Prevention of DoS Attack in MANET Using BIOS Serial Number

Upasana Chaudhari[1], Dhanashri Patil[2], Maya Sonawane[3], Shital Randhe[4]

U.G. Students
Department of Computer Engineering,
SSBT's College of Engineering and Technology, Jalgaon, India

***Abstract* – DoS Attacks are one of the major problems in MANET. It is totally based on TCP/IP architectures. There is less security on TCP/IP protocols so that MANET runs on TCP/IP protocols. The existing solution gives optimal solution is that preventing and detecting attacks by using IP and MAC addresses. But in wireless network hackers break the security in the form of IP spoofing and MAC spoofing by using fake IP and fake MAC addresses. To overcome this problem, we detect attack by comparing IP address with the MAC address and BIOS serial number in register database. IF IP and MAC get fail to detect spoofing attack then DoS attack uses BIOS Serial number because BIOS serial number is common for all devices such as PC's, Mobile phones etc. It cannot change to any ways.**

***Index Terms*— DoS Attacks, MANETs, Security, Wireless communication.**

I. INTRODUCTION

MANET is defined as Mobile Ad-Hoc Network which is used in Government sector, also important for military purpose, also used in field like automated battlefields. Also it have applications in virtual classroom, conference meeting, vehicular computing, voting system and so more. Its use is more where security is more important. IP address and MAC address are important concepts we are going to use in MANET. IP spoofing directs to the creation of Internet Protocol (IP) packet with the help of forged source IP address with the purpose of concealing the identity of the sender. IP address holds source and destination address of the packet. Hackers can use any values occurring without definite aim of IP address as forged source address but because of the operating system attackers cannot used an IP address which is currently used by another user is working on a same machine. In the same network whenever new IP is allocated to the user, detect whether same IP address is used by the another user is in the network which is same. So for that a table is created to store the information of all users that are currently active in the user in the network. The table stores IP address, corresponding MAC address for comparing to detect IP and MAC spoofing with BIOS serial number. Bios serial number is same for all devices and it is useful for identification of accurate mobile user [1].

II. RELATED WORK

Attackers in their spoofed packets, they spoofed different types of IP addresses to use as source IP addresses. This spoofed source IP addresses may be random IP addresses or fixed spoofed IP addresses [2]. To protect from such IP and MAC spoofed attacks there are no promising solutions are available. On network layer detection of DoS attacks are in the form worm hole, gray hole, black hole in such case intrusion can be detected but cannot be completely prevented [3] . Whether a receive packet have spoofed source IP address or not for that variety of methods that helps in determining has been put forward. A host can determine the receive packet is spoofed or not by following two methods. First is routing based method that depends on routers and other network device to recognize spoofed packets and second is non-routing methods which apply both active n passive techniques. Host can be used this techniques to detect if the receive packet is spoofed [2].

III. IMPLEMENTATION

MANET is mobile Ad-Hoc network which is one of the wireless network with movable device and gives better result for wireless application. Total implementation of proposed work is based on three steps such as Dynamic server, Static server and Client implementation.

a. Step 1 : Dynamic Server

By some networking Microsoft commands , Dynamic server store IP and MAC address of all mobile user when they are connected with MANET.

b. Step 2 : Static Server

At the time of client registration and login, static server take the IP addresses corresponding MAC addresses with BIOS serial number which comes from client and store into static database for registration and login.

c. Step 3 : Client Implementation

Client waiting response from static server to check whether connection is true or spoofed by sending the IP address and MAC address and BIOS Serial to the static server. If it is spoofed or fake then shut down mobile host properly.

IV. PROPOSED WORK

Detection and Prevention are two scheme used in handling DoS attack. Location of an attacker and taking appropriate action these two task are involving in detection method. For detecting DoS attack source monitoring nodes activity and tracing an attacker can be helpful. To defend the network from attack existing schemes in MANETs use for prevention only mechanism or detection strategies. In ad-hoc networking environment, it can prevent but cannot eliminate attack. When attacker is mobile, such mechanism determining attack route or attack generating domain. Hence our proposal is the combination of prevention and detection and improves the performance and provides the security in MANET [4].

V. RESULT

In our proposed system, DoS attack will be detected and prevented by the server. Detection of IP and MAC attack has been design to detect IP and MAC spoofed attack which is made up of database and three routines developed at server side . First routine is IP check routine which is used for comparing received IP address with the value that is store in database. For spoofing detection and second is MAC check routine compare received MAC with the stored MAC value and third is BIOS check routine which detect true mobile host otherwise spoofed mobile host.

CONCLUSION

The proposed system can detect and prevent IP and MAC spoofing attack . In this system we pull out source IP, MAC address and compared with our databases . Hence this method is very simple and efficient to detect attack in the same network . The implementation of propose system is done on IP and MAC which is checked by server. If it is fail to find out spoofed mobile device then BIOS check true serial number and after that server find spoofed mobile device. This is one of the effective method that can be used to increase the performance of the network. Thus the proposed system describe about routing protocols as well as security related to the MANET.

FUTURE SCOPE

1. The proposed system is to verify successful authentication of source IP and MAC address and also find out the attacker by comparing IP addresses corresponding MAC address with BIOS serial number which is store in database.
2. It provides secure communication over MANET area and also evaluates the performance of the network.
3. IN MANET combining many wireless network contains research of Distributed Denial of Services. So we proposed system for preventing and detecting DoS attacks in MANETs.

REFERENCES

[1] Prevent DoS attacks in VOIP communication over MANET area
Tamboli Sachin P etel. IEEE - International Conference on Research and Development Prospects on Engineering and Technology (ICRDPET 2013) March 29, 30 - 2013 Vol. 4

[2] Noureldien A. Noureldien Mashair O. Hussein ―Block Spoofed Packets at Source (BSPS): A method for Detecting and Preventing All Types of Spoofed Source IP Packets and SYN Flooding Packets at Source: A Theoretical Framework, IEEE 2009.

[3] Jhaveri "DoS Attacks in MANET: Survey" in 2nd International Conference Advance Computing & Communication Technologies (ACCT-2012).

[4] Detection and Prevention of Denial of Services (DoS) Attacks in Mobile Ad Hoc Networks using Reputation – Based Incentive Scheme : Mieso K . Denko Department of Computing and Information Science University of Guelph, Guelph, Ontario, Canada, N1G 2W1