Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 09, September-2016

Link Failure Detection and enhanced reliability in Mobile Adhoc Network

Supriya Pandey, Pratibha Devi Umesh
Technocrats Institute of Technology and Science
Bhopal, M.P. India

***Abstract* - Manet is a network which works on concept of having network without any infrastructure.Ad hoc network decreases the dependence of infrastructure and deploy the speed.The concepts dynamic source routing is based on the source routing which means the initiator of the packet provides an orderly list of nodes according to which packet traverses in the network.The packet delivery ratio is compared with the threshold value. If packet delivery ratio drop to the threshold value then Source node randomly choose the cooperative bait address, of one node neighbor to bait malicious node, then send bait request. If any node reply RREP from other route except neighbor node then start the reverse tracing program and send test packets, check messages to detect malicious node, source node list malicious node onto black hole list, set alarm packet and end the transmission. This paper proposed a novel method to find link failure detection in MANET. The experimental results showed that our method is well suited for MANET with DSR protocol.**

Keywords:Mobile adhoc network, link failure detection, reliability, security, DSR

I. INTRODUCTION

Digital information are growing using the networks of mobile devices anywhere at any time and becoming the need of today.Manet is a network which works on concept of having network without any infrastructure. Such network consists of mobile nodes which are free to move. They come together for a span of time for give and take process means to receive and give the information in return. All information is used by each device, can be assumed as producers and consumers in an ad-hoc network [1]. While nodes are moving in the network they interchange the information to each other and may continue to move here and there and so the network must be prepared. Ad hoc network decreases the dependence of infrastructure and deploy the speed. Mobile devices are not having the centralized control, therefore they are free to move, and hence the topology of such network changes expeditiously.MANET's[2] having number of node demands high quality of processing power, high bandwidth and memory to provide definite routing information, though induces traffic overhead in the network.Every mobile node is free to move in any ways and can change their link at any time.AODV[3] is an approachable routing set of rules i.e.it founds a source to an endpoint only on request.Route discovery is the action of finding the best path from source node to destination node done by the originator. This mechanism starts on when a source node is wish to send a packet to the destination and is not finding the best path in its route cache.Route maintenance is the process of maintaining the routes in network if the link failure occurred. DSR follows this mechanism to delete the broken link from the network while propagating the packet from the source to the destination.Other ways the node will revert the route on the basis of route record in the Route Reply message header (symmetric links). In the event of lethal transmission, the Route Maintenance Phase will start where the Route Error packets are generated at a node. Again, the Route Discovery Phase is initiates.

The steps in our proposed work is to setup the scenario, set the threshold value for packet delivery ratio. Because the blackhole attacked node can also generate the RREP signal. If message from the authenticated node then system is marked as an authenticated and source can transmit data to the specified and secured path. The packet delivery ratio is compared with the threshold value. If packet delivery ratio drop to the threshold value then Source node randomly choose the cooperative bait address, of one node neighbor to bait malicious node, then send bait request. If any node reply RREP from other route except neighbor node then start the reverse tracing program and send test packets, check messages to detect malicious node, source node list malicious node onto black hole list, set alarm packet and end the transmission.

In this paper section 2 provides the literature review relevant for the context. Section 3 provides the proposed methodology, proposed algorithm and description of proposed methodology. Section 4 represents the implementation of proposed methodology, discussion on simulation Results and performance analysis of simulation results. Section 5 concludes the paper.

II. BACKGROUND AND LITERATURE SURVEY

The concepts dynamic source routing is based on the source routing which means the initiator of the packet provides an orderly list of nodes according to which packet traverses in the network. The key note this routing pattern is that intermediate nodes need not to track the information of the routing through which packet will traverse in the network as source node already has a decision regarding the routes. Utilization of source routing allows the packet to travel in the loop free environment, elude the requirements for updating the routing information in the intermediate node, allows the node to forward the packet to store the routing information in them for future. All aspects of protocol operate entirely on demand [4]. DSR[5] works in completely self configuring and organizing without pre existence of structured network for any existing network infrastructure or administration. The protocol works on the two important mechanisms. i.e. "Route

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 09, September-2016

Discovery" and "Route Maintenance"[6]. Route discovery is a method of finding out the secure route in the network, when a source node's having a desire to transmit the data packet to the destination node, where every node holds a route cache of source routes it has understood or overheard. Route maintenance is the mechanism by which originator device recognize the alteration occurred in the network topology[7] such that it understands about the longevity of the route available to the destination because of the node in the route list is moved out of the range.Best path between the source node and destination node is determined the process of discovery where route maintenance ensures about the loop free path. Route reply will only generate by the projected node when the route request will reach to it. It will generate the route reply according to the route received in the route request packet.

Other ways the node will revert the route on the basis of route record in the Route Reply message header (symmetric links). In the event of lethal transmission, the Route Maintenance Phase will start where the Route Error packets are generated at a node. Again, the Route Discovery Phase is initiates.

DSR works a finding the route and uses that route called source route. Sender has a complete knowledge of particular sequence orders of the network nodes to reach at the destination. The initiator than pass this packet into the network interface wireless medium to the first node which is identified by the route in its route cache. If that node is not the destined address, it forward the packet following by the further node mentioned in the route cache. Once after another, process is continuous, until not reached to the final destination. After reaching to its desire end it will deliver the packet to the transport layer of the host. Since the routing decision is made at source which make easy to obviate the loops in route. It is a Starmark feature of DSR. Source route traverse in the network on control packets in the form of route request and route reply while traversing if any node hears the source route than it can include the information in its route cache. Protocol itself broadcast the topological knowledge in the network among the nodes. Source route carries the correct information of route as it being tested by the packet flowing in the network along with them. DSR utilize the source routes where packet travels according to obtained source route from the route cache itself or by finding through the flooding in the network. This makes DSR to gain the benefits in terms of mounted information, free from the loop that to without overhead cost.

Route discovery is the action of finding the best path from source node to destination node done by the originator. This mechanism starts on when a source node is wish to send a packet to the destination and is not finding the best path in its route cache.

In route discovery primarily the initiator node will first search the route from source to destination by utilizing its route cache. If the initiator fined the path it will start sending the packet in a transmission range[8] by wireless medium.Route maintenance is the process of maintaining the routes in network if the link failure occurred. DSR follows this mechanism to delete the broken link from the network while propagating the packet from the source to the destination. The basic concept of route maintenance in DSR is that every node is responsible for acknowledging that the next node in the source path had received the packet. If any node does not received such confirmation it will send error message to the originator or the initiator in the network. After when the originator receives[9] the error message from the particular node, it deletes that route from route cache and opt the other best route available in its cache.

III. PROPOSED WORK

In proposed work the packet delivery ratio is compared with the threshold value. If packet delivery ratio drop to the threshold value then Source node randomly choose the cooperative bait address, of one node neighbor to bait malicious node, then send bait request. If any node reply RREP from other route except neighbor node then start the reverse tracing program and send test packets, check messages to detect malicious node, source node list malicious node onto black hole list, set alarm packet and end the transmission.

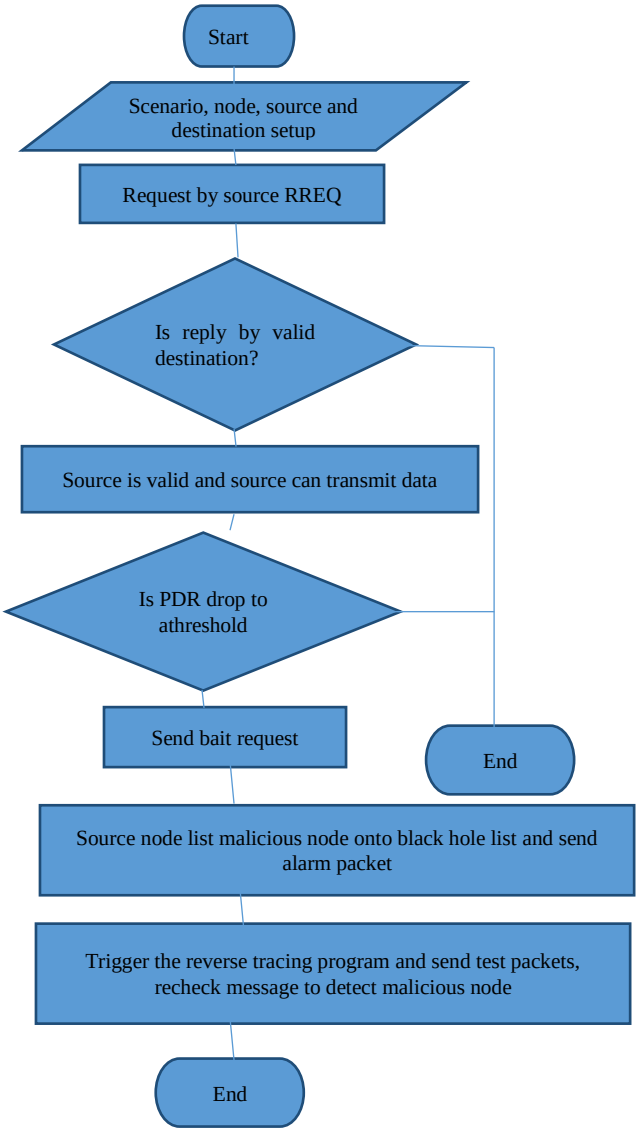

Fig 1 Flow diagram of proposed algorithm

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 09, September-2016

Step 1: Scenario setup, Node setup, Routing protocol setup, Source and destination setup
Threshold value setup
Step 2: Request send by source RREQ
Step 3: Check whether reply RREP by valid and authenticated node
If node is authenticated then
Marked system is valid
Source can transmit data
Else if
Check hop count of the system
If hop count exceeded then
System is invalid
Goto End
Else if hop count is less then
Linked failure in system
Report to the system
Else
Goto step 2 request send by RREQ
End if
Step 4: Check packet delivery ratio of the system
If packet delivery ratio drop to the threshold then
Source node randomly choose the cooperative bait address of one node neighbor to bait malicious node
Send bait request
If any node reply RREP from other route except neighbor node then
Start the reverse tracing program and send test packets
Check messages to detect malicious node
Source node list malicious node onto black hole list
Set alarm packet
Goto End
Else
Goto End
End if
End

The first step in our work is to setup the scenario i.e. to setup the node used in algorithm. To setup the source and destination used in the system. Set the threshold value for packet delivery ratio. It also set the routing parameters, routing protocols, packet size, dimensional area, and rate of transmission. The next step is to send the request generated by source RREQ. The next step is to check whether the source get the reply RREP by valid and authenticated node. Because the blackhole attacked node can also generate the RREP signal. If message from the authenticated node then system is marked as an authenticated and source can transmit data to the specified and secured path. If RREP reply is from invalid or unauthenticated node then first count the number of hops. If number of hop counts exceeded then marked system is invalid and exit from the network. If number of nodes count is less than system may occur link failure report to the system. To find another secure neighbor node go to the RREQ source request step. The next step is to check packet delivery ratio of the network. The packet delivery ratio is compared with the threshold value. If packet delivery ratio drop to the threshold value then Source node randomly choose the cooperative bait address, of one node neighbor to bait malicious node, then send bait request. If any node reply RREP from other route except neighbor node then start the reverse
tracing program and send test packets, check messages to detect malicious node, source node list malicious node onto black hole list, set alarm packet and end the transmission.

IV IMPLEMENTATION

For implementation of our proposed algorithm we used Network Simulator 2 (NS2) simulator.For simulation we have used i3 3.0 GHz machine with 4GB RAM. The program is developed in TCL language and some functions are also implemented in C/C++ language. NS2 is used as simulation environment.

In our simulation work, we have different the amount of nodes from 50 to 300, which are arbitrarily positioned in dissimilar parts of positioning part with a static density. For this simulation, we have used the network parameters, such as Dimension, Number of nodes, traffic, transmission rate, Routing protocol, transmission range, sensitivity, transmission power etc., are used.

Table 1 Simulation scenario

1. Average Delay: This metric describes the newness of data containers. It is defined as the average period amongst the moment a data packet is sent by a data source and the instant the sink accepts the data container.
2. Node Energy Consumption (Ea): The node energy consumption measures the typical energy degenerate by the node in order to communicate a data container from the source to the sink.
3. Data Delivery Ratio (R): This metric designates both the damage ratio of the routing procedure and the energy compulsory to receive data packets. This represents the ratio among the number of data containers that are sent by the source and the amount of data containers that are received by the sink.

The different implementation scenario is represented in following section. We have observed many scenarios with different nodes, simulation time and speed.

Scenario-A: Number of nodes-30, pause time-10 sec, max. speed of nodes 5 m/s, simulation time 100 sec, area 500m X 500m.

Scenario-B: Number of nodes-100, pause time-10 sec, max. speed of nodes 10 m/s, simulation time 100 sec, area 500m X 500m.

Scenario-C: Number of nodes-150, pause time-10 sec, max. speed of nodes 40 m/s, simulation time 100 sec, area 500m X 500m.

Scenario-D: Number of nodes-200, pause time-20 sec, max. speed of nodes 50 m/s, simulation time 100 sec, area 500m X 500m.

Scenario-E: Number of nodes-250, pause time-10 sec, max. speed of nodes 5 m/s, simulation time 100 sec, area 500m X 500m.

Scenario-F: Number of nodes-300, pause time-10 sec, max. speed of nodes 10 m/s, simulation time 100 sec, area 500m X 500m.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 09, September-2016

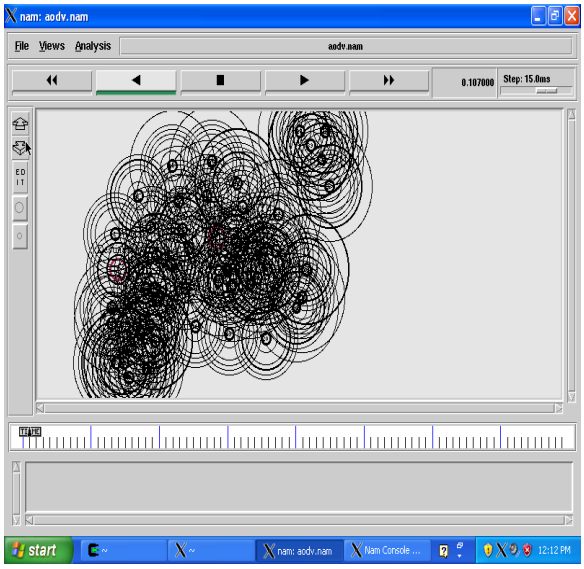

Fig 2 Implementation scenario with Flooding

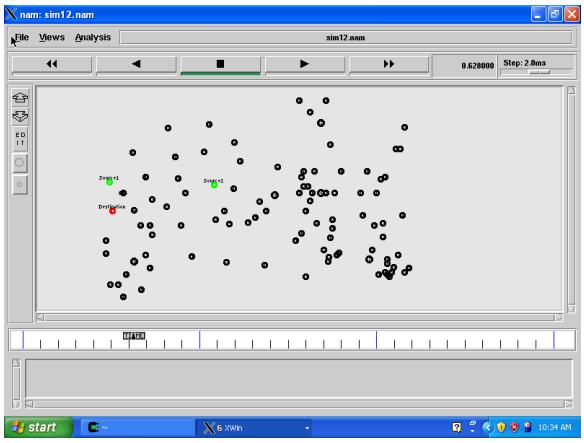

Fig 3 Implementation scenario with attack

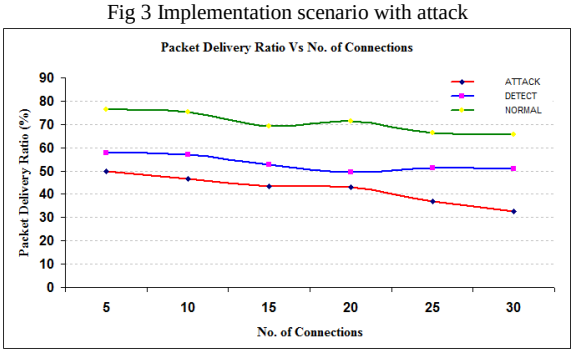

Fig4 Packet Delivery Ratio (%) Vs Max No. of Connections

Following is the graph plotted for packet delivery ratio(%) vs maximum number of connections. Active connections varies from 5 to 30. Scenarios G to L, at 15 m/s of node speed, are plotted for DSR under blackhole attack, DSR with detection module and normal DSR.

Number of mobile nodes	30,50,100,150,200 250,300
Simulated area dimension	500m X 500m
Simulation duration	100s
Transmission range	250 m
Routing Procedure	DSR
Transport Layer	FTP, TCP
Traffic flow type	CBR
Packet size in bytes	28 – 512 bytes
Quantity of traffic links	20 , 8
Max. Speeds in m/s	30
Movement Model	Random Waypoint
Max. mode speed	5 m/s – 30 m/ss
No. of connections between nodes	5 – 30
Pause time	10s
Rate (packet per sec)	2 pkts/sec

Table 1: Simulation Parameters

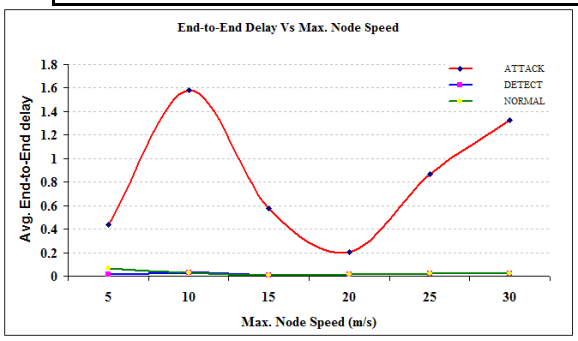

Figure 5 End-to-end delay (sec) Vs Max Node Speed (m/s)
Following is the graph plotted for end-to-end delay (sec) vs maximum node speed (m/s). Node speed varies from 5 m/s to 30 m/s. Scenarios A to F, at 15 connections, are plotted for DSR under blackhole attack, DSR with detection module and normal DSR.

V.CONCLUSION AND FUTURE WORK

MANET's having number of node demands high quality of processing power, high bandwidth and memory to provide definite routing information, though induces traffic overhead in the network. Every mobile node is free to move in any ways and can change their link at any time. AODV is an approachable routing set of rules i.e.it founds a source to an endpoint only on request.This paper proposed a novel method to find link failure detection in MANET. The experimental results showed that our method is well suited for MANET with DSR protocol.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 09, September-2016

REFERENCES

[1] David A. Maltz, "On demand routing in multi-hopwireless mobile ad-hoc network" CMU-CS-01-130, PhD. Desertion, School of computer science Carnegie Mellon University, Pittsburgh PA- 2001.

[2] Josh Broch ,David A. Maltz , David B Jhonson, Yih-chunhee, JorjetaJatchene, " A Performance Comparison of Multi-Hop Wireless Ad-hoc Network Routing Protocol", Computer Science Department Carnegie Mellon University Pittsburg PA 15213 , Available at http : //www . monarch .cs.cmu.edu/

[3] shodhgana.inflibnet.ac.in/ bitstream/10603/42611/5/05.

[4] Charlos De Cordeiro and Dharma P. Agarwal " Mobile ad-hoc networking",OBR Research Centre for Distributed and Mobile Computing,ECECS,University of Cicinnati –USA.

[5] Amit N Thakre ,MrsM.Y.Joshi "Performance Analysis of AODV & DSR routing Protocol in Mobile ad-hoc network", IJCA special Issue on "mobile ad-hoc network"MANETs 2010.

[6] Qiang Ma, Kebin Liu, Zhichao Cao, Tong Zhu, Yunhao Liu, Link Scanner: Faulty Link Detection for Wireless Sensor Networks, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 14, pp 4428-4438, Aug 2015

[7] S. S. Ahuja, S. Ramasubramanian, and M. M. Krunz, "Single-link failure detection in all-optical networks using monitoring cycles and paths," IEEE/ACM Trans. Netw., vol. 17, no. 4, pp. 1080–1093, Aug. 2009.

[8] Q. Cao, T. Abdelzaher, J. Stankovic, K. Whitehouse, and L. Luo, "Declarative tracepoints: A programmable and application independent debugging system for wireless sensor networks," in Proc. ACM SenSys, Raleigh, NC, USA, 2008, pp. 85–98.

[9] A. Cerpa, J. L. Wong, L. Kuang, M. Potkonjak, and D. Estrin, "Statistical model of lossy links in wireless sensor networks," in Proc. IEEE IPSN, 2005, pp. 81–88.