Yatish Patil, et. al. International Journal of Engineering Research and Applications
www.ijera.com
ISSN: 2248-9622, Vol. 10, Issue 5, (Series-I) May 2020, pp. 36-40

RESEARCH ARTICLE OPEN ACCESS

IP Threshold-based Detection & Defense method for DDoS attack 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-400614*
[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

Date of Submission: 28-04-2020 Date of Acceptance: 11-05-2020

I. INTRODUCTION

MobileAdhoc Networks(MANETs)normallyconsist 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 wiredandwirelessnetworks,MANETsareexposedto security threats because of its elementary attributes like decentralized infrastructure, arbitrarytopology, absence of association, and resource constraints [1].

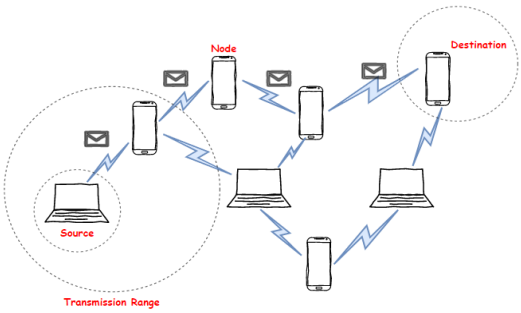

Fig -1: MobileAdhocNetworks(MANETs)

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 [2].

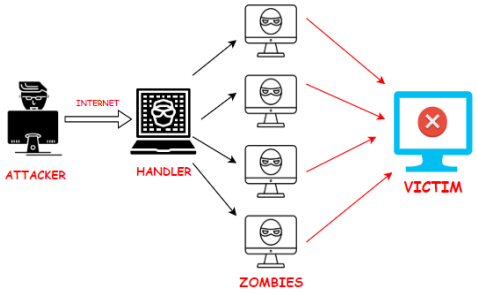

Fig -2: Typical DDOS Attack Organization

II. 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.

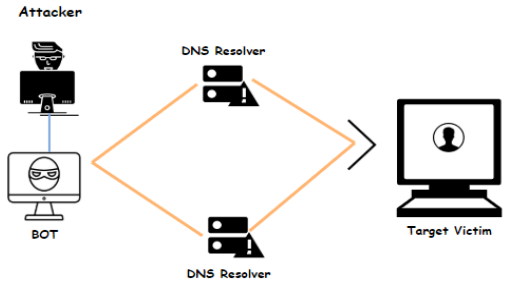

Fig-3: DDOS Attack

III. METHODOLOGY

Improved AODV

Improved AODV is one of the good options available to prevent DDOS attack in the Mobile ad hoc network it is reactive routing protocol and didn't uses ant kind of data structures to do the routing like the proactive routing protocol it didn't hold the all the routing paths the AODV works best with good power efficiency in the above paper they used MAC authentication to identify the sender is authorized or not but this method with symmetric encryption consumes lot of resources which is not suitable in case of mobile devices that is the disadvantage of the this method[3].

Entropy based

Entropy is the unit of the uncertainty it is mostly used in probabilistic approaches, It is one of the best approaches to prevent DDoS it didn't consume much resources if the

dataset kept small enough entropy based DDoS are very good in the server client architecture, but in Mobile ad hoc network we the data rate can vary as per the need of senders so highly sensitive algorithm like entropy has chances to treat high data rate as a DDoS which may lead to packet drop of authorized packets[4].

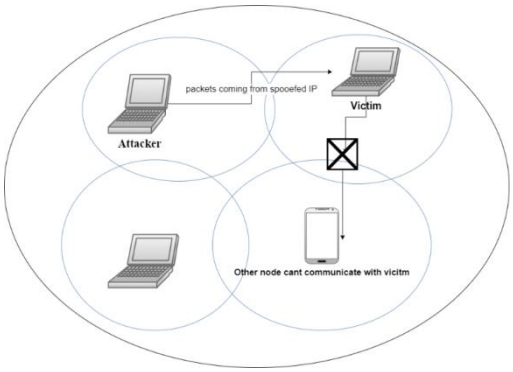

Fig-4: Architecture

IV. WORKING PRINCIPLE

The system is based on previously implemented DDoS Preventive measures. It consist of Advanced Protection Mechanisms in-order to detect a Distributed Denial of Service(DDos) attack originating from a particular node connected in an Ad-hoc network., and also protecting the attacked node. The Algorithm designed is simple but effective. Firstly we have created our own Ad-Hoc network through which all the computing nodes (Laptops/Desktops including Mobile devices) are connected. Next step was to trigger a DDoS attack from a node to which we named as "Attacker Node" in our context. For this we require "IP address" of the node which attacker wants to target. Now. As the Attack is being triggered over a network for that particular IP address, the Target Node gets affected first and slowly the whole network gets down resulting in Distributed Denial of Service Attack. As a preventive measure, next step comes into action of "Protection of Attacked Nodes". For this we have algorithm designed which will initially detect the attack node and its corresponding IP address and will generate a log file. We have named this algorithm as "Detection Algorithm". The Log file generated depicts which attacking nodes generates a high traffic on the network. To prevent the nodes from being more flooded with random traffic generated by attacker, the protective measure applied here. This protective measures includes an algorithm which acts as a barrier to over flooding of packets.

In this "Defense Algorithm" we have used an approach of "Network Interfaces" means, when an attack has been triggered and detected by our algorithm a small message will be circulated and here our algorithm starts working. In protecting phase we aimed to directly target the Wireless Network Interface (WLAN) to which the node is

connected to Ad-Hoc wireless network. This will eventually takes down the respected nodes WLAN Interface and will change or re-allocate a new Interface Address to that particular node which was being attacked. This Approach has a minor drawback. i.e., the newly allocated address needs some time in order to activate and get connect to our hosted Ad-Hoc Network. To reduce the complexity of algorithm and code we have merged the two algorithms ("Detection Algorithm" and "Defense Algorithm") making it as a single standalone algorithm as "Detection & Defense Algorithm". This system is very simple and economical yet effective in our tested environment.

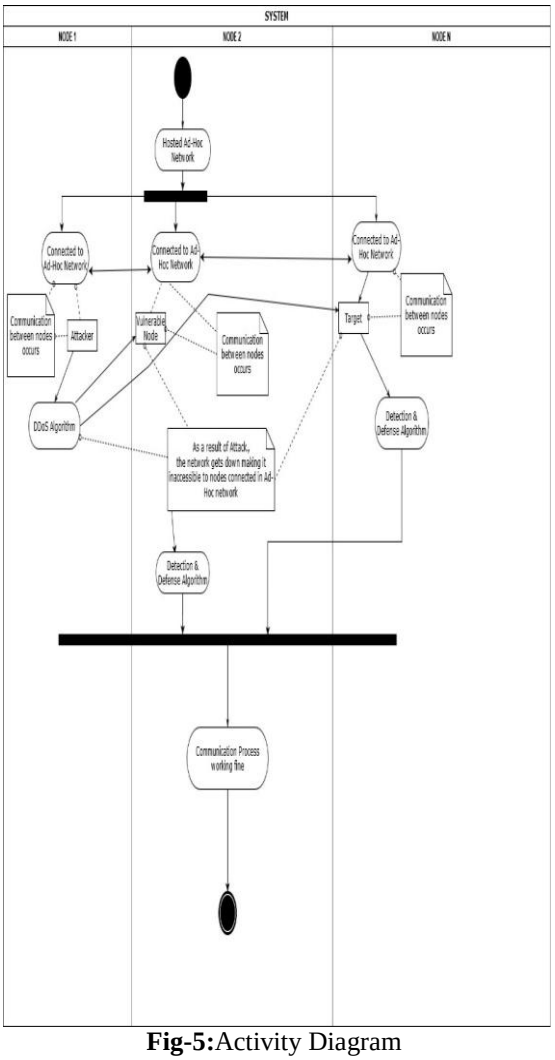

Fig-5: Activity Diagram

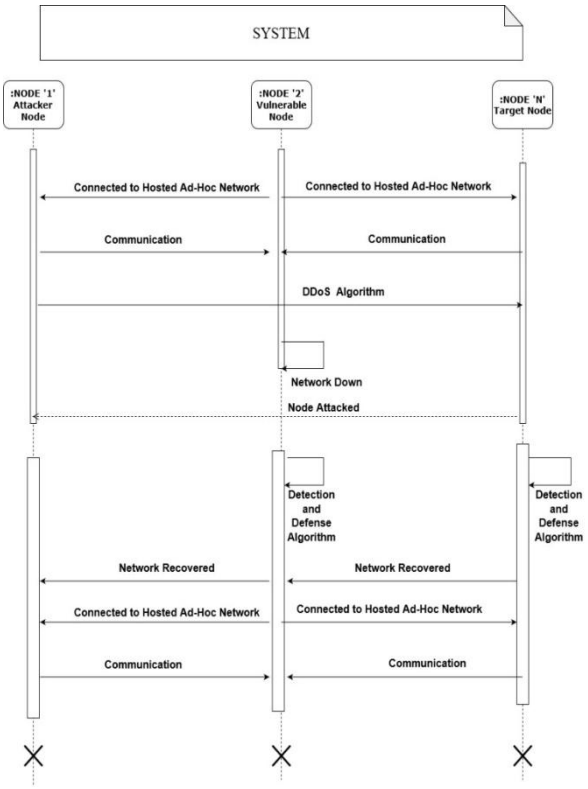

Fig-6: Sequence Diagram

V. MANET ENVIRONMENT CREATION ,DDOS ATTACK DETECTION AND WIRESHARK ANALYSIS SCREENSHOTS-

-This figure depicts the Ad-Hoc Network created using Windows CLI(command-prompt).The list of IP addresses are logged when a device is connected to this interface.

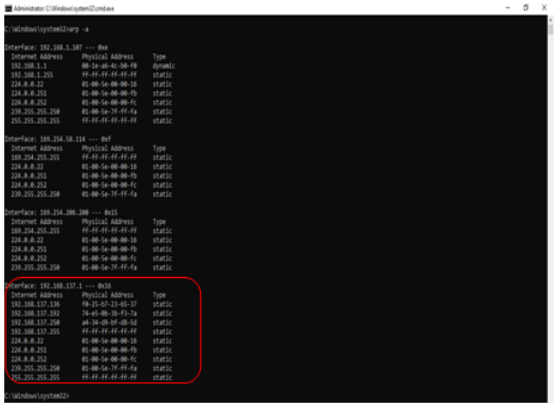

Fig-7: Interface created for MANET

-Here our "**Detection & Defense Algorithm"** starts to detect a ddos Attack from attacker node and a log file is created in the background in the text format(reflecting the IP address of the attacker)

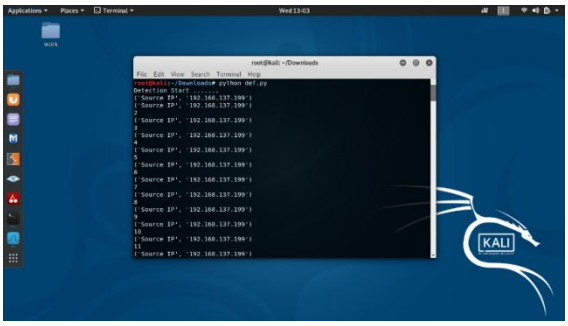

Fig-8: Algorithm detecting the actual Attacker IP

-After successful attack.,the victims device gets disconnected from the network,resulting in "loss of communication" with other devices.

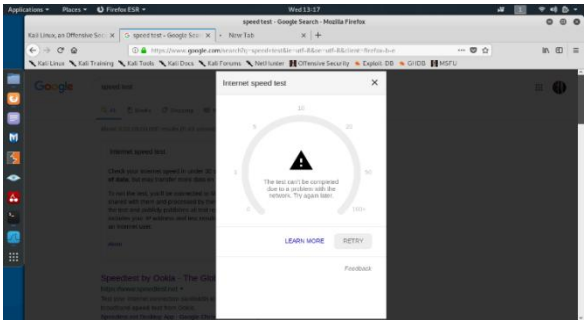

Fig-9: Network is getting down

-Next phase in our **"Detection & Defense Algorithm"** will act here., i.e., our **Defense Mechanism** will allocate a new IP Address to the victims device inorder to continue with the communication operations.
This IP address is allocated at temporary basis(that means we are not actually changing the hardware-WLAN card of the device).

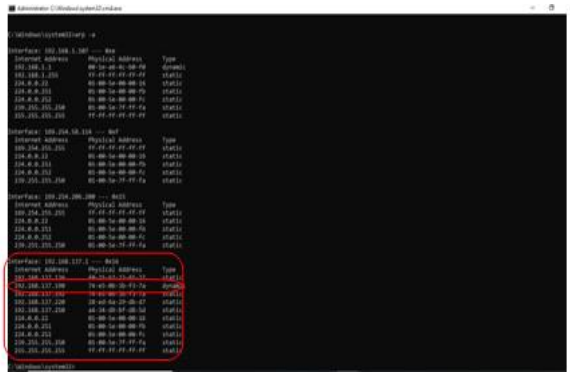

Fig-10: Restored Network by assigning new IP to machine

-After successful allocation of new address., the device starts communicating again and the network speed is back to its normal state.

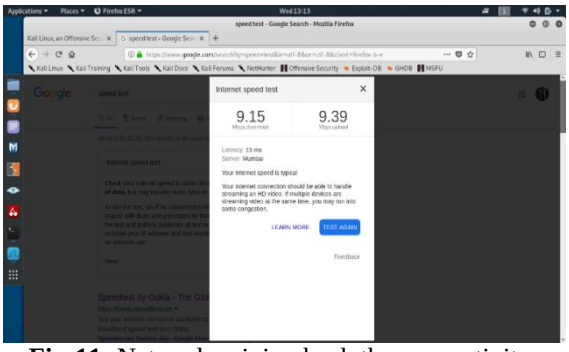

Fig-11: Network gaining back the connectivity

-This shows wireshark analysis of how much traffic is generated at victims node when ddos Script is shooted by attacker.

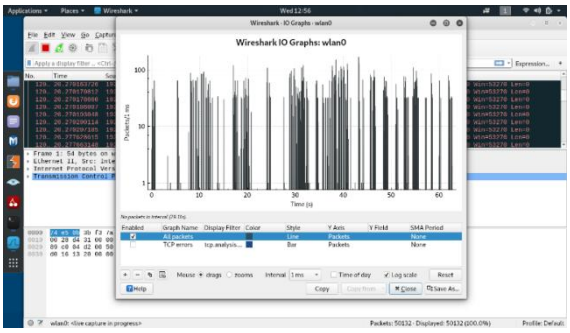

Fig -12: Wireshark Analysis

-TCP Packets sequence scenario analyzed with the help of **Wireshark Networking Tool.**

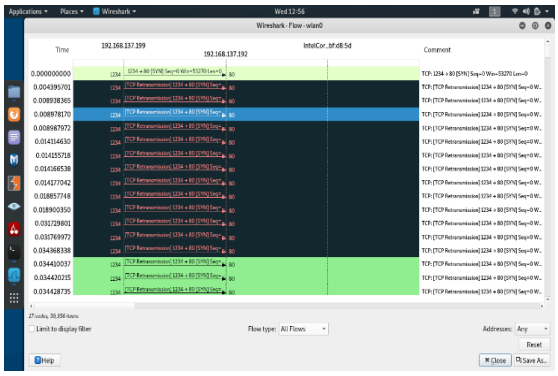

Fig-13: Wireshark DDOS attack representation

VI. CONCLUSIONS

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.

The Hybrid approach is designed in a way to provide security with minimum cost of implementation and this method not only reduce the computational tasks as well as it reduce the resource utilization hence it is very effective in ad hoc

network like MANET so it can be used in real world scenario to provide good protection against the DDOS attack in the MANET .

REFERENCES

[1]. Samia Khan,Fazirulhisyam Hashim, Mohd Fadlee A. Rasid, Thinagaran Perumal2018 Published 2nd International Conference on Telematics and Future generationnetworks(TAFGEN).10.1109/TAFGEN.2018.8580488

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

[3]. Samia Khan,Fazirulhisyam Hashim, Mohd Fadlee A. Rasid, Thinagaran Perumal2018 2nd International Conference on Telematics and Future Generation Networks (TAFGEN).10.1109/TAFGEN.2018.8580488

[4]. 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

[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]. Yatish Patil, Niraj Palkar, Rehan Sayed, Prof. Ranjit Mane, "Hybrid Approach for DDoS Protection in MANET" Dept. of Computer Engineering, Bharti Vidyapeeth College of Engineering, Navi-Mumbai, Maharashtra, India.

[7]. Vaishali Kansal and Mayank Dave ," Proactive DDoS attack detection and isolation", Department of Computer Engineering National Institute of Technology Kurukshetra, Haryana, India

[8]. Mohammed A. Saleh and Azizah Abdul Manaf,"Optimal Specifications for a Protective Framework Against HTTP-based DoS and DDoS Attack"sFaculty of ComputingUniversiti Teknologi Malaysia (UTM)Johor Bahru, Malaysia.

[9]. Jiahui Jiao, Benjun Ye, Yue Zhao, Rebecca J. Stones,Gang Wang, Xiaoguang Liu, Shaoyan Wang, Guangjun Xie" Detecting TCP-based DDoS Attacks in BaiduCloud Computing Data Centers"Nankai-Baidu Joint Lab, College of Computer and Control Engineering, Nankai University

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

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

[12]. Anteneh Girma ,Moses Garuba, Jiang Li and Chunmei Liu" Analysis of DDoS Attacks and an Introduction of a HybridStatistical Model to Detect DDoS Attacks on Cloud Computing Environment" Systems and Computer Systems and ComputerScience Departmentt Howard University .

Yatish Patil, et. al. "IP Threshold-based Detection & Defense method for DDoS attack in MANET." *International Journal of Engineering Research and Applications (IJERA*), vol.10 (05), 2020, pp 36-40.