Secure Routing with Detection Black Hole in MANET: A Study

Kulwinder singh[1], Shilpa sharma[2]

Student of Lovely Professional University, India[1]

Assistant Professor, Dept of CSE, Lovely Professional University, India[2]

ABSTRACT: - MANET is dynamic, self-organised and less infrastructure network. That has multiple nodes whose provide temporary infrastructure of nodes for establishing connections and transfer information. MANET is facing various types of attacks, Black hole is one of them. In there that survey paper shows various updated work on Black hole attack in using various protocols. In that paper our work in related to examine to research and proposed techniques to detection of the malicious node in AODV infrastructure in MANET. The proposed method in papers in this paper focuses on AODV. Our research work is related to use of HOPs and SN from the established network and propose technique for better use of HOPs and SN with using Blacklist and identification of excited nodes in Networks.

Keywords: - MANET, AODV, HOPs, SN.

I. INTRODUCTION

MANET basically related to an ease deployed infrastructure for connect the various types of devices for communication. That is based on wireless infrastructure that manage the transfer of information with help of nodes. As nature of MANET nodes are medium of transfer the information. These nodes has no fixed platforms. Devices whose are connected to through of that infrastructure that are not fixed [1].

According to nodes that will in network in multiple times. That nodes transfer's information source to destination through of connection with each other. These nodes are source of connected multiple devices in the Network.

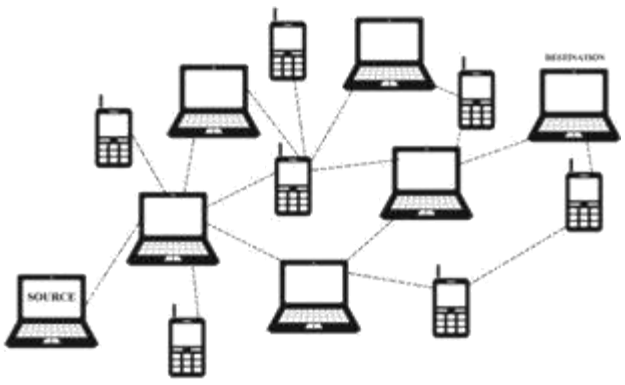

Fig. 1. Infrastructure of MANET

In the traditional network systems, there are many fixed points, those known as base stations, who's helped for connect the devices. But in those if devices may change location or leave range, then 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 networking sector.Mobile Ad Hoc network is a focus point for research for its flexibility and simple, ease installations. It uses limited resources and provide the easily deployed structure. Nodes work within the group for establish a co-operationbetweeneach 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.

In the diagram shows about the host movement and topology changed frequently. In the MANET nodes has capable to change their positions and links in the network. There has no cellular infrastructure, there are multiple HOPs in wireless network. Data must be forwarding via selected route with help of various node, those provide services as intermediate [7].

Classification of Ad Hoc Routing Protocols:-

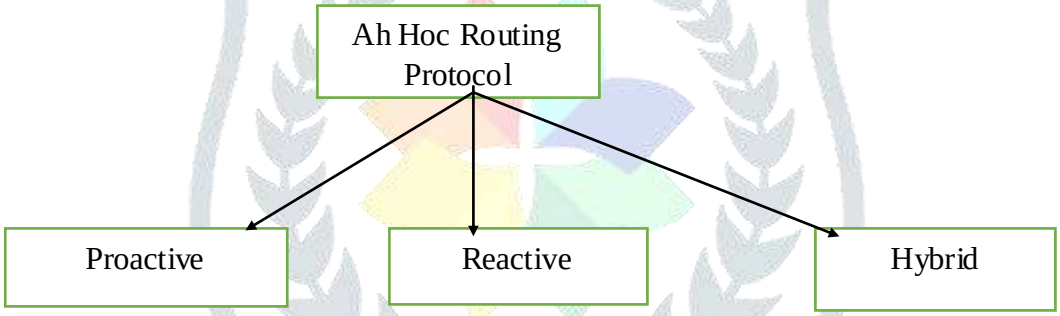

Fig 2. Ad Hoc routing Protocols

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 betweensources to destination will be measure then nose 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 route through the various nodes will be examine. Source node take path according to SN and HOP counts and RRER recognize the errors between paths after a specific updating if node are changed and notify for new discover new path.

Proactive Protocol: - that protocols works on the method to find out the route from the previous reactive protocols. That protocol use previous path who has used for establish the network. In the network whole nodes information is kept in form of tables. These tables helps to analyse information about the various routes and regarding to theirs updatingup to previous one route changes. That information provide

to source node any time for choose route. We have Optimized Link state Routing Protocol as an example of that's topology.

Hybrid protocol: - these protocol manage routing on the basis of use of reactive and proactive protocol according to specific demand of structure for forwarding packets. This protocol help to establish network with combination of proactive and reactive protocols features.

There are some populated routing algorithms in MANET:-

Destination Sequence Distance Vector Protocol: - that is a improve 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 destination. Node has two tables one for forwarding packets and one manage the incremental routing packets for transfer. If topology is change then node sends an update information about packet to theirs neighbour's nodes in the network.

Dynamic Source Routing: -that protocol prefers to source routing, in that packets has header holds the routed information with list of nodes for pass route. Hope by hop mechanism is not used. That have advantage that there have 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 discover 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 addressing a destination for identifies the route. That packet still work up to reach the particular destination. If any information may be provide about close the route from the node then that packet node find out new neighbours for reach the destination. In here the shortest topology is not more importance.

AODV*:* - it 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 are 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 change during another call for transformation. So, it mandatory that every time allocation of effective fresh path for through nodes. RREQ transfer by a source node to another nodes to check out various possible paths to destination. A destination node provide the RREP as response regarding to path for sending packet with identified the nodes of path. That RREP helps in generate the HOP counts and SN regarding to paths.

Route maintains: - In network if any node updatingaccords, that effective trans motion of packets, that information will be provide through RRER from the path of nodes. If any change is happen then a source node restart process of discover route in new established environment of node, which hold new relations between nodes in network.

Black hole attack: - AODV routing structure faces various types of attacks. One of those is black hole attack. This attack is related to malicious node that uses routing protocol and determine itself for having

the shortest path for transfer packet to the destination node. Malicious node determine itself with help of provide the response of 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 provide the packet to route of malicious node then the malicious node take packet. There are two major possibities that either malicious node will drop the packet or send to another unexpected path. Whole times the packets goes waste.According to fig 3. Source send RREQ to nodes for find out the destination. If there are nearest node is destination node that will reply. Otherwise that request will forwarding to node to another node. If malicious node is in network that sends RREP to destination for sure to that has shortest path or that is destination node. In case source will provide packet to that node then packet should be dropped or forward another unexpected nodes in network.

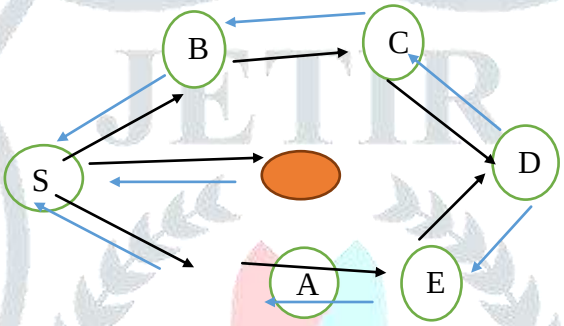

Fig 3. Malicious node in MANET

.

II. LITERATURE SURVEY

DurgeshWadbude et al [1] discussed that network topology changes frequently, therefore AODV, DSR are used for being efficient adaptive routing protocols. Security is the important challenge in Mobile Ad hoc Networks as the transmission medium is wireless. The attacks due to the misconduct of malicious nodes are modification, fabrication, masquerade and denial of service (DOS) attacks. In this paper, they proposed an efficient secure AODV routing protocol. On the basis of the simulation, the results show that the proposed routing algorithm provides a better security and network performance than the present works. The results obtained from the simulation shows the enhancement in the network performance, considering the overhead, and end to end delay to the secure AODV routing protocol.

Sanjay Ramaswamyet al[2] proposed the solution for identifying multiple black hole nodes . The solution is based on the modified AODV protocol by presenting the cross checking and data routing information table (DRI). In which the table is maintained for every single entry of the node. For the transfer of the packets the authors relied on the trusted nodes.

An algorithmic approach for improving the security of AODV protocol is introduced by Rajib Das et al with the ability to identify and remove the black hole nodes in MANET [3]. An extra (additional) route is proposed to the intermediate node and it can send RREPmessage to the source node for discovering the

path to the destination node is present or not. The proposed approach cannot be used to identify a cooperative black hole attack consists of many malicious nodes. Along with the routing table there is a data routing information (DRI) table which can be used for recognizing multiple black hole nodes. On simulating the proposed algorithm, it is observed that there is reduction in network throughput and packets delivery ratio.

Author singh et al in this[9] the focus point for evaluate the malicious attack with help of compare the DSN and SSN .if in here DSN is very greater from the SSN then the that route response reply will be discarded.

In [8] according to theirs method peak value will be adopted for check out the RREPs. Peak value is calculated with using values of RREP sequence number. Sequence number and numbers of replies counts in the table within the particular time slots as RREPs. Peak value helpful for generate result according to compareDSN and peak value. IF DSN has higher value than the peak value then that route is discarded.

Author Raj et al [10] the proposal technique is working on encryption. Public key used theirs for secure the massage and responses during the RREQ acknowledgement. Pubic key used for encryption of message and decryption message by source node and destination node. Sender encrypts message by receiver public key and destination node uses public key of source node. If another RREPs comes that will be discarded.

According to Author Sachan et al in [11]used the technique of authentication of nodes and message with help of Hash MAC. That is secure platform for authentication without any problem of number of keys distributions. HMAC provide shared the key to whole nodes that are source, intermediates node and destination. That helps to easily authentication message and nodes during the specific route source to destination.

Proposal method in [12] 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 check out any hop is repeated if is there in network after timer expired. That hop show the secure route from source to destination.

Author kshirsagar et al [13] provide the method for determine the nodes in the route with examine them with send numbers of packets. Neighbour node will obtain packets if that generate RREP and send packets to another node. If that do notforward packets to another node that recognize as a malicious node and marked it.

According [14] 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 request. There will be malicious node. That route will be marked as rejected route.

In the proposed method [15] is 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 provide trust values of nodes with RREP to 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 destination node.

Author varshey et al [16] provide the method of detected malicious node in the AODV. That provide the Watchdog AODV (WAODV) for take ensures selected node will forward packet to next node in the route until packets received to the destination node. Any node will detect as a misbehaviour on t node at time of examination by Watchdog, then no packets will be send to that particular path. Any other node or path will select by Watchdog.

According to [5] in that proposed method a specific threshold will used for detection of fake RREP from the malicious node. That value will be update automatically. Node provide SN to the source node that SN value will check with threshold value. If RREP node SN has higher value than threshold, where that node will exit that route has 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 determine 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 routesof Sequence Number of nodes will be determine.
- Hop and SN helps for select the route for forwarding packets.

According to proposal method the source node will send RREQ to destination through intermediate nodes. That RREQ have also a specific bit combination for determine that particular route from the destination. That RREQ receive to node that will be identify by route binary value and node specific bits value's combination. Whole nodes of route will be identify by these unique values. The destination node will reply to destination with hop, SN andunique bits values, that help for identify route for forwarding packets.

If there is any malicious node then that route binary value return only route value, that do 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 new route, that will be easily identified between a specific slot times.Destination provide the RREP with verify route and identify nodes.Source node obtains the hop counts, SN and route addresses.

Route information will be update before selected path.That route have no destination, that will keep in blacklist and route will be discard.After that whole route will check as theirs hop and SN. Route that will have lowest hop and highest SN that will select for forwarding packet, If after update any node will be change theirs position, that can be recognize which route that was belong. 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 add itself into route.

IV. CONCLUSIONS AND FUTURE WORK

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

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

REFERENCES

[1]DurgeshWadbude and VineetRichariya"An Efficient Secure AODV Routing Protocol MANET", International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 4, April -2012

[2]Sanjay Ramaswamy, Huirong Fu, ManoharSreekantaradhya, John Dixon and KendallNygard "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks".

[3]Rajib Das, BipulSyamPurkayastha and Prodipto Das "Security Measures for Black Hole Attack in MANET: An Approach".

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

[5] 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

[6] 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.

[7] YibeltalFantahunAlem, Zhao Cheng Xuan, "Preventing Black Hole Attack in Mobile Ad Hoc Networks using Animally Detection", 2nd International conference on Future Computer and Communication 2010.

[8] 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.

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

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

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

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

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

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

[15] 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.

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