IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-7, Issue-6, June 2019 E-ISSN: 2347-2693

Dynamic PID based approach for preventing DDOS attack in IP network

Vinutha Yadav D[1]*, Nagaraj J[2]

[1, 2]Dayananda Sagar College of Engineering , Bengaluru, Karnataka

DOI: https://doi.org/10.26438/ijcse/v7i6.512517 | Available online at: www.ijcseonline.org

Accepted: 10/Jun/2019, Published: 30/Jun/2019

***Abstract*—** One of the most common attack known as DDOS(distributed denial-of-service) attack are threat to the net. In DDOS attack the intruder makes use of scattered zombies in order to transfer a huge quantity of traffic to the targeted host, so that the legal users will not be able to access the network services or resources. The main cause for this attack to happen is the use of static PID's, as this static PID's remain constant throughout the session the intruder can easily trap these PID's used and launch the DDOS attack. In order to overcome this problem, here in this project work we plan, estimate and evaluate the use of dynamic PID. Here we make use of 16 characters pseudorandom dynamic PID's . In dynamic mode these PID's keep on changing throughout the session , this makes hard for the intruders to track the PID's and launch the attack.

***Keywords*— DDOS, Static PID, Zombies, Dynamic PID.**

I. INTRODUCTION

Distributed Denial of service(DDOS) attack is defined as an attack thrown by various intruder's host to single or multiple target system, by this the target system will no longer be able to deliver the network services or resources to its requested user. All this happens by distribution of huge quantity of requests at the same time by intruder's host to target system, this is termed as filling the capacity of the target system so that target system will no longer be active to respond to its legal users. By this the target system responds weakly or sometimes it may trash completely.

DDOS attacks are dissemination of DOS attack's. The process where one intruder system attack a single target system is known as DOS attack, this is one to one process. But in case of DDOS attack single or multiple intruder systems can be used to attack the target system, by this we can tell that DDOS attack causes more dangerous actions compared to DOS attack. DDOS attack harms server the most compared to DOS attack's. Therefore it's hard to handle DDOS attack than DOS attack's. To perform DDOS attack's the intruder makes use of a group of computer system's called as botnets. The intruder injects viruses and worms into the botnets and then launch the DDOS attack's. It is hard to find the attacker because the attacker uses the deceived IP addresses in the botnets which are all under the control of intruder's. Some of the well-known applications where DDOS attacks happen frequently are banking systems, debit credit transactions, online payments , hospital management system etc. The main of the intruder to launch this attack is to take revenge on their enemies, grab important information, to destroy the information system etc. In order to stop the target host from responding to the legal users the intruder makes use the complete capacity of the target system by sending unwanted packets to the target system at the same time when the legal user sends the request.

The figure below briefs about the DDOS attack:

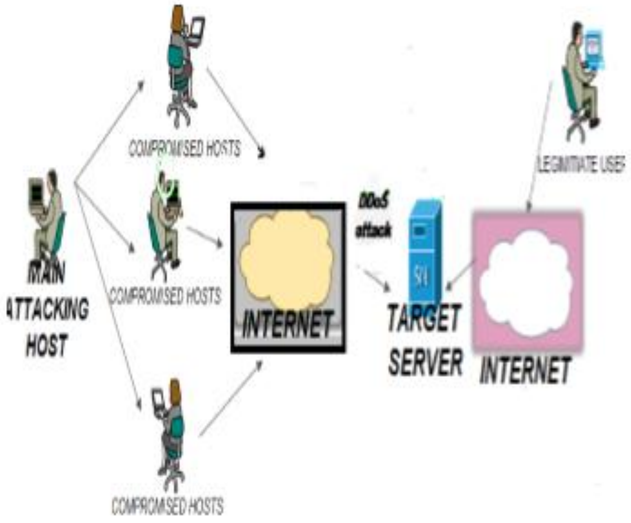


Figure 1:DDOS attack

Rest of the paper is organized as follows, Section I contains the introduction of DDOS attack, , Section II contain the related work of how DDOS was launched and what techniques where used to overcome it, Section III contain the proposed work and its architecture, Section IV contain the experimental results of snapshots which describes how the attack is launched and how it can be reduced using dynamic PID's, section V concludes research work .

II. RELATED WORK

Yang Xiang (2011) [1] has discussed about the most destructive type of attack known as low rate DDoS attacks. Two new approaches generalized entropy and information distance approaches are considered to detect the low rate DDOS attacks. The previous approaches Shannon entropy and kullback-liebler distance was also studied in this paper and Compare it with the new approaches. The alpha value of generalized entropy and information distance metric was adjusted to improve the detection rate. With the help of these two new metrics, it would be easy to differentiate between the legitimate traffic and the normal traffic. At last IP trace back method is used to find source of the attacker .This method is useful to stop the attack by examining the attacker.so this paper shows that the proposed technique is used to detect the attack low rate traffic and more reduce the attack rate.

M.Vijaylakshmi, Dr.S.Mercy Shalinie, A.Arun Pragash (2012)[2] has studied that IP traceback is the appropriate approach to find the source of the attack. This metric was used to detect the DDoS attacks in the network by tracing the router which is nearer to the incoming traffic. The tracing of the router is done by packet marking scheme in which each incoming packet is marked and then send to the network. This detection technique is used when the attacker launches the attack by sending spoofed IP addresses. These kind of attacks is performed in network and application layer. Proactive traffic shaping and reactive filtering mechanism were also used. It is used to evaluate the efficiency of the system and in this paper the test bed used was NTRO sensor smart and secure environment. The main contribution of this paper is to determine the attacker.

H.Bhuyan (2012)[8] has studied about the issues and the various challenges of the detection schemes which come under DDoS Attacks. The motive of this paper is to compare all the available techniques of detection. This study showed that all the methods of detection are not able to satisfy all needs of the network security or defense. Some possible solutions are also considered in this paper against DDoS attacks. Description of various kinds of tools is also described integrate its protocol and type of attack the tool can launch. This paper gives the revision of all the detection methods, and tools to perform an attack.

Ahmad Sanmorino (2013) [3] has proposed a pattern of matching detection technique that overcome the drawbacks of the other detection techniques of the DDoS attacks. Traffic flows through the network is checked based on the specified pattern and can easily find that packet is malicious or not. This technique of detection has an advantage of lower cost of infrastructure since it only uses routers and switches which exist already. It does not use high technology resources such as multicore CPU technology. This paper shows three topological environment which consists of 3 phases. In the Ist environment normal behavior of the traffic was shown, In the second phase unsecured network with attacks launched on it was shown. In the third phase handling of the attack was shown with firewall and successful dropout the packets.

PyungKoo(2013) [5] has studied that pseudo states in the router are one of the best method to protect the services. As routers, switches and other devices on the network are not much capable to differentiate between all the packets.so the service oriented based detection mechanism using pseudo state (SDM-P) is used to counter the attack packets before it falls into the network. A Hash key algorithm is used to evaluate the performance of this detection scheme. In other techniques the attack is detected when the services accommodation gets down, but proposed technique is used for the detection before entering the data packets. The implementation has done on the NS-2 platform to identify the difference between the packet whether it is legitimate packet out the attacker's packet.

According to the survey all the existing PID's are static in nature , which leads to easy DDOS attack by intruder. To overcome this our proposed solution deals with dynamic PID's throughout the session.

III. PROPOSED WORK

This work focuses on the plan, execution, estimation and use of the dynamic PID's and their processes. In this work we make use of 16 characters pseudorandom dynamic PIS's. In case of dynamic PID the PID's keep on changing throughout the session they update themselves after the pre-defined interval rate in order to transfer the packets to its destination host. In case if these dynamic PID's are trapped and if any unwanted requests are forwarded to the server by the intruder they all become invalid after some pre-defined specified time and the requests sent by the intruder using the trapped PID's these requests become invalid and discarded. Furthermore, the intruder may try to keep track of all the new PID's generated throughout the session and launch the DDOS attack , this raises the attacking rate and causes more overhead and confusion among the intruders, this in turn misguides the intruders.

Advantages of project

1. The cost of attacking is high , so attacks are reduced
2. Attacker can be identified.

The proposed System's architecture is shown below:

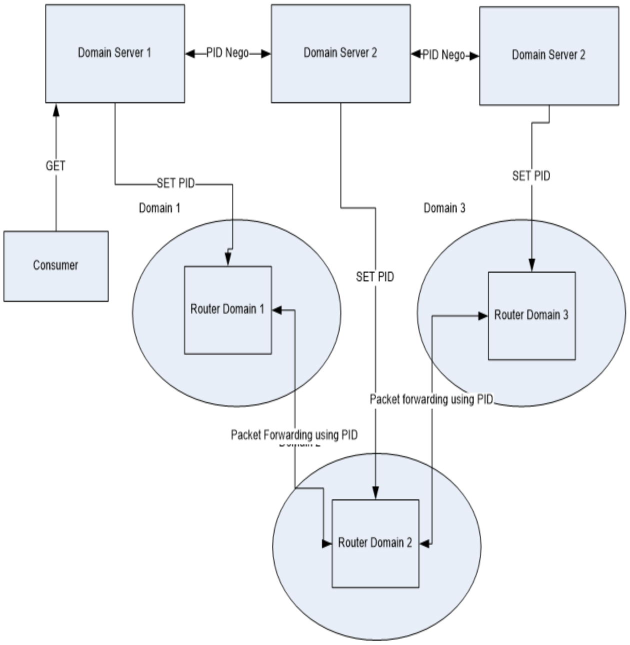


Figure 2: system architecture

There are three important components in the architecture

1. Consumer
2. Domain Name Server
3. Router

Consumer: When a client wants to access webpage or download content from server, it sends the GET request to its domain name server.

Domain Name Server: Domain name server on receiving GET request from it consumers, it negotiates with its next hop domain server. A PID is created identifying the router at domain and forwarded to next hop Domain server. Like this way, it happens till the Domain name server where the Consumer requested Web server is present. All Domain Name servers along the path from consumer to Web server refresh and generate new PID but still identify the same connection every refresh interval. Domain Name server advertise the next hop PID to its router.

Router: In every packet from consumer, the PID path(list of PID) along which the packet should be forwarded comes. Router checks the PID and forwards the packet to next hop. Router has the routing table mapping the PID to next hop domain. This information is provided by its domain name server.

Flow Chart

The flow chart of the PID handling in case of static routing is below:

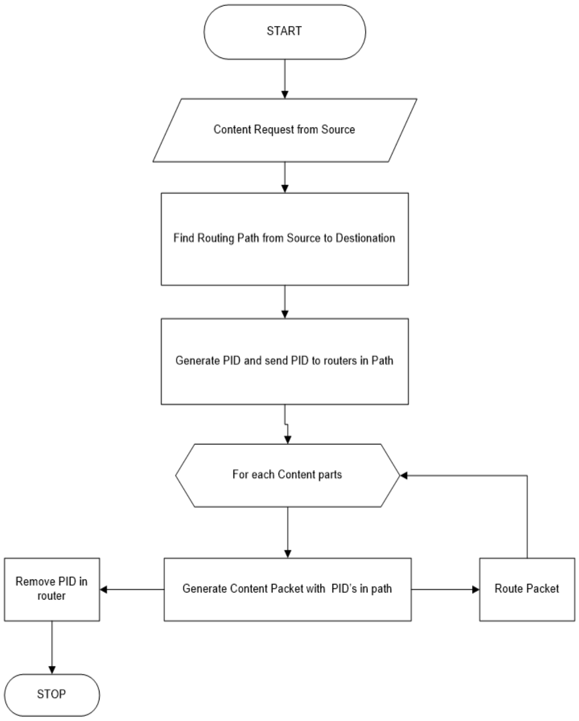

START
Content Request from Source
Find Routing Path from Source to Destionation
Generate PID and send PID to routers in Path
For each Content parts
Remove PID in router
Generate Content Packet with PID's in path
Route Packet
STOP

Figure 3:Flow chart in case of static routing

The flow chart of the PID handling in case of dynamic routing is below:

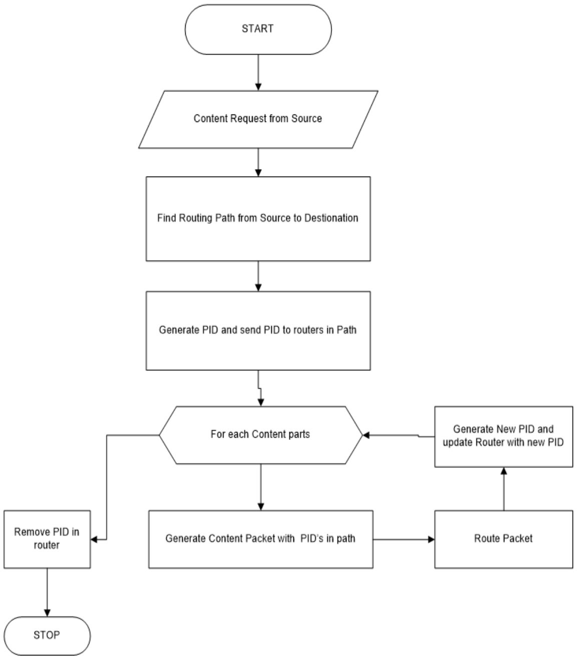

START
Content Request from Source
Find Routing Path from Source to Destionation
Generate PID and send PID to routers in Path
For each Content parts
Generate New PID and update Router with new PID
Remove PID in router
Generate Content Packet with PID's in path
Route Packet
STOP

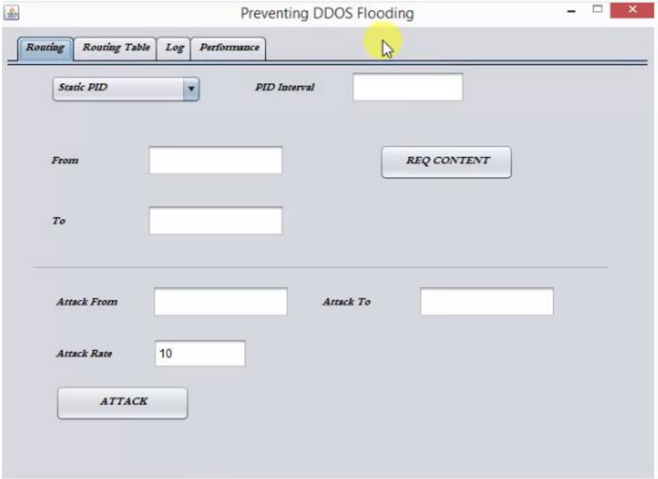
Figure 4:Flow chart in case of dynamic routing

IV. EXPERIMENTAL ANALYSIS

The following snapshots define the results or outputs that we will get after step by step execution of all the modules of the system.

Interpretation:

After successful compilation of the developed code all the outputs observed where recorded and snapped successfully and displayed below.



Static PID

Attack Rate: 10

Figure 5: Application is started.

This application gives us the option of selecting source and destination routers and request content among them. And also we can launch an attack between these two routers and observe the attack rate in both static and dynamic routing.

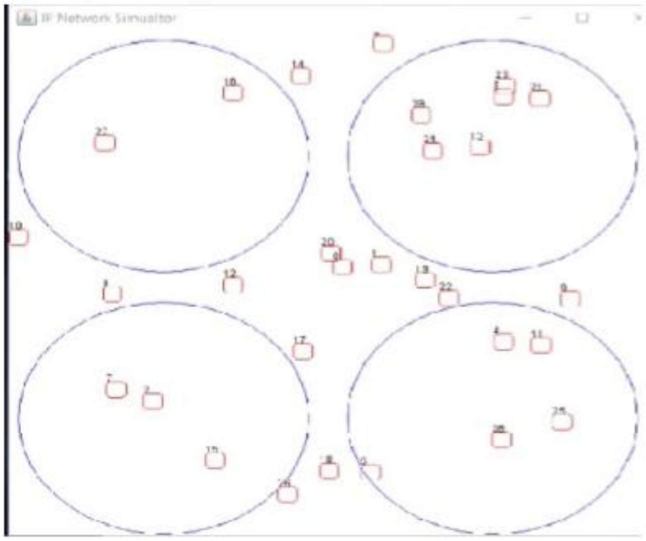
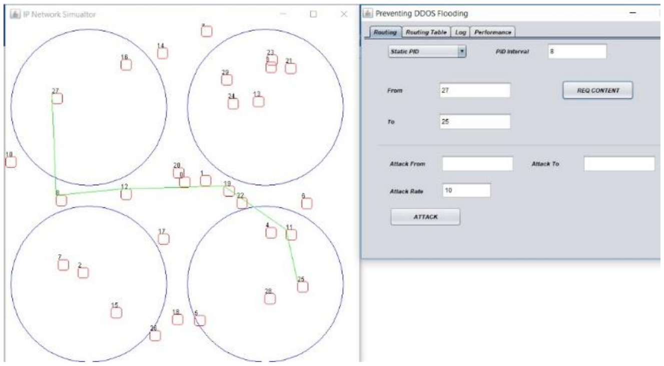


Figure 6:Routers are placed in the network

This snapshot consists of four network domains where each domain has routers in them here we can choose the source and destination routers and request content among them.

Execution in case of static mode



Static PID PID Interval 8

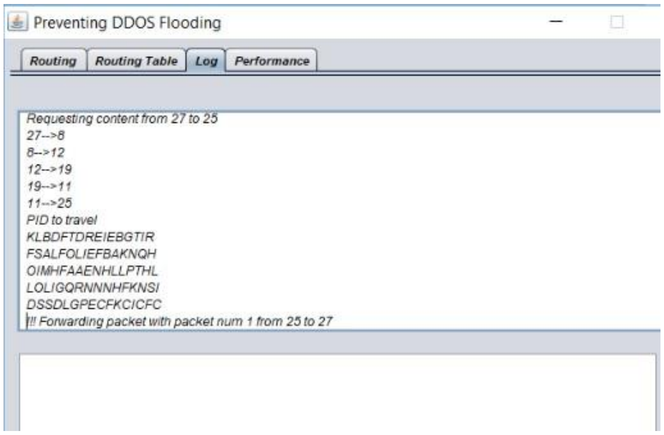
From 27

To 25

Attack Rate 10

Figure 7:Routing path is established

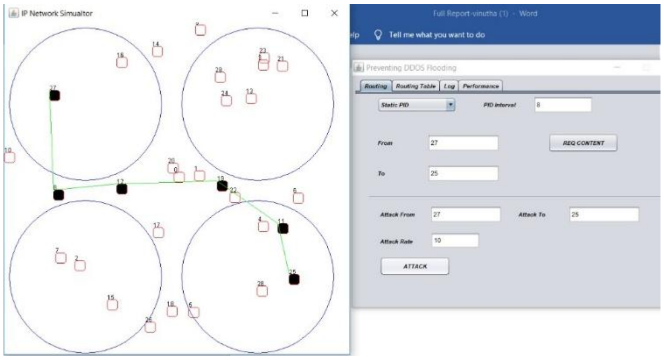
Once the content is requested the routing path is established between the source and destination routers.



```
Requesting content from 27 to 25
27-->8
8-->12
12-->19
19-->11
11-->25
PID to travel
KLBDFTDREIEBGTIR
FSALFOLIEFBAKNQH
OIMHFAAENHLLPTHL
LOLIGQRNNNHFKNSI
DSSDLGPECFKCICFC
!!! Forwarding packet with packet num 1 from 25 to 27
```

Figure 8:PID's in the path

Once the routing path is established the PIDs are generated among the path all these PIDs are 16 characters pseudorandom PIDs they remain constant throughout the session that is they are static in nature.



Static PID PID Interval 8

From 27

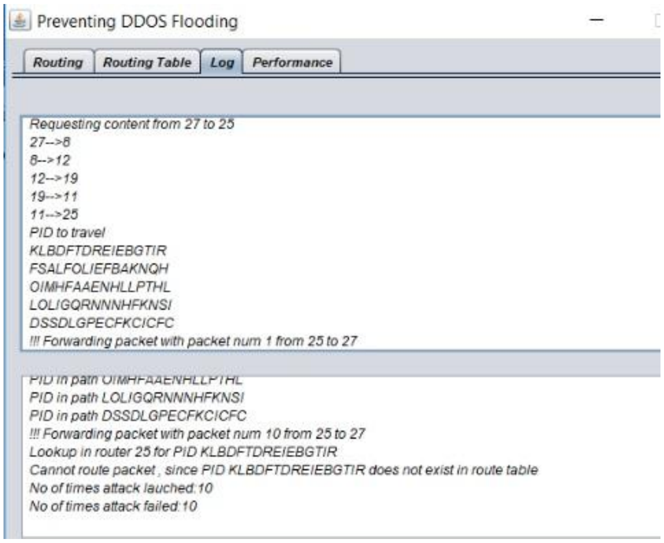
To 25

Attack From 27 Attack To 25

Attack Rate 10

Figure 9: Attack launched

Now attack can be launched between the source and destination routers in static mode.



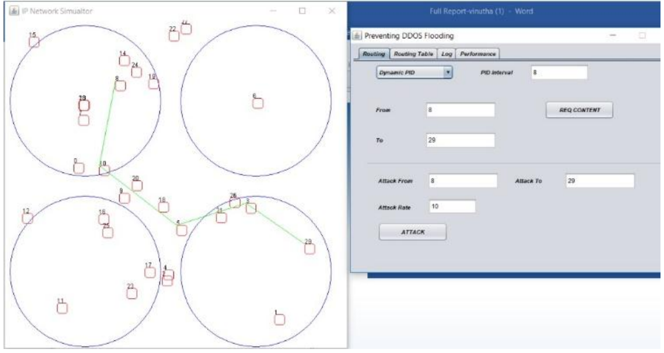
```
Requesting content from 27 to 25
27-->8
8-->12
12-->19
19-->11
11-->25
PID to travel
KLBDFTDREIEBGTIR
FSALFOLIEFBAKNQH
OIMHFAAENHLLPTHL
LOLIGQRNNNHFKNSI
DSSDLGPECFKCICFC
!!! Forwarding packet with packet num 1 from 25 to 27
```

```
PID in path OIMHFAAENHLLPTHL
PID in path LOLIGQRNNNHFKNSI
PID in path DSSDLGPECFKCICFC
!!! Forwarding packet with packet num 10 from 25 to 27
Lookup in router 25 for PID KLBDFTDREIEBGTIR
Cannot route packet , since PID KLBDFTDREIEBGTIR does not exist in route table
No of times attack lauched:10
No of times attack failed:10
```

Figure 10: summary of attack in case of static PID

As the PIDs remain constant in static mode its easy to launch DDOS attack by intruder so the attack was successful all the time in static mode.

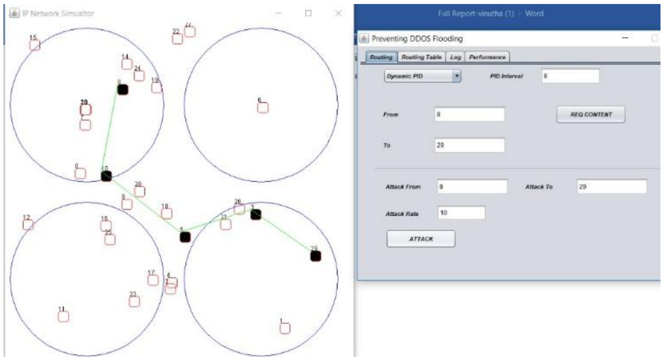
Execution in dynamic mode



Dynamic PID
PID Interval: 8
From: 8
To: 29
Attack From: 8
Attack To: 29
Attack Rate: 10

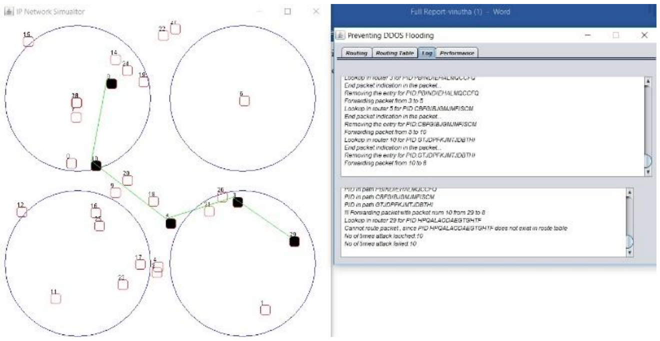
Figure 11:Execution in case of dynamic PID

We can switch to dynamic mode and request content from source to destination and also launch attack and see the attack rate in case of dynamic mode. Here we specify the interval rate at which the PIDs keep on changing after the interval rate, here the interval rate is 8 so after each 8 packets the PIDs keep on changing through- out the session.



Dynamic PID
PID Interval: 8
From: 8
To: 29
Attack From: 8
Attack To: 29
Attack Rate: 10

Figure 12:Attack launched in case of dynamic mode



```
Lookup in router 3 for PID PBINDIEHALMQCCFQ
End packet indication in the packet...
Removing the entry for PID:PBINDIEHALMQCCFQ
Forwarding packet from 3 to 5
Lookup in router 5 for PID CBFGIBJGMJMFISCM
End packet indication in the packet...
Removing the entry for PID:CBFGIBJGMJMFISCM
Forwarding packet from 5 to 10
Lookup in router 10 for PID GTJDPFKJMTJDBTHI
End packet indication in the packet...
Removing the entry for PID:GTJDPFKJMTJDBTHI
Forwarding packet from 10 to 8
```

```
PID in path PBINDIEHALMQCCFQ
PID in path CBFGIBJGMJMFISCM
PID in path GTJDPFKJMTJDBTHI
!!! Forwarding packet with packet num 10 from 29 to 8
Lookup in router 29 for PID HPQALACDAEGTGHTF
Cannot route packet , since PID HPQALACDAEGTGHTF does not exist in route table
No of times attack lauched:10
No of times attack failed:10
```

Figure 13: Summary of Attack launched in case of dynamic mode

As the PIDs keep on changing after the interval rate throughout the session the attack rate is reduced in dynamic mode compared to static mode. In case of dynamic routing the attack failed all the time as the PIDs keeping changing its hard to track PIDs and launch attack. Thus we can conclude that DDOS attack can be prevented by using dynamic PIDs.

V. CONCLUSION

Here in this project work, we present the plan, execution , estimation and use of dynamic PID's and their process mechanism. In this dynamic mode the PID's keep on changing throughout the session at a pre-defined interval rate. Path identifiers are the data communication system that help us in forwarding the packets to its respective destination hosts .Here in this project work a 16 characters pseudorandom PID's are generated in both static and dynamic mode. In static mode these PID's remain constant throughout the session but in case of dynamic mode they keep on changing after every pre-defined interval rate. In case if the intruder traps the PID they become invalid after the interval rate so its hard for him to keep track of every newly generated PID's and launch the DDOS attack's. Thus we can prove that by this work to some extent we can avoid DDOS flooding attack's.

REFERENCES

.

[1]. Yang Xiang, Ke Li, and Wanlei Zhou, Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 6, NO. 2, JUNE 2011.

[2]. Vijayalakshmi, Shalinie, Arun Pragash, IP Traceback System for Network and Application Layer Attacks, Recent Trends In Information Technology (ICRTIT), 2012 International Conference

[3]. Ahmad Sanmorino1, Setiadi Yazid2, DDoS Attack detection method and mitigation using pattern of the flow,2013 International conference of Information and communication technology(ICoICT)

[4]. Muhammad Aamir , Muhammad Arif, Study and Performance Evaluation on Recent DDoS Trends ofAttack & Defense, I.J. Information Technology and Computer Science, 2013, 08, 54-65

[5]. PyungKoo Park, SeongMin Yoo, Chungnam Nat, Service-Oriented DDoS Detection Mechanism Using Pseudo State in a Flow Router , 2013 International Conference on Information Science and Applications (ICISA)

[6]. Saman Taghavi Zargar, Joshi, Member, IEEE, and David Tipper,A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, ACCEPTED FOR PUBLICATION (2013)

[7]. Ilker Ozcelik, Yu Fu , Richard R. Brooks ,DoS Detection is Easier Now, 2013 Second GENI Research and Educational Experiment Workshop.

[8].Monowar H. Bhuyan1, H. J. Kashyap1,D. K.Bhattacharyya, Detecting Distributed Denial of Service Attacks: Methods, Tools and Future Directions, The Computer Journal first published online March 28, 2013

Authors Profile

Vinutha Yadav D has pursed Bachelor of Engineering from Visvesvaraya Technology University, Belagavi in 2017 and currently pursuing masters in M.Tech from Dayananda Sagar College of Engineering Bengaluru, Karnataka.

Nagaraj J pursed his Bachelor of Engineering, Masters and Ph.D from Visvesvaraya Technology University, and working as Assistant Professor in Department of CSE, DSCE, Bangalore.