An Approach to Avoid Flooding Attack in MANET

Garima Pahare[1], Surbhi Kaushik[2]

[1]*PG scholar, Department of ECE, RGPV University, Indore, India*

[2]*Assistant Professor, Department of ECE, RGPV University, Indore, India*

Abstract - Mobile ad-hoc network is kind of wireless networks consist mobile nodes to retrieve and process information. Mobile nodes are small kind of device having small battery, microprocessor along with storage. Due to low prize and wide scope of applications, it is one of the popular solutions for several applications. Open nature of communications make it vulnerable for various security threats such as black hole, wormhole attack, DDOS attack, Sybil attack etc. Here, flooding attack is one of most severe security threat in sensor networks.Distributed Denial of Service (DDOS) attack is such kind of attack which aims to disrupt the network by draining resource capability. Here, Attacker communicates worthless messages formally known as false packet to increase network traffic and make target node busy in useless activity. The complete work observes that, DDOS attack does not require any study about network vulnerability. The major challenge with mobile network is energy issue. Its life is directly proportional with battery capacity. Thus draining in battery energy directly degrades the life of node. This project observed it as severe problem and proposed a solution to overcome the problem of power draining due to DDOS attack. Subsequently, Power draining is the major thread; where attacker not only exhausts the network traffic but also degrades the life of node as well network. The objective of this study is to detect and prevent mobile ad-hoc networks from unwanted power draining due to flooding attack. NS-2 simulator has been used to simulate and evaluate the MANET, Flooding Attack, and AODV.

Keywords: MANET, Flooding Attack, AODV.

1. INTRODUCTION

A Mobile Ad-hoc Network is a collection of independent mobile nodes that can communicate to each other via radio waves. The mobile nodes that are in radio range of each other can directly communicate, whereas others need the aid of intermediate nodes to route their packets. Each of the nodes has a wireless interface to communicate with each other. These networks are fully distributed, and can work at any place without the help of any fixed infrastructure as access points or base stations. Figure 1 shows a simple ad-hoc network with 3 nodes. Node 1 and node 3 are not within range of each other; however the node 2 can be used to forward packets between node 1and nodes 2. The node 2 will act as a router and these three nodes together form an ad-hoc network.

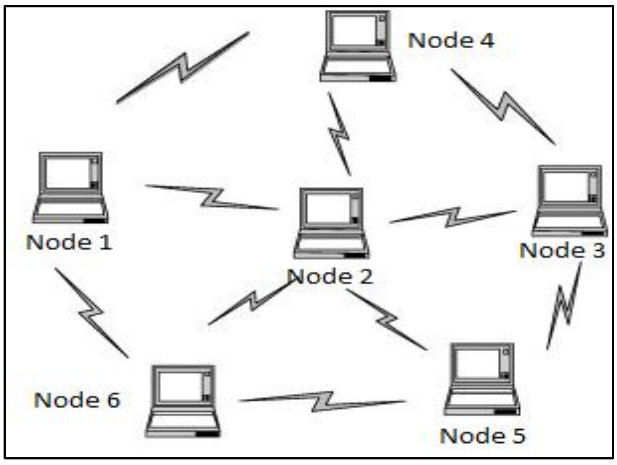

Figure 1: Mobile Ad-hoc Networks

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology.

Distributed denial of service attacks or Flooding attack are based on the principal: "Power of many is greater than power of few" Such attacks are launched subsequent to subversion and/or compromise of legitimate client machines of the network. These compromised machines then participate in the attack process.

This work describes the efficient strategy to detect and prevent power draining in MANET. In MANET, the mobile nodes are not much in power, computation, and battery life of a node so it is very difficult to detect any attack in the network. In terms of Flooding attack, it is very difficult to detect because the nodes which are the parts of the route path between the source and destination and the nodes of wireless networks are less in power and less in memory so encryption and decryption of the packets are not possible, that is a reason why this networks needs an efficient technique to

detect the attacker nodes in the networks. DYMO routing protocol will be used to send the packets in network. DYMO routing protocol is on-demand routing protocol, it search a route when source is required to send a packets to destination node.

2. PROBLEM DOMAIN

The DYMO routing protocol is a popular reactive routing protocol in wireless networks, but DYMO routing protocol designed for better performance of the network not for security of node, secure protocols are generally designed to have features such as authentication, integrity, confidentiality and non-repudiation. For security purpose DYMO have vulnerabilities and it is easily manipulate by malicious node to destroy its network routing.

The open nature of wireless medium also makes it easy for outsider attackers to interfere and interrupt the legitimate traffic. This concept classifies the attacks into two broad categories, namely Passive and Active attacks. In Passive attack, the adversary only eavesdrop upon the packets content, while packets may get dropped or altered on way in case of Active attacks.

Several attack such as DDOS attack, Wormhole attack, Black-hole attack, Gray-hole attack, Jamming attack, Sybil attack, Node repudiation etc. always may apply on conventional DYMO routing protocol and compromise the security of network. Furthermore, among the all the security attacks DDOS attack is one of severe attack which not only create congestion into network communication but also consume unnecessarily battery power which reduce the life of mobile node as well as mobile network too.[2,5]

The DDOS attack is a serious threat in mobile networks as it impacts the functions of the network resources. In this attack, malicious node either directly flood on targeted node or attempt to flood into victim node. When thousands of unwanted packets arrive with extra processing load, intermediate node or targeted nodes have to pay more power than regular. These attacks decrement the important functions of a network like routing, resource allocation, message integrity, etc. by reducing the node life.

3. SOLUTION DOMAIN

The primary requirement of the work is to configure the static battery and energy consumption model with mobile nodes. Subsequently, evaluation of power consumption in normal condition is expected. Afterwards, power consumption during DDOS attack, detection and prevention technique would help to find improvement into node lifetime.

On the basis of the outcome and observation the desired algorithm has been designed and tested in the same environment in order to perform comparison analysis and observe that the algorithm gives required results.

This study will provide a base for designing the algorithm and its requirements. This work will completely analyze the DDOS attack on the Mobile Ad-hoc Networks. The objective of this study is to minimize the denial of service attack in the MANET in order to transmit data without any problem.

The proposed work will perform a security aware formulation and also define it in order to enhance the security in MANET and its performance in comparison with the previous algorithm. In order to simulate our research NS2 will be used. NS2 is a viable version of Open Source panet. It is a rapid GUI based model designing, animation and analysis system used to design high-fidelity commercial protocols and device models. It provides the facility to perform comparative performance evaluation of different protocols at the same time. It has a modular and layered stack design. It also supports parallel execution thus providing scalability for wider range of networks.

Following steps will be used to implement and simulate proposed solution.

1. Design and Creation of Mobile Ad-hoc Networks Scenarios.
2. Implementation of DDOS attack using Overwhelming Flooding.
3. Observation of Total consumed Power before and after attack to evaluate power drain.
4. Implementation of service request based detection method to identify malicious nodes.
5. By-Pass Malicious nodes to prevent genuine node from power loss.
6. Observe and evaluate the consumed power and power drain due to preventive technique.

The complete work will not only avoid DDOS attack but also avoid the situation of power drain. Proposed work will help to sustain node life as it naturally deserve.

4. PROPOSED METHODOLOGY

Flow Chart of Proposed Solution

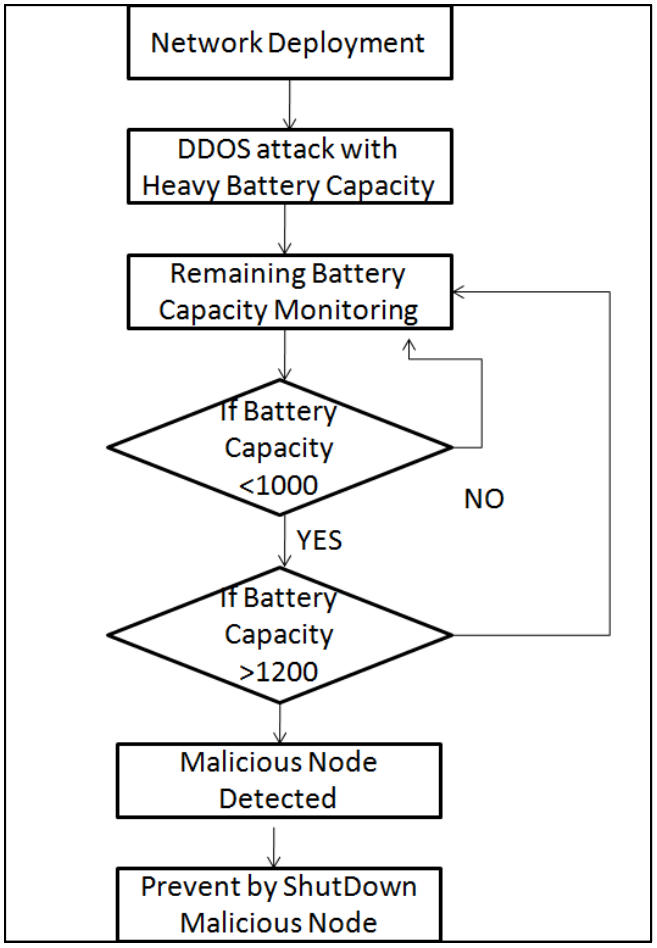

Figure 2: Flow Representation of Solution

5. CONCLUSION

The MANET is a kind of wireless network that consist of thousands of sensor nodes deployed in the open field. WSN provides the solution to the real world application like military and civilian tasks at very low cost with absolute performance. Further, Small data storage capacity, low power battery, low bandwidth and low computational power make it more complex and vulnerable to many security threats.

The complete study is based on study of targeted flooding attack in DYMO routing protocol to degrade battery capacity and reduce node lifetime. Three situations has been developed and evaluated on basis of energy consumption, throughout, packet delivery ratio and end-to end delay. Battery capacity based detection and prevention mechanism has been developed.

REFERENCES

[1] Baig, Z., Salah, K., "*Multi-Agent pattern recognition mechanism for detecting distributed denial of service attacks*" IET Information Security, 4(4), 333-343, United Kingdom, DOI: 10.1049/iet-ifs.2009.0255.

[2] Jaydip Sen, "A Survey on Wireless Sensor Network Security", In proceedings, *International Journal of Communication Networks and Information Security (IJICNIS),* Vol 1, No 2, Augest-2009.

[3] Sriram Nandha Premnath, Sneha Kumar Kasera, "Battery-Draining-Denial-of-Service Attack on Bluetooth Devices", Project Report School of Computing University of Utah ,2012.

[4] T. Martin , M. Hsiao , D. Ha and J. Krishnaswami "*Denial-of-service attacks on battery-powered mobile computers*", Proc. 2nd IEEE Annual Conf. Pervasive Computing Commun. (PerCom), pp.309 -318 2004.

[5] K. Gill, S.-H. Yang and W. Wang "*Scheme for preventing low-level denial-of-service attacks on wireless sensor network-based home automation systems*" IET Wirel. Sens. Syst., 2012, Vol. 2, Iss. 4, pp. 361–368

[6] Manju.V.C, Senthil Lekha.S. L.and Dr.Sasi Kumar M. "*Mechanisms for Detecting and Preventing Denial of Sleep Attacks on Wireless Sensor Networks*" Proceedings of2013 IEEE Conference on Information and Communication Technologies (ICT 2013) Mechanisms. IEEE: 978-1-4673-5758-6/13

[7] Eugene Y. Vasserman and Nicholas Hopper, "Vampire attacks: Draining life from wireless ad-hoc sensor n etworks, " IEEE Transactions on Mobile Computing Vol.12 No.2 (2013) 1-15.

[8] Jayan Krishnaswami " Denial-of-Service Attacks on Battery-Powered Mobile Computers" Thesis Master of Science from Virginia Polytechnic Institute and State University, 2004