Advances in Computational Sciences and Technology
ISSN 0973-6107 Volume 10, Number 8 (2017) pp. 2257-2272

http://www.ripublication.com

DDos Defense: Enhanced Flooding Detection and Confidence-Based Filtering Method

Dr. V. Naga Lakshmi
Professor & HOD/Department of MCA
GITAM Institute of Science, GITAM University, Visakhapatnam, India

Shameena Begum
Research Scholar
GITAM Institute of Science, GITAM University, Visakhapatnam, India

Abstract

Distributed Denial of Service (DDoS) attack is a critical threat to the Web-based and Client-Server applications and resource allocation to defense the DDoS attack has become a major challenge. To overcome these challenges, in this paper we proposed a HTTP GET Flooding Detection and Confidence-Based filtering method for DDoS Attack Defense in Web application. HTTP Get flooding attack is the most critical and frequently attempted attack. To overcome this attack an early stage HTTP GET Flooding Detection technique is connected. The dynamic resource allocation is applied to automatically coordinate the available resources (CPU, Memory, I/O and Bandwidth) of a server to relieve DDoS attacks on individual clients. After CBF (Confidence-Based Filtering) score is calculated for each packet, resource analysis is done to determine whether to discard the packet/request or not.

Index terms: HTTP, CBF, DDoS, Client-Server, Attack Flooding, Resource, Confidence.

I. INTRODUCTION

A. Client-Server Architecture

Denials of Service (DoS) attacks are undoubtedly a very serious problem in the Internet, whose impact has been well demonstrated in the computer network literature. The main aim of DoS is the disruption of services by attempting to limit access to a machine or service instead of subverting the service itself. This kind of attack aims at rendering a network incapable of providing normal service by targeting either the network's bandwidth or its connectivity. These attacks achieve their goal by sending at a victim a stream of packets that swamps his network or processing capacity denying access to his regular clients.

Consumers and the businesses user can use applications without installation and access their personal files at any computer with web access using the client-server. It provided efficient computing by centralizing information storage, process and bandwidth. It is served up by real hardware but it seems too provided by real server hardware and it is usually used to network-based services. Many researchers are looking forward to use the client-server approach for many different applications.

Distributed Denial of Service (DDoS), is a relatively simple, yet very powerful technique to attack Internet resources. DDoS attacks add the many-to-one dimension to the DoS problem making the prevention and mitigation of such attacks more difficult and the impact proportionally severe. DDoS exploits the inherent weakness of the Internet system architecture, its open resource access model, which ironically, also happens to be its greatest advantage.

The infrastructure is shared by potentially millions of users and once attacker got the share infrastructure benefit and using the resource to deploy attacks in more efficient ways. since client-server users usually share computing resources, so such attacks are more effective in the client-server environment e.g., being connected through the same switch, sharing with the same data storage and file systems, even with potential attackers

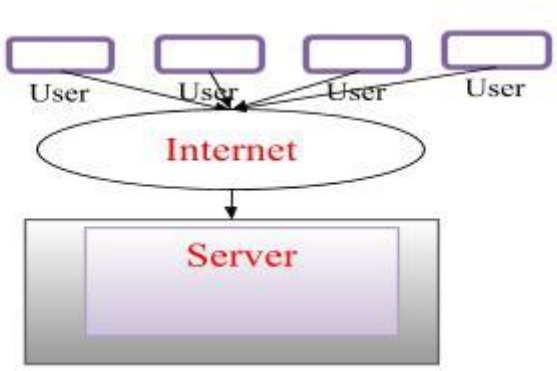

Figure 1. Client-Server Architecture

B. Security Attacks in Network

Client-Server security refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of client-server architecture. It evolves as a sub-domain of computer security, network security, and, more broadly, information security. There are many forms of client-server attacks. Among them important attacks that exist are DDoS attacks against client server, Hypertext Transfer Protocol (HTTP) based Denial of Service (H-DoS), Extensible Markup Language (XML) based Denial of Service(X-DoS), and Hypertext Transfer Protocol (HTTP) based Denial of Service (H-DoS).

1) Denial of Service Attack Against client-server: It becomes a most common security threat in client-server architecture and the attack intentionally compromises the availability of the machines, and it is typically against the affected users.

2) HTTP Based DDOS Attack: In HTTP based system, sending the request in many ways, the two main being GET and POST. When an HTTPclient (say, a Web browser) talks to an HTTPserver (a Web server), A GET request is what is used for"normal links", including images; such requests are meant to retrieve a static piece of data, the URL pointing to that piece of data. When a URL is entered in the URL bar, a GET is also done.

3) Distributed Denial-Of-Service Attack against client server: In this multiple systems targets a single target. Multiple compromised systems or compromise multiple machines attack and causing denial of service for client server users of the targeted system. A computer under the control ofan intruder is called as a zombie or bot.

4) XML based DDOS attack: These are extremely asymmetric. An attacker needs to spend only a fraction of the processing power or bandwidth that the victim needs to spend to handle the payload, to deliver the attack payload. Worse still, DoS vulnerabilities in code that processes XML are also extremely widespread.

Compromised machines are one of the key security threats on the Internet; they are often used to launch various security attacks such as DDoS, spamming, and identity theft. In this work we address this issue by investigating effective solutions to automatically identify compromised machines in a network. These attacks flood the system with an excessive amount of attack traffic thereby consuming bandwidth and network resources. So, in order to achieve protection against such attacks this paper will establish a defense mechanism fighting immediately against these attacks [1-10].

C. Distributed Denial of Service (DDoS)

DDoS is one of the malicious attacks which causes inestimable loss in Internet business. DDoS attacker may target towards the diminution of network or memory resources of network either by exhausting of victim bandwidth or by stealing the sensitive information from the victim end [2]. Distributed denial of service attacks are basically denial of service attacks commit by many systems at the same time on a single victim. Existing DDoS defense mechanisms could not resolve the problem completely due to their own limitations.

Denial of service attacks have become a growing problem over the last few years resulting in large losses for the victims. One good example of this loss is the attacks of Yahoo, CNN, and Amazon in February of 2000 which had an estimated loss of several million to over a billion dollars [14].

Distributed Denial of Service (DDoS) attacks are a virulent, frequent type of attack on the availability of Internet services and resources. DDoS attackers infiltrate large numbers of computers by exploiting software vulnerabilities, to set up DDoS attack networks. These unwitting computers are then invoked to wage a coordinated, large-scale attack against one or more victim systems. Distributed Denial of Service attacks are exercised by attackers in various forms. These attacks vary from single attacking source to a networked attacking infrastructure. They also vary in degree of automation, from manual efforts to fully automated attacks.

The main aim of a DDOS attack is the interruption of services by attempting to limit access to a machine or service instead of subverting the service itself. This kind of attack aims at rendering a network incapable of providing normal service by targeting either the network's bandwidth or its connectivity. These attacks achieve their goal by sending at a victim a stream of packets that swamps his network or processing capacity denying access to his regular clients.

Rate-based detection engines are also not successful at detecting HTTP flood attacks, as the traffic volume of HTTP floods may be under detection thresholds. It is very hard for network security devices to distinguish between legitimate HTTP traffic and malicious HTTP traffic, and if not handled correctly, it could cause a high number of false-positive detections. HTTP flood attacks may be one of the most advanced non-vulnerability threats facing web servers today. [13]

II. RELATED WORK

Shui Yu et. al., [12] have implemented a dynamic resource allocation strategy to counter DDoS attacks against individual network customers. When a DDoS attack occurs, we employ the idle resources of the network to clone sufficient intrusion prevention servers for the victim in order to quickly filter out attack packets and

guarantee the quality of the service for benign users simultaneously. The proposed method benefits from the dynamic resource allocation feature of network platforms, and it is easy to implement. They establish a queueing theory based model to estimate the resource allocation against various attack strengths. Real-world data set based analysis and experiments help us to conclude that it is possible to defeat DDoS attacks in a network based environment with affordable costs.

Junho Choi et. al., [13] has proposed a method of integration between HTTP GET flooding among DDOS attacks and MapReduce processing for fast attack detection in network computing environment. This method is possible to ensure the availability of the target system for accurate and reliable detection based on HTTP GET flooding.

A.M. Lonea et. al., [15] has proposed a quantitative solution for analyzing alerts generated by the IDSs, using the Dempster-Shafer theory (DST) operations in 3-valued logic and the fault-tree analysis (FTA) for the mentioned flooding attacks. Their solution quantitatively represents the imprecision and efficiently utilizes it in IDS to reduce the false alarm rates by the representation of the ignorance.

Wanchun Douaet. al. [11] has proposed a Confidence-Based Filtering method, named CBF. This method was deployed by two periods, i.e., non-attack period and attack period. More specially, legitimate packets are collected in the non-attack period, for extracting attribute pairs to generate a nominal profile. With the nominal profile, the CBF method is promoted by calculating the score of a particular packet in the attack period, to determine whether to discard it or not.

III. PROBLEM STATEMENT & PROPOSED METHODOLOGY

1. The method was not concerned about available resources. In client-server application systems the resource allocation is very important, but there is no resource allocation mechanism.
2. The method is not effective on attacks of HTTP GET Request.

To solve above problems, in this paper we proposed a HTTP GET flooding detection method and confidence-based filtering method for DDoS attack defense in network based environment.

Initially, HTTP GET flooding detection method is applied to detect the early DDoS attack. The HTTP Get flooding attack [13] is the most critical and frequently attempted attacks and the threshold is generated from the characteristics of HTTP GET Request behaviors. DDoS detection method based on a threshold for HTTP GET Request is short of accurateness since the threshold is bound to be high.

The dynamic resource allocation [12] is applied to automatically coordinate the available resources (CPU, Memory, IO, bandwidth) of a network to mitigate DDoS

attacks on individual network customers. After resources allocated, CBF (Confidence-Based Filtering) [13] is calculated for each packet, to determine whether to discard it or not. This method was deployed by two periods, i.e., non-attack period and attack period.

IV. OVERVIEW OF THE PROPOSED WORK

A Two-Stage Detection System, HTTP GET Flooding Detection and Confidence-Based Filtering (CBF) method is proposed to defend against DDoS Attacks.

In this research work, at first HTTP GET Flooding attack system is connected to identify the early DDoS attacks. The CBF Module will check the incoming requests based on the Threshold value. Threshold is the value that is set based on the characteristics of the requests arriving per second. This module is then connected to Resource Analysis module to check whether the server has adequate resources to defeat the DDos Attack.

The following figure shows the architecture of the proposed system to detect the risk of the DDoS attacks in web based application using the modules Confidence-Based Filtering and and Resource Analysis connected together.

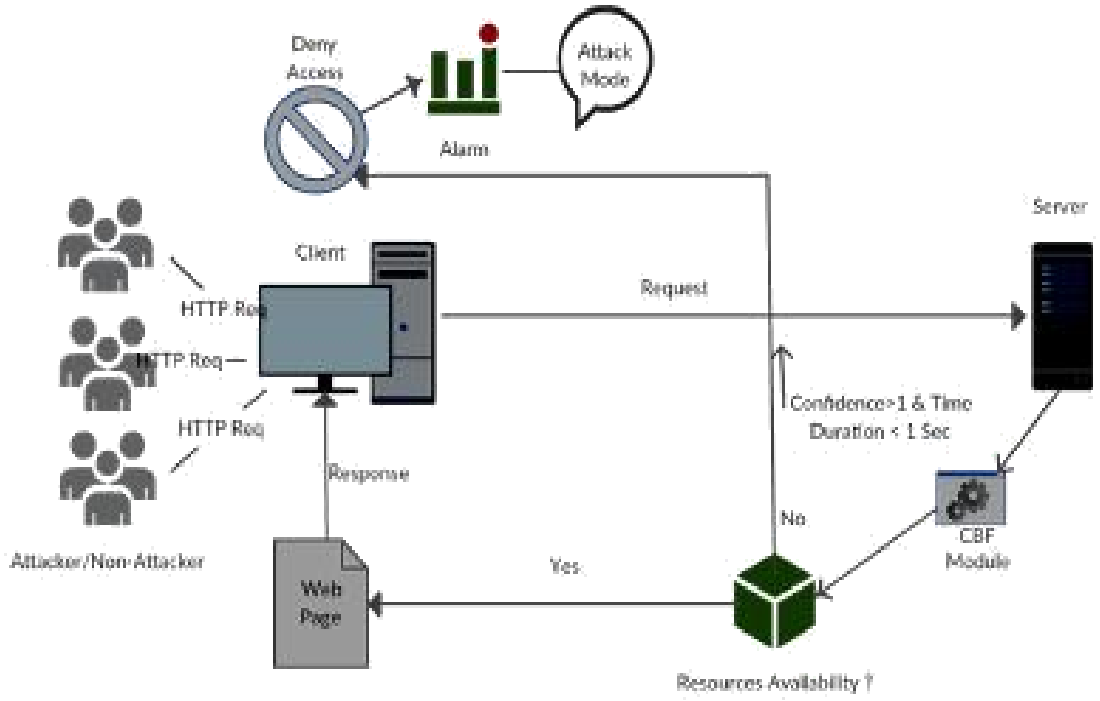

Figure 2: Architecture of Proposed System

This technique depends on the bundle recognition and obstructing the parcels utilizing limit. Examination of solicitation worth taking into account bundle checking is most vital part in this strategy (Luo and Chang, 2005).

The division of typical client and attacker depends on figuring of GRPS (GET Request Per Second) in light of the fact that ordinary client does not persistently ask for a same page in the meantime.

In this system demonstrate, every hub has a list which contain bundle data of packet source ID, destination ID, Flag and Ratio. Asset Analysis is a benchmark to check whether the Server has adequate held or sit out of gear assets to conquer a DDoS attack (Abhilash and Kumar, 2011).

Table 1: Packet Information

User Id	No.of requests	Source ID	Destination ID	Flag (0,1)	Ratio

In the above table, every hub has the bundle data and banner worth is 0 or 1. On the off chance that flag is 1 toss the bundle and flag is 0 means permit the parcel. Here flag is a paired segment to check whether the bundle is trusted one or not. In the event that it is now stamped as endowed one in any other hub then it will be checked by every single other hub in the middle of source and destination. If any source hub checked it as entrusted then all hubs will toss that bundle.

Detection of DDoS attack is done utilizing three stages and those are

1. Checking the typical condition of every system.
2. Defining the parameters and those are data appropriation of parcel header, the greatest worth, least estimation of activity, CPU utilization, Load, bundle size, checking of stream utilizing ridiculing location.
3. Calculating the limit worth by setting the Threshold value.

Total Workflow

To distinguish the early DDoS attacks, HTTP GET Flooding attack technique is connected. In HTTP GET flooding attack, every time system state is checked. Parameters are characterized to compute the limit esteem and those parameters are bundle header, the most extreme quality, least estimation of activity, CPU use, Load, parcel size, checking of stream utilizing satirizing location. Threshold value is set based on the capability of the server. On the off chance that the edge quality is less the mean worth, and then it can be happened the false-positive and on the off chance that it is more prominent than the mean quality, then it is attacker (Kumar and Selvakumar, 2011).

The general procedure of Resource Analysis system and CBF Technique can be isolated into two periods: intrusion and non-intrusion period. After HTTP Get flooding attack, asset investigation is connected under the non-intrusion period. CBF quality is ascertained in non-intrusion period and packet data table will be upgraded with most recent qualities.

Confidence is the ratio of number of requests arriving per second to the maximum Threshold Value.

$$C = R_i / T$$

Where C- Confidence or Ratio

R_i – Incoming Requests Per Second

T- Threshold Value

The Threshold is the metric that indicates the number of requests per second (RPS) that can be served by the Server application.

For example,1 million requests means 70 RPS. 100 million requests mean 7,000 RPS. A regular server can process a lot of requests during a whole day. But 2,000 RPS is a decent amount of load for a normal server for a regular service. (WordPress, 2013)

In Non-Intrusion period, as soon as the client or web browser sends the requests, the Confidence-Based Filtering Module will check the count of incoming requests and calculates the confidence value. Normally, in this period there is a fixed delay between consecutive requests.

If the Value of the Confidence is less than the value 1, then the client can be treated as Non-attacker and the Flag value is set to 0. The Asset Analysis is done to serve the client. If assets are adequate then Access Status is set to True and allow the users to have the access to the requested web pages.

An Intrusion or Attack period is a period where the attackers creating botnets

integrates their random number of requests along with the normal or legitimate users. In this case, the server is overwhelmed by the huge number of requests sent by the concurrent users with random or no delay.

The Confidence-Based Filtering Module will check the count of incoming requests and calculates the confidence value. Undoubtedly, the Value of the Confidence is more than 1, and the requests from these botnets arrive in less duration compared to the normal user requests. Hence the Flag value is set to 1, indicating the Attack Period True.

The Resource Analysis like the CPU load, CPU time, Memory, Process Time is also done now at this stage, to serve the requests as per the availability and if the intruders are requesting more than the allocated resources, the Access Status is set to False to deny their more incoming requests that are requesting massive resources.

Further an alarm is set to indicate the Emergency Signal to signify the Status of the Server being in Attack Mode.

The following figure 3 shows the workflow of the proposed system to detect whether the server is attack mode.

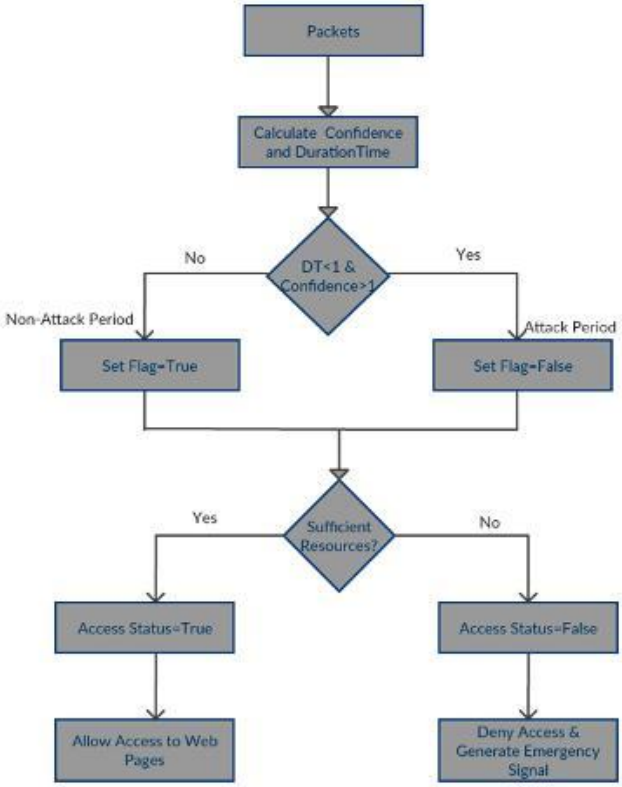

Figure 3: Total Workflow

V. IMPLEMENTATION

This DDoS System is implemented using NetBean 8.1 and Spring tool suite IDE. Apache tomcat 7.0 running as web server. Here Java SE, Servlet and Html are used as web technology. For showing robot attack, Swing technology is used. The result analysis is also given below.

GET Flooding can be separated by normal user and zombie PC attack through calculation of GRPS (GET Request per Second). A normal user in non-attack mode does not repetitively request a same page at the same time whereas a botnet in attack mode sends thousands of requests with no delay to flood the victim. (Choi.J,2013).

Figure 4 Home Screen to send requests both in attack and non-attack mode

Figure 5. Client Application to send requests in Normal Mode

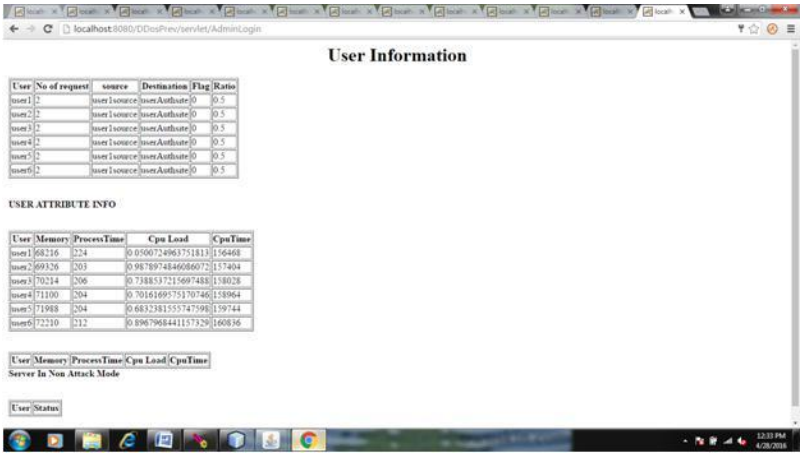

Figure 6. Server Application displaying the Status of Normal

Mode with Resource Information

Figure 7. User Interface to attack the server by integrating the attack requests with the normal requests

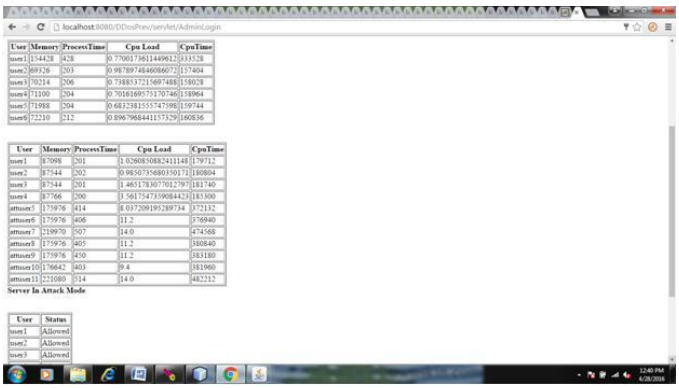

Figure 8. Server Application displaying the Status of Non-Attack Mode with Resource Information

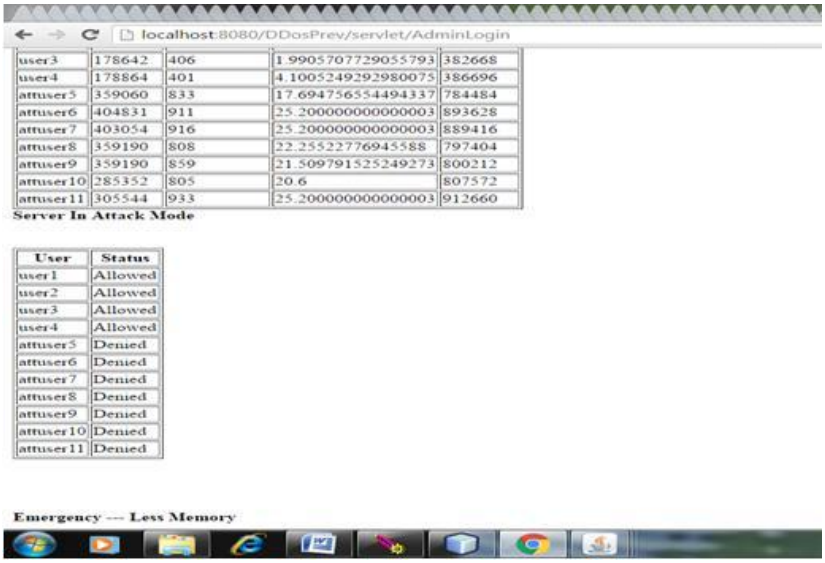

Figure 9. List of users allowed and denied with Status of Server being in Attack Mode and Emergency Signal to show insufficient resources

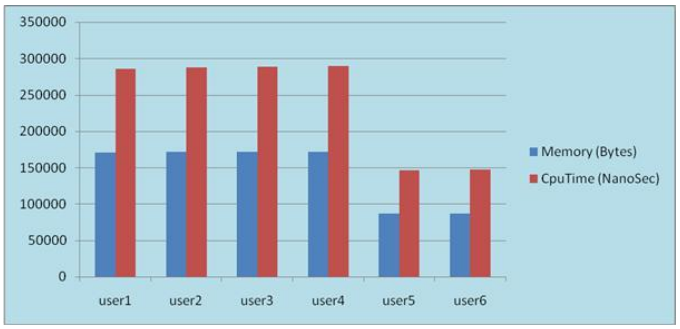

Figure 10. Graph Showing the consumption of Memory (in Bytes) and CPU Time (in NanoSec)I in Normal behaviour or Non-Attack Period

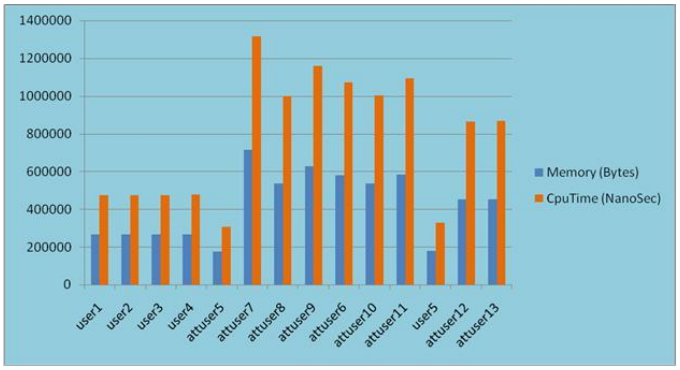

Figure 11. Graph Showing the consumption of Memory (in Bytes) and CPU Time (in NanoSec) in Attack Period

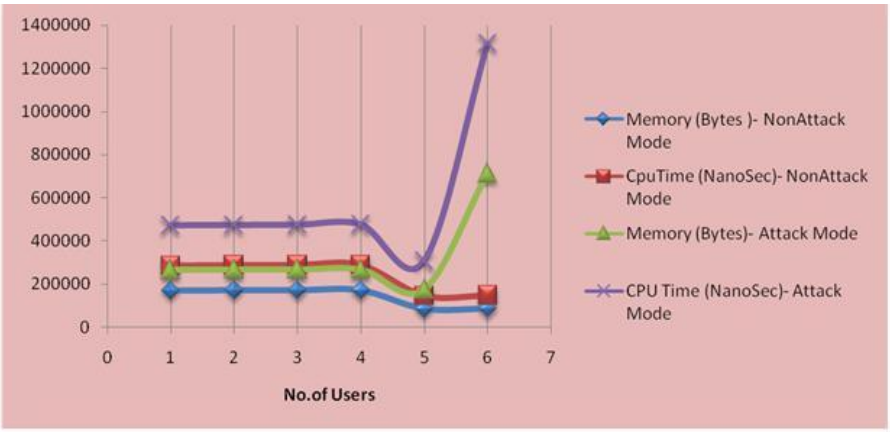

Figure 12. Comparision Graph Showing the consumption of Memory (in Bytes) and CPU Time (in NanoSec) in both Attack and Non-Attack Modes

VI. RESULT ANALYSIS

Recently, a number of research works have been done on DDoS Attack Defense in network. The resource allocation to defense the DDoS attack has become a major challenge.

To overcome these challenges, a HTTP GET flooding detection and Confidence-Based Filtering method for DDoS Attack Defense in network is proposed.

HTTP Get flooding attack is the most critical and frequently attempted attack. To overcome this attack an early stage HTTP GET Flooding Detection method is applied. The dynamic resource allocation is applied to automatically coordinate the available resources (CPU, Memory, I/O, Bandwidth) of a network to mitigate DDoS attacks on individual users.

After CBF (Confidence-Based Filtering) is calculated for each packet resource analysis is done to determine whether to discard it or not.HTTP Requests are served to the users until the allocated resources are exhausted even in case of non intrusion period. As soon it gets noticed that resources are worn out, it stops responding to the requests and deny the access to the web pages violating the unavailability of the server which is an intention of an attacker or botnet.

VII. CONCLUSION

DDoS assaults exhibit a genuine issue in the Internet and test its rate of development and ample acknowledgment by the overall population, suspicious government and private organizations. HTTP surge attacks are volumetric attacks, frequently utilizing a botnet "zombie armed force", a gathering of Internet-associated PCs. Each of which

has been malevolently assumed control, for the most part with the help of malware like Trojan Horses.

A modern Layer 7 attack, HTTP surges do not utilize twisted parcels, parodying or reflection strategies, and require less data transmission than different attacks to cut down the focused on location or server (Chang, 2000).

All things considered, they request more inside and out comprehension about the focused in the vicinity or application, and every attack must be uniquely created to be compelling. This makes HTTP surge attacks essentially harder to identify and obstruct (Kumar and Selvakumar, 2012).

Recently, a number of research works have been done on DDoS Attack Defense in network. The resource allocation to defense the DDoS attack has become a major challenge. To overcome these challenges, in this paper we proposed a HTTP GET flooding detection and Confidence-Based filtering method for DDoS Attack Defense in network. HTTP Get flooding attack is the most critical and frequently attempted attack. To overcome this attack an early stage HTTP GET Flooding Detection method is applied. The dynamic resource allocation is applied to automatically coordinate the available resources (CPU, Memory, I/O, Bandwidth) of a network to mitigate DDoS attacks on individual users. After resources allocated, CBF (Confidence-Based Filtering) is calculated for each packet, to determine whether to discard it or not.

REFERENCES

[1]. Aamir, Muhammad, and Muhammad Arif. "Study and Performance Evaluation on Recent DDoS Trends of Attack & Defense." International Journal of Information Technology and Computer Science (IJITCS) 5, no. 8 (2013): 54.

[2]. Rani, Rupa, and A. K. Vatsa. "CARD (Continuous and Random Dropping) based DRDOS Attack Detection and Prevention Techniques in MANET." International Journal of Engineering and Technology 2, no. 8 (2012): 1449-1456.

[3]. Chu, Weibo, Xiaohong Guan, John CS Lui, Zhongmin Cai, and Xiaohong Shi. "Secure Cache Provision: Provable DDOS Prevention for Randomly Partitioned Services with Replication." In Distributed Computing Systems Workshops (ICDCSW), 2013 IEEE 33rd International Conference on, pp. 58-63. IEEE, 2013.

[4]. Kavitha, C. "Prevention of Vulnerable Virtual Machines against DDOS Attacks in the Network.", IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 2, Apr-May, 2014.

[5]. Zakarya, Muhammad. "DDoS Verification and Attack Packet Dropping Algorithm in Network Computing." World Applied Sciences Journal 23, no. 11 (2013): 1418-1424.

[6]. Navaz, AS Syed, V. Sangeetha, and C. Prabhadevi. "Entropy based anomaly detection system to prevent DDoS attacks in network." International Journal of Computer Applications (0975–8887) Volume (2013).

[7]. Goyal, Upma, Gayatri Bhatti, and Sandeep Mehmi. "A Dual Mechanism for defeating DDoS Attacks in Network Computing Model." International Journal of Application or Innovation in Engineering & Management (IJAIEM) 2, no. 3 (2013).

[8]. Jeyanthi, N., N. Ch SN Iyengar, PC Mogan Kumar, and A. Kannammal. "An enhanced entropy approach to detect and prevent DDoS in network environment." International Journal of Communication Networks and Information Security (IJCNIS) 5, no. 2 (2013).

[9]. Charanya, R., M. Aramudhan, K. Mohan, and S. Nithya. "Levels of Security Issues in Network Computing." International Journal of Engineering and Technology 5 (2013).

[10]. Muthukumaravel, A., S. Prasanna, and S. Deepa. "Supporting Various Techniques to optimize and secure application performance in a Network Computing Security in a effective manner." International Journal of Emerging Technology and Advanced Engineering, ISSN: 2250-2459.

[11]. Dou, Wanchun, Qi Chen, and Jinjun Chen. "A confidence-based filtering method for DDoS attack defense in network environment." Future Generation Computer Systems 29, no. 7 (2013): 1838-1850

[12]. Yu, Shui, Yonghong Tian, Song Guo, and D. Wu. "Can we beat ddos attacks in networks?.", IEEE, 2013.

[13]. Choi, Junho, Chang Choi, Byeongkyu Ko, Dongjin Choi, and Pankoo Kim. "Detecting web based DDoS attack using MapReduce operations in network computing environment." Journal of Internet Services and Information Security 3, no. 3/4 (2013): 28-37.

[14]. Hashmi, Mohd Jameel, Manish Saxena, and Dhirendra B. Singh. "Intrusion Prevention System based Defence Techniques to manage DDoS Attacks." International Journal of Computer Science & Applications (TIJCSA) 1, no. 8 (2012): 2278-1080.

[15]. Lonea, Alina Madalina, Daniela Elena Popescu, and Huaglory Tianfield. "Detecting ddos attacks in network computing environment." International Journal of Computers Communications & Control 8, no. 1 (2012): 70-78.

[16]. L. Kleinrock, Queueing Systems. Wiley Interscience, 1975, vol. I:Theory.

[17]. Abhilash C. S., Sunil kumar P. V. (2011). Mitigation of DDOS (DDoS) Threats, *Conference on Advances in Computational Techniques (CACT)*.

[18]. Kumar, P. A. R., & Selvakumar, S. (2011). Distributed denial of service attack detection using an ensemble of neural classifier. *Computer Communications*, 34(11), 1328-1341.

[19]. Kumar, P. A. R., & Selvakumar, S. (2012). M2KMIX: identifying the type of high rate flooding attacks using a mixture of expert systems. *International journal of Computer Network and Information Security*, 4(1), 1.

[20]. https://wrongsideofmemphis.wordpress.com/2013/10/21/requests-per-second-a-reference

[21]. Luo, X., & Chang, R. K. (2005, February). On a New Class of Pulsing Denial-of-Service Attacks and the Defense. In *NDSS*.

[22]. Chang, R.K.C .(2000). Defending In opposition to Flooding Based Distributed Denial-of-Service Attacks: *A Tutorial, IEEE Commun. Mag.*, 40(10), 42-51.

AUTHORS PROFILE:

Dr. V. Naga Lakshmi is Head and Professor of Computer Science at GITAM University, Visakhapatnam, India. Her research interests include Cryptograph and Network Security, Database Security and Network Computing. She has 18 years of teaching and research and One year Industry experience. She has published more than 25 publications in International and National journals and Proceedings. She was the Organizing Chair of Technoholix-2009 and an active organizin gcommittee member for seminars, conferences, workshops of the department and institute. She also served as a member of PC in various International conferences, reviewer in many Journals and life member of CSI.

Shameena Begum is an Assistant Professor in Information Technology, Sasi Institute of Technology & Engineering, Tadepalligudem, India. Her research interests include Network Security, Computer Networks and Network computing. She has 12 years of Experience in teaching and One year in Industry. She received M. Tech degree and currently pursuing Ph.D. in GITA University, Visakhapatnam.