International Journal of Engineering, Management, Humanities and Social Sciences Paradigms (IJEMHS)
Volume 30, Issue 02, Quarter 02 (April to June 2018)
An Indexed and Referred Journal with Impact Factor: 2.75
ISSN (online): 2347-601x
www.ijemhs.com

To Study DoS Attacks in Wireless Networks

Chanchal Maan[1], Dr. Ajay Kumar Dagar[2] and Ajay Kumar[3]

[1]M. Tech. Scholar, WCTM, Gurgaon, Haryana (India)
maanchanchal@gmail.com
[2]Associate Professor, WCTM, Gurgaon, Haryana (India)
ajaydagarwctm@gmail.com
[3]Assistant Professor, WCTM, Gurgaon, Haryana (India)
ajaykd64@yahoo.com

Publishing Date: May 10, 2018

Abstract

From some Past years, the speed and unwavering quality of communication over wireless network has been expanded seriously. One area of awesome enthusiasm for distributed system is wireless network that permits coordinated effort in real time. Wireless networks empower client to convey and transfer data with each other with no wired medium between them. Denials of Service attacks are real risk in wireless systems. This paper gives a study of these attacks.

Keywords: *Wireless Networks, Security and Privacy, Denial of Service Attack.*

1. Introduction

In beginning Internet was intended for receptiveness. In any case, it has poor security. On the Internet, anybody can send bundles to anybody without being confirmed. Because of which attackers can make a phony character. All systems associated with the Internet are plausible targets for attacks since the transparency of the Internet makes them available to assault movement. Point of A Denial of Service (DoS) assault is to stop the service gave by a target. The targets can be assaulted in light of the fact that they are associated with general society Internet. In Distributed Denial of Service (DDoS) assault, activity of a DoS assault originates from various sources. By utilizing multiple assault sources, the energy of a DDoS assault is opened up and the issue of safeguard turns out to be more muddled. This paper gives a review of DOS ATTACK and how to limit it.

2. Wireless Networks

Wireless networks are picking up popularity to its crest today on the grounds that each client needs wireless connectivity. Wireless Networks encourage clients to convey and exchange data with each other with no wired medium between them. One reason of the notoriety of these networks is generally entrance of wireless devices. Wireless applications and devices essentially accentuate on Wireless Local Area Networks (WLANs).

The task method of such network is remain solitary, or might be appended with one or multiple points to give web and connectivity to cellular networks.

These networks show the same traditional issues of wireless communications i.e. battery control, bandwidth constraints, improvement of transmission quality and coverage issues.

3. Background and Problem Statement

The Internet: Firstly the Internet was made in 1969 as a research network supported by the Advanced Research Projects Agency (ARPA) of the Department of Defense (DoD) in the United States of America. The point was to give an open network to researchers to share their research assets. Henceforth, receptiveness and improvement of the network were the plan needs while security issues to a lesser extent a worry. The frequency of the Morris Worm in 1988 denoted the primary real PC security on the Internet. Be that as it may, the world was very little subject to the Internet as it is presently. The Internet was restricted to research and instructive groups until the late 1990s. Henceforth, very little mindfulness was paid to Internet security.

In the most recent decade, development and accomplishment of the Internet is changing its customary part. The Internet isn't only a device for the researchers. Presently, it has turned into the principle framework of the worldwide information society. Web is utilized by government to give information to the nationals and the world and they will increasingly utilize the Internet to give taxpayer supported organizations. Organizations' trade and offer information with their divisions, clients, accomplices and provider effectively. Research and instructive establishments depend more on the Internet as a medium for spreading their research revelations quickly. Tragically, with the expanding client of the Internet, the assaults to the Internet have likewise expanded quickly.

All the more vitally, customary tasks in fundamental administrations, for example, control, solution, saving money, transportation, and defense are in effect dynamically supplanted by less expensive. Web based assaults can be propelled anyplace on the planet, and lamentably no Internet based administrations are shielded from these assaults. Subsequently, the security and unwavering quality of the Internet benefits on-line organizations, as well as an issue for national security.

4. Basic Concepts

Here we introduce some basic concepts on which this paper is based.

4.1 Source, Router and Victim

A **source** is a device that can generate Internet traffic. Source can be a company's web server, university's mail server or a home PC connected to the Internet. Source becomes an attack source when it is used to generate attack traffic.

We define a third party as a device that is used by an attacker to generate attack traffic without notice. A **victim** is defined as a system that provides an Internet service and whose service is disrupted during an attack.

A **target** is defined as a system that will be attacked by an attacker. If target's services are damaged during an attack, then the target becomes a victim. The victim could be a regional DNS server a government's web server or an ISP's router. Depending on actual network conditions, a connected device could be a victim or source or both.
The **end host** is defined as a device that connects to the end of the Internet.

The term **edge router** is referring to the router that provides access to the Internet for the sub-network that we are defending. We define a user's upstream routers as the routers that connect the user to Internet. Given two routers A and B, if A is B's upstream router, then B will be A's downstream router. These definitions are illustrated in Fig. 1.

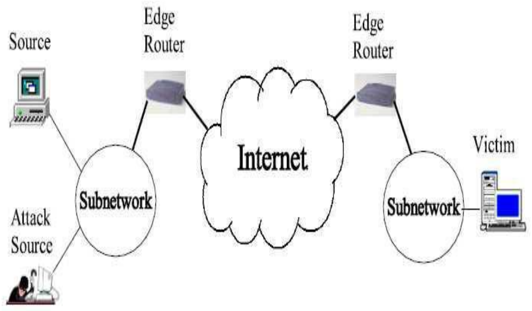

Figure 1: A simple model of the Internet

4.2 Definition of Attacks

In general, a denial of service (DoS) attack is any attack which makes an on-line service (e.g., Web Service) unavailable. We define a bandwidth attack as which consumes a target's resources through a huge traffic volume.

The distributed denial of service (DDoS) attack is a bandwidth attack whose attack traffic comes from various sources. For launching a DDoS attack, firstly an attacker usually compromises many insecure computers connected to Internet. Later a DDoS attack is launched from these in secured computers.

The reflector attack is an attack where third-parties (reflectors) are used to bounce attack traffic from the attacker to the target. A reflector can be any network device for eg., a web server and router. The attacker can make the attack traffic highly distributed by using many reflectors. The reflector attack is a type of DDoS attack.

Relation between different types of attacks is illustrated in Figure 2.

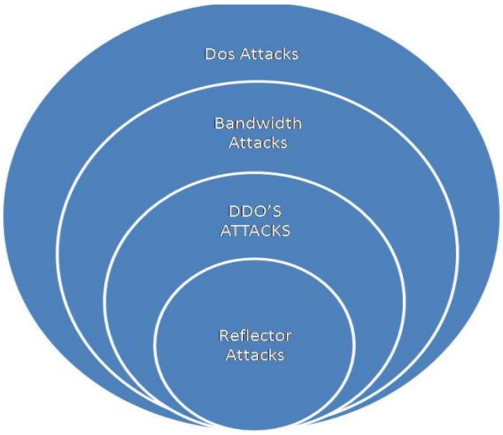

Figure 2: Relation of different types of attacks

4.3 DOS Attack

In a mobile network, reliability and security is one of the major concerns. In this work we are dealing one of the specific security attack called DOS (Denial of Service). In this attack some internal node of the network perform the flooding or transfer huge amount of data over the network, so that the communication over a node, node pair or the network get slow. This situation is called delay of service.

Denial of service (DoS) attack is a security problem. In this, the attacker's plan is to make the service provided by the victim unavailable to authorized users rather than obtain unauthorized access.

DoS attacks have two types: In first type of this attack has the aim of disrupting the services provided by the victim by exploiting a software vulnerability of the system. Form e.g.”ping-of-death" attack sends a packet with an illegal payload (i.e., more than 64K bytes), which causes some operating systems to lock up due to overflow. The second type of is known as a bandwidth attack based on the volume of traffic. Bandwidth attacks became a major security concern after massive bandwidth attacks paralyzed many high profile web sites, such as yahoo and CNN causing substantial financial loss in February 2000

.

Aim of bandwidth attack is to disable the services provided by the victim by sending a too much volume of useless traffic.

4.3.1 DDOS Attack

It is a bandwidth attack whose attack traffic comes from multiple sources.

DDoS the challenging attack, gains success to stop the victim from helping the legitimate users. There are two types of DDoS attacks

(1) First type deals with the idea of attacking the system by exploiting its protocol vulnerabilities

(2) Second type concentrates on the attack traffic which is known as Flooding-based DDoS attack.

4.3.1.1 Flooding Based DDoS Attacks

Flooding-based DDoS attack sends a huge volume of unwanted traffic to the victim, thus resulting in the consumption of a massive amount of network resources.

Flooding based DDoS attacks has two types:

(1) Direct and (2) Reflector attack

(1) In the Direct attack, the attacker sends the UDP, ICMP, TCP and many other packets directly to the victim. Direct attacks involve three mechanisms: UDP data flooding, ICMP echo flooding and TCP SYN flooding.

Now, in all DDoS attacks, a process known as IP spoofing is consider which helps to hide the real address of the attacker.

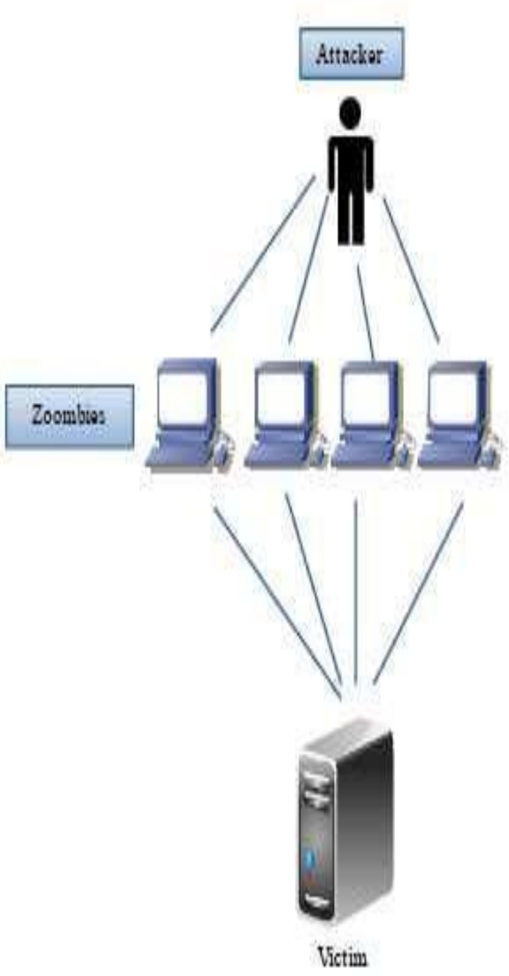

Figure 3: Direct Flooding Attacks

(2) In the Reflector attack, the response packets from the Reflector, the victim. A Reflector is a indirect attack in which intermediary nodes is known as reflector. A reflector is a host returning a packet if it receives a request packet.Victim does not need to send the response packets back to the Reflectors.

Reflector attacks depend on the protocol features in the victim. The protocol sends a reply message to the victim will be used for the Reflector attack.

To bear Flooding based attacks- one must increase the resources and bandwidth of the network.

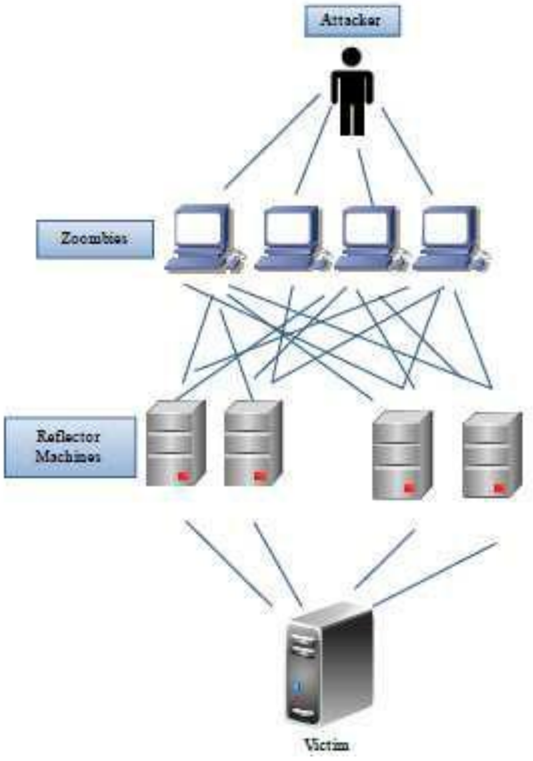

Figure 4: Indirect Flooding Attacks

4.4 DDOS Classification

The DDoS attacks can also be classified as follow:

1) **Network Device Level:** DDOS attacks at the Network Device Level lay more stress to exhaust the hardware resources of network devices or try to take the advantage of loopholes in the software. For example a possible attack on a router can be buffer over run error in password checking routines by typing extremely long passwords which can cause a router to crash.

2) OS Level: These types of attacks take advantage of the pitfalls left behind by the operating system while implementing the protocols. Common example is ICMP echo requests also called Ping of Death having total data size grater then the IP packet size which can cause certain operating systems to freeze, crash or reboot due to buffer overflow.

3) Application level: The attacks at application level bring down either a service or sometimes the whole system by taking advantage of certain flaws of network applications that are running on the system or by using such applications to withdraw the resources from the system. Most common examples of such attacks are:

- HTTP flood attacks
- Mail bombs
- DNS based Attacks

4) Data Flooding: In these types of attacks the attacker transmits the large amount of data to exhaust the recourses of the system or the device. Three categories of this type of attack are:

• Amplification attacks: Smurf attack and Fraggle attack

• Oscillation attacks,
• Simple flooding.

5) Protocol level: DDOS may take benefit of certain standard protocol features for example several attacks exploit the fact that IP source addresses can be spoofed. The different types of protocol level attacks are

• TCP SYN flood where the attacker requests for multiple TCP session initiation, but does not finalize the TCP handshake after the responding by server to the request. Thus these half open TCP sessions consume more memory of victim.

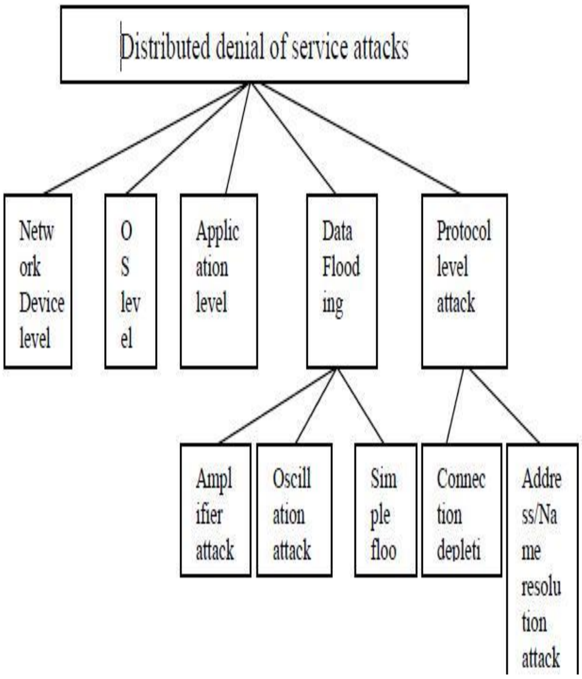

Figure 5: DDOS classification

5. Minimization of DOS Attack

In a mobile network, reliability and security is one of the real concerns. In this work we are giving one of the particular security attack called DOS (Denial of Service). In this attack some internal node of the network exchanges tremendous measure of data over the network, with the goal that the correspondence over the network gets moderate. This circumstance is called delay of service. Dos attack can be limit by applying the confinement over the bandwidth to limit the activity over the affected node. As the activity will be controlled at the source, the entire correspondence will goes typical.

6. Conclusion

In this paper, we considered one of the significant security threats in the Internet denial of service (DOS attack) and gave a full survey of DoS attacks and their countermeasures.

We dissected different distinctive attacks, built up a more down to earth arrangement technique for DoS attacks. Significance of Mobile networks can't be prevented as the world from securing figuring is getting versatile and minimized. Dissimilar to wired networks, mobile networks represent various difficulties to security arrangements because of their wireless shared medium, unusual topology, heterogeneous assets and stringent asset limitations and so on. The Security research area is as yet open the same number of the arrangements is composed keeping a restricted size situation and constrained sort of attacks and vulnerabilities.

As the communication will be performed over a congestion free path, the energy and the delay over the network will be decreased. The displayed approaches are powerful regarding energy and the time and additionally give a reliable route over the network. The got results demonstrate that the exhibited approach has enhanced the network dependability and the energy.

References

[1] J. A. Rochlis and M. W. Eichin "With microscope and tweezers: The worm from MIT's perspective" Communications of the ACM 32(6), 689-698 (1989).

[2] G.Bhatti, R. Singh and P. Singh, "A look back at Issues in the layers of TCP/IP Model," International Journal of Enhanced Research in Management & Computer Applications, Vol. 1, Issue 2, November2012.

[3] L. Garber. "Denial-of-service attacks rip the Internet". IEEE Computer 33(4),12-17 (2000).

[4] D. J. Marchette Computer Intrusion Detection and Network Monitoring: A Statistical Viewpoint (Springer, 2001).

[5] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: Classification and state-of-the-art," Computer Networks: the Int. J. Computer and Telecommunications Networking, Vol. 44, No. 5, April 2004, pp. 643–666

[6] H. F. Lipson. "Tracking and tracing cyber-attacks: Technical challenges and global policy issues" Special Report CMU/SEI-2002-SR-009, CERT Coordination Center (2002).

[7] L. Garber. "Denial-of-service attacks rip the Internet". IEEE Computer 33(4),12-17 (2000).