ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Implementation of Defence Mechanism Based on Novel Traceback Scheme

Shubhangi R. Sardar, S. M. Chaware

P.G. Student, Department of Computer Engineering, TSSM's BSCOER, Narhe, Pune, Maharashtra, India

HOD, Department of Computer Engineering, TSSM's BSCOER, Narhe, Pune, Maharashtra, India

ABSTRACT: Distributed Denial of Service (DDoS) is amongst the most troublesome security issues to address. While several existing procedures (e.g., IP traceback) concentrate on following the area of attackers sometime later. DDoS is still an imperative security challenge for machine networks. Filter based DDoS defense is considered as a successful methodology, since it can defend against both victim-resource consumption attacks and link-congestion attacks. Deterministic Flow Marking (DFM) plan is used for extensive distributed attacks to the source node found in the LAN behind the edge routers. The deterministic system is picked over the probabilistic technique is because of the higher traceback correctness. Three main components which are DDoS detection component, IP Traceback component, Traffic control and Packet Filtering component have been introduced. The main objective of this method is to place the packet filtering and traffic control component close to the attack source and the victim respectively. By doing so, the traffic control component at the victim side and packet filtering component at the attacker side aims to set up a limit on the packet forwarding rate and improves the throughput of the legitimate traffic. DDoS packet tends to appear as legitimate packet, so filtering them with no impact on legitimate traffic is challenging.

KEYWORDS: DDoS, IP Traceback, Flow Marking, Authentication, Filtering.

I. INTRODUCTION

Now a days, much consideration has been paid for securing the internet foundation that has turned into an all-inclusive medium for a extensive scope of correspondences. A few security methodologies have been proposed for securing this foundation. The particular security issue, which is the principle center of this study, is anonymous attacks. Because of trusting nature of IP protocol, which initially exclude security as a configuration standard, the source IP location of a packet is not confirmed. Attackers are normally fascinated by hiding their character with fake locations[11].

(Distributed) Denial of Service ((D)DoS) attacks are case of unknown attacks where at present there is no apparent approach to avoid or follow them. While keeping all attacks on the internet is a long way from reality, at list a mechanism of recognizing the source(s) of the attack is required in a circumstance when prevention fails. This is the purpose behind planning IP traceback procedures[1][9][10].

Traceback is a name given to any strategy for dependably deciding the source of traffic on the system. Denial of Service (DoS) attacks represent an expanding danger to today's internet [9]. More genuine DSoS attacks are often mounted from hundreds or indeed a large number of hosts. A genuine issue to battle these DoS attacks is that attackers use erroneous, or spoofed IP addresses in the assault packets and henceforth mask the genuine root of the attacks. Because of the stateless nature of the internet, it is a troublesome issue to focus the source of these spoofed IP packets, which is known as the IP traceback problem[4][6].

To discover the wellspring of such an assault, few IP traceback systems are proposed. These approaches generally oblige that a few routers along the assault way insert stamping data to the packets to perceive the personality of the routers. In the wake of gathering a suitable number of stamped bundles, the exploited person has the capacity discover the assault way or the wellspring of the assault. In spite of the fact that the IP traceback methodologies[1][10][12] let

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

the victimized person to figure the wellspring of an assault. In general they can not diminish the effect of the assault while the attack is in advancement[3][12].

In this work, our objective is to investigate how far we can push a guard/security framework to relieve the effect of such an assault while the assault is in advancement. Our targets are to minimize the trouble of sifting on the partaking switches; to minimize the quantity of adjustments needed on the current conventions being used; and to augment the survival rate for the authentic movement under an escalated assault. To accomplish such an answer, here defense approach has been proposed. The proposed framework safeguards against DDoS assaults by organizing between the guard frameworks at the source and the victimized person closes. This requires correspondence between the exploited person and the sifting switches so the separating might be found as far away as could reasonably be expected from the victimized person.

II. RELATED WORK

In existing system many traceback approaches have been projected. On the basis of basic principle, processing mode and location the existing traceback schemes are categories.

Basic Principle:

If classified with basic principle, the offered traceback methods are discriminated into marking and logging groups. In marking methods [10], the travelling packets are added with particular information by some or all routers in the path. Using this information, even if the IP is spoofed, the attacker can be traced down. In logging method [9], the routers keep some information associated to the travelling packet. This information can be later on used to traceback to the sender node from which the packet has been originated.

Requirement of large amount of memory and CPU usage at routers of the attacked path creates a basic problem for logging method, as it stores information about each and every packet passed through the router [4].

Processing Mode:

Based on the processing mode, traceback schemes are distinguished in two groups: deterministic and probabilistic. In deterministic method, the packet should be practiced at source as well as at target, despite of marking or logging. Though this method provides superior accuracy, it requires more dispensation overhead at both source and the target, in assessment to the probabilistic method. Probabilistic methods are somewhat analogous to the deterministic methods, only the required processing time and bandwidth is comparatively less. Most of the existing traceback methods are probabilistic[1][10][11].

Location:

From the aspect of classification by locations, presented traceback methods can be divided into two groups: those that send traceback information by the edge routers next to the source, called source group and in the network by some or all routers in the assault path called network group. Most of the present traceback methods belong to the network group. The basic purpose of the group is to identify attack path entirely or moderately [2][13].

These methods requires inclusion of all routers and highly consumes resources such as processing time and memory. While, source group method aims at identifying the attack source and not the attack path [1][6].

On Deterministic Packet Marking [1] present a novel approach to IP traceback Deterministic Packet Marking (DPM). DPM is based on marking all packets at ingress interfaces. DPM is scalable, simple to implement, and introduces no bandwidth and practically no processing overhead on the network equipment. It is capable of tracing thousands of simultaneous attackers during a DDoS attack. This defense approach does not work in a situation where the purpose of the attack is to consume the victimˆas bandwidth, because it only relies on the DDoS packet filtering at the victim side [3].

In Probabilistic Packet Marking (PPM) for IP traceback against Denial-of-Service attack is presented in [13]. Non-preemptive PPM is performed while a marked packet is coming, but compensates the reduction of marking probability in marked-free packets. The non-preemptive compensation makes the probability of each marked packet arrived at the victim is equal to its original marking probability. This scheme efficiently improves the convergent amount of marked

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

packets required for reconstructing the complete attack path. The complexity for reconstruction at the destination side is more.

Another approach for detecting and responding to the spoofed attacks is to use IP tunneling between the entire edge routers and several tracing centers [8]. Once a DDoS attack is detected, the edge router forwards the victim traffic to the tracking centre. In doing so, the point of attack traffic entry to the internet can be detected. Besides the considerable overhead of IP tunneling on the edge routers, the tracking centre processes a large amount of traffic during the attack.

The other mechanism to counter the spoofed attacks is to employ an IP traceback. There are several attempts to integrate the traceback mechanisms with the real-time DDoS defense systems to react to the attacks while they are in progress [3][5][14][15].

Here, in [5] mechanism is suggested where the IP traceback and the packet filtering are integrated and work together. Thus, the victim resources are preserved, even before the traceback is completed. However, such a feature does not exist in the current traceback approaches. Secondly, the victim sends the identified attack path to all of the filtering routers. To avoid the extra communication overhead between the victim and the filtering router, the number of filtering routers and consequently, the distance between the defense systems and the victim is required to be low (in terms of the number of hops).

However the proximity of the defense systems and the victim may cause the filtering routers to be overwhelmed by an intense attack where the attackers are highly distributed over the network and can generate a high volume of attack traffic. More importantly, if the defense system is located near the victim, when a legitimate packet reaches to the filtering router, it most likely carries the marking information of an infected router, and therefore there is a low probability for it to escape the filtering.

The aforementioned defense system has been changed [4] to only rely on the edge router near the victim for both of the IP traceback and the packet filtering purposes. This defense scheme is interesting but if the attack is widely distributed over the Internet, this approach cannot differentiate between the legitimate and the attack traffic appropriately.

Pi approach that is a deterministic packet marking (DPM) mechanism and embeds the path fingerprint into every packet was proposed [2]. This defense approach does not work in a situation where the purpose of the attack is to consume the victim's bandwidth, because it only relies on the DDoS packet filtering at the victim side.

Limitations of Existing Traceback Methods:

- Heavy computational load for path reconstruction.
- Traceback is performed after an attack is identified and no initial defense is provided against attack.
- Existing methods contain involvement of routers along the path and consume their processing time and memory.
- Distance between the defense system and the victim is too far which results in extra communication overhead.

III. PROPOSED SYSTEM DESIGN

A. *System Overview:*

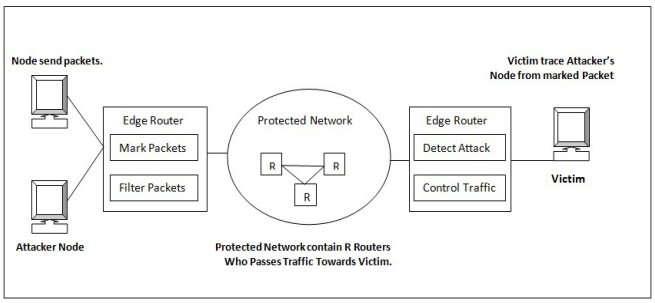

Fig. 1 Proposed System Architecture

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Fig 1. shows the proposed system architecture. Its blocks are explained below.

Normal Node: It sends legitimate traffic towards the victim through edge router.

Attacker Node: This node is responsible for attack in a network.

Edge Router: Edge router at source end receives packets from sender node. It marks the packet with packet marking scheme of DFM and send it towards the victim through protected network. This router is responsible for filtering the packets based on information received from victim end edge router if attack is found. Victim end edge router performs two operations: attack detection and traffic control. It will detect attack based on the information received from protected network and inform sender nodes through traffic control component to filter packets.

Protected Network: It consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.

Victim: Victim will trace the attacker node based on a information in marked packets and willreach and block the attacker node.

Packet Formation and Forwarding:
This module includes sending of packets from source to destination.

Detailed description of proposed system is explained below.

DDOS Detection segment:
This segment is utilized at the victimized person end edge network for perceiving abnormal changes on the network traffic. There are a few algorithms and instruments for catching DDOS attacks that can be utilized for this segment. The main moto in this paper is not to propose another DDOS detection algorithm.

IP Traceback segment:
The IP traceback segment utilizes the DFM traceback method to recognize the wellspring of a DDOS attack. This traceback instrument comprises of a light weight stream checking module running on the edge switches i.e. mark encoding and an imprint unraveling module running on the victimized person end i.e. mark decoding to deduce the wellspring of traffic focused around the data separated from the stamped parcels. A definite depiction of the DFM system could be found in our past work.

Traffic Control Segment:
This part comprises of two modules:

- Traffic Adjustment (TA) module.
- Packet Filtering (PF) module.

The TA module runs on the exploited person or the outskirt door gadget (e.g. firewall)of the exploited person network. In the wake of discovering the wellspring of the attack, utilizing IP traceback segment, the TA module sends an appeal message, which conveys attack traffic data, to the protection framework at the source-end edge network. Then again, the PF module runs on every edge switch and channels, filter packets that are administered to the exploited person based on the guidelines issued from the TA module.

Traffic Adjustment (TA) is used to control attack traffic . To select the rate limit for the specific router, traffic history for the TA module need to be considered, on the evaluation of traffic history the average traffic rate limit is considered as maximum traffic tolerance limit for the router. There are some phases to defense DDoS attack.

Connection Establishment:
The connection between sender and receiver is established by three way handshake algorithm .

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Congestion or Traffic Avoidance:

Traffic or congestion avoidance is performed by packet filtering module after receiving the message which says that destination is under the DDoS flooding attack. After flooding detection, the message is forwarded to source and the transfer rate is halved to the previous transmission rate and the process continues till the sender get the message that sending rate is tolerable.

Slow Start:

This phase is performed by packet filtering module. In this module, after the flooding attack when the destination is able to tolerate the current packet forwarding rate, the packet forwarding rate is increased linearly. Each increment in the rate is checked by victim response whether the current rate is tolerable or not and the victim should not go under the congestion. Packet drop rate is calculated by

$$\text{Drop Rate} = \frac{Sum\ Droped}{Sum\ Droped + Sum\ Sent} \quad \ldots\ldots\ldots\ldots \text{Eq. 1}$$

Where,

Sum Dropped – Number of packets dropped.

Sum Sent – Number of packets transmitted by sender.

Connection Termination:

The current dropping rate is zero means either the flooding attack is finished or the current packet forwarding rate is tolerable. If the current transmission rate is zero then PF module removes the rate limit and it terminates the virtual connection between the TA and PF.

B. Algorithm:

Step 1: Select file to be send;
Step 2: Generate a packet;
Step 3: Mark flow on packet at edge router;
Step 4: At intermediate node
Step 5: If attacker is present
Step 6: Random number of packets are flooded;
Step 7: Forward all packets;
Step 8: End if
Step 9: At Receiver Node
Step 10: Receiver all incoming packets
Step 11: check packet rate
Step 12: if(Current_rate > RateLimit)
Step 13: Flooding attack detected;
Step 14 :Notify packet filtering module;
Step 15 :Start packet filtering;
Step 16 :Start IP traceback;
Step 17 : End If.
Step 18: Check current packet rate;
Step 19 : if(Current_Rate < Rate_Limit)
Step 20 :Receive all packets;
Step 21 : End If

C. Mathematical Model:

Let S, be a system such that,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

S = {*s, e, X, Y, T, fme, DD, NDD, ffriend, MEMshared, CPUCoreCnt, φ*}
Where,
S− Proposed System
s− Initial state at T (init) i.e. constructor of a class i.e. SendPackets() function .

e−End state of destructor of a class i.e. ReceivePackets()function.
X− Input of system i.e. marked packets.
Y− Output of system i.e. filtered packets.
T− Set of serialized steps to be performed in pipelined machine cycle. In a given system serialized steps are Send Packets, Mark Packets, DDoS Detection, Traffic Control, Packet Filtering, IP traceback, Block Attacker, Receive Packets.
fme− Main algorithm resulting into outcome Y, mainly focus on success defined for the solution. In a given system it will be IP Tracebak and Traffic Adjustment algorithm.
DD− Deterministic Data, loading or assigning marks in IP header.
NDD− Non Deterministic Data of the system is time required to perform Traffic_Adjustment(), Packet_Filtering() and IP_Traceback().
Ffriend− Set of random variables, {0, 1}.
MEMshared− Memory required to process all these operations, memory will be allocated to every running process.
CPUCoreCnt− More the number of count double the speed and performance.
φ− Null value if any.

IV. EXPERIMENTAL SETUP

Real time dataset is most important for evaluation of any defense system. Due to privacy and legal issues there are very few dataset publicly present. For experimental result own dataset created by own network systems will be used and the transmission rates recorded for that system will be considered.

The system is built using Java framework(version jdk 6)on Windows platform. The Netbeans (version 6.9) is used as a development tool. The system doesn't require any specific hardware to run, any standard machine is capable of running the application.

To implement the proposed system a test network setup is needed including two separate LANs. One LAN is responsible for sending DDoS attack packets i.e. for introducing flooding in network. Second LAN is responsible for sending normal packets at normal data rate. Both LAN are connected to edge router. Two programs need to be implemented. One for TA module which will run on victim end and second for PF module which will run on edge router. Apart from this the DFM IP traceback algorithm's encoding and decoding module will be implemented at every edge router.

V. RESULTS AND DISCUSSION

Initially current packet forwarding rate is linearly. If suddenly after some time the packet forwarding rate is increased with higher rate and it goes beyond the tolerance threshold then the router is under the DDoS flooding attack. There should be high survival rate for legitimate traffic to achieve good defense against DDoS attack. To achieve this three parameters are considered:

Rate Limit (RL): It is a maximum rate of incoming packets from DDoS attacker that the victim can tolerate. It is defined by TA module before establishing connection between PF module. Unit of RL is Mb/s.

Increasing Rate (IR): In slow start phase, the PF module should gradually increase the forwarding rate by IR. IR can be calculated as a fraction of the last forwarding rate before the PF module performs the congestion avoidance phase and limit of IR is Mb/s.

Waiting Time (Wt): This parameter indicates the time intervals (in seconds) between each update in the forwarding rate during the slow start phase.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

All the three factor RL,IR and Wt are responsible for higher survival rate. These three factors should provide higher incoming rate of normal packets and lower incoming rate of attacker packet. If the survival rate is high then more the DDoS attack is tolerated by the system .

A. Results:

The following table shows dataset which is initial implementation result. It will be used for evaluating other experimentation parameter such as Attack Reduction Rate and Computational Cost. RL is calculated for PF and TA module based on this data rate given in table. Given table shows the initial implementation results and respective graph. Data rate is defined as the unit of data transmitted per unit time.

$$\text{DataRate (R)} = \frac{DataSize}{TimeRequired} \qquad \text{.....Eq. 2}$$

Sr. No	Data Size (Kb)	Time (ms)	Data Rate (Kbpms)
1	500	63	7.93
2	1000	94	10.63
3	1500	156	9.61
4	2000	203	9.85
5	2500	265	9.43
6	3000	297	10.10
7	3500	344	10.17
8	4000	391	10.23
9	4500	468	9.61
10	5000	484	10.33

Table 1: Values For Dataset And Normal Data Rate

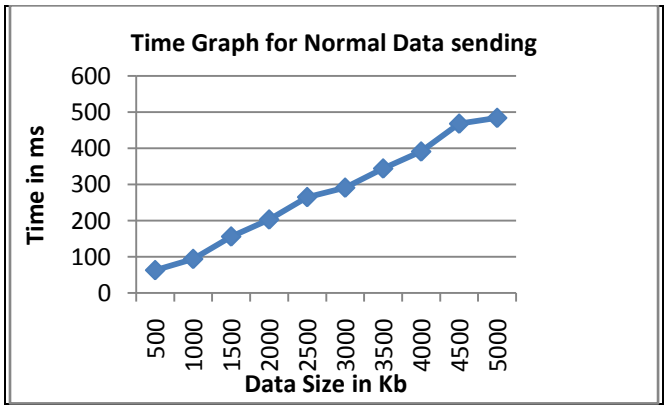

Fig. 2. Legitimate Traffic Data Rate

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Figure 2 shows graph of normal data rate based on given dataset. Flooding data rate is more than normal data rate and Filtering data rate or drop rate should be less than normal data rate.

RL is evaluated from the dataset by considering the number of times the data is transmitted from sender to receiver. RL is a threshold value. Therefore, flooding rate is greater than RL and filtering or drop rate should be less than RL.

Graph in figure 3 shows the time required for receiving packets at victim end. It shows two scenarios, one when attacker node is detected and second when edge router is detected. If exact attacker node is detected, then there is no need to perform packet filtering. Therefore time required to receive legitimate traffic is less.

In second scenario, only edge router of attacker node is detected. Therefore, packet filtering needs to be done at network to allow legitimate traffic only. Packet filtering requires more time.

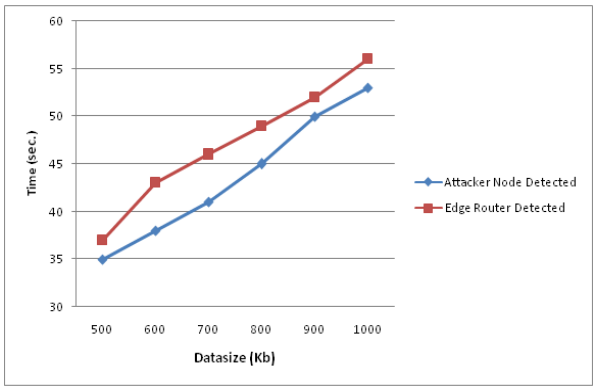

Fig. 3 Attack Traffic Data Rate.

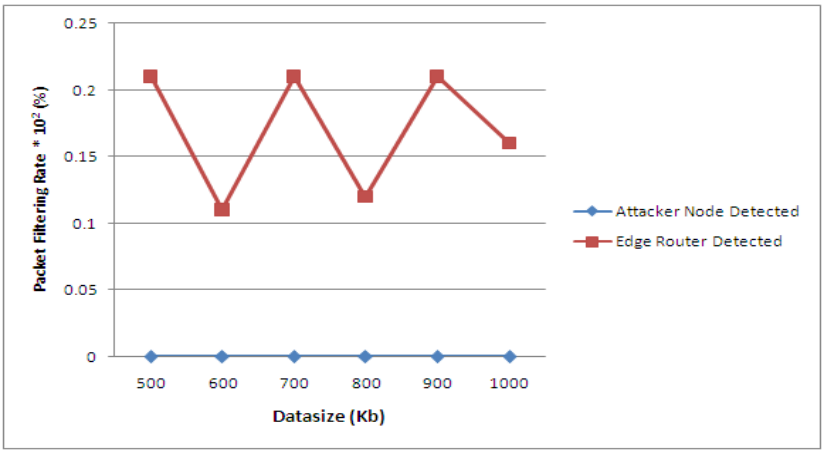

Fig. 4. Packet Filtering With and Without Defense System

Graph in figure 4 shows packet filtering rate in case of DoS attack. Graph shows two scenarios. When attacker node is detected, there is no need of packet filtering. Therefore, packet filtering rate is 0 in first scenario. In second scenario, when attacker's edge router is detected, packet forwarding rate is depends on RL and it varies based on incoming data rate.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

B. Attack Reduction Rate:

To determine attack reduction rate RL need to be considered. If the RL is low then it is more effective such that the small changes in data rates will be detected but it is undesirable. If the RL is high then it maximizes the impact of DDoS attack. When incoming traffic rates touches the RL, TA module on victim starts processing with PF module on attacker's edge router. RL is dependent on many factors such as traffic history, network bandwidth, CPU and memory usage of victim, etc. In first scenario in figure 3 & 4, attack is reduced to 100%. In second scenario, packet filtering is preventing a victim from attacker and attack rate is reduced.

C. Computational Cost:

To investigate the processing overhead of edge router that has direct impact on transmission, communication latency between TA and PF module need to be considered. Therefore, Wt is related to computational cost. If the waiting time increases then communication between TA and PF module decreases. Therefore, selecting an appropriate value for Wt parameter is tradeoff between the communication overhead and delay in the rate limit removal after the attack is over.

VI. CONCLUSION AND FUTURE SCOPE

Selecting the best method for packet marking is the key point in tracing the source IP. Challenges of previous IP traceback methods was, reconstructing the attack path efficiently and tracing exact attacker node hidden by a NAT or proxy server. These challenges are overcome by DFM IP traceback approach. In addition it provides optional authentication method. DFM provides higher traceback accuracy and authentication, but victim resources in attach path are consumed even before the traceback is completed. Therefore, a need arises to provide a mechanism to preserve the resources in attach path even before the IP traceback. To address this issue a traceback based defense mechanism is provided. It uses the strategy of detecting the attack and finding the attacker node when attack is in progress. Results shows attack is reduced 100% when exact attacker node is detected. When edge router in attacker network is detected, it reduced the DoS attack effect on victim. It prevents victim resources from being consumed even before attack is completed. There is a scope for reducing packet filtering rate, so drop rate will reduce automatically.

REFERENCES

1. Ansari N. and Belenky, "On deterministic packet marking", Computer Networks:The International Journal of Computer and Telecommunications Networking, Vol.51. No. 10, pp. 2677-2700, JUL 2007.
2. A. Yaar, A. Perrig, D. Song, "Pi: A Path Identification Mechanism to DefendAgainst DDOS Attacks", Proc. Symposium on Security and Privacy, 2003.
3. A. Yaar, A. Perrig and D. Song, "StackPi: new packet marking and filtering mechanisms for DDoS and IP Spoofing Defense", IEEE Journal on Selected Areas inComm., vol. 24, no. 10, pp. 1853a1863, Oct. 2006. ˆ
4. B. Gong., K. Sarac, "IP Traceback based on Packet Marking and Packet Logging",University of Texas at Dallas, 2005.
5. M. Sung and J. Xu, "IP traceback-based intelligent packet filtering: a novel technique for defending against Internet DDoS attacks", IEEE Transactions on Paralleland Distributed Systems, vol. 14, no. 9, pp. 861a872, Sep. 2003. ˆ
6. M. T. Goodrich, "Efficient Packet Marking for Large-Scale IP Trace back", Proc.Ninth ACM Conference of Computer and Communication Security, 2002.
7. M. Yang, "RIHT: A Novel Hybrid IP Traceback Scheme", IEEE Transactions onInformation Forensics and Security, vol. 7, no 2, pp. 789-797, Apr. 2012.
8. R. Stone, "CenterTrack: an IP overlay network for tracking DoS floods", 9th Conf.USENIX Security Symposium, Denver, pp. 199a212, 2000. ˆ
9. S. Matsuda et al., "Design and Implementation of Unauthorized Access TracingSystem", SAINT 2002.
10. S. Savage, D. Wetherall, A. Karlin and T. Anderson, "Network Support for IPTraceback", IEEE/ACM Transactions on Networking, 2001.
11. T. Subbulakshmi, I. A. A. Guru and S. M. Shalinie, "Attack Source Identificationat Router Level in Real Time using marking Algorithm Deployed in ProgrammableRouters", ICRTIT, 2011.
12. V. Aghaei-Foroushani and A.N. Zincir-Heywood, "Deterministic and authenticatedflow marking for IP traceback", The 27th IEEE International Conference on Advanced Information Networking and Applications (AINA), pp. 397-404, Barcelona,Mar. 2013.
13. Y. Tseng, H. Chen and W. Hsieh, "Probabilistic Packet Marking with NonPreemptive Compensation", IEEE Communications Letters, vol. 8, no. 6, pp.359a361, JUN 2004. ˆ
14. Y. You, M. Zulkernine and A. Haque, "A distributed defense framework forflooding-based DDoS attacks", 3rd Int. Conf. Availability, Reliability and Security,pp. 245a252,
15. Barcelona, Mar. 2008. ˆZ. Gao, N. Ansari, "Tracing Cyber Attacks from the Practical Perspective", IEEECommunications Magazine, 2005.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

BIOGRAPHY

Shubhangi R. Sardar is a Post Graduate student persuing M.E. in Computer Engineering from TSSM's BSCOER, Narhe, Pune, Savitribai Phule Pune University. She received Bachelor's Degree in Computer Engineering from Amaravati University in 2011.

S. M. Chaware is a Professor & Head Of Computer Engineering in TSSM's, BSCOER, Narhe, Pune, Savitribai Phule Pune University. He has completed his P.hd(Computer Engineering). His area of interest is in Information & Network Security, Wireless Network, Natural Language Processing, Information Retrieval.