International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Detection And Mitigation of Distributed Denial of Service Attack by Signature based Intrusion Detection System

Hardik M. Shingala[1], Mukesh Sakle[2]

[1] Computer Science & Engineering, Parul Institute of Engineering & Technology, P.O.Limda, Ta.Waghodia - 391760
Dist. Vadodara, Gujarat (India)

[2]Assistant Professor, Information Technology, Parul Institute of Engineering &Technology, P.O.Limda, Ta.Waghodia - 391760
Dist. Vadodara, Gujarat (India)

Abstract: ***Distributed Denial of Service (DDoS) attack is the most effective and comparatively easy to create. This attack has a terrible effect on the network. This attack can be carried out easily. But as the problem is the solutions are also for the attack. Here we propose an idea of IDS which is inside router and can protect it much better than any other protocol change. Because as we see that all protocol must need to coordinate with each other and that is not possible because not all router uses same security as ours. So to solve this problem we need to have a standalone system that can handle this kind of attack. The Intrusion Detection System (IDS) is one solution that we proposed here which will help us to identify that when the attack is going on and after that to protect our router form that attack. Here we proposed a signature based host IDS so that all the signatures of the attack is inside the IDS from the beginning and thus we can identify the packets as quickly as possible.***

Keywords: Distributed Denial-of-Service Attack, Intrusion Detection System

1. Introduction

A computer network is a system that allows a many number of computers to be interconnected. Network is a mode of access between distant places for the data to transfer easily to one computer to another. During the process of sending and receiving data there are risks of files being hacked. So, in order to protect such attempts by hackers, network security is essential. The main purpose of setting up network security is to avoid the misuse or unauthorized access to the network or its component parts. Networks are large and small in size but for network security, size is not an issue. So for a network to be protected against losses, it is important to secure it with strict rules, which can do through network security.

1.1 Issue of network security

Network security is very important to protect confidential documents against misuse of the system. There are a number of drawbacks that can arise if network security is not launched:

1) **Violation of Confidentiality**: Every business has some information that is required to be kept confidential from other competitors and even from their own employees.
2) **Damaging Data:** Data is an important and valuable asset for any company or sole proprietor as it is the core of what your information is based on. So, backup scripts are also set for the data to be stored on other available media. If the data is damaged by any means, then the victim will face severe loss and can cripple the business severely.
3) **Manipulation of Data:** When data is hacked, the hacker often leaves behind a token of accomplishment which shows how easily your network can be accessed without network security. Even riskier than all this is the manipulation of data in which the data is changed with another type. If your data is built up with values and numbers then they can be changed and the result gets devastating when reconciled and all the hard work is lost or destroyed.

1.2 Need of Attribute for secure network

1) **Access:** Authorized users are provided the rights to communicate
2) **Confidentiality:** Information in the network remains private
3) **Authentication:** Ensure the users of the network are authenticated or not
4) **Integrity:** Ensure the message has not been modified in transit
5) **Non-repudiation:** Ensure the user does not refute that he used the network

We are creating an Intrusion Detection System to protect router from bandwidth starvation attack. After creating an attack to router next task is to identify the attack packets which are ICMP echo request packets. Here we have to identify the packets entering inside the router. To identify packets we are using signature based Intrusion Detection System (IDS) approach. This means that the signature of the packet is already inside IDS to protect against this kind of attack. After identifying the attack on router IDS can take impropriate steps to prevent the attack from happening.

Bandwidth Starvation attack also known as DDoS (Distributed Denial of Service) attack is quite effective and have a devastating effect on network. In this attack attacker floods tons packets in to network towards the target server. In order to do so the attacker takes over many PCs that is connected to the internet and converts them in to zombies.

Zombies are the kind of PCs which are controlled by the attacker and can make them to do anything that they are no supposed to do.

The attacker communicates with the army of zombies which are called botnet and make those PCs send packets into network towards the target server. To protect this attack there are many algorithms but the main problem is that these algorithms need to be not in to two three but all the other routers to. But as we know that it is not possible that all routers have same algorithm as we are using for the router we tries to protect. Because of this problem to protect router we need one protection mechanism such that it can protect router without relying on any other router.

1.3 Modules of IDS

Data gathering: this module collects audit data (network activities) from a given network in normal condition within its observable radio transmission range.

Profile generation: this module has two subsystems:

1) Data preparation: here the collected data are prepared for creating normal behavior profile. Processes like filtering, aggregation, data suppression are applied here.
2) Profiler (Profile generator): the second phase is made up of several techniques like clustering, classification rule mining or SVM where normal profile is made by the preprocessed data. A normal profile is an aggregated rule set of multiple training data segments.

Anomaly Detection: This phase detect anomaly in the network with the help of derived rule set in this module, test data profiles are compared with the expected normal profiles. Any rules with deviations beyond a threshold interval are considered as anomalies. Suppose some rule generated from test data was not previously available in normal profile then it will be detected as anomaly, it is considered as an anomaly rule; if the rule is in the rule set, but its support and confidence level is beyond the interval [minimum - threshold, maximum + threshold], the pattern described by the rule becomes unusual, is consider as an anomaly rule.

Decision tacking system: when any anomaly rule trigger that will be attended locally as well as globally by giving alert to the neighbours when the support and confidence of anomaly rule goes above tolerated level. Here are some attack those are possible at different layer.

2. Literature Survey

2.1 Denial of Service Attack (DoS) on Networks

DoS are the disruption of services by attempting to limit access to a machine or service instead of subverting the service itself [8].

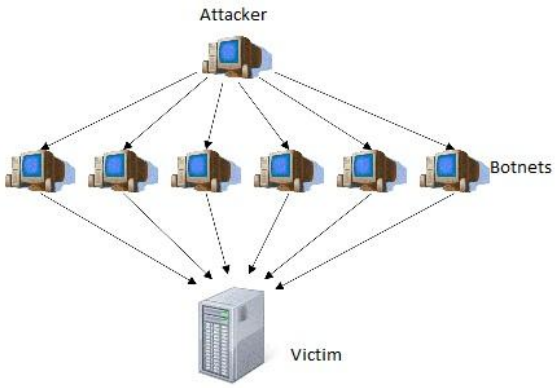


Figure 1: DoS Attack Scenario

2.1.1 Distributed Denial of Service (DDoS) Attack on network

DDoS attack uses many computers to launch a large scale coordinated DoS attack against one or more targets. DDoS attack has the capability to exhaust victim's computing and communication resources within a short period of time.
DDoS attack is done by dropping data/packets, flooding the network with extra messages, corrupting routing tables, counterfeiting network acknowledgements.

2.1.2 Attackers Motivations for doing the DDoS attacks

Financial/economical gain
Revenge
Ideological belief
Intellectual challenge
Cyber warfare

2.1.3 Network level DDoS flooding attacks: These attacks are launched using UDP, TCP, ICMP protocol packets. The types of attacks in this category are as follows [6]:

Flooding attacks: Attackers focus on disturbing genuine user's connectivity by exhausting victim network's bandwidth (e.g., Spoofed/non-spoofed UDP flood, ICMP flood, VoIP Flood and etc.)[6].

Protocol take advantage of action flooding attacks: Attackers takes advantage of specific features or implementation bugs of some of the victim's protocols in order to consume the victim's resources (e.g., TCP SYN flood, TCP SYN-ACK flood, ACK & PUSH ACK flood and etc.)[6].

Reflection-based flooding attacks: Attackers generally send forged requests (e.g., ICMP echo request) instead of direct requests to the reflectors; so, those reflectors send their replies to the victim and consume victim's resources (e.g., Smurf and Fraggle attacks). [6]

Amplification-based flooding attacks: Attackers take advantage of services to produce multiple messages for each message they receive to increase the traffic towards the victim. Botnets have been frequently used for reflection and amplification purposes. Reflection amplification techniques are generally used as Smurf attack where the attackers send requests with spoofed source IP addresses (Reflection) to a large

number of reflectors by take advantage of spoofing IP broadcast feature of the packets (Amplification).[6]

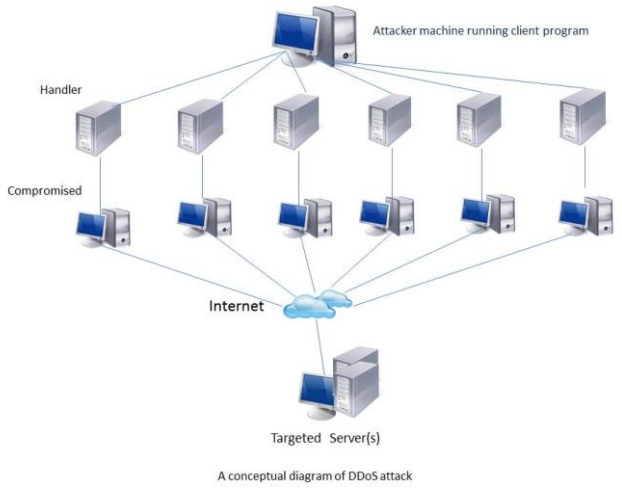


Figure 2: DDoS Attack Scenario

2.2 Analysis of a denial of service attack on TCP [1] (SYN Flooding)

2.2.1 SYN KILL [1]

Software tool called SYN KILL that lessen the impact of SYN flooding attacks, and in many cases defeat attacks completely. The program requires the ability to monitor and inject network traffic to and from the machines it is protecting. Ethernet is an example for a networking technology that satisfies this requirement. The program is called a monitor, because it reads and examines all TCP packets on the LAN after setting its network interface into promiscuous mode. The program is called active, because it can generate TCP packets in response to observed traffic and inject them into the network. Here SYN request go through SYN KILL and then the victim and then victim sends the ACK to the source. Now the software sends ACK to the victim on behalf of the source and waits till the time out. If the sources do not reply in time the connection is dropped and software sends reset packet to the victim. If reply comes then communication goes on.

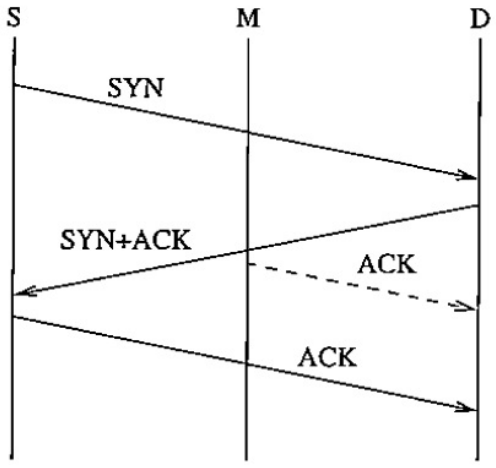


Figure 3: Flow of SYN KILLS

2.2.2 DelAy pRoBing (DARB) [2]

Delay is estimated using a method called DelAy pRoBing (DARB). The DARB traces outgoing paths toward network destinations by sending packets width special time to live (TTL) fields in the IP layer and then recording their time of deaths. The IP TTL field limits the lifetime of packets transmitted across the Internet and is decremented by each forwarding device (routers). If the TTL field reaches zero before the destination host is reached, the router drops the offending packets and transmits an ICMP(Internet Control Message Protocol) TTL exceeded in transmit error message to the original host, informing the original host of the packets timeout. If the packet has been created appropriately, the destination host should return null packet to the original host when the packet reaches its destination. The time stamps of both the sent out packets and ICMP replied packets are recorded to calculate the delay between the original host and each router. The adopted DARP is similar to trace route, which works by sending packets with progressively longer TTL value.

2.3 Adaptive bandwidth allocation approach to defend DDoS attack [3] (Data Flooding Attack)

2.3.1 Adaptive Bandwidth Allocation [3]

By separating normal users from malicious users by of the Average Packet Rate (ARP), and balancing bandwidths according to bandwidth flows, Quality by User (QBS) is attained to safeguard the normal users. Usually packet flows of normal users are in small amount and in short time span, which might flood the network and stop network providers from providing services to users.

2.3.2 Ingress/Egress filtering [4]

Ingress Filtering is a restrictive mechanism to drop traffic with IP address that do not match a domain prefix connected to the ingress router. Egress filtering is an outbound filter, which ensures that only assigned or allocated IP address space leaves the network. A key requirement for ingress or egress filtering is knowledge of the expected IP addresses at a particular port. For some networks with complicated topologies, it is not easy to obtain this knowledge.

2.3.3 SIFF (Stateless Internet Flow Filter) [5]

The SIFF system provides a server with the ability to establish privileged communication with whatever clients. Privileged packets carry capabilities that are verified by the routers in the network, and are dropped when the verification fails. SIFF are programmed to give preferential treatment to privileged packets, so that privileged packets are never dropped in favor of unprivileged ones.

2.3.4 Router based packet filtering [4]

Route based filtering extends ingress filtering and users the route information to filter out spoofed IP packets. If an unexpected source address appears in an IP packet on a link, then it is assumed that the source address has been spoofed, and hence the packet can be filtered. RPF uses information about the BGP routing topology to filter traffic with spoofed source addresses. But recent router changes, BGP message spoofing and proper IP selection can bypass this filtering.

2.3.5 History based IP filtering [4]

Normal day IP and attack day IP are different is the base idea for this filtering technique. It uses the IP Address Database

(IAD) to keep trace of the IP address. In attack if IP is in IAD then only allowed otherwise it is dropped.

2.3.6 Capability based method [4]

Source first sends request packets to its destination. Router marks are added to request packet while passing through the router. If permission is granted then destination returns the capabilities, if not then it does not supply the capabilities in the returned packet. A system requires high computational complexity and space.

2.3.7 Secure Overlay Service (SOS) [4]

All traffic first sent to Secure Overlay Access Point (SOAP). Authenticated traffic routed to node called beacon by consistent hash mapping. From there another node called secret servlet for further authentication.

3. Proposed System

We have a flowchart of a simple signature based IDS configured inside the router. Here first packet comes and identified inside IDS of signature database. After that it gives the result of the signature and acts accordingly. If the signature matches than the packet is malicious and it discards else it sends the packet for further processing.

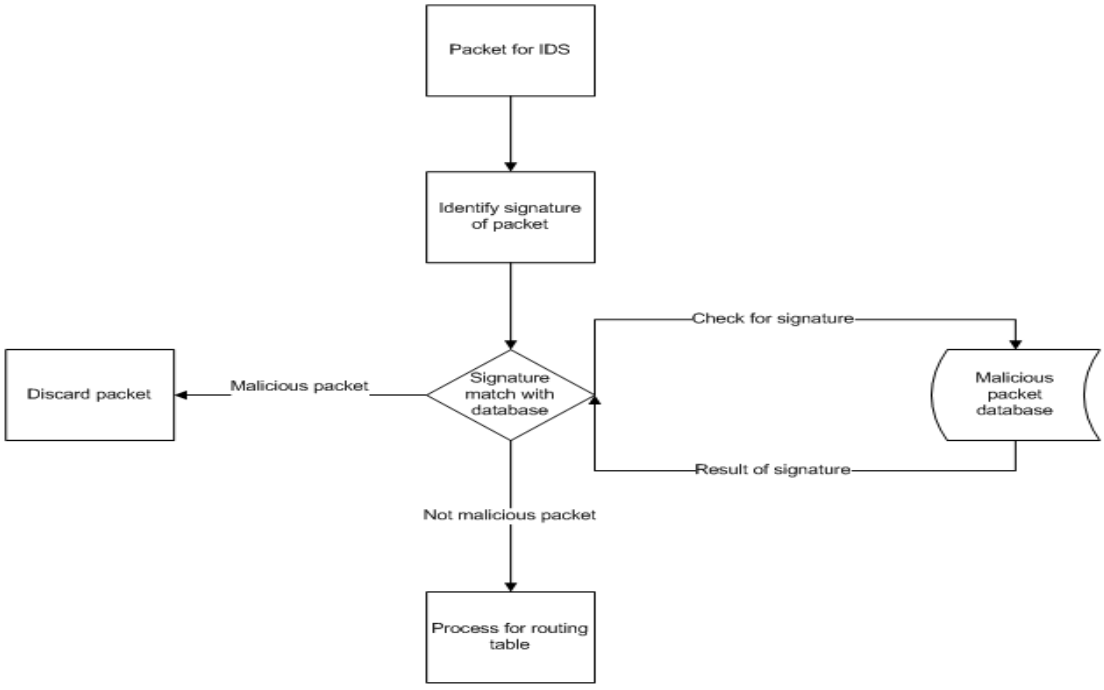


Figure 4: Simple IDS flowchart

After knowing the signature of a packet detecting of attack packet is the next thing that any IDS must do. For detect any attack packet IDS needs to have a database of the attack packet signature which are identified as attack packet signature. Here we have one database of packet signature in which we are detecting only ICMP packets and not any other packets.

Now here in ICMP packet one signature which is very important and which is if the ICMP packet is echo request packet than maximum size of the packet is 64 bytes and if the packet is echo reply than maximum packet size is 76 bytes. As it is defined in normal scenario ICMP packet size is no more than 76 bytes but in attack scenario packet size is more than normal scenario which is working as the signature of the packet and the attack packet can be identified from all normal packets. Normally this kind of packet is allowed inside the network but if this packet stays in network than it can create DDoS attack on the destination of the ICMP packet.

Here in this case of ICMP we can determine whether the packet is attack packet or normal packet from looking just by its payload. But not all the packets have the same signature. TCP packets can have big size of data like 1300 or 1400 bytes so for detecting TCP attack detection other signature like fragmentation and other things needs to be checked.

After getting the packet type of packet and the signature of the packet are determined. Here the database contains the attack packet signature so if the signature does not match than the packet is normal packet but if the signature does match than the packet is an attack packet and the administrator is informed about the attack. Here the IDS contains the database of IP address the attack packets, so if the IP address is in the database than it do nothing but inform the administrator but if the IP address is not in the database than it writes the IP address in the database and then notify the administrator.

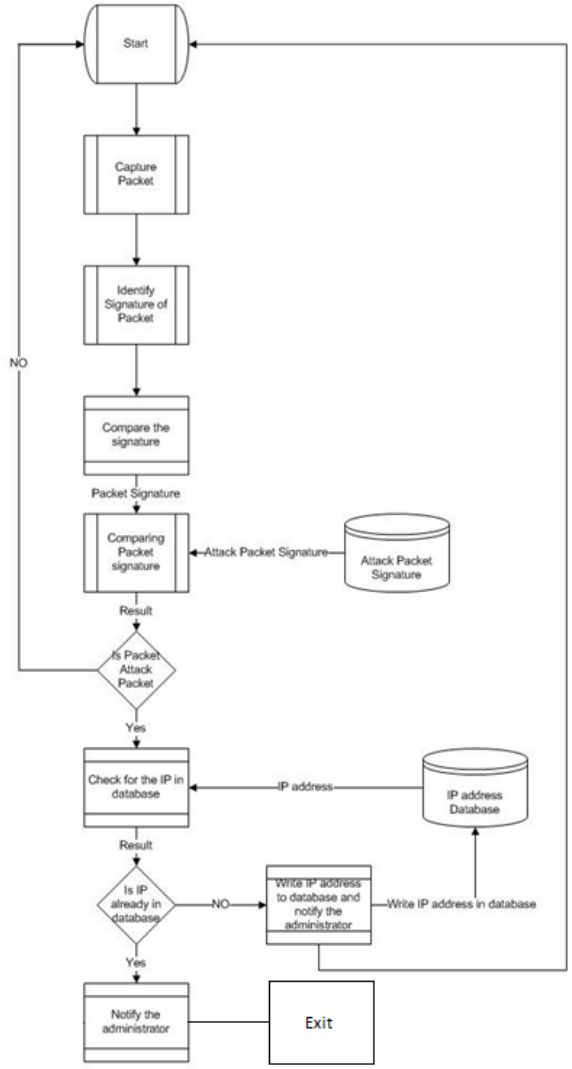


Figure 5: Simple IDS Flowchart

3.1 Performance Evaluation Metrics

1. Throughput - Throughput is the measure of how fast we can actually send packets through network. The number of packets delivered to the receiver provides the throughput of the network. The throughput is defined as the total amount of data a receiver actually receives from the sender divided by the time it takes for receiver to get the last packet.
Mathematically, it can be defined as:

Throughput= N/1000

Where N is the number of bits received successfully by all destinations

2. Packets Dropped - Some of the packets generated by the source will get dropped in the network due to high mobility of the nodes, congestion of the network etc.

3. Packet Delivery Ratio - The ratio of the data packets delivered to the destinations to those generated by the CBR sources. It is the fraction of packets sent by the application that are received by the receivers.
Mathematically, it can be defined as:

PDR= S1÷ S2

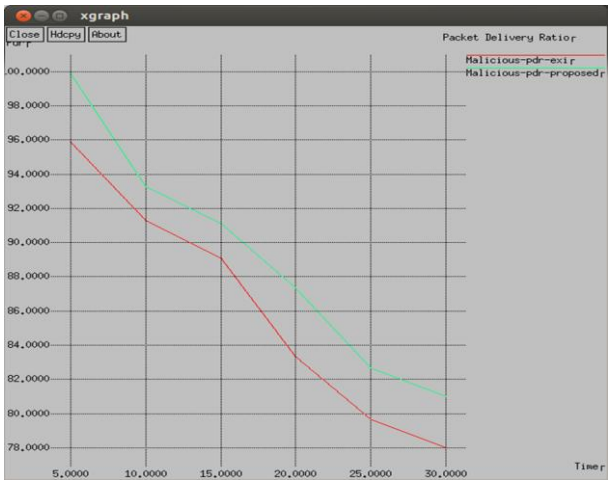
Where, S1 is the sum of data packets received by the each destination and S2 is the sum of data packets generated by the each source.

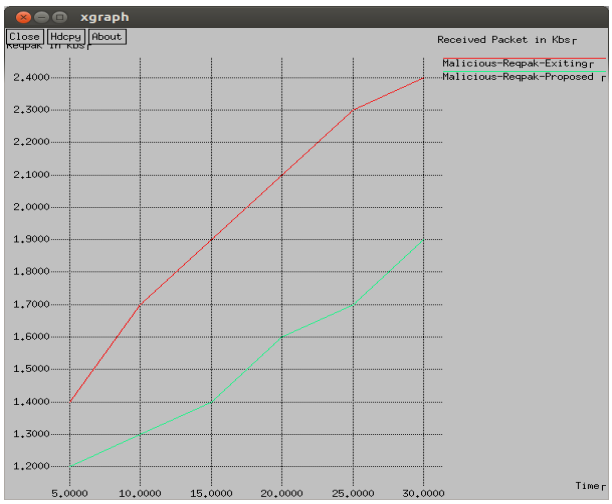
4. End-to-End Delay – End-to-End delay indicates how long it took for a packet to travel from the source to the application layer of the destination i.e. the total time taken by each packet to reach the destination. Average End-to-End delay of data packets includes all possible delays caused by buffering during route discovery, queuing delay at the interface, retransmission delays at the MAC, propagation and transfer times.
Mathematically, it can be defined as:

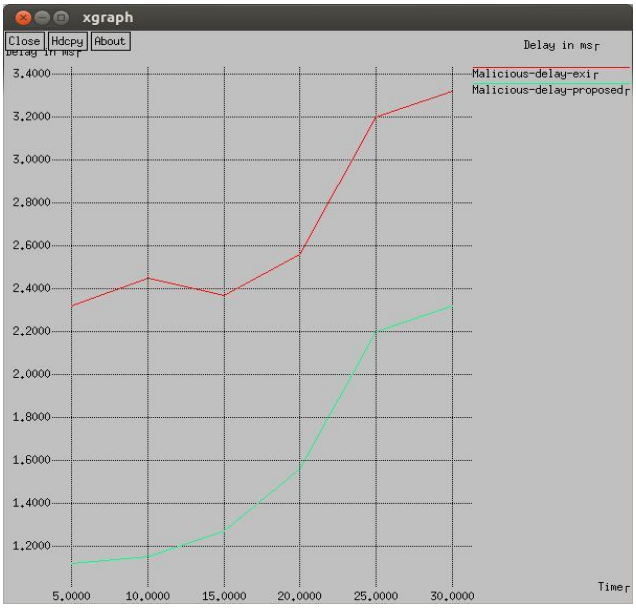
Avg. EED=S/N

Where S is the sum of the time spent to deliver packets for each destination, and N is the number of packets received by the all destination nodes.

4. Result Analysis







5. Conclusion

Intermediate results show that ICMP echo request packets can create a bandwidth starvation attack. This attack has very tremendous effect on the network that no other packets can reach to the destination because of all the ICMP echo request packets are in process. IDS can detect the attack packet of ICMP echo request but CPU process increases drastically and the network utilization at the incoming side of the system. As a result performance of the system decreases.

6. Future Work

As we seen that ICMP echo request create a bandwidth starvation attack. In future reduce CPU utilization in system so that performance of the system could increase and optimizing the performance of the IDS and I would focus to identify the packet in router and then detect those packets and stopping them by taking place any kind of attack.

7. Acknowledgments

With the cooperation of my guide, I am highly indebted to **Asst. Prof. Mukesh Sakle**, for his valuable guidance and supervision regarding my topic as well as for providing necessary information.

References

[1] C. L. Schube, I. V. Krsul, M. G. Kuhn, E. H. Spafford, A. Sundaram, and D. Zamboni, "Analysis of a denial of service attack on tcp," IEEE Computer Society Washington, no. 208, 1997.
[2] B. Xiao, W. Chen, Y. He and E. H.-M. Sha," An active detecting method against syn flooding attack," Academic Press, inc. Orlando, FL, USA, vol. 68, pp.56,470, Apr. 2008.
[3] C.-H. Lin, J.-C. Liu, H.-C. Huang and T.-C. Yang, "Using adaptive bandwidth allocation approach to defend ddos attack." in MUE, pp. 176-181, IEEE Computer Society, 2008.
[4] B. B. Gupta, R. C. Joshi and M. Misra, "Distributed denial of service prevention techniques," CoRR, vol. abs/1208.3557, 2012.
[5] A. Yaar, A. Perrig and D. Sond, "Siff: A stateless internet flow filter to mitigate ddos flooding attacks," in IEEE Symposium on Security and privacy, pp. 130-143, 2004.
[6] Saman Taghavi Zargar, James Joshi, David Tipper, A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks,IEEE,2013
[7] http://ryanmarle.blogspot.in/2012/09/the-importance-of-network-security-to.html
[8] http://en.wikipedia.org/wiki/denial-of-service_attack
[9] http://www.e-zest.net/blog/stop-ddos-attacks/
[10] http://en.wikipedia.org/wiki/smurf_attack
[11] Mark Merkow, Jim Breithaupt, Information Security: principles and practice, 2nd Edn, Pearson publication, 2007, pp 256-261