Enhancement of AODV under Flooding Attack

Aman Yadav[1], Parul Dua[2]

M.Tech Research Scholar, Doon valley institute of engg. & tech.
Assistant Professor, Doon valley institute of engg. & tech.

Abstract— **A Mobile Ad-Hoc Network (MANET) are future wireless networks consists of mobile nodes which communicate on-the-move without base stations. MANETS are mobile; it uses wireless connections to connect to various networks. This can be a standard LAN Network, or another medium, such as a WI-FI or satellite transmission. Some MANETs are allowing only local area of wireless devices (such as a group of LAN computers), while others may be connected to the Internet. Due to the dynamic nature of MANETs, they are not very secure, so it is important to be cautious what data is sent over a MANET. This can be improved by implementing various security concerns. MANET involves various attacks such as DoS, Brute Force attack etc. In this paper provides the performance analysis of AODV routing protocols under the impact of flooding attack. The performance of the routing protocols always degrades when the network is under the influence of any kind of denial of service attack. In this paper we have selected AODV routing protocol for our study. In our work we have analyzed the performance of the AODV routing protocol under the presence of flooding attack. To analyze how much the performance of the network deteriorates under the presence of attack we have taken the various network parameters via throughput, packet delivery ratio and end to end delay.**

Keywords— **Ad-Hoc Network (MANET), Vehicular Ad Hoc Network (VANET), Ad-hoc On Demand Distance Vector (AODV), Flooding Attack, Security**

I. INTRODUCTION

Mobile Ad-Hoc Networks are autonomous and decentralized wireless systems. MANETs consist of mobile nodes that are free in moving in and out in the network. Nodes are the systems or devices i.e. mobile phone, laptop, personal digital assistance, MP3 player and personal computer that are participating in the network and are mobile. These nodes can act as host/router or both at the same time. They can form arbitrary topologies depending on their connectivity with each other in the network. These nodes have the ability to configure themselves and because of their self configuration ability, they can be deployed urgently without the need of any infrastructure [1,2].

Security is one of the most challenging and in request issue of ad hoc network. At the networking layer, the routing information must be protected from any attack against *confidentiality*, *authenticity*, *integrity* and *availability* of the information. Most of these are connected with encryption methods and access methods of the network. From the nature of ad hoc networks, these methods are not centralized, but rather distributed. The availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANETs often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defence mechanism. ([2], [3]). Nodes in the MANET share the wireless medium and the topology of the network changes erratically and dynamically. In MANET, breaking of communication link is very frequent, as nodes are free to move to anywhere. The density of nodes and the number of nodes are depends on the applications in which we are using MANET.

MANET has given rise to many applications like Tactical networks, Wireless Sensor Network, Data Networks, Device Networks, etc. With many applications there are still some design issues and challenges to overcome. In this paper we present the Flooding Attack under AODV protocol. So in next section we discuss about AODV protocol.

Figure 1: Mobile ad hoc network

II. AODV PROTOCOL

Ad hoc On-Demand Distance Vector (AODV) Routing is a routing protocol for mobile ad hoc networks (MANETs) and other wireless ad hoc networks. It is jointly developed in Nokia Research Center, University of California, Santa Barbara and University of Cincinnati by C. Perkins, E. Belding-Royer and S. Das[4]. AODV is subclass of Distance Vector Routing Protocols (DV). In a Distance Vector every node knows its neighbours and the costs to reach them. A node maintains its own routing table, storing all nodes in the network, the distance and the next hop to them. If a node is not reachable the distance to it is set to infinity. Every node sends its neighbours periodically its whole routing table. So they can check if there is a useful route to another node using this neighbour as next hop. When a link breaks a Count-To- Infinity could happen. AODV is an 'on demand routing protocol' with small delay. That means that routes are only established when needed to reduce traffic overhead[5]. AODV supports Unicast, Broadcast and Multicast without any further protocols. The Count-To-Infinity and loop problem is solved with sequence numbers and the registration of the costs. In AODV every hop has the constant cost of one. The routes age very quickly in order to accommodate the movement of the mobile nodes. Link breakages can locally be repaired very efficiently. To characterize the AODV with the five criteria used by Keshav AODV is distributed, hop-by-hop, deterministic, single path and state dependent. AODV uses IP in a special way. It treats an IP address just as an unique identifier. They are implemented as subnets. Only one router in each of them is responsible to operate the AODV for the whole subnet and serves as a default gateway. It has to maintain a sequence number for the whole subnet and to forward every package. AODV defines three types of control messages for route maintenance:[6]

RREQ – A RouteRequest carries the source identifier, the destination identifier, the source sequence number , the destination sequence number, the broadcast identifier , and the time to live (TTL) field. Destination sequence number indicates the freshness of the route that is accepted by the source. When an intermediate node receives a RouteRequest, it either forwards it or prepares a RouteReply if it has a valid route to the destination. The validity of a route at the intermediate node is determined by comparing the sequence number at the intermediate node with the destination sequence number in the RouteRequest packet. If a RouteRequest is received multiple times, which is indicated by the source identifier-broadcast identifier pair, the duplicate copies are discarded. All intermediate nodes having valid routes to the destination, or the destination node itself, are allowed to send RouteReply packets to the source

RREP - As the RREP propagates back to the source, nodes set up forward pointers to the destination. Once the source node receives the RREP, it may begin to forward data packets to the destination. If the source later receives a RREP containing a greater sequence number or contains the same sequence number with a smaller hopcount, it may update its routing information for that destination and begin using the better route. The reason one can unicast the message back, is that every route forwarding a RREQ caches a route back to the originator.

RERR - As long as the route remains active, it will continue to be maintained. A route is considered active as long as there are data packets periodically travelling from the source to the destination along that path. Once the source stops sending data packets, the links will time out and eventually be deleted from the intermediate node routing tables. If a link break occurs while the route is active, the node upstream of the break propagates a route error (RERR) message to the source node to inform it of the now unreachable destination(s). After receiving the RERR, if the source node still desires the route, it can reinitiate route discovery.[7]

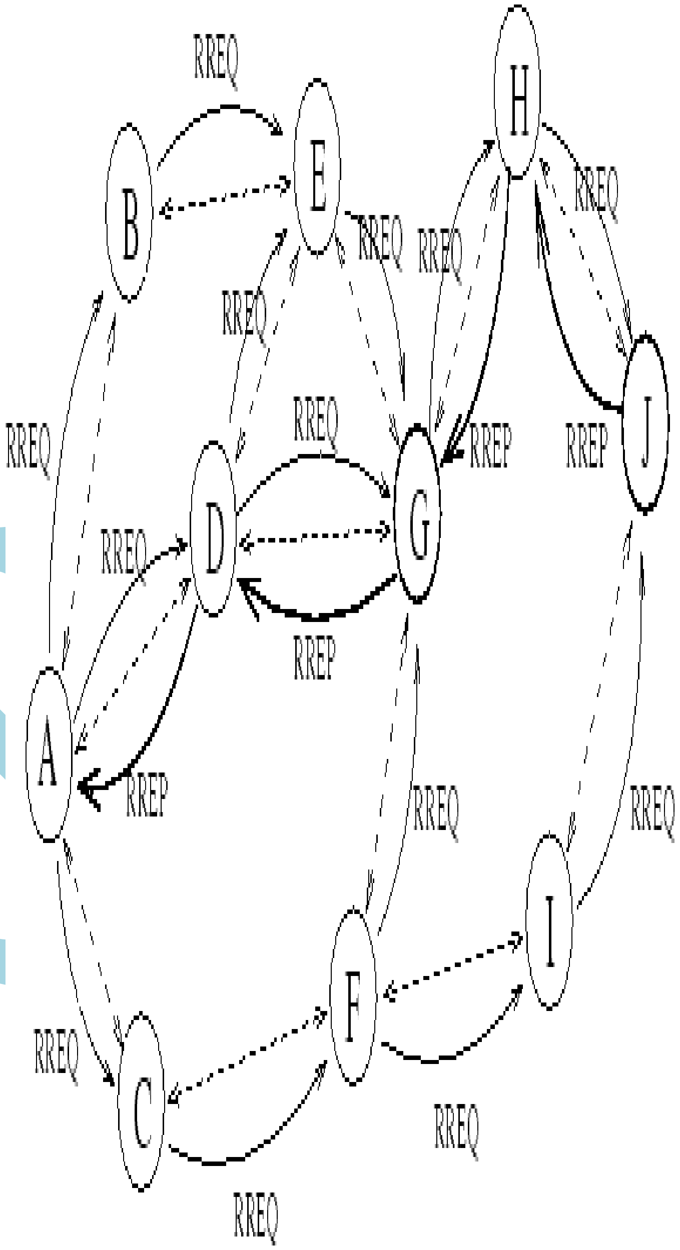

Figure 2: A possible path for a route reply if A wishes to find a route to J.

Here the node A need to set up a route to node J.

1. To establish the route, A needs to broadcast RREQ packet to all the other neighboring nodes in the network.
2. When node J receives the RREQ packet, it sends back a RREP packet.
3. This packet is unicasted to the sender node (ie A) through the other neighboring nodes.

III. PROBLEM STATEMENT

We have selected AODV routing protocol for our study. In our work we have analyzed the performance of the AODV routing protocol under the presence of flooding attack. To analyze how much the performance of the network deteriorates under the presence of attack we have taken the various network parameters via throughput, packet delivery ratio and end to end delay. We have taken five scenarios for our study. Keeping the total number of nodes to be fixed to 30 we have varied the number of attacker nodes firstly three then four then five and then six and then finally seven. From our network simulation we would try to analyze the impact of the increase in the number of attacker nodes in the network. The simulation work is carried out using the NS 2 simulator. We compared the results of these simulations to understand the network and node behaviours. The results of the simulation show that the packet loss increases in the network by increasing the number of flooding nodes. Mobile Ad hoc networks may also experience packet loss due to parameters employed. In our four simulations of network, we noticed that the variation of data loss due to network parameters such as the distribution of the nodes changed.

IV. RESULTS

We compared the results of these simulations to understand the network and node behaviors. The results of the simulation show that the packet loss increases in the network by increasing the number of flooding nodes. Mobile Ad hoc networks may also experience packet loss due to parameters employed. In our four simulations of network, we noticed that the variation of data loss due to network parameters such as the distribution of the nodes changed.

Throughput:

The average rate at which the total number of data packet is delivered successfully from one node to another over a communication network is known as throughput. The result is found as per KB/Sec. It is calculated by

Throughput= (number of delivered packet * packet size) / total duration of simulation

The results of the simulation show that the throughput in the network decreases by increasing the number of flooding nodes in the network. It is obvious that the throughput for the case with AODV, without attack, is higher than the throughput of AODV under attack as also shown in figure 3. The throughput keeps on decreasing as the numbers of malicious nodes are increased in the network keeping the total number of nodes constant in each scenario. This is because of the fewer routing forwarding and routing traffic. Here the malicious node discards the data rather than forwarding it to the destination, thus effecting throughput.

As throughput is the ratio of the total data received from source to the time it takes till the receiver receives the last packet. A lower delay translates into higher throughput. The overall low throughput of AODV is due to route reply. As the malicious node immediately sends its route reply and the data is sent to the malicious node which discard all the data. The network throughput is much lower.

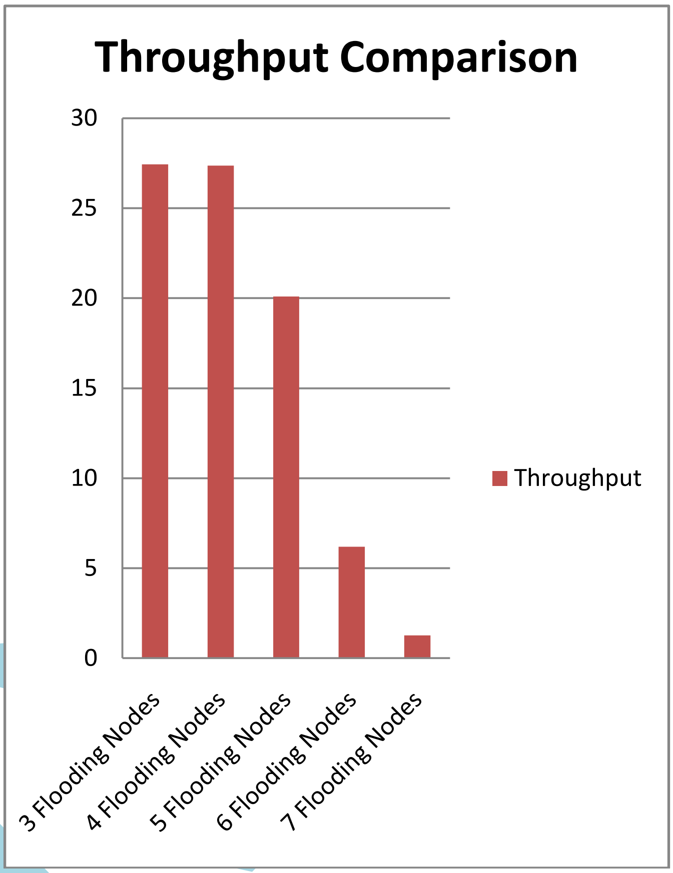

Figure 3: Throughput comparison with Flooding Nodes

Packet delivery Ratio (PDR):

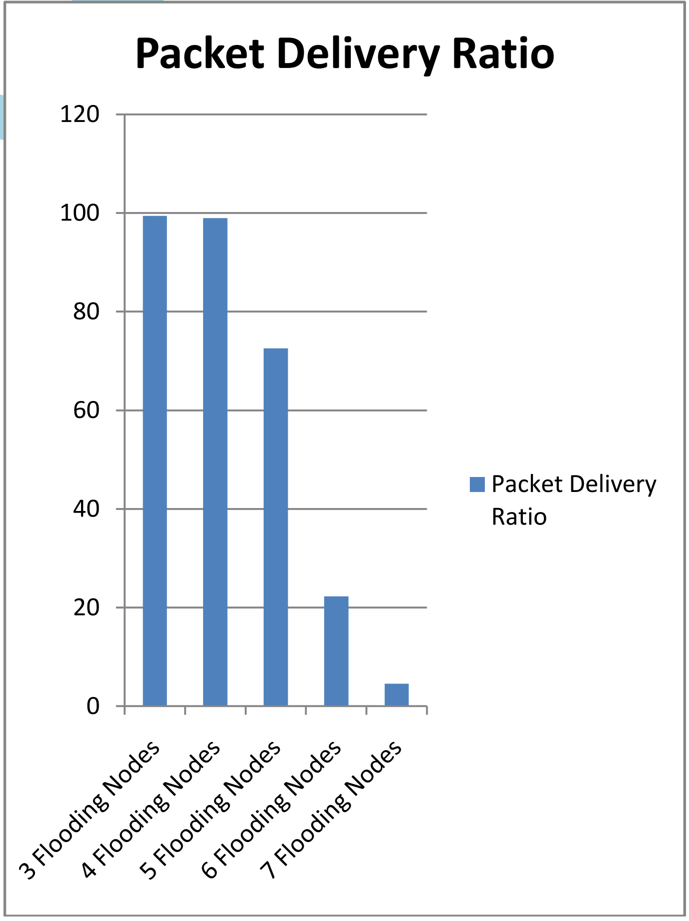

Figure 4: Packet Delivery ratio with Flooding Nodes

This is the ratio of total number of packets successfully received by the destination nodes to the number of packets sent by the source nodes throughout the simulation. It also describes the loss rate that of the packets, which in turn affects the maximum throughput that the network can support.
PDR= (Packets Received / Packets Sent)
This is due to increased congestion in the routes due to the false route requests generated in the network by the flooding attacker nodes. As the number of such nodes are increased in the network packet delivery ratio for AODV routing protocol decreases because of the increase in the false route requests generated in the network as shown in figure 4

End to End delay
End-to-end Delay: the average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted.
∑ (arrive time – send time) / ∑ Number of connections

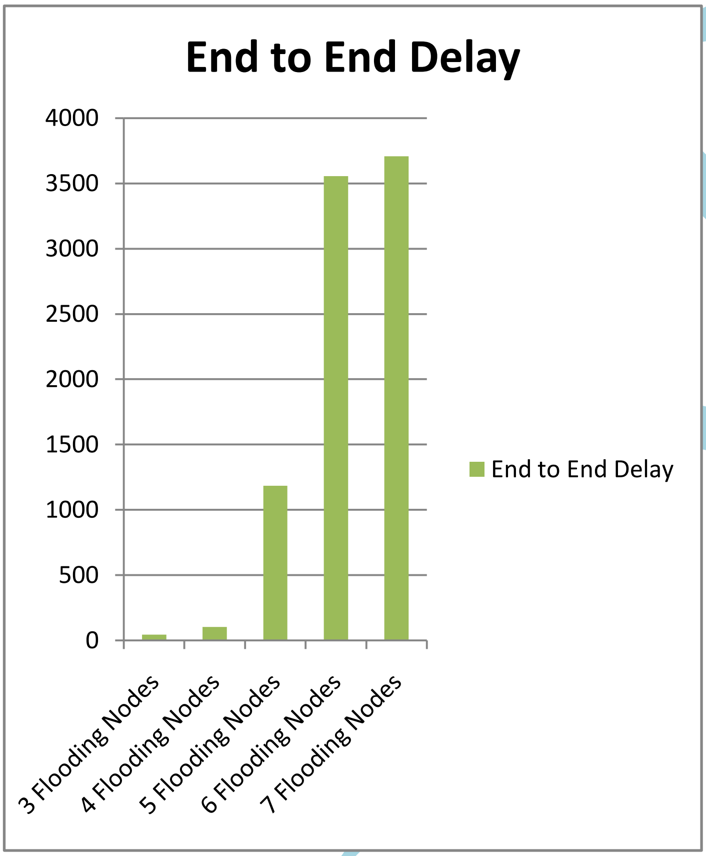

Figure 5: End to End Delay with Flooding Nodes

The results of the simulation show that the number of packets successfully delivered in the network decreases by increasing the number of attacker nodes in the network. This is due to the fact that more and more number of packets is dropped because of the increased congestion created by the flooding nodes. Since the packet drop is increased the more and more retransmissions are required for the successful delivery of the packets. More and more retransmissions leading to more end to end delay.

V. PROPOSED WORK

Generally, it is the case that a node does not send a message to a specific node, because of network topology discovery purposes. Then the transmission is done primarily by using flooding technique. That is the transmission of the message without designating a destination node and sending to any available node at the transmission range of the sender. This technique is very useful method for neighbor discovery. Neighbor nodes for a node S are the nodes that S can send/receive message directly.

VI. CONCLUSIONS AND FUTURE SCOPE

In our study, we analyzed effect of the Flooding Attack in an AODV Network. For this purpose, we implemented an AODV protocol that behaves as Flooding Attack in NS-2. We simulated five scenarios where each one has 30 nodes that use AODV protocol and also simulated the same scenarios after introducing firstly three Flooding Attack Node then four then five then six and finally seven into the network. Our simulation results are analyzed below: Having simulated the Flooding Attack, we saw that the packet loss is increased in the ad-hoc network. The overall end to end delay is also increased in the network. If the number of Flooding Attack Nodes is increased then the data loss would also be expected to increase. Thus from our simulation study we conclude that the flooding attack degrades the performance of the network. The more the number of attacker nodes the more severe the impact of attack.
We simulated the Flooding Attack in the Ad-hoc Networks and investigated its affects. In our study, we used the AODV routing protocol. But the other routing protocols could be simulated as well. All routing protocols are expected to present different results. Therefore, the best routing protocol for minimizing the Flooding Attack may be determined. In our thesis, we try to simulate the flooding attack effect in the network. But detection of the Flooding Attack Node is another future work. There are many Intrusion Detection Systems (IDS) for ad-hoc networks. These IDSs could be tested to determine which one is the best to detect the Flooding Attack. Additionally, we used UDP connection to be able to count the packets at sending and receiving nodes. If we had used the TCP connection between nodes, the sending node would be the end of the connection, since ACK packets do not reach the sending node. This would be another solution for finding the Flooding Attack Node. This takes place after the route determination mechanism of the AODV protocol and finds the route in a much longer period. Finding the Flooding Attack node with connection oriented protocols could be another work as a future.

VII. REFERENCES

[1] C.E.Perkins and E.M.Royer, “Ad-Hoc on Demand Distance Vector Routing”, Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, pp.90-100, Feb, 1999.
[2] S. Bouam and J. B. Othman, “Data Security in Ad hoc Networks using MultiPath Routing,” in Proc. of the 14th IEEE PIMRC, pp. 1331-1335, Sept. 7-10, 2003.
[3] Gagandeep, Aashima and Pawan Kumar “Analysis of Different Security Attacks in MANETs on Protocol

Stack". International Journal of Engineering and Advanced Technology (IJEAT), Volume-1, Issue-5, June 2012.

[4] Perkins, C.; Belding-Royer, E.; Das, S. (July 2003). Ad hoc On-Demand Distance Vector (AODV) Routing. IETF. RFC 3561. Retrieved 2010-06-18

[5] Mobile Ad Hoc Networking Working Group – AODV http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv

[6] IETF Manet Working Group AODV Draft http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv-08.txt

[7] A. Jamalipour, "Self-organizing networks [message from the editor-in-chief]," IEEE Wireless Communications, vol. 15, no. 6, pp.2-3, Dec. 2008.