International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 04 | Apr 2020 www.irjet.net p-ISSN: 2395-0072

Hybrid Approach for DDoS Protection in MANET

Yatish Patil[1], Niraj Palkar[2], Rehan Sayed[3], Prof. Ranjit Mane[4]

[1]302 SS Park, Raintree Road, Kharghar, Navi Mumbai -410210
[2]Kalwa, Thane-400605
[3]Belapur CBD, Navi Mumbai-410210
[4]Prof. Dept. of Computer Engineering, Bharti Vidyapeeth College of Engineering, Navi-Mumbai, Maharashtra, India.

Abstract - *The system is an advancement to ad-hoc wireless network & its security. A mobile ad-hoc network(MANET) faces a malicious activities cause, unlike any other network manet cannot support heavy security algorithms techniques and algorithms because of lack of power supply, less computing power, finite bandwidth, and dynamically changing topology of the connected devices in network . The proposed scheme is distributed in nature it has the capability to protect distributed dos (ddos) attack.*

***Key Words*: Ad-hoc Wireless Network, Manet, ddos, Topology, Security, etc**

1. INTRODUCTION

Mobile Ad hoc Networks (MANETs) normally consist of several nodes that are interconnected to form infrastructure-less networks. In MANETs, the communication between the nodes is coordinated by individual nodes without any infrastructure. Hence, MANET is regarded as having a fully decentralized topology . Nonetheless, compared to traditional wired and wireless networks, MANETs are exposed to security threats because of its elementary attributes like decentralized infrastructure, arbitrary topology, absence of association, and resource constraints [1].

1.1 What Exactly a MANET is?

In the MANET nodes simply configure together to form the network. In this type of network single hop and multi-hop type of communication is possible which forms a direct and indirect type of communication. When two or more nodes are in the range of each other they can directly communicate with each other through direct communication. In the mean while multi-hop type of communication is the one in which nodes can directly communicate through intermediate nodes.

To establish a connection that is a secure and efficient path from source to destination various types of routing protocols is used such as proactive, reactive and hybrid. Now in the reactive routing protocols, nodes gather the network information to establish a path to the destination. Also, in the proactive routing protocols, the source node uses the network predefined information to establish a path to the destination.

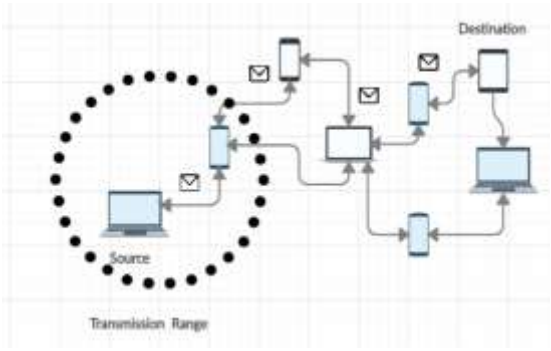

Fig -1: Mobile Ad hoc Networks (MANETs)

In hybrid routing protocol, source node gathers network information and it uses a predefined information for the path establishment to the destination node. One of the property of MANET is self-configuring its node, many malicious nodes may join the network which are responsible for various types of active and passive attacks. In the context of MANET, routing, security and QoS are the three major issues which can be resolved in future to make communication more efficient and reliable came into existence in the recent time. The routing protocols are broadly classified into reactive, proactive. Each node function as the source, sink, and router, in MANET. The packets are transferred to other nodes for communication. The nodes find optimal path for transferring packets for easy communication [2].

1.2 What Exactly DDOS is?

A Distributed Denial of Service (DDoS) attack is a type of malicious attack using distributed computing resources, coordinated attack on the availability of services of a host server (application server, storage ,database Server, or DNS server) or network resource, launched indirectly through many compromised systems called botnets on the Internet. DDoS attacks have been a major challenge to the researchers and big security issue to the environment. In the era of modern technology very sophisticated approaches are utilized, such as by assuming multiple targets on the resources, applications or network, hackers use multiple vectors and do not take any risk of missing their target machine/resources in a single attack campaign. The Distributed Denial of Service(DDoS) attacks can be volumetric, designed to disrupt a host service and make it

unapproachable, or attack application layers, targeting a specific service on the host. DDoS use of multiple botnet machines to amplify attacks could make it very challenging to stop it or to trace back the hackers [3].

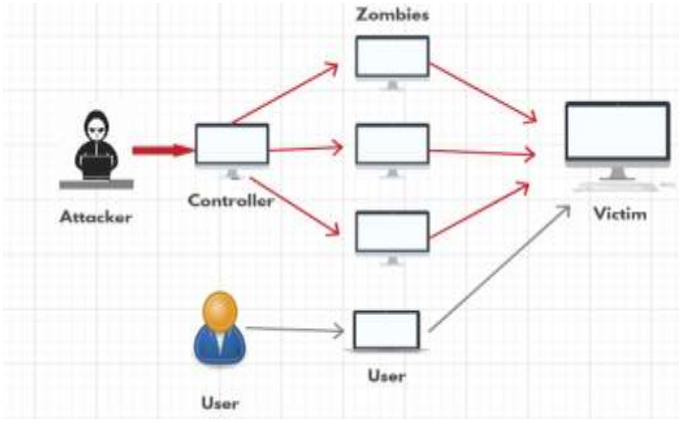

Fig -2: Typical DDOS Attack Organization

Following are the types of DDOS Attacks:

- **SYN Flood**- In Syn flood attack hackers exploit weaknesses in the TCP connection three-way handshake, which is the communication process between host ,client and the server.
- **UDP Flood**- UDP flood Attack aims to targets random ports on a computer or network with UDP packets. Then the host checks for the application listening at those ports, but no application is found.
- **Ping of Death**-Ping of Death Attack manipulates IP protocols by sending malicious pings to a system. This was a popular type of DDoS earlier but is less effective today.
- **ICMP Flood-**In ICMP Flood Attackers attack on the server with spoofed huge ICMP packets sent from a large set of source IPs and generate large amount of traffic on server.
- **Smurf Attack**- In smurf Attack attackers exploits IP and ICMP using a malware program called smurf. It spoofs an IP address and using ICMP, it pings IP addresses on a given network [4].

2. PROBLEM STATEMENT

In Current Era of Technology the attacks on Systems are very common, let it be a high-end computing device(s) or small personal device(s). This attacks leads to destruction of high amount of resources & usages of them preventing legitimate users to gain access to the system for which they are requesting.

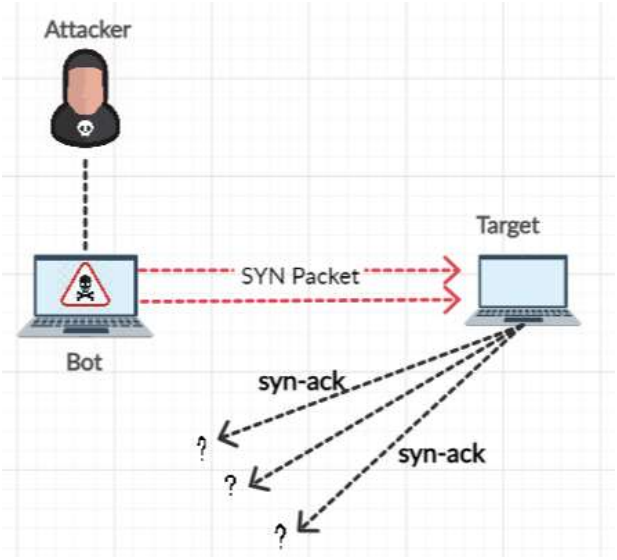

Fig-3: DDOS Attack

2.1 LITERATURE REVIEW

According to M.Duraipandian and C.Palanisamy (Associate Professor),"By sending large amount of data flows from multiple sites, Distributed Denial-of-Service (DDoS) attacks target the victims. Many of the DDoS defense methods need to be implemented simultaneously and collaboratively on several nodes to tackle this kind of Attacks, making them difficult to implement, especially on nodes that need to maintain round-the-clock Internet connectivity. The different defense methods depends on random or probabilistic means to detect the traffic which is not legitimate and discard it, which necessitates that a certain percentage of legitimate packets be dropped in the process, reducing the overall Quality of Service. They proposed an Intelligent Agent Based Defense Architecture for Distributed Denial of Service(DDoS) Attacks., which is fully distributed and provides an early warning when pre-attack activities are detected, using trust mechanisms. The proposed architecture includes improved technique of Hop-Count Filtering (HCF) approach. By Observing the simulated results, the results can be predicted as following: the proposed system architecture achieves a high throughput with low packet drop, by detecting and isolating the attack traffic flows [5].

According to Samia Khan,Fazirulhisyam Hashim, Mohd Fadlee A. Rasid, Thinagaran Perumal , ". In this paper, an authentication mechanism based on lightweight encryption algorithm and Media Access Control (MAC) authentication are proposed for black hole and Distributed Denial of Service (DDoS) attacks. The proposed technique is validated in Network Simulator 2 (NS2) whose results show that the approach offers prompt route verification with high throughput and generating less routing overhead avoiding black hole attacks"[6].

According to Jae-Hyun Jun, Hyunju Oh and Sung-Ho Kim, Increase in Internet users, increases in distributed denial of

service(DDoS) attacks that present a very serious threat to the stability of the internet. The DDoS is a kind of powerful attack attack, which is consuming all of the computing or communication resources necessary for the service, is very difficult to protect in comparisons to Low Rate DoS attacks(LDoS). The risk is posed by attacks on large network, such as the internet, demands effective detection method. Therefore, an IDS on large network is needed to monitor efficient real-time detection. In this paper, we propose a method or approach using some mechanisms of Machine Learning like entropy-based detection mechanism against DDoS attacks in order to guarantee the flow transmission of legitimate packets and prevent the flood of abnormal packets. The NS3/OMNET simulation results can be used show that our ideas can provide protection services in DDoS attacks[7].

3. CONCLUSIONS

In this paper, based on the information which came from flow, the DDoS attack detection method is proposed by using entropy. As the DDoS attack is detected, according to control method, the attack traffic of attacker or zombie host is able to be controlled. From the previous method, the destination of attack is able to provide continuously normal service to general users. The performance of detection of suggested method presents through the result of experiment.

The main aim behind the development of this system is to provide a better & efficient way for users to use the wireless devices without being highly exposed to the vulnerable.

REFERENCES

[1] Samia Khan,Fazirulhisyam Hashim, Mohd Fadlee A. Rasid, Thinagaran Perumal 2018 Published 2nd International Conference on Telematics and Future GenerationNetworks(TAFGEN).10.1109/TAFGEN.2018.8580488

[2] https://www.techsparks.co.in/tools-and-technologies/thesis-in-mobile-ad-hoc-network/

[3] Antench Girma, Moses Garuba , Jiang Li , Chunmei Liu 2015 12th International Conference on Information Technology 10.1109/ITNG.2015.40

[4] https://www.esecurityplanet.com/networksecurity/types-of-ddos- attacks .html bySue-Marquette-Poremba

[5] M.Duraipandian, C.Palanisamy Associate Professor, "An Intelligent Agent Based Defense Architecture for DDoS Attacks" Department of IT, SVS College of Engineering, Coimbatore & Research Scholar, Anna University, India

[6] Samia Khan,Fazirulhisyam Hashim, Mohd Fadlee A. Rasid, Thinagaran Perumal 2018 2nd International Conference on Telematics and Future Generation Networks (TAFGEN).10.1109/TAFGEN.2018.8580488

[7] Jae-Hyun Jun ; Hyunju Oh ; Sung-Ho Kim Published 2011 IEEE 2nd International Conference on Networked Embedded Systems for Enterprise Applications 10.1109/NESEA.2011.6144944