International Journal of Advanced Information Science and Technology (IJAIST) *ISSN: 2319:2682*
Vol.4, No.12, December 2015 DOI:10.15693/ijaist/2015.v4i12.76-82

HTTP GET Flooding Detection and Confidence-Based Filtering Method for DDoS Attack Defense in Networks

Dr.V.NagaLakshmi
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 is 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 and 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.**

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

.

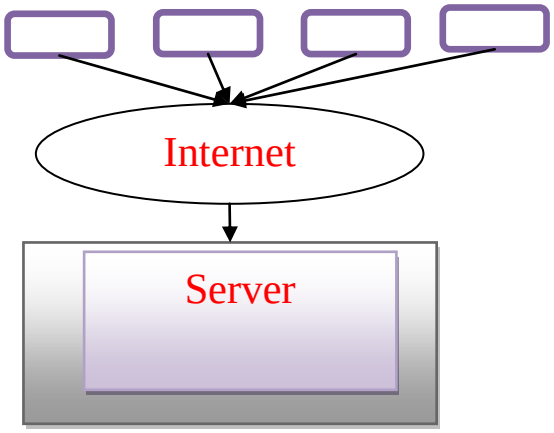

Figure 1. Client-Server Architecture

B. Security Attacks in Network

Client-Server security refers to a broad setof 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 networks 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-attackperiod, 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 concern about available resources. In client-server application systems the resource allocation is very important , but this paper 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

In HTTP Get flooding attack is the most critical and frequently attempted attacks, so this method is applied to detect the early DDoS attack. If this attack is not happen, then defiantly DDoS attack is happens. Resource Analysis is done to check whether the network has sufficient resources to prevent DDoS attack and main Quality of Services of user.

The overall process of Resource Analysis method can be divided into twoperiods: non-attack period and attack period and the overall process of CBF method can be divided into twoperiods: non-attack period and attack period.

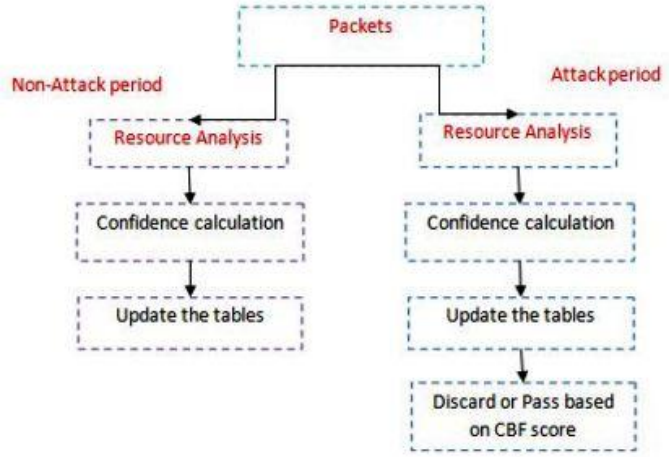

Figure 2: Overall Process

After HTTP Getflooding attack, resource analysis is applied under the non-attack period. CBF value is calculated in non-attack period and packet information table and TTL and minC value's table were updates with latest values. First the number of appearances of value pairs will be counted andtheir confidence values calculated. Then these confidence valuesare used to update packet information table and TTL and minC value's table. If the network has sufficient resources then only it go for CBF value calculation, otherwise it will wait or give an emergency signal to administrator.

A. HTTP GET Flooding Attack

In this paper, initially HTTP GET Flooding attack method is applied to detect the early DDoS attacks. In this network model, each node has list which contain packet information (packet source ID, destination ID, packet ID).

S.No.	ID	Source ID	Destination ID	Flag (0,1)
---	---	-----	----------	
---	---	-----	----------	
---	---	-----	----------	

Table 1: Packet Information

In the above table, each node has the packet information and flag value is 0 or 1. If flag is 0 discard the packet and flag is 1 means allow the packet. Here flag is a binary component to check whether the packet is trusted one or not. If it is already marked as entrusted one in any another node then it will check by all other nodes in between source and destination. If any source node marked it as entrusted then all nodes will discard that packet.

This method is based on the packet detection and blocking the packets using threshold. Analysis of request value based on packet checking is most important part in this method. Web server protection and traffic blocking is done by using the policy based threshold.

The division of normal user and attacker is based on calculation of GRPS(GET Request per Second) because normal user does not continually request a same page at the same time.

In Detection of DDoS attack is done using three steps and those are

1. Checking the normal state of each network.
2. Defining the parameters and those are information distribution of packet header, the maximum value, minimum value of traffic, CPU usage, Load, packet size, monitoring of flow using spoofing address.
3. Calculating the threshold value (using equation (1)).

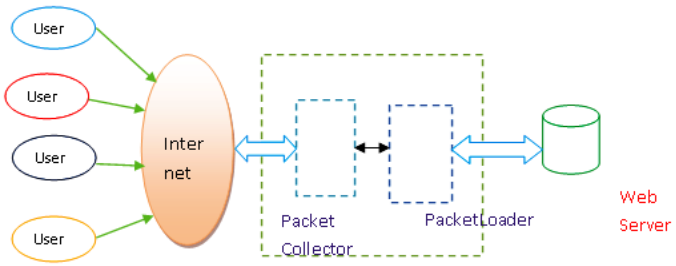

Figure 3: HTTP GET Flooding Attack

Traffic analysis is combined in parameters to improve the reliability of traffic features and this reliability is measured using extract parameter based on entropy statistical method. The threshold value is calculated using the following equation

$$TH(x) = \sum_{x=1}^{i} m_i \log m_i \qquad (1)$$

In equation (1), TH is the threshold value, mi is the probability mass function. mi gives the probability that a discrete random variable isexactly equal to some value.

If the threshold value is less the mean value, then it can be occurred the false-positive and if it is greater than the mean value, then it is attacker. The source address is get using the GRPS.

B. Resource Analysis

Resource Analysis is a benchmark to check whether the network has sufficient reserved or idle resources to overcome a DDoS attack. If the network has sufficient resources to overcome the DDoS attack, then CBF method is applied.

Let R be the resource analysis of a system and S is specific requirements of different resources, such as S =< CPU,memory, I/O, bandwidth >.

1. Resource Analysis for Non-attack Cases:

Let packet arrival rate as Pa, and the service rate as Ps. The ratio of the arrival rate and the service rate is known as utility rate. Utility rate is calculated using the following equation

$$P_k = \frac{P_a}{P_s} \qquad (2)$$

In equation (2), Pk is the probability of k arrivals fora given time interval and ifPk< 1 then the system is in a stable state.Based on queuing theory [16], we know the probabilityof the system stays state πk (namely, there are kpackets in the system) is

$$\Pi_0 = 1 - \frac{P_a}{P_s}$$

$$\Pi_k = \left(\frac{P_a}{P_s}\right)^k \Pi_0 \qquad (3)$$

The average time spent in the system is

$$T_n = \frac{1}{P_a - P_s} \qquad (4)$$

In equation (4), Tn meets users' expectations ofservice.We will use Tn as a benchmark of QoS for benignusers when the server is under a DDoSattack.

Confidence-Based Filtering Method for non-attacking cases:

The concept of confidence [11] reflects how much trust we can put on a correlation pattern between an attribute pair.Confidence is the frequency of appearances of attributes in the packet flows. The confidence for single attributes is calculated using the following equation:

$$C(P_i = p_{i,j}) = \frac{A(P_i = p_{i,j})}{A_a} \qquad (5)$$

In equation (5), C is confidence of single attribute and where i = 1, 2, 3, …, a, j = 1, 2, 3, …, ni. The confidence for double attributes is calculated using the following equation:

$$C(P_{i1} = p_{i1,j1}, P_{i2} = p_{i2,j2}) = \frac{A(P_{i1} = p_{i1,j1}, P_{i2} = p_{i2,j2})}{A_a} \quad (6)$$

In equation (6), i1 = 1, 2, 3, …, n, i2 = 1, 2, 3, …, n, j1 = 1, 2,3, …, n1, j2= 1, 2, 3, …, n2.

A	Number of the attributes
Pi	i-th attribute in the packet, ($1 \leq i \leq n$)
n_i	Number of values which attribute Pi can have
$P_{i,j}$	j-th value of attribute Pi, ($1 \leq j \leq ni$)
T	Time interval in packet flows
P	Packet in the packet flows
C	Confidence of attribute
minC	Minimum confidence value

Table 2: Key terms appeared in this paper.

In CBF method, each packet TTL value is extracted and stored in the table. The table format is given below

Packet ID	TTL	minC

Table 3: TTL and minC value's table

1. Start
2. Define Count = count the number of appearances of single attribute
3. T = threshold value
4. For each appearance of single attribute
5. {
6. Count= Count+1;
7. Calculate the C (confidence value) value using equation (1)
8. }
9. If (C < T) // confidence value is less than the threshold value
10. {
11. Select the single attribute
12. Merge single attribute to generate candidate attribute value pairs
13. Calculate the C value for candidate attribute value pairs using the equation (1)
14. Update the TTL and minC value's table
15. Allow the packets
16. Update the packet information table with flag = 1
17. }
18. Else
19. Discard
20. End

Algorithm 1: algorithm for CBF in non-attack period

In the above algorithm, threshold value is average value of all previous values. For each appearance of single attribute confidence value is calculated using the equation (6). Each those values are updated in TTL and minC value's table. If confidence values is less than the threshold value, those packets are allowed and packet information table is updated with flag=1.

2. Resource Analysis for Attacking Cases

In attacking case, the user can access the single server of multiple server form the clone. Let assume DDos attack is on multiple server. In a given time interval, the total number of arrivals to a victim is known as attack strength. Busy rate of multiple servers is calculated using the following equation

$$P_k = \frac{rP_a}{mP_s} \quad (7)$$

In equation (7), r is a real number, m is the number of multiple servers and r represents an attack strength as r times of the arrival rate of non-attack case.As previously discussed, in order to guarantee the QoSfor benign users during a DDoS attack, the condition ofEquation (5) has to be satisfied. Therefore,

$$\frac{1}{P_s} + \frac{1}{rP_a} \frac{(\frac{rP_a}{P_s})^m}{m!} \frac{\prod_0}{(1-\frac{rP_a}{mP_s})^2} \leq \frac{1}{P_s - P_a} \quad (8)$$

For simplicity, let

$$f(r,m) = \frac{P_a}{P_s} - (P_s - P_a)\frac{1}{P_s m!}\frac{(rP_a)^{m-1}}{(1-\frac{rP_a}{mP_s})^2}\frac{\prod_0}{} \quad (9)$$

In equation(9),π0 is calculated using equation (3) and this will work when m = 1,2,3…. If the equation is stratifies then the network has sufficient idle or reserved resources,which can be used to counter DDoS attacks.

Confidence-based filtering method in the attack period:

In attacking period, confidence vales are calculated using the equation (6) and those values are updated in TTL and minC value's table. The table has all the values which are calculated previously at other nodes. All the values are compared with minC value and if the values are less than allow the packets, otherwise discard the packets.

C. Total Workflow

To detect the earyly DDoS attacks, HTTP GET Flooding attack method is applied. In HTTP GET Flooding attack, each time network state is checked. Parameters are defined to calculate the threshold value and those parameters are packet header, the maximum value, minimum value of traffic, CPU usage, Load, packet size, monitoring of flow using spoofing address. Threshold value is calculated using the equation (1). If the threshold value is less the mean value, then it can be occurred the false-positive and if it is greater than the mean value, then it is attacker.

All the packets are extracted and those are divided into two periods. One is non-attack period and second one is attack period. In attacking period, initially resource are analyzed and if sufficient resource are there then CBF method is applied, otherwise emergency signal is send to server administrator. In CBF method, confidence value is calculated and packet information table and TTL and minC value's tables are updated. If a confidence value is less than the threshold value, those packets are allowed, otherwise discarded.

In non-attacking period, resource are analyzed and if sufficient resource are there then CBF method is applied, otherwise emergency signal is send to network administrator. Confidence vales are calculated and those values are updated in TTL and minC value's table.. All the values are compared with minC value and if the values are less than allow the packets, otherwise packets are discarded.

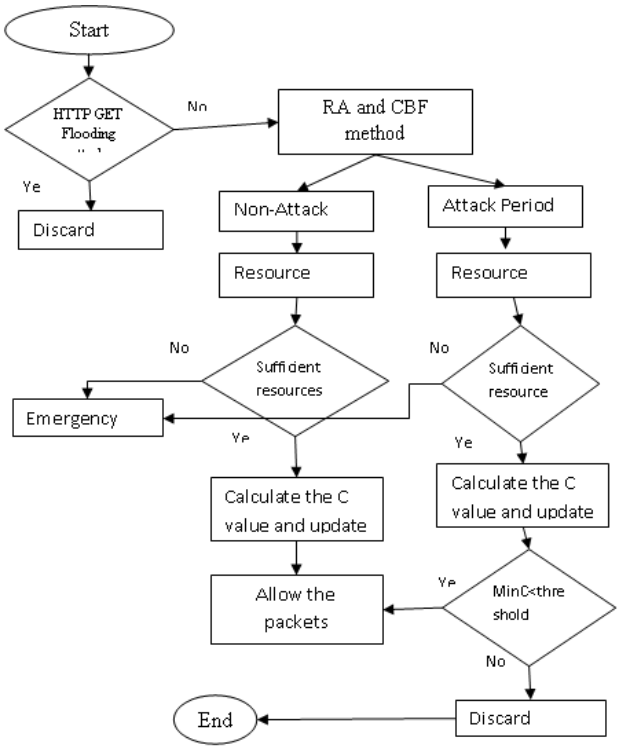

Figure 4: Total Workflow

V. CONCLUSION

Recently, a number of research works have been done on DDoS Attack Defense in network. The resource allocation to defense the DDoS attack is 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]. 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]. 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]. 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]. 5. Zakarya, Muhammad. "DDoS Verification and Attack Packet Dropping Algorithm in Network Computing." World Applied Sciences Journal 23, no. 11 (2013): 1418-1424.

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

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

Authors Profile

Dr.V. Naga Lakshmi is Head and Professor of Computer Science at GITAM University, Visakhapatnam, India. Her research interests include Cryptography and Network Security, Database Security and Network Computing. She has 16 years of teaching and research and one year Industry experience. She has published more than 20 publications in International and National journals and Proceedings. She was the Organizing Chair of Technoholix-2009 and an active organizing committee 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 10 years of Experience in teaching and One year in Industry. She received M. Tech degree and currently pursuing Ph.D. in GITAM University, Visakhapatnam.