ISSN:0975-9646

Enhancement in AODV protocol to select the secure and shortest path in Mobile Ad hoc Network

Gagandeep Singh Hundal[1*], Rajeev Bedi[2], Dr. Sunil Kumar Gupta[3]

[1]*M.Tech Student, CSE Dept., BCET Gurdaspur, Punjab, India*
[2]*Assistant Professor BCET Gurdaspur, Punjab, India*
[3]*Associate Professor, BCET Gurdaspur, Punjab, India*
*gagandeep.hundal@gmail.com

***Abstract* - Mobile Ad hoc networks are infrastructure less type of network which have auto configurable mobile nodes. These mobile nodes are free to move while communicating with each other. Due to the mobile nature of the nodes, link failure often occurs which causes the reduction in efficiency of the network. Therefore to counter the link failure problem, an arrangement has to be made to avoid link failure by providing an alternate path for communication. In this paper, a new technique has been proposed to overcome the problem of link failure which in turn enhances the performance of the network and AODV protocol. This also results in reducing packet loss.**

***Keywords:* MANET, AODV, link Failure, beacon frames.**

I. INTRODUCTION

A wireless ad hoc network is the collection of mobile nodes, without any centralized control over the nodes in the network. Every node in the network act as both a router and a packet forwarder. The mobile nodes are free to move in any direction. Thus the network topology changes frequently. MANETs are a kind of wireless ad-hoc networks that usually has a routable networking environment on top of a Link Layer ad hoc network. The routing protocols are broadly classified as proactive and reactive routing protocols. The reactive routing protocols are the protocols which establish link between source and destination when required.On the other hand, the proactive routing protocols are protocols which establish link between source and destination on the basis of predefined routing tables which are stored with the mobile nodes. The simulation result shows that the reactive protocols are more efficient than reactive protocols for mobile ad hoc networks. In simulating the proposed work, AODV routing protocol has been used. Security is the biggest issue in the ad hoc routing applications. In ad hoc networks it is quite challenging to cater to security needs of the network due to lack of central authority, topology changes because of node mobility, shared radio channel and limited availability of resources. There are many applications of the ad hoc networks both in commercial environment, military operations and other security purposes.

II. LINK FAILURE PROBLEM

Link failure problem is a common problem in MANET which is caused due the mobile nature of MANET nodes. When the nodes participating in communication move, they may move out of each other's coverage area. Thus causing link breakage. In the diagram below, link problem is shown where in first part of diagram A can communicate with B and B cam communicate with C so there is a link between A → B → C. but in second part of diagram node B moved towards C so B is out of range for A so there is a link failure occurred between A and C.

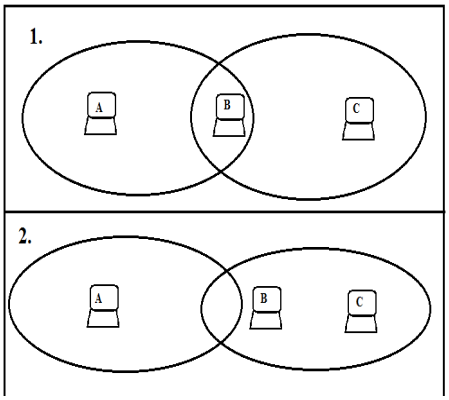

Fig 1**:** Link failure problem

III. LITRATURE REVIEW

Dimitri Marandin (2005), demonstrated the detection of broken links to nodes using hello messages and the feedback provided by Medium Access Control (MAC) layer. The reception of hello messages signifies link availability with the source of hello message. But this technique requires that each node transmits a hello message at regular intervals. MAC layer feedback works better than hello messages when the network load is low. When the load on the network is high, the number incorrect link failure decisions from MAC layer feedback also increases. This results in low throughput (High Packet Loss). Two performance metrics namely Goodput and Energy Efficiency were used. Simulation results show that the average energy expenditure per packet received is less in case of MAC feedback.

Khalid Zahedi *et. al.* **(2011),** proposed the link breakage prediction technique. In this method, the Received Signal Strength Indicator (RSSI) value will be used by a node along an active route to predict a link breakage. The availability of a link is evaluated and a packet named Soon Link Breakage Warning (SLBW) is generated if there is a possibility of link breakage. Simulation results show an increase in packet delivery ratio and decrease the packet loss and end to end delay.

Mrs. Sunita Nandgave-Usturge (2012), discuss about the routing in mobile ad hoc networks. The main reason of

link failure in mobile ad hoc networks is mobility, interference and congestion. Mobility means each node is free to move within its transmission range. In MANET congestion occurs when the amount of data sent to the network exceeds the available capacity. Such situation leads to increased buffer space usage in intermediate nodes, leading to data losses. Congestion is detected at transport layer. TCP is a window based reliable transport layer protocol that achieves reliability through sequence number and acknowledgement. Congestion is main reason for performance degradation of TCP. Packet loss reasons are node mobility and link layer congestion. Cross layer approach is used to improve TCP performance. Cross layer approach is used to solve route failures. AODV has better congestion avoidance mechanisms. This paper addresses four signal strength based congestion control mechanisms AODV, Reliable AODV, MAODV, and CLS_AODV.

Parveen Yadav *et. al.* **(2012)** proposed a novel routing algorithm for route maintenance using link failure localization (DSR-LFL). The algorithm takes decision based on the location of the failure link in source route. The proposed algorithm helps in improving the scalability and route maintenance. It improves the packet salvaging and delivery ratio and reduces the number of error messages.

Humaira Ehsan *et. al* **[2012],** elaborated various kinds of attacks in MANET and simulation of these attacks was done using ns-2 simulator. Various attacks namely black hole attack, selfish node behavior, RREQ flooding and selective forwarding attack are used draw major inferences about the impact of these attacks on the network. If the attacker node is on the route between the source and the destination, then the malicious node would have a major role in performance degradation. Moreover, if the attacker node is in one part of the network, while the communication between source and destination takes palace in another part of the network, then the impact of the attacker node would be minimal.

K. Shanwaz *et.al.* **(2012),** proposed a modification to the existing DSR protocol by adding a link breakage prediction algorithm. The signal power strength from the received packets is used to predict the time when the link breakage could occur. A warning is sent to the source node of the packet if the link is going to break soon. A proactive route rebuilding is done by the source node to avoid disconnection. The intermediate nodes monitor the signal strength based on a threshold signal value to inform the source node about the likelihood of any route disconnection. This technique reduces dropped data packets.

Mr. S.A. Jain *et.al.* **(2012**), illustrated the different mechanisms used for link failure detection by using alternate route finding. Ant colony algorithm has been used in mobile Ad-hoc network to find an alternate route for next to next node. In Ant colony optimization, overhead parameter will also improve as the control packets used are only forward ants and backward ants. It also avoids undesired re-transmissions from the source. Thus improving the throughput and end to end delay.

Abedalmotaleb Zadin *et. al.* **(2013),** proposed a node protection protocol which allows for the establishment of stable connection in MANETs. In recovery of node protection path when a primary path is broken, a total of two nodes are randomly switched off each from a different path. In link protection technique when the primary path is broken, the backup path is not useful. A message is sent to the source and the source recalculates the path to the destination. The last reachable node locally uses the backup path that covers the unreachable node thus saving the recalculation of the whole path. Greedy-based Backup Routing protocol Node Protection (GBR-NP) shows number of packets delivered and delivery rate.

IV. METHODOLOGY

According to the proposed solution, the link failure problem can be solved on the basis of beacon frame range concept. Maximum existence of beacon frames is found and dynamically shift the path so as to avoid link failure and enhancing the performance of the network.

A is the Adjacency matrix representation of given network; n is the no. of nodes and node a acts as source and node b acts as destination.

Step 1: Give the range of the network node and set all other elements that are outside the range to 0.

Step 2: Find the Neighbor of Each node of network starting from node a to node b.

Step 3: Find the path from source to destination with the high vicinity nodes and store it in an array.

Step 4: Search the neighbor list and pick a node of high vicinity from the list and put that node in the array.

Step 5: Compare this node with the other neighboring nodes in the network. If node has the low vicinity, then replace this node with another.

Step 6: Compare the neighbor list of the generated node with all the elements of array otherwise, Pick a random node from the list with high vicinity and put it in the array. Finally we get the list of nodes that provide a safe path.

All the above steps result in a network of the high vicinity nodes. In this network, the source node chooses the node which is in its vicinity, is with higher signal strength. Suppose if a node has the 45 percent vicinity, and the path that chooses by the source having the 50 percent vicinity. As the node of vicinity 50 moves from its position then its vicinity will also reduce. In that case the source node will shift the route to the node having the vicinity 45. Thus link failure can be contained by applying this method. The packet loss also reduces. A pathis generated, in which no node with low vicinity is included. The proposed algorithm provides a network having the secure and reliable data transmission.

V. RESULTS AND DISCUSSIONS

Simulation is done using NS-2 simulator. The figures shown below compare the proposed method with method (which adds an extra node when link failure occurs). The graphs show two lines: red line for the traditional approach, green for the proposed method.

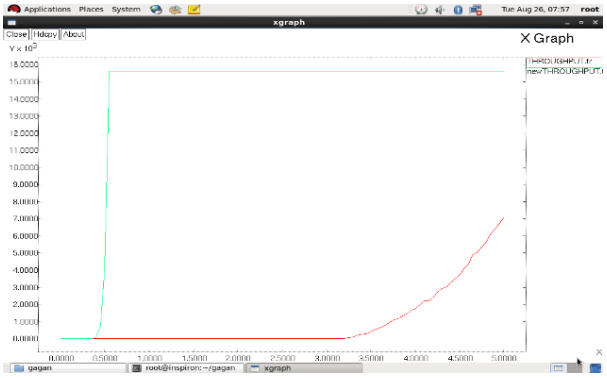

Fig 2: Throughput Graph

Figure 2 shows the graph for difference in throughput. The proposed method shows a considerable increase in throughput.

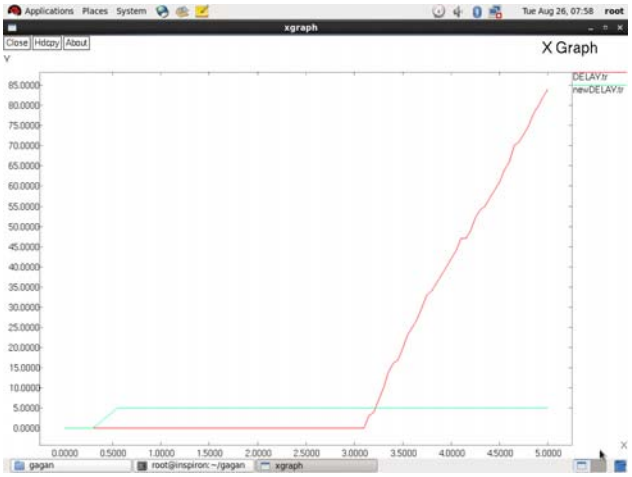

Fig 3: Delay graph

Figure 3 shows the difference in delay caused. The delay in proposed method is quite low.

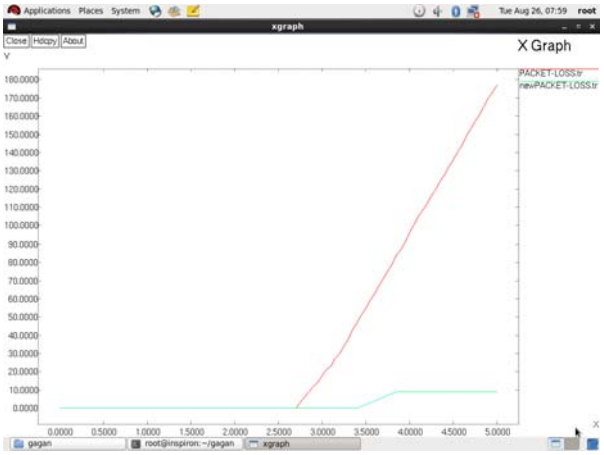

Fig 4: Packet loss graph

Figure 4 shows the Packet loss graph. Increase in throughput will result in decrease in packet loss and vice versa.

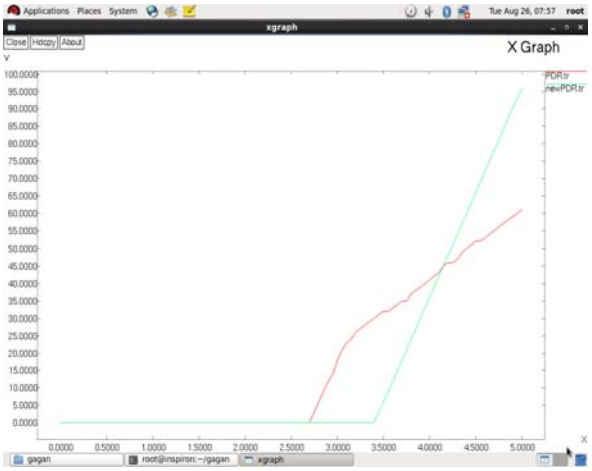

Fig 5:PDR graph

Figure 5 shows the difference in PDR. Packet delivery ratio increases when link failure problem gets eliminated by using the proposed method.

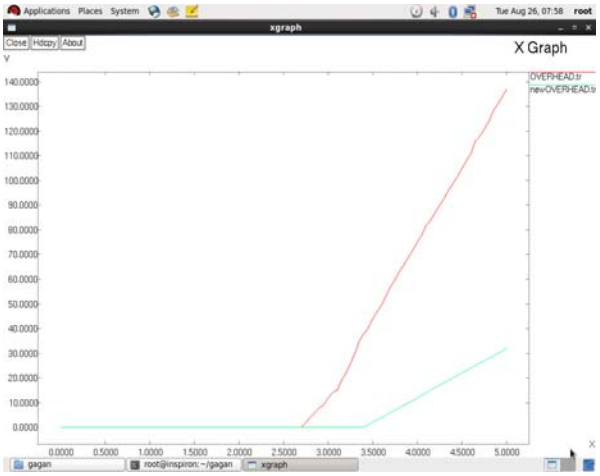

Fig 6: Overhead graph

Figure 6 shows the graph for overhead caused due to link failure problem. The overhead gets reduced when link failure problem is eliminated using the proposed method.

VI. CONCLUSION AND FUTURE SCOPE

In this paper, the routing approaches in ad hoc networks from security view of point, are considered. It presented the requirements that need to be addressed for secure routing. The low vicinity nodes in the ad hoc routing are analyzed. Existing routing algorithm for ad hoc networks are not much secure. The proposed algorithm presented in this paper considers the high vicinity between the nodes. These nodes are used for data transmission. The path that is chosen by the source node may consist large no. of nodes. Hence the path of network becomes large, so the future work can also be done to choose the lesser number of nodes with high vicinity.The Security research area is still open as many of the provided solutions are designed keeping a limited size scenario and limited kind of attacks.

REFERENCES

[1] Deng, H., Li, W., & Agrawal, D. P. (2002). Routing Security in Wireless Ad-Hoc Network. *IEEE Communication Magazine* , 70-75.

[2] Ehsan, H., & Khan, F. A. (2012). Malicious AODV. *IEEE International Conference on Trust, Security & privacy and Computing and Communiaction* , 1181-1187.

[3] Jain, S. A., & Kadam, A. A. (2012). A Study of Congestion Control mechanism using Link Failure Detection in MANET. *International Journal of Engineering Research & Application* , 1009-1012.

[4] Marandin, D. (2005). Performance Evaluation of Failed link Detection in Mobile Adhoc network. *IEEE* , 398-404.

[5] Nandgave-Usturge, S. (2011). Study of Congestion Control using AODV & Signal Strength by avoiding Link Failure in MANET. *International Conference on Communication, Information and Computing Technology* , 1-5.

[6] Shanwaz, K., & Babu Rao, D. S. (2012). Reducing Link Failure in MANETs using Link Breakage Prediction Algorithm. *International Journal of Engineering Research & Technology* , 01-06.

[7] Yadav, P., Bhattacharjee, J., & Soni, R. (2012). A Novel Routing Algorithm based on Link Failure Localization for MANET. *International Journal on Computer Science & Engineering* , 1738-1748.

[8] Zadin, A., & Fevens, T. (2013). Maintaining Path Stability with Node Failure in Mobile Adhoc Networks. *Elsevier International Symposium on Intelligent Systems, Techniques for Ad hoc & Wireless Sensor Networks* , 1068-1073.

[9] Zahedi, K., & Ismail, A. S. (2011). Route Maintenance Approach for Link Breakage Prediction in Mobile Adhoc Network. *International Journal of Advanced Computer Science & Application* , 23-30.