iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** IX **Month of publication:** September 2014

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

DDoS Services Attacks In Mobile Ad-hoc Network

Anju[#1], Vinod Saroha[*2]

[#] *M.Tech(NS),BPSMV Sonipat, Asstt. Prof. in BPSMV Sonipat*

Abstract--- In vision of the growing demand for wireless information and data services, it is very important to providing faster and reliable mobile access to users. Today's, not only mobile phones, but also laptops and PDAs are used by people in their professional and private lives. These devices are used separately for the most part that is their applications do not interact. Sometimes, a group of mobile devices form a unstructured, temporary network as they move towards each other. This allows users to share documents, secret information and other useful information. This kind of unstructured, temporary network referred to as mobile ad hoc networks sometimes just called ad hoc networks or multi-hop wireless networks, and are expected to play an important role in our daily lives in near future. As the use of ad-hoc network increased the security concerned also needed to prevent the network from malicious users. In wired network , it is easy to provided security during transmission than the Mobile ad-hoc network. DDoS attack is a big problem in MANET. In these, paper we discussed about DDoS attacks and there detection mechanisms.

Keywords--- DDoS, MANETs, UDP, TCP SYN, Routing Protocol, Attacks, Prevent, Detection, hop.

I. INTRODUCTION

MANET is a unstructured network that can be established with no fixed infrastructure. All its nodes act as routers and perform its detection and maintenance of paths to other nodes in the. Its routing protocol has to be able to deal with the new challenges i.e nodes mobility, limited bandwidth and limited power supply , security maintenance, quality of services,. These challenges set new demands on MANET routing protocols.

Ad hoc networks have a large range of military and commercial applications. It is ideal in areas where establishing an infrastructure network is not possible or when the purpose of the network is transient.

Security in MANETs is hard to achieve due to spontaneous network and fully decentralized topology as well as the vulnerabilities and limitations of wireless data transmissions. Existing solutions that are applied in wired networks can be used to obtain a certain level of security. However, these solutions are not always be suitable to wireless networks. Therefore ad hoc networks have their own vulnerabilities that cannot be always tackled by these wired network security solutions. One of the distinct features of MANETs is that all nodes have to be performing in the routing process. Traditional routing protocols designed for wired networks cannot be useful in ad hoc networks. The major factor is that the wireless medium is less secure than wired network. The routing protocol provides the upper limit to security in any packet network. If routing can be misdirected, the entire network can be blocked.

ISSN: 2321-9653

This problem is enlarged in ad hoc networks. Another difficulty is that it is hard to decide compromised nodes from nodes that are affliction from broken links. Current wireless research states that MANET presents a larger security problem than conventional wired and wireless networks. DDoS attacks has also become large problem for users. A DDoS attack is a distributed, major attempt by malicious users to flood the victim network with huge number of packets. This exhausts the sufferer network of resources such as bandwidth, computing power, etc. The victim is incapable to provide services to its legal clients and network performance is greatly deteriorated.

II. BACKGROUND

There are two distinct approaches for enabling wireless communications between mobile hosts [1]. The one approach is to use a fixed network communications that provides wireless access points. In this network, a wireless host communicates with the network through an access point within its contact radius. When it goes out of range of one access point than connects with a new access point and starts communicating through it. An example is the cellular network infrastructure. A most important problem of this approach is handoff, which tries to handle the situation when a connection should be smoothly handed over from one access point to another access point without noticeable delay or packet loss. Another problem is based on a fixed infrastructure are limited to places.

The second approach is the wireless ad- hoc network with no fixed infrastructure. Laptops and PDAs that communicate directly with each other are examples of nodes in an ad hoc network. Each of the nodes has a wireless interface and communicates with others over either radio or infrared channels. some well-known ad hoc network applications are:

- Two-way Work
- Crisis-management Applications
- Personal Area Networking and Bluetooth

MANETs Characteristics and Challenges:

- Dynamic topologies
- Bandwidth-constrained, variable capacity links
- Energy-constrained operation.
- Security

*Security Attacks in MANETs:*The security attacks in MANETs are **A**ctive attacks and **P**assive attacks.***A**ctive **A**ttack* is an attack when disobedient node has to paid some energy costs in order to perform the threat and consider as malicious node . ***P**assive **A**ttacks* are mainly due to lack of support with the purpose of saving energy selfishly and considered as selfish.

Various types of attacks in MANETs are: **D**enial **o**f **S**ervice, **I**mpersonation,**M**odification, **F**abrication, **R**eplay, **E**avesdropping , **M**alicious **S**oftware and **L**ack **o**f **C**ooperation.

III. DISTRIBUTED DENIAL OF SERVICE (DDoS) ATTACK

*DoS Attack:*A denial of service attack is categorized by an unambiguous attempt by an attacker to prevent legal users of a service from using the required resources [3]. DoS attacks include:

- Flood a network
- Interrupt connections between two machines
- Prevent a particular individual from accessing a service
- Disorder service to a specific system or person.

DDoS Attack is a distributed, large-scale attempt by malicious users to flood the victim network with an huge

ISSN: 2321-9653

number of packets [4]. This exhausts the victim network of resources such as bandwidth, computing power, etc. The sufferer node is unable to provide services to its legal clients and network performance is very much deteriorated. The distributed format the many to one dimension. A distributed denial of service attack is consists of four elements, as shown in Figure 1.The following steps take place during a distributed attack:

- The real attacker sends an "execute" message to the control master program.
- The control master program receives the "execute" message and propagates the command to the attack daemons under its control.
- Upon receiving the attack command, the attack daemons begin the attack on the victim.

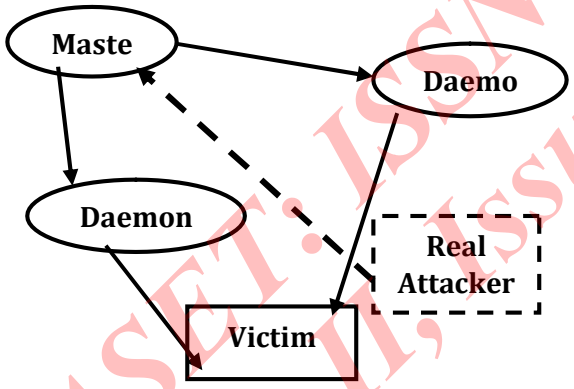


Figure 1: The four Components of DDoS Attacks**.**

Architecture of DDoS Attacks: The flooding traffic reaches the victim, the attacker must work together with all its agents. This communication is provided with the help of control channels between the agents and the attacker [5]. This teamwork requires all agents send traffic based on command signals received from the attacker. The network which consists of the attacker, agents, and control channels is called the attack networks. The attack networks are divided into three types:

- The agent-handle model
- The Internet Relay Chat (IRC)-based model
- The reflector model.

The agent-handler model consists of four components: attacker, handlers, and agents and victim [6]. Figure 2 shown the architecture of the model.

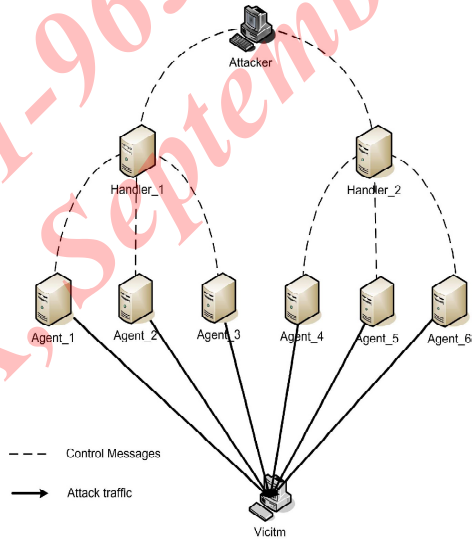


Figure 2: Typical architecture of a DDoS attack.

The IRC-based model is not that much unlike than the agent-handler model except that instead of communication between an attacker and agents based on handlers, an IRC communication channel is used to connect the attacker to agents [4].The reflector-based DDoS attack raises the bar for tracing out the real attacker by hiding the attacker behind a large number of reflectors.

DDoS Attack Taxonomy: DDoS attacks are divided into two basic classes:

ISSN: 2321-9653

- Bandwidth depletion attacks
- Resource depletion attacks.

Bandwidth Depletion Attacks is considered to flood the victim network with unnecessary traffic that prevents legal traffic from reaching the main victim. Example of bandwidth depletion attacks are:

- Flood attacks
- Amplification attacks.

Flood Attacks involves sending large volumes of traffic t victim system, to block the victim system's netw bandwidth with IP traffic. It have been done using b UDP and ICMP packets.

An *flood attack* occurs when the large volumes of ICMP_ECHO_REPLY packets and UDP " Destination unreachable" send to the victim system.

Amplification Attacks involves the attacker to send messages to a broadcast IP address, using this to cause all systems in the subnet reached by the broadcast address to send a reply to the victim system. The example of an amplification attack : *Smurf attack and Fraggle attack.*

Resource Depletion Attacks considered to tie up the resources of a victim system to prevent it from using that resources and unable to process legal requests for service. The example of resource depletion attack is: misusing the TCP SYN protocol, and the other misusing the PUSH+ACK protocol.

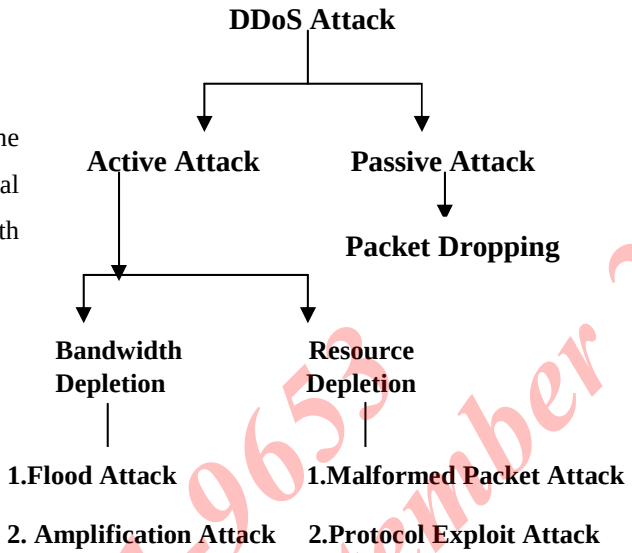


Figure 3: DDoS Attack Taxonomy

The Smurf attack: The attacker sends a huge amount of ICMP echo packets to the router at 128Kbps. The attacker modifies the packets by changing the source IP to the IP address of the victim's computer so replies to the echo packets will be sent to that address. The destination address of the packets is a broadcast address.. A same attack that uses UDP echo packets instead of ICMP echo packets is called a Fraggle attack.

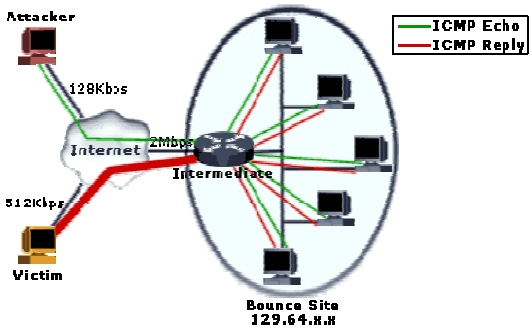


Figure 4: Smurf Attack in progress.

ISSN: 2321-9653

IV. DETECTION OF DDOS ATTACKS

It is important that a detection system identifies both the malicious node and attack types. Without them, it is hard to resolve how to respond significantly without interrupting normal communication. [9]. The basic idea is to find out the detailed attack information from a set of identification rules, which are pre-computed for known attacks.For each attack, the node that runs the corresponding detection rule the is called *monitoring node*, and the node whose behavior is being analyzed known as *monitored node*. Now, some notations of statistics (features) used in these rules are described. Here, K is used to represent the monitoring node and k the monitored node.

- $\#_{(*,\ k)}$: the number of incoming packets on the monitored node k.
- $\#_{(k,\ *)}$: the number of outgoing packets from the monitored node k.
- $\#_{([k],\ *)}$: the number of outgoing packets of which the monitored node k is the source.
- $\#_{(*,\ [k])}$: the number of incoming packets of which the monitored node k is the destination.
- $\#_{([s],\ k)}$: the number of incoming packets on k of which node s is the source.
- $\#_{(k,\ [d])}$: the number of outgoing packets from k of which node d is the destination.
- $\#_{(k,\ n)}$: the number of outgoing packets from k of which n is the next hop.
- $\#_{([s],\ K,\ k)}$: the number of packets that are originated from s and transmitted from K to k.
- $\#_{([s],\ K,\ [k])}$: the number of packets that are originated from s and transmitted from K to k, of which k is the final destination.
- $\#_{([s],\ [d])}$: the number of packets received on the monitored node (k) which is originated from s and destined to d.

These statistics are computed over sampling interval time T_s and over long period T. We always assume that time interval T is multiples of T_s.

Detection of Malicious Packet Dropping Based DDoS Attack:

Unconditional Packet Dropping: calculate the statistics Forward Percentage over time period T.

$$FP_k = \frac{\#^T_{(k,\ K)} - \#^T_{([k],\ K)}}{\#^T_{(K,\ k)} - \#^T_{(K,\ [k])}}$$

Random Packet Dropping: Calculate the same statistics FP as Unconditional Packet Dropping. If the denominator is not zero and FP_m is less than a chosen threshold ε_{FP} ($\varepsilon_{FP} < 1$) but not zero, the attack is detected as Random Packet Dropping and node k is identified as the attacker.

Selective Packet Dropping: Calculate the statistics Local Forward Percentage over a time period T for each source s.

$$LFP^s_m = \frac{\#^T_{([s],\ k,\ K)}}{\#^T_{([s],\ M,\ k)} - \#^T_{([s],\ K,\ [k])}}$$

If the denominator is not zero and the statistics is zero (unconditional dropping), the attack is unconditional Packet Dropping targeted at s. Likewise, if the LFP is less than ε_{LFP} ($\varepsilon_{LFP} < 1$), the attack is random Packet Dropping targeted at s. In either case, m is identified as the attacker.

V. CONCLUSIONS

This paper presents introduction to MANETs and DDoS attacks. We presented the security goals and challenges that the field of ad hoc networking faces. It also presents various security goals for MANETs and types of attacks in MANETs.

we have discussed two types of DDoS attacks and their attack mechanisms. These are: Malicious Packet Dropping Based DDoS attack and Flooding Based DDoS attack. Then, we have presented their detection mechanism which will help in detecting attacking node and attack type.

ACKNOWLEDGEMENT

I want to acknowledge my guide Mr.. Vinod Saroha (Asst. prof. In CSE&IT deptt., BPSMV,Sonipat) for his guidelines. I also want to thank my parent's for their support.

REFERENCES

[1] Schiller J; Mobile Communication; Second Edition, Pearson Edition.

[2] R. Duggirala; A Novel Route Maintenance Technique for Ad Hoc Routing Protocols; M.S. Thesis; University of Cincinnati; November 2000.

[3] Pfleeger C P, Pfleeger S L; Security in Computing; Third Edition, Pearson Edition.

[4] Stephen M. Specht and Ruby B. Lee; Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures; Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems, 2004 International Workshop on Security in Parallel and Distributed Systems, pp. 543-550; September 2004.

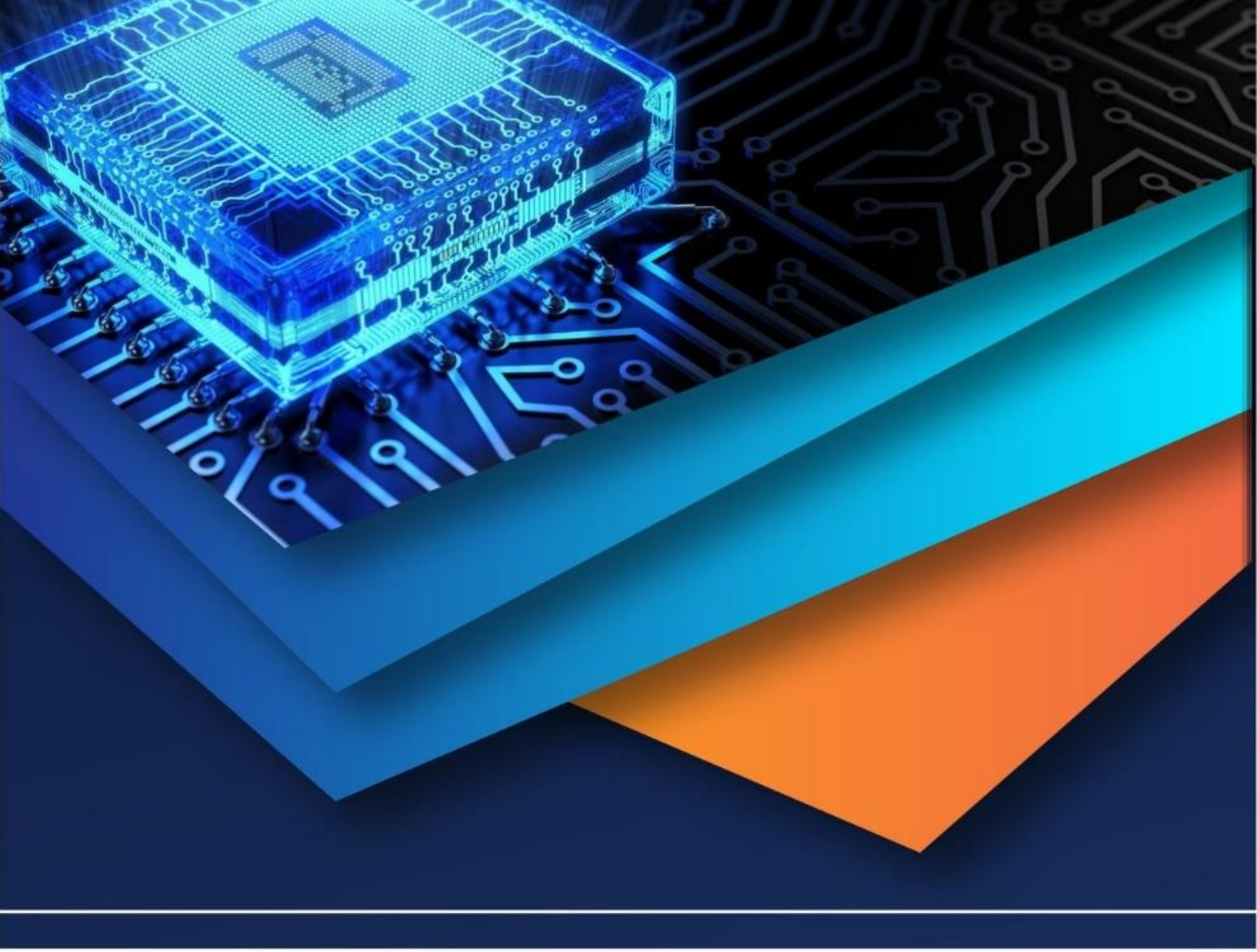
[5] J. MÄolsÄa; Mitigating denial of service attacks in computer networks; PhD thesis; Helsinki University of Technology, Espoo, Finland; June 2006.

[6] Yonghua You; A defense framework for flooding-based DDoS attacks; Master of Sc. Thesis; Queen's University Kingston, Ontario, Canada; August 2007.

[7] TFreak;smurf.c;www.phreak.org/archives/exploits/denial/smurf.c; May 6, 2003.

[8] Federal Computer Incident Response Center (FedCIRC); Defense Tactics for Distributed Denial of Service Attacks; Washington, DC; 2000.

[9] Yi-an Huang and Wenke Lee; A Cooperative Intrusion Detection System for Ad Hoc Networks; www.cc.gatech.edu/~wenke/papers/sasn.pdf.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY