Analysis of Route Discovery Message Flooding Attack in Mobile Ad-Hoc Network

Nupur Agrawal
Department of CSE
SVITS, Indore,
Madhya Pradesh, India

Upendra Dwivedi
Department of CSE
SVITS, Indore,
Madhya Pradesh, India

ABSTRACT
The Mobile ad-hoc network (MANET) is a self-design infra-structure less networks of mobile nodes. Each node in a network acts as a router and can travel on any route in a network. And it also have constantly changing topology. There are various types of attack in Manet which reduce the performance of network. One of them is flooding attack which occurs when a network is heavily loaded with traffic which includes the route request packet for connection. Flooding is the reason for traffic and congestion in the network and also the incompleteness of legal connection. In this paper the detection of flooding attack is done by analyzing the behavior of nodes so that the legal connection can be established. By these analyses the efficiency of the system increases and resource utilization is done properly..

Keywords
MANET, RREQ Packets, Routing Protocols

1. INTRODUCTION
A mobile ad-hoc network is a organize by itself spadework less network of mobile devices linked by a network. Each device in MANET is enabled to travel on any route, and will therefore alter its path to other devices frequently. In MANET topology also changes instantly in the network. Each node should forward traffic recognizable to its own use, means every node in the network also acts as a router. Such networks may operate by themselves or may be joined to the large Internet. It is the autonomous system of mobile hosts.

A lot of researches in the last few years are predicted and implemented but the most important contributions were the trust based security. In a challenge to upgrade security in MANET lots of researchers created in a field, some have recommended new techniques and implemented innovative improvements in the protocol and some of them have recommended new protocols.

Various types of attack are there, which try to degrade the performance of the network. Flooding attacks occur when a network becomes so heavily loaded with traffic with unnecessary packets initiating requests for connection which can no longer preform genuine connection request. Flooding is the reason for traffic and congestion in the network which lead to incompleteness of legal connection. Once this buffer is full with request of the packets, traffic become uncontrollable and no further connections can be created, and the result is a Denial of Service [1].

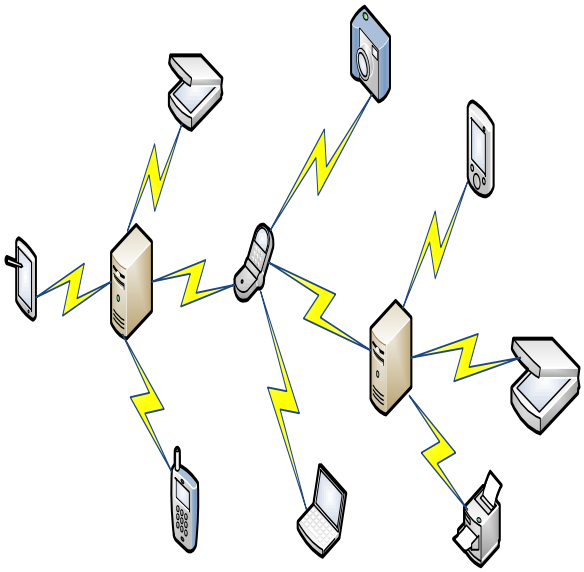

Fig.1. Mobile Ad-Hoc Network

A mobile ad hoc network (MANET) is a vibrant wireless network that can be formed without any infrastructure in which each node can proceed as a router. MANET does not have a partial nature to join the network or access the network information. So, the both legitimate nodes and malicious nodes can enter in the network. It is accessible for legitimate network users as well as malicious attackers, because malicious nodes can behave as normal nodes. In the existence of malicious nodes, the main problem faced in MANET is to design the robust security solution that can provide security to MANET from different routing attacks. Several techniques have been proposed using various cryptographic techniques for the routing attacks against MANET. But, this technique is not solving the problem of MANET resource limitation, i.e. finite bandwidth and battery power, since they establish the heavy traffic load to interchange and verifying keys. The existing security contraversy in MANET are analysed. Different routing attacks, such as flooding, Blackhole, link spoofing, Wormhole are studied and prevention solution for these attacks [2].

If the network does not fulfill all the security principles then there are the possibility that network is under the security attack. There are various security concerns in MANET. Secure routing protocols also developed like ARAN, SRP, BISS, SEAD for securing the network and research is done on the improvement of these protocols [5].

2. LITERATURE SURVEY

Many significant works has been done to secure routing protocols against attacks on routing traffic. In this paper, author describes about MANETs various restrictions because of its routing protocols. The MANET security is the main concern as it is becoming popular. There are various types of possible attack one of them is Denial of Service Attacks (DOS). The attack of initiating fake Route Requests packets and Data packets is called Flooding attack or DOS attack. This type of attack can support to hogging of network resources. This type of attack is hard to detect since malicious nodes mimic normal nodes in all conditions. In this article distrusted filtering mechanism is proposed to moderate such situations and reduce the loss of throughput. This tool could stop the specific kind of DOS attack and does not use any extra network bandwidth. In this research work author work on flooding attack on basis of Blacklist limit and Rate limit [7].

In this paper, author represents a prevention technique for flooding attack. Mobile ad hoc networks will come into view in environments where the nodes of the networks have little or no physical protection. The nodes of mobile ad hoc networks are at risk and may be compromised. The networks are vulnerable to denial of service (DOS) attacks formed through compromised nodes or intruders. This can involve the network as denial of service attack, when used in conflict to on-demand routing protocols for MANET, like AODV, DSR. The intruder sends Route Request packets to immerse the communication bandwidth and node thus valid communication cannot be made for a long time. This paper explains the new strategy developed Flooding Attack Prevention (FAP), a defense in opposition to the Ad Hoc Flooding Attack in mobile ad hoc networks. When the attacker node broadcast packets beyond the limit of the Route Request, the neighbors of the attacker trace the behavior of the sender and check its trust by a trust function. Once the threshold is exceeded, nodes will not accept any request in the future from that node [8].

In this work, author target on the flooding attack and effort to asset out the solution based on trust function. Mobile ad hoc is achieving a reputation because low cost mobile devices are easily available. MANET have the ability to serve instant wireless networking application while implementation of wired network is not possible easily and costly. MANETs are defenseless to various types of attack because of its features like constant changing topology, resource limitation and absence of any centralized structure. Denial of service type of attacks is possible in the MANET in many ways. One of these type attack is flooding attack in which attacker sends the unnecessary packets to consume the network resources. Possibility of flooding attack is mostly in all most all on demand routing protocol. In this work of research author present a technique to moderate the effect of the RREQ flooding attack in MANET using a trust estimation function in the DSR on demand routing protocol [9].

In this work author proposed a new technique for the detection and prevention of a distributed DoS attack. In wireless ad-hoc networks there is highly possibility of distributed denial of service (DDoS) rush (attacks) because of its distinctive characteristics such as open network architecture and mutual wireless medium. A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to cause a computer resource inaccessible to its genuine users. The denial of service (DOS) does not result in information hacking or loss but can be very unsafe. Significant hard work has been made towards making an ad-hoc network secure and secure from DDoS attacks. This paper explains how various detection parameters in cooperation work as a single and proficient method to detect various DDoS attacks in Manets. In this research work a technique to prevent DDoS attacks in Manet is also found out which help in preventing the attacks to communicate with the network [10].

3. MANET SECURITY ISSUES

MANET MANET is a large domain of research. Flooding attack is broadly classified in two domains data flooding and RREQ flooding attacks. For data flooding attacks a lot of efforts and algorithms and improvements are proposed and designed. But too few efforts and algorithm are found in RREQ flooding attacks thus required to propose a new algorithm for RREQ flooding attack prevention and detection over MANET environment.

The flooding attack is possible in all most all the on demand routing protocols, and according to use data packet it is categorized into main parts first RREQ flooding and second Data flooding. In the RREQ flooding attack, the attacker broadcast the many RREQ packets per time interval to nodes in the network for the intention of decreasing battery power of the legitimate nodes so that legal connection not established between the network and communication will not accomplish. This type of malicious activity may occur in the network by attacker node.

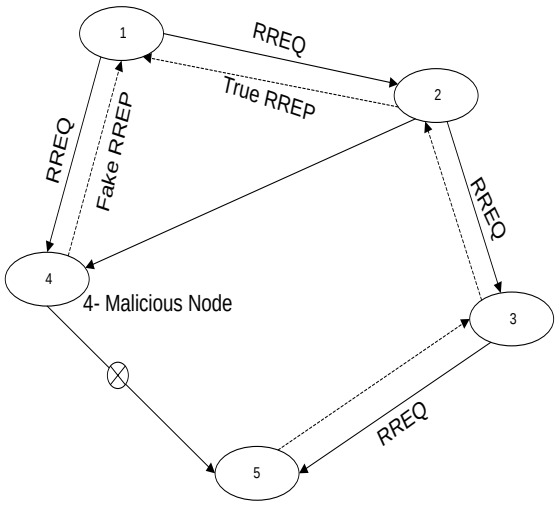

Fig.2. Route Discovery Process in Manet

Route Request Message, it is end when any node (source node) wants to communicate with other node and it does contain the path or route to that node(destination node) then it broadcast the RREQ message in the network to all the neighboring nodes. That source node contains the broadcast id in it so that when that message travels to through every node its value increases automatically and route is discovered. But if in this route any malicious node is present then the route which is discovered is not correct and message will not reach the destination node.

Route Reply Message, this message is unicast by the neighbor node to the source node. RREP is a message which is sent by the neighbor node in a reply of RREQ message which contain the fresh route to the destination node. It is unicast when that node receives the RREQ message and also when it has the

route to the destination otherwise it is not send. In this malicious node can send the fake RREP to the source node. In the Figure.2, RREQ and RREP message are sent and received by the source node and the destination, and it also contain the malicious node which drop the packet and send the fake RREP message to the source node.

In different paper different approaches have been used and their solution has been made. In [7] the author only concentrate on Denial of Service Attack but it doesn't solve the problem of malicious nodes. In [8] the author proposed Flooding Attack Prevention in which the attacker node behavior is checked and if it is not acceptable then is blocked forever. In these approaches malicious node detection is not done and also the efficiency of the system decreases. The main objective of this study is to detect the flooding attack caused in the network and to solve the problem of network partition and minimize the packet drop.

4. FLOODING ATTACKS EVALUATION

Flooding Attack is a major issue, which comes out in the environments where there are some known attacks. Some systematic approach to analyze attacks is introduced. In this paper it is analyzed that there is a system in which a malicious node is present and legal node is there. The malicious node will unnecessarily broadcast the RREQ packets in the network to the neighbor nodes because of which the network gets halt. In simulation real time environment which has the nodes or hosts connected to each other or to the routers. In table, the traffic source is constant-bit-rate with varying numbers of nodes. In this connection of nodes every node can send and receive packets from every other node in a network. The table shows how simulation is set. In which two different protocols are taken for the evaluation of this simulation. In the fig.3 and fig. 4, for every protocol nodes are varied and their throughput and pdf values are calculated using ns-2 simulator.

NS-2 is built using object oriented language C++ and OTCL (object oriented variant of Tool Command Language).The simulation scripts written in OTCL are interpreted by NS-2. The user writes his simulation as an OTCL script. The integrated simulations were carried out adopting ns 2.31 network simulator which is a discrete event driven simulator refined at UC Berkeley. The goal of NS2 is to support research and education in networking. It is applicable for designing new protocols, comparing different protocols and traffic evaluations. In this paper, NS-2 simulator is used for analysis of flooding attack in Manet.

In this paper, flooding attack is analyses in which the behavior of the node is evaluated. In which the record of RREQ packets which are send and received by the nodes from the other nodes in the network is captured. In this evaluation it is taken out that the battery of the network is wasted and packets are also dropped. This analysis is done so that the flooding attack is detected and their prevention is done for making the smooth network transmission. So, by this evaluation we will find the malicious node in the network and make a scheme in which the access amount of data transfer is reduced so that the flooding doesn't occur. In this evaluation it tries to reduce the problem by setting the certain limit. In this paper two protocols AODV and DSDV are compared by using the network simulation. In which the nodes and throughput are varying according to the AODV and DSDV protocols. AODV and DSDV are two routing protocols of manet. The AODV establishes the route to destination node only when it is need which involves RREQ and RREP packets for route discovery process. DSDV is a table-driven routing scheme who's aim main was to solve the problem of routing loop.

Table 1. Parameters of Simulation

Simulator	NS-2.35
Routing Protocol	AODV, DSDV
Topology	500 x 600
Mobility Model	Random Way Point
No. of Nodes	20,30,40,50,60,70,80,90
Data Rate	0.5
Transmission Range	50m
Simulation Time	150s
Packet Size	512 Bytes
Traffic	Constant Bit Rate(CBR)

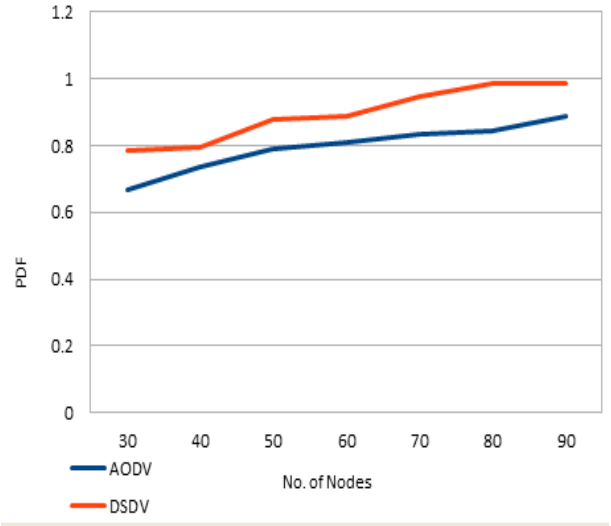

Fig.3.Comparison of protocols by varying the nodes

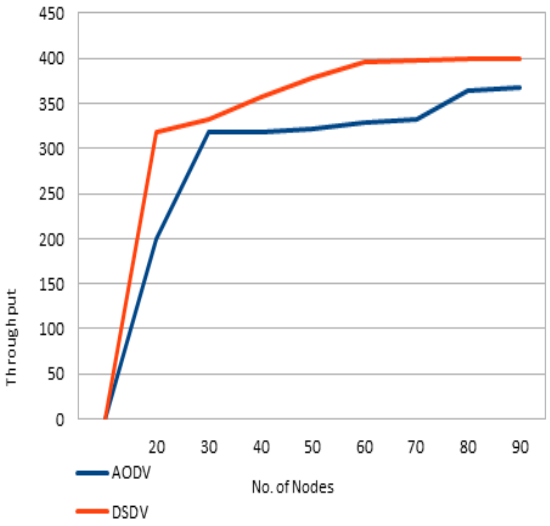

Fig.4.Comparison of protocols by varying the nodes

5. CONCLUSION

A mobile ad-hoc network is a organize by itself spadework less network of mobile devices linked by a network. Ad-hoc network is famous for its unusual characteristics like instant changing topology, mobility of nodes, unavailability. In which the flooding attack will be the destroying one. As Manet is not having any central hub due to which the flooding act occurs and affect the system because of which the genuine connection between the nodes doesn't take place. And also malicious nodes are not detected. For detecting the flooding attack, this survey is done in which the behavior of the nodes is analyzed by using the history table. And the efficiency of the system is increases and also make the proper utilization of the system resources by using this method.

6. REFERENCES

[1] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, and Nei kato "Asurvey of routing attacks inmobile ad hoc networks",ieee wireless communications october 2007 85 1536-1284/07/$20.00 © 2007 ieee

[2] Rashid Hafeez khokhar, MD Asri ngadi, Satria mandala "A review of current routing attacks in mobile ad hoc networks", international journal of computer science and security, volume (z) issue (3)

[3] Yi-an huang and wenke " Attack analysis and detection for adhoc routing protocols" e. jonsson et al. (eds.): raid 2004, lncs 3224, pp. 125–145, 2004.springer-verlag berlin heidelberg 2004

[4] Venkatesan Balakrishnan, Vijay Varadharajan, Udaya Kiran Tupakula "Defense against Flooding and Packet Drop Attacks in MANET" INSS Research Group, Department of Computing, Macquarie University,North Ryde, Sydney, NSW Australia 2109.

[5] Krishan kumar1, Yogesh kumar2, Gaurav Pruthi "A review of MANET security protocols" ijcsms international journal of computer science and management studies, vol. 11, issue 03, oct 2011

[6] Abhay Kumar, Rai Rajiv Ranjan Tewari, Saurabh Kant Upadhyay "Different types of attacks on integrated MANET"-internet communication international journal of computer science and security (ijcss) volume (4): issue (3) 265

[7] Jian-Hua song1, 2, Fan Hong1, Yu Zhang1 "Effective filtering scheme against rreq flooding attack in mobile ad hoc networks " proceedings of the seventh international conference on parallel and distributed computing, applications and technologies (pdcat'06)0- 7695-2736-1/06 $20.00 © 2006

[8] MS Neetu Singh Chouhan, MS Shweta Yadav "Flooding attack prevention in MANET" international journal of computer technology and electronics engineering (ijctee) volume 1, issue 3

[9] Shishir k. Shandilya, Sunita sahu "A trust based security scheme for rreq flooding attackin MANET",international journal of computer applications (0975 – 8887)volume 5– no.12, august 2010

[10] Neha Singh , Sumit chaudhary Kapil kumar verma " Explicit query based detection and preventiontechniques for DDOS in MANET", international journal of computer applications (0975 – 8887)volume 53– no.2, september 2012

[11] Meghna Chhabra and B.B. Gupta, "An Efficient Scheme to Prevent DDOS Flooding Attacks in Mobile Ad-Hoc Network (MANET)", in Research Journal of Applied Sciences, Engineering and Technology, ISSN: 2033-2039, Vol. 7, Issue. 10, March 2014.

[12] HyoJin Kim, Ramachandra Bhargav Chitti and JooSeok Song, "Handling Malicious Flooding Attacks through Enhancement of Packet Processing Technique in Mobile Ad Hoc Networks", in Journal of Information Processing Systems, DOI : 10.3745/JIPS.2011.7.1.137, Vol.7, No.1, March 2011.