ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

A Relative Study for Detection and Prevention of DDoS Attacks

Ms. Anjusree.S[1] Mrs. V.Praveena[2]

PG Scholar, Department of CSE, Dr N.G.P Institute of Technology, Coimbatore, India [1]

Associate Professor, Department of CSE, Dr N.G.P Institute of Technology, Coimbatore, India [2]

ABSTRACT: Wireless Mobile Adhoc Network (MANET) which is an emerging technology that have a great potency to be applied in commercial applications and battlefields. MANET is infrastructure less and each node contains routing capability with no centralized control. Each device in a MANET is independent to move and it can alter its connections frequently. So the major challenge in MANET is security, because it does not have a centralized control. Adhoc network also contains sensor network, so it also faces the problem faced by sensor networks. There are many security attacks in MANET and DDoS (Distributed denial of service) is one among them. Our main aim is to view the effect of DDoS.

Keywords: Security, Denial of Service, Challenges, DDoS attack.

I. INTRODUCTION

MANET is a collection of two or more devices or nodes and it has the capability to operate interactively and wireless communications which make them interact with each other without the need of centralized control. It is an independent system in which nodes are connected by wireless links and they can send data to each other. As it does not have a centralized system so the routing decision can be made by the node itself. There is lack of security due to its mobility and self routing capability. A ddos attack is a negotiated large scale attack. In this paper we are focussing on some of the detection and prevention techniques of ddos attacks. DDoS attacks are a throng of cooperated systems that will attack a single target thus causing denial-of-service for the users at directed system. The incoming messages floods the directed system thereby it refutes the services to legitimate users.

II. DDOS ATTACK

A. DOS AND DDOS ATTACKS

Denial-of-Service attack is an attempt that makes the network resource and machine unavailable to the intended users [3]. The attacks occur when the services is blocked by another user intentionally. This type of attack doesn't cause any damage to the data but it does not provide the required resource [2].DDoS attack is a mass of compromised systems, which attacks a single target that causes denial-of –service for the users in targeted system. As shown in Figure 1, DDoS attacks consist of following components:

a. Real Attacker
b. Master hosts or handlers are capable of handling Multiple agents.
c. Zombie hosts that generate packets.
d. Target host or Victim. [2].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

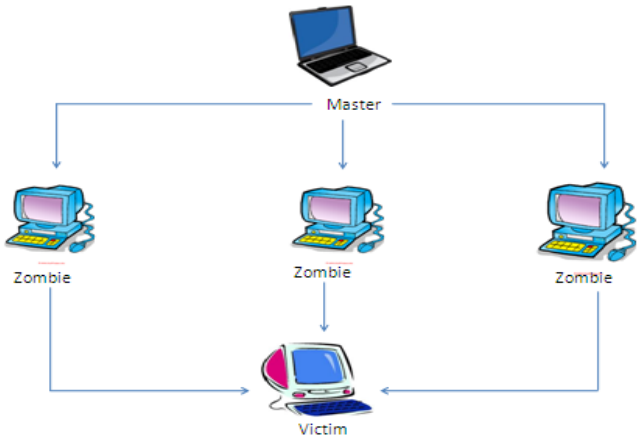

Figure 1: DDoS attack [2]

B. TYPES OF DDOS ATTACKS

DDoS attacks can be extensively classified in to three classes:

a. Volume Based Attacks: It mainly includes ICMP floods, UDP floods, spoofed packet floods. The attack's aim is to soak the bandwidth of site which is attacked [4].
b. Protocol Attacks: It mainly includes ping of death, SYN floods, smurf DDoS, fragmented packet attacks and more. This attack consumes the resource of actual server [4].
c. Application Layer Attacks**:** It includes Zero-day DDoS attacks; Slowloris.The goal of this attack is to crash the web server [4].

The following are the major DDoS attacks:

- *UDP Flood*: This attack mainly submerges random ports with UDP packets on a remote host, it causes to check for application listening at the port and it replies with an ICMP Destination Unreachable packet and ultimately it leads to inaccessibility [4].

- *Ping Flood*: It has the similar principle to that of UDP Flood attack, it defeats the target resource with ping packets and it sends packets as fast as possible without the expectancy of replies. It can consume both incoming and outgoing bandwidth [4].

- *SYN Flood*: It is a form of DoS attack in which the attacker sends SYN requests to the destination to consume the resources and it make the system passive to rightful user [4].

- *Ping of Death*: It is a type of attack in which the attacker sends some deformed or spiteful pings to the computer. It floods the prey with ping traffic which is a type of DoS attack. The size of the ping is normally 56bytes. In some cases buffer overflow occurs which cause the system smash [4].

- *Slowloris:* This attack is dangerous especially to tomcat and dhttpd.It s attack which enables on server to take another server, but it does not affect ports and services on the target network. This attack consumes all the available connections on web server and it does not allow other clients to reach sites on web server [4].

- *Zero-day DDoS:* It is a new attack which utilizes previously unknown vulnerabilities. This attack are used and shared by the users before the target developer knows about the vulnerability [5].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

III.LITERATURE SURVEY

In [1] the author introduced the intrusion detection system and gives a survey about different DoS/DDoS attacks. The author had observed that CUSUM-based detection technique. An IDS is a software or hardware that are used to identify unauthorized traffic that are against the policy of the network [6].IDS can be classified as serving component either for network-based or host-based or combination of both. In a network- based IDS network traffic is monitored whereas in host-based IDS operating system log files and application are monitored. The host-based is located in a single host and the network-based is located on a machine that is separated from the host.

Network-based IDS,it can be usually used to detect attacks such as DoS attacks,worms,botnets,scans and other type of attacks[6].Network IDS can be categorised in to two types based on detection: anomaly-based detection and signature-based detection. Signature-based attack is used for comparing widely-known attack signatures or patterns from traffic monitored. If there is any match, it produces an alarm for the eventual attack [7].Anomaly-based IDS are also known as behaviour-based in which it compares the network traffic with previous normal network traffic. If any deviation occurs gives the warning of attack. The normal traffic can be classified in to two: trained and standard. The standard is based on standard protocols. The trained traffic can be used to determine the threshold value that can be used for future detection.Anamoly-based detection system mainly consists of three phases: parameterization, training and detection [8].The system parameters are defined in parameterization phase. The normal behaviour of traffic is defined in training phase. In detection phase, the traffic behaviour is compared with training phase. If the result of the comparison exceeds the threshold value, an alarm is caused.

The experimental analysis of the author concluded that Cumulative Sum is one of the detection algorithms that perform well as compared to other techniques less memory resources and computation. It perform better than other techniques because it is non-parametric, it does not require training and is robust towards attack profile variations.

In[9] ,the author had mainly concentrated on two types of DDoS attacks: Malicious Packet Dropping based DDoS attack and Flooding Based DDoS attack[10].The aim of Malicious Packet Dropping based DDoS attack is to assault the victim in order to drop some packets or all packets that are ready for forwarding when no congestion occurs. The Flooding Based DDoS attack is based on large volume of attack traffic and it attempts to crowd the victim's network bandwidth with unwanted data. As a result the required data cannot reach the victim due to lack of bandwidth resource. In this paper the author compared these two attacks and proposed a technique called Disable IP Broadcast technique.

This paper describes some detection techniques for different types of DDoS attacks:

- *Packet Dropping Attack*: In this attack, it make some nodes malicious and this malicious nodes drops some or all packets that are ready for forwarding when there is no occurrence of congestion. Unconditional Packet Dropping technique is used to detect the Packet Dropping Attack in which they examine the Forward Percentage (FP) [11].

$$FPm = \frac{\text{Packets actually forwarded}}{\text{Packets to be send}}$$

- *Flooding Attack*: The Flooding Based DDoS attack is based on large volume of attack traffic and it attempts to crowd the victim's network bandwidth with unwanted data. As a result the required data cannot reach the victim due to lack of bandwidth resource. Malicious Flooding on Specific Target is the technique used to monitor the number of requests in a period of time to the destination. If it is more than the threshold value, then the attack is malicious flooding.

This paper introduces some prevention technique for Flooding based DDoS attack. According to [12, 13, 14], DDoS defence mechanism is classified in to two categories: local and global. Local solutions can be implemented on victim node without from an outsider's cooperation. Global solutions require cooperation from subnets of internets.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

The local solution mainly includes:

- Local Filtering: In this method, the packet is filtered at the local router and then detects it.
- Changing IPs: In this method, victim's IP address is changed.
- Creating Client Bottlenecks: The objective is to limit the attacking capability by creating a bottleneck in Zombie computers.

The global solution mainly includes:

- Improving the security of entire internet: Improve the security of all computers connected to internet.
- Using Globally Coordinated Filters: This is mainly used to prevent the mass attacking of packets at a time.
- Tracing the Source IP Address: The main goal is to find the attackers path and find the right attacker and take rightful actions.

The proposed prevention technique used in this paper is Disabling IP Broadcasts. A broadcast is defined as a data packet that is fated for multiple hosts. This broadcast occurs in both network and data-link layer. The data-link broadcast can be given to all hosts in a physical network and the network broadcasts can be given to all hosts in a logical network.TCP is used to support these broadcasts. In this approach all broadcast address is set to all ones, so that all hosts can receive the broadcasts and broadcast address is set to a specific number in the portion of network and setting all ones on the broadcast portion to receive the broadcasts. This paper explains that by setting broadcast address to some specific network number and some subnet number, so that all the hosts on subnet can receive the broadcast.

The main advantage of proposed scheme in this paper is that it requires only limited modifications to existing ones. It does not have extra expense. It is efficient in its established routes, complexity of computation and reservation of resources.

In [15], author proposed an Intrusion prevention system against DDoS attacks, and the network becomes more secure and it can detect malicious node and behavior through Intrusion prevention system (IPS).In this paper author proposed a scheme in Manet's security issues which is related to routing protocols. This work is done through network simulator-2 and it is used to measure the network performance. This paper applies Intrusion Prevention system so that network can become totally secure from attack and it can also detect malicious node and activity through IPS and it can detect via Intrusion Detection System. This scheme can also be used for detecting DoS.

In[16],this paper present a method for determining Intrusion or any misbehave that occurs in MANET by using IDS and it protect the network from DDoS and it analyze the result on the basis of packet delivery ratio, routing load and IDS time. Effective IDS is not only used for prevention but also strengthens the intrusion prevention measures. In this paper it proposes a new defense mechanism and it contains a Flow Monitoring Table (FMT) for mobile node. The table contains sender id, receiver id, protocol type, transport info, event time, node coordinate axis and application layer info. Based on these parameters DDoS, network and IDS case is analysed.In this, first is creation of profile which is normal. Second module describes the attack module in which an attacker node is created to send unwanted packet to the neighboring node. The third module is Intrusion Detection System, it checks the normal and abnormal behavior of the network based on parameters. In this paper NS-2 is used to analyze TCP at normal time and DDoS time, IDS case, routing load, packet delivery ratio and analysis of packet sends and receives. The simulation results conclude that the IDS 99.9% recoverable.

In [17], the paper investigates some mechanisms against DDoS attacks. It mainly uses the IP address spoofing to disguise the flow of attack. This paper is a scheme which is based on firewall in which it can distinguish packets and filter the attack packets before it reaches the victim. This scheme has low implement cost compared to another mechanism. This scheme allows firewall to arrange itself so that attack can be easily detected.IP address spoofing is used in DDoS attacks which is to hide the identity of the source address.

This paper explains that a good protection towards DDoS can be done by continuous overseeing. The attack packets should be stopped before it overwhelms the victim, so that service to the legitimate user is not denied. The cost of implementation should be low.IP spoofing is used in DoS/DDoS attacks to hide the location of source. This spoofing is also used in reflector attacks [18].The author says if the spoofed packets are distinguished easily, then those packets can

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

be filtered by firewall to avoid attacks. This paper explains about packet marking method which helps to identify the DDoS attack packets from those sent from legitimate users. This method is mainly used to record path information. It explains that if there is any increase in packet size, a method is put all information in a fixed space, so the router keeps all IP address in that space and if the space contains the same number, it then calculates the exclusive-or of the previous value and it places the new value. So this says that marking does not affect the length when the packet travels through the network.

In this paper the header in an IP packet is used as marking field.PPM [19] scheme is used for marking. In this paper, the scheme explains that the packet which travels through the router will insert a mark on the ID field, so that the generated marking of two packets will be distinct. This paper says that the attackers can spoof the marking of the packet if the router's hash function is known. So in order to avoid the spoofing of marking each router maintains a 16-bit key while marking is computed. To detect the beginning of DDoS attack a counter is used called total-Mismatches-Counter (TMC) which is used to count the number packets that cannot be matched by firewall. This paper proposes a new method called MDADF which is a low cost and efficient method against DDoS attacks. This method mainly consists of two processes: marking and filtering processes. It also includes mechanism to report and detect DDoS in a timely manner.

In [20], the author proposed a new method to detect DDoS attacks using ant-based framework which make use of tasteful and stateless signatures and it conserves only rightful packets and it avoids infected packets. This paper proposes this framework that can be employed in all existing networks and it can be used to prevent forged messages from spreading across the network. It makes use of pre-authentication filters to identify messages which are not genuine. The main contributions of this paper are: less computational load, energy wastage is less and it saves the lifetime of network, and it neglects the false warning. The proposed system is using heterogeneous system which has more battery and processing power compared to other nodes. The framework mainly includes DDoS detecting ants (DDA), filtering, Traffic Monitoring Ants (TFA) which can be applied to stateless and stateful signatures.DDA is used to identify DDoS attacks. Filtering is mainly used to identify false attacks and to perform appropriate actions.

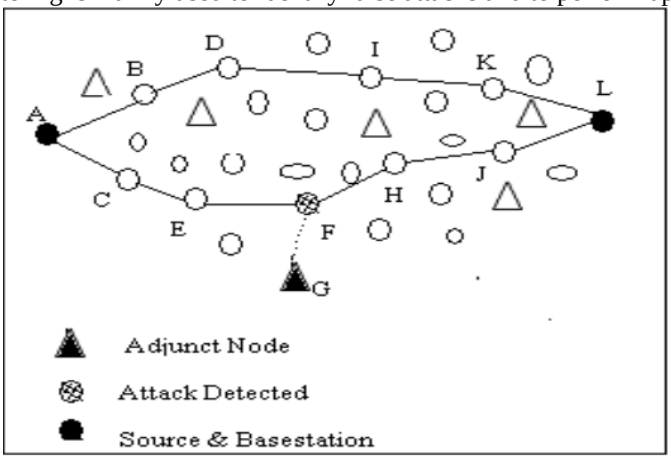

Fig 2: High level view of proposed work [20]

DDA is used to collect information about the network state. These ants have genuine properties such as distributed problem, vigorous and decentralized approach. It can tackle with any network changes and can also communicate with any other ants.

Filtering module is used to filter malicious traffic by using pattern matching. The author concluded that by using stateful and stateless approaches, it can consider only those packets present in these approaches and packets can be dropped. This approach can also track the source of the attack without using any specific trace back technique.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

IV. CONCLUSION

In this paper, we have done a comparative study for detecting and preventing DDoS attacks. There are different methods based on intrusion prevention scheme and filtration scheme. Different techniques can be used to prevent the DDoS attacks in which some modified technique is described in other papers. On the basis of our study we have concluded that for detecting this attack will require less cost, complexity, and wastage of energy is less. It is one of the serious attacks in wireless and wired infrastructures and it can be controlled to some extent and research work is in progression to cast away the attack. These surveys inspect some possible solutions and also furnish some classifications and analyze the possibility of the techniques.

REFERENCES

[1] Mohammed Alenezi, Martin J Reed," Methodologies for detecting DoS/DDoS attacks against network servers", ICSNC : The Seventh International Conference on Systems and Networks Communications,2012.

[2] Dhwani Garg," DDOS Mitigation Techniques-A Survey", International Journal of Advances in Computer Networks and its Security.

[3] http://en.wikipedia.org/wiki/Denial-of-service_attack.

[4] http://www.incapsula.com/ddos/ddos-attacks.

[5] http://en.wikipedia.org/wiki/Zero-day_attack.

[6] T. M. Wu, "Intrusion Detection Systems ", Information Assurance Technology Analysis Centre (IATAC), September 2009.

[7] F. Dressler, G. Munz, G. Carle, "Attack detection using cooperating autonomous detection system(CATS),"Wilhelm-Schickard Institute of Computer Science, Computer Networks and Internet, 2004.

[8] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Macia-Fernandez, E. Vazquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," computers &security, vol.28, pp. 18-28, 2009.

[9] Mukesh Kumar, Naresh Kumar," Detection and Prevention of DDoS Attack in manet's using Disable IP Broadcast Technique", International Journal of Application or Innovation in Engineering & Management, Volume 2, Issue 7, July 2013.

[10] Vasilios A. Siris et al, "Provider-based deterministic packet marking against distributed DoS attacks," Journal of Network and Computer Applications, Volume 30, Issue 3,, pp. 858-876, August 2007.

[11] Yi-an Huang et al, "A Cooperative Intrusion Detection System for Ad Hoc Networks," In Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03), Fairfax VA, October 2003.

[12] S. Kannan, T. Maragatham, S. Karthi , V.P. Arunachalam," A Study of Attacks, Attack Detection and Prevention Methods in Proactive and Reactive Routing Protocols", International Business Management, 2011.

[13] Hwee-Xian Tan, Winston K. G. Seah," Framework for Statistical Filtering Against DDOS Attacks in MANETs", Proceedings of the Second IEEE International Conference on Embedded Software and Systems; 2005.

[14] Xianjun Geng, Andrew B. Whinston," Defeating Distributed Denial of Service Attacks", February, 2000.

[15] Sitesh Kumar Sinha, Dr. R.K. Singh, Krishna kumar Pandey, Mukesh Kumar Sahu," Distributed Denial of Service attack Prevention using Critical Link Method in MANET", International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE)Volume 2, Issue 3, March 2013.

[16] Ramratan Ahirwal, Leeladhar Mahour," Analysis of DDoS Attack Effect and Protection Scheme in Wireless Mobile Ad-hoc Network", International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 06 June 2012.

[17] Yao Chen, Shantanu Das, Pulak Dhar, Abdulmotaleb El Saddik, Amiya Nayak," Detecting and Preventing IP-spoofed Distributed DoS Attacks", International Journal of Network Security, Vol.7, No.1, PP .70–81, July 2008.

[18] Y. Chen," A Novel Marking-based Detection and Fil-tering Scheme against Distributed Denial of Service Attack", Master's Thesis, University of Ottawa, 2006.

[19] S. Savage, D. Wetherall, A. Karlin, and T. Ander-son, "Practical network support for IP traceback,", in Proceedings of ACM SIGCOMM'00, Aug. 2000.

[20] Dimple Juneja, Neha Arora," An Ant Based Framework for Preventing DDoS Attack in Wireless Sensor Networks", International Journal of Advancements in Technology- ISSN 0976-4860, Vol 1, No 1 (June 2010) © IJoAT.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

BIOGRAPHY

Ms. Anjusree.S

She received her B.E degree in Information Technology from Nandha College of Technology in 2012.She is currently with the Post graduate in Dr N.G.P Institute of Technology and now works on the project in Network Security.

Mrs. V.Praveena

She received her B.E. degree in Computer Science and Engineering from Maharaja Engineering College under Bharathiyar University in 2002. She completed her M.E in Computer Science and Engineering from Karpagam University in 2011. She is pursuing her Ph.D. in Anna University Chennai. She has 11 years of Teaching Experience. Her area of interest is Network Security.