Performance Analysis on Web based traffic control for DDoS attacks

S.Palanivel Rajan
Assistant Professor,
Department of Electronics & Communication Engineering,
M.Kumarasamy College of Engineering,
Karur, Tamil Nadu, India.
palanivelrajanme@gmail.com

S.Vijayprasath
Assistant Professor,
Department of Electronics & Communication Engineering,
M.Kumarasamy College of Engineering,
Karur, Tamil Nadu, India.
vijayprasaths.ece@mkce.ac.in

Abstract— Increase in the usage of internet from mailing a friend to e-learning, e-commerce, e-medicine, internet have tremendous growth as well as flaws such as raise in internet traffic leading to congestion .There are information security related active attack which cause internet traffic and make a resource unavailable to user . DoS and DDoS are an active attack that threatens the availability of a resource. In this proposed work we emphasis on how to overcome the traffic caused by DDoS attack. To mitigate the effect of DDoS we have used signature that is been generated whenever a client is logging in. Signature uses a lightweight hash algorithm which has an advantage of reduction in number of codes used with a lower development cost. Log is created for each operation on network and this file can be kept at any location. Also we have situation where traffic is completely controlled by limiting user's request/response. There is a backend Database used for holding information regarding users.

Keywords* — *Lightweight hash algorithm, service signature verification.

INTRODUCTION

Increase in the usage of internet

The internet is a global system of interconnected computer networks that use the standard Internet protocol suite (often called TCP/IP, although not all applications use TCP) to serve billions of users worldwide. It is a *network of networks* that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic, wireless and optical networking technologies. The Internet carries an extensive range of information resources and services, such as the inter-linked hypertext documents of the World Wide Web (WWW) and the infrastructures support email.

Most traditional communications media including telephone, music, film, and television are reshaped or redefined by the Internet, giving birth to new services such as Voice over Internet Protocol (VoIP) and Internet Protocol Television (IPTV). Newspaper, book and other print publishing are adapting to site technology, or are reshaped into blogging and web feeds. The Internet has enabled and accelerated new forms of human interactions through instant messaging, Internet forums, and social networking. Online shopping has boomed both for major retail outlets and small artisans and traders. Business-to-business and financial services on the Internet affect supply chains across entire industries [9]. As Internet is increasingly being used in almost every aspect of our lives, it is becoming a critical resource whose disruption has serious implications. Blocking availability of an Internet service may imply large financial losses, as in the case of an attack that prevented users from having steady connectivity to major e-commerce Web sites such as Yahoo, Amazon, eBay, E*Trade, Buy.com, ZDNet and CNN [12]. Despite substantial discussion of the Internet's impact on individual activities, there is an absence of a theoretically grounded measure of Internet usage for the provisioning of information required by decision-makers [11].

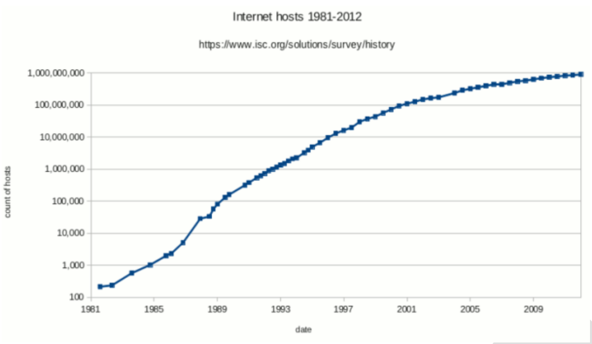


Fig. 1. Internet Usage(1981-2012)

DDoS

Distributed Denial of service (DDoS) attacks is designed to disrupt network services, by intentionally blocking or degrading the available resources used by them. One of the major problems for DDoS detection methods is the difficulty of differentiating DDoS attack packets from legitimate packets [13], since attackers mimic their attack traffic amongst legitimate traffic in order to hide their attack. This makes DDoS attacks a very serious threat to computers users [14]. A Distributed Denial of Service (DDoS) Attack is composed of four elements, as shown in *Fig. 2*.

- The real attacker.

- The handlers, which are compromised hosts with a special program running on them, capable of controlling agents.

- The attack daemon agents or zombie hosts, who are compromised hosts that are running a special program and are responsible for generating a stream of packets towards the intended victim. Those machines are commonly external to the victims own network, to avoid efficient response from the victim, and external to the network of the attacker, to avoid liability if the attack is traced back.

- A victim or target host.

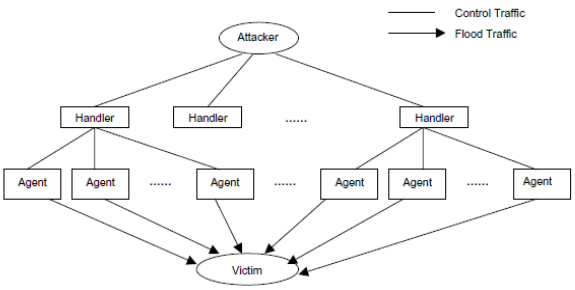


Fig. 2. Architecture of DDoS attack

The following steps take place while preparing and conducting a DDoS attack:

1. *Selection of agents*: The attacker chooses the agents that will perform the attack. These machines need to have some vulnerability that the attacker can use to gain access to them. They should also have abundant resources that will enable them to generate powerful attack streams. At the beginning this process was performed manually, but it was soon automated by scanning tools.

2. *Compromise:* The attacker exploits the security holes and vulnerabilities of the agent machines and plants the attack code. Furthermore he tries to protect the code from discovery and deactivation. Self propagating tools such as the Ramen worm and Code

Red soon automated this phase. The owners and users of the agent systems typically have no knowledge that their system has been compromised and that they will be taking part in a DDoS attack. When participating in a DDoS attack, each agent program uses only a small amount of resources (both in memory and bandwidth), so that the users of computers experience minimal change in performance.

3. *Communication:* The attacker communicates with any number of handlers to identify which agents are up and running, when to schedule attacks, or when to upgrade agents. Depending on how the attacker configures the DDoS attack network, agents can be instructed to communicate with a single handler or multiple handlers. The communication between attacker and handler and between the handler and agents can be via TCP, UDP, or ICMP protocols.

4. *Attack*: At this step the attacker commands the onset of the attack. The victim, the duration of the attack as well as special features of the attack such as the type, length, TTL, port numbers etc, can be adjusted. The variety of the properties of attack packets can be beneficial for the attacker, in order to avoid detection.

DoS attacks based on protocol features take advantage of certain standard protocol features. For example several attacks exploit the fact that IP source addresses can be spoofed. Several types of DoS attacks have focused on DNS, and many of these involve attacking DNS cache on name servers. An attacker who owns a name server may coerce a victim name server into caching false records by querying the victim about the attackers own site [18].

Distributed denial-of-service (DDoS) attacks pose an immense threat to the Internet, and many defense mechanisms have been proposed to combat the problem. Attackers constantly modify their tools to bypass these security systems, and researchers in turn modify their approaches to handle new attacks. The DDoS is quickly becoming more and more complex, and has reached the point where it is difficult to see the forest for the trees. On one hand, this hinders an understanding of the DDoS phenomenon. The variety of known attacks creates the impression that the problem space is vast, and hard to explore and address. On the other hand, existing defense systems deploy various strategies to counter the problem, and it is difficult to understand their similarities and differences assess their effectiveness and cost, and to compare them to each other [10].

The Light-Weight Hash function is used to verify the digital signature of the particular clients. The lightweight instance conjecturally provides at least 64-bit security against all attacks. By using this hash function we have to perform the digital signature. The digital signature of the uploaded and downloaded file can be stored in server side. The need for lightweight (that is, compact, low-power, low-energy) cryptographic hash functions has been repeatedly expressed by professionals, notably to implement cryptographic protocols in RFID technology. At the time of writing, however, no algorithm exists that provides satisfactory security and performance. The ongoing SHA-3 Competition will not help, as it concerns general-purpose designs and focuses on software performance. Lightweight hashes are indeed necessary in all applications that need to minimize the amount of hardware and the power and energy consumption [5].

The scope of the project is to prevent the network from the attackers. In order to maintain the security and traffic control. By using this process we prevent the attack insist from the attacker. In security basis the adaptive device is not allowed. The end-to-end principle is a powerful method. This method is used to forwarding the packet. The traffic control not allows the packet rate to increase. The owner has to restrict their own packets by using traffic control method. Trace back method is used to store a back log of packet hashes. This control handover is performed at each activated adaptive device on the network path of an IP packet.

SYSTEM ANALYSIS

Existing System

In our existing system we had to check the IP-address of the particular client and server. IP-address has to be checked by giving the source and destination address of the particular clients. To overcome this process we have to insert the digital signature process. The signature has to store in server side only. The digital signature of the particular client can get by giving the port number for that particular client. The signature verification is done by using the hash algorithm. The traffic can be monitored by the network traffic control method. The traffic can be measure to introduce the traffic ownership process. The network users known source and destination IP-address of the network packet. By using this traffic method we prevent misuse and malicious interference. The inclusion of this method is the adaptive device. Adaptive device is used to re-route the packets. The adaptive device can provide contextual information about the particular client. Disadvantages that are present in existing system are packet loss on intermediate links could be measured for network debugging purposes, Collateral damage caused by misconfigurations or malicious behavior of users, Traffic control not allows the packet rate to increase.

Methodology

In our proposed system we have to introduce the trace back method. The method is based on packet marking approach to avoid storing state at routers. Instead of inserting its entire IP address into the packet, each node inserts only the part of the IP address to indicate its presence on the path.

This method supports the network forensics by sampling the traces of suspicious network activity. Before forwarding a packet the router inserts the IP address of its output interface into the packet.

In this router inserts its outer-interface IP address into the forward packet. Upon receiving an attack packet, the victim disposes whose elements are the routers that compose the attack path. To reconstruct the attack path, the following procedure is used. Initially the victim checks for the presence of all neighbor routers in the received attack packet. Then we have to introduce the k-nn classification method to indicate the status of the networks. The network statuses are attack, pre-attack and normal.

Differential attacks cover all attacks that exploit non-ideal propagation of differences in a cryptographic algorithm. A large majority of attacks on hash functions are at least partially differential. The Security requirements of hash function are collision resistance, second pre-image resistance and also the pre-image resistance. The advantages of our proposed methodology are that it can minimize memory requirements, provide security and performance. The advantage of the ciphers is their simplicity and their performance flexibility. We use real network traffic information to discover the self-similar pattern for legitimate traffic, and use this information as a benchmark for our prediction algorithm, to determine if any new traffic that enters the network is DDoS traffic or legitimate traffic.

SYSTEM DESIGN

- Always when a user needs to access the server he must have been registered to the server. The registered user is given a key which is sent to his mail.
- When a user sends request to server, the signature of sender is verified.
  - The traffic monitoring system checks for the pattern of request from sender monitors and reply with action when the request is not a attack.
  - Log is created for each operation on network and this file can be kept at any location.

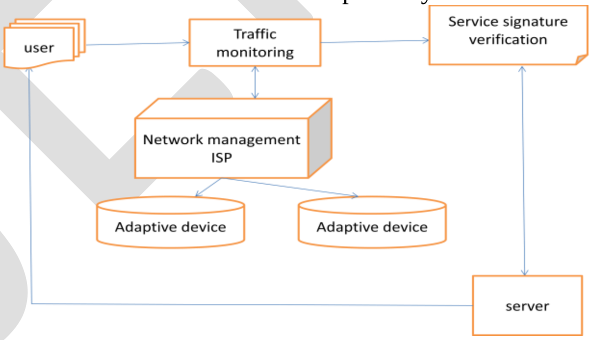


Fig. 3. System Architecture

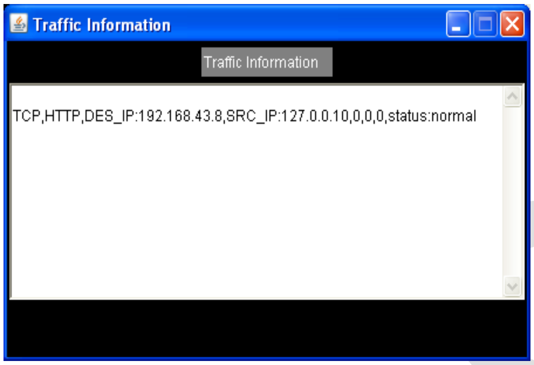
The Light-Weight Hash function is used to verify the digital signature of the particular clients. This is mainly used to maintain the security of the system performance. Hash functions can serve many different purposes, within applications ranging from digital signatures and message authentication codes to secure passwords storage, key derivation, or forensics data identification.

The lightweight instance conjecturally provides at least 64-bit security against all attacks. The primitives used in hash functions are Message Authentication Code, Pseudorandom generator, stream cipher, random Access Stream cipher and Key Derivation Function. By using this hash function we have to perform the digital signature. The digital signature of the uploaded and downloaded file can be stored in server side.

RESULTS

The fig. 4 indicates that the traffic has not occurred with status normal, source and destination IP address

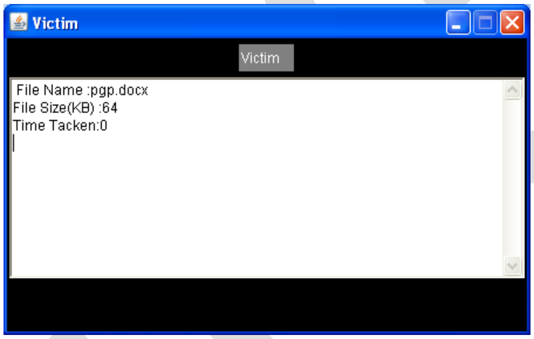
.



```
TCP,HTTP,DES_IP:192.168.43.8,SRC_IP:127.0.0.10,0,0,0,status:normal
```

Fig .4. Traffic information

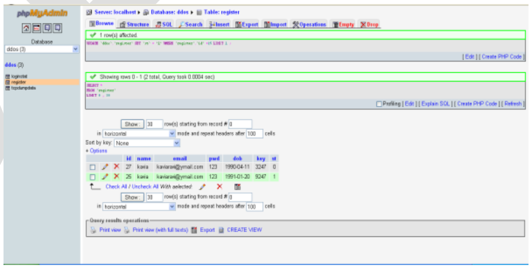
Fig.5 indicates that the file pgp.docx has been uploaded to server of size 64kb with time taken is zero seconds. This is server side information which shows the security of the system is high. When there is packet of same size and same pattern these information's will help us in the detection of DDoS.



```
 File Name :pgp.docx
File Size(KB) :64
Time Tacken:0
```

Fig.5. Server information

Database contains the logged in information and list of users who have registered to the server is shown in fig.6. Database also helps us in verifying whether an intended user is logged in or not.



1 row(s) affected.

```
UPDATE `ddos`.`register` SET `st` = '1' WHERE `register`.`id` =25 LIMIT 1 ;
```

Showing rows 0 - 1 (2 total, Query took 0.0004 sec)

```
SELECT *
FROM `register`
LIMIT 0 , 30
```

Show : 30 row(s) starting from record # 0
in horizontal mode and repeat headers after 100 cells
Sort by key: None

			id	name	email	pwd	dob	key	st
□		✗	27	kavia	kaviaravi@ymail.com	123	1990-04-11	3247	0
□		✗	25	kavia	kaviaravi@ymail.com	123	1991-01-20	9247	1

Show : 30 row(s) starting from record # 0
in horizontal mode and repeat headers after 100 cells

Fig.6. Database

CONCLUSION

This proposed work offers a new distributed traffic control system that enables ISPs to deploy new applications within the network and to safely delegate the partial network control to network users. Proposes a model to measure the effectiveness of filtering malicious traffic along with an effective trace back technique to control DDOS attacks generated. The methods based data mining are suitable for the detection. Then, the current network status is classified to determine the class to which it belongs to. Hence, our method can classify the current network status well to detect DDoS attacks early and the fault tolerance level was around 3%.

REFERENCES:

[1] S. Savage, D. Wetherall, A. Karlin, and T. Anderson., "Practical Network Support for IP Traceback.", ACM Sigcomm, 2000.

[2] A. C. Snoeren, C. Partridge, L. A. Sanchez, and C. E. Jones. "Hash-Based IP Traceback", ACM Sigcomm, 2001.

[3] Rafael P. Laufer, Pedro B. Velloso, Daniel de O. Cunha, IgorMoraes, Marco D. D. Bicudo, Marcelo D. D. Moreira, Otto Carlos M. B. Duarte, "Towards Stateless Single-Packet IP Trace back," Technical Report GTA- 06-38, COPPE/UFRJ, 2006.

[4] Sung M, Xu J. "IP trace back-based intelligent packet filtering: a novel technique for defending against internet DDoS attacks", International conference on network protocols, 2002.

[5] Jean-Philippe Aumasson, Luca Henzen, Willi Meier, and Maria Naya-Plasencia. "Quark: A lightweight hash", Mangard and Standaert, 2012.

[6] Andrey Bogdanov, Miroslav Knezevic, Gregor Leander, Deniz Toz, Kerem Varici, and Ingrid Verbauwhede, "*SPONGENT:* A lightweight hash function", In Bart Preneel and Tsuyoshi Takagi, editors, CHES, volume 6917 of LNCS, pages 312-325. Springer, 2011.

[7] D. X. Song and A. Perrig., "Advanced and Authenticated Marking Schemes for IP Traceback", IEEEInfocom, 2001.

[8] D¨ubendorfer, Matthias Bossardt, Bernhard Plattner, "Adaptive Distributed Traffic Control Service for DDoS Attack Mitigation", 19th IEEE International Parallel and Distributed Processing Symposium, 2006.

[9] http://en.wikipedia.org/wiki/Public Internet.

[10] Jelena Mirkovic, Peter Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms", ACM, 2004.

[11] Ambrose P J, Rai A, Ramprasad, "Internet usage for information provisioning: theoretical construct development and empirical validation in the clinical decision making context", IEEE transaction on engineering, 2006.

[12] Sandoval, G. and Wolverton, T.2000. Leading web sites under attack. CENT News. http://news.cnet.com/Leading-Web-site-under-attack/2100-1017 3-236683.html.

[13] K.Kumar, R.C.Joshi, and K.singh, "A distributed approach using entropy to detect ddos attacks in isp domain," in Intl.Conf.in Signal Processing, Communication and Networking (ICSCN), 2007,pp.331-337.

[14] G.Carl, G.Kesidis, R.R. Brooks, and S.Rai, "Denial-of-Service attack detection techniques," IEEE Internet Computing, vol.10,no.1,pp 82-89,2006.

[15] K. Park, G. Kim, and M. Crovella, "On the relationship between file sizes, transport protocols, and self-similar network traffic," in *IEEE* International Conference on Network Protocols, 1996, pp. 171–180.

[16] K. Park and W. Willinger, Self-similar network traffic and performance evaluation. Wiley New York, 2000.

[17] Y. Xiang, Y. Lin, W. L. Lei, and S. J. Huang, "Detecting ddos attack based on network self-similarity," Communications, IEEE Proceedings,vol. 151, no. 3, pp. 292–295, 2004