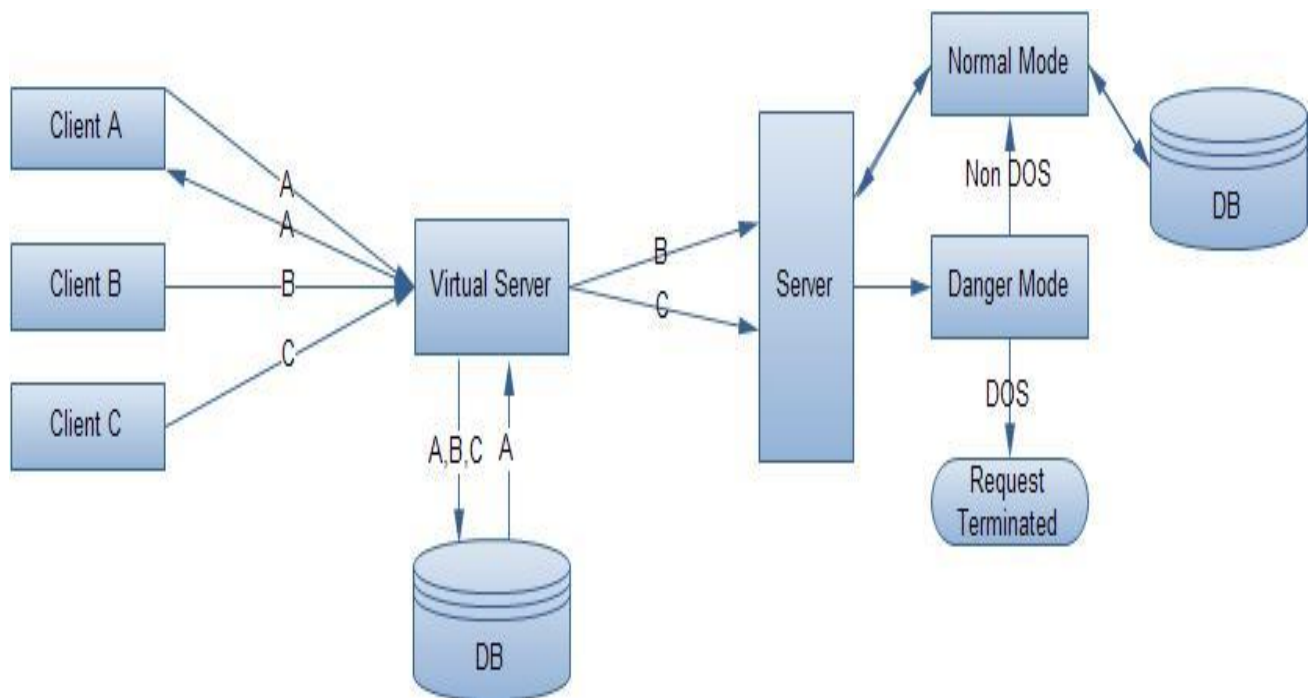
## 3. GROUP TESTING MODULE

This group testing module is the main module in which the attacker is identified with the help of this approach. This GT approach is mainly used to study the time and delay that take place during the data transfer. The GT based approach is mainly used for identifying the delay based on each and every individual bandwidth .For a low bandwidth system there may be huge delay which cause DOS and for a high bandwidth there may be less delay which will try to send the data in time as per the expected arrival time. This GT based approach mainly calculates the type of attack that occur within the network.



#### 4. VICTIM/DETECTION MODULE

The victim model in our general framework consists of multiple back-end servers, which can be Web/application servers, database servers, and distributed file systems. This victim module is nothing but detection of modes based on user request. Here in the module if the user tries to send the request with some delay it is identified as attacker module or danger mode and if the same request is received in within the time, it is identified as normal mode.



#### V.CONCLUSION

We finally implemented a simple technique for detecting application DOS attack by means of a new group testing algorithm. This NGT Algorithm is mainly motivated and proposed by various primitive methods that are available in literature, all the primitive methods failed in achieving high accuracy compared with our proposed NGT Algorithm. For this NGT Algorithm we divided into two sub algorithms for detecting the denial of service attackers. First method is Group Testing based approach and second one is correlation analysis (CA). By conducting various experiments on our proposed mechanism, our simulation results demonstrated that our proposed mechanism is best in terms of finding the denial of service attacks in a distributed network.

## VI. REFERENCES

- [1] .U. D. Khartad and R. K. Krishna, "Route Request Flooding Attack Using Trust Based Security Scheme in Manet," International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN), Vol. 1, No. 4, 2012, p. 27.
- [2]. R. Guo, G. R. Chang, R. D. Hou, Y. H. Qin, B. J. Sun, A. Liu, Y. Jia and D. Peng, "Research on Counter Bandwidth Depletion DDoS Attacks Based on Genetic Algorithm.
- [3]. H.-J. Kim, R. B. Chitti and J. S. Song, "Handling Malicious Flooding Attacks through Enhancement of Packet Processing Technique in Mobile Ad Hoc Networks," Journal of Information Processing Systems, Vol. 7, No. 1, 2011, pp. 137-150.
- [4].*The Philosophy of Anonymous* "Radicalphilosophy.com. 2010-12-17. Retrieved 2013-09-10.
- [5] "Understanding Denial-of-Service Attacks". US-CERT. 6 February 2013. Retrieved 26 May 2016.
- [6] .TFreak, 2003. [www.phreak.org/archives/exploits/denial/smurf.c](http://www.phreak.org/archives/exploits/denial/smurf.c)
- [7].*The Philosophy of Anonymous* "Radicalphilosophy.com. 2010-12-17. Retrieved 2013-09-10.
- [8] K. Lee, J. Kim, K. H. Kwon, Y. Han, and S. Kim, "DDoS attack detection method using luster analysis," Expert Systems with Applications, vol. 34, no. 3, pp. 1659-1665, 2008.
- [9]. Fed CIRC, "Defense Tactics for Distributed Denial of Service Attacks," Federal Computer Incident Response Center, Washington DC, 2000.
- [10]. "Brand.com President Mike Zammuto Reveals Blackmail Attempt". 5 March 2014. Archived from the original on 11 March 2014.
- [11]. "Brand.com's Mike Zammuto Discusses Meetup.com Extortion". 5 March 2014. Archived from the original on 13 March 2014.

## VII .ABOUT THE AUTHORS



**Ms. D.SRIJA** is currently pursuing 2 Years M.SC in Computer Science at College of Engineering, Andhra University, Visakhapatnam, AP, India . Her areas of interest includes Networking, Security and Web Mining.



**Dr. K.VENKATA RAO** is a Honorary director of A.U Computer Centre and a Professor, in Computer Science and Systems Engineering, College of Engineering, Andhra University, Visakhapatnam, AP, India. He has more than 23 years of experience in teaching field. His research interest includes Image Processing, Security and Big data analyst.