A Review: Denial of Service Attack MANET

Mamta Jha[1] Rajesh Singh[2] S.S. Dhakad[3]
[1,2,3]Department of Computer Science & Engineering
[1,2,3]NITM Gwalior, India

Abstract— MANET is an emerging method and have high strength to be applied in the serious conditions like commercial applications and battlefields such as traffic surveillance, building, MANET is organization less, with no any central supervisor exist and also all node hold routing capability, Every device in the MANET is independently free to move in every direction, and will therefore modification its connections to other devices frequently. Denial of Service (DoS) and Distributed DoS (DDoS) attacks are two of the most harmful threats to the network functionality. Many of the protection methods established in a fixed wired network are no applicable to this novl in a mobile environment. How to thwart the Denial of Service attacks differently effectively and save the vital secure-sensitive ad hoc networks obtainable for its intended use are needed. The DOS (denial of service), DDoS (Distributed denial-of-service) attacks are a rapidly rising problem. The multitude and variation of both the attacks and the defense approaches is overwhelming. These attacks lead to the degradation or the prevention of legitimate use of network resources. In this paper kind of attacks are presented which are attacked on an ad-hoc network. The motive of the study is aware about different service availability attacks and its effects on network operation.

Key words: denial of service, Distributed denial-of-service, MANET

I. INTRODUCTION

MANET is a self-configuring network of the mobile devices that attached by links. All devices in the MANET are able to move independently in different route, and will therefore vary its links to other devices frequently. All must be onward traffic unconnected to its specific use, and therefore be a router. The main issue in creating a MANET is preparing all devices to the constantly keep up the knowledge required for the correctly route traffic. Such that network may operate by themselves or may be connected to the superior Internet. There are commonly two kinds of ad hoc routing protocols, proactive and reactive routing protocols. The main motive of this paper centers on reactive routing protocols which establish routes between the communicating nodes when wanted applying a route detection procedure including Route Requests and Route Replies, a procedure which can be simply misused for the denial-of-service attacks. The kind of security attack in MANET is denial of service attack (DoS).

A DoS attack is an attempt to prevent legitimate users of a service or network resource from accessing that service or resource. A Distributed Denial-Of-Service (DDoS) attack is a distributed, large-scale attempt by malicious users to flood the victim network with an enormous number of packets. This exhausts the victim network of resources such as bandwidth, computing power, etc. The victim is unable to provide services to its legitimate clients and network performance is greatly deteriorated. Networks are mainly vulnerable to the DOS attack launched through the compromised between intruders or nodes. The intruder broadcasts a mass Route Request packet. A lot of attacking Data packets to use the communication node and bandwidth resources so that the legal communication cannot be reserved. In this paper, we have analyzed two types of attacks namely flooding attack and black hole attack in detail. The resisting mechanisms over these attacks are proposed and the effectiveness of the proposed schemes is validated with simulations.[1]

Denial of service (DoS) attacks[2] are very common in the world of internet today. Increasing pace of such attacks has made servers and network devices on the internet at greater risk than ever before. Due to the same reason, organizations and people carrying large servers and data on the internet are now making greater plans and investments to be secure and defend themselves against a number of cyber-attacks including Denial of Service. The traditional architecture of World Wide Web is vulnerable to serious kinds of threats including DoS attacks. The attackers are now quicker in launching such attacks because they have sophisticated and automated DoS attack tools available which require minimal human effort. The attack aims to deny or degrade normal services for legitimate users by sending huge traffic to the victim (machines or networks) to exhaust services, connection capacity or the bandwidth. In a broader classification, types of DoS attacks can be mentioned as in figure 1. In figure 1, five types of DoS attacks are mentioned. In network device level attacks, the target is some hardware device on the network such as a router. The attack is launched by exploiting some software bug or hardware resource vulnerability. In Operating System (OS)level attacks, vulnerabilities of operating system in the victim machine are used to launch DoS attack. In application level attacks, bugs or vulnerabilities in the application are identified to exploit them for DoS attack. Port scanning for identifying open ports of a remote application is very common in this perspective. Such attacks are now getting more popular as they present the traffic to a network and its devices similar to the legitimate traffic. Therefore, in a scenario where most of other attacks are now identifiable, application level attacks offer more success rate to attackers. In data flood attacks, targets are the connection capacity of a remote host or the bandwidth of a network. Heavy traffic is generated by the attacker towards the victim to exhaust connectivity or bandwidth resources so that normal services are denied or degraded for requests of legitimate users. In protocol feature attacks, the weaknesses of some protocol features are used to exploit them for launching a DoS attack. For example, the source IP address of a data packet(which relates to Internet Protocol and is a part of TCP/IP stack) can be spoofed by an attacker to launch a DoS attack which can be harder to trace due to a fake address [2].

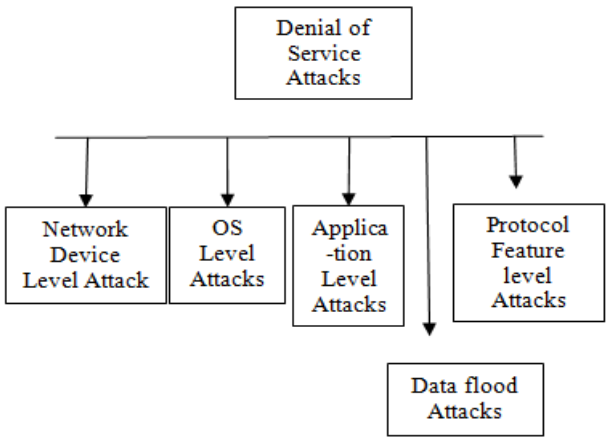

Fig. 1: DOS attack types in a broader classification.

II. VARIOUS ATTACKS IN MANET

A. *Exterior Attack:*

Exterior attacks are carried out by the nodes that do not go to the network. It causes congestion sends incorrect routing knowledge or may causes absence of the services.

B. *Interior Attack:*

Interior attacks are from nodes that are the portion of the network. The malicious node in an interior attack from network gains illegal access and the copies as a genuine node. It can be examine traffic between the an-other nodes and may be share in other network actions.

C. *DOS attack:*

This attack main goal to the attack accessibility of the node or whole network. If the attack is successful the facilities will not existing. The attacker commonly uses radio signal jamming and the battery exhaustion technique.

D. *Impersonation:*

If the verification machinery is not correctly implemented a hateful node can performance as a honest node and monitor the network traffic. It can also send bogus routing packets, and find access to the few confidential knowledge.

E. *Eavesdropping:*

This is the passive attack. The node basically detects the trusted knowledge. This knowledge can be later used by the malicious node. The secure knowledge like private key, password, location, public key ,etc. may be fetched by eavesdropper.

F. *Routing Attacks:*

The malicious node makes routing services a target because it's an significant facility in MANETs. There are two main flavors this routing attack. One is an attack on the routing protocol and another is attack on the delivery mechanism or packet forwarding. The first is goal at blocking the broadcast of routing knowledge to a node. The latter is goal at troubling the packet distribution against a predefined route.

G. *Black Hole Attack:*

In this attack, an attacker promotes a zero metric for totally destinations producing totally nodes around to route packets towards it. A malicious node sends bogus routing knowledge, claiming that it has an optimum route and causes other good nodes to route documents packets through malicious one.

H. *Wormhole Attack:*

In the wormhole attack, an attacker gets packets at single point in network, tunnels them to another point in network, and then replays them into network from that point. Routing may be disturbed when routing control the information are tunneled. This type of tunnel between the two colluding attacks is called as a wormhole.

I. *Replay Attack:*

An attacker that executes a replay attack are retransmitted the legal documents continually to inject the network routing traffic that has been captured previously. This attack commonly targets the freshness of routes, but can also be used to undermine poorly designed secure results.

J. *Man- In- The- Middle Attack:*

An attacker site between source and destination and sniffs any knowledge being sent between the two nodes. In few cases, attacker may be impersonating the source to communicate with the destination or impersonate the destination to response to the source.

K. *Gray-Hole Attack:*

This type of attack is also called as routing misbehavior attack which leads to reducing of messages. The Gray hole attack has two stages. In the first stage the node promote itself as having a lawful route to receiver while in second stage, nodes drops interrupted packets with a certain probability [3]

III. 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 [5]. 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 [4].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 2, DDoS attacks consist of following components:

- Real Attacker
- Master hosts or handlers are capable of handling Multiple agents.
- Zombie hosts that generate packets.
- Target host or Victim. [4].

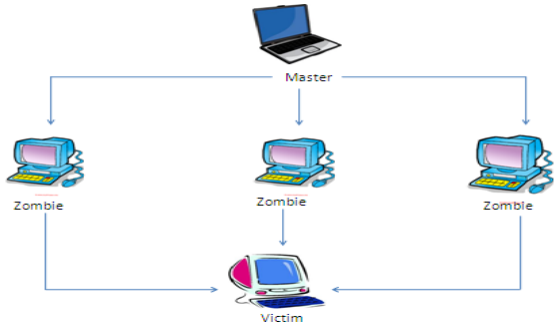

Fig. 2: DDoS attack

B. Types of DDOS Attacks:

DDoS attacks can be extensively classified into three classes:

- 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 [6].
- 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 [6].
- Application Layer Attacks**:** It includes Zero-day DDoS attacks; Slowloris.The goal of this attack is to crash the web server [6].

The following are the major DDoS attacks:

1) 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 [6].

2) 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 [6].

3) 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 [6].

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 [6].

5) 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 [6].

6) 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 [7].

IV. LITERATURE SURVEY

Rutvij H. Jhaveri[8] present the survey of a DoS (Denial-of-Service) attacks on the network layer namely Grayhole attack, Wormhole attack, Blackhole attack and which are the serious threats for MANETs. also discuss few suggested solutions to detect and prevent these attacks. MANETs have unique characteristics like, limited resources, dynamic topology, lack of centralized administration and wireless radio medium; as a result, they are not protected to the several kinds of the attacks in several layers of the protocol stack. All node in a MANET is proficient of acting as a router. Routing is one of the features having various security concerns.

Rajdeep Singh [9] discussed few attacks on the MANET and Distributed Denial-of-Service also provide the security against the DDOS attack. All device in the MANET is independently free to the move in any route, and therefore modification its connections to the other devices frequently. MANETs are a type of wireless ad hoc networks that commonly has a routable networking environment on the highest of a link layer ad hoc network. There are numerous secure attacks in MANET and Distributed denial of service (DDoS) is one of them.

In [10] 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 [11].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.

Hwee-Xian Tan [12] studies the vulnerability of MANETs to DDoS attacks and provide an overview of constant filtering, which is commonly used as a security mechanism against DDoS attacks in wired networks. Also propose a structure for statistical filtering in MANETs to combat DDoS attacks.

Mukesh Kumar [13] a technique is proposed that can prevent a specific kind of DDoS attack named flood attack which Disable IP Broadcast. MANET has no any clear line of defence so it is manageable to the both malicious attackers and legitimate network users. In the presence of hostile nodes, one of the central Tasks in MANET is to proposal the robust secure result that can prevent MANET from various Ddos attacks. Individual mechanisms have been proposed applying numers cryptographic methods to countermeasures these attacks against MANET.

Xiapu Luo et al [14] have presented the central problem of the identifying PDoS (pulsing denial of service) attacks which send a series of attack pulses to decrease TCP throughput. Wei-Shen Lai et al [15] have proposed a scheme to monitor the traffic pattern in order to alleviate distributed denial of service attacks. Shabana Mehfuz1 et al [16] have proposed a new secure power-aware ant routing algorithm (SPA-ARA) for mobile ad hoc networks that is inspired from ant colony optimization (ACO) algorithms such as swarm intelligent technique. Xiaoxin Wu et al [17] proposed a denial of service mitigation method that uses the digital signatures to authenticate legitimate packets, and drop packets that do not pass the confirmation Ping Yi, Zhoulin Dai, Shiyong Zhang and Yiping Zhong [18] have presented a new denial of the service attack and its defense in the ad hoc networks. The new denial of service attack, called AHFA (Ad Hoc Flooding Attack), can outcome in DOS when used against the on-demand routing protocols for the mobile ad hoc networks.

Buchegger and Boudec [19] propose that despite the fact that the networks only function properly if

participating nodes forwarding and conjoin in routing. However, it may be advantageous for individual nodes not to cooperate. They suggest a protocol, known as CONFIDANT, which goals at discovering and isolating mischievous nodes, thus making disobedience unattractive. Here misbehaving nodes are excluded from forwarding routes. It includes a trust manager to evaluate the level of trust of alert reports. But it is not clear how fast the trust level can be adjusted for compromised node especially if it has a high trust level initially [20].

Mukesh Kumar [21] a technique is proposed that can prevent a specific kind of DDoS attack named flood attack which Disable IP Broadcast. MANET has not clear line of the protection so it is accessible to the both malicious attackers and legitimate network users. In the presence of hostile nodes, one of the highest Tasks in MANET is to design the robust secure solution that can prevent MANET from various DDoS attacks. Separate mechanisms have been proposed applying several cryptographic methods to countermeasures these attacks against MANET.

A DoS attack defense strategy has been proposed by Liu and Shen [22]. In this scheme, every individual node is assigned the duty to supervise its neighbors. Each node arranges its buffer uniformly to every neighbor nodes. For example, if there are N neighbor nodes, every one of them will get 1/N buffer space. If any of them takes more buffer space than 1/N, succeeding packets will be dropped from it. In addition, each node assigns priorities to its neighbors based on the transmission rates. Specifically, if a neighbor node sends M packets per second, then its priority value is set as 1/M. A node handles the incoming packets according to the priority values of the senders.

B. B. Gupta[23]present a comprehensive study of the wide range of distributed denial of service attacks and defense approaches offered to combat them. Suggest an integrated solution for completely defending against the flooding distributed denial of service attacks at the ISP (Internet Service Provider) level. DDoS (Distributed denial of service) attacks on user machines, federation and framework of the Internet has become highly publicized incidents and call for instant solution. It is a complicated and the main issue is characterized by the explicit attempt of the attackers to the avoid access to resources by legitimate users for which they have approval. verious systems have been suggested on how to defend against these attacks, yet the difficult still wants a complete solution.

V. Conclusion

DDoS attack is one advanced method for attacking network system it prevent legitimate user from using network resources. Major contributions of this paper are a need of distributed defense mechanism and its evaluation. This paper described a comprehensive survey of causes of DDoS attack and its defense mechanism. According to this survey most of the defense approach had used rate limiting mechanism. DoS and DDoS can be done locally and remotely, and it is one of the most common types of security attacks, because it requires only regular and inexpensive resources, and does not require high technical knowledge. The frequency and sophistication of DoS and DDoS are rapidly increasing based on several techniques including direct attacks, remote controlled attacks, reflective attacks, worms, and viruses. The proposed security mechanism prevents smart object networks from remotely initiated DoS (and DDoS) network and transport layer attacks.

References

[1] Arunmozhi Annamalai, Venkataramani Yegnanarayanan," Secured System against DDoS Attack in Mobile Adhoc Network", Arunmozhi Annamalai, Venkataramani Yegnanarayanan E-ISSN:, Issue 9, Volume 11, September 2012,pp:331-341.
[2] L. Zhang, S. Yu, D. Wu, and P. Watters, "A Survey on Latest Botnet Attack and Defense," Proc. of 10th Intl' Conference On Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE, pp. 53 60, November 2011.
[3] Anurag Kumar, Akshay Kumar, Anubha Dhaka and Garima Chaudhary," INTRUSION DETECTION AGAINST DENIALOF SERVICE ATTACKS IN MANETENVIRONMENT", International Journal of Emerging Trends & Technology in Computer Science *(IJETTCS)*, Volume 2, Issue 4, July – August 2013,pp:145-152.
[4] Dhwani Garg," DDOS Mitigation Techniques-A Survey", International Journal of Advances in Computer Networks and its Security.
[5] http://en.wikipedia.org/wiki/Denial-of-service_attack.
[6] http://www.incapsula.com/ddos/ddos-attacks.
[7] http://en.wikipedia.org/wiki/Zero-day_attack.
[8] Rutvij H. Jhaveri, in Second International Conference on "Advanced Computing & Communication Technologies", 2012.
[9] Prajeet Sharma, Niresh Sharma, Rajdeep Singh International Journal of Computer Applications (0975 – 8887) Volume 41– No.21, March 2012.
[10] 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.
[11] T. M. Wu, "Intrusion Detection Systems ", Information Assurance Technology Analysis Centre (IATAC), September 2009.
[12] "Hwee-Xian Tan, Winston K. G. Seah" in "Second International Conference on Embedded Software and Systems" (ICESS'05).
[13] "Mukesh Kumar & Naresh Kumar" in "International Journal of Application or Innovation in Engineering & Management (IJAIEM) Volume 2, Issue 7, July 2013 ISSN 2319 – 4847.
[14] Xiapu Luo, Edmond W.W.Chan,Rocky K.C.Chang: Detecting Pulsing Denial-of-Service Attacks with Nondeterministic Attack Intervals, EURASIP Journal on Advances in Signal Processing (2009)
[15] Wei-Shen Lai, Chu-Hsing Lin , Jung-Chun Liu , Hsun-Chi Huang, Tsung-Che Yang: Using Adaptive Bandwidth Allocation Approach to Defend DDoS Attacks, International Journal of Software Engineering and Its Applications, Vol. 2, No. 4, pp. 61-72 (2008)
[16] Shabana Mehfuz, Doja,M.N.: Swarm Intelligent Power-Aware Detection of Unauthorized and

Compromised Nodes in MANETs‖, Journal of Artificial Evolution and Applications (2008)
[17] Xiaoxin Wu, David,K.Y.Yau, Mitigating Denial-of-Service Attacks in MANET by Distributed Packet Filtering: A Game-theoretic Approach, in Proceedings of the 2nd ACM symposium on Information, computer and communication security, pp 365-367 (2006)
[18] Security Scheme for Distributed DoS in Mobile Ad Hoc Networks, ACM, Newyork,USA (2004) Ping Yi, Zhoulin Dai, Shiyong Zhang, Yiping Zhong: A New Routing Attack in Mobile Ad Hoc Networks, International Journal of Information Technology, Vol. 11, No.2 (2005)
[19] S. Buchegger and J. Boudec, "Performance Analysis of the Confidant Protocol," Proc. Int'l Symp, Mobile Ad Hoc Networking and Computing, 2002.
[20] Y.Huang and W.Lee A cooperative IDS for adhoc network Security of adhoc and sensor networks ACM 2003,pp.135-145
[21] Mukesh Kumar & Naresh Kumar" in "International Journal of Application or Innovation in Engineering & Management (IJAIEM) Volume 2, Issue 7, July 2013 ISSN 2319 – 4847
[22] Y. Liu and L. Shen, "Defense of DoS Attack Focusing on Protecting Resource in Mobile Ad Hoc Networks," Computer Knowledge and Technology 2007 3(16), 2007.
[23] "B. B. Gupta, R. C. Joshi and Manoj Mishra" in Information Security Journal: A Global Perspective, 18:224–247, 2009.

