Cyber Times International Journal of Technology & Management

Vol. 11 Issue 1, October 2017 – March 2018

TABLE OF CONTENTS

PROPOSED FORMULA TO ENUMERATE ICMP DOS/ DDOS ATTACK

Pulkit Gambhir
Student, B-Tech – MSIT
Guru Gobind Singh Indraprastha University
gambhirpulkit203@gmail.com

Dr. Anup Girdhar
CEO-Founder
Sedulity Solutions & Technologies
anup@sedulitygroups.com

ABSTRACT

The Information Technology Amendment Act-2008, Section-43(f) states, about the DoS (Denial of Service) attack[11]. The implementation of DoS and DDoS attack by the attacker may vary and based on different types of services and protocols. The proposed work is to implement the DoS and DDoS attack and accordingly the formula to revamp the "ping of death" attack using ICMP. "Ping of death" is based on ICMP to choke the services of the target machine by sending unlimited packets. As with the victim's machine network being choked the attacker's system network is also compromised. So when the attackers want to attack the target machine on a massive scale they use DDoS attack in which it uses several systems to attack one target system. The advantage is that in DDoS the network of attacker's system is not compromised to a larger extent as it follows a distributed approach. This research proposes the different relationships between the parameters obtained a formula for the percentage of network choked and the value of the proportionality constant 'k'.

KEYWORDS: *DoS, DDoS, ICMP, Ping of Death.*

I. INTRODUCTION

ICMP is a connectionless protocol which stands for Internet Control Message Protocol. It is this protocol which is used to tell that whether a system is able to communicate with the specified domain name or IP address or not[4]. In this process we use a command called "ping". The syntax for using the ping command is <Ping domain name/IP address>. The information that can be gathered from this command is:
Operating system of the target machine can be checked. Windows by default send 32 bytes and Linux by default send 64 bytes to the specified ISP address or domain name.

TTL (Time To Live): This is basically the time taken to;

a. Accept the packet.
b. Process the packet
c. Release the packet

The type of operating system can also be checked from the value of TTL

if TTL=32, then it is an old Linux router
if TTL=64, then the system has a Linux OS
if TTL=124, then the system has a Windows OS
if TTL=255, then it is an old windows based router[4].

If any router is available in the networks then the value of TTL is reduced by 1. The reduction should not be more than 30; otherwise the packet sent would be lost.

- Minimum, Maximum, Average-These are all time parameters. It tells us the time in which the response comes back.
- Request Timed Out-This message is received when the specified IP address or domain name has disabled or blocked its ICMP.

DOS (DENIAL OF SERVICE)

DoS attack is basically an attack in which an attacker sends an unlimited amount of packets to the target machine so that the target's system network can get choked. It is also known as "Ping of Death". We can use more than 1 terminal to choke the target's system network by 100%.

The syntax for this DoS attack using ICMP is-
ping -l <size of packet> -t <IP address/Domain Name>[4]

- -l: it is used to specify the length of the packet.
- -t: it is used for sending unlimited packets.

Maximum size of the packets can be 65500 bytes. So "ping of death" attack does not exist more because the maximum limit is reduced to 65500 and if we add more size, it simply drops the packet request.

DDOS (DISTRIBUTED DENIAL OF SERVICE)

When a packet of specific size is sent to the target machine, it chokes its network and comes back and chokes the attacker's network as well. So when unlimited amount of packets are sent to the target machine to choke its network by x%, the attacker's system network also gets choked by x%.

So DDoS attack can be applied to attack the target machine. In this attack several systems are used to attack one target system. So in this process, as several systems (let's say n) will be attacking 1 system and choking it by x%, whereas on the attacker's side each system will get choked by (x/n)% where n is the no. of system attacking using same no. of terminals(command prompts). So, a distributed approach takes place in this process.

II. NEED OF THE STUDY

This paper is of importance as the formula constructed for percentage of network choked gives information about the parameters involved in the process and also the user can estimate the amount of damage a machine can get with a given link speed, terminals and the size of packet.

III. METHODOLOGY

This is basically a process to categorize the research into two parts, i.e.,

SURVEYS AND GATHERING INFORMATION

Two different surveys have been conducted using ICMP. Ping command has been used and packets of different sizes are sent to a virtual window. The information gathered is as follows;

- percentage of network utilization
- link speed
- networking graph
- size of packets(in bytes)

CALCULATIONS

The numbers of systems used in DDoS attack have been calculated after specifying number of terminals to be used on every system.

By doing surveys, gathering information and through calculation, there will be enough parameters to propose the relationships between different parameters, a formula for the percentage of network choked of the target machine and a value for the proportionality constant 'k'.

IV. HYPOTHESIS

In this experiment it has been found out that while doing a DDoS attack, the attacker should know the maximum limit of the packet (in bytes) which can be sent to the target machine. By knowing the amount of bytes of the packet that can be transmitted to the target machine, the attacker can estimate the exact number of systems that the host computer has to be differentiated into. It is important to specify the maximum number of terminals by a single machine which may vary from user to user. In the following surveys the maximum no. of terminal used by a single system is taken as 10 in Survey 1 and 2.

SURVEY 1

In the first survey a DDoS attack has been done on a virtual window using ping command. Now as seen in Fig. 1 that when an unlimited amount of packets(each of 65500 bytes i.e. the maximum amount of bytes in a packet allowed) are sent to the IP of the target machine at the speed of 1000mbps it chokes 0.1% of the target's system network. Now similarly when the attack is done by 10 terminals (command prompts) it will choke 1% of the target's system network. As the attacker's system network will also get choked in the process so, attacker has to use DDoS attack to choke the target's system network by 100%. So, in this process the attacker can figure out that if 1 system, by opening 10 terminals can choke 1% of its own system network as well as the target system network, so in order to choke 100% of the target's system network the attacker needs 100 systems (with 10 terminals giving the same ping command and transmitting unlimited packets (65500 bytes) to the target's system) where each system network of the attacker has been choked by 1%.

CALCULATIONS

no. of terminal/s =1
No. of packets =unlimited
size of a single packet=65500
link speed=1000mbps
network choked=0.1%

when the no. of terminals=1000
network choked will be (0.1*1000)=100% [which is not acceptable to attacker as it chokes the attacker's system network]

So, DDoS attack has to be taken machine where the no of terminals has to be differentiated w.r.t the no of terminals for one system.

So, the no. of computers will be=dt/dn [t=no of terminal and n=maximum no of terminals on one system]

so,
t=1000
n=10

so the no. of computers for choking 100% of the target's system when attaker's system is sending unlimited packets of 65500 bytes each @ 1000mbps will be 1000/10=100.

Now, when link speed is 100 mbps-:
no. of terminal/s =1
No. of packets =unlimited
size of a single packet=65500
link speed=100mbps
network chocked=1%

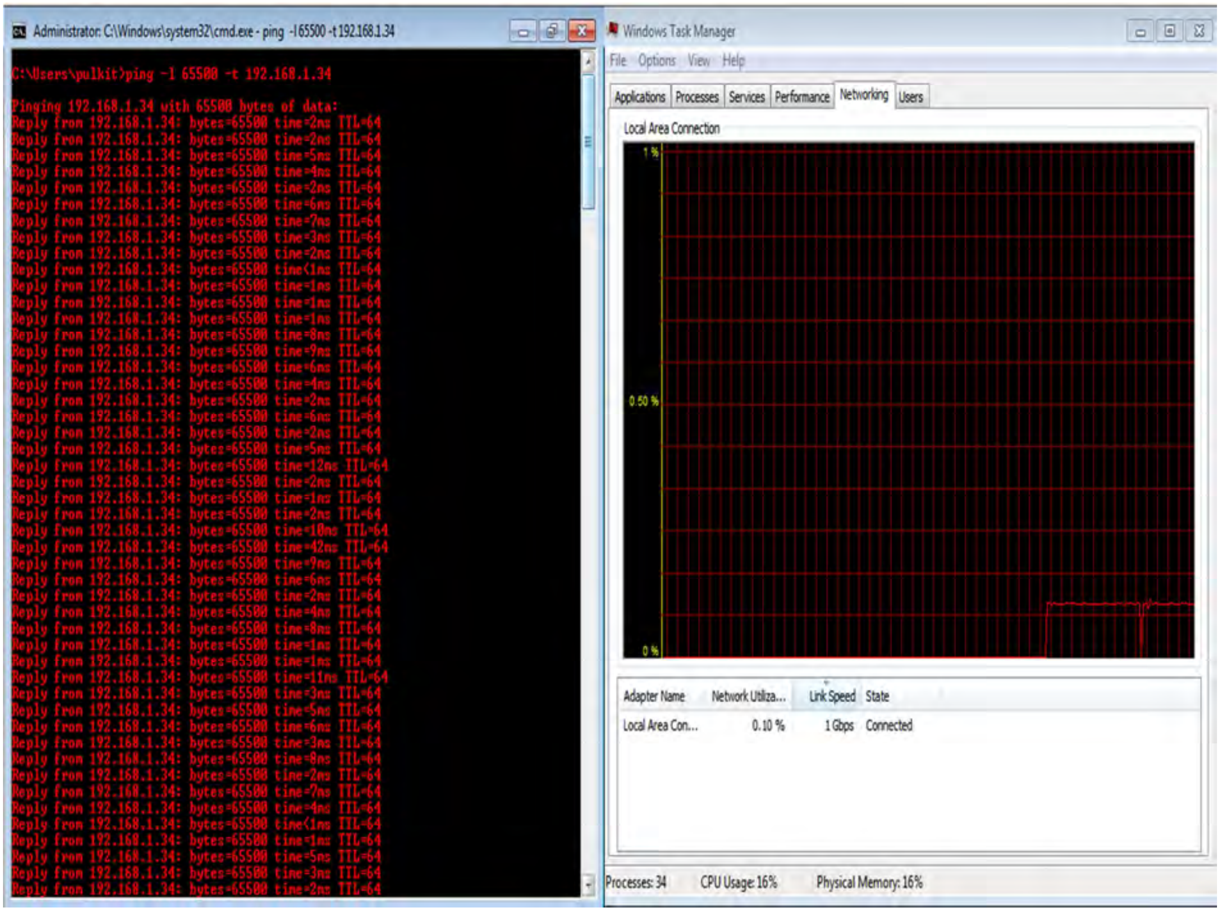
when the no. of terminals=100

network choked will be (1*100)=100% [which is not acceptable to attacker as it chokes the attacker's system network]

So, DDoS attack has to be taken machine where the no. of terminals has to be differentiated w.r.t the no of terminals for one system.

So, the no. of computers will be=dt/dn [t=no. of terminal and n=maximum no. of terminals on one system]

t=100
n=10
which implies, that the no. of computers for choking 100% of the target's system when attacker's system is sending unlimited packets of 65500 bytes each @ 100mbps will be 100/10=10.


Administrator: C:\Windows\system32\cmd.exe - ping -l 65500 -t 192.168.1.34

```
C:\Users\pulkit>ping -l 65500 -t 192.168.1.34

Pinging 192.168.1.34 with 65500 bytes of data:
Reply from 192.168.1.34: bytes=65500 time=2ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=2ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=5ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=4ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=2ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=6ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=7ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=3ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=2ms TTL=64
Reply from 192.168.1.34: bytes=65500 time<1ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=1ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=1ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=1ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=8ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=9ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=6ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=4ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=2ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=6ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=2ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=5ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=12ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=2ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=1ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=2ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=10ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=42ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=9ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=6ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=2ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=4ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=8ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=1ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=1ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=11ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=3ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=5ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=6ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=3ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=8ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=2ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=7ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=4ms TTL=64
Reply from 192.168.1.34: bytes=65500 time<1ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=1ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=5ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=3ms TTL=64
Reply from 192.168.1.34: bytes=65500 time=2ms TTL=64
```

Adapter Name	Network Utiliza...	Link Speed	State
Local Area Con...	0.10 %	1 Gbps	Connected

Processes: 34 CPU Usage: 16% Physical Memory: 16%

Figure 1: Showing the Network Choked

SURVEY 2

In this survey certain limit has been taken on the packets. As observed form the previous survey that the no. of systems for choking 100% of the target's system network when attacker's system is sending unlimited packets of 65500 bytes each @ 1000mbps will be 100. When a limit is put on the maximum size of packet the no. of systems used for DDoS attacks are increased. Now let us assume that the maximum limit be 32750 bytes for each packet. As we know that the size of each packet is 32750 byte and is choking 0.05% of the target's system network at the speed of 1000mbps. As we know from Survey 1 that maximum network choked with one terminal can reach up to 0.1%. So in order to reach 0.1% we experimentally prove that we need 2 terminals.

So one system with 10 terminals will choke up to 0.5% of the target's system.

CALCULATIONS

no. of terminal/s we are working on=1
No. of packets =unlimited
size of a single packet=32750
link speed=1000mbps
Network choked=0.05%

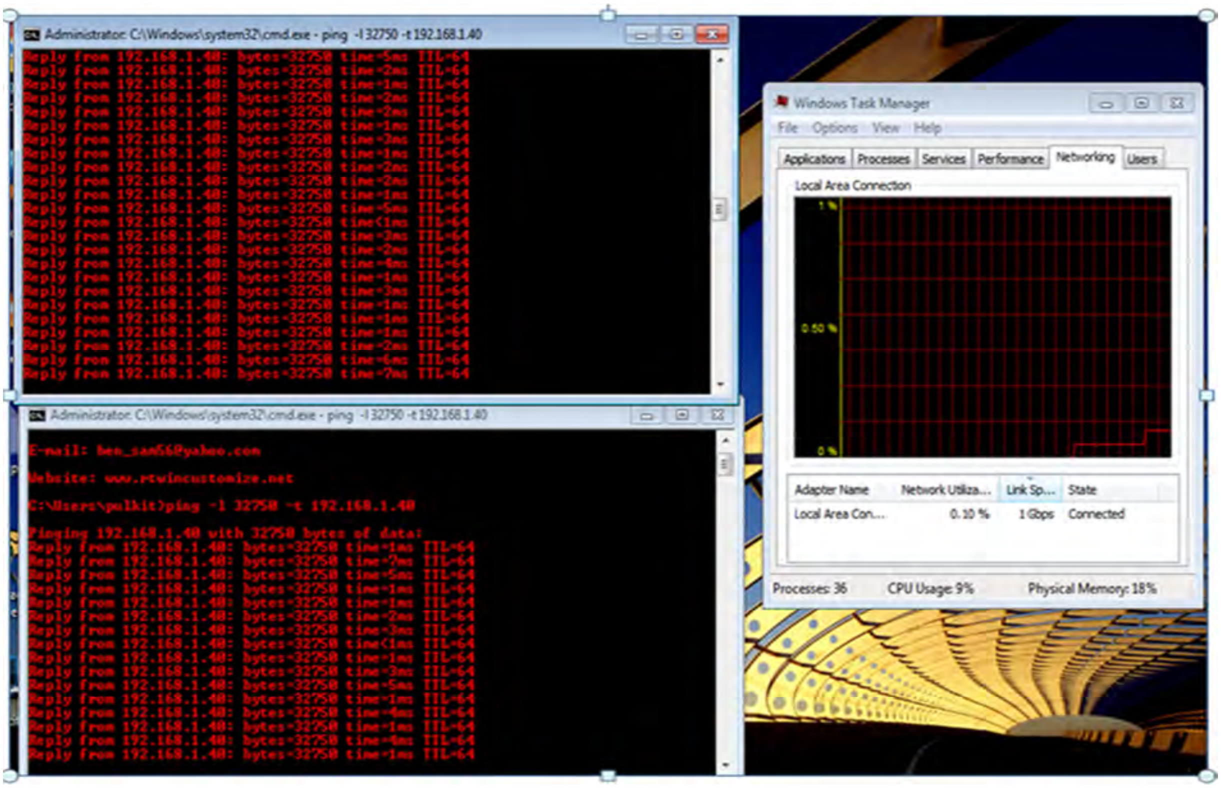
when the no. of terminals=2000
Network choked will be (0.05*2000)=100% [which is not acceptable to attacker as it chokes the attacker's system network]

So, DDoS attack has to be taken machine where the no. of terminals has to be differentiated w.r.t. the no. of terminals for one system.
So, the no. of computers will be=dt/dn [t=no. of terminals and n=maximum no. of terminal attacker wants to choose]
t=2000
n=10
which implies, that the no. of computers for choking 100% of the target's system when attacker’s system is sending unlimited packets of 32750 bytes each @ 1000mbps will be 200/10=200.

Now, when link speed is 100 mbps-:
no. of terminal/s =1
No. of packets =unlimited
size of a single packet=32750
link speed=100mbps
Network choked=0.5%

when the no. of terminals=200
Network choked will be (0.5*100)=100% [which is not acceptable to attacker as it chokes the attacker's system network]
So DDoS attack has to be taken machine where the no. of terminals has to be differentiated w.r.t the no. of terminals for one system.

So, the no. of computers will be=dt/dn [t=no. of terminal and n=maximum no. of terminals on one system]
so,
t=200
n=10
so, the no. of computers for choking 100% of the target's system when attaker's system is sending unlimited packets of 32750 bytes each @ 100mbps will be 200/10=20.



Administrator: C:\Windows\system32\cmd.exe - ping -l 32750 -t 192.168.1.40

```
Reply from 192.168.1.40: bytes=32750 time=5ms TTL=64
Reply from 192.168.1.40: bytes=32750 time=2ms TTL=64
Reply from 192.168.1.40: bytes=32750 time=1ms TTL=64
Reply from 192.168.1.40: bytes=32750 time=2ms TTL=64
Reply from 192.168.1.40: bytes=32750 time=2ms TTL=64
Reply from 192.168.1.40: bytes=32750 time=1ms TTL=64
Reply from 192.168.1.40: bytes=32750 time=2ms TTL=64
Reply from 192.168.1.40: bytes=32750 time=1ms TTL=64
Reply from 192.168.1.40: bytes=32750 time=2ms TTL=64
Reply from 192.168.1.40: bytes=32750 time=2ms TTL=64
Reply from 192.168.1.40: bytes=32750 time=1ms TTL=64
Reply from 192.168.1.40: bytes=32750 time=5ms TTL=64
Reply from 192.168.1.40: bytes=32750 time<1ms TTL=64
Reply from 192.168.1.40: bytes=32750 time=3ms TTL=64
Reply from 192.168.1.40: bytes=32750 time=2ms TTL=64
Reply from 192.168.1.40: bytes=32750 time=4ms TTL=64
Reply from 192.168.1.40: bytes=32750 time=1ms TTL=64
Reply from 192.168.1.40: bytes=32750 time=3ms TTL=64
Reply from 192.168.1.40: bytes=32750 time=1ms TTL=64
Reply from 192.168.1.40: bytes=32750 time=1ms TTL=64
Reply from 192.168.1.40: bytes=32750 time=1ms TTL=64
Reply from 192.168.1.40: bytes=32750 time=2ms TTL=64
Reply from 192.168.1.40: bytes=32750 time=6ms TTL=64
Reply from 192.168.1.40: bytes=32750 time=7ms TTL=64
```

Administrator: C:\Windows\system32\cmd.exe - ping -l 32750 -t 192.168.1.40

```
E-mail: ben_san56@yahoo.com

Website: www.rtwincustomize.net

C:\Users\pulkit>ping -l 32750 -t 192.168.1.40

Pinging 192.168.1.40 with 32750 bytes of data:
Reply from 192.168.1.40: bytes=32750 time=1ms TTL=64
Reply from 192.168.1.40: bytes=32750 time=7ms TTL=64
Reply from 192.168.1.40: bytes=32750 time=5ms TTL=64
Reply from 192.168.1.40: bytes=32750 time=1ms TTL=64
Reply from 192.168.1.40: bytes=32750 time=1ms TTL=64
Reply from 192.168.1.40: bytes=32750 time=2ms TTL=64
Reply from 192.168.1.40: bytes=32750 time=3ms TTL=64
Reply from 192.168.1.40: bytes=32750 time<1ms TTL=64
Reply from 192.168.1.40: bytes=32750 time=1ms TTL=64
Reply from 192.168.1.40: bytes=32750 time=3ms TTL=64
Reply from 192.168.1.40: bytes=32750 time=5ms TTL=64
Reply from 192.168.1.40: bytes=32750 time=1ms TTL=64
Reply from 192.168.1.40: bytes=32750 time=4ms TTL=64
Reply from 192.168.1.40: bytes=32750 time=1ms TTL=64
Reply from 192.168.1.40: bytes=32750 time=4ms TTL=64
Reply from 192.168.1.40: bytes=32750 time=1ms TTL=64
```

Adapter Name	Network Utiliza...	Link Sp...	State
Local Area Con...	0.10 %	1 Gbps	Connected

Processes: 36 CPU Usage: 9% Physical Memory: 18%

Figure 2: Screeshot showing network choked

V. RELATED WORKS

As numerous researches are going on to prevent DDoS attacks, researchers are able to find numerous safety measures to avoid DDoS attacks. A statistical approach can also be applied to analyse the distribution of network traffic to recognize the normal network traffic[1]. A fundamental weakness of the Internet is IP Spoofing. As attacker can gain control of larger numbers of the compromised computers, attackers can direct these “zombies” encrypted, only “zombies” can be exposed not the attackers[2].

A proactive technique that can be implemented on the customers' side is Enhanced D-DoS-Mitigation. It consists of a firewall, a verifier node(VN), an Intrusion Prevention System(IPS) device and a Reverse Proxy(RP) in front of the system[3]. Websites which have disabled ICMP packets simply show RTO, but then the I.P address of the websites can be obtained and the packet size can be manipulated[4].

DDoS can be demonstrated by stimulating a distribution zombie program that will carry a Ping of Death attack[6]. Loss of network resources causes economic loss, work delays and a loss of communication between network users. Hardware based checking and filtering mechanism can provide an additional layer of defence against DDoS attack[7]. The TCP/IP protocol should be examined to understand DDoS attacks[8].

The ideal time to mitigate a DDoS attack is right at the launching location by not allowing it to reach the target over WAN circuits[9]. Rate limiting and BCP3 are also two processes applied for mitigation of DDoS attacks[10].

A cracking code was developed by V. Priyadharshini and Dr. K. Kuppusamy which maintains a status table which keeps the I.P address. If a person signs on the website for the first time, it makes the status as a genuine user. If the user with the same I.P address signs for the 2nd, 3rd and the 4th time, it marks the status as a normal user. If the user signs for the fifth time, the status changes to attacker, and that specific I.P is deprived of the services[12]. This research proposes different relationships between the parameters obtained after using ping command. Based upon that, a formula for the percentage of network choked has been constructed and the value of proportionality constant 'k' has been found out.

VI. RESULT AND DISCUSSION

So according to the above surveys it has been found out that the attacker should know about the maximum limit of the size on the packet, then the attacker can determine the number of systems with which the attacker needs to attack the target machine. The attackers must specify the number of terminals they want to use on each system. The user will be able know the percentage of network choked of the system with given size of packet, number of terminals and link speed.

VII. FINDINGS

From the above surveys the following relations can be found out:

1. The percentage of network choked (%NC) is directly proportional to the size of 1 packet (SP).
2. The percentage of network choked (%NC) is proportional to the no. of terminals (T).
3. The percentage of network choked (%NC) is inversely proportional to the link speed(S).
4. As it takes 2000 terminals to choke 100% of target's system network when packet size is 32750 and it takes 1000 terminals to choke the target's system network by 100% when packet size is 65500. So, a unitary approach is there.

Combining points 1,2 and 3 we can say-:
%NC is proportional to (SP*T)/S...............(1)
which implies, %NC=k(SP(in megabits)*T)/S(in megabits) where k is a proportionality constant..........(2)

Putting the above formula in the first survey, k can be calculated.
The value of k is found out to be 190.83969hertz (approx).

VIII. FUTURE SCOPE & LIMITATION

The future scope of this research is to propose relationship between more parameters that can be obtained in the process and derive a formula accordingly.

In order to calculate the percentage of network choked we should know the total number of terminals used in attack, size of 1 packet and the link speed which may vary from user to user.

IX. CONCLUSION

DDoS is an attack which can cause serious damage to the victim's system network. This research focuses to construct a formula for the percentage of network choked based upon the relationship of the parameters obtained. The proportionality constant “k” has also been found out. This can be helpful for a person manipulating the packet size for ICMP as the person can estimate to what extent the system's network can get choked with a given number of terminals and link speed.

X. ACKNOWLEDGEMENT

This research has been proposed by reviewing different research papers and after reviewing them, we got the idea to propose different relations between different parameters and constructing a formula for network choked.

REFERENCES

[1] Anup Bhange, Amber Syed, Satyendra Singh Thakur,February,2012,”DDoS Attacks Impact On Network Traffic and its Detection Approach”, International Journal of Computer Application,Vol.40, Issue No.11, 36-40.

[2] B.B Gupta, R.C Joshi, Manoj Misra, April 2010, “Distributed Denial of Service Prevention Techniques”, International Journal of Computer and Electrical Engineering. Vol. 2, Issue No.2, 268-276.

[3] D.H Raibhagkar, Dr. S. S Sherekar, Dr. V. M Thakare,21st May,2017,”DDoS Attack on Cloud Access” International Journal on New Frontiers of Engineering, Science, Management and Humanities. Vol. 6, Issue 5, 53-57.

[4] Harshita, Ruchikaa Nayyar, March-April-2017,”Detection of ICMP Flood DDoS Attack, International Journal of Computer Science Trends and Technology (IJCST)”,Vol.5 Issue-2,199-205.

[5] Himanshi Bajaj, Indu Sibal, Dr. Anup Girdhar, 2014, Study of DoS/DDoS Attack using ICMP Protocol”, Cyber Times International Journal of Technology & Management, Vol.8 Issue2,8-16.

[6] Khaled M.Elleithy, Drazen Blagovic, Wang Cheng, Paul Sideleau, 2005,”Denial of Service Attack: Analysis Implementation and Comparison”, Journal of Systemic Cybernics, and informatics 3.1(2005):66-71.

[7] Keyur Chauhan, Vivek Prasad, September, 2015,”Distributed Denial of Service (DDoS) Attack Techniques and Prevention on Cloud Environment”, International Journal of Innovation and Advancement in Computer Science, Volume 4,210-215.

[8] K.Saranya, N.Aparna, June-2016,”Prevention of Vulnerability on DDoS Attack Towards Wireless Networks”, International Journal of Merging Technology and Advance Research in Computing, Volume 4, Issue 14, 1-12.

[9] K. Santhi, February 2017,”Detection Parameters and Mitigation in Cloud Environment”, International Journal for Modern Trends in Science and Technology, Volume 3, 79-82.

[10] Rajnish Kumar Misra, Amarnath Singh, Vipin Kumar Gupta, May-June, 2015”Study of Recent Trends of Distributed Denial of Service Attack and Handling Approach”, International Journal of Computer Science Trends and Technology(IJCST), Volume 3, Issue 3, 13-17.

[11] Universal Law Publishing an Imprint of Lexis Nexis, 2000 “The Information Technology Act”, 2000, Page no.24.

[12] V.Priyadharshini, Dr. K.K Kuppusamy,May-June,2012,”Prevention of DDoS Attacks using New Cracking Algorithm”, International Journal of Engineering Research and Application, Vol. 2, Issue 3, 2263-2267.