Impact of Flash Crowd Attack in Online Retail Applications

[1]Thrimurthi M [2]Adithya B A [3]Thandavamurthi H R
[1, 2, 3] Department of Electronics and Communication
Malnad College of Engineering
Hassan, India

Gururaj H L
Department of Computer science and Engineering
Malnad College of Engineering
Hassan, India

***Abstract* - Now days the usage of internet has been enormously increased. Online shopping has acquired widely in day today event. Mean which these online shopping is affected by various advanced network security attacks Flash Crowd Attack is the one of the advanced attack, where huge amount of dummy requests are sent at a time and thus putting lot of pressure on server machine and degrade the efficiency. Also authorized client can't receive the acknowledgement notification. We found that this attack might cause lot of problems to online buy user in the coming days. This paper depicts the minimization Flash Crowd Attack and discuses various issue of this attack.**

Keywords - Flash Crowd Attack; DoS; Energy

I. INTRODUCTION

The opponent can try for criminal entry to the services provided by network affect the independent node and this is named as Denial of Service (DoS) attack. DoS attack is like a concern some to a network [1]. This type of systems accommodates services like server processes and routing in the network. At a given stop of these action handled by a small amount of traffic depends on the performance of bandwidth, memory usage, power consumption and hardware [8]. Service may not be serve by the servers and the actual traffic is ignore when the saturation point of this outreach [4] [5].

An upgrade form of common DoS attack can be called as a Distributed Denial of Service (DDoS) [1]. The attack may not be on single computer rather it as set of equipment's used as a master- slave constructed machine in networks has multi-tiered structure. The root names many Internet services depleted by the integrated attacks [9]. Network attacker will crack the system into group of intermediate systems, this can be downloading on a system that is connected to internet through auto router software and installed as DDoS freeware package. As a result the compose machine is made as "slave" who was serving as "master" tool, and a cracker uses the composed machine to crack other network connected systems [2].

With single point of contact it can check thousands of machines [11]. Distributed DoS acts as a critical risk to the network connected. In paper [11] they have done a survey on this which says it's been expand hugely in latest stage. With an excess of advantages in current world like financial benefit, some group of tricky information is composed which boost to do crime. Encrypting memory, renewal of data, obfuscation of coding implementing peer-to-peer expertise and mimicking of flash crowd techniques are used to covering their spot on networks. Flash crowd authorized issues some of the bob up messages with a funny wish to attack the server. In paper [13] they made flash crowds to beat below radar to trace layout of network traffic so it is called as flash crowd attacks and it is been done from decades.

In the current era, most easy way for an opponent is to crack applications. They found a way to disturb application resources such as "flash crowd attacks" [4] [8]. They may act as a true application processor by set up the network and produce legal demand for the applications to reverse the victim. This type of attack is powerful, challenging since it is active in authorized resources so they act like they are authorized user in a network [16].

Due to bulky usage of the Internet for varying application technology has implement low power and low cost consuming WSNs. As a result of this primary nature of networks, it is open to many attacks [10]. These types of attacks may be performed on different layers of the network. Some of them can be corrected and it can be resolved using some of the protocols to avoid attacks. These kinds of cracking are not so easy to name it and put a stop to [6].

II. RELATEDWORK

Flash Crowd Attack (FCA) was first termed in a fictional short story. FCA is one of the agnate forms of Distributed

ISBN: 978-0-9957075-6-6 *DOI: 10.24032/ijeacs/0205/02*

Denial of Service (DDoS). It drifts the service demand along with the victim node that is produced from different sources [11]. FCAs are just challenging since they have the capacity to request accepted and critical data. The Flash crowd Attacks are hard to find since the attack appeal are identical to those of accepted requests [13].

DoS attacks & flash crowd attacks can both burden the server with their requests, but unlike DoS attacks which are legible malicious requests [7], flash attacks contains the rightful requests too. A flash is a supreme surge in traffic to a appropriate node in WSN introduce a effective increase in the load and putting stress on the node and its links, which may lead to failure of the complete path[13] [14].

They often burden web sites to an extent in which the services are spoil or degraded completely. Flash Crowd Attack is well known for over whelming well-provisioned services, effecting HTTP clients to time-out when trying to admittance the server resources. Stuff of FCAs on the servers at the web sites and nodes in the network infrastructure are evident and can prove incisive. Traffic jam at the network layer may avoid few amounts of requests from reaching servers [15].

From the data collected by varies flash crowds with varies domains, we can know many attributes of flash crowds, in view of online service and also by the view of salesperson of large content [5].

III. NETWORK MODEL

The typical point to point data link having end points and there is no packet data. Whole authorization for deleting the data that has to be transplant will be control by the server/host on either side. Via RS-232 a cable was in between a computer and the medium of communication. Adjacent machine are connected by wires directly between their interface cards.

In order to denote a wire or other connections which interface a pair of machine or the circuits in computer architecture and computer networking is also called by the term conventional point-to-point data link, when compared to rest of the topologies like bus and hybrid which connect many devices.

A. CSMA Network:

Carrier Sense Multiple Access (CSMA) is a probabilistic media access control (MAC) protocol in which a node checks the absence of other traffic before transmitting on an own transmission medium [13].

Carrier sense can be defined as a process in which before start of transmission the transmitter will analyses or check the response from the other end to detect or verify if there is any other transmission on the link, i.e. it tries to achieve information about a carrier wave which may have been transmitted from a different source before trying to transmit data. The station will halt idle till the current transmission of data completes before starting the transmission of shared data if a carrier is sensed. It's based on a principal "listen before talk" or "sense before transmit". Multiple accesses mean that multiple source and destination send and receive on the medium. Transmitted data will be received by each and every node in the medium if transmitted by a source.

B. CSMA/CD:

Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is the usage of LAN by Ethernet as shown in Fig 3.1. To access a network a device verifies or establishes if it's free or not. If the connected network is engaged with two devices utilizes the link simultaneously which results in their collision attack. As a result of which they both devices withdraw for some time before attempting [16] [13].

Messages are exchanged between host and client on the basis of response and request mechanism. A response will be produced by the host for a request from client. This is an illustration for inter process communication.

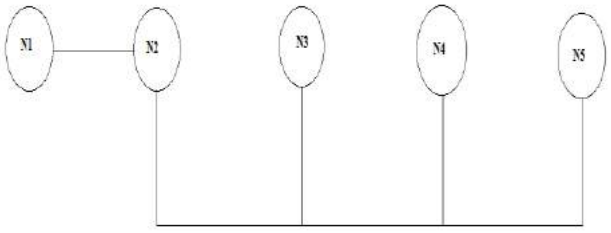

Fig 3.1 CSMA and Point-to-Point Mo‹1el

In order to connect, there must be a common language and some certain set of rules and regulation must be followed in order to access a conclusion of what to anticipate between each other for client and host. A protocol of communication defines the common language and the set of rules. Operation of protocols among client-server will be based on application layer. An API like web service will be used by the host to make exchange of information simple.

C. Flash Crowd Attach Network Model

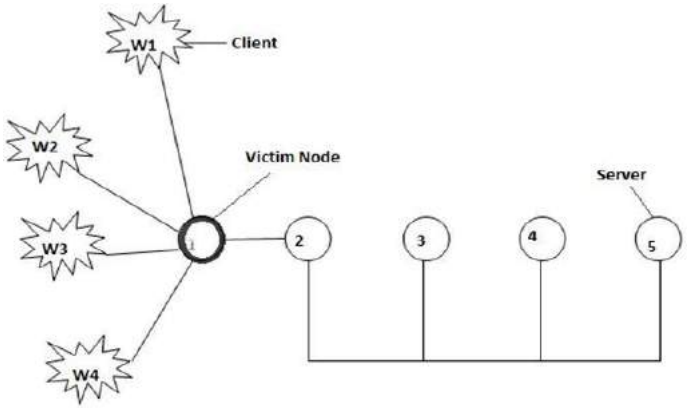

Fig 3.2 Flash Crowd Attack Model

A gateway will be part of two networks which use different protocols in computer networking and tele-

ISBN: 978-0-9957075-6-6 DOI: 10.24032/ijeacs/0205/02

communications. A protocol will be transferred data to next one by gateway as depicted in Fig 3.2.

In the Fig 3.3, we have connecting the wireless nodes with that of the original simulated CSMA and point to point network. This gives us the new network model for the Flash Crowd Attack. The several Wi-Fi nodes directly attached with the access point 1, which act as a victim node in the flash crowd attack. The access point gets oppress by the requests of the wireless Wi-Fi nodes on it. In the next section, we brief analyze about the similar real-time model.

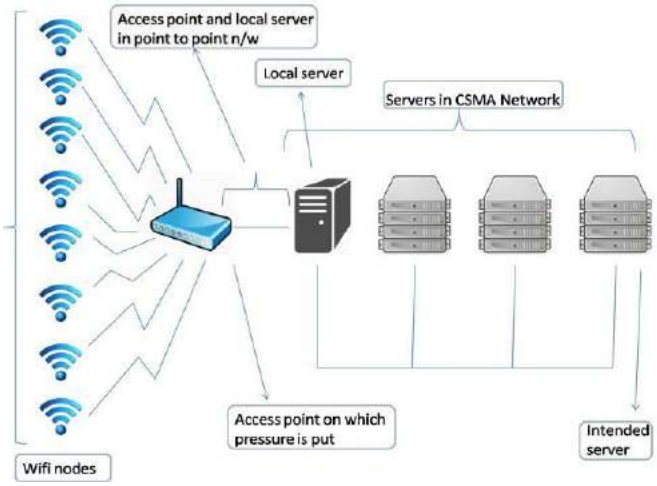

Fig 3.3: Flash Crowd Attack Model in a Real-Time Application

The above fig 3.3 shows the typical scenario of the Flash Crowd Attack model in a real-time application. The fig3.3 consists of 8 Wi-Fi wireless nodes which are connected to the access point. Thus all Wi-Fi nodes generate requests that will pass through this access point. So access point will gain lot of load from the requests of these Wi-Fi nodes. Then the access point will integrated with a local server in a point-to-point connection. Then all these local servers are connected to a CSMA network to each other. The server at the end is called as intended server. The notification from the Wi-Fi nodes will be served by the intended server.

Eavesdropper is an attacker or opponent, who keeps recording and analyzing the secret information that transmitting between the sender and receiver. This of security attack is known as Eavesdropping. Eavesdropping leads to flash crowd attack. Enormous generate dummy requests to a single server at the same time leads to breakdown of server. All Users (clients) are intent to use the their respective websites (servers) when it has broadcast and user interested to do shopping when the online applications give good offers like Electronic goods are 80% offer, Flash sale Big Billion days in Flip kart. So number user can access the respective server at the same time enormous requests will be sent to sever which can't able to reply back for all the real clients. This type of attack is called Flash Crowd Attack. The server lost its power and may stop it work at one point of time because of dummy requests from the fake nodes

We had research many online retail applications for better understanding of security. In this generation people rapidly use online applications. So in our survey many applications with flash crowd attack.

All online market, messengers, online shopping applications such as Flip-kart way2SMS, Amazon, Snap deal, EBay and many other applications are not completely secured. Even today also they are using Hypertext Transfer Protocol (HTTP) as a protocol of application layer in OSI model. We can easily catch the username and password using a network tool wire shark NS3. Wire-shark is a network protocol analyzer which catches (capture) the real time information completely such as bank transactions details, online retail account which might affect the human territory. G-Mail is the one of the online mailing secured application which uses RSA cryptographic algorithm and HTTPS protocol.

Way2SMS is an online portal massage communication where they give users to send unlimited text messages for a person to person communication. All user register using their ten digits mobile phone number. The registered ten digit mobile phone number is the username. Each and every time users should be login using the same registered phone number. Unauthorized person can register using some others mobile number. This leads to an attack called eavesdropping [12].

IV. Result Analysis

The ns-3 simulator is a discrete-event network simulator intend to use for research and educational use. We analyze the results of our plane for various situations using graphical representation.

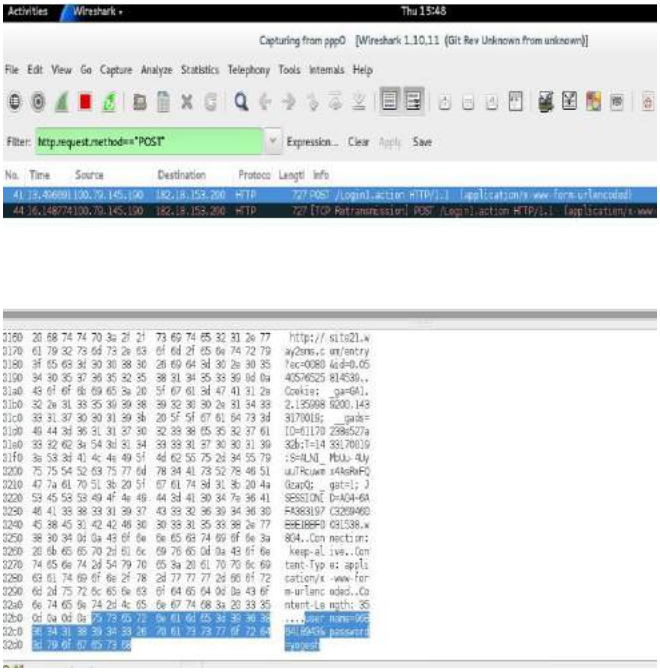

Figure 4.1 Cyber Attack- Eaves dropping attack.

ISBN: 978-0-9957075-6-6 *DOI: 10.24032/ijeacs/0205/02*

The cyber-attack is determined using an online retail application. Using a network analyzer tool Wire- shark had captured the password and username of the Flip-kart user's account which uses HTTP protocol and is plotted in the Fig 4.1. This attack is called Eavesdropping attack.

Eavesdropping attack finally comes to flash-crowd attack. The FCA network model is constructed using NS3 (network simulator-3) and the network animation of the same is shown below in Fig 4.2. In the network model, 10.1.3.1, 10.1.3.2, 10.1.3.3, 10.1.3.4, 10.1.3.5,

And 10.1.3.6 is the client nodes IP address. 10.1.3.7 is the Access point IP address where, all the requests will be comes in to a server 10.1.3.7.

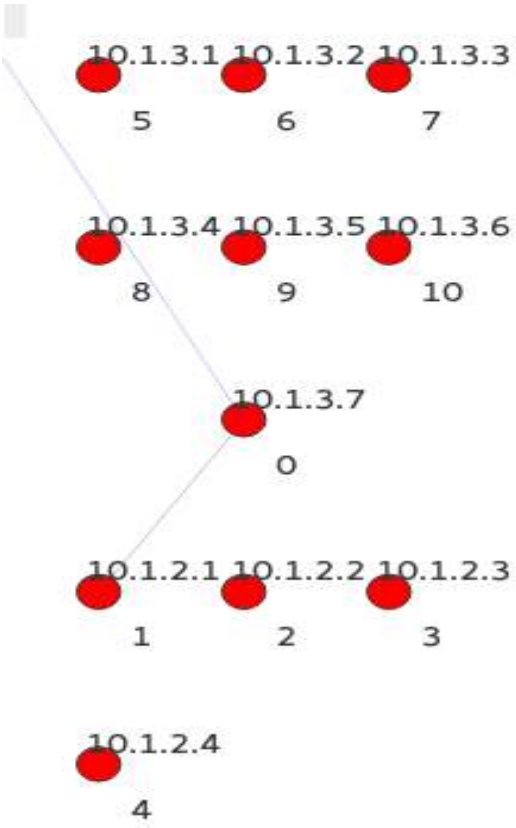

Fig 4.2 Node deployment using NetAnim

By using address Resolution Protocol (ARP) to find the MAC address of server Wi-Fi node. Once we get the MAC address of server using ARP, all clients will starts to send the data packets (request) to the server at the same time as depicted in Fig 4.3

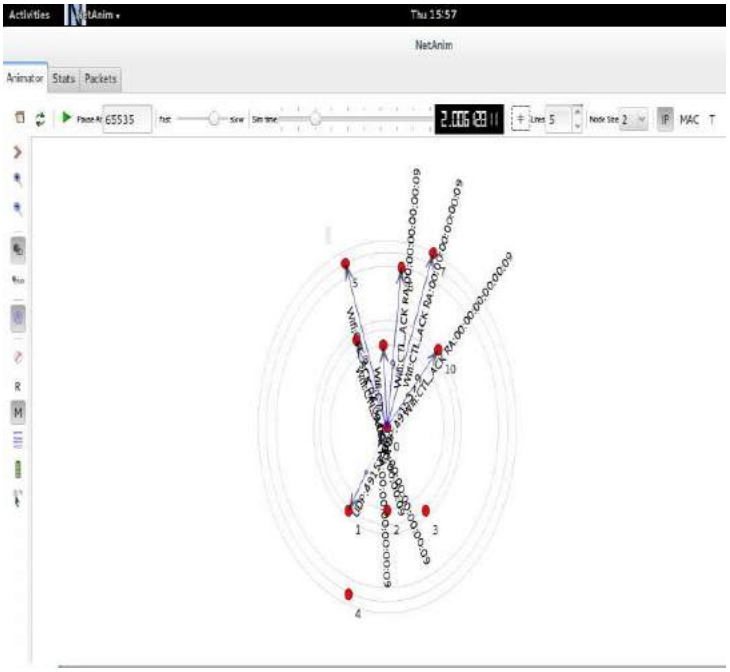

Fig 4.3 Sending Data Packets to Server by various Clients

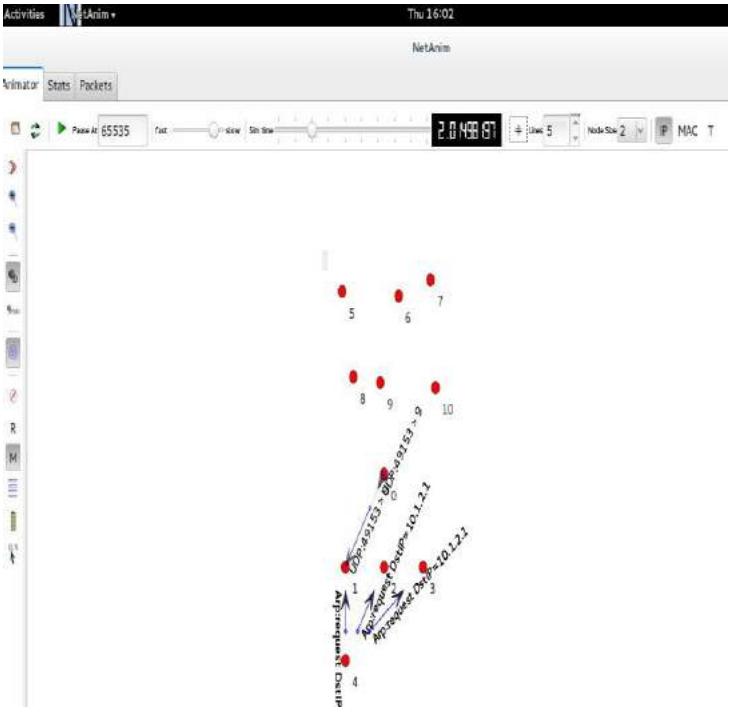

Fig 4.4 Finding the IP Address of Source by Server

The server gets request of various clients and replying confirmation massage to few clients is shown in the Figure 4.4

ISBN: 978-0-9957075-6-6 *DOI: 10.24032/ijeacs/0205/02*

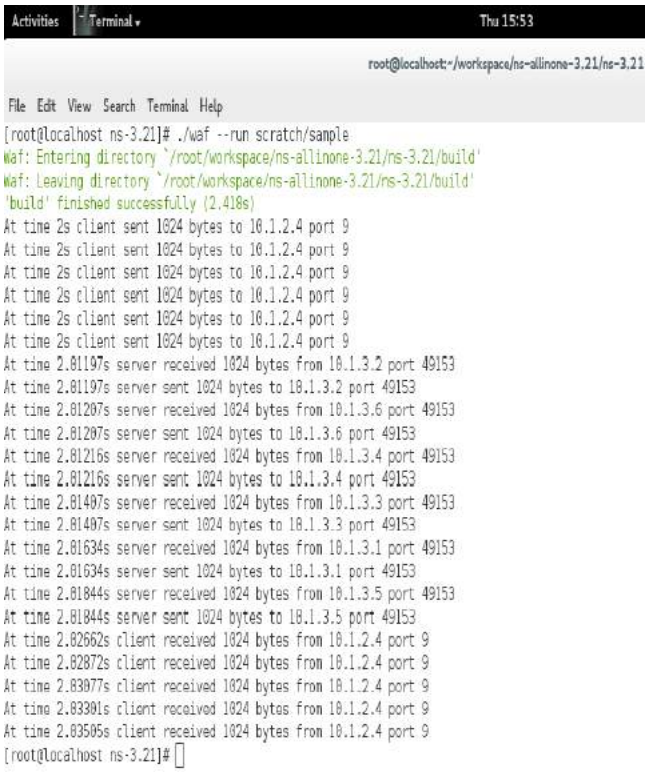

Fig 4.5 Six Clients and One Server Communication

At time 2 second all six clients' sends the request to a server 10.1.2.4. But the sever cant able to reply for all the clients, the server 10.1.2.4 replied only for four clients in our model that can be clearly depicted in the Fig4.5.

As the number of user increases, the energy of the server keeps decreases that can be clearly depicted in the Fig4.6.

In real time scenario many real clients may not receive the conformation massage instead the opponents may receive the reply which is a flash crowd attack. To capture all data packets we will use Wire shark tool, they we can capture all data packets of each user and interface.

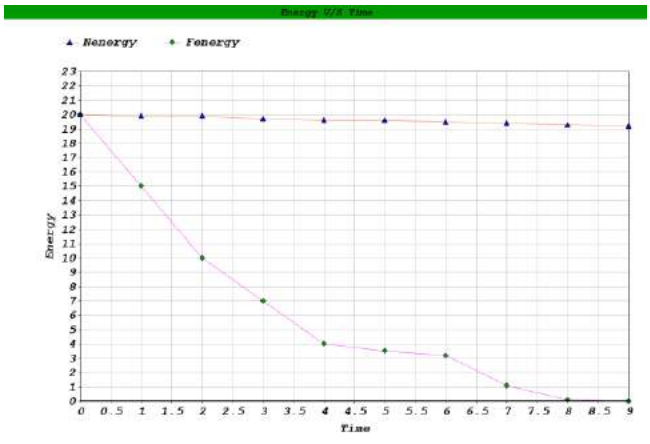

Fig 4.6 Energy Graph of Flash Crowd Attacks

The Energy Graph of Flash Crowd Attacks can analyzed in fig 4.6,we can observe that energy is constant when FCA is not present but when we consider FC attack the energy of end server will decreased drastically. This also leads to decrees life time of the server as the number of dummy requests increases.

This problem can minimized by server will send ARP reply packets back to the clients, when server gets the request from various clients. The server once gets the MAC address of various clients the server will start sending the conformation massage back to respected clients.

V. CONCLUSION

In our research we had analyzed Flash Crowd Attack can't be removed completely, with respect to our simulation result but it can be minimized only to a certain level. We can only decrease effects on the server by identifying the authorized client to that of fake client for send back the data packet to real client. More number of clients it will effect on the server machine, and hence some authorized clients cannot get the service notification that is intended to have. There is a lot of way for eliminating these effects. Instead of having just one server machine to all the clients, we can implement more than server machine. Introducing of more number of server machines will reduce the pressure on one server machine, and there will be equal load balancing.

Apart from determine the real clients from that of dummy clients we can also derive a system of ARP at server side or on the side of access point to identify the authorized or real clients from that of dummy clients

REFERENCES

[1] Gururaj H L , Praveen K S , Ramesh B, -Minimizing the Impact of Flash Crowd Attack in Online Retail Applications, 2017 11 the International Conference on Intelligent Systems and Control (ISCO).

[2] M. Edman and B. Yener, -On anonymity in an electronic society: A survey of anonymous communication systems,I ACM Comput. Surv., vol. 42, no. 1, 2009.

[3] B. Stone-Gross, M. Cova, L. Cavallaro, B. Gilbert, M. Szydlowski, R. Kemmerer, C. Kruegel, and G. Vigna, -Your botnet is my botnet: Analysis of a botnet takeover,‖ in Proc.ACMConf. Comput. Commun. Security, 2009.

[4] Z. Li, A. Goyal, Y. Chen, and V. Paxson, -Towards situational awareness of large-scale botnet probing events,‖ IEEE Trans. Inf. Forensics Security, vol. 6, no. 1, pp. 175–188, Mar. 2011.

[5] C. A. Shue, A. J. Kalafut, and M. Gupta, -Abnormally malicious autonomous systems and their internet connectivity,‖ IEEE/ACM Trans. Netw., vol. 20, no. 1, pp. 220–230, Feb. 2012.

[6] N. Jiang, J. Cao, Y. Jin, L. E. Li, and Z.-L. Zhang, -Identifying suspicious activities through DNS failure graph analysis in Proc. IEEE Int. Conf. Netw. Protocols, 2010, pp. 144–153.

[7] S. Yadav, A. K. K. Reddy, A. L. N. Reddy, and S. Ranjan, Detecting algorithmically generated malicious domain names,‖ in Proc. Internet Meas. Conf., 2010, pp. 48–61.

[8] N. Ianelli and A. Hackworth, -Botnets as vehicle for online crime,‖ in Proc. 18th Annu. 1st Conf., 2006.

ISBN: 978-0-9957075-6-6 *DOI: 10.24032/ijeacs/0205/02*

[9] P. Wang, S. Sparks, and C. C. Zou, "An advanced hybrid peertopeer botnet," IEEE Trans. Dependable Secure Comput., vol. 7, no. 2, pp. 113- 127, Mar'/Apr. 2010.

[10] M. Bailey, E. Cooke, F. Jahanian, Y. Xu, and M. Karir, "A survey of botnet technology and defenses," in Proc. Cybersecurity Appl. Technol. Conf Homeland Security, 2009.

[11] S. Yu, W. Zhou, and R. Doss, "Information theory based detection against network behavior mimicking DDoS attack," IEEE Comrnun. Lett., vol. 12, no. 4, pp. 319- 321, Apr. 2008.

[12] A. Schen-ef, N. Lan·ieu, P. Owezarski, P. Borgnat, and P. Abry, "Non-Gaussian and long memory statistical characterizations for internet traffic with anomalies," IEEE Trans. Dependable Secure Comput., vol. 4, no. I, pp. 56-70, Jan./Mar. 2007.

[13] A. EI-Atawy, E. AI-Shaer, T. Tran, and R. Boutaba, "Adaptive early packet filtering for protecting firewalls againstDOSattacks," in Proc. IEEE Conf. Comput. Commun. (lNFOCOM), 2009.

[14] Shui Yu, Wanlei Zhou, Weijia Jia, Song Guo, Yong Xiang, and Feilong Tang " Discriminating DDoS Attacks from Flash Crowds Flow Correction Coefficient" IEEE transactions on parallel and distributed systems, vol. 23, no. 6, June 2012.

[15] Ms P.Rajani Reddy, Mr R shiva, Ms C.Malathi 'Techniques to Differentiate DDos Attacks from Flash Crowd" International Journal of Advanced Research in Computer Science and Software Engineering.

[16] Shui Yu, Song Guo, and Ivan Stojmenovic, "Fool Me If You Can: Mimicking Attacks and Anti-Attacks in Cyberspace" IEEE Transactions on Computers, Vol. 64, No. I , Jan 2015.

AUTHOR PROFILE

Thrimurthi M, purduing his Electronic and Commucication Engineerin in Malnad College of Engineering, Hassan. He is member of IEEE Computer Society, Bengalore Section . He is research iterests in Communication System, Embedded System, Multimedia Networking

Adithya B A, purduing his Electronic and Commucication Engineerin in Malnad College of Engineering, Hassan. He is member of IEEE Computer Society, Bengalore Section . He is research iterests in Communication System, Embedded System, Multimedia Networking.

Thandavamurthi H R, purduing his Electronic and Commucication Engineerin in Malnad College of Engineering, Hassan. He is member of IEEE Computer Society, Bengalore Section . He is research iterests in Communication System, Embedded System, Multimedia Networking.

Guruj H L, received his B.E (2010) and M.Tech (2013) in Computer Science and Engineering from Visvesvaraya Technological University, Belagaum.Karnataka. He is pursuing his doctoral degree in Malnad College of Engineering, Hassan. Currently he is working as an Assistant Professor in the Department of Computer Science and Engineering, Malnad College of Engineering, Hassan, India. He is a member of IEEE Computer Society, Bangalore Section. He has awarded with Young Scientist International Travel Support under SERB, DST, Govt of India in December 2016. He has research interests in congestion control algorithms, security issues in cloud computing and routing protocols for multi-hop wireless networks, QoS-aware routing algorithms in ad hoc networks and multimedia networks.