A New Technique for AODV Based Secure Routing with Detection Black Hole in MANET

Kulwinder singh[1], Shilpa sharma[2]
Student of Lovely Professional University, India[1]
Assistant Professor, Dept of CSE, Lovely Professional University, India[2]
[1]kulwindersingh4526@gmail.com, [2]shilpa.sharma@lpu.co.in

Abstract- MANET is dynamic, self-organised and infrastructure less network. That has multiple nodes whose provide a temporary infrastructure of nodes for establishing connections and transfer information. According to MANET nature, there are many possible attacks, the Black hole is one of them. MANET has various routing structure. AODV is reactive routing protocol. We have various techniques for maintains secure platform from attacks. But according to nature of the network, there are high possibilities of attack malicious node. That is a reason of loss packets. There is much technique, who are suggested by various experts. This paper work is related to identify the malicious node with help of creating black list and route addresses. In here HOP counts and SN used from previous techniques. Route addresses refer to route addresses and node addresses. The black list is a list of an inspected maliciously route. There will be helpful for ease identification of attacker nodes.

Keywords: - MANET, AODV, HOP, SN

I. INTRODUCTION

In the traditional network systems, there are many fixed points, those known as base stations, who's helped for connecting the devices. But in those, if devices may change location or leave the range, then the whole connection is aborted. Wireless environment is more effective, in that scenario information is transferring anywhere with a better connectivity through of the electrical signals [1]. That environment of Networks is a reason of resolution in the networking sector. Mobile Ad Hoc network is a focus point for research for its flexibility and simple, easy installations. It uses limited resources and provides the easily deployed structure. Nodes work within the group for establishing a co-operation between each other's for manage route to transfer the packets source to destination [2]. MANET has dynamic topology, open medium for transitions and no clear central control management.

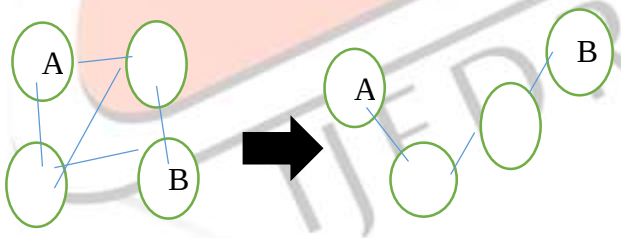

Fig.1 Nodes topology in MANET

In the Fig 1. Shows the host movement and topology changed frequently. In the MANET nodes has capable of changing their positions and links in the network. There has no cellular infrastructure, there are multiple HOPs in a wireless network. Data must be forwarding via selected route with help of various node, those provide services as intermediate [5].

Classification of MANETs routing protocols:-

MANETs has three categories regarding routing protocols:-

Reactive protocol: - These are on demand driven reactive protocol. These protocol helps to set the route when demanded. These protocols establish the routed source to destination on time for transfer the information through packets. Bandwidth between sources to the destination will measure the node transmitting packets to one node to another node up to destination node. In this method RREQ sends by the source node to destination and RREP having a description of the route through the various nodes will be examined. Source node takes path according to SN and HOP counts and RRER recognize the errors between paths after a specific updating if the node is changed and notify for new discover new path [2].

Proactive Protocol*: -* that protocols work on the method to find out the route from the previous reactive protocols. That protocol use previous path who has used for establishing the network. In the network whole nodes, information is kept in form of tables. These tables help to analyze information about the various routes and regarding theirs updating up to previous one route changes. That information provides to source node any time for choose route. We have Optimized Link state Routing Protocol as an example of that's topology.

Hybrid protocol: - this protocol manages to route on the basis of the use of reactive and proactive protocol according to specific demand of structure for forwarding packets

In this section we discuss some popular routing algorithms proposed for MANETs:-

Destination Sequence Distance Vector Protocol: - that is an improved version of classical Bellman-Ford routing algorithm. A node holds the information about all possible routes in the Routing Information Table for transfer packets with help of possible hops for transfer paths to the destination. Node has two tables one for forwarding packets and one manages the incremental routing packets for transfer. If the topology changes then node sends an update information about the packet to their neighbor's nodes in the network.

Dynamic Source Routing Algorithm*:* -that protocol prefers to source routing, in that packets have header holds the routed information with the list of nodes for a pass route. Hope by hop mechanism is not used. That has advantage that there has no requirement for collect information about routing paths updating .network is not use the route for a long time to destination.

Temporally Ordered Routing Algorithm: -works on discovering on demand structure that provide multiple routes for transfer packet and conform routes fast as well as possible. It has link reversal technique. A node broadcast a QUERY packet that helps to address a destination for identifies the route. That packet still works up to reach the particular destination. If any information may be provided about close the route from the node then that packet node find out new neighbors for reach the destination. In here the shortest topology is not more importance.

Ad Hoc On-Demand Distance Vector (AODV):- AODV has been developed for MANET and it standardized by IETF.it works for the on demand route search. It comes in a reactive protocol [6].

AODV is working two types of modules for search and maintains route-

Search route: - AODV demands route from various nodes at a specific time period for transfer packets. These routes may be changed during another call for transformation. So, it mandatory that every time allocation of the effective fresh path for through nodes. RREQ transfer by a source node to another node to check out various possible paths to the destination. A destination node provides the RREP as the response regarding path for sending the packet with identified the nodes of the path. That RREP helps in generate the HOP counts and SN regarding paths.

Route maintainer: - In the network, if any node updating accords, that effective trans motion of packets, that information will be provided through RRER from the path of nodes. If any change is happening then a source node restart process of discovering route in a new established environment of the node, which holds new relations between nodes in the network.

Black hole attack: - AODV routing structure faces various types of attacks. One of those is black hole attack. This attack is related to the malicious node that uses routing protocol and determines itself for having the shortest path for transfer packet to the destination node. The malicious node determines itself with help of providing the response to the request from the source node. In the table of responses from the various nodes according to low HOP and high SN show by the malicious node route. If source node provides the packet to a route of the malicious node then the malicious node take the packet. According to Fig 2. In their malicious is a part of whole nodes. This node is a reason of packets dropping. That node will try for capturing packet with fake identification.

There are two major possibilities that either malicious node will drop the packet or send to another unexpected path. Whole times the packets go waste.

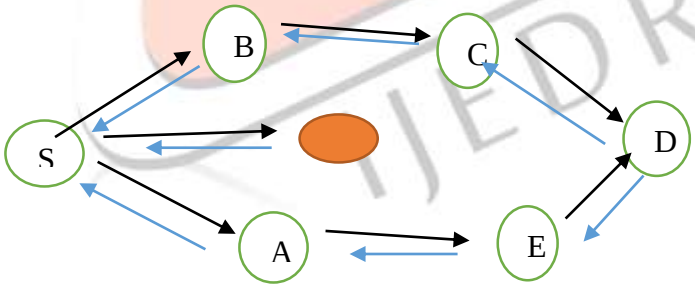

Fig 2. Malicious node in MANET

II. LITERATURE SURVEY

Author Singh et al in this[6] the focus point for evaluating the malicious attack with help of comparing the DSN and SSN .if in here DSN is very greater from the SSN then that route response reply will be discarded.

In [5] according to theirs, method peak value will be adopted for check out the RREPs. The peak value is calculated with using values of RREP sequence number. Sequence number and numbers of replies count in the table within the particular time slots as RREPs. Peak value helpful for generating result according to compare DSN and peak value. IF DSN has the higher value than the peak value then that route is discarded.

Author Raj et al [7] the proposed technique is working on encryption. The public key used theirs for secure the message and responses during the RREQ acknowledgment. The pubic key used for encryption of message and decryption message by the source node and destination node. The sender encrypts the message by receiver public key and destination node uses the public key of the source node. If another RREPs comes that will be discarded.

According to Author Sachan et al in [8] used the technique of authentication of nodes and message with help of Hash MAC. That is the secure platform for authentication without any problem of a number of keys distributions. HMAC provide shared the

key to whole nodes that are the source, intermediates node, and destination. That helps to easily authentication message and nodes during the specific route source to destination.

Proposal method in [9] according to the source node takes RREPs from whole routes. The table counts various hops from the route. These value store until the timer expired. Then the source node checks out any hop is repeated if is there in the network after the timer expired. That hop shows the secure route from source to destination.

Author kshirsagar et al [10] provide the method for determining the nodes in the route with examining them with send numbers of packets. Neighbour node will obtain packets if that generate RREP and send packets to another node. If that do not forward packets to another node that recognizes as a malicious node and marked it.

According [11] in that method a further route request (FRREQ) send to the next hop node of RREP generator of next node. In here assumption is required in that we that there will not any malicious node in next hop node in the route. If there will be any malicious node that will no reply of the request. There will be the malicious node. That route will be marked as rejected route.

In the proposed method [12] is a use of trust field. Trust field used for assign the trust values to the nodes. Intermediate nodes generate trust values from accepted RREQ from the source node. The destination node provides trust values of nodes with RREP to the source node. Source node will select the highest trust value node from whole trust values. That route will be select for send the packets between sources to the destination node.

Author varshey et al [13] provide the method of detected malicious node in the AODV. That provides the Watchdog AODV (WAODV) for taking ensures selected node will forward the packet to next node in the route until packets received to the destination node. Any node will detect as a misbehavior on t node at the time of examination by Watchdog, then no packets will be sent to that particular path. Any other node or path will select by Watchdog.

According to [2] in that proposed method a specific threshold will be used for detection of fake RREP from the malicious node. That value will be updated automatically. Node provides SN to the source node that SN value will check with a threshold value. If RREP node SN has the higher value than the threshold, where that node will exit that route has the malicious node.

III. PROPOSED METHOD

Assumption:-

- Source node has storage capacity according to demands of storage value.
- There are multiple routes for forwarding packets source to destination
- Source node determines the routes by specific binary value.
- Each and every node identify by using specific binary value and route binary value, that combination of values identify source and destination.
- Hop will be count according to routes of Sequence Number of nodes will be determined.
- Hop and SN help for selecting the route for forwarding packets.

This arrow recognize the RREQ and identify the route with route address

This arrow identifies the route from D to A, with hold hop counts, SN and Route and unique node addresses. In here proposed method is work on two basic terms identify node by using the address of route and node.

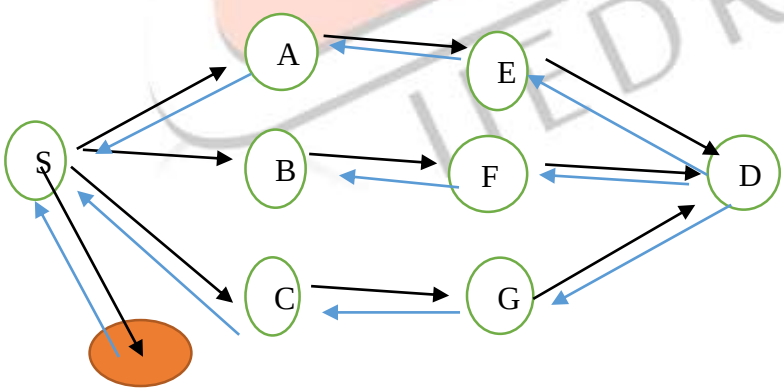

Fig 3. Route identification and maliciously attack detection in MANET

According to Fig 3. And Fig 4. Blacklist of maliciously route Source sends RREQ to the nearest node to recognize for the destination. Source node provides unique bits address to that route request. That RREQ will send with route address.

Flow Graph is explained whole steps regarding methodology working. Black list and node's addresses are held by the source that will store the information about the possible routes.

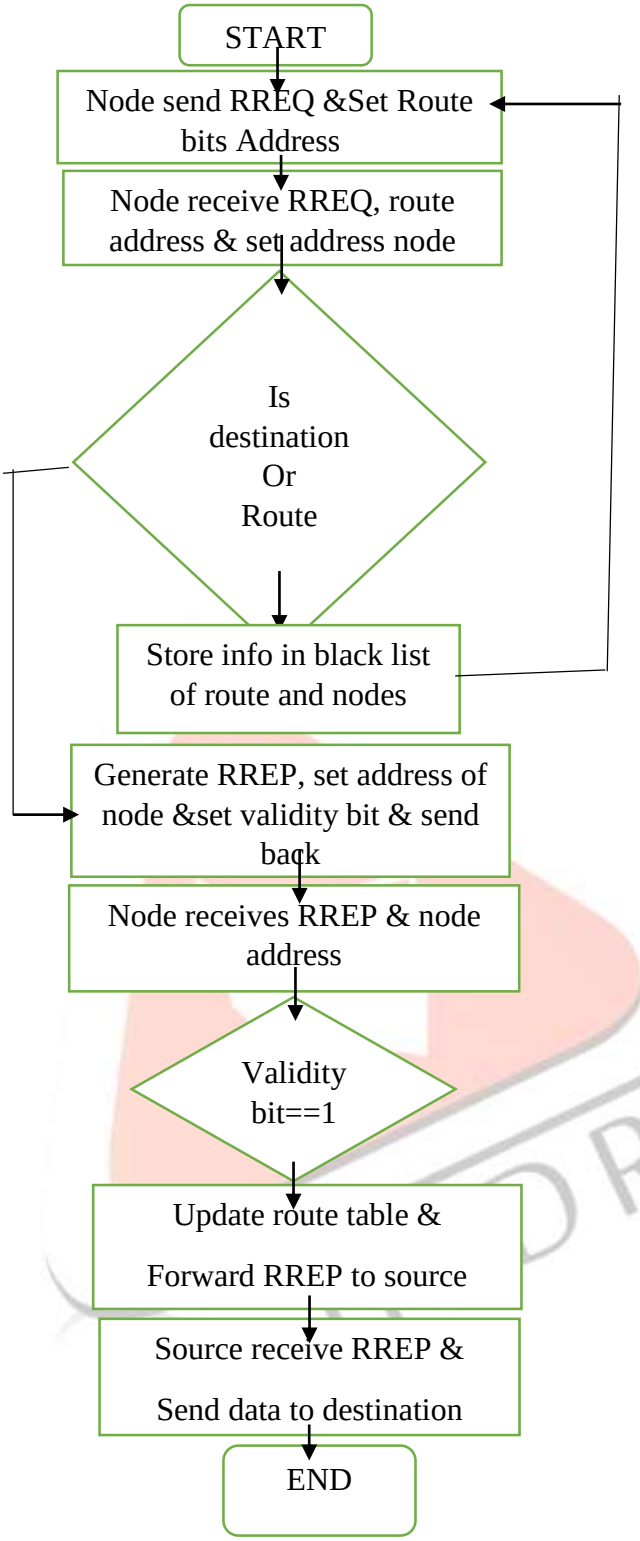

Fig 4. Flow Graph of Proposed Technique

According to proposal method, the source node will send RREQ to the destination through intermediate nodes. That RREQ has also a specific bit combination for determining that particular route from the destination. That RREQ receives to the node that will be identified by route binary value and node specific bits value's combination. Whole nodes of the route will be identified by these unique values. The destination node will reply to the destination with hop, SN, and unique bits values that help for identifying route for forwarding packets. If there is any malicious node then that route binary value return only route value, which does not provide unique bits for node identification values. That will recognize as that node have no any neighbour for forwarding packets to next node. That route will discard from the list of routes for send packets. According to AODV nature, if any node will establish itself old to a new route, that will be easily identified between specific slot times.

Destination provides the RREP with verify route and identify nodes. Source node obtains the hop counts, SN and route addresses.

Route information will be updated before selected path. That route has no destination, that will keep in blacklist and route will be discarded. After that whole route will check as their hop and SN. The route that will have the lowest hop and highest SN that will select for forwarding packet, If after update any node will change their position, that can recognize which route that belonged. In here the addresses of route and node will be fixed after authentication. If any new will be added that have mandatory to obtain addresses for adding itself into the route.

IV. CONCLUSIONS AND FUTURE WORK

Mobile wireless networks like MANET provides an open medium for connectivity that is a reason for various security threats. AODV is reactive protocol the help for establishing routes for forwarding packets. There are HOP counts and SN helps to eliminate attacks of the black hole. In our proposed method we provide a technique of recognizing route and node by using addresses. That is helpful to recognize maliciously attacks. In that malicious route will be blacklisted. In proposal technique source node has a specific storage for store the information regarding addresses of the route, HOP, SN and updating information according to nodes will store.

According to nature of nodes behaviors, it is required to solve the problem of identifying nodes who's left one route to another route, identify malicious node traveling in the network.

REFERENCES

[1] H. Lan Nguyan and U. Trang Nguyan, "A Study of different types of attacks on multicast in mobile ad hoc networks", Ad Hoc Network, Vol.6, NO.1, 2007

[2] Sagar R Deshmukh, P N Chatur, Nikhil B Bhople, "AODV-Based Secure Routing Against Black hole Attack in MANET", IEEE International Conference On Recent Trends In EICT, May 20-21,2016

[3] M. Medadian, A. mebadi and E. Shahri, "Combat with Black hole Attacks in AODV Routing Protocol", in Proceedings of the 2009 IEEE 9th Malaysia International Conference on Communications, pp 550-535, 2009.

[4] Yibeltal Fantahun Alem, Zhao Cheng Xuan, "Preventing Black Hole Attack in Mobile Ad Hoc Networks using Animally Detection", 2nd International Conference on Future Computer and Communication 2010.

[5] R. Jhaveri, S.Patel, D.Jinwala, "A Novel Approach for Gray hole and Black Hole Attacks in MANETs", Int. conf. on Advanced Computing & Comm. Technologies, 2012.

[6] H.Singh, M.Singh, "Securing MANET Routing Protocol under Black Hole Attack", IJIRCCE, 2013.

[7] P.Raj, P.Swades, "DPRAODV: A Dynamic Learning System against Black Hole Attack in Aodv Based Manet", IJCSI Issues, Vol 2, 2009.

[8] P.Sachan, P.Khilar, "Securing AODV Routing Approach to Overcome Black Hole Attack in MANETs", International Journal of Innovations in Engineering and Technology, 2013.

[9] V. Sankaranarayanan, "Prevention of Black Hole attack in MANET", IEEE, 2007

[10] D. Kshirsagar, D. Patil, "Black hole Attack Detection and Prevention by Real Time Monitoring", IEEE, 2013

[11] R. Sharma, R. Shrivastava, "Modified AODV Protocol to Prevent Black Hole Attack in MANET", International Journal of Computer Science and Network Security, 2014.

[12] T. Ghosh, N. Pissinou, K. Makki, "Collaborative Trust-Based Secure Routing against Colluding Malicious Nodes in Multihop AdHoc Networks", International Conference on Local Computer NW, IEEE.

[13] T. Varshney, T. Sharmaa, P. Sharma, "Implementation of Watchdog Protocol with AODV in MANET", International Conference on Communication Systems and Network Technologies, IEEE 2014