Volume 6, Issue 9, September 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Comparative Analysis of DDoS Attack Prevention Methods Using PPM, PANA and EMPAN

Dr. S. Malathi
Head, Department of Computer Science, Rabiammal Ahamed Maideen College for Women,
Tiruvarur, Tamilnadu, India

Abstract- The Internet, a modern wonder for a layman, is not that simple as it looks. It can provide god's plenty of information in a nanosecond. The possibilities of sharing information through networking have been growing in geometrical progression. Consequently it is to be noted that the attacks on the networks are also growing in equal proportion. In this connection, it is to be noted that the attacks on networks, especially DDoS (Distributed Denial-of-Service) attacks are also alarmingly growing in equal proportion. Distribution of information is being carried out between the server and the clients. The clients make requests for the data from the server and the server provides the response to the client's request. Sometimes the client can wishfully damage the server performance by sending continuous or anomalous requests. Consequently the server performance becomes degraded. This paper discusses how best the degradation of the performance can be prevented using the algorithms PPM, PANA and EMPAN.

Keywords- Internet, attacks, DDoS, degradation, PPM, PANA, EMPAN

I. INTRODUCTION

Internet is part and parcel of modern life. It has become indispensable. One can get god's plenty of information at a finger touch. But the information flow can be denied and corrupted by unique devices deployed by some people, whom one can call as intruders or hackers. Attacks on networks and home computers have increased and the reasons are many. Some of them are clueless user base, malicious users, homogeneous computing environment and increasing connectivity. The internet protocols were not designed with security in mind and most of the authentication is based on the IP address, which as is well known, can be easily spoofed. Fig 1 shows the architecture of DDoS attacks [1].

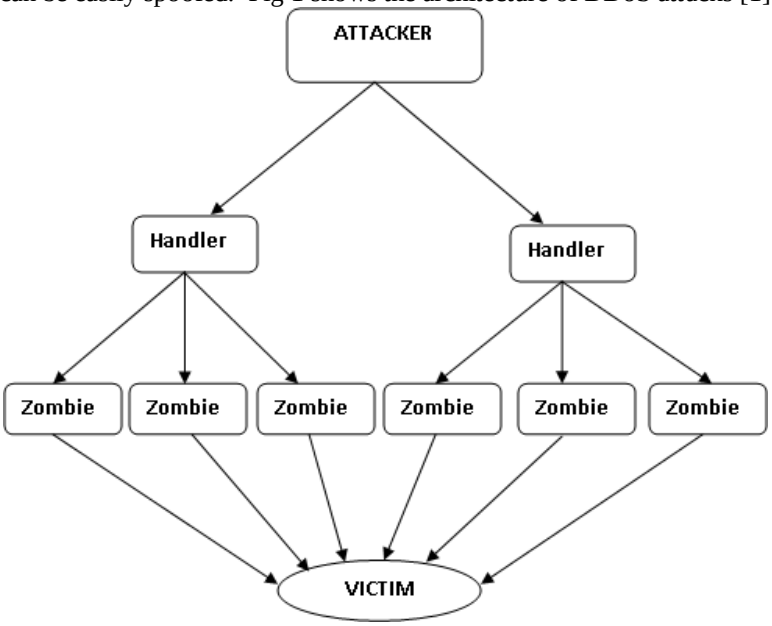

Fig 1: Architecture of DDoS attacks

It is composed four elements. First element is **Victim.** It is a target host that has been chosen to receive the brunt of the attack. Next component is **Zombie or attack daemons**, these are the agent programs that actually conduct the attack on the target victim. These are usually deployed on host computers. These daemons affect both the target and the host computers. The task of deploying these attack daemons requires the attacker to gain access and penetrate the host computers. Third component is **Handler.** Its task is to coordinate the attack and is deployed in a host (master). The last one is **Attacker,** the mastermind behind the attack. By using a control master program, the attacker can stay behind the scenes of the attack.

The DDoS attacks sequence is as follows. The attacker sends an "execute" message to the handler or control master program. It receives the "execute" message and propagates the command to the attack daemons under its control. Upon receiving the attack command, the attack daemons begin the attack on the victim. Even though it might appear that the real attacker doesn't have much to do except to send out the "execute" command, in reality he/she actually has to plan the execution of a successful distributed denial of service attack. Fig 2 is what the website may look after a successful DoS attacks. DDoS attacks can be divided into three types [2]. These are volume based attacks, protocol attacks and application layer attacks.

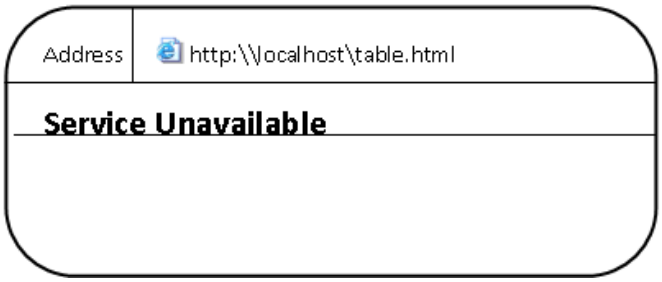

Fig 2: Effect of DDoS Attack

II. RELATED WORK

In [12], sound a warning that DDoS attacks pose an increasingly grave threat to the internet infrastructure and the other popular internet sites. Alarmingly, the DDoS attacks are observed on the large backbone of the networks [11].

Common internet attacks methods are broken down into more categories. Some attacks gain system knowledge or personal information, such as eavesdropping and phishing. Some attacks can interfere with the system's intended function, such as viruses, worms and Trojans. Some other attacks are when the system's resources are consumed uselessly; these can be caused by denial of service (DoS) attack. Duration of most DDoS attacks is not very long [14]. The vast majority of DDoS attacks, 93.2 percent, were less than 30 minutes in duration. Many efforts have been untiringly made to prevent such attacks with some success. Dealing with DDoS attacks has proven to be extremely difficult. The following are the main challenges that face researchers in this field [13].

Distinction between attack traffic and legitimate traffic before reaching the target*:* Malicious packets differ from the legitimate ones in intent not in content. This is due to the fact that attackers use the same Internet protocols used by legitimate users and generate packets that appear to be genuine. Therefore, attack traffic characterization is a very challenging problem. DDoS countermeasures should perform accurate traffic characterization. Otherwise, legitimate traffic can be affected considerably.

Deployment of DDoS countermeasures: coming up with DDoS countermeasures that are transparent to existing Internet protocols represents a major challenge. Most of the known DDoS countermeasures require either a network support an end-system support or a protocol modification. Such requirements may stand against deploying these countermeasures, because it is very difficult to enforce deployment of DDoS countermeasures in an uncontrolled domain such as the Internet.

Handling huge volume of attack traffic at high Internet speeds: most of the reported DDoS attacks are based on brute force approach, where an overwhelming number of packets overload the victim. On the other hand, DDoS countermeasures usually involve some kind of packet processing such as marking, validation, storage, filtering, etc. Given the fact that DDoS attacks are characterized by huge packet volumes, performing these tasks at very high Internet speeds is a major challenge.

Detection and handling of sophisticated DDoS attacks: New generation of sophisticated DDoS attacks is emerging in different forms. These attacks can lead to degradation of service rather than completely blocking of service. Moreover, these attacks use much lower amount of traffic as compared to the flooding-based attacks. Therefore, conventional DDoS detection methods will not be able to identify the existence of an attack. Developing fast and accurate detection schemes are an important issue in this context. Also, it is equally important to develop effective prevention and mitigation schemes to handle these attacks.

Determining the number of attackers: Since attackers employ source address spoofing widely, it is difficult to know if the attack traffic is originating from a single source or from multiple sources, and if it is originating from multiple sources, then what is the actual number of these sources. Knowing the number of attack sources may lead to strategic defense decisions in certain cases.

III. DDOS ATTACK PREVENTION METHODS

A thorough study of the literature survey necessitates ensuring further progress so that it could throw much light on the areas that have been traversed so far and provide fresh insight into as to what direction the research is to be carried out henceforth. Obviously there have been several attempts in this direction. This paper focuses on the vital experiments namely PPM, PANA and EMPAN.

A. Tracing Attackers Through PPM

The probabilistic packet marking (PPM) algorithm [5] is used to solve the IP traceback problem. It is a used to discover the Internet map or an attack graph during a distributed denial-of-service attack. The PPM algorithm consists of

two procedures: The packet marking procedure and graph reconstruct procedure. In the packet marking procedure the Packets randomly encode every edge of the attack graph and the graph reconstruction procedure obtains the constructed graph from this encoded information. Here the constructed graph should be the same as the attack graph. The constructed graph is the graph obtained by the PPM algorithm and attack graph is the set of paths the attack packets has been traversed.

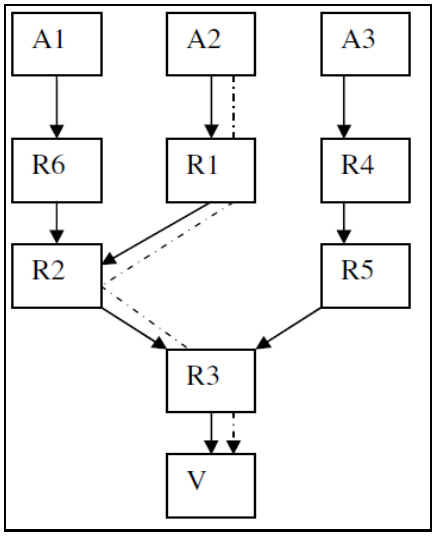

Fig 3: An attack graph containing attack path

The network can be viewed as a directed graph G = (V,E) where V is the set of nodes and E is the set of edges. V may be a single host under attack, or a network border device such as a firewall or intrusion detection system that represents many such hosts. Every potential attack origin Ai is a leaf in a tree rooted at V and every router Ri is an internal node along a path between some Ai and V. The attack path from Ai is the ordered list of routers between Ai and V that the attack packet has traversed, e.g. the dotted line in the figure 1 indicate the attack path: (R1, R2,R3). The distance of Ri from V on a path is the number of routers between Ri and V on the path, e.g. the distance of R1 to V in the path (R1, R2, R3) is 2. The attack graph is the graph composed of the attack path e.g., the attack graph in the example will be the graph containing the attack path (R1,R2,R3) and it refers to the packets used in DDOS attacks as attack packets.

1) Packet Marking Procedure:

To implement an IP traceback service previously they used to allocate enough space in an IP packet header so that one can use this space to record the traversed path of a packet. For example, each router, beside performing the normal packet forwarding and routing functions, records or appends its own ID in the pre-allocated space at the packet's header. In this analogy when a victim receives a marked packet, victim can examine the packet's header and obtain the complete traverse path information of the marked packet. However, one major problem about this simple approach is that the length of a traversed path (e.g., number of hops) of a packet is not fixed. Therefore, it is impossible to pre-allocate sufficient amount of space in the packet's header in advance. Another technical difficulty of recording complete path information of each packet to the victim is that if an attacker can potentially manipulate this path information and fill in false router's identification in the packet's header it misleads the victim site. The packet marking algorithm proposed by Savage instead of recording the complete path information of a packet, only records each edge traversed from the attacker to the victim site in a probabilistic fashion.

The routers encode the information in three marking fields of an attack packet: (start, end, distance). The start and end fields store the IP addresses of the two routers at the end points of the marked edge. The distance field records the number of hops between the marked edge and the victim site. In the PPM a packet stores the information of an edge in the IP header. The pseudo code of the procedure is given below. The router determines how the packet can be processed depending on the random number generated. If x is smaller than the predefined marking probability pm, the router chooses to start encoding an edge. The router sets the start field of the incoming packet to the routers address and resets the distance field to zero. If x is greater than pm, the router chooses to end encoding an edge by setting the router's address in the end field.

Algorithm

```
for each packet w
let x be a random number from [0..1)
if x < pm then
write R into w.start and 0 into w.distance
else
if w.distance = 0 then
write R into w.end
increment w.distance
```


2) Graph Reconstruction Procedure:

A victim V, upon receiving packets, first needs filtering of unmarked packets (since they don't carry any information in the attack graph construction). The victim needs to execute the graph construction algorithm for all the collected marked packets and re-construct the attack graph. Figure 3 illustrates the attack graph construction algorithm.

Algorithm

```
let G be a tree with root being victim V ;
let edges in G be tuples(start,end,distance);
for (each received marked packet w)
{
if (w.distance==0) then
insert edge (w.start,V ,0) into G ;
else
insert edge (w.start, w.end, w.distance) into G ;
}
remove any edge (x,y,d) with d _ distance from x to V in G ;
extract path (Ri…Rj) by enumerating acyclic paths in G ;
```

B. PANA Authentication To IP Spoofing

PANA [6] can be used in environments with Network layer security and link layer security. It is used ISN mechanism to prevent blind DoS and off-path attacks and Cookie mechanism for prevent non-blind DoS attack. An access control framework using PANA defines the four following functional entities to authenticate network from attacks. These are PANA Client (PaC), PANA Authentication Agent (PAA), Authentication server (AS) and Enforcement Point (EP).

PANA Client (PaC): The PaC is the client implementation of PANA. This entity resides on the node that is requesting network access. PaCs can be end hosts, such as laptops, PDAs, cell phones, desktop PCs, or routers that are connected to a network via a wired or wireless interface. A PaC is responsible for requesting network access and engaging in the authentication process using PANA.

PANA Authentication Agent (PAA): The PAA is the server implementation of PANA. A PAA is in charge of interfacing with the PaCs for authenticating and authorizing them for the network access service. The PAA consults an authentication server in order to verify the credentials and rights of a PaC. If the authentication server resides on the same node as the PAA, an API is sufficient for this interaction. When they are separated (a much more common case in public access networks), a protocol needs to run between the two.

Authentication Server (AS): The server implementation that is in charge of verifying the credentials of a PaC that is requesting the network access service. The AS receives requests from the PAA on behalf of the PaCs, and responds with the result of verification together with the authorization parameters (e.g., allowed bandwidth, IP configuration, etc). This is the server that terminates the EAP and the EAP methods. The AS might be hosted on the same node as the PAA, on a dedicated node on the access network, or on a central server somewhere in the Internet.

Enforcement Point (EP): The access control implementation that is in charge of allowing access (data traffic) of authorized clients while preventing access by others. An EP learns the attributes of the authorized clients from the PAA. The EP uses non-cryptographic or cryptographic filters to selectively allow and discard data packets. These filters may be applied at the link layer or the IP layer [PANA-IPSEC]. When cryptographic access control is used, a secure association protocol needs to run between the PaC and EP. After completion of the secure association protocol, link- or network layer per-packet security (for example TKIP, IPsec ESP) is enabled for integrity protection, data origin authentication, replay protection and optionally confidentiality protection.

However, as PANA architecture uses periodic re-authentication, the IP spoofing is effective only for a small duration. Even PANA authentication is run on an insecure channel that is vulnerable to eavesdropping and spoofing.

C. Methodology of EMPAN

The aim of this method EMPAN (Efficient Monitoring method for Preventing DDoS Attacks on Networks) is to develop an efficient method in order to deny the services to the hackers and improve the server performance using the DDoS technique. This is summed up below:

In order to detect the intruders, the entry of all clients and their activities are maintained as history. The history also contains the information about the clients with their corresponding entry time, date and their accessing site. Based on the history, we can identify all the clients accessing the server. The IP address of clients to access the website is found by IP watcher and the File watcher is responsible to monitor the files stored in the database and analyse the modifications made in the file. This is carried out in paper [7].

Each client entering the internet is assigned a unique IP address. This IP address is also stored in the history along with the clients' entry details. Based on this IP address, we can identify the particular client. This identification is successfully done by grouping the IP addresses from the history and count the number of occurrence of the same IP address under the same date. Thus we identify the client who utilizes the site for the maximum number of times on the same day.

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. This is done by GI Time Frequency Algorithm discussed in paper [8]. This algorithm is used to group the intruders under the Intruders list and thus prevent them from accessing the website. The IP address in the Intruders List is maintained permanently in order to check the upcoming client. If the client in the list tries to enter again, then the access permission is denied by not giving any response to that kind of clients, using the DDoS mechanism. If other clients enter into the site, the history is maintained in order to determine their performance. 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 the disappointment of genuine customer. To avoid this kind of disappointment, clients are to be screened and genuine customers alone are to be allowed during peak hours and the unauthorized users are to be blocked.

A database of all records about the clients is maintained continuously by the server. This database determines the category of the clients such as registered and unregistered clients. If the entry of the client is found in the database, it means they are considered registered clients. Otherwise, they are considered unregistered clients. All the registered and unregistered clients who access to the web page are added into the access count. The access count is the count that can be incremented every time when the client sends the request.

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 and not in intruder list found by GI time frequency algorithm, 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. The Warning Count is the count that can be incremented once when the unregistered client sends anomalous request. After the peak hours, the client in the warning list is taken out and the warning count is compared with the threshold value. If the value matched, then the client is added into the blocked list. Otherwise, the client is provided with proper response. This is carried out in paper [9].

However, there need to be a caution about IP spoofing which means the IP addresses are changeable by those who seek hacking the information and it can lead to security damage and confidentiality of information. IP watcher and file watcher, The GI time frequency algorithm and categorizing the clients during peak hours of server were carried out only by means of IP addresses. In order to maintain the confidentiality and to boost the performance of the web server, the MAC address is to be used along with IP address [10].

The server stores MAC address along with IP address on the database. If any client enters into the network, the server validates the client with both IP address and MAC address. If both the addresses found valid, then the server allows the client to access to the information. Otherwise, it blocks the client. If the client modifies the IP address to access to the information, the server finds that the client is not valid to access to the information by means of MAC address. Thus, there is no way to hack the information by spoofing the IP address and thus it provides security to the machine and also keeps the data secured from unauthorized people accessing.

Thus this methodology makes an attempt to provide an efficient and well suitable algorithm to identify the attack or threat made by the clients on server performance and prevent the server from that kind of attack using IP watcher, GI time frequency algorithm and target customer behaviours with MAC address along with IP address.

ALGORITHM

Step 1: **Analysis the User**

```
Identify the entered User's IP Address
If IP address found in User List then
    Check the corresponding MAC Address of the IP Address
    If MAC address in User List match with User MAC Address then
    User Status="Registered User"
    Else
    User Status="Malicious User. IP Spoofing happened."
    Block the User IP
    End if
Else
    User Status="Unregistered User"
End if
```

Step 2: **Response to Registered User**

```
Store the user entry into the Log
Accept the Request
If user IP already in Log then
    If log.date = current date then
            Calculate the time frequency, tf
            If tf<=1 minutes and count<=5 then
                    Process the Request
            Else
                    Block the User IP
```



```
                    Add IP into the Blocked List
                End if
            Else
                Process the Request
                Store it in log
            End if
        Else if User IP in Blocked List then
            Status = "Blocked IP. Access Denied"
            Else
            Process the Request
            Store it in Log
            End if
        End if
```

Step 3: **Response to Unregistered User**

```
Accept the User Request
If request time not match with server peak time then
    If User IP already in Warning List then
    Increment the count for the User IP
            If count>=3 then
            Block the IP
            Else
            Response to the User
            End if
    Else
            Process the request
            Message "Server Busy.. Try again later.."
    End if
Else
Process the request
End if
```

D. Comparison of PPM, PANA AND EMPAN

Analysing DDoS attack prevention methods namely PPM and PANA Using the factors such as which mechanisms to be used, status of Prevention of IP spoofing and Time Consumption and scalability.

Table I. Comparison of PPM, PANA and EMPAN

FACTORS	PPM	PANA	EMPAN
Mechanisms used	Packet Marking Procedure Graph Reconstruction Procedure	ISN for Blind DDos Cookie mechanism for Non Blind DDos	IPwatcher, File watcher
Prevention of IP spoofing	The source IP address of a packet is not authenticated	IP spoofing is effective only for a small duration	Controlled by using of MAC addresses
Time Consumption and scalability	Attack Path reconstruction for lost packet has taken much more time.	run on an insecure channel, it take more time for finding eavesdropping and IP spoofing	Access classified as peak hours and non-peak hours, authorized users get access the site fast during peak hours.

IV. CONCLUSIONS

In this paper the survey has thrown adequate light on the research works that have been carried out so far on the DDoS attacks. The objectives of the researchers and the comparison results of PPM, PANA and EMPAN are carried out. Apart from this, the areas yet to be covered that could give a lead for further research is also understood with special reference to DDoS attacks.

REFERENCES

[1] Puneet Zaroo, "A Survey of DDoS attacks and some DDoS defense mechanisms", Advanced Information Assurance (CS 626).

[2] DDoS protection services, http://www.incapsula.com/ddos/ddos-attacks, INCAPSULA,DDoS centre.

[3] Common Types of Network Attacks, http://technet.microsoft.com/en- us/library/cc959354.aspx.

[4] Bhavya Daya, "Network Security: History, Importance, and Future", University of Florida Department of Electrical and Computer Engineering.

[5] Y.bhavani p.niranjan reddy, "An efficient IP traceback through packet marking algorithm", IJNSA, vol.2, no.3, july 2010.
[6] Jayaraman. P, Lopez. M. R, Ohba. Y, Parthasarathy, Yegin. A "Protocol for Carrying Authentication for Network Access (PANA) Framework", RFC 5193.
[7] Kuppusamy K and Malathi S, "A new Methodology to Prevent DDos Attacks using File Watcher and IP Watcher", IJARCS.IFO journal, Vol. 2, No. 1,Jan-Feb 2011, PP.391-396.
[8] Kuppusamy K and Malathi S, "An Effective Preventionof Attacks using GI Time Frequency Algorithm under DDoS", IJNSA journal, Vol. 3, No. 6, Nov 2011, PP.249-257.
[9] Kuppusamy K and Malathi S, "Prevention of Attacks under DDoS Using Target Customer Behavior", IJCSI journal, volume 9, Issue 5 No.2, September 2012, PP. 301-307.
[10] Dr. Malathi S, "Prevention of IP Spoofing Attack under DDoS Using IP and MAC Address", International Journal of Computer Technology & Applications,Vol 7(4), ISSN:2229-6093 , pp.610-616.
[11] Craig Labovitz, Danny McPherson, and Farnam Jahanian, "Infrastructure attack detection and mitigation", SIGCOMM 2005, August 2005. Tutorial.
[12] Massive DDoS attack hit DNS root servers, http:// www.internet news. com /ent-news/article.php/1486981, October 2002.
[13] Basheer Nayef Al-Duwairi, "Mitigation and traceback countermeasures for DDoS attacks" , Ph.D thesis, Iowa State University, Ames, Iowa, 2005.
[14] Common DDoS attack and Mid-year security thread report 2012, NSFOCUS website, www.nsfocus.com.

ABOUT AUTHOR

Dr. S.MALATHI, Head and Assistant Professor, Department of Computer Science, Rabiammal Ahamed Maideen College for Women, Thiruvarur, Tamil Nadu, India. She received her Ph.D Degree in Manonmaniyam Sundaranar University, Tirunelvelli. She has extensive research interests including Network security, web designing and image processing. She has published many International Academic research papers. She has attended many National and International conferences and workshops. She has been invited as a resource person in various colleges. She has published a book entitled "HTML AND JAVA SCRIPTING".

