RESEARCH ARTICLE OPEN ACCESS

Detecting And Preventing Of Dos Attacks By Dynamic Path Identifier Networks

P.Sudharsanarao [1], S.Durga Prasad [2]
Department of Computer Science Eingneering
Baba Institute of Technology and Sciences
Andhra Pradesh - India

ABSTRACT

These days, Denial of service (DoS) attacks, have turned into a noteworthy security threat to networks and to the Internet, DoS is destructive to networks as it defers genuine clients from getting to the server, when all is said in done, a few investigates were done to recognize and keep DoS from happening in a wide area network (WAN), however less inquires about were done on Local Area Network (LAN.), yet, detecting and averting DoS attacks is as yet a testing errand, particularly in LAN. In the meantime, as of late here are expanding interests in utilizing way identifiers PIDs that recognize ways between network elements as between space routing objects, since doing this not just aides tending to the routing adaptability and multi-way routing issues yet in addition can encourage the and reception of various routing structures. Which networks publicize the PIDs of way all through the Internet and a sender in the network builds its select pathlets into a conclusion to-end source course.

***Keywords*:-** DDoS Attack, Inter Domain, PID, attackers.

I. INTRODUCTION

This exploration researches the denial of service issue, with regards to services gave over a network, and adds to enhanced systems for demonstrating, detecting, and forestalling denial of service attacks against these services. While the greater part of at present utilized denial of service attacks expect to pre-emptively devour the network transmission capacity of exploited people, a lot of research exertion is as of now being coordinated at this issue. This exploration is rather worried about tending to the inescapable relocation of denial of service attacks up the convention stack to the application layer. Specifically compelling is the denial of service obstruction of key foundation conventions Along with the base advancements of PIDs and dynamic way identifiers, the theory features and talks about the significance of supporting innovations like combination, Big Data investigation and Develops that improve the business estimation of assembly. The end, outlines the entire work and calls attention to its advantages and shortages. It additionally talks about the following stages that could be taken to enhance the result. It sets inquiries for further work in this subject. Denial of services attacks (DOS) is a consistent risk to sites. DOS has gotten expanded consideration as it can prompt a serious lost of income if a site is taken offline for a significant measure of time; see [1-4]. There are numerous sorts of denial of service attacks yet two of the most well-known are Ping of Death and TCP SYN Flood. We have actualized these two strategies and include Distributed DOS (DDOS) too. In a Ping of Death assault, a host sends several ping demands (ICMP Echo Requests) with a huge or unlawful bundle size to another host in endeavor to thump it offline or to keep it so caught up with reacting with ICMP Echo answers that it can't service its customers. A TCP SYN Flood assault exploits the standard TCP three-path handshake by sending a demand for association with an invalid return address. In this paper we exhibit DDOS by making a worm like program that introduces programs on remote machines to assault a specific server. These assailants tune in out of sight for a message from an ace program that will advise these aggressors to dispatch a DOS assault against a machine. DDOS attacks are hard to stop since they can be originating from anyplace on the planet. We will actualize a DDOS assault by propelling the Ping of Death execution against an unfortunate casualty PC from a few different workstations. Presently, we manage a networking situation where the framework turns out to be increasingly confounded. The blast of cell phones, coming of cloud services and server virtualization are among the patterns driving the networking business to rethink customary structures of network. Presently since more gadgets are associated with the network, distinctive situations may organize an alternate parameter. Speed may be critical at times, though some circumstance requests a superior constant correspondence. There is a need to progressively design data, and in these cases the SDN becomes possibly the most important factor. Software Defined Networks [1] are utilized to isolate physical gear that store the information from their control instrument. In this framework, gadgets are available to store information and to deal with the information stream. By doing this, the general networking framework substantially more sensible and canny. One control plane can be utilized to oversee individual networking units, for example, switches and switches. Because of new networking model which permits dynamic software-based command over parcel routing, the switches and switches will never again be costly, disengaged, and restrictive equipment. The Denial-of-Service (DoS) assault is the most well-known vindictive assault. This assault developed progressively confused with the coming of IP spoofing and portable processing. Because of the simplicity of assault, anybody can cut down a site with a straightforward direction incite. The enterprises and governments keep on investigating better methods for assault counteractive action and identification. The deft acknowledgment of SDN makes new difficulties with respect to execution of security applications and versatility. So as to test new security applications successfully, a certifiable Design and Simulation system is vital. The objective of this paper is to build up a Design and Simulation system for DoS attacks on SDN networks. To accomplish this objective we utilize an accessible open source SDN reproduction device, Mininet [4] and for DoS assault age, IP flooding is utilized.

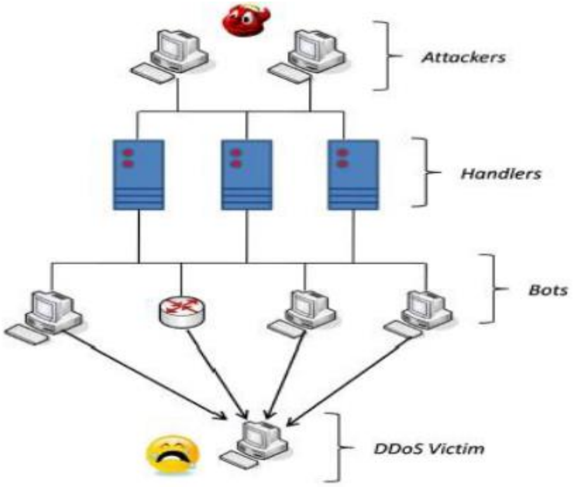

Fig 1. DDOS Attacks

II. RELATED WORK

1. Pack Wang, et al. talked about in [4] The creator propose approach FC-ANN, in view of Fuzzy grouping utilizing ANN calculation. They partition the engineering into three sections, Fuzzy Clustering Module, ANN module, Fuzzy Aggregation Module and chips away at KDD database. The consequence of the framework demonstrates that fluffy grouping with ANN gets the normal precision 96.71%, more prominent than BPNN for attacks other than flooding assault. Be that as it may, requirements to enhance the execution in the flooding kind of assault. 2. S.Chavan et al. proposed in [5], in that they utilize fake neural network (ANN) and fluffy Inference frameworks (FIS) together for the IDS. In that they make new neurons by utilizing ANN calculation and furthermore utilizes Fuzzy decides by utilizing calculation that utilization grunt to work there IDS so the aftereffect of the framework is rely on the execution of the Snort instrument. EFuNN took few moments to prepare the IDS models, ANN took couple of minutes to combine. Aside from U2R, the created fluffy surmising framework could identify with high exactness. The execution was debased when utilized all the 41 factors, which likewise delineates the significance of info variable determination. Additionally the examination results likewise uncover the significance of info variable decrease. By having under 40% of the first number of info factors. 3. Mitrokotsa et al. proposed in [6] In which they propose a methodology by utilizing developing SOM for discovery of DoS assault dependent on traffic order, for example, typical and strange. The methodology concentrating on the identification of DoS attacks in KDD99 information. In spite of the fact that their work demonstrated high precision (between 98.3% to 99.81%) and a low false alert rate (between 2.9% to 0.1%), the preparation methodology experienced a high computational overhead, particularly when the span of the preparation set was more than 10,000. 4. A.M. Chandrasekhar et al. proposed in [7],In that they proposed an idea of IDS by utilizing K-means and two arrangement calculations that is fluffy neural network and SVM classifiers. The proposed procedure has four noteworthy advances: initial one is to utilize Kmeans calculation to produce diverse preparing subsets. And after that neuro-fluffy models are prepared by utilizing that preparation subsets. After that characterization utilizing Support Vector Machine (SVM). The outcome demonstrates that the

general execution of their framework performs exceptionally well and accomplished 98.94% exactness if there should arise an occurrence of DOS interruption. 5. M. S. Abadeh et al. in [8], in that they endeavored to enhance fluffy guidelines by utilizing local pursuit administrators to look through their neighborhood the iterative learning approach. Arrangement rates of the three methodologies are superior to the triumphant passage at the Normal, DoS and Probe classes they accomplished 84.7% and 92.4%. 6. G.H. Kayacik et al. proposed in [9], In that they propose a methodology for IDS that depends on a progressive system of KSOMs. They attempt to characterize how far an interruption recognition approach utilizing a succession of various leveled SOMs utilizing just 6 highlights from the 41 highlights of KDD dataset. This grouping calculation essentially decreased the measurements seen by neurons in SOMs from the second layer. When contrasting their outcomes and best directed learning arrangements, their techniques have demonstrated a comparable identification rate however a higher FP rate. The real reason, in their point of view, is the accessibility of appropriate boosting calculations for unsupervised learning. 7. C. Jirapummin, N. et al. in [10], in that they propose framework dependent on SOM and Resilient Propagation Neural Network (RPROP) so as to accomplish ID joined with representation and order on ordinary traffic and interruptions. In tests, they perform both quantitative and subjective investigation. From IDS reproduction results accomplishes over 90% recognition rate and under 5% false alert rate in three chose assault programs. 8. Zheng Zhang et al. in [11],they portrays CIDS (Correlation Intrusion Detection System), a novel methodology in the recognition of DoS attacks that uses the adjustment in cross-relationship between's chosen highlights. As the DOS assault develops the cross-connections rise in this way noteworthy the assault..

III. DDOS ATTACKS CLASSIFICATION

On the basis of TCP/IP Protocol vulnerabilities, DDoS attacks are classified as shown in Fig.2

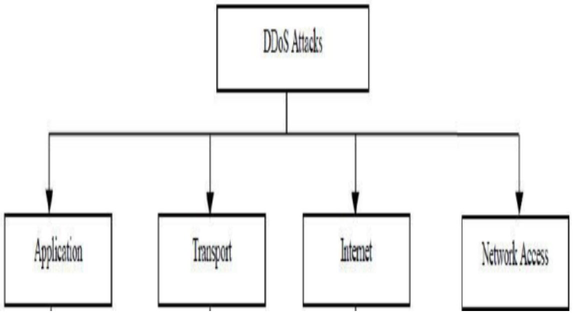

Fig. 2: Classification of DDoS Attacks Based On TCP/IP Vulnerabilities

A. Application Layer DDoS Attacks: An application layer DDoS attack is prepared mainly for explicit targeted purposes, including disrupting transactions and access to databases. They require a smaller amount of resources and often supplement network layer attacks. An attack is masked to look like legitimate traffic, except it targets particular application packets. The attack on the application layer can dislocate services such as the retrieval of information or search function as well as web browser function, email services and photo applications.

Following are some application layer DDoS attacks:

a) HTTP/HTTPS Flooding: HTTP flood is a type of Distributed Denial of Service (DDoS) attack in which the attacker feats HTTP GET or POST requests which looks real to attack a web server or application. HTTP flood attacks are volumetric attacks, frequently using a botnet —zombie army‖—a group of Internetconnected computers, each of which has been spitefully taken over, usually with the help of malware like Trojan Horses. An erudite Layer 7 attack, HTTP floods do not use deformed packets, spoofing or reflection techniques, and involve less bandwidth than other attacks to bring down the targeted site or server. This attack is disgrading in nature.

b) FTP Flooding: In this type of attack, the attacker exploits apparently-legitimate FTP requests to outbreak a FTP server or application. This attack is disgrading in nature.

c) Telnet DDoS: In this type of attack, the attacker distantly login into target system and the perform attack. This attack is disgrading in nature.

d) Mail Bombs: Attacker sends a immense amount of e-mail to a specific person or system. A huge amount of mail may solely fill up the recipient's disk space on the server. This attack is degrading in nature.

e) SQL Slammer: It is a computer worm that triggered a denial of service on some Internet hosts and intensely slowed down general Internet traffic.

f) DNS Flood: DNS floods are endeavored to exhaust server-side assets (e.g., memory or CPU) with a flood of UDP requests, created by scripts running on several conceded botnet machines.

B. Transport Layer DDoS Attacks: These types of attacks are usually encompassed of volumetric attacks that aim to devastate the target machine, denying or consuming resources until the server goes offline. In these types of DDoS attacks, malicious traffic (TCP / UDP) is used to flood the victim.The major categories of DDoS attacks under transport layer are following:

a) SYN Flooding: It is a form of denial-of-service attack in which an attacker sends a subsequence of SYN requests to a target's system in an attempt to ingest enough server resources to make the system unresponsive to legitimate traffic. It is generally degrading in nature. It is shown below:

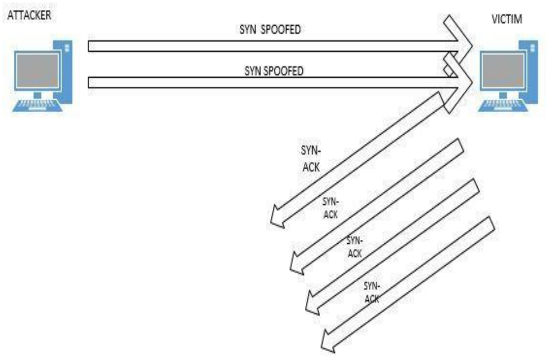

Fig 3: DDoS SYN Flooding

b) UDP Flooding : The attacker sends UDP packets, naturally big ones, to single destination or to random ports.It is generally disruptive in nature.It is shown below:

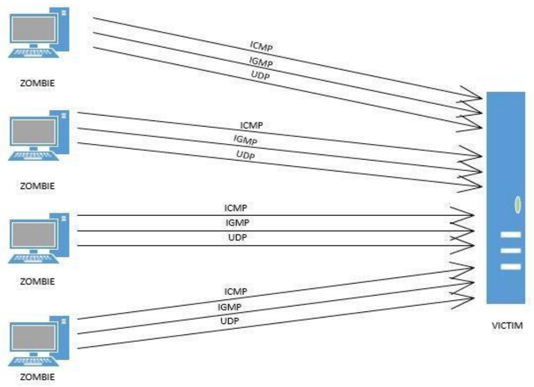

Fig 4: UDP Flooding

c) **TCP Null Flooding:** In this type of attack the invader send packets that have the no TCP segment flags set (six possible) which is invalid. This type of section may be used in port scanning. It is generally degrading in nature. Following are the six TCP flags:

- URG (U) – indicates that the Urgent pointer field is noteworthy
- ACK (A) – indicates that the Acknowledgment field is noteworthy. All packets after the initial SYN packet sent by the client should have this flag set.
- PSH (P) – Push function. Asks to push the buffered data to the receiving application.
- RST (R) – Reset the connection
- SYN (S) – Synchronize sequence numbers. Only the first packet sent from each end should have this flag set. Some other flags and fields modify meaning based on this flag, and some are only valid for when it is set, and others when it is clear.
- FIN (F) – No more data from sender.

C. Internet Layer DDoS Attack: These types of attacks occur due to vulnerability in internet layer protocols of the TCP/IP model. They are following:

a) **Smurf Attack:** In this type of attack, large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP Broadcast address. This attack is disgrading in nature. It is shown below:

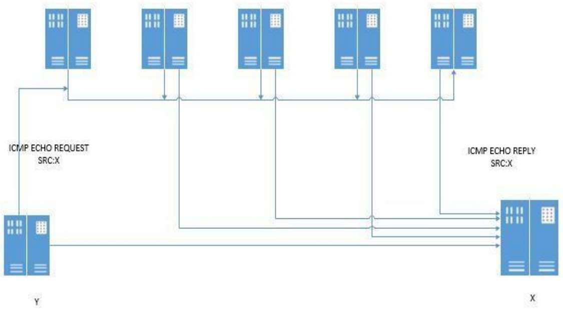

Fig. 5: Smurf Attack

b) **Fraggle Attack :**It is similar to smurf attack but insted of ICMP packets,large numbers of UDP packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP Broadcast address.This attack is disgrading in nature.

c) **TearDrop Attack: It** involves sending fragmented packets to a target machine. Since the machine receiving such packets cannot reassemble them due to a bug in TCP/IP fragmentation reassembly, the packets overlap one another, crashing the target network device.This attack is disgrading in nature.It is shown below :

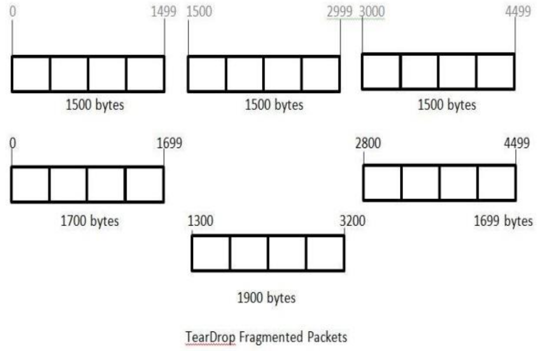

Fig. 6: Tear Drop Attack

In fig 6. there are three normal fragmented IP packets are having size 1500 bytes whereas the teardrop fragmented packets have varying sizes of 1700 bytes,1699 bytes and 1900 bytes respectively.When these teardrop fragmented packets are send to viictim machine,the machine will remain busy in assembling these fragments and will end up in denying services to other legitimate clients.Since these packets have different sizes,the machine is not able to reassemble these packets.

d) **ICMP Flooding:** Attacker overwhelms the victim with ICMP Echo Request (ping) packets.The attacker hopes that the victim will respond with ICMP Echo Reply packets, thus consuming both outgoing bandwidth as well as incoming bandwidth. If the target system is slow enough, enough CPU cycles can be consumed and the user notices a significant slowdown.This attack is disgrading in nature.It is shown below :

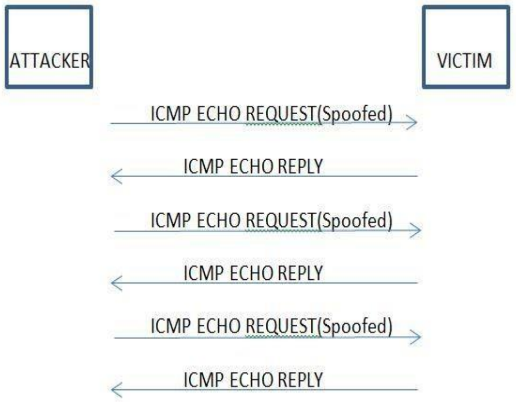
ATTACKER
VICTIM
ICMP ECHO REQUEST(Spoofed)
ICMP ECHO REPLY
ICMP ECHO REQUEST(Spoofed)
ICMP ECHO REPLY
ICMP ECHO REQUEST(Spoofed)
ICMP ECHO REPLY

Fig.7: ICMP Flooding

D. Network Access Layer DDoS Attack: These type of attacks exploit the weakness of network layer and its protocols. Following are the major types of DDoS attacks falls under this category:

a) **VLAN Hopping:** VLAN hopping is a computer security exploit, a method of attacking networked resources on a Virtual LAN (VLAN). This attack is disruptive in nature.As shown in fig 9. the attacker launches VLAN hopping attack by spoffing Dynamic Trunking Protocol(DTP) messages and causes the switch to enter trunking mode.

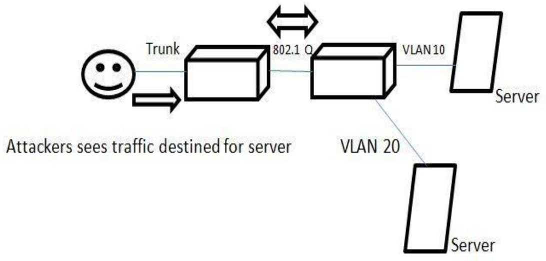

Fig.8: VLAN Hopping

b) **MAC Flooding:** MAC flooding is a method engaged to compromise the security of network switches. This attack is disgrading in nature.

c) **DHCP Attack :** Attacker avert hosts from gaining access to the network by refuting them an IP address by overwhelming all of the available IP address in the DHCP Pool. This attack is disruptive in nature. It is shown below :

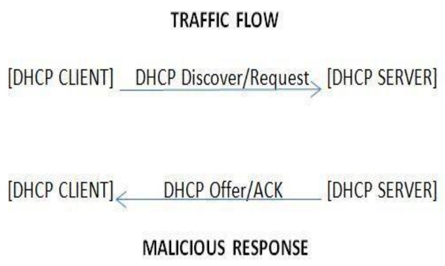

Fig.9: DHCP Attack

d) **ARP Spoofing:** ARP spoofing is a type of attack in which a malevolent actor sends falsified ARP (Address Resolution Protocol) messages over a local area network. This attack is disgrading in nature. Fig. 10 shows normal ARP traffic pattern. The sniffer snorts the traffic and sends malicious ARP messages to the target computer as shown in fig.11

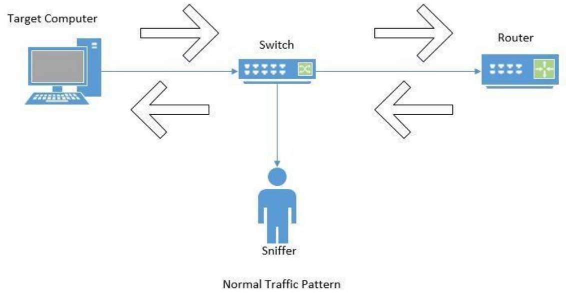

Fig.10 ARP Attack Normal Traffic

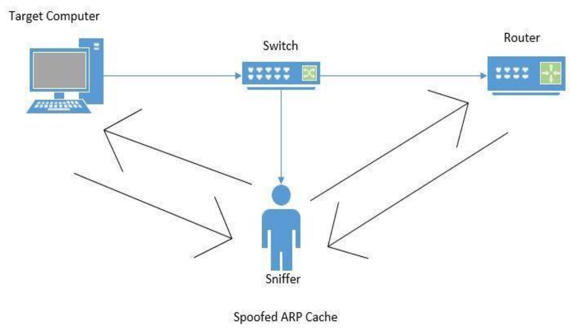

Fig.11: ARP Attack Malicious Traffic

Following are the reasons for speedy growth of Application Layer DDoS Attacks:

- These attacks are some of the most difficult attacks to alleviate against because they impersonate human behavior as they interrelate with the user interface.
- Attacker requires less resources and needs only information of susceptible IP and ports.
- Difficult to stop because they look authentic to classic firewalls which let them pass freely.
- Defending this classification of attack is difficult because network devices like switches, routers etc have no security at application layer.

IV. PROPOSED METHOD

The Source will peruse a file, give signature to all nodes, assign group PIDs to all groups and then send to particular user. After receipt the file he will get answer from the receiver. The Source can have skilled of employing the data file and adjusting keys / PIDs to all nodes before sending data to router.

The Router succeeds a multiple Groups to afford data storage service. In Group n-number of nodes are extant, and in a Router will patterned all PIDs and it will excellent the Neighbor node path. The router also will accomplish the following operations such as AdjustMac for all nodes, View all node details with Group PIDs and Data Signatures, Receive Data, Find neighbor nodes Path, Find Type of attackers, Send Attackers to NW Group Manager, Find Routing path, Find time delay and Throughput.

The group manager can allocate key for all and every group and a group each node has a couple of group public/private keys delivered by the group manager. Group name scheme can deliver authentications without worrying the anonymity. Every associate in a group may have a pair of group public and private keys issued by the group trust expert. Only the group trust authority can suggestion the signer's individuality and cancel the group keys. If any attacker will found in a node then the group manager will classify and then send to the specific users.

All the receivers can accept the data file from the provision supplier. The service provider will direct data file to router and router will join to all groups and guide to the particular receiver, without varying any file contents. The employer can only access the data file. For the user level, all the rights are specified by the NGM consultant and the Data users are meticulous by the NGM Authority only. Users may effort to contact data files within the router.

The attacker can occur the node in three ways Passive attack, DOS attack and Impression attack. Dos attack incomes he will inject fake Group to the particular node, Passive attack means he will alteration the IP address of the particular node and Impression attack means he will inject malicious data to the particular node.

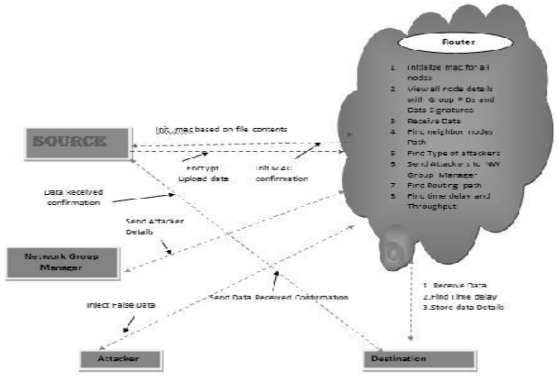
Router
1. Initialize mac for all nodes
2. View all node details with Group IDs and Data Signatures
3. Receive Data
4. Find neighbor nodes Path
5. Find Type of attackers
6. Send Attackers to NW Group Manager
7. Find Routing path
8. Find time delay and Throughput
SOURCE
Init. mac based on file contents
Encrypt Upload data
Init mac confirmation
Data Received confirmation
Send Attacker Details
Network Group Manager
Inject False Data
Send Data Received Confirmation
1. Receive Data
2.Find time delay
3.Store data Details
Attacker
Destination

Fig 12. Proposed Architecture diagram

V. CONCLUSION

In this paper, we proposed an approach for detecting and preventing DoS attacks, the proposed approach is called DPDoS and based on ensemble method from data mining, the proposed approach structure and components were presented and explained, it involved the following steps for detecting and preventing DoS attacks: data acquisition, DoS identification labeling, preprocessing, processing stage, and finally evaluation of the approach, in addition to a defense mechanism by PfSense firewall and snort tool. For evaluation purposes, we used confusion matrix method provided by Rapid Miner environment, experimental results show our approach performed significant improvement on Fmeasure results up to (99.95%), misclassifications (0.03) and accuracy (99.96%). The experimental results confirm our thesis, which says that the ensemble method has better accuracy than single classification techniques, our approach achieved the best classification accuracy for detecting DoS attacks, and preventing DoS attacks by a defense mechanism (snort tool on PfSense firewall) Possible directions for future work include applying mining techniques on dataset, to modify the approach to classify many types of DoS attacks on network. In addition, we will classify new types of attacks such as Probing, User to Root and Remote to User Attacks that can be applied by our approach, moreover, we will use many types of worms or intrusions that can be applied by our approach. Finally, we will try to make our approach to detect many types of threats, DoS attacks and worms with accepted and sufficient accuracy.

REFERENCES

[1] Hoda Waguih, „A Data Mining Approach for the Detection of Denial of Service Attack‟ IAES International Journal of Artificial Intelligence (IJ-AI), Vol. 2, No. 2, June 2013, pp. 99-106

[2] Yi-Chi Wu, Huei-Ru Tseng, Wuu Yang* and Rong-Hong Jan‟ DDoS detection and traceback with decision tree and grey relational analysis‟ Int. J. Ad Hoc and Ubiquitous Computing, Vol. 7, No. 2, 2011

[3] Dewan Md. Farid, Nouria Harbi, Emna Bahri, Mohammad Zahidur Rahman, Chowdhury Mofizur Rahman,‟ Attacks Classification in Adaptive Intrusion Detection using Decision Tree „International Journal of Computer, Electrical, Automation, Control and Information Engineering, Vol:4, No:3, 2010

[4] Majed Tabash, Tawfiq Barhoom, „An Approach for Detecting and Preventing DoS Attacks in LAN‟,International Journal of Computer Trends and Technology (IJCTT) ,Volume 18 Number 6 – Dec 2014

[5] Kiri Wagsta,Claire Cardie ,Seth Rogers ,Stefan Schroedl,‟ Constrained K-means Clustering with Background Knowledge‟ Proceedings of the

Eighteenth International Conference on Machine Learning, 2001, p. 577-584.

[6] Mangesh D. Salunke ,Prof. Ruhi Kabra,‟ Denial-of-Service Attack Detection „International Journal of Innovative Research in Advanced Engineering (IJIRAE) „„Volume 1 Issue 11 (November 2014)

[7] Xiaonan Zang, Athichart Tangpong, George Kesidis and David J. Miller, „Botnet Detection Through Fine Flow Classification‟,CSE Dept Technical Report No. CSE11-001, Jan. 31, 2011.

[8] Mangesh Salunke, Ruhi Kabra, Ashish Kumar.‟ Layered architecture for DoS attack detection system by combine approach of Naive bayes and Improved K-means Clustering Algorithm‟, International Research Journal of Engineering and Technology (IRJET), Volume: 02 Issue: 03 ,June-2015

[9] V.Vapnik.The Nature of Statistical Learning Theory. NY:Springer-Verlag.1995

[10] Vipin Das , Vijaya Pathak, Sattvik Sharma, Sreevathsan, MVVNS.Srikanth,Gireesh Kumar T,‟ NETWORK INTRUSION DETECTION SYSTEM BASED ON MACHINE LEARNING ALGORITHMS‟, International Journal of Computer Science & Information Technology (IJCSIT), Vol 2, No 6, December 2010

P.Sudharsanarao is presently pursuing M.Tech (CST) Department of Computer Science Engineering from Baba Institute of Technology and Sciences,Visakhapatnam.

S.Durga Prasad , M.TECH is working as an Associate Professor in the Department of Computer Science and Engineering in Baba Institute of Technology and Sciences, Visakhapatnam.