Aman Yadav et al. International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 3, Issue 2, June 2016, pp. 162-164

Improvement for Flooding Attack in MANET Using AODV Protocol

Aman Yadav[1], Ms. Parul Dua[2]

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

Abstract— **This paper provides the performance analysis of AODV routing protocols under the effect of flooding attack. The actual performance of the routing protocols always degrades when the network is under the influence of any kind of denial of service attack. A Mobile Ad-Hoc Network (MANET) is a type of** ad hoc network **that switches the locations and or it can rearrange itself on the fly. Because MANETS are mobile, it uses wireless connections to connect to various networks. This can be a standard LAN connection, 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 desktop computers), while others may be connected to the Internet. For example, A Vehicular Ad Hoc Network (VANET), is a type of MANET that allows vehicles to communicate with roadside equipment. Sometimes the vehicles may not have a direct Internet connection; In that case wireless roadside equipment may be connected to the Internet, allowing data from the vehicles to be sent over the Internet. Vehicle data used to measure the traffic conditions or trucking fleets. 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 black hole attack, wormhole attack etc.**

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].

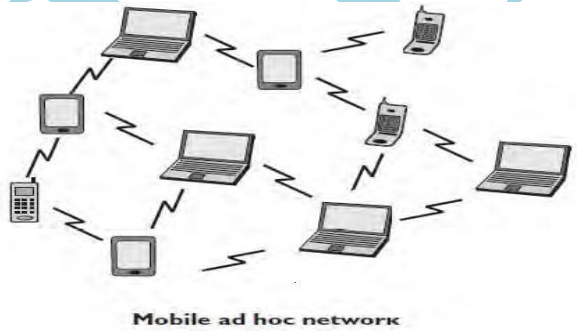

Figure 1: Mobile ad hoc network

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]).In this paper we present the Flooding Attack under AODV protocol. So in next section we discuss about AODV protocol.

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.

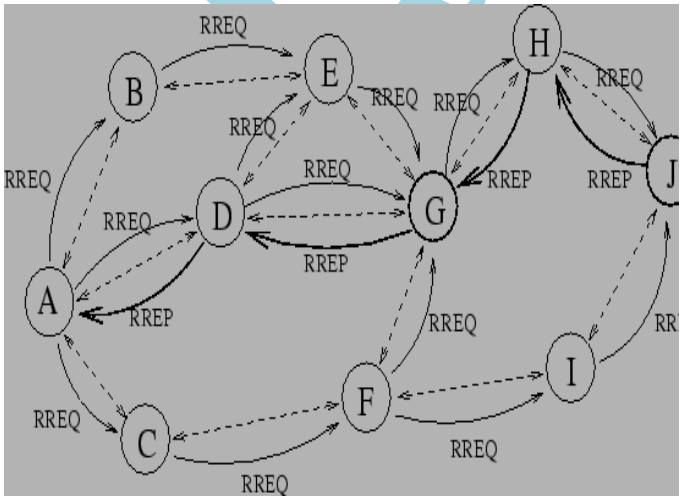

Figure 2: A possible path for a route reply if A wishes to find a route to J.

III. FLOODING ATTACK

The flooding attack is an attack that attempts to cause a failure in a computer system or other data processing entity by providing more input than entry can process properly [7]. Flooding is a type of Denial of Service (DoS) attack in MANET. Intentional flooding may lead to disturbances in the networking operation. This kind of attack consumes battery power, storage space and bandwidth. Flooding the excessive number of packets may degrade the performance of the network. Their study considers hello flooding attack. As the hello packets are continuously flooded by the malicious node, the neighbor node is not able to process other packets. The functioning of the legitimate node is diverted and destroys the networking operation. Absence of hello packet during the periodical hello interval may lead to wrong assumption that the neighbor node has moved away. So one of the intermediate neighbor nodes sends Route Error (RERR) message and the source node reinitiates the route discovery process. In a random fashion the hello interval values are changed and convey this information to other nodes in the network in a secured manner. This study identifies and prevents the flooding attack. This methodology considers the performance parameters such as packet delivery ratio, delay and throughput. The algorithm is implemented in Secure AODV and tested in ad hoc environment. Flood attacks occur when a network or service becomes incapable of providing service to its clients, thereby causing incomplete connection requests. By flooding a server or host with connections that cannot be completed, the flood attack eventually tries to fill the host's memory buffer thereby not accepting further connections, which causes a Denial of Service attack. ([8],[9])

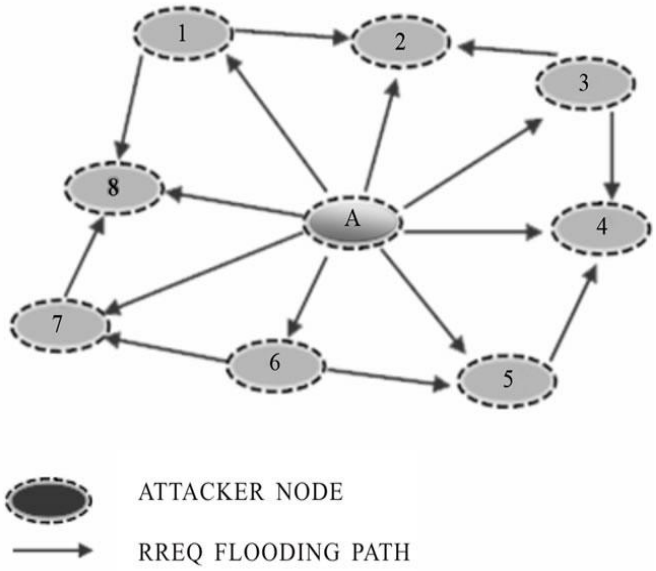

Figure 3 the RREQ flooding attack.

Effect of Flooding Attacks:-

Flooding Attack can seriously degrade the performance of reactive routing protocols and affect a node in the following ways.[10]

(a) Degrade the Performance in Buffer:-The buffer used by the routing protocol may exceed the limit since a reactive protocol needs to buffer data packets when the RREQ packets are being sent by the source node. Also, if a large number of data packets originating from the application layer are actually unreachable, genuine

data packets in the buffer may be replaced by these unreachable data packets, based on the buffer management scheme used.

(b) Degrade the Performance in Wireless Interface: - the buffer used by the wireless network interface may overflow due to the large number of RREQs sent in the route discovery process. Similarly, genuine data packets may be dropped if routing packets have higher priority over data packets.

(c) Degrade the Performance in RREQ Packets:- Since RREQ packets are broadcasted into the entire network, the increased number of RREQ packets in the network leads to more collision in MAC layer and thereby congestion in the network and delays for the data packets. Protocols like TCP that is sensitive to round trip times and congestion in the network gets affected.

IV. EXPECTED RESULTS

We have selected AODV routing protocol for our study. In our work we have analysed the performance of the AODV routing protocol under the presence of flooding attack. To analyse 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 analyse 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.

V. CONCLUSION

We simulated the Flooding Attack in the Ad-hoc Networks and investigated its affects. In this paper, we used the AODV routing protocol, Flooding Attack and their impact on MANET. 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 this paper, we try to simulate the flooding attack effect in the network. Having simulated the Flooding Attack, we saw that the packet loss is increased in the ad-hoc 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.

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.

[8]. Madhavi, S. and K Duraiswamy “Flooding Attack Aware Secure AODV.” Journal of computer science, 9 (1): 105-113, 2013

[9]. S. Saraeian, F. Adibniya, M. G. Zadeh and S. A. Abtahi, “Performance Evaluation of AODV Protocol under DDoS Attacks in MANET,” World Academy of Science, Engineering and Technology, Vol. 45, 2008, p. 501.

[10]. M. B. Guddhe and M. U. Kharat, “Core Assisted Defense against Flooding Attacks in MANET,” 2009. http://www.nsnam.org

