Smurf Attack prevention without blocking valid users

Thesis

Submitted By

16-32760-3	MD. Jamir Hossain
16-32693-3	Wahid Niazy
16-33001-3	Suantar Sarker
16-32678-3	Shawon Sarder

Department of Computer Science

Faculty of Science & IT

American International University Bangladesh

December, 2019

Declaration

We declare that this thesis is our original work and has not been submitted in any form for another degree or diploma at any university or other institute of tertiary education. Information derived from the published and unpublished work of others has been acknowledged in the text and a list of references is given.

MD. Jamir Hossain
16-32760-3
Faculty of Science & Technology

Wahid Niazy
16-32693-3
Faculty of Science & Technology

Suantar Sarker
16-33001-3
Faculty of Science & Technology

Shawon Sarder
16-32678-3
Faculty of Science & Technology

Approval

The thesis titled “Smurf Attack prevention without blocking valid users” has been submitted to the following respected members of the board of examiners of the department of computer science in partial fulfilment of the requirements for the degree of Bachelor of Science in Computer Science on 24th December 2019 and has been accepted as satisfactory.

MD. ASIFUL ISLAM
Lecturer & Supervisor
Department of Computer Science
American International University-Bangladesh

SHAHRIN CHOWDHURY
Assistant Professor & External
Department of Computer Science
American International University-Bangladesh

DR. M. M. Mahbubul Syeed
Associate Professor & Head
Department of Computer Science
American International University-Bangladesh

Professor Dr. Tafazzal Hossain
Dean
Faculty of Science & Information Technology
American International University-Bangladesh

Dr. Carmen Z. Lamagna
Vice Chancellor
American International University-Bangladesh

Acknowledgement

First, we would be thankful to almighty God for this help in successfully completing our thesis on time. And also we would like to express our heartfelt thanks to the faculty of Science & Technology for keeping this thesis credit in our curriculum in our graduation program.

A lots of thanks to our beloved supervisor **MD. Asiful Islam**, from the bottom of our heart for this kind of encouragement, direction, inspiration us to complete our thesis.

Finally, we would like to show our gratitude to our beloved parents, friends, and our beloved teacher who advice and motivate us all the time.

Abstract

Nowadays Smurf attack is a very well-known Distributed Denial of Service (DDoS) attack because of its easy execution process. It is also one kind of Amplification attack. Smurf attack can take down any big server very easily with their Amplification method. As this type of attack has done by spoofed IP address so it is difficult to catch the attacker. In many previous work they prevent Smurf attack by disabling IP broadcast address and also blocking ICMP packets for all users. So we are proposing an algorithm by which the Smurf attack will be prevented. This algorithm will be implemented in firewall which will not block Internet Control Message Protocol Message for valid users. The broadcasting service for the valid users will be available

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction

1.1 Denial-of –service (DOS):

The word Denial-of –service (DOS) means a form to attack on a computer system over a network. An attacker tries to disturb legitimate traffic of a server of internet network by performing denial-of -service attack. An attacker uses one device and one internet connection to execute a denial of service attack. When attacker attempt to perform attack from large number of computers under the network and internet connection to flood of a targeted server that attack is called Distributed Denial-Of-Service attack. The main difference between Dos and DDos is in DoS attack attacker attempt to perform the attack by using a single computer and an internet connection but in DDoS attack attacker attempt to perform the attack by using a large number of computer or host under the network and internet connection. In DDoS attack attacker use every computer or host as a bot. Attacker control the group of bot which is basically known as botnet.

The attacker's main goal to seek DDoS is to interrupt a targeted server's normal traffic. Attacker not try to damage a server or machine permanently by performing DDoS attack. Attacker tries to interrupt a server's normal traffic for some time by carrying out the attack. Attacker wants that the server will busy for certain time. DDoS attack is like a traffic jam on a road, where the regular traffic of that road want to reach in their aim destination without any interference. But when a large number of irregular traffic are added in their desired road for a certain time then there a jam will be occurred for that time, and the highway will be busy for some time. That is why the regular traffic for that highway will suffer. They will not arrive in their desired destination with in time. Like the regular traffic of the highway, when the DDoS attack happen on a server or a network the legitimate host or user under the network wound not make transmission within time. The legitimate user under the network wound not receive any service that time, because the server is busy to response a large number of traffic.

The attacker main target to perform DD0S attack is:

1. To consume more computational resources. When DDoS attack happen the bandwidth of the server consume more, it take more disk space. Because large number of traffic the server need more time to process.
2. To disrupt information of configuration. When DDoS attack happen it disrupt routing information of the server.
3. To disrupt physical component of network.

1.2 Existing Works

In [1] they try to stop Smurf attack by disabling IP broadcast address. In their paper they briefly discuss about packet dropping attack and flooding attack. As a flood attack they chose Smurf attack. They describe Smurf attack and how the Smurf attack is done by the attacker. To execute Smurf attack, an attacker target broadcast address of a network server. A broadcast can take place on the network layer and dita-link layer. To a specific physical network, data link transmissions are sent to all the host that are connected to that physical network. They described how amplification has been done to execute Smurf attack. Amplifie is typically calculate by original traffic size with number of broadcast the attacker used to execute Smurf attack and number of host under every broadcast. In their solution they try to disable broadcast IP address. If the broadcast IP address is disabled, then the attacker can not amplifie the traffic size. So that host computer under that broadcast address can not be a part of Smurf attack. They won't receive any kind of ICMP request from their broadcast address. So that the possibilaty of ICMP flood attack and Smurf attack will be decrease. In their research they also shown some different result by attempting Smurf attack. Their proposed solution is very easy to implement. But the user of every host under that network will suffer. Because of disabling broadcast the server can not broadcast any broadcast message. The host under the also can't sent any kind of Internet Message Control Protocol packets.

In [2] they proposed a solution where the system will detect the DDoS attack and prevent it from analysis of Per IP traffic. It is real time basis detection and prevention system. The algorithm need to implement on leaf router. In this system they are utilizing Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) to prevent and detect. The DDoS algorithm has two part Recognition and Decision. The recognition Algorithm is to find out attack. To detect Flooding attacks, a non parametric CUSUM algorithm are applied.It will check the IP behavior and try to match with negative IP behavior. In their solution they try to prevent Smurf attack by set a number of packet for per second. For a second of time a number of packets are set which is known a threshold. In their solution they also shown some result with changing the number of synchronize message. They attempt with 10 synchronize message, 80 synchronize message and with 1000 synchronize message per second. And it shows different result for every attempt. When the treshold value are exceeded the server will drop all new incoming packets. Their solution is used for both Domain Name System Protocol (DNS) attack and Smurf attack for detect the attack. But when a valid user send a packet to the server, when the server is under attack by the attacker the valid user packet will be drop or block by the server because the treshold value is exceeded.

In [3] their study propose another methodology dependent on the conduct of the Internet Control Message Protocol packets. Their methodology finds the wellspring of an immediate and an intelligent Internet Control Message Protocol attacks, utilizing few attack Internet Control Message packets. Like every research paper they also describe Smurf attack and how they work and what are the things related to the attack. They proposed a traceback way to deal with find the source IP address of Internet Control Message Protocol flooding attacks which is actually SMURF attack. Their methodology depends on the conduct of the Internet Control Message Protocol packets. They have actualized and recreated this methodology changing several parameters. Results show the capacity of this strategy to find the genuine source IP address of the attack utilizing few assault Internet Control Message Protocol packets. In packet logging approach the Internet Control Message Protocol packets that are passed through the routers that data are stored. They use bloom filter to store the information of routed parcel. When an attack is distinguished, the victim server sends traceback solicitations to its upstream switches to recreate the attackers way. The benefit of this methodology is the capacity to recreate the assault way with just one Internet Control Message Protocol attack packet. In packet marking the routers embed data in one Internet Control Message Protocol packets so as to find the source IP address of a stream. The victim server figure out the marking and remakes the assault way, which are the addresses of the switches between the attacker and victim server. In Internet Control Message Protocol trackback routers convey out-of-band traceback data to the goal of the stream to recreate the assault way. Internet Control Message Protocol packets contain data about the marking switch. The victim server gathers the Internet Control Message Protocol packets during the attack and concentrates traceback data. The unfortunate casualty will have the option to remake the assault way. They have built up a particular test system so as to assess the quantity of packets expected to traceback the attacker. They figure the quantity of assault packets dependent on the likelihood of checking. They utilized an Internet Control Message Protocol information field of just 16 bytes, all together not to meddle with different applications utilizing ICMP reverberation solicitation or answers. They utilized 15 marking switches since it is the normal way length in the Internet. In their framework, the router don't verify themselves before playing out the checking, so aggressors who know about the traceback framework, can send parodied markings to meddle with the recreation procedure. With the probabilistic checking, most mock markings will be overwritten by real routers.

In [4] they have briefly discussed about Smurf attack and Amplification attack. Their research shows how amplification factor affects the Smurf attack and the connection among the attackers original traffic, moderate unprotected system and the last intensified attack traffic. They have briefly described about Internet Control Message Protocol message format and how it is utilized and their roles in Smurf attack. They also shown design of how Smurf attack works and how the attacker utilized the middle network to make their work done. In their paper they said Smurf attack fundamentally abuses the Internet Control Message Protocol messages that are one of the most usually utilized diagnostics devices as often as possible used to investigate the issues in the system. They also describes how victim server is swamp with Internet Control Message Protocol echo reply message resulting in asset weariness making the server busy thus cannot give service to legal users. In attack Amplification section they found out how the attack ratio increases. The attacker targets as many broadcast domain which is middle network to amplify their traffic. They characterize another term called Attack Amplification factor which is the proportion of the measure of data transfer capacity produced by the in-between network and the measure of the transmission capacity utilized by the attacker to send Ping messages to the unprotected middle systems. There also shows many example how using slow speed network can take down large server. They have also proposed solution to prevent Smurf attack is by disabling IP broadcast address from the firewall and also reject all Internet Control Message Protocol echo messages. But still attackers can do the attack due to misconfiguration in firewall system.

In [5] they described about possible types of Distributed Denial of Service (DDoS). The prevention of Distributed Denial of Service (DDoS) can done some methods. They described about the software back grounds configuration with which the Distributed Denial of Service (DDoS) is done. The possible type of attack is described very elaborately. The different types of pattern of Distributed Denial of Service (DDoS) attack has been discussed. Some generalized solution has been proposed to prevent Distributed Denial of Service (DDoS) attack in a specific server. They discussed about architectures of Distributed Denial of Service (DDoS) attack. Handler based algorithm and IRC based algorithm has been introduced. All possible types and sub types of Distributed Denial of Service (DDoS) attack has been discussed. Smurf attack is under amplification attack which is under bandwidth depletion as Distributed Denial of Service (DDoS) is mainly two types bandwidth depletion and resource depletion. Different layer for executing Distributed Denial of Service (DDoS) attack has been introduced. Many software are introduced which help attacker to execute the Distributed Denial of Service (DDoS) attack. In Distributed Denial of Service (DDoS) attack many bots are used to execute the attack. More specifically they are the secondary victim in a Distributed Denial of Service (DDoS) attack. The secondary victim event do not they are attacked by an attacker. They have discussed about Egress Filtering which is used for the scanning a network. The introduce load balancing, throttling and describes honeypots which can mitigate Distributed Denial of

Service (DDoS) attack. The data during the Distributed Denial of Service (DDoS) attack is stored which can help the developer to prevent the Distributed Denial of Service (DDoS) letter.

In [6] they have discussed about four types of Distributed Denial of Service (DDoS) attack. They are Smurf attack, TCP SYN, UDP flood and ping of death attack which are common in Distributed Denial of Service (DDoS) attack. They proposed algorithms for prevention of all of these four as well as detecting the specific attacker. They mainly make three types of Distributed Denial of Service (DDoS) attack. According to them to make a successful Smurf attack an attacker have to complete five steps. In the Smurf attack the attacker use backdoor mechanism. To make a successful Smurf attack only Internet Control Message Protocol is used by the attacker which is a very common protocol in the network. In their proposed algorithm to detect a Smurf attack they checked the packet type and the IP address is spoofed or not they said it a Smurf attack and make a defense against the attack. The system also takes report of the attacks done to the server. To defense the attacks they checked the packet count in a second. If the threshold is exceeded then all the traffic coming in to the server will be dropped by the system or fire wall. The algorithms are implemented in the FIPS mainly. They measured their algorithm with positive rates and accuracy to detect the attacks on the server.

In [7] this paper They proposed a system to defend DDoS attack in IoT scenario. There is a less resource contain in IoT device that is a it is need to perform on less power. This system all the device will be connected on network through a default router. There is only one router to communicate between server and device. Default router is considering here as sole of connection between external network and internal network. Risk Mechanism algorithm will be implemented on default router. All incoming traffic IP is check first to here in router. It will work on low rate attack. The algorithm will check payload size if the payload size is more than normal size than packet will be dropped. For all incoming packet it will check payload. There is already some predefine scenario for normal packet. It will also check request type with normal scenario. In finding any kind of thread is external server in this mechanism. In which IP the risk will be found it will save the IP in risk factor to the server. For further request from traffic will not allow. For any incoming traffic it matches the IP from server. If IP in risk server the IP found it will not allow it to network. All kind of low rate attack detect wisely in this method. Due to checking rigorously packet size and normal packet scenario, there is very few chances to occur low rate DDoS attack in this method.

In [8] this paper they comprehensively analyze and categorize the different type of DDoS attack and their potential solution are explained. The target of DDoS is to make disruption of service. They categorized DDoS in Level of Computerization, Attack on Network, Oppressed Vulnerabilities, Influence, Attack Intensity Dynamics. Level of Computerization attack done directly on server or Personal Computer. Attack on network mainly done by using Transmission control protocol (TCP) and user datagram protocol (UDP). Oppressed Vulnerabilities are mainly flood attack. This attack could be done using user datagram protocol (UDP) flood, Transmission control protocol (TCP) flood, SYN flood and Internet Control Message Protocol (ICMP) flood. Influence is all kind of attack which done by IP spoofing. There is Smurf Attack, Fragile Attack, TCP SYN, PUSH + ACK, SLOWLORIS attack mainly done. Attack Intensity Dynamics are continuous packet sending attack and variable length packet sending. In continuous packet sending there are Ping Flood, HTTP flood attack. Variable length packet sending is there are Ping of death, where a variable length of packet are modifying. The counter mechanism is define on the basis of attack type. For Computerization type of attack it should be hide all port. The attack done directly through unused port. For controlling attack through TCP protocol and UDP protocol ,there should be check file size before entering traffic on network. To prevent IP spoofing there should backtracking process on incoming path and find out real attacker. To prevent ping flood attack there should a fixed maximum number of ping request at a time. To prevent ping of death there is need to check Internet Control Message Protocol (ICMP) request packet size. There are analyzing a round figure parameter of all DDoS.

Chapter 2 : Types of DDoS

There are three main categories to describe types of DDoS attack:

1. Volume Based: In volume based Distributed denial of service attack, attacker main target is to saturate the bandwidth of the site that are attacked. In volume based attack bit per second are used to measure the magnitude of the attack. UDP flood and ICMP flood are the example of volume based DDoS attack.

2. Protocol Based: In protocol based DDoS attack, attacker main target is to consume server resource. Attacker attempt to consume actual resource of the server. Attack magnitude is measured by number of packets by per second. SYN flood, ping of death and Smurf attack are the example of protocol based DDoS attack.

3. Application layer Based: In application layer based DDoS attack, attacker target to crash or freeze the target server. It is measured by number of request in per second. Windows and Zero-day DDoS are the example of application layer based DDoS attack.

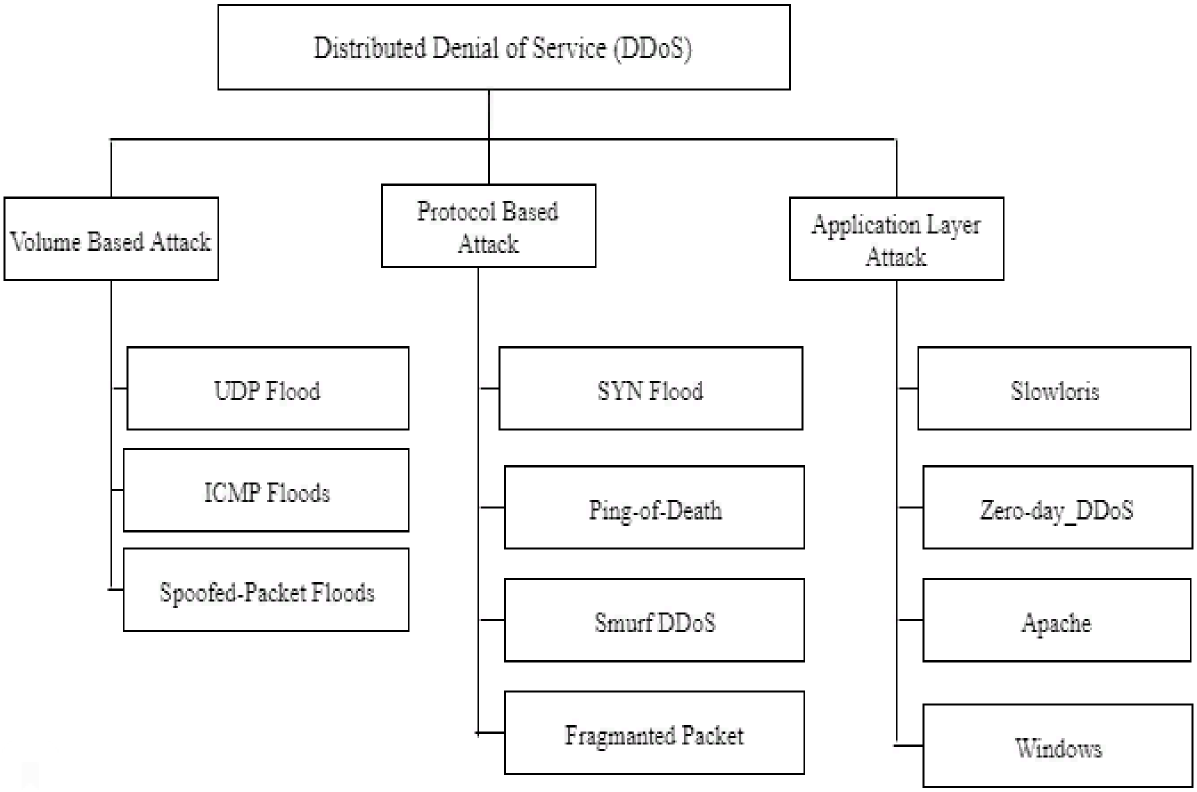

Figure 2.1: Types of DDoS

2.1 UDP flood attack:

User datagram protocol (UDP) is one of the protocol of internet protocol suite. UDP flood attack is one of the volume based type of distributed denial of service attack. To perform UDP flood attack, an attacker sent a large number of user datagram packet to a targeted server.

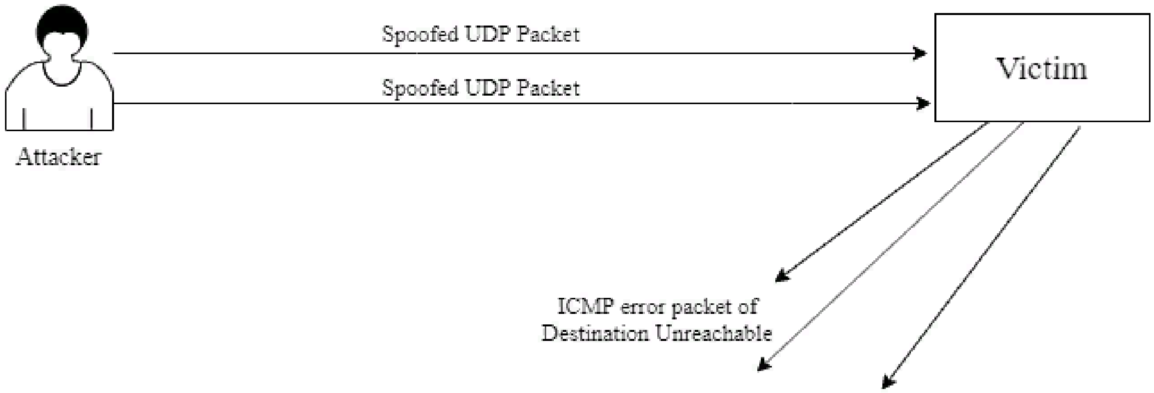

Figure 2.2: UDP Flood

In UDP flood attack a targeted server is flooded with User datagram protocol packets. It attempts to overwhelm ability process request and respond the request appropriately. Attacker target a random port on the host with it's IP address that are containing UDP packets. When the receiving host receive the UDP packets it check for the applications that are associated with the datagrams. There nothing will be found by the receiving host and it send back a destination unreachable packet to the sender. Attacker send more and more UDP packets and the victim received it and answered back. The system will be unresponsive to the other client under the network. In the UDP flood attack, IP address of the packet may also spoofed by the attacker. By spoofing the packets IP address attacker ensure that the return ICMP message won't reach in their host.
By limiting the ICMP response most of the operating system try to prevent UDP flood attack. But it impact on legitimate traffic.

2.2 SYN flood attack:

SYN flood is a protocol based Distributed denial of service attack. By performing this attack, attacker main target is to make a targeted server unreachable for the legitimate traffic under the network. Attacker try to make the server busy, that legitimate user of the network cannot get service from the server with in time.

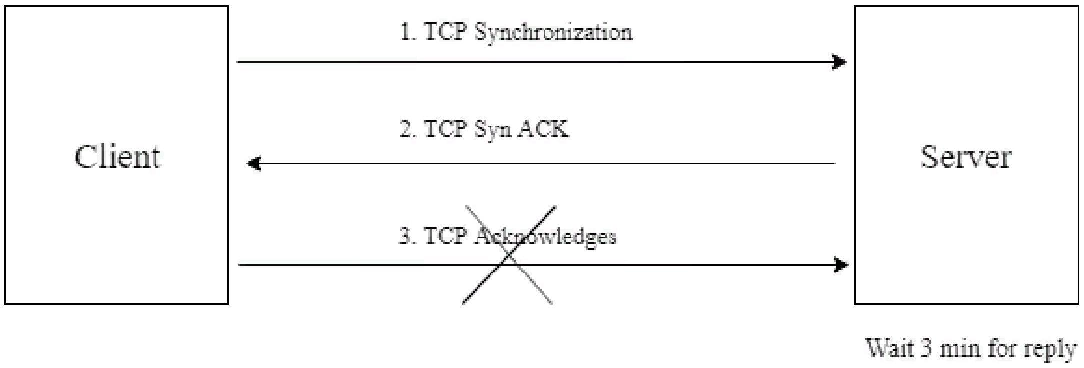

Figure 2.3: TCP SYN

To perform this attack, attacker use handshake proccess of TCP connesction. Attacker first send a connection request to the target server whethere the server is ready or not to receive any request with a high volume Synchronize packet with a spoofed IP address. When the server receive a request, the server respond to thait initial packet with a synchronize packet acknowledgment and open a port that the server is ready to reaceive response. When the server is waiting to receive final acknowledgment from the client, the attacker do not send back any acknowledgment. Attacker continues to send more synchronize message. By receiving more synchronize message the server open all port for the client that they sent back their final acknowledgment.The client won’t send back any reply ,and server will waiting to receive acknowledgment from the client. The server wait 3 minutes to receive acknowledgement from the client. All the port of the server are busy for the legit user under the network. All the Ports of the server are used by the attacker. The Syn flood attack is also called a half way connection. The attacker main target is to make busy all the available ports of the server.

Cloudflare is one of the solution to prevent Syn flood attack. The cloudflare are standing between Syn flood and the server. Handshake process in the cloud are handle by the cloudflare. It won’t make any connection between targeted server untill the TCP handshake proccess is not complete.

2.3 Smurf Attack:

Smurf attack is one of the most known Distributed denial of service attack in computer network. Smurf attack is a protocol based distributed denial of service attack. In smurf attack attacker attempt to make a server busy by sending a huge number of internet traffic to a targeted server. Actually attacker attempt with Internet Control Message (ICMP) to a targeted server. Internet Control Message are used in computer network operating system for sending error message. Smurf attack is done by ICMP reply and request message.

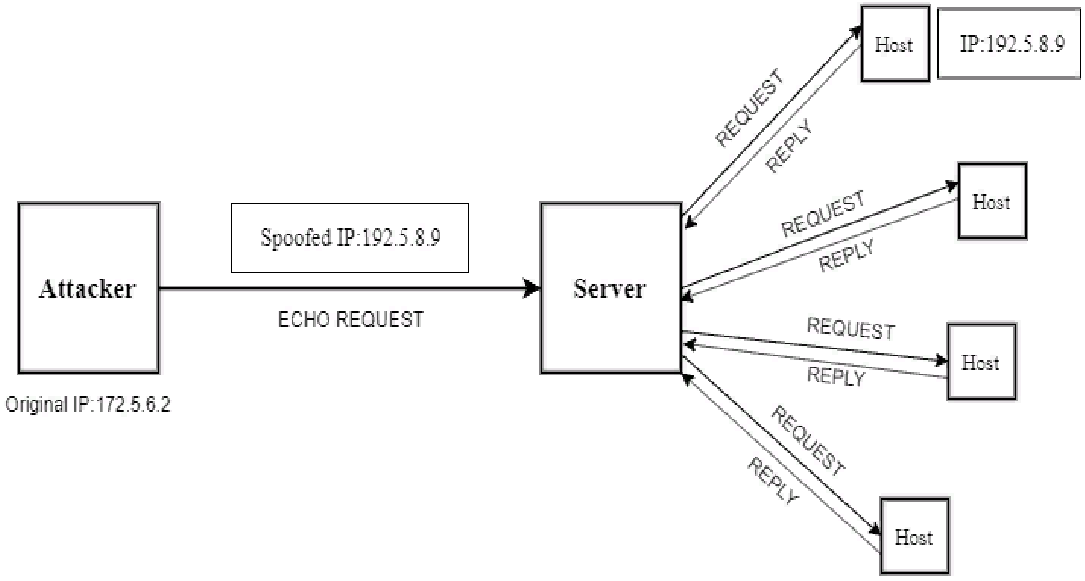

Figure 2.4: Smurf Attack

To perform smurf attack, attacker first identify the IP address of the targete server. Attacker sent a large number of ICMP packets broadcast of the targeted server. When attacker send a packet to the boardcast all the host under the broadcast receive the request packet that are sent by attacker with a spoofed IP address. Because of spoofing the IP address server can’t identify whether the IP of the request packet is valid or not. Attacker IP address is look like a valid IP address that are under the network. By using multiple broadcast attacker amplifies the attack traffic. When all the host under the broadcast receive the ICMP request packet, the host send back a ICMP reply for that message with same message that are received from the attacker. The targeted srever goes down when all the host under the network reply back ICMP packets. When attacker attack, attacker maximize the data field of ICMP message. ICMP message field is maximum, that’s why bandwidth of the server will be full. The server become busy for a certain time by receiving a lots of ICMP reply.

2.4 Ping of Death

Ping of death is very common type Distributed Denial of Service attack. It is mainly use to attack on personal computer or a IP device.

In this attack, victim got malware ping command from multiple network.

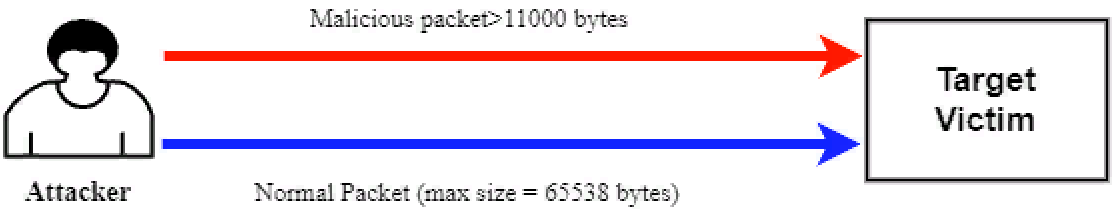
Malicious packet>11000 bytes
Target Victim
Attacker
Normal Packet (max size = 65538 bytes)

Figure 2.5: Ping of Death

Attacker send at a time many malicious ping command from many network to a computer.

For a ping command usually the packet contain 32 bytes. But the maximum size of the packet can contain 65,535 byte. If the packet contain more than 65,535 byte than the recipient IP couldn’t response and it will go on out of service.

The attacker main target was to create file more than maximum byte. There for attacker use a strategy. The original IP packet offset can contain 65,528 byte data. In offset more byte can not be added. There is a additional a fragment size for header file. Attacker add 20 byte of IP Header with original offset. So the total size of packet reached 65,548 which exceed the limit of original IP packet which recipient could attempt. Attacker send this saturated packet from multiple network. So the recipient device go on a death situation.

Ping of death attack occurs in data link layer usually. Cause fragment are allocated in data link layer. Attacker mainly targeted to modify fragment packet with more than maximum length. In IPv4 device attack through this more. But in later of 2013 there was found a vulnerability in IPv6 for ping of death. There can be remotely Distributed Denial of Service can be done in IPv6.

To check each Internet Control Message Protocol (ICMP) packet or Transmission Control Protocol (TCP) packet this attack cannot be prevented. Cause original offset is less than maximum byte. To prevent this there should be checked size of each fragment. Which include total packet size including IP header. Through this way this attack can be blocked. Many firewall by default check whole fragment size before receiving packet. But many of them often fail to check whole size of packet, they only check the IP packet offset size. This type of situation attacker can easily crackdown an IP.

2.5 SLOWLORIS

In Distributed Deniel of Service attack slowloris is highly targeted attack. This attack mainly used for attack on a specific server. Attacker used HTTP request for this attack. It is a tool based attack. This tool used to create connection between targeted server and attacker for http request. It is don't affect on anothe ports or services. Only aim is to disable http request from server through this attack.

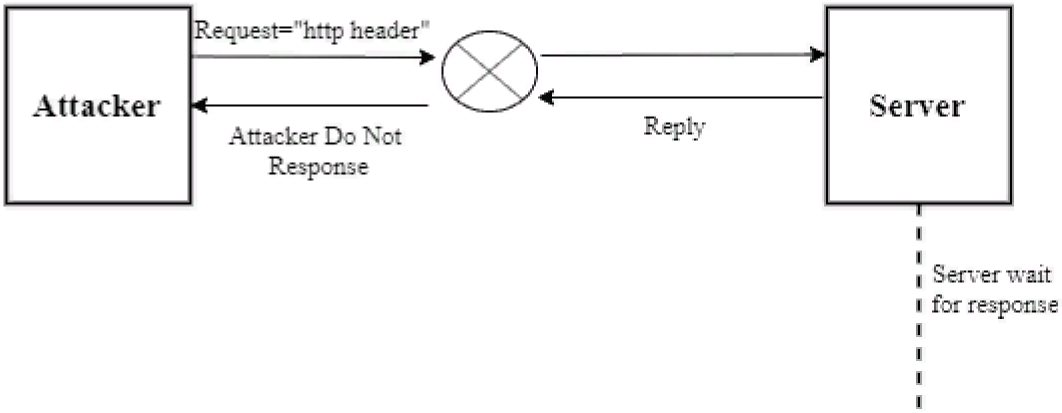

Figure 2.6: SLOWLORIS

Attacker create an thread and split that thread to multiple network across attacker server. This scenario only occur using partial http request. Attacker do not create a full http request. To busy server with partial http request. victim server got this type http request from multiple network simultaneously.

It is application layer attack which is not like other categorical attack. It is done on specific tool. It is "Low and slow" type attack. This attack traffic is very much lower than other request so server could response for this attack fast. Attacker main strategy is using very light weight bandwidth for this attack.

Its continuously send HTTP request to a specific server but could not complete the request. It is not respond on when server reply. Server keep waiting for response but it could not response. When request time over and server get ready for legal response then another request of attacker go on server. Which already ready on other network. Cause attacker split one attack to multiple network. Attacker continuously making incomplete request for server so that server could not attempt other http request. No legal user can connect on server for http request during this attack. For using low bandwidth request n simultaneously request server can only response attacker request. It can not identify valid request.

To prevent this attack there should be increase host number of whose can connected at a time. At a time how much host can connect this number can make reduce this attack. There are others solution for blocking the path which continuously send only HTTP header. Most highly usable server are use many protocol to protect from this attack.

2.6 MEMCACHED Attack

In order to Distributed Denial of Service attack MEMCACHAED attack is one of the less cracking attack. The main target to busy victim with mostly traffic. Attacker load the normal traffic with malicious traffic. So the traffic on internet of the victim get overload. Victim could not make establish a connection for overloading traffic. So victim get out services of regular internet.

For attacking MEMCACHED attack attacker need to spoof victim ip firstly. Through spoofing IP attacker request on vulnerable MEMCACHED server. The attacker request on UDP protocol. For MEMCACHED attack UDP protocol is vulnerable. In this protocol targeted IP could not check the data size of UDP response. So attacker create UDP request on server.

Attacker generate a request from spoofing IP but the respond is much more larger than original request. Attacker use MEMCACHED amplification for making the respond huge. Vulnerable server could not detect this amplification, so its respond on the request. But the respond is go on to valid user IP. So the valid IP could not load this type of huge response. Whole internet infrastructure get overload on MEMCACHED server response. It could not make able to response any type of request for this large data.

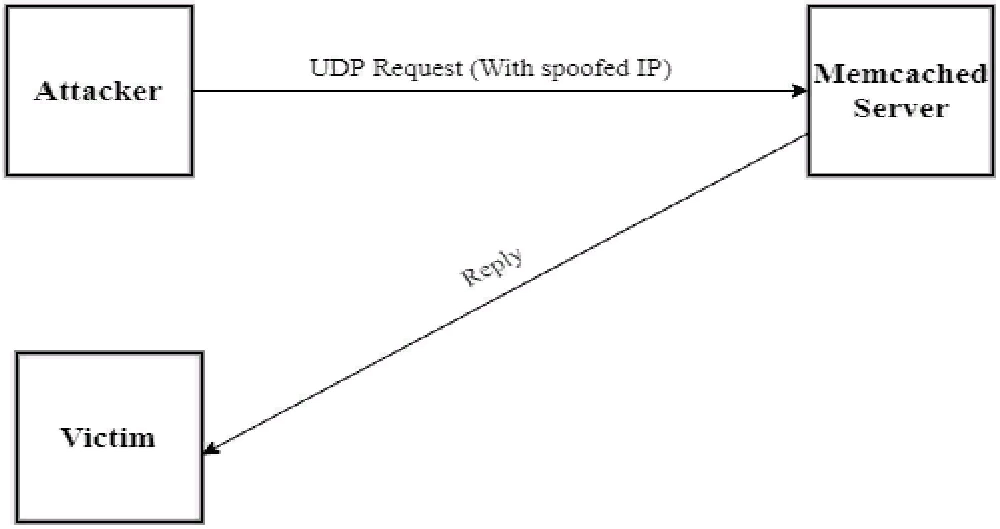

Figure 2.7: MEMCACHED Attack

Respond packet size is such huge that is make this one most dangerous attack. The MEMCACHED amplification size can be 51,200 time larger of actually packet. So if the normal request size is 2 byte the respond could be in 102400 byte which is 100KB. This massive amplification make this attack more powerful. This is one type of reflection based attack.

To prevent this type of attack it will be better to stop UDP request on MEMCACHED server. If MEMCACHED server does not response on UDP request there is very few chance to occur this attack. There can be also prevent it through firewalling on MEMCACHED server. So it couldn’t saturated any request. IPv4 has face this problem, in IPv6 there is packet filtering method for UDP protocol so this attack couldn’t occur in IPv6 using device.

2.7 HTTP Flood

HTTP flood is one of the well-known Distributed Denial of Service attack. This attack occurs on server. Attacker target a server to make busy so legal user cannot be go on server. HTTP request done for visiting web page. Attacker try to create maximum number of possible bot net he can create. From multiple bot host, attacker make http request on server. Server got multiple maximum resources request at a time. So the server busy with response those bot user. Therefor the server could not establish connection for valid user. Server get overloaded from those request. Server get out of service for valid user.

Attacker use low bandwidth for generating the request. And try to collect maximum resources of server. So low bandwidth request web server response fast of attacker request and maximum resources request make server more busy. From multiple bot host request to network of server, server lost the capabilities of handling new request.

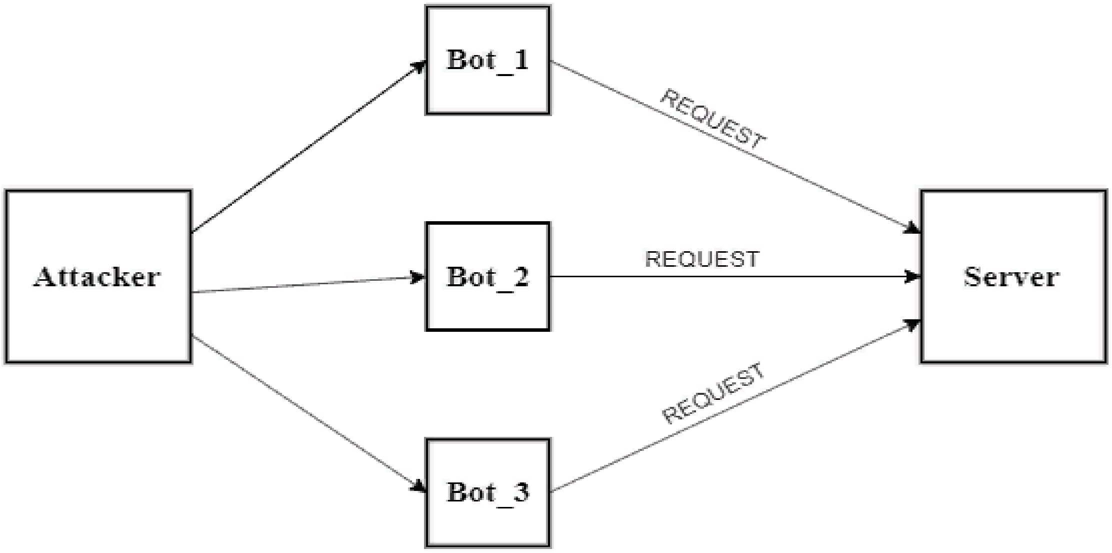

Figure 2.8: HTTP Flood

HTTP flood attack occurs in application layer. There are two types of request generate for this attack those are GET request and POST request. For database based server that mean in which server database using more to save something or retrieve something there are used HTTP POST request. To attack those type of server POST request use. To attack on others server HTTP GET request are using.

Application layer attack is more complex. There are the main techniques to prevent thus type of attack is identifying bot host. If server could identify bot host before taking request it is quite impossible to attack without bot host. But it is very much tough to identify bot for server. Various Captcha was created to identify bot but its sometime kill important time of valid user.

Chapter 3: Background Study

3.1 Parameters used by attacker in Smurf Attack

3.1.1 ICMP

The word ICMP means Internet Control Message Protocol. Internet Control Message Protocol (ICMP) is one of the basic protocol of internet protocol. Basically it is used for sending error message in network operating system if there any error is occurred. Error message are generated and send to the source by IP network device when any error occurd. Any Computer on the IP network can send ICMP message, receive ICMP message and also process it. Basically ICMP is not used to send data between system. It is only use for error message. For example, Suppose a host under the network send a request for service, if the service is not available then a error message is sent to the source that the requested service is not available.

3.1.2 ICMP ECHO

The ICMP echo message is generated by the IP network device, and it sent to source if any error is occurred. The ICMP Echo is an ICMP message.Actually ICMP echo request data is expected that it will be received a same data that are received by the receiver in request message. The ICMP ehco is also known as Ping.

3.1.3 Broadcast

Broadcast of a network maens an IP address of a subnet. Every subnet under a network has a broadcast address or IP. When a large number of host of an IP network are divided into a group of IP address that are called subnet of that IP network. All the host under that subnet are connected with their broadcast address. It is used for sending broadcast messages.When a server want to send a message or packet for every host of that subnet, it is easy to send the message or packet in broadcast instead of sending the message for every single host at a time. It save process time. For example, a university has a network system, and it has four department CSE, EEE,BBA and Architect. Every department has multiple host. Every department is divided into a subent. In subnet of CSE department has 150 valid IP address or host. The server want's to send a message for every host under CSE department. If the server send the messge to the host individually it take much time. The server will be busy for a several period of time. If the server send the message to CSE department subnet broadcast, then all the host under CSE department receive that message. It will be very easy for the server, and the server will not be busy for long time.It take less time to process. When an attacker attempt to perform a smurf attack, attacker send a request message to the broadcast of targeted server.

3.1.4 ICMP message format

Internet Control Message Protocol (ICMP) message are used to sent error message. To send message It follow a format which is called ICMP message format. Every ICMP packets have a header which is 64 bit and a varible size data segment.

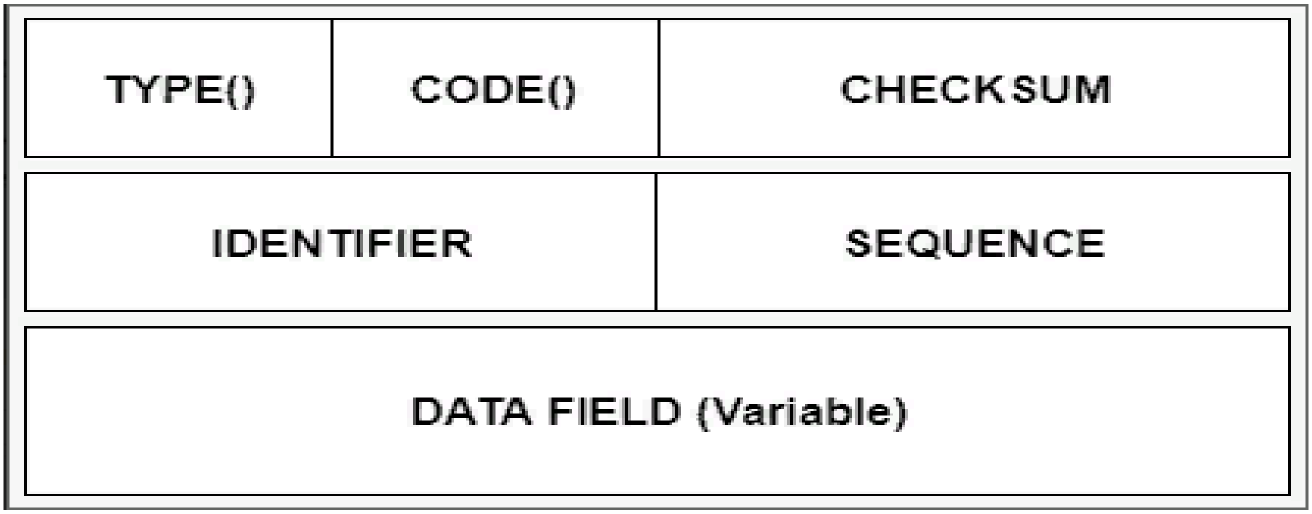

Figure 3.1: ICMP Message Format

The avobe figure is show the format that a ICMP message follows. The first 32 bit is type, code and checksum which is fixed. The last 32 bit is identifier, sequence and data field which variable and depend on the type or code of a ICMP packets.

3.1.5 TYPE VALUE

The type section of a ICMP message format determines the type of a field message form. The type of a message that is created by ICMP is split in two categories. One is for error message reporting and another one is for ICMP query message.
Error Reporting Messages are used when any kind of error is occurred. Destination unreachable error, network error, Time exceed, source quench is the example of error reporting message in ICMP.

In ICMP query message the ICMP make communication about status of a host. Echo request and reply, Time stamp request and reply are the example of ICMP query message. In Smurf attack an attacker used to send a ICMP query message. Actually from ICMP query message an attacker use ICMP echo request and Echo reply to execute Smurf attack. The type code of an Echo reply is 0, and type code 8 is used for echo request.

3.1.6 Code

The Code section of a ICMP message format determines the sub-type of error of an error message. If there any error has occurred, then the code section of ICMP indicates what kind of error occurred. For example, if requested time is exceeded then code section will indicate that time exceeded error is occurred. Which code is 11.

3.1.7 Checksum

The section Checksum of a ICMP message format is used to detect errors. It is calculated by header of a ICMP packet and data.

3.1.8 Identifier

Identifier is an optional section of ICMP message format. The optional value is set by the user of source host. By adding this optional value the user of source host try to match echo request and replies.

3.1.9 Sequence

Sequence is also an optional value set by user of source host to meet echo request and received.

3.1.10 Data field

Data field section of a ICMP message format contain all the information about the ICMP data packet. The data field size is 32 byte for a normal ICMP data packet. 64 kilobyte is the maximum size of a it. Data field section of a ICMP message format is the only variable that can be changed. When an attacker tries to execute a Smurf attack, the attacker maximize the size of the data field. Attacker send an ICMP echo request message maximizing the data field size to the broadcast. Reply from the host under the network will be same data field size. The server take more time to proccess the message instead of normal size. The server will be busy for a certain time to proccess all those reply message. The attacker try to saturate server bandwidth by maximizing data field size.

3.1.11 IP Address Spoofing

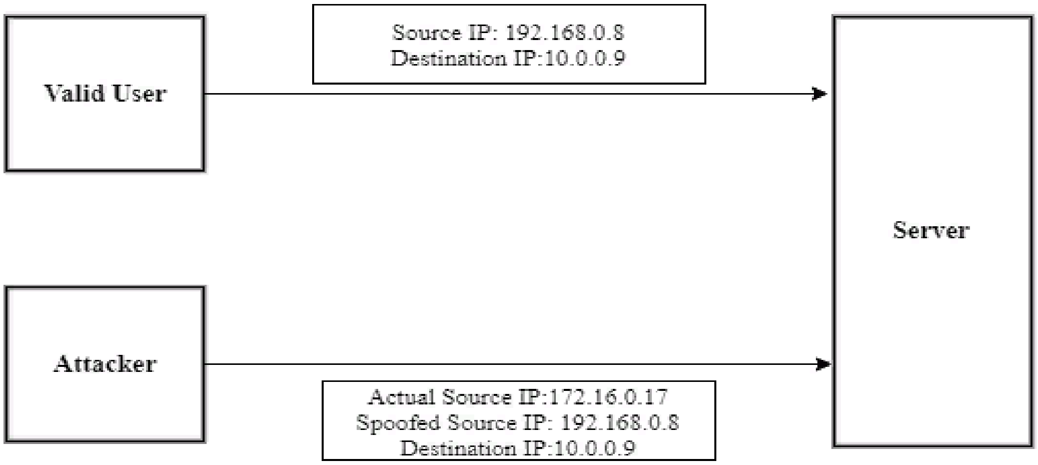

Figure 3.2: IP Spoofing

The word spoofing is used to mention to header falsification, the addition of bogus or misdirecting data in email. Fake headers are to deceive the receivers or system applications and also the message content. IP Spoofing is the formation of Internet Protocol (IP) packets which have an altered source address so as to obscure the identification of the host. It is a strategy frequently utilized by attackers to summon distributed denial-of-service (DDoS) attack against a victim server. IP address Spoofing including the utilization of a valid users IP address can be utilized by hackers to conquer organize safety efforts, for example, verification dependent on IP addresses. This kind of attack is best where trust connections exist between appliances. For instance, it is basic on some corporate systems to have inside system trust one another, so clients can sign in without a username or secret phrase gave they are interfacing from another machine on the inward system. By spoofing an association from a confided in machine, an attacker on a similar system might have the option to get to the objective machine without confirmation. There are some ways to prevent IP Spoofing, one way is packet filtering which restrict all the packets that advance to the outer side of the network. Still there is chance of spoofing because of faulty implementation of devices.

3.2 How Smurf Attack works

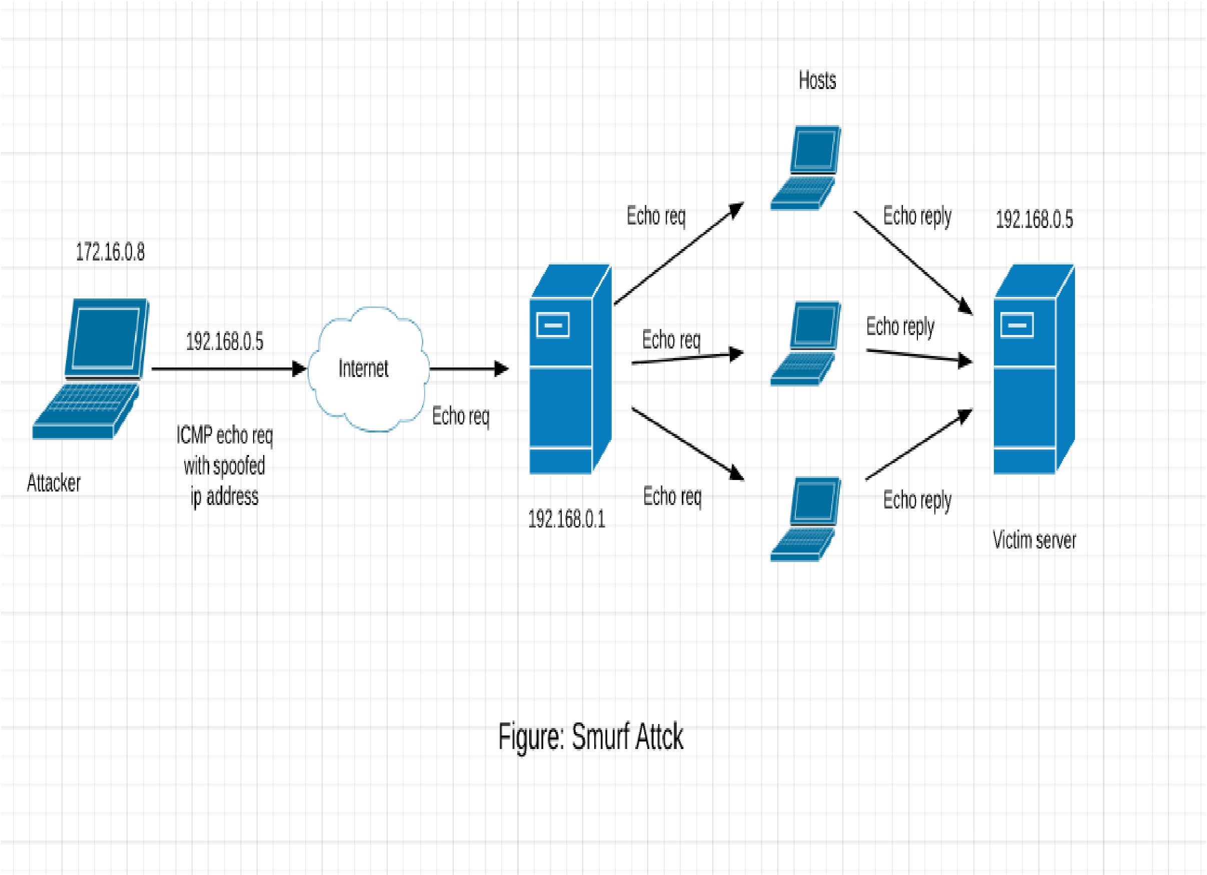

Figure 3.3: Smurf Attack

Smurf attack is one kind of distributed denial-of-service (DDoS) attack which happens in network level. In Smurf attack huge quantity of ICMP echo request and reply messages with manipulating the data field are send to the victim computer. Attackers fill the data field to its maximum length because data field is the only variable that can be changed in the ICMP packet. The attacker utilize enormous ICMP packet to immerse the bandwidth of victim server. ICMP echo request and reply messages are actually ping messages which are send to the broadcast domain with spoofed IP address by the attacker. Every broadcast domain have n number of hosts under them depending on their class. In figure 3.3 the attacker with IP address 172.16.0.8 sends an ICMP echo request with spoofed IP address 192.168.0.5 which is a victim server to the broadcast domain. The broadcast domain which is intermediate unprotected network will think that the ICMP echo request came from the IP address 192.168.0.5 which is actually victim server. The ICMP echo request are than forwarded to the hosts that are under the broadcast domain. The hosts than send ICMP echo reply to the victim server. The victim server will get one multiply number of hosts each broadcast domain ICMP echo reply for every ICMP echo request. The broadcast domain boost the distributed denial-of-service (DDoS) traffic going to the victim server. The attacker targets more than one broadcast domain to boost the traffic and make the victim server overflow with ICMP echo reply resulting in bandwidth consumption of the victim server. This is how the victim server will go down and cannot give service to legal users.

3.3 Attack Amplification

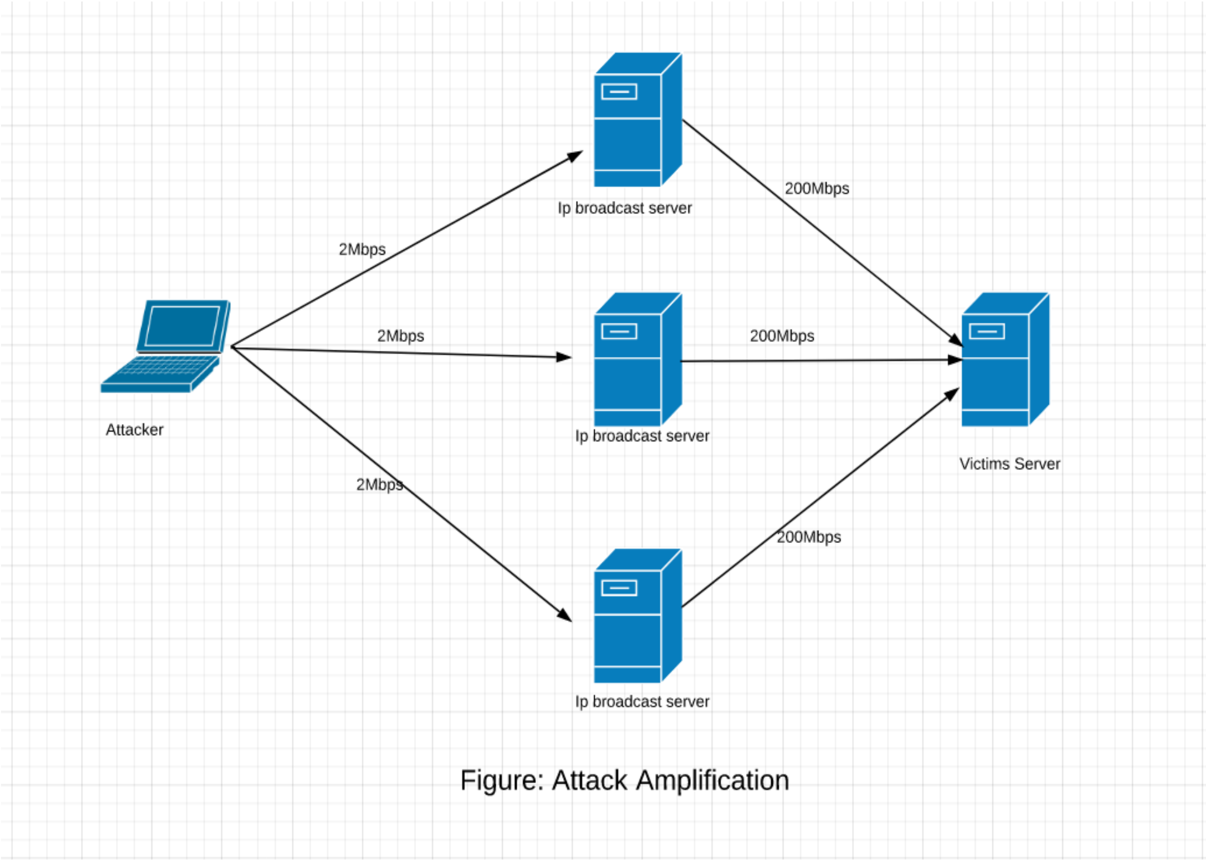

Figure 3.4: Attack Amplification

The figure 3.4 describes how attacker amplifies the original traffic. The broadcast domain is known as the attack amplifier as it is utilized to enhance the heap of the Smurf attack traffic contingent upon how large the broadcast domain is. The quantity of hosts in a broadcast domain relies upon the kind of the IP network. For instance the class-B IP network broadcast domain contain 65535 hosts and class-C IP network broadcast domain contain 255 hosts. On the off chance that such broadcast domain in a class-B network is unprotected or not all around designed to secure against Smurf attack then for each ICMP echo request with spoofed IP address, 65535 ICMP reply will be sent to the victim server by the broadcast domain. In figure above the attacker original traffic is 2 Megabyte per second and giving three ICMP echo request to broadcast domain of n number of hosts amplifies the traffic to 600 Megabyte per second. The amplified traffic is equal to original traffic multiply number of broadcast domain multiply hosts per broadcast domain. This is how the original traffic is amplified and the victim server become busy handling huge amount of attack traffic thus cannot give service to valid users. This is how the attacker successfully achieves Smurf attack. For example if attacker internet speed is 1 Megabyte per second and ICMP echo request to 5 class-C IP network broadcast domain than the amplified traffic is equal to 5 × 255× 1Mbps = 1.275 Gigabyte per second, this huge amplified traffic can easily masticate any victim server.

As appeared in Table-1, it takes 2 Class-C IP network broadcast domain for the attacker on a moderate dial up modem of only 64 Kilobyte per second internet speed to bite up the transmission capacity of a fragmentary T3 line. On the off chance that an attacker has an internet speed of 1 Megabyte per second, simply using 3 broadcast domain of a Class-C IP network, it can bite up bandwidth of OC-24, which is more than 5th times the bandwidth of OC-3. Also using modem of 128 Kilobyte per second and targeting 1 broadcast domain of a Class-B IP network, it can bite up data transfer capacity of an OC-192 line. Moreover, as appeared in the Table 3.1, an attacker on using broadband internet of 2 Megabyte per second can misuse an unprotected 2 Class-B IP network broadcast domain to bite up the data transmission of a victim server of OC-3840 line. The attacker would now be able to create significantly higher transmission capacity to overpower any amazing server with fast connections on the Web today.

Different kinds of IP network	Original Traffic	Number of unprotected intermediate broadcast domain used in this attack	Amplified Traffic	Different kinds of network link consumed by the attacker
Class-C	Modem =64 Kbps	2	2× 255 × 64Kbps = 32.64Mbps	T3
Class-C	Broadband = 1Mbps	3	3× 255 × 1Mbps = 765Mbps	OC-24
Class-B	Modem =128 Kbps	1	1× 65535 × 128Kbps = 8389Mbps	OC-192
Class-B	Broadband = 2Mbps	2	2× 65535 × 2Mbps =262Gbps	OC-3840

Table 3.1: Attack Amplification for various kinds IP networks.

3.4 Firewall

3.4.1 What is firewall

To prevent unauthorized action the concept of firewall are made. Firewall was a software or hardware based platform which difine by set of rules to check incoming and outgoing

traffic on internet. Firewall maintain the safety of internet. To connect on internet it is ensure the authorized access and block the unauthorised access. Firewall work like defense, it is protect data from unauthorized access. Firewall made upon different rules. It is work based on those rules. It do three things with every incoming and outcoming traffic. It is accept traffic, reject traffic and block traffic. Every action perform on the basis of define rules. If the traffic from which user is legal in the view of firewall rules it will accept the traffic. If the traffic is request unlegal activity it will block the traffic or simply reject the traffic on the basis of rules. So in short firewall work as barricade between user and internet which allow only valid
request.

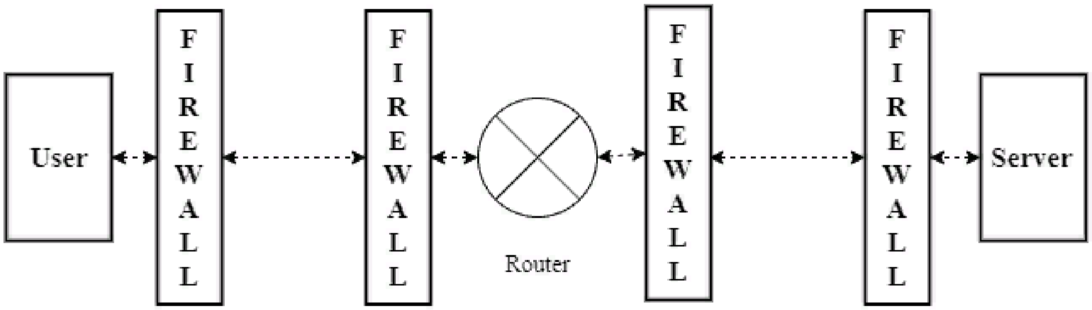

Figure 3.5: Firewall Setup on Network

If the traffic is request illegal activity it will block the traffic or simply reject the traffic on the basis of rules. So in short firewall work as barricade between user and internet which allow only valid request.

3.4.2 Firewall Rules

Firewall is nothing without rules. Each firewall has a set of rules. Firewall decide every action on the basis of rules. So which traffic will enter the network or which traffic will block from network this kind of decision are define in firewall rules. Every firewall has a set of rules, some of are define in default. The default rules can not be changed. To add some rules these should be merged with predefine rules. For secure more there can be add new rules on firewall. But some of firewall don't allow to add new rules. There also can be designed new firewall setup as per our privacy of network. The rules will work for both inbound and outbound traffic. Inbound rules set for which traffic will allow to our network and outbound rules set for which traffic will go from our network. To add new device on our network firewall rules have to add for the perticular device or port. To deny some type of request or IP there need to add new rules. Those rules should be add in Access List. From access list firewall check which traffic have permission and which traffic have to deny. There are two type of Access list, First one Standard Access List which work 0-99 number. Second one Extended Access List which work 100-199 number. To block some specific traffic new rules can make through access list.

3.4.3 Firewall Type

Firewall is the security of private network from other network. To secure data from unauthorised action there was various type firewall has been implemented. Most secure firewall is Basion Host device. It is mainly a computer which is highly configured and mostly secured. It is near to impossible to break Basion host security level. To ensure safety of data, Basion host use as firewall for outside network to private network.
In the based of connection to Basion host and router there are three types of firewall.

1) Screened host firewall
2) Dual Home firewall
3) Screened Subnet firewall

3.4.3.1 Screened host

In screened host subnet all traffic from the outside network for public server come first to basion host. Basion host allows for public server. But all connection are in bus topology. So attacker easily attack on private server cause its already across the basion host. It allows all traffic for public server request. So attacker easily got chance to enter private network. Cause every connection are in bus topology. It is most vulnerable design which made for Basion host. It is not used in real life for security issue.

3.4.3.2 Dual Home Firewall

Dual home firewall is mostly secure firewall setup. In Basion host there are two port for dual home technique. One port establishing connection for public server another is connected to private server. Authenticate user directly go on private server from separated port. From outside network request for Public server go on public server network from other port. They can't enter in private server network. To enter private network attackers need to break Basion host. They it very much tough for attacker. So that private server is safe through extra port. But Basion host is very much costly device. For configure another port on Basion host is very much costly. So it is use very few in real life.

3.4.3.3 Screened Subnet

It is the only Basion host firewall type Which use in industrial level highly. In meaning of security and cost it is a best of firewall type. In this method the in coming request for public server first pass from Basion to public server. But when a user pass through Basion host every log details of the user are monitoring. The private network is secured by Extra Router. To access on private network attacker need to breach Router security. In that time Basion host easily block the attacker. If Basion find any wrong activity on public server it block and reject the user. The area of secured by Basion host is de militarized zone. The use of extra router is very much less cost for connect through extra port. So it is rapidly use on market.

Chapter 4: Proposed Solution

4.1 Proposed Algorithm

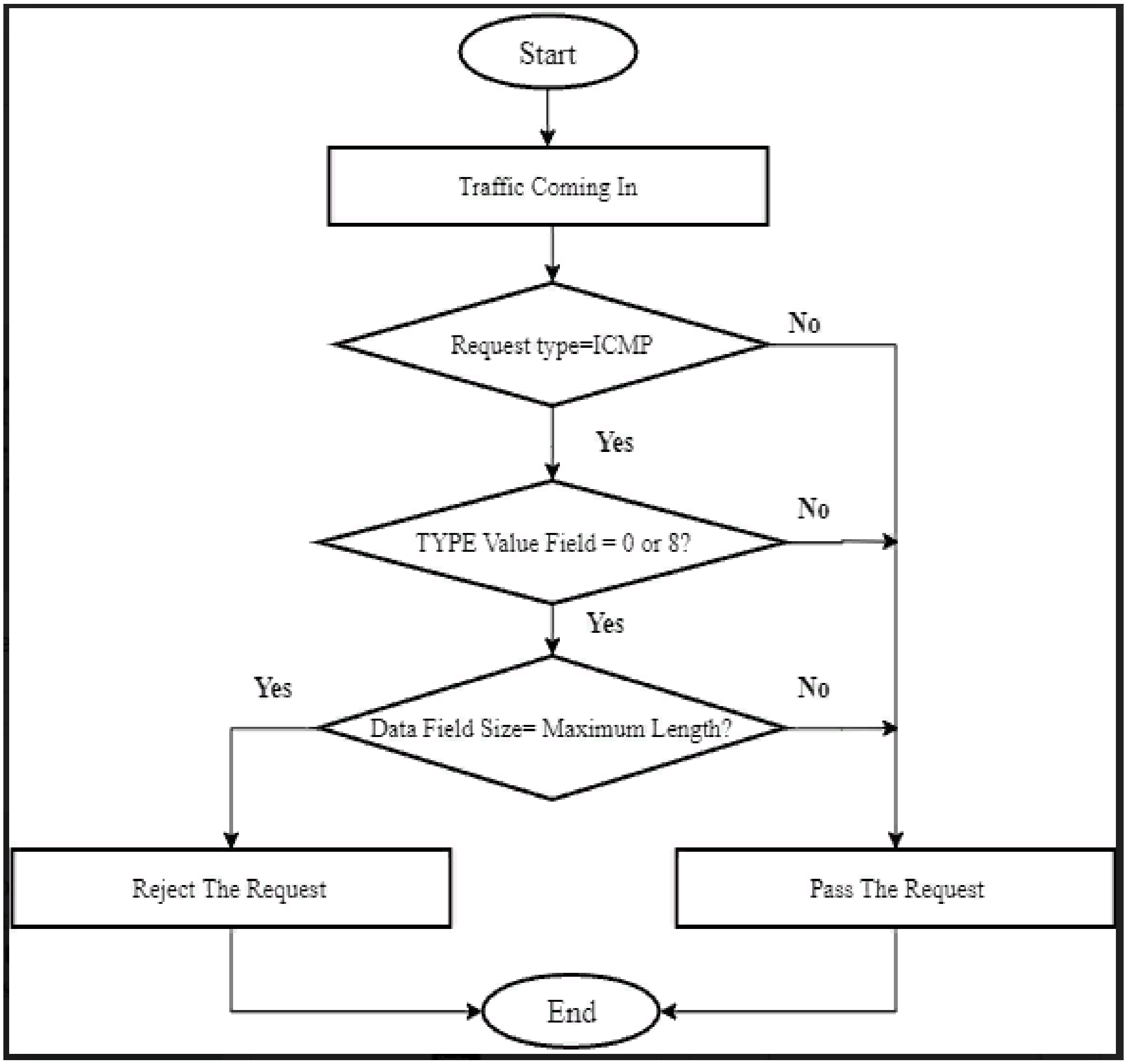

Figure 4.1: Proposed algorithm to prevent Smurf Attack

In our proposed algorithm, we want to prevent Smurf attack without violating service to the valid users. Smurf Attack done by the attacker to slow down one’s server with intention to hampering the victim. The purpose of this algorithm is to prevent Smurf attack with checking three parameter of Internet Control Message Protocol (ICMP). The Smurf attack only be executed by the ICMP packet which is a very common protocol in our communication system.

So the Fist checking of incoming traffic is its type. Type means what type of packet is coming to the server. It is known that Smurf attack is only done with ICMP packet. So the first parameter of checking is that the packet is ICMP or not. If the incoming packet is ICMP then it going to checked further. But if the packet is not ICMP type then it going to pass to the server without checking further.

The second parameter there going to checked is the type value of the ICMP packet. The type value varies on traffic type. Smurf attack can be done only by ECHO REQUEST MESSAGE and ECHO REPLY MESSAGE. For this type the value of TYPE in a ICMP packet is fixed. For ECHO REQUEST MESSAGE the value of TYPE field is “8” and for ECHO REPLY MESSAGE the value of TYPE field is “0”. So if the TYPE field value is not “0” or “8” then it going to pass the packet to the server. But if the packet’s TYPE field value matches with “0” or “8” that means it can go to attack the server. So the packet going to be checked further.

The third parameter is size of the Data Field of the ICMP packet which has come through two checking before. The Data Field is the only variable which can be changed the attacker. With natural Data Field the size of the Internet Control Message Protocol packet is “32 bytes”. The property of the Internet Control Message Protocol can be bit more. But the Smurf attacker maximize the size of the Data Field. By maximizing the Data Field, the size of the ICMP packet can be raise to “64 kilo byte”. The size difference is huge. This larger size helps the attacker to saturate the bandwidth of a server or victim. So the attacker attacks with the ICMP packets with maximum Data Field. So in third and last checking the Data Field of the ICMP packet coming to the server is going to be checked. If the data filed size is maximum, then the packet going to reject. But if the Data Field property is not highest then the packet is permitted to go to the following server.

In a Smurf attack the attacker used spoofed IP address. The spoofed IP address makes the attacker untraceable. It is not a reliable connection to the valid user if a server blocks his or her IP address. The valid users may want to broadcast any message. But if the server stops broadcasting service for the valid users so the connection is not enough reliable for the valid users. In our proposed solution all the traffic coming to the server is accepted first. But it is rejected by the firewall checking its three parameter. This three parameter can easily define a traffic moto against doing Smurf attack. The solution is to prevent the Smurf attack without violating the service to the valid users of the server.

4.2 Where to implement

For securing a network from unauthorized access or unethical traffic the firewall has been implement. Firewall ensure the security of network from unauthorized action on network. Every router and computer have firewall, from firewall the action has been taken for each incoming and outgoing traffic.

Our proposal was for prevent Smurf Attack. We made the solution by checking traffic request in 3 steps. 1st step is check whether its ICMP request or not. 2nd step is to check what is type value whether its 0 or 8 and 3rd step and the main step is check data field size whether it is in normal size or more than normal.

For implementing this we need to add new rules in firewall. To build our solution we need to merge our solution with firewall rules. The implementing process are given bellow,

1. We have to set an IF ELSE rules in firewall.
2. We have to merge a algorithm with Access List in firewall.
3. In access list we will add rules for check whether it ICMP request or not. If the request is ICMP it will go for another check.
4. If it is not ICMP it will not be entering to our algorithm. It will go for further rules of firewall.
5. For ICMP request the ACL rules check its packet types value. If data type is 8 or 0 it will go for final check.
6. If data type is not 8 or 0 then it will go for others rules of firewall our algorithm will pass the packet.
7. Final step is to check data field size, normal ICMP request is made within 32 to 64 bytes. Our 3rd rules in ACL is to check what is the size of data field.

```
8.  IF(Data Field<65535)
    {
    Pass the packet;
    };


9.  IF(Data Field=> 65535)
    {
    Block the packet;
    };
```

This set of rules have to add in router firewall. For every Inbound and out bound request router will check those criteria. If the criteria satisfy then it will pass the packet to network. If request is not normal then specific packet will be drop. It will not pass through router.

4.3 Advantage over other solution

By executing Smurf attack, an attacker try to make a server busy for a certain time. Attacker try to execute this attack by sending a Inetrnet Control Protocol Message packets in broadcast with a spoofed IP address which is like a valid host under the targeted server. Attacker use a spoofed IP address so it is impossible for the server to detect whether the request IP is valid or not. The server cannot detect the IP address so it is difficult for the the to block invalid ICMP request message. To block invalid request some solution are already done. But in these solution there are some drawback.

1. Disable IP Broadcast. So when the server want to send any broadcast message it is impossible because broadcast is blocked.
2. Block all ICMP packets. ICMP packets are used for sending error message. So it is impossible to send back any error message when any error occurred.
3. The router will drop valid users packet when the threshold values are exceeded. For a second of time a number of packets are set which is known a threshold per second. If the threshold is exceed then server will drop all other packets.

In our solution we first check whether the packets is Internet Control Message Protocol packet or not. If the packet is a ICMP packet then we re-check the data field of ICMP packet that it is maximum or not.If the the data field is maximum then the server will block that particular packet. Here are some advantages of our solution over other solution.

1. Doesn’t disable IP broadcast. So when the server want to broadcast any message, the server will easily broadcast it.
2. Doesn’t block all ICMP request. So that valid user can send ICMP request.
3. Doesn’t block IP address. In our solution when any data packet is came from any host under the network with maximum data field size, then we just block that particular packet, doesn’t block the IP address. So valid user packets are also blocked for that particular time if treshold exceed.
4. The router will not drop the packets when the threshold values are exceeded. In our solution there is no thershold for a second. So how much packets are came to the server in a second server can not drop or block any packet if the data field size is normal. So valid user can not suffer any problem.

Chapter 5: Conclusion and Future Works

5.1 Conclusion

In this paper we have discussed fully about Distributed Denial of Service (DDoS) and more specifically on Smurf attack. In our suggested algorithm, it is a process to prevent Smurf attack to a specific server. But it is not possible to detect the real attacker as the is using spoofed IP address which is valid. The process is receiving all the traffic coming to the server without checking their validity but the traffics are not going to the server so the performance of the server will not be hampered. The router have to check the Internet Control Message Protocol data field which is maximize by the attacker. In this paper, various segments utilized in Smurf attack have been introduced, and how the attack traffic is intensified towards the victim server. It is appeared in this paper it is feasible for a Smurf attack to weaken an extremely fast connection such as OC-24, OC-192 or even OC-3840 connections by enhancing attack data transmission regardless of whether an attacker is just using a modem.

5.2 Future Work

In future our algorithm can be improved by adding a database in the system which will contain all valid users IP address. This database can check source IP address of the incoming traffic with the existing data saved on the database. It can also keep record of the source IP address which is sending Internet Control Message Protocol message with maximum size data field. This saved record can help to obtain a threshold value by which we can compare the data field size without checking it with maximum data field size.

Chapter 6: References

[1] Y. Chaba, Y. Singh, and P. Aneja, \Performance Analysis of Disable IP Broadcast Technique for Prevention of Flooding-Based DDoS Attack in MANET," vol. 4, no. 3, pp. 178{183, 2009.

[2] G. Zhao, \A real-time DDoS attack detection and prevention system based on per-IP tra_c behavioral analysis A Real-Time DDoS Attack Detection and Prevention System Based on per-IP Tra_c Behavioral Analysis," no. August 2010, 2016.

[3] H. Guerid, A. Serhrouchni, M. Achemlal, and K. Mittig, \A Novel Trace-back Approach for Direct and Reected ICMP Attacks," 2011. 7

[4] S. Kumar and S. Member, \Smurf-based Distributed Denial of Service (DDoS) Attack Amplification in Internet," no. 0521585, 2007.

[5] S. M. Specht, \Distributed Denial of Service : Taxonomies of Attacks, Tools , and Distributed Denial of Service : Taxonomies of Attacks ,Tools and Countermeasures," no. January, 2004.

[6] M. Azahari, M. Yusof, F. Hani, M. Ali, and M. Y. Darus, \Detection and Defense Algorithms of Di_erent Types of DDoS Attacks," vol. 9, no. 5, 2017.

[7] R. Vishwakarma and A. K. Jain, \A survey of ddos attacking techniques and defence mechanisms in the iot network," Telecommunication Sys-tems, pp. 1{23, 2019.

[8] U. Tariq, M. Hong, and K.-s. Lhee, \A Comprehensive Categorization of DDoS Attack and DDoS Defense Techniques *," no. Mic, pp. 1025{1036, 2006. 8