DDoS Attack's Simulation using Legitimate and Attack Real Data Sets

Jaswinder Singh, Krishan Kumar, Monika Sachdeva, Navjot Sidhu

Abstract— In this day and age, the internet is the new resource tool for the masses. It has changed the way we live in society and the way people interact with each other. There are about nine hundred million people, who are using internet now a day. They can use the internet to communicate with each other from all over the world, business can do their work over the internet, and students can take online classes and many more. Therefore, the availability of internet is very critical for the socio economic growth of the society. Distributed Denial of Service (DDoS) is one of the major threats for the current Internet because of its ability to create a huge volume of malicious data. As a result of it services of internet are severely degraded. One of the biggest challenges before researchers is to find the details of such attacks because due to damaging reputation issues, most of the commercial sites do not even disclose that they were blitzed by such attacks. In this project work, we have used the real time attack and legitimate traces in order to perform the simulation of DDoS attacks. We have simulated the network topology and attach the real time traces with the topology. The impact of attack is measured in terms of metrics such as throughput and percentage link utilization.

Index Terms— Internet, Distributed Denial of Service Attack, throughput, percentage link utilization, network, simulation, attack traffic, legitimate traffic

1 INTRODUCTION

INTERNET security includes aspects such as confidentiality, authentication, integrity and non repudiation, availability. Traditional security solutions concentrate on protecting the network connection's confidentiality and integrity, protecting the server from break-in, and protecting the client's private information from unintended disclosure. A lot of protocols and mechanisms have been developed that address these issues individually [1]. One area that has been neglected so far is service availability in the presence of denial of service (DoS) attacks, and their distributed variants (DDoS).

The network needs security against attackers and hackers. Network Security includes two basic securities. The first is the security of data information i.e. to protect the information from unauthorized access and loss. And the second is computer security i.e. to protect data and to thwart hackers. Here network security not only means security in a single network rather in any network or network of networks. Now need of network security has broken into two needs. One is the need of information security and other is the need of computer security. On internet or any network of an organization, thousands of important information is exchanged daily. This information can be misused by attackers.

The current architecture of Internet carries many security holes in it, which creates opportunities for attacker to launch a successful attack. Before going through the detail about DDoS
attacks, it is useful to have a classification over internet attacks. As per [2], definition of an attack can be a series of steps taken by an attacker to achieve an unauthorized result. An attacker uses a tool to exploit a vulnerability to perform an action on a target in order to achieve an unauthorized result.

One of the major security problems in the current Internet, a denial-of-service (DoS) attack always attempts to stop the victim from serving legitimate users. Denial-of-service (DoS) and distributed-denial-of-service (DDoS) attacks cause a serious danger to Internet operation. A distributed denial-of-service (DDoS) attack is a DoS attack which relies on multiple compromised hosts in the network to attack the victim [3]. There are two types of DDoS attacks. The first type of DDoS attacks aim of attacking the victim to force it not to serve legitimate users by exploiting software and protocol vulnerabilities. The second type of DDoS attack is based on a massive volume of attack traffic, which is known as a flooding-based DDoS attack. A flooding-based DDoS attack attempts to congest the victim's network bandwidth with real-looking but unwanted data. As a result, legitimate packets cannot reach the victim due to a lack of bandwidth resource.

2 DOS AND DDOS

DoS and DDoS attacks are simple in design and generated without requiring any special skill or resource. The attack tools can be obtained easily online and the attack goal is attained by generating sufficiently large amount of malicious traffic. The main difference between DoS and DDoS attacks is amount of attack traffic used. DoS attacks use one attack machine to generate malicious traffic while

- *Jaswinder Singh is currently pursuing Masters of Technology degree in Computer Science & Engineering from Punjab Technical University, Jalandhar, Punjab, India. E-mail: sidhujangirana @ gmail.com*
- *Krishan Kumar is currently an Associate Professor at PIT (Kapurthala), Punjab, India. E-mail:k.salujapitk@gmail.com*
- *Monika Sachdeva is currently an Assistant Professor at SBSCET (Ferozepur), Punjab, India. E-mail:monika.sal@rediffmail.com*
- *Navjot Sidhu is currently an Assistant Professor at Central University of Punjab (Bathinda), Punjab, India. E-mail: navjotsidhu8@gmail.com*

DDoS attacks use large numbers of attack machines [4].

2.1 Denial of Service Attack

Denial-of-Service (DoS) attacks generally achieve their goal by sending large volumes of malicious packets that exhaust some key resources available and prevent the legitimate clients to take service from the victim. DoS attacks are also called *bandwidth attacks* as they occupy a significant proportion of the available bandwidth. The aim of a bandwidth attack is to consume critical resources in a network service. Possible target resources may include CPU capacity in a server, or Internet link capacity. By exhausting these critical resources, the attacker can prevent legitimate users from accessing the service.

2.2 Distributed Denial of Service Attack

Distributed denial-of-service (DDoS) attacks are simply denial-of-service attacks performed from multiple agents. All machines simultaneously start generating as many packets as they can toward the victim. A large number of participating agents overload resources of the victim.

A typical DDoS attack contains two stages. Before real attack traffic reaches the victim, the attacker must cooperate with all its DDoS agents. Therefore, there must be control channels between the agents and the attacker. This cooperation requires all agents send traffic based on commands received from the attacker. So the first stage is to compromise defenceless systems that are available in the Internet and install attack tools in these compromised systems. This is known as turning the computers into "zombies" [5]. In the second stage, the attacker sends an *attack command* to the "zombies" through a secure channel to launch a bandwidth attack against the targeted victim.

Attackers can gain control of these computers via direct or indirect attacks. Direct attacks refer to sending malicious data packets that exploit a vulnerable computer. On the other hand, indirect attacks can exploit insecure actions that may be performed by users. These attacks generally require human interaction.

3 Related Work

Jelena Mirkovic, P. Reiher [8] proposed taxonomy of distributed denial-of-service attacks. The attack taxonomy is illustrated using both known and potential attack mechanisms. Vrizlynn L. L. Thing, Morris Sloman, and Naranker Dulay [9] present a detailed study of the source code of the popular DDoS attack bots, Agobot, SDBot, RBot and Spybot to provide an in-depth understanding of the attacks in order to facilitate the design of more effective and efficient detection and mitigation techniques. Tao Peng, Christopher Leckie, Kotagiri Ramamohanarao [5] presented a survey of denial of service attacks and the methods that had been proposed for defense against these attacks. In this survey, they analyzed the design decisions in the Internet that have created the potential for denial of service attacks. Monika Sachdeva, Gurvinder Singh, Krishan Kumar and Kuldip Singh [1] measured the DDoS attack's impact on web services. Authors simulated network topology and generated legitimate web traffic. The attack traffic is generated at different strengths to measure attack impact on web services. The attack impact is measured in terms of metrics such as throughput, response time, no of active connections, no of request dropouts, ratio of average serve to request rate, percentage link utilization, and normal packet survival ratio. Authors concentrated on web application so accordingly the performance metrics are identified for measuring the impact of DDoS attacks. Ketki Arora, Krishan Kumar, Monika Sachdeva [2] presented an overview on DDoS problem and major factors causing DDoS attacks. Authors discuss brief detail of most recent DDoS incidents on online organizations.

4 Experiment Setup

In order to perform the simulation of DDoS attacks, we have performed a number of experiments. To setup a satisfactory simulation for measuring DDoS impact, we should consider topology, legitimate traffic and attack traffic. The following subsection describes in more details about the test methodology and chosen performance metrics.

4.1 Environment Used

The cost of building a real distributed testing environment is very high. Simulation is an important method in network research, as simulation can be used to analyze network related problems under different protocols, cross traffic and topologies with much less cost [3]. The most well known network simulator is NS2 [20]. NS2 simulator covers a large number of applications, protocols, network types, network elements and traffic models. Therefore we use NS2 simulator for our work.

4.2 Simulation Methodology

In our simulation methodology, first step is to create a network topology using a NS2 Tcl script. Next step is to attach the legitimate traffic datasets in order to run legitimate traffic on nodes of the topology. After this, in order to generate attack traffic, real time attack traces are attached with our topology. These attack datasets are analyzed by CoralReef. Then simulation is again performed. Now whole of the traffic is monitored and off-line analysis is done. The output trace file is then used for measuring the attack.

Simulation topology used for this experiment have legitimate client pool contains various nodes that are used to generate legitimate traffic. In order to generate legitimate traffic real time traces are used. Using these traces the nodes generate TCP traffic. An attacker uses UDP traffic to launch an attack. The purpose of attack is to consume the bandwidth of the bottleneck link so that legitimate traffic could not send the packets. The simulation time is 50 seconds. The

legitimate traffic is based on TCP so it goes through slow start phase. The total number of legitimate clients, in legitimate client pool, is 8. The total traffic load and bottleneck bandwidth represent the scenario of a busy link.

In our experiments legitimate traffic is generated using real time traces [18]. The legitimate traffic is based on TCP. Here we have considered 8 legitimate clients that want to communicate with TCP Sink node. Again for generating DDoS attack real time datasets are used [22]. The volume and complexity of traffic in datasets is very high and very difficult to understand. The traces used for generating attack are stored in pcap format. So we have chosen CoralReef to perform the analysis of pcap traces. CoralReef is a de facto standard tool to analyze network traces.

After analyzing the traces we came to know that all UDP packets in the traces are attack traffic. 130 hosts send the UDP packets to a single host, which is the scenario of DDoS attacks. In simulation, attack traffic from all attackers' starts at 20 second and stops at 40 second.

4.3 Performance Metrics

Common performance metrics to measure the impact of DDoS attacks, used by various researchers are throughput without attack and with attack. Some others use the percentage of failed transactions as a metric in their work. According to [1] various network performance metrics are affected when DDoS attacks are launched. In current work, our focus is on performing the simulation of DDoS attack using real legitimate and attack datasets and then measure the effect of attack using following metrics:

1. Throughput (t): Throughput is defined as rate of sending and receiving the data by a network. It is a good measure of the channel capacity of the communication links in the internet. When attack is launched, legitimate and attack traffic, both use the bottleneck link. So throughput is defined as number of bits of legitimate traffic received at the destination per second.
2. Percentage Link Utilization (p): Percentage link utilization is defined as percentage of bandwidth that is being used for good put.

5 Result Analysis

All the experiments are conducted in simulated environment and the impact of DDoS attack using real time traces is measured using a number of parameters. The effect of DDoS attack on the performance of web services using all parameters is analysed below.

5.1 Throughput

During DDoS attack, attack traffic fills the bottleneck link in order to force the legitimate packets to drop. Throughput is defined as the number of bits per second of legitimate traffic that are received at the destination. As shown in fig. 1, at time 0 the throughput starts increasing slowly due to slow start phase of TCP. Once it reaches near to bandwidth of bottleneck link, it remains stable there when there is no attack. When attack is launched at 20 sec, it declines immediately. As the attack rate is high during attack throughput reaches to zero.

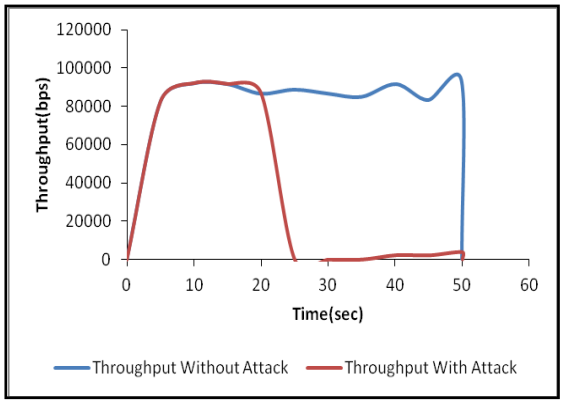

Fig.1: Throughput with and without attack

5.2 Percentage Link Utilization

Percentage Link utilization is defined as percentage of bandwidth that is being used for Throughput. As shown in fig.2 percentage of link utilization is near to 100% when there is no attack. When attack is launched the percentage reaches to zero due to impact of attack.

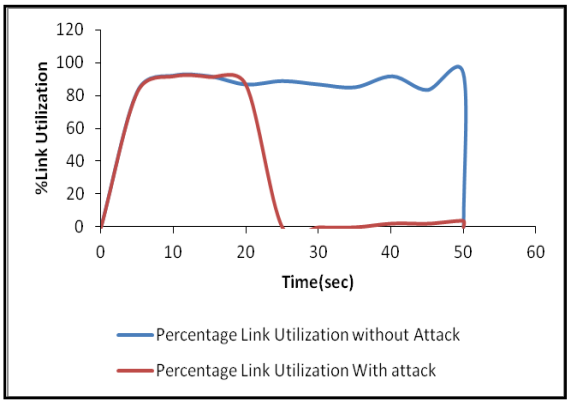

Fig.2: Percenage Link Utilization with and without attack

6 Conclusion

There is an alarming increase in the number of DDoS attack

incidents. Not only, DDoS incidents are growing day by day but the technique to attack, botnet size, and attack traffic are also attaining new heights. Effective defense measures needed to prevent and mitigate these attacks is the current need of the hour.

In order to complete this work, we concentrated on DDoS Attacks and identify different types of DDoS attacks. As objective of this work is to perform the simulation of DDoS attacks on legitimate and attack real datasets. So we have concentrated on the different datasets and perform the analysis of various datasets. After performing the analysis we have chosen the dataset that can generate a large amount of attack traffic. At the end measurement of degradation of services is done in terms of Goodput and Percentage link utilization.

REFERENCES

[1] Monika Sachdeva, Gurvinder Singh, Krishan Kumar and Kuldip Singh, "Measuring Impact of DDOS Attacks on Web Services", *Journal of Information Assurance and Security 5*, p.p 392-400, January 2010.

[2] Ketki Arora, Krishan Kumar, Monika Sachdeva, "Impact Analysis of Recent DDoS Attacks", *International Journal on Computer Science and Engineering (IJCSE),* Vol.3, No.2, p.p. 877-884, Feb. 2011.

[3] Yonghua You, "A Defense Framework for Flooding-based DDoS Attacks", Master's Thesis, Queen's University Kingston, Ontario, Canada August 2007.

[4] J. Mirkovic. D-WARD: Source-End Defense Against Distributed Denial-of-service Attacks, Ph.D. Thesis, University of California, Los Angeles, 2003.

[5] Tao Peng, Christopher Leckie, Kotagiri Ramamohanarao, "Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems", *ACM Computing Surveys*, Vol. 39, No. 1, Article 3, April 2007.

[6] Gary C. Kessler, "Defenses Against Distributed Denial of Service Attacks", Available at: "*http://www.garykessler.net/library/ddos.html*".

[7] Christos Douligeris and Aikaterini Mitrokotsa, "DDoS attacks and defense mechanisms: a classification", *Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology (ISSPIT 2003),* p.p 190-193, 14-17 Dec. 2003.

[8] J. Mirkovic and P. Reiher. "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms", *ACM SIGCOMM Computer Communications Review*, Volume 34, Issue 2, pp. 39-53, April, 2004.

[9] Vrizlynn L. L. Thing, Morris Sloman, and Naranker Dulay, "A Survey of Bots Used for Distributed Denial of Service Attacks", *IFIP International Federation for Information Processing*, Volume 232, New Approaches for Security, Privacy and Trust in Complex Environments, eds. Venter, H., Eloff, M., Labuschagne, L., Eloff, J., von Solms, R., (Boston: Springer), pp. 229-240, 2007.

[10] Monika Sachdeva, Gurvinder Singh, Krishan Kumar, and Kuldip Singh, "DDoS Incidents and their Impact: A Review", *The International Arab Journal of Information Technology*, Vol. 7, No. 1, January 2010.

[11] CERT Coordination Center, "Trends in Denial of Service Attack Technology", Available at: *http://www.cert.org/archive/pdf/DoS_trends.pdf*, October 2001.

[12] DDoS History In Brief, Available at: "*http://www.anml.iu.edu/ddos/history.html*".

[13] Dr. James H. Yu and Tom K. Le, "Internet and Network Security", *Journal of Industrial Technology,* Volume 17, Number 1, January 2001.

[14] J. Mirkovic, S. Dietrich, D. Dittrich and P. Reiher, *Internet Denial of Service*, Prentice Hall, December 2004.

[15] P. Owezarski, "On the impact of DoS attacks on Internet traffic characteristics and QoS", *14th IEEE International Conference and Computer Communications and Networks (ICCCN'2005)*, San Diego, CA, USA, 17-19 October 2005.

[16] Charalampos Patrikakis, Michalis Masikos, and Olga Zouraraki, "Distributed Denial of Service Attacks", *The Internet Protocol Journal,* Vol.7, No. 4, 2004.

[17] CERT Coordination Center, "Denial of service attacks", Available at: *http://www.cert.org/techtips/denial of service.html*, March 2007.

[18] UCLA CSD Packet Traces. Available at: "*http://fmg-www.cs.ucla.edu/ddos/traces/*", [last accessed July, 2011].

[19] David Moore, Ken Keys, Ryan Koga, Edouard Lagache and k claffy, "The CoralReef software suite as a tool for system and network administrators", *Proceedings of the 15th Systems Administration Conference (LISA-2001)*, 2001.

[20] NS Documentation. Available at: "*http://www.isi.edu/nsnam/ns*", [last accessed July, 2011].

[21] CoralReef Documentation, Available at: "*http://www.caida.org/tools/measurement/coralreef/doc"* [last accessed October, 2011].

[22] CAIDA Datasets, Available at: "http://www.caida.org/data/passive/ddos-20070804_dataset.xml".

[23] Navjot Sidhu, Krishan Kumar, Sukhwinder Singh, Monika Sachdeva and Jaswinder Singh, "Measuring DDOS Attack's impact on web services using real time traces" , *Proceedings of International Conference on Computer Engineering & Technology (ICCET'10)*, p.p. G-174-179, 2010.

Jaswinder Singh has done B.Tech. Computer Science & Engineering from Punjab Technical University Jalandhar, Punjab, India in year 2006. He is pursuing M.Tech. Computer Science & Engineering from Punjab Technical University, Jalandhar, Punjab, India. His research interests include Distributed Denial-of-Service and Design and analysis of algorithms.

Dr. Krishan Kumar has done B.Tech. Computer Science and Engineering from National Institute of Technology NIT, Hamirpur in 1995. He finished his MS Software Systems from BITS Pilani in 2001. In Feb. 2008, he finished his Ph. D. from Department of Electronics & Computer Engineering at Indian Institute of Technology, Roorkee. Currently, he is an Associate Professor at PIT Punjab Technical University, Jalandhar, Punjab, India. His general research Interests are in the areas of Information Security and Computer Networks. Specific research interests include Intrusion Detection, Protection from Internet Attacks, Web performance and Network architecture/protocols.

Monika Sachdeva has done B.Tech. Computer Science and Engineering from National Institute of Technology NIT, Jalandhar in 1997. She finished her MS software systems from BITS Pilani in 2002. Currently she is an Assisitant Professor at SBS College of Engineering & Technology, Ferozepur, Punjab, India. Her research interests include Web Services, Distributed Denial-of-Service, and Design and Analysis of algorithms.

Navjot Sidhu has done B.Tech. Computer Science & Engineering from Punjab Technical University, Jalandhar, Punjab, India in year 2007. She finished her M.Tech. Computer Engineering from Punjabi University Patiala, Punjab, India. She is currently working as an Assistant Professor at Central University of Punjab (Bathinda), India. Her research interests include Web Services and Distributed Denial-of-Service, Computer Networks and Databases.