ISSN:0975-9646

Prioritizing Packets and Reducing Congestion using Filtering and Rate-Limiting Mechanisms along with Security

Reddy.Nagarjuna[#1], Mr.V.V.Gopala Rao[*2],

[#]*M. Tech. Student, Department of Computer Science and Engineering, Aditya Engineering College, Surampalem, Peddapuram, East Godavari District, Andhra Pradesh, India*

[*]*Associate Professor, Department of Information Technology, Aditya Engineering College Surampalem, Peddapuram, East Godavari District, Andhra Pradesh, India*

***Abstract*— Now a day, the major problem in internet is Bandwidth Distributed Denial-of-Service attacks. Bandwidth Distributed Denial of service is a serious threat which disrupts the operation of the infrastructure by causing congestion, i.e. excessive amount of traffic. To reduce the congestion various mechanisms are introduced. In this paper, the proposed mechanisms are Filtering, Rate-Limiting along with the Security. The advantages of this proposed mechanisms are, it is easy to verify whether the packet is authorized or not and when congestion occurs, priorities are given to authorized packets based on time delay and packet length and only those packets having the high priority will be transferred to the destination first. This in turn reduces the attack within the network. By implementing these mechanisms at the router, there is a chance to reduce the congestion occurred by Bandwidth Distributed Denial of Service attacks.**

Keywords- Denial of Service, Cumulative Distribution Function, Capability, overlay networks, packet filtering.

I. INTRODUCTION

In Bandwidth Distributed Denial-of-Service (BW-DDoS) attacks, the attacker will control some of the systems which are called compromised systems. By those compromised systems the attacker will send continuous flow of messages to the destination to disrupt the services provided by the destination to the authorized users. The Bandwidth Distributed Denial-of-Service attacks shown in below Fig. 1,

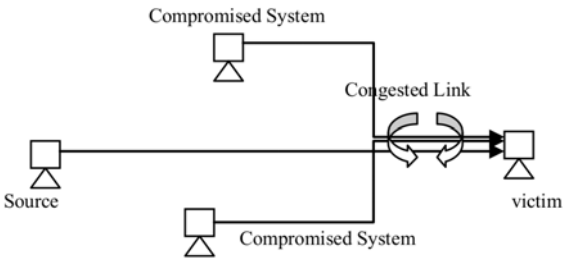

Fig. 1 Bandwidth Distributed Denial of Service

The compromised systems are either zombies or puppets. Zombies are the software agents having the high privileges and having the complete control of the machine on which they are executed. Puppets are the programs and they acquire by fooling users into browsing attacker's website.

Some of the attacks occurred by the Bandwidth Distributed Denial-of-Service attacks.

1. *UDP Flood attack*: This attack will occur when the attacker will send the continuous packets to the destination using UDP.
2. *DNS Amplification attack*: It is a type of attack, where the attacker will send the responses as a legitimate host to the victim host by hiding himself.
3. *Core melt attack*: It is a new attack mechanism, where the packets will be transferred between the attackers, and not towards a victim host [1].

and other attacks like Max SYN, Optimistic Acknowledgement, and ACK Storm etc.

To reduce these types of attacks, some of the mechanisms like Filtering, Rate-Limiting implemented at the router and for the purpose of security of the network, Security Overlay Service architecture are provided.

II. SECURITY MECHANISMS

A. Filtering

This mechanism is implemented at the router (or) gateway to destroy the unauthorized packets which are coming from outside the network. In this paper, the filtering is done by using LOT (Lightweight Opportunistic Tunnelling) protocol as shown in below Fig. 2.

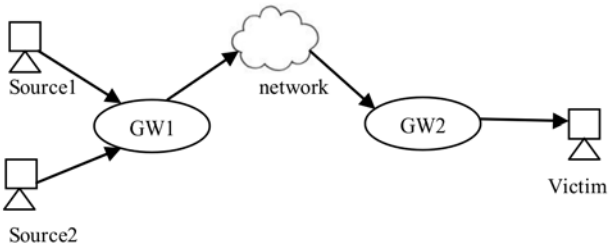

Fig. 2 LOT is deployed in between the two gateways.

In this protocol, there are two phases. One is the Hello phase and another one is the Network block validation phase.

In Hello phase, the Hello Request is transferred from one gateway to another gateway. The Hello Request contains a description of the network block behind a gateway and a cryptographic cookie, this cookie is calculated by using the strongest encryption algorithm which is AES (Advanced Encryption Standard) performed

on destination address and current time. A network block is described by a tuple (base-address, l), where base address is the network address and l is the number of bits in the network part of the address.

After completion of Hello phase successfully, the Network block validation phase begins. In this phase, the gateway1 will send the cookie along with the IP address for first time; from next onwards gateway1 performs response verification. The other side gateway (gateway2) will also perform response verification. The response verification will be done by using the pseudo random function (AES-CMAC). This verification continuously is done for some iteration. After last iteration, both gateways will store the pseudo random values and used it as session keys. After completion of validation phase successfully, tunnel will be established. If we want to send the packets in between the gateways through the tunnel, add the periodic tag and transfer. The periodic tag was calculated by using (1).

$$PeriodicTag = PRF_{SessionKey}(i) \quad (1)$$

Where PRF is the Pseudo Random Function and (i) is the difference between the current time and the tunnel creation time [2].

B. Rate-Limiting

This mechanism is implemented at the router and worked when the network link has congested. This mechanism is applicable in several forms that are used to check the packets whether they are authorized or not. If the packets are authorized and also in those authorized packets which are having the high priority are transferred to the destination. Otherwise the packets are discarded.

The Rate-Limiting is applicable in three forms.

- Capabilities.
- Packet Tagging.
- Scheduling based

1) Capabilities

In this form, the keyed hash function is used to generate the capabilities. When the source (client) connects with the destination (server), the DTA packet transfers from source (client) to destination (server) through the routers, each router will calculate marking for the packet, attach that marking to the packet, forwards that packet to the next router and at last the router will attach the marking, forwards to the destination. The marking is calculated as the last z-bits of output to the keyed hash function. The inputs to the keyed hash function are the key, IP address of the current router, IP address of the last-hop router, and the source and destination IP address of the packet being forwarded. The packet by the destination along with the marking, that marking will consider as the token id for the source (client). The destination (server) retransmits that token id to the source (client). Again the routers will calculate the marking for the packet which is transferred by the destination (server). After the packet transferred to the source (client), the source (client) will get that token id along with the destination (server) token id. The above process is showed in below Fig. 3 and explained briefly,

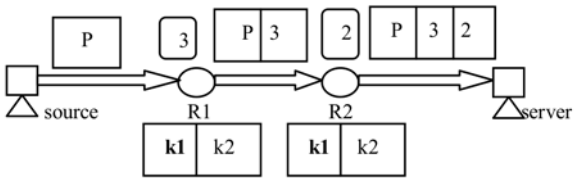

Fig. 3 Source connects with the server

From the above Fig. 3, the router (R1) calculates the hash code with key k1 for the source packet, attach the last bits '3' to the packet, forward that packet to the router (R2), the router (R2) do the same process, attach the last bits '2' to the packet and forwards the packet to the server. The server keeps that token in the capability field of the packet and forwards that packet to the source. When the server sends the packet to the source, the routers will calculate the token for the server. The source will receive the packet from the server, gets the token from capability field and reverse the bits. Finally the token id for the source is '23'.

When the source sends the EXP packet along with the token id to the destination, the router calculates the marking for the packet and compare with the token id send by the source, if they are equal, the router changes the key, calculates the marking, attach that marking to the packet and update that marking to the client. The above process is showed in below Fig. 4, and explained briefly.

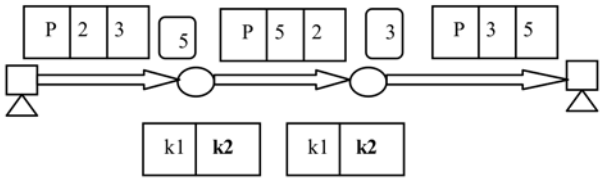

Fig. 4 Source sends the packet with token id

From the above Fig. 4, when the source sends the packet to the server along with the token id, the router (R1) calculates the hash code to the packet and compares last bit '3' of hash code with the last bit '3' of token id. If both are equal, the router will calculates the hash code with different key (k2), attach the last z bits of the hash code '5' to the packet by shifting the bits in the packet to the right, gives the high priority for the packet and forwards the packet to the next router (R2). Otherwise the router will give the low priority for the packet. The same process will be done by the router (R2) and forwards the packet to the server.

Whenever the congestion occurs, the low priority packets are discarded and the packets having the high priority will forward to the destination by the router. This process will do until the packet is received by the destination [3].

2) Packet Tagging

In this form, the Cumulative Distribution Function (CDF) model is used as a utility function, to find out the threshold value based on the time delay of some transmissions between the source and destination at some time't'. The router calculates the time delay of the arrived packets and gives the priority to the packets. If the time delay of the packet is less than or equal to the threshold

value, then the packet will tagged as the high priority otherwise the packet will tagged as low priority. Whenever the congestion occurs across the network link, the high priority packets are transferred to the destination and the low priority packets are discarded [4]. By consider the time delay as a threshold value, the advantage is there is no loss of authorized packets.

3) Scheduling based

In this form, the weighted fair queue scheduling algorithm is used. This algorithm is used when the network link has congested and also to prioritize the packets among the authorized packets. Packets which are having the high priority are transferred first [5].

C. Security

To provide the security from the denial-of-service attacks, the system follows the Security Overlay Service architecture shown in below Fig. 5. The goal of this architecture is to provide communication between the confirmed user and a target.

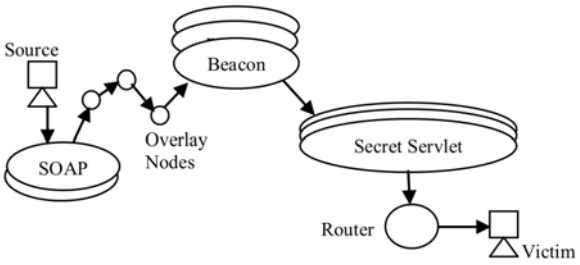

Fig. 5 Security Overlay Service Architecture

In this architecture after client connected to the server, the server selects some of the nodes that act as secret servlets. In this architecture there is SOAP (Secure Overlay Access Point). This node verifies whether the client has access to the network or not. If yes, it forwards the packet or otherwise it discards the packet. The network follows Chord-based overlay routing. In this routing mechanism, the nodes are connected in rounded manner. Each node has a list of some other connected nodes. If the packet arrives at the node it forwards the packet randomly to other node. Whenever the packet arrives at the secret servlet, it forwards the packet to the destination. At the destination, before going the packet to the destination, the packet arrives to the router. In router, the filtering mechanism is implemented means if the packet arrives with the token id; it calculates the marking for the packet and compared with the token id. If both are same, then the packet forwards to the destination otherwise the packet is discarded [6].

III. Security Mechanisms Location

Security mechanisms can be deployed at different places in the network near at the source, at the destination (or) at the router. By implementing these Security mechanisms at the router there is a chance to reduce the attacks and congestion occurred by BW-DDoS attacks.

IV. Experimental Results

A. Key based hash algorithm

In this paper, MD5, SHA-1 and RIPEMD-160 are compared in Table I, to find that which algorithm is generating hash code at less time, that algorithm will be used as key based hash algorithm.

TABLE I. Algorithm and Time (ms) to generate the Hash code

Algorithm	Hash Code generated in mille seconds
MD5	>10 ms
SHA-1	<1 ms
RIPEMD-160	<1 ms

According to above Table I, SHA-1 and RIPEMD-160 are generating hash code within the less time. In this paper, used SHA-1 algorithm for generating the hash code because RIPEMD-160 generating the hash code is very small and also it follows the MD4 structure.

B. Cumulative Distribution Function

The use of CDF captures the acceptance probability of a particular time delay as follows. Let $Y_j(t)$ be a random variable that represents the time delay of the packet for flow j at time t and let $y_j(t)$ be the time delay. Then the CDF of $Y_j(t)$ is denoted as

$$\Pr[Y_j(t) \le y_j(t)] = \phi_{j,t}(y_j(t)) \quad (2)$$

Let $r_{j,1}(t), r_{j,2}(t), \ldots, r_{j,N}(t)$ be the N measurements taken for flow I at a particular time of day t over some historical data set. Then the CDF is denoted as

$$\phi_{j,t}(y_j(t)) = \frac{\#measurements \le y_j(t)}{N}$$

$$= \frac{1}{N} = \sum_{k=1}^{N} I(r_{j,k}(t) \le y_j(t)) \quad (3)$$

Where $I(r_{j,k}(t) \le y_j(t))$ is the indicator that the measurement $r_{j,k}(t)$ is less than or equal to $y_j(t)$.

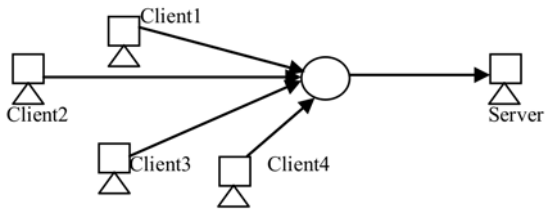

Fig. 6 Multiple Clients connected to the Server

Consider the Table II, it contains the time delays of same time‘t’ for the above Fig. 6, and taken the acceptance probability as 80%.

TABLE III. TIME DELAYS AND THE CORRESPONDING TIME DELAY ALLOCATION

Flow	Time delays at some time 't' (mille seconds)					Threshold value
Client1,Server	2	2	3	3	5	3
Client2,Server	3	4	6	7	3	6
Client3,Server	5	6	6	5	5	6
Client4,Server	4	4	4	4	4	4

In the first flow, the time delays of (Client1, Server) are 2, 2, 3, 3, 5. Among these time delays, which time delay is satisfying the above (3), is taken as a threshold value. How means, $2 \leq 3$ gives 20% acceptance probability, $2 \leq 3$ gives 20%, $3 \leq 3$ gives 20%, $3 \leq 3$ gives 20%. 3 are giving the acceptance probability 80%. So, 3 are considered as a threshold value.

In the second flow, the time delays of (Client2, Server) are 3, 4, 6, 7, 2. Among these, 6 are giving the acceptance probability 80%. How means, $3 \leq 6$ gives 20% acceptance probability, $4 \leq 6$ gives 20%, $2 \leq 6$ gives 20%, $6 \leq 6$ gives 20%. So, 6 are considered as a threshold value.

C. Weighted Fair Queue Scheduling Algorithm

This algorithm gives the high priority to authorized packets for which packets having the lowest length and those packets was transferred to the destination first, and next the lower length packet is transferred, and so on.

Consider the Table III, which contains the packets, its length and its priority per flow.

TABLE IIIII. WEIGHTED FAIR QUEUE SCHEDULING ALGORITHM

Flow	Packets	Length (in bytes)	Priority
Client1,Server	P1	1467	3
	P2	750	1
	P3	1150	2
	P4	2250	4
Client2,Server	P1	962	3
	P2	128	1
	P3	1069	4
	P4	854	2
Client3,Server	P1	564	2
	P2	694	3
	P3	1245	4
	P4	90	1
Client4,Server	P1	1467	4
	P2	854	3
	P3	694	2
	P4	283	1

In the first flow, the packet 2 which is having 750 bytes was transferred first, next the packet 3 having 1150 bytes was transferred, next the packet 1 having 1467 bytes was transferred and last the packet 4 having 2250 bytes was transferred.

V. CONCLUSION

In this paper, the system follows Security Overlay Service Architecture. It is a powerful way of countering Denial of Service attacks. It is implemented at the router by following the mechanisms of filtering and rate-limiting. By these mechanisms, there is a priority of authorized packets and reduce the congestion generated by Denial of Service attacks within the network and also from outside the network.

ACKNOWLEDGMENT

I would like to express my gratitude to my Guide Mr. V.V. Gopala Rao, M. Tech., Associate Professor, without his guidance, this paper is not possible. His understanding encouragement and personal guidance have provided the basis for this paper.

REFERENCES

[1] "The Core melt Attack" by Ahren Studer and Adrian Perrig, Carnegie Mellon University 2009.

[2] Y. Gilad, A. Perrig "LOT: A defense against IP spoofing and flooding attacks" ACM TRANSACTIONS ON INFORMATION AND SYSTEM SECURITY, JULY 2012.

[3] Abraham Yaar, Adrian Perrig, Dawn Song "SIFF: A Stateless Internet Flow Filter to Mitigate DDoS Flooding Attacks" 2004.

[4] Jerry Chou, Bill Lin, Subhabrata Sen, Oliver Spatscheck "Proactive Surge Protection: A Defense Mechanism for Bandwidth-Based Attacks" 2009.

[5] Y. Gev, M. Geva, and A. Herzberg, "Backward traffic throttling to mitigate bandwidth floods," in Globecom 2012 – Communication and

[6] Information System Security Symposium (GC12 CISS), Anaheim, CA, USA, Dec. 2012.

[7] A. D. Keromytis, V. Misra, and D. Rubenstein, "SOS: an architecture for mitigating DDoS attacks," IEEE Journal on Selected Areas in Communications, vol. 22, no. 1, pp. 176–188, 2004.

AUTHORS PROFILE

Reddy Nagarjuna received the B. Tech. Degree in Computer Science and Engineering from Akula Sree Ramulu Institute of Engineering and Technology, permanently affiliated to J.N.T.U. Kakinada, Andhra Pradesh, India. Presently working for M. Tech. Degree in Computer Science and Engineering at Aditya Engineering College, affiliated to J.N.T.U. Kakinada, Andhra Pradesh, India.

Mr.V.V.Gopala Rao working as Associate Professor in Aditya Engineering College, Surampalem, Andhra Pradesh, India. He received the M. Tech. Degree from Acharya Nagarjuna University, Andhra Pradesh, India. He is interested to work in Network Security.