Prevention of Attacks under DDoS Using Target Customer Behavior

K.Kuppusamy [1] and S.Malathi [2]

**[1] Department of Computer Science &Engineering, Alagappa University
Karaikudi, Tamil Nadu, India**

**[2] Research Scholar, Manonmaniam Sundaranar University
Tirunelvelli, Tamil Nadu, India**

Abstract

The possibility of sharing information through networking has been growing in geometrical progression. In this connection it is to be noted network attacks, in other words, DDoS attacks also are growing in equal proportion. Sharing of information is being carried out by means of server and client. The client requests for the data from the server and the server provides the response for the client-request. Here the client can violate the server performance by sending continuous or anomaly requests. The result is the server performance becomes degraded. This paper discusses how best the degradation of the performance can be prevented using some algorithm proposed in the methodology. In this work the blocking is done using a different mechanism based on the category of the client.

Keyword: *Server, Client, Response, Request Degradation, Category,*

1. Introduction

Of the several means for communication, most commonly used technology is the networking. The information is shared by the methodology of sending and receiving the request and response respectively. This is done by using client-server architecture.

In this client-server architecture, the client can send requests to the server and the server accepts the request, and provides response to the request. In the case of multiple requests to the same server, the server responds to the client request in a FIFO manner. In this case, the server performance can be degraded due to multiple requests sent to the server by the clients. This is termed as **attack.** This kind of attack may be avoided by means of the technique termed as **DDoS (Distributed Denial of Service).**

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its legitimate users. It generally consists of the concerted efforts of a person or persons to prevent an Internet site or service temporarily or indefinitely from functioning efficiently. The Denial of Service Attack (DoS attack) means that the server will not be able to provide response to the client request. The clients who make multiple requests continuously are blocked and they are prevented from accessing to the server.

In paper [1], it was discussed the client is blocked based upon the number of accesses made by the client. If the number of access exceeds a certain limit, the server would stop responding to the client and thus the client is totally blocked. For example, if this is to be implemented on a commercial organization, there is a possibility of blocking the genuine customer also. Thus this would lead to genuine customer dissatisfaction.

To avoid this kind of dissatisfaction, this paper provides an efficient methodology to block the user based on the category consideration. In that case the user gets response according to the categorization.

There is more number of clients accessing to the server seeking immediate response to their requests but the website is only one. In this case the server begins to provide response based on the client categorization. That is, if the client is an authorized user, then they are provided with the response for all their requests. Otherwise, they are blocked from accessing to the server. Thus the hackers can be easily identified and they are blocked from access.

The proposed methodology not only prohibits the access of unauthorized users or the non-registered clients, but also prohibits the access of authorized users those who send multiple requests often. This is the core of the problem. Thus the first step in the proposed methodology

Copyright (c) 2012 International Journal of Computer Science Issues. All Rights Reserved.

is categorizing users as authorized user or unauthorized user. The next step is providing response to the authorized users and blocking the unauthorized users. The unauthorized users are further categorized based on two types of counts time-namely, access counts and warning counts. The access count users can be permitted to have access to the server even though they are considered unauthorized users. Thus by implementing this methodology in an organization would help provide both mechanisms such as preventing the unauthorized users and also preventing the server performance becoming degraded.

2. Related work

When the number of users gets increased accessing to the websites, the performance of the server gets down and the response time gets increased. When the process becomes slow, the ratio of the users accessing to the site also goes down. This situation may also happen due to the attack by some unwanted users called as Hackers or Intruders. Hackers are the persons who abuse the server bandwidth unnecessarily in order to make the server performance low and thus make the site useless.

In paper [1], it was implemented a special kind of technique to recognize the attack carried out by the hackers and block them from using the site. This is termed as Denial of Services. And this is carried out among the web users and is commonly referred to as Distributed Denial of Services (DDoS). To improve server performance and to deny the accessibility permissions of the hackers are proposed in this paper.

Unicast reverse path forwarding (uRPF) [2] requires that a packet is forwarded only when the interface that the packet arrives on is exactly the same used by the router to reach the source IP of the packet. If the interface does not match, the packet is dropped. While simple, the scheme is limited given that Internet routing is inherently asymmetric, i.e., the forward and reverse paths between a pair of hosts are often quite different. In Hop-Count Filtering (HCF) [3], each end system maintains a mapping between IP address aggregates and valid hop counts from the origin to the end system. Packets that arrive with a different hop count are suspicious and are therefore discarded or marked for further processing.

In [5], Li et al., described SAVE, a new protocol for networks to propagate valid network prefixes along the same paths that data packets will follow. Routers along the paths can thus construct the appropriate filters using the prefix and path information. Bremler-Barr and Levy proposed a spoofing prevention method (SPM) [6], where packets exchanged between members of the SPM scheme carry an authentication key associated with the source and destination AS domains.

Recently, there is an anecdotal evidence of attackers to stage attacks utilizing bot-nets1 [7]. In this case, since the attacks are carried out through intermediaries, i.e., the compromised .bots, it is tempting to believe that the use of IP spoofing is less of a factor than previously. However, recent studies present evidence to the contrary and show that IP spoofing is still a commonly observed phenomenon [8], [9].

Man-in-the-middle attacks, such as variants of TCP hijack and DNS poisoning attacks [10], [11], are carried out by the attacker masquerading as the host at the other end of a valid transaction.

One of the factors that complicate the mechanisms for policing such attacks is IP spoofing, the act of forging the source addresses in IP packets. By masquerading as a different host, an attacker can hide its actual identity and location, rendering source-based packet filtering less effective. It has been shown that a large part of the Internet is vulnerable to IP spoofing [12]

The idea of IDPF is motivated by the work carried out by Park and Lee [13], which was the first effort to evaluate the relationship between topology and the effectiveness of route, based packet filtering. The authors stated that packet filters that are constructed based on the global routing information can significantly limit IP spoofing when deployed in just a small number of ASes. In this work, they extend the idea and demonstrate that filters that are built based on local BGP updates can also be effective.

Distributed Denial of Service (DDoS) attacks pose an increasingly grave threat to the Internet, as evidenced by recent DDoS attacks mounted on both popular Internet sites [15] and the Internet infrastructure [14]. Alarmingly, DDoS attacks are observed on a daily basis on most of the large backbone networks [4].

The Bogon Route Server Project [16] maintains a list of bogon network prefixes that are not routable on the public Internet. Recently IP trace-back mechanisms based on probabilistic packet marking (PPM) have been proposed for achieving trace-back of DoS attacks.

Effective mitigation of denial of service (DoS) attack is a pressing problem on the Internet. In many instances, DoS attacks can be prevented if the spoofed source IP address

Copyright (c) 2012 International Journal of Computer Science Issues. All Rights Reserved.

is traced back to its origin which allows assigning penalties to the offending party or isolating the compromised hosts and domains from the rest of the network. Recently IP trace-back mechanisms based on probabilistic packet marking (PPM) have been proposed for achieving trace-back of DoS attacks.

In [17], it shows the attacker's ability to inject misleading information—and give a comprehensive analysis of the effectiveness of PPM under single-source and distributed DoS attacks, complemented by numerical evaluations. They remark that PPM is not perfect and suffers under two additional they access (they are not unique to PPM, however, and are shared by the other approaches).

First, PPM is reactive in the sense that damage must occur before corrective actions— including source identification—can be undertaken by the victim. Second, PPM does not scale they all under distributed DoS (DDoS) attacks in the sense that the more hosts an attacker is able to compromise and use as a distributed attack site, the greater the effort needed (approximately proportional) to identify the attack sites.

Firewalls offer a protection for private networks against both internal and external attacks. However, configuring firewalls to ensure the protections is a difficult task. The main reason is the lack of methodology to analyse the security of firewall configurations. IP spoofing attack is an attack in which an attacker can impersonate another person towards a victim.

Also in the paper [17], it shows that probabilistic packet marking—of interest due to its efficiency and implement ability vis-à-vis deterministic packet marking and logging or messaging based schemes—suffers under spoofing of the marking field in the IP header by the attacker which can impede trace back by the victim.

It also shows that there is a trade-off between the ability of the victim to localize the attacker and the severity of the DoS attack, which is represented as a function of the marking probability, path length, and traffic volume. The optimal decision problem—the victim can choose the marking probability whereas the attacker can choose the spoofed marking value, source address, and attack volume—can be expressed as a constrained mini-max optimization problem, where the victim chooses the marking probability such that the number of forgeable attack paths is minimized.

Here it shows that the attacker's ability to hide his location is curtailed by increasing the marking probability; however, the latter is upper-bounded due to sampling constraints. In typical IP internets, the attacker's address can be localized to within 2–5 equally likely sites which render PPM effective against single source attacks. Under distributed DoS attacks, the uncertainty achievable by the attacker can be amplified, which diminishes the effectiveness of PPM.

Denial of service (DoS) is a pressing problem on the Internet as evidenced by recent attacks on commercial servers and ISPs and their consequent disruption of services [18]. DoS attacks [19], [20], [21], [22], [23], [24] consume resources associated with various network elements—e.g., The servers, routers, firewalls, and end hosts—which impede the efficient functioning and provisioning of services in accordance with their intended purpose.

A number of recent works have studied the problem of tracing the physical source of a DoS attack [22]. Several types of DoS attacks have been identified [18], [20], [22],[23] with the most basic DoS attack demanding more resources than the target system or network can supply. Resources may be network bandwidth, file system space, processes, or network connections [22]. While host-based DoS attacks are more easily traced and managed, network-based DoS attacks which exploit their accessibility of the TCP/IP protocol suite represent a more subtle and challenging threat [22]. Network-based DoS attacks, by default, employ spoofing to forge the source address of DoS packets to hide the identity of the physical source [24].

During a DoS attack, an attacker may try to gauge the impact of the attack using various service requests including them and ICMP echo requests. Thus, logging of such events and activities can reveal information about the attacker's source. The victim uses information inscribed in packets to trace the attack back to its source. In both methods, overhead in the form of variable-length marking fields that depend on path length or traffic overhead due to extra messaging packets are incurred.

The inter-domain packet filter (IDPF) to mitigate the level of IP spoofing on the internet was proposed in the paper [22]. IDPFs are constructed from the information implicit in BGP route updates and are deployed in network border routers and also the proposed and studied an inter-domain packet filter (IDPF) architecture as an effective countermeasure to the IP spoofing-based DDoS attacks. IDPFs rely on BGP update messages exchanged between neighboring as is on the Internet to infer the validity of source address of a packet forwarded by a neighbor. They stated that IDPFs

Copyright (c) 2012 International Journal of Computer Science Issues. All Rights Reserved.

can be easily deployed on the current BGP-based Internet routing architecture.

In the latter, with a certain probability a packet—however formatted by the attacker—will travel through untouched, which can impede the victim's ability to identify the true attack path. More generally, the number of forgeable paths that are from an information-theoretic point-of-view indistinguishable with respect to their validity from the true attack path can further render source identification difficult if their numbers are large.

Probabilistic packet marking [25] achieves the best of both worlds—space efficiency in the form of constant marking field and processing efficiency in the form of minimal router support—at the expense of introducing uncertainty due to probabilistic sampling of a flow's path. The latter has two important, and opposing, effects: (a) discovery of correct path information by sampling which aids the victim's objective of trace-back, and (b) injection of corrupted information by the attacker.

In this paper some more improvements with special features have been proposed for discussion.

3. Methodology

3.1 Proposed Method

The aim of the proposed work is to prevent the attack made on the server by the client by accessing the server continuously. The summary of the work is as follows:

In the research paper [1], it was discussed how the unauthorized clients can be blocked based on the number of accesses made on the server. Thus to overcome this kind of problem it is proposed a more efficient methodology to block the users based upon the category. The functionality of our methodology is described as follows:

A database is maintained continuously between the server and the client, which is used to maintain the record about the clients. With the help of this database, the server can easily determine the category of the client. That is, if the entry of the client is found in the database means, they are considered to be registered client. Otherwise, they are considered to be unregistered client. Thus the first step of maintaining the database provides the way to analyse and categorize the client.

{x: / x is a set of all registered users}

Based upon the category of the client, the process is to be proceeded. The server collects the requests from the client and it can process the request and provide the response to the client. This process is carried out normally when the server process minimum number of client request.

In case of peak hours of the server, the process is carried out as follows: In the peak period of the server, the client request is analysed before it is to be processed. If the client sends the request for the first time or if the client sends the request with proper interval of the time period, it is to be considered as normal request and this is to be processed by the server.

In case, the client sends the request continuously during this peak period, then the client is considered to be the anomaly client and the request is considered to be the anomalous request or attacks.

The next step of the proposed work is to categorize the anomaly clients who send the attack. This is carried out with the help of the database maintained in the first step. Based upon the entry in the database, the client category is detected whether they are registered client or non-registered client.

In the case of non-registered client, they are blocked temporarily until the peak period is over. In case of registered client, the client is provided with response in spite of the peak period. In the proposed methodology, two types of counts are maintained. These are **Access Count** and **Warning Count**.

The ***Access Count*** is the count that can be incremented every time when the client sends the request. The **Warning Count** is the count that can be incremented once when the unregistered client sends anomalous request.

The non-registered client can be blocked temporarily and the access count is incremented by one along with the warning count during the peak period. After the peak period of the server, the client can be unblocked and they are provided with the response. In this kind of processing, the unregistered client can be blocked permanently when the warning count reaches certain limit. Otherwise, their request is to be processed and the response is provided to the client.

Block_list=access_count(Warning_count=threshold_limit)

Copyright (c) 2012 International Journal of Computer Science Issues. All Rights Reserved.

This proposed methodology consists of algorithm to maintain the user list and to prevent the attacks. The algorithm named Modified GI time frequency Algorithm and its explanation is given below.

3.2 Algorithm

```
--------------------------------------------------------------------------
Modified GI time frequency Algorithm
--------------------------------------------------------------------------
Step-1: Database Maintenance
Maintain the user list, X
?(X) =set of all registered users

Step-2: Analyse the User
Get the usemame of the incoming user.
User_Name=name of the incoming user
Match it with the user list in the database
For i=0 to X.count
    If User_Name=X(i).Name then
X.Access_Count++
Status="Registered"
    Else
X.Access_Count++
Status="Unregistered"
    End if
Next

Step-3: Response to the Request
If Status="Registered" then
Process the Request and send the Response
End if
If Status="Unregistered" then
            Add name to the warning list, W
            W.Name=User_Name
            W.warning_count++
If W.warning_count < Threshold_Value
If Server_peak_period=True
    Add User to Temp_Blocked List
    Temp_Block=User_name
End if
Else
            Block the user permanently
            P_Block=User_name
End if
If Server_peak_period ! = True
Unlock the user in Warning list, W
W.Name.Status=Unlock
Process the Request and the Response
End if
End if
-----------------------------------------------------------------------------
```

3.4 Block Diagram

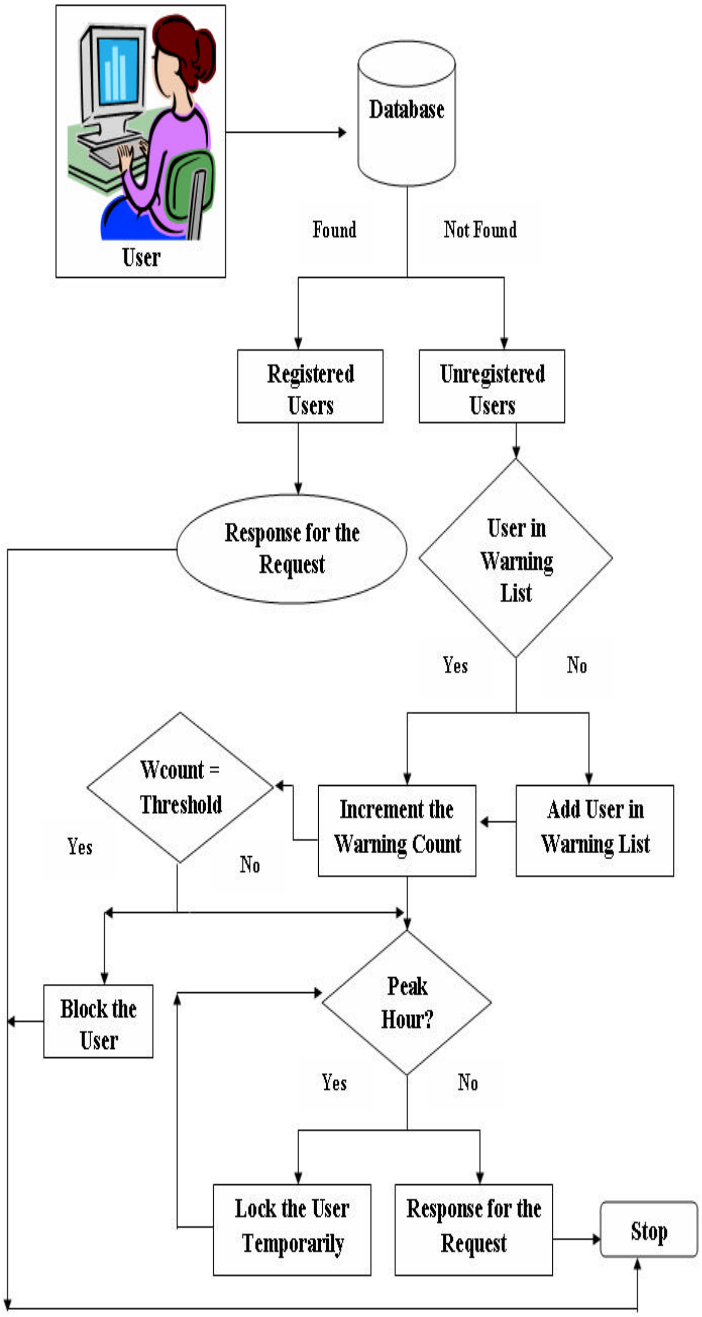

Fig. 1 prevention of attacks under DDoS

3.3 Algorithm Explanation

Thus in this algorithm, there exist three steps to prevent the attacks such as follows: In the first step, the user list is

Copyright (c) 2012 International Journal of Computer Science Issues. All Rights Reserved.

maintained in the database which would help the server to keep track of the registered client.
The second step is the analysis of user. The user is analysed with the help of the database list. Based on the analysis report, the third step is executed as follows: If the client is registered one, then they are to be provided with correct response, in spite of the business peak hours.

If the client is unregistered, then the peak hour is taken into consideration. If the requested time is the server peak hour, then the client is added in the warning list with incremented warning count. After the peak hours, the user in the warning list is taken out and the warning is compared with the threshold value. If the value matched, then the user is added into the blocked list. Otherwise, the user is provided with proper response.

4. Experimental results

The experimental result of this paper is carried out by implementing the algorithm in a suitable area such as in the commercial website. In this commercial site, we categorize the user into two groups such as: Registered Users and non-Registered Users.

First, the Registered Users are allowed to access the site. They provide the request and wait for the response. To this kind of user, the server provides response without analyzing the request. For each and every request of the registered users, the responses are provided.

After this, the second category of users namely unregistered users are allowed to access to the server. If this kind of unauthorized user is found accessing to the server during the peak hour, his request is temporarily blocked and this client is added in the list of **warning count.** These users are again monitored whether they exceed the threshold limit. If they found so, they are categorized under block list permanently. If they are found accessing to the site with in the threshold limit, they are allowed to have access to the site.

Thus the experimental setup was constructed and the demonstration was made and the entry is noted to identify the difference between the attacks made by both kinds of users.

5. Conclusion

The aim of the paper is to propose an efficient methodology to prevent the attack on server performance and to improve the reliability on the clients. To implement this, an algorithm is proposed to categorize the client and analyse the type of request. Based upon the analysis report, the user is blocked or provided with proper response.

This methodology is well suited for an organization where they require both the protection and also customer responsibility. Thus the proposed algorithm is suitable for satisfying the organization's requirements.

Thus this paper makes an attempt to provide an efficient and well suitable algorithm to identify the attack or threat made by the user on server performance and prevent the server from that kind of attack. In future, this algorithm can be enhanced with proper steps to satisfy large number of requests.

References

[1] Dr.K.Kuppusamy and S.Malathi, "An Effective Prevention of Attacks using GI Time Frequency Algorithm under DDoS", IJNSA journal, Vol. 3, No. 6, November 2011, PP. 249-257.

[2] Team Cymru Inc "Bogon route server project", http: //www.cymru.com/BGP/bogon-rs.html.

[3] Kihong Park, Heejo Lee, "On the Effectiveness of Probabilistic Packet Marking for IP Traceback under Denial of Service Attack", Network Systems Lab, Department of Computer Sciences, Purdue University, West Lafayette.

[4] Craig Labovitz, Danny McPherson and Farnam Jahanian, "Infrastructure attack detection and mitigation", ACM SIGCOMM 2005 conference, August 2005.

[5] J. Li, J. Mirkovic, M. Wang, P. Reiher and L. Zhang, "SAVE:Source Address Validity Enforcement protocol", In IEEE INFOCOM, Vol.6, No.2, June 2002, pp. 81-95.

[6] Bremler-Barr and H. Levy, "Spooling prevention method", In Proc. IEEE INFOCOM, 2005, vol.1.

[7] Srikanth Kandula, Dina Katabi, Matthais Jacob and Arthur Berger, "Surviving Organized DDoS Attacks that Mimic Flash Crowds", NSDI'05 Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation, 2005, Vol.2, PP 287 – 300.

[8] D. Moore, G. Voelker and S. Savage "Inferring internet Denial-of-Service activity", In proceedings of 10th Usenix Security Symposium, August 2001, PP.9-22.

[9] R. Pang, V. Yegneswaran, P. Barford, V. Paxson and L. Peterson. "Characteristics of internet background radiation", In Proceedings of ACM Internet Measurement Conference, October 2004.

[10] M. Dalal, "Improving TCP's robustness to blind in-window attacks", Internet- Draft, May 2005, work in progress.

Copyright (c) 2012 International Journal of Computer Science Issues. All Rights Reserved.

[11] J. Stewart, “DNS cache poisoning - the next generation”, Technical report, LURHQ, January 2003.

[12] R. Beverly and S. Bauer. “The Spoofer Project: Inferring the extent of Internet source address filtering on the internet”, In Proceedings of Usenix Steps to Reducing Unwanted Traffic on the Internet Workshop SRUTI'05, 2005, PP.53-59.

[13] K. Park and H. Lee, “On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets”, In Proceedings of ACM SIGCOMM,2001, Vol. 31, Issue .4, PP. 15-26.

[14] F.Baker, “Requirements for IP version 4 routers”, RFC 1812, 1995.

[15] C.Jin, H.Wang, and K. Shin, “Hop-count filtering: an effective defense against spoofed ddos traffic”, In Proceedings of the 10th ACM conference on Computer and communications security, October 2003, PP. 30-41.

[16] Ryan naraine, “Massive DDoS attack hit DNS root servers”, http://www.internetnews.com/dev-news/article.php/1486981, October 2002.

[17] Matt Richtel, “Yahoo attributes a lengthy service failure to an attack”, http://partners.nytimes.com/library /tech/00/02/biztech/articles/08yahoo.html , February 2000.

[18] Lee Garber, “Denial-of-service attacks rip the Internet,” Computer, April 2000, Vol.33, No. 4, pp. 12–17.

[19] John Elliott, “Distributed denial of service attack and the zombie ant effect”, IT Professional, March/April 2000, pp. 55–57.

[20] Jari Hautio and Tom Weckstrom, “Denial of service attacks”, March 1999, http://www.hut.fi/u/tweckstr/hakkeri/DoS paper.html.

[21] John D. Howard, An Analysis of Security Incidents on the Internet, Ph.D. thesis, Carnegie Mellon University, Pittsburgh, USA, Aug. 1998.

[22] Zhenhai Duan, Xin Yuan and Jaideep Chandrashekar, “Constructing Inter-Domain Packet Filters to Control IP Spoofing Based on BGP Updates”, 25th IEEE International Conference on Computer Communications. Proceedings (2006), pp. 1-12.

[23] Computer Emergency Response Team, “Denial of service,” Feb. 1999, Tech Tips, http://www.cert.org/tech tips/denial of service.html.

[24] Computer Emergency Response Team (CERT), “CERT Advisory CA-2000-01 Denial-of-service developments,” 2000, http://www.cert.org/advisories/CA-2000-01.html.

[25] Night Axis and Rain Forest Puppy, “Purgatory 101: Learning to cope with the SYNs of the Internet, Some practical approaches to introducing accountability and responsibility on public internet”, 2000, http://dl.packetstormsecurity.net/papers/contest/RFP.txt .

Dr.K.Kuppusamy is working as a Professor in the Department of Computer Science and Engineering, Alagappa University, Karaikukdi, Tamilnadu, India. He received his Ph.D in Computer Science and Engineering from Alagappa University, Karaikudi, Tamilnadu in the year 2007. He has 2 4 years of teaching experience at PG level in the field of Computer Science. He has published many papers in International & National Journals and presented in National and International conferences. His areas of research interests include Information/Network Security, Algorithms, Neural Networks, Fault Tolerant Computing, Software Engineering and Optimization Techniques.

Mrs.S.Malathi is working as an Assistant professor in the Department of Computer Science, Rabiammal Ahamed Maideen College, Tiruvarur, Tamilnadu, India. She has 13 years of teaching experience in the field of Computer Science. She has guided around 10 M.Phil., scholars. She has published one book and more research papers. Her area of interest is Network Security.

Copyright (c) 2012 International Journal of Computer Science Issues. All Rights Reserved.