International Journal of Security and Its Applications
Vol.9, No.8 (2015), pp.303-316
http://dx.doi.org/10.14257/ijsia.2015.9.8.27

Impact Evaluation of Distributed Denial of Service Attacks using NS2

[1]Raghav Vadehra, [2]Nitika Chowdhary and [3]Jyoteesh Malhotra

[1,3]ECE Dept., GNDU RC Jalandhar
[2]CSE Dept., GNDU RC Jalandhar
raghav.vadehra12@gmail.com[1], nitu.expert@gmail.com[2], jyoteesh@gmail.com[3]

Abstract

Distributed Denial of Service (DDoS) attacks has been a prominent threat to the Internet community. The attack effect is recognized by large number of client base due to the dependency of majority users on World Wide Web. In such an attack, the attacker targets a machine or a server to thwart its services to the intended users. These attacks are majorly motivated by the presence of multiple groups of hackers present on the Internet. As the research has progressed in this field, researchers have encountered a lot many ways through which attacks have been successful launched. In early years of its birth, the Internet was not designed keeping in mind various possible security aspects thus it lacked this immunity in present day. This paper covers the advent of the DDoS attacks along-with their types. We have also designed certain simulation scenarios based on flooding based DDoS attacks to measure its impact on legitimate users. A discussion on the present solutions to combat such attack situations concludes our work.

Keywords: *distributed denial of service attacks (ddos), botnet, zombie*

1. Introduction

Distributed Denial of Service (DDoS) attack is an attempt to make a machine or resource unavailable to the intended users. DDoS attack generally consists of efforts to indefinitely interrupt or suspend services of a host connected to the internet. The attack effect can either be crashing down the servers or slowing them down. To launch an attack, attacker first compromises the vulnerable hosts like the systems which do not have firewalls installed on them. These systems known as zombies then are forced to launch a heavy stream of unsolicited packets towards the victim. Disruption in services caused this causes a heavy loss of revenue. Hence, it becomes really important to develop methodologies that could help to encounter such attacks.

This paper is divided into seven sections; Section 2 provides background of DDoS attacks and explains various terms related to these attacks and their architecture of DDoS attacks along-with types of attacks and their impact on different layers of TCP/IP. Section 3 explains different simulation methodology and parameters used to study flooding based attacks in wired networks. Section 4 discusses results based on different scenarios of simulation. Section 5 is future work and finally, Section 6 gives concluding remarks on DDoS attacks.

2. Background

It is hard to get back to dates as to when do the first attack happened. However, the attack of 1999 against the servers of University of Minnesota was accounted for rendering 227 systems unusable for a couple of days. It was followed by the world's largest attack of that time in February 2000, when number of websites went offline for several hours.

ISSN: 1738-9976 IJSIA
Copyright ⓒ 2015 SERSC

Since then several DDoS attacks hit the network and lead to enormous financial and data loss. Recently, a DDoS attack which targeted the most popular sites like Copyright.com, BMI.com, and etc. lead to service shutdown for 10 minutes [1]. According to Arsaa Almori et al. [1] most of the DDoS attacks involve flooding at the network and transport levels. A DDoS attack is launched by a large network of compromised machines called Botnet. Software programs that control the computer for a specific purpose are called bots. Bot is derived from term 'ro–bot' which runs on small scripts that are designed to perform specific predefined functions in an automated fashion [2]. Botnet is remotely controlled by its Botmaster. Botnets acquire vulnerable machines using methods utilized by other malwares and thus create an infrastructure between them systems to perform malicious activities.

Some of the definitions to provide a better insight into how attacks are actually made feasible are [2]:

a. Bot: It is typically an executable file capable of performing specific functions each of which can be triggered by a specific command. A bot when installed on to the machine copies itself into configurable install directory and changes system each time it is rebooted.
b. Zombie: It is the compromised internet host on which the malicious bot is installed. Once infected the target host are called as Zombies. According to Webroots [3] bad bots perform malicious tasks allowing an attacker to take control over an affected computer for a criminal to control remotely.
c. Control Channel: It is a private IRC (Internet Relay Chat) channel created by attacker as a meeting point for all the bots to join once they are installed on an infected machine and are online, it comprises of a channel name and a password key to authenticate
d. IRC Server: It is a server providing IRC services, this could be legitimate public server like DALNET or another attacker's compromised machine to perform attack.
e. DDoS attacks have become so prominent that they cannot be confined to one or two types. According to Ruby B. Lee et al. [9] different kinds of attacks that are used by attackers to render the system useless are as follows:

a. Bandwidth Depletion Attack**:** These are mainly flooding based DDoS attacks in which victim server's network bandwidth gets congested when zombies flood the network with unwanted traffic that prevents legitimate traffic to reach the victim system [10].
b. Resource Depletion Attack**:** This attack ties up the resources of the victim server and prevents it to process legitimate requests [10].
c. Amplification Attack: Broadcast address is used to amplify attack by zombies which causes all the systems in the subnet to send replies to the targeted victim so as to paralyse its network with the incoming flow of acknowledgements and replies.
d. Malformed Packet Attack: In this type of attack malformed packets are sent by the zombies to the victim system in order to crash it. For instance, packets with the same source and destination address ties up the resources of the victim.

2.1. DDoS Attack Architectures

The attacker is hidden behind the layers of multiple zombies. There exist multiple DDoS attacker communication models that have emerged in past decade. These models are discussed in subsequent sections.

 Copyright ⓒ 2015 SERSC

2.1.1. Agent Handler Model: The main players of the attack are:-

a. Attacker: The main source that starts the attack.
b. Handler: Malicious software installed on the system which works according to the attacker.
c. Agent: The handler (software) when installed on the system makes that system an agent (bots/zombies) spread the attack on to the other machines.
d. Victim: Primary victim or main server under attack.

2.1.2. IRC based DDoS Attack: In IRC based DDoS attack model, attacker communicates with the agents through IRC channel. It is difficult to track this type of DDoS attack as attackers use legitimate ports for sending commands to agents. Moreover, high volume of traffic in IRC channels help attackers to hide their presence.

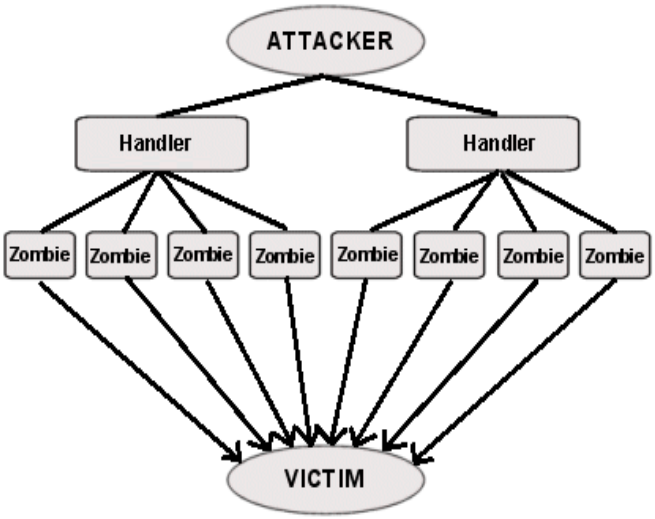


Figure 1. Agent Handler Model of DDoS Attack

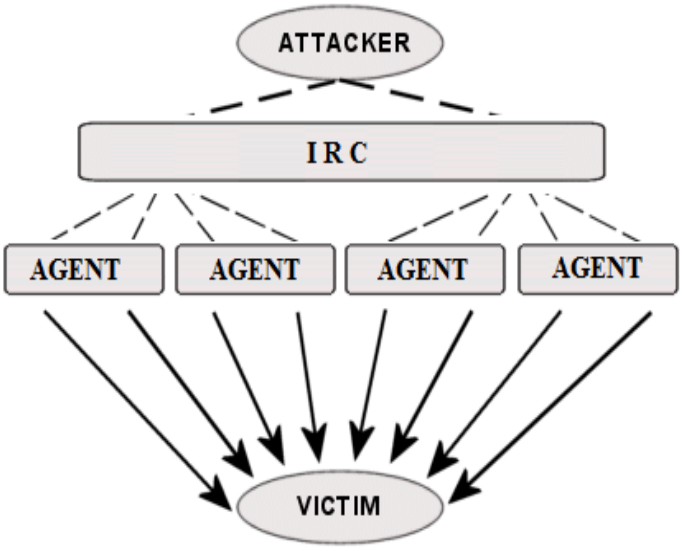


Figure 2. IRC Model of DDoS Attack

Copyright ⓒ 2015 SERSC

2.2. Types of DDoS Attacks

The following section gives a brief description of various types of attacks and their impacts on different layers of TCP/IP. This section describes the research done by different authors in this field.

Table 1. DDoS Attacks and Their Impact

S.NO	DDOS ATTACK	ATTACK TYPE	ATTACKED LAYER	ATTACK DESCRIPTION
1.	TCP-SYN Attack	Resource Depletion	Transport layer-This type of attack uses transport layer protocols i.e. TCP-SYN and thereby reaching limits of bandwidth and connection of hosts.	Essra Alomari et al. [1] described the TCP-SYN Attack. It exploits the weakness of three way handshake sequence of TCP connection. SYN request is sent with spoofed source address is sent to victim. Victim unknowingly accepts the request and sends a SYN+ACK only to be kept waiting for a cross confirmation from the source which in real sense has been spoofed to some other IP address. Hence, it results in denial of service because of binding of resources of the victim.
2.	UDP Flood Attack	Bandwidth Depletion	Transport layer-UDP is another transport layer protocol that is used for DDoS attack.	UDP packets flood the random or specified ports of the victim system for unknown applications and if the application is not found then the victim replies with the ICMP Destination Unreachable Packet resulting in system slowdown as described by Ruby B. Lee et al. in [9].
3.	ICMP Flood Attack	Bandwidth Depletion	Network layer-Uses ICMP (which is a network layer protocol) to block the network bandwidth and firewall with extra load.	Stephen M. Specht et al. [9] described the ICMP flood attack. ICMP ECHO REQUEST packets flood the victim's system i.e. sending packets as fast as possible without waiting for the reply. Hence, it saturates the bandwidth of victim's network connection.
4.	PUSH+ACK Attack	Resource Depletion	Transport layer	In this attack multiple agents send TCP packets to

 Copyright ⓒ 2015 SERSC

				the victim system with PUSH and ACK bits set to zero. Hence, victim unloads all the data in the TCP buffer which leads to system crash [9].
5.	Ping of Death	Resource Depletion	Network layer- Packets which are Protocol Data Units (PDU) of network layer are used for making erroneous fragments.	In Ping of Death attack victim system ends up with the IP packets which are larger than 65,535 bytes when reassembled from the malicious fragments [3].
6.	IP address and packet options attack	Resource Depletion	Network layer	IP address attack- It confuses the victim system with same source and destination address IP Packet Options- Victim system takes additional time to analyse the traffic because of randomized optional fields and QOS bits set to one [9].
7.	Smurf Attack	Bandwidth Depletion Amplification Attack	Network layer	Attacker sends ICMP ECHO REQUEST packets (with return address spoofed to victim's IP address) to network amplifier and which again sends the packets to the systems within the broadcast address range. These systems send the ICMP ECHO REPLY to the victim which saturates the bandwidth of connection [9].
8.	Fraggle Attack	Bandwidth Depletion Amplification Attack	Transport layer	Attacker sends UDP packets (with return address spoofed to victim's echo service port) to ports of the system which supports character generation. Thus the network falls in infinite loop in which system sends character generated to the echo service of the victim and receives echo reply which again leads to the

Copyright ⓒ 2015 SERSC

				same process. Hence this attack blocks the bandwidth of the connection [9].
9.	NTP Amplification	Bandwidth Depletion	Transport and Application layer	Attackers attack the victim servers with UDP traffic with the help of Network Time Protocol(NTP) servers [3].
10.	HTTP Flood Attack	Resource Depletion	Application layer-Overloads the specific services of Application level infrastructure.	This attack uses HTTP GET or POST requests to block the resources of the web server or application. For instance, a request to download a large file from bot to server can significantly consume victim's resources [3].
11.	SIP Flood Attack	Resource Depletion and Bandwidth Depletion	Application layer-Targets login pages with random user Ids and passwords.	B.B. Gupta et al. [1] illustrated SIP flood attack. Attackers flood the Session Initiation Protocol(SIP) proxy servers with SIP INVITE packets with the help of Botnet. It consumes the network bandwidth and server resources of the server making it incapable of providing VOIP service.
12.	Distributed Reflector Attacks	Resource Depletion and Bandwidth Depletion	Application layer	It hides the sources of attack and makes the attack even more distributed in nature. Attacker attacks the zombies which again floods traffic on the victim via third parties. Hence, making it difficult to identify the attack sources. For instance, DNS(Domain Name System) Amplification attack [1].
13.	Slowloris Attack	Resource Depletion	Application layer-Uses high volume HTTP GET Flood or HTTP POST Flood to crash the server.	It targets the victim server by sending partial requests. It constantly sends HTTP headers without completing the request. Hence, victim's connection remains open for a long time which later leads to denial of legitimate connections from clients [3].

 Copyright ⓒ 2015 SERSC

14.	ARP Poisoning	LAN Attack	Network and Data link layer- It disrupts legitimate flow of data with the help of malicious MAC frames.	Address Resolution Protocol(ARP) Spoofing Attack is carried when attacker sends false ARP packets to gateway informing that its MAC address should be associated with the target's IP address. Hence, allowing attacker to drop or not forwarding the packets to the destination.

It is critically important to understand the nature of DDoS attacks in order to develop their countermeasures. These attacks do not rely on any network protocol only but instead exploits the asymmetry between the Internet and the victim. Thus, many researchers are doing the impact analysis of these attacks.

Vern Paxson described the reflector based DDoS attacks in [12]. These attacks hide the sources of attack and make the attack even more distributed in nature. Attacker spoofs requests from victim to large set of internet servers which again floods traffic on the victim. Ketki Arora *et al.* [5] described the effect of flooding based DDoS attack in which the attackers congest the link between ISP edge router and victim's access router. In this attack incoming requests are dropped due to buffer overflow and the stage comes when legitimate clients are denied of service due to bottleneck bandwidth. Vyas Sekar *et al.* [11] analysed the effect the large DDoS attacks based on multiple data sources. Different attack characters like attack duration, packet count, packet rate and protocol type were considered during the analysis. Rocky K.C. Chang [7] described the combination of various protocol based attacks *i.e.* TCP-SYN, SYN-ACK and ICMP. Moreover, he compared two Internet firewall approach, called route based packet filtering and distributed attack detection.

Many of the researchers have studied tools used in the DDoS attacks. For instance, David Dittrich *et al.* [8] analysed Shaft, which is a malware used in DDoS attack and also provided comparative analysis of different tools. Vulnerability analysis of the network is also very necessary in case of these attacks. Salim Hariri *et al.* [6] described several techniques to analyse the network. Graph based network vulnerability analysis, Attack trees and survivability analysis of network specifications are some of those approaches.

3. Simulation Methodology

This section deals with different simulation scenarios based on Flooding based DDoS attacks. In order to describe these attacks NS2 simulator is used. NS-2 is an discrete event based simulator which is used to study both wireless and wired networks. It has support for traffic sources like HTTP, FTP, CBR etc. And network protocols such as TCP or UDP. Methodology of simulation to study DDoS attacks is explained with the help of flow diagram as illustrated in the Figure 3.

Copyright ⓒ 2015 SERSC

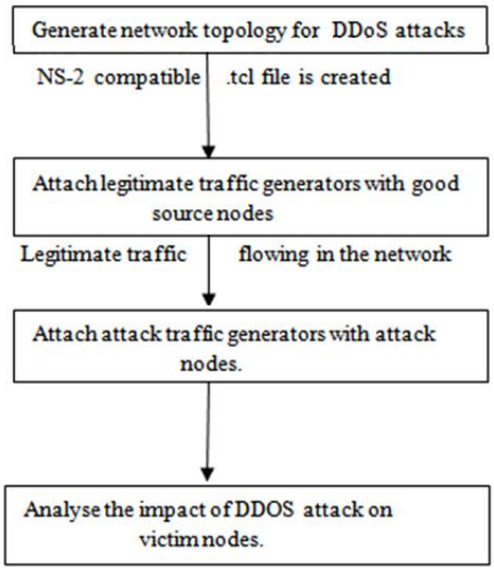


Figure 3. Simulation methodology

First and foremost network topology is generated in .tcl file. Legitimate and attack traffic generators are attached in the network. Next phase involves monitoring traffic flow with the help of simulation parameters at victim or intermediate nodes. And last step involves analysing the traffic flow during DDoS attack and comparing it with the normal scenario (with legitimate traffic generators only).

Performance Metrics

In our simulation we measure the following two metrics:
1. Packet Ids of Dropped Packets
2. Packet Dropping Ratio (PDR)

Packet Dropping Ratio is calculated as follows:

PDR= Number of dropped packets/Number of generated packets

4. Results and Discussion

Effect of DDoS attack on network is explained graphically with the help of different scenarios. Different topologies with and without the presence of attackers have been simulated using NS2. In subsequent subsection we simulate two different attack scenarios and measure the attack effect.

4.1. Scenario 1

This scenario has two cases of network. One with two normal legitimate nodes and other hit by flooding based DoS attack.

 Copyright ⓒ 2015 SERSC

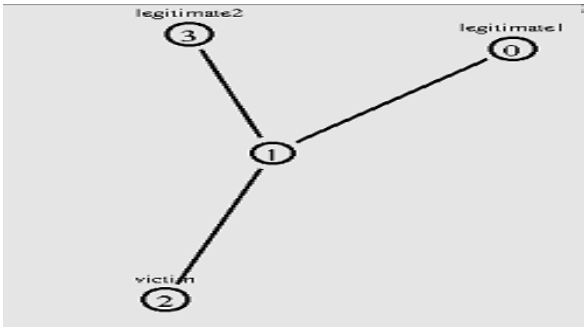


Figure 4. Network in Normal Mode

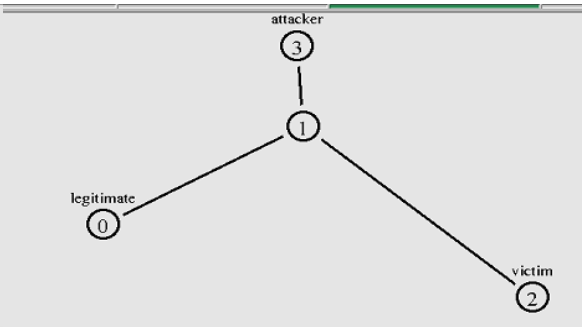


Figure 5. DoS Attack on Network

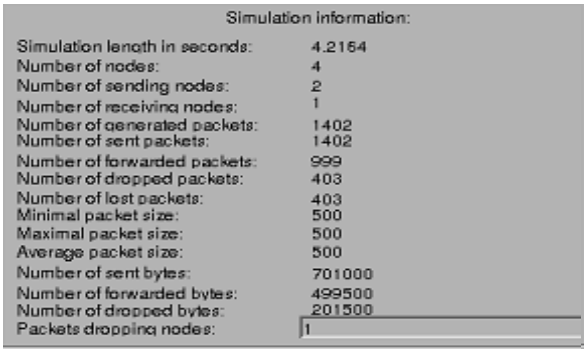


Figure 6. Simulation Information of Network in Normal Mode

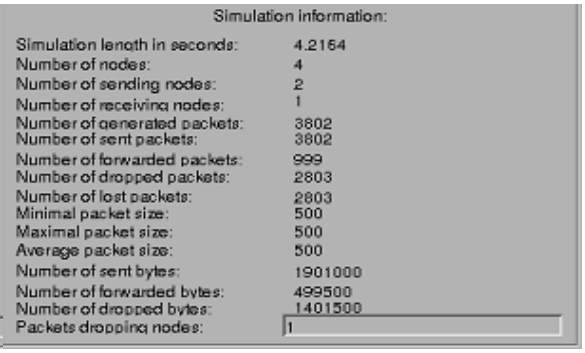


Figure 7. Simulation Information of DoS Attack on Network

From the Figures 6 and 7, It is evident that PDR of network with legitimate users only is 0.287(403/1402) and for network with one attacker is 0.737(2803/3802). It is clear that there is formidable increase in PDR in case of DoS attack.

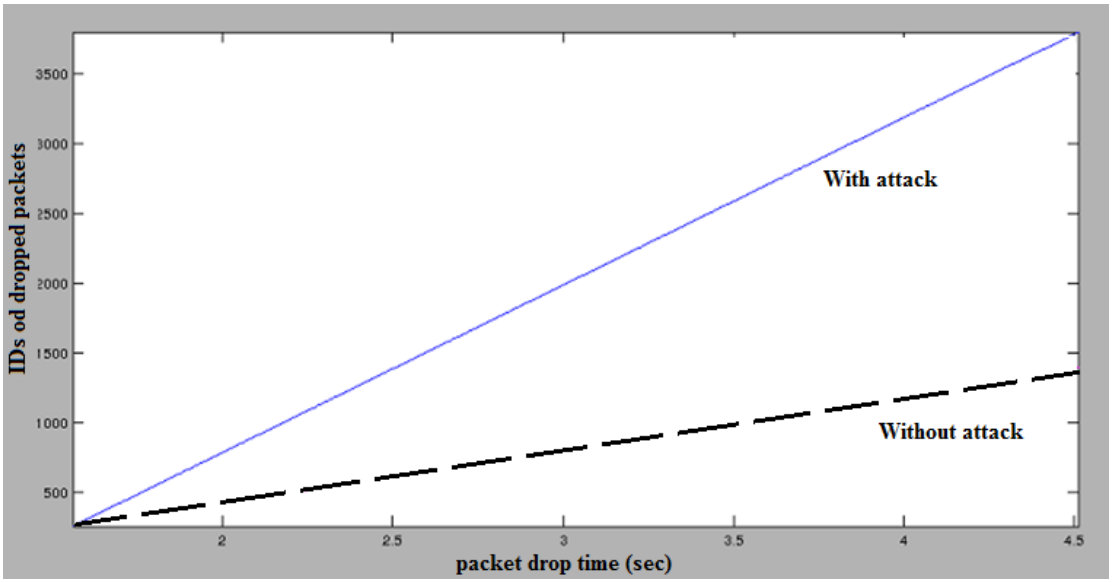
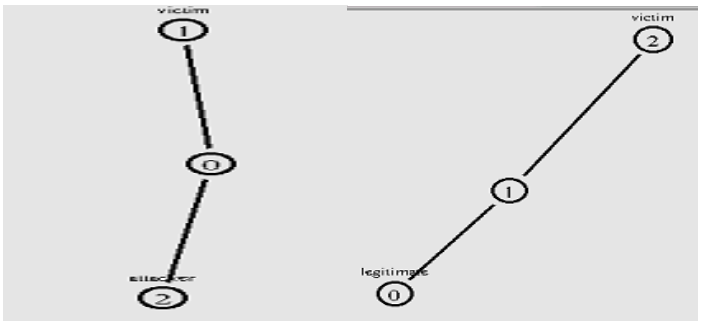


Figure 8. Comparison of Ids of Dropped Packets in DDoS Attack and Normal Network

ISSN: 1738-9976 IJSIA
Copyright ⓒ 2015 SERSC

Figure 8 illustrates that there is huge increase in the range of packet ids that are dropped in networks which suffer DoS attack. However it is not evident that considerable amount of legitimate packets are dropped. To prove that the victim system is denied of the packets from legitimate user we consider another two network cases.



(a) (b)

Figure 9 (a): Network with One Attacker and Victim; 9(b): Network with One Legitimate Node and Victim

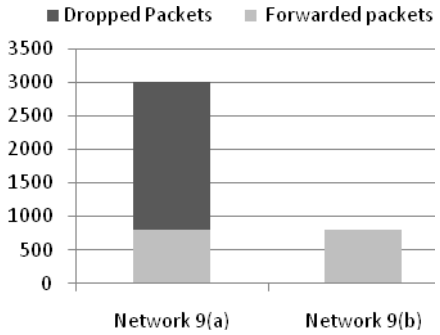


Figure 10. Packet Summary of Both Networks

Considering the legitimate and the attacker's traffic separately as shown in figure 9(a) and 9(b) and then comparing them with the networks in figure 5, following results are obtained:
Total generated packets from legitimate users-801
Total dropped packets from legitimate users-601

Therefore, PDR of legitimate users is 0.750 which is very high. Hence, it is clear that victim system is denied of the packets from legitimate users.

4.2. Scenario 2

Now considering the second scenario. This scenario has two cases of network. One with four normal legitimate nodes and other hit by flooding based DDoS attack by two attackers.

 Copyright ⓒ 2015 SERSC

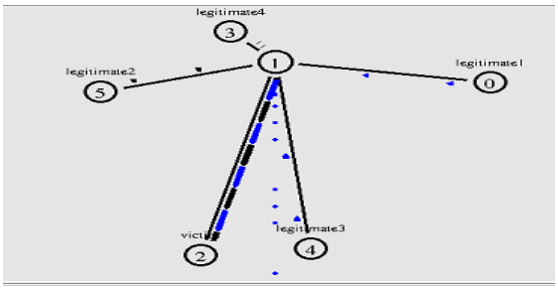


Figure 11. Network with Legitimate Users

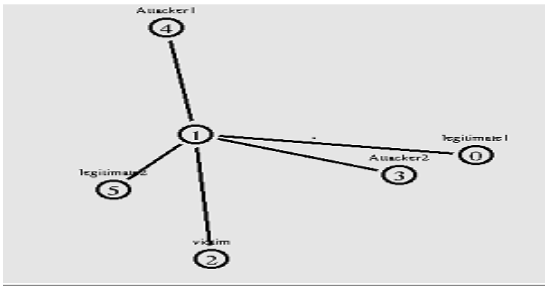
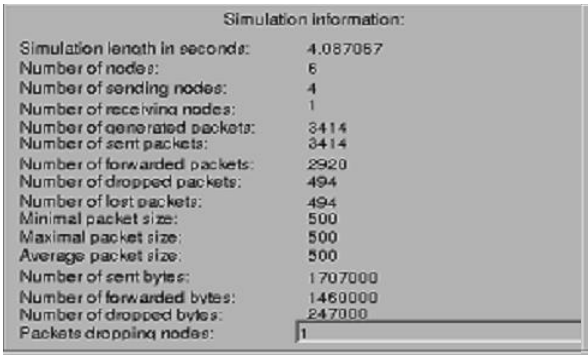
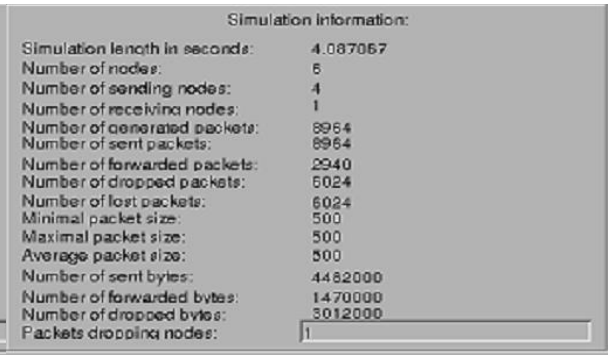


Figure 12. DDoS Attack on Network



Simulation information:	
Simulation length in seconds:	4.087057
Number of nodes:	6
Number of sending nodes:	4
Number of receiving nodes:	1
Number of generated packets:	3414
Number of sent packets:	3414
Number of forwarded packets:	2920
Number of dropped packets:	494
Number of lost packets:	494
Minimal packet size:	500
Maximal packet size:	500
Average packet size:	500
Number of sent bytes:	1707000
Number of forwarded bytes:	1460000
Number of dropped bytes:	247000
Packets dropping nodes:	1

Figure 13. Simulation Information of Network Described in figure 11



Simulation information:	
Simulation length in seconds:	4.087057
Number of nodes:	6
Number of sending nodes:	4
Number of receiving nodes:	1
Number of generated packets:	8964
Number of sent packets:	8964
Number of forwarded packets:	2940
Number of dropped packets:	6024
Number of lost packets:	6024
Minimal packet size:	500
Maximal packet size:	500
Average packet size:	500
Number of sent bytes:	4482000
Number of forwarded bytes:	1470000
Number of dropped bytes:	3012000
Packets dropping nodes:	1

Figure 14. Simulation Information of Network Described in figure 12

4.3. Outcome

PDR of network with four legitimate users and network hit by DDoS attack (two legitimate and two attackers) is 0.144 and 0.672 respectively. Therefore, it is clear that there is high probability of packets being dropped in network hit by DDoS attack. Moreover, it is cumbersome to detect attacks in this scenario because of the following reasons:

a. Two legitimate nodes turn to zombies (attackers) after sometime. So, it is difficult to find out source of the attack.
b. Attackers hit the network at the same time when there is normal increase in traffic in order to confuse the victim system.

Hence, it is very difficult to detect and even find the attack source in case of DDoS attacks. Thus, highly robust defensive techniques are required to combat these attacks.

5. Future Work

Our overall objective to study the impact of DDoS attacks is to answer the challenges posed in reliable detection of these attacks. As a result our future remaining work is to find impactful and effectual method to detect and mitigate DDoS attacks. In this regard, as the first part of our future work we will propose a new hybrid model based on entropy variations of network parameters like source or destination IP address, port address etc. in order to detect these attacks. In second part, we will incorporate some DDoS mitigation strategies and will also implement reliable trace back method to find and block sources of DDoS attacks.

6. Conclusion

This paper provides a deep insight of DDoS attacks and its impact on different layers of TCP/IP communication stack. The paper classifies these attacks based on its type and

ISSN: 1738-9976 IJSIA
Copyright ⓒ 2015 SERSC

impact on different layers of TCP/IP. Different simulation scenarios were designed and the result on the performance of a network when under attack was analyzed. The results signify a detrimental impact of such attacks on the legitimate client base of a particular victim under attack. However, DDoS defensive techniques like rate limiting, throttling and IP trace back are some of the most significant countermeasures to combat these attacks. Thus, if the countermeasures are not taken at appropriate moment, DDoS attacks can pose a serious threat to the existing network systems, which can lead to high data and economic losses.

References

[1] E. Alomari, B. B Gupta, S. Karupayyah, S. Manickam and R. Alfaris, "Botnet based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art", International Journal of Computer Applications, vol. 49, no. 7, (**2012**) July, pp. 24-32.
[2] A. Tyagi and G. Aghilla, "A Wide Scale Survey on Botnet", International Journal of Computer Applications, vol. 34, no. 9, (**2011**) November, pp. 10-23.
[3] Incapsula, Specific DDoS Attack types, available at http://www.incapsula.com/ddos/ddos-attacks/
[4] A. Mittal, A. K. Shrivastava and M. Manoria, "A Review of DDOS Attack and its Countermeasures in TCP Based Networks", International Journal of Computer Science & Engineering Survey (IJCSES), vol. 2, no. 4, (**2011**) November, pp. 177-187.
[5] K. Arora, K. Kumar and M. Sachdeva, "Impact Analysis of Recent DDoS Attacks", International Journal on Computer Science and Engineering, vol. 3, no. 2, (**2011**) February, pp. 877-844.
[6] S. Hariri, G. Qu, T. Dharmagadda, M. Ramkishore, S. Cauligi and Raghvendra, "Impact Analysis of Faults and Attacks in Large Scale Networks", IEEE Security and Privacy, IEEE Computer Society, vol. 1, no. 5, (**2003**) September– October, pp. 49-54.
[7] R. K. C. Chang, "Defending Against Flooding based Distributed Denial of Service Attacks: A Tutorial, IEEE Communications Magazine, vol. 40, no. 10, (**2002**) October, pp. 42-51.
[8] D. Dittrich, N. Long and S. Dietrich, "Analyzing Distributed Denial of Service Tools: The Shaft Case", Available at: https://www.usenix.org/legacy/event/lisa2000/full_papers/dietrich/dietrich_html/
[9] S. M. Specht and R. B. Lee, "Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures", Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems, International Workshop on Security in Parallel and Distributed Systems, (**2004**) September, pp. 543-550.
[10] S. A. Arunmozhi and Y. Venkataramani, "DDoS Attack and Defense Scheme in Wireless Ad hoc Networks", International Journal of Network Security & Its Applications, vol. 3, no. 3, (**2011**) May, pp. 182-187.
[11] V. Sekar, Z. M. Mao, O. Spatscheck, J. V. der Merwe and R. Vasudevan, "Analyzing Large DDoS Attacks using Multiple Data Sources", SIGCOMM Workshops, Pisa, Italy (**2006**) September, Available at: https://web.eecs.umich.edu/~zmao/Papers/spoof.pdf
[12] Vern Paxson. An analysis of using reflectors for using distributed denial of service attacks. ACM SIGCOMM Computer Communication Review, Vol. 31(3), pp. 38-47 (July 2001).

Authors

Raghav Vadehra, (BTech) he received the Bachelor's degree in Electronics and Communication Engineering, in 2013. He worked as Associate System Engineer in Tata Consultancy Services Limited for one year. Currently, he is a student of MTech in Electronics and Communication Department at Guru Nanak Dev University, Regional Campus, Jalandhar (INDIA). His research area of interest is network security.

Nitika Chowdhary, (BTech, MTech) she received the masters's degree in computer science and engineering, in 2013 and the bachelor's degree in information technology, in 2011 from Punjab Technical University, India. She is currently working as Assistant Professor in Computer Science and Engineering Department at Guru Nanak Dev University

 Copyright ⓒ 2015 SERSC

Regional Campus Jalandhar. Her research interests include security, distributed networks, and cloud computing.

Jyoteesh Malhotra, (BTech, MTech, PhD) is involved in teaching and research in Electronics and Communication Department at Guru Nanak Dev University Regional Campus Jalandhar, India. His research area of interest includes statistical modeling of fading channels, Fading mitigation techniques in wireless communication, wireless networks, and wireless BAN. Dr. Malhotra has more than 100 research publication and authored two books. He is a life member of ISTE and editorial board member of many international journal of repute.

Copyright ⓒ 2015 SERSC

Copyright ⓒ 2015 SERSC