Selective on-demand protocol for finding reliable nodes to form stable paths in ADHOC networks

T. Rajamohan Reddy,
M.Tech Student,
ASCET,Gudur.

N. Sobharani,
Asst Professor, Dept. Of CSE,
ASCET,Gudur.

Abstract: **A wireless adhoc network consists of a group of wireless nodes which can dynamically self-organize themselves into a temporary topology to form a network without using any existing infrastructure. Generally adhoc networks are formed only when there is need and maintained for one time purpose. Node mobility is one of the significant factors that decreases the performance of adhoc networks and restricts network stability. Selection of reliable paths is an effective way to tackle the node mobility problem. Current methods of reliable path selection suffer from various shortcomings (Ex: More hardware requirements). In adhoc networks, mobility of the nodes causes frequent link failures; due to this, routes are disconnected. So route selection and topology maintenance is a challenging issue. In this work, we propose a method for identifying set of reliable adjacent nodes in the network and extends the capabilities of AODV routing protocol. Simulation results show that our approach is better than the traditional AODV routing protocol.**

Keywords: **ADHOC network, node mobility, link failures, AODV protocol**

I INTRODUCTION

An Ad Hoc Network (MANET) is a wireless network consisting of mobile nodes, which can communicate with each other without any infrastructure support. In these networks, nodes typically cooperate with each other, by forwarding packets for nodes which are not in the communication range of the source node.

Typically, routing protocols are classified according to the route discovery philosophy, into either reactive or proactive. **Reactive** protocols are on-demand. Route-discovery mechanisms are initiated only when a packet is available for transmission, and no route is available. On the other hand, **proactive** protocols are table-driven. Routes are precomputed and stored in a table, so that route will be available whenever a packet is available for transmission.

Our work is based on link stability in wireless networks. Link stability is unique to wireless network. Link stability refers to the ability of a link to survive for a certain duration. The higher the link stability, the longer is the link duration. The stability of a link depends on how long two nodes, which form that link, remain as neighbours. Two nodes are neighbours when they remain within each other's communication range, or the signal strength is above certain threshold. Mobility causes link breakage and leads to route recovery. Transport layer performance degrades as a result of packet loss and trigger congestion control mechanism. A more stable link should therefore be preferred. However, routing algorithms that are based only on link stability have either been shown to exhibit little improvement over hop-count based algorithm or the improvement comes when link lifetime can be accurately predicted. A crucial issue with stability based routing algorithm is that much longer routes can be obtained compare to hop-count based routing.

This paper is organized as follows. In Section II, describes the process flow of AODV. Section III we briefly review some enhancements to AODV protocol. Section IV presents our proposed work. Section V shows the simulation results and finally Section VI concludes the paper.

II AODV

Adhoc on demand distance vector routing protocol [4] is an on demand routing protocol. In this protocol, routing discovery process is initiated when route is required. In this protocol, If source node or intermediate node moves then the moving nodes realizes link failure and send this link failure notification to its upstream neighbors and so on till it reaches to source. So, source can reinitiate route discovery if needed. Fig.1 presents process flow of AODV. Fig.1 considers three actors such as source, destination and intermediate node in which all processes are defined and eleven activities are designed for this same process.

In AODV, Nodes i and j are said to be neighbors if the received transmission power of one of them and maximum power exceeds some given threshold τ. Assume directed edge(i,j) $\in$ E [5] iff $\delta(i,j) <= d_k(i)$, where $d_k(i)$ is the distance between node u and its k-closest neighbors.

It has been analyzed that performance of network gradually decreases in certain following cases: If transmission range of node is larger than transmission range of network.

(i) If neighbor node is flooding unnecessary RREQ messages to other nodes.
(ii) If time is high to reach hello messages between two nodes.
(iii) If packet dropping ratio of a neighbour node is maximum.

All above four cases shows that presence of any one case

decreases performance of on demand routing protocol.

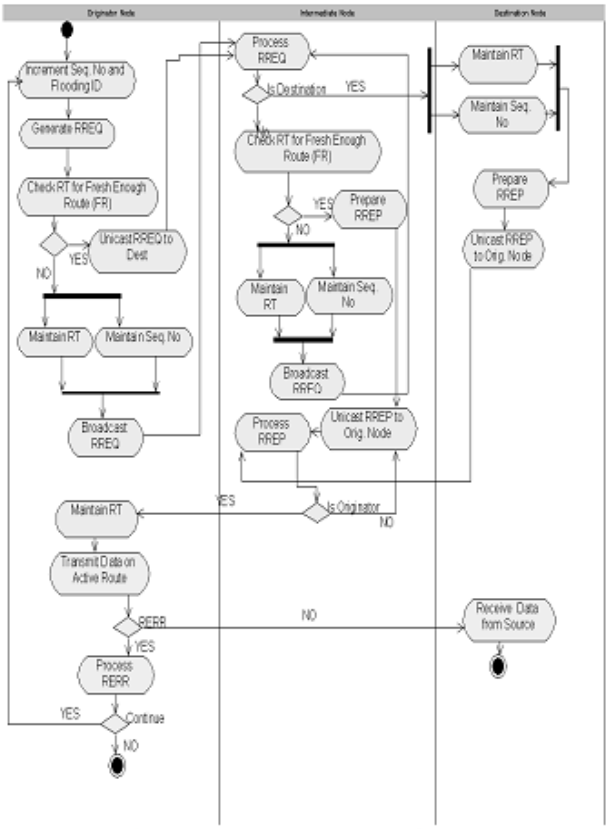

Figure 1: Process Flow of AODV

III LITERATURE SURVEY

REAODV: In [1] a route enhanced AODV is proposed which reduces the routing overhead and also decreases the end-to-end delay.

EnfantAODV: The authors in [2] proposed an ENFAT-AODV protocol. In that every node maintains two paths. Main path and backup path. Backup path will be used whenever main path (node/link) failures occur.

PWAODV: In [3] the authors have used NCR (Neighbour Change Ratio) in order to detect the neighbours which are not mobile. So that stable paths can be constructed through this technique. By this frequent broken paths will be reduced. It reduces route cost and delay.

IV PROPOSED WORK

In this approach, initially all nodes maintain their own transmission range. It has been assumed the transmission range of the network is 250 meters (refer Table.2 Appendix A). Now, transmission range (NTr) of each node present in the network with the total transmission of network (TTrN) of the node is compared. Determination of transmission power is required to send a message between node n and its neighbor n1. It can be measured by calculating the received power of hello message. When node n receives hello messages from a neighbor node n1, it can estimate the minimum power level needed to reach n1 by comparing the received power of hello message with maximum transmit power. This approach is enhanced by adding parameters in the neighbor table such as flow capacity, signal strength. Reaching time of hello messages between node and its neighbor is calculated. Address of node is stored into the neighbor table based on their transmission range. If (NTr > TTrN), then adjust energy of this node accordingly, otherwise calculate signal strength by using equation (1). If threshold value is maximum then evaluate position of node and also set timer for the same. Further work is preceded by calculating the flow capacity of a node as mentioned in equation (2) . If flow capacity of a node is good then store address of a node otherwise remove address of the node from routing table (refer Figure.2).

Suggested algorithm is an optimal solution for finding good nodes. Categorization of nodes is based on performance metrics such as transmission range and power of node, signal strength, capacity of node for high packet forwarding and relative position of node. Neighbor routing table maintains address of node for maintaining record of the entire nodes. These stored nodes are used for data transmission and forwarding. This approach minimizes energy consumption of node and increases its battery life. Thus any node can forward data to other node if they exist with in the range of 250 meters. And location or relative position of node can be verified by using routing table.

Definition 1: Signal Strength of a node is computed by using well known formula which is as follows:

$$\text{Transmitter}_{\text{signal strength}} = \begin{cases} S_H - \left\{ \dfrac{S_H - S_{threshold} * T}{e} \right\} & \text{if farther } (T > e) \\ S_H & \text{closer } (T < e) \\ S_{thresh} & \text{Otherwise} \end{cases}$$

---------(1)

Where S_H is signal strength of hello message and T is the time period between two successive hello packets and e Is the link connectivity between i and j.

Definition 2: Assume a graph G (V, E) [8]. The capacity of directed edge is denoted as C_{ij} source s and destination d. F is assumed as a flow in G where E belongs to edge (i, j).

If for all (i, j) Є E; $0 <= F_{ii} <= C_{ii;}$ s.t.

$$\sum_{j:(s,j)\in E} F_{sj} - \sum_{i:(i,s)\in E} F_{is} \qquad \text{---------- (2)}$$

Let F_{is} and F_{sj} be the counter of amount of bytes that flowed on the link (i, j) upto time t in packets.

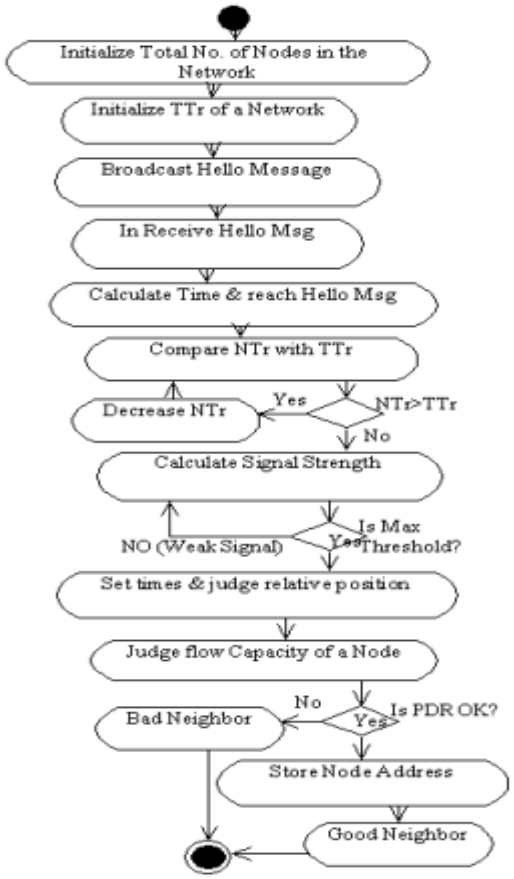

Fig.2. Process flow of proposed algorithm

Thus, If signal strength range is negligible then discard this node and delete entry of this node from the neighbor table. Otherwise calculate flow capacity of a node by considering equation (2). Based on flow capacity and packet delivery ratio, good neighbors are identified.

Complexity Computation between AODV and proposed: By adding new parameters into the routing table, suggested approach increases size of routing table. Thus storage complexity of suggested approach is same as AODV i.e. O(N), where N is the total number of nodes present in the network. It slightly increases overhead by using hello messages but it provides good communication between source and destination as compared to AODV (RFC (3561)). Thus communication complexity of suggested algorithm in O (N).

Cao Minh Trang et. Al [9] has suggested an effective approach for an intrusion detection system in AODV routing protocol. But this approach was not suitable against impersonation attack and also its accuracy decreases in case of high mobility. Our approach is not limited to specific attacks. Performance of each node is evaluated and analyzed individually. And evaluation is done by increasing number of nodes and network size in the networks. But suggested approach has some limitation. By increasing size of network or number of nodes, this approach may increase costing factor. Critical analyze is being done to find an effective results as discussed in next section.

V SIMULATION RESULTS

Proposed approach for neighbor node detection in mobile adhoc networks is identified and compare its result with existing routing protocol AODV using ns2[5]. Initially it has been assumed that all nodes have their own transmission range with dynamic movement.

Mobility scenario is generated by using random way point model with 6-10 nodes in an area of 750m by 750m. The simulation parameters are mentioned below:

Simulation Parameters	Values
Nodes	6-10
Simulation time	100 sec
MAC Layer	IEEE 802.11
Packet Size	512
Pause Time	0-100 sec
Initial energy	50
Transmission Range	250m
CS Range	550 m
Transmission threshold power	0.281838
Txpower and RxPower	0.173, 0.05

TABLE 1: Simulation Parameters

Results are examined by using performance metrics packet delivery percentage (by using equation (3)) and throughput.

The performance of suggested approach is evaluated by using following metrics:

(i) The packet delivery ratio (PDR) between the number of packets produced by CBR sources and number of packets received by CBR sink at final destination.

(ii) Average throughput is calculated by bytes received by destination per second

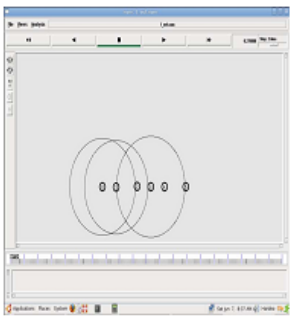

Figure 3: Coverage Area of Nodes

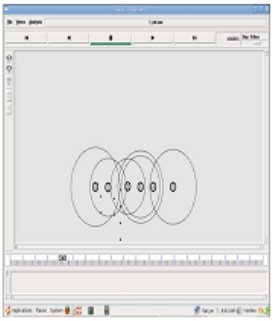

Figure.4: Dropping of Data Packets

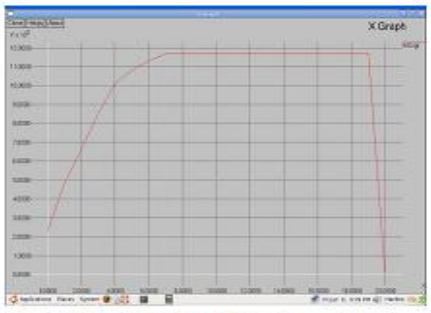

Fig. 5. Packet Delivery Ratio for node 0 (it receives more packets)

Fig. [3-6] provide simulation scenario of a node in terms of coverage area then their packet delivery ratio of each node.

Suggested approach demonstrate high quality in terms of good packet delivery and throughput which is almost above 90% where as performance of AODV lies between 80%-85% .

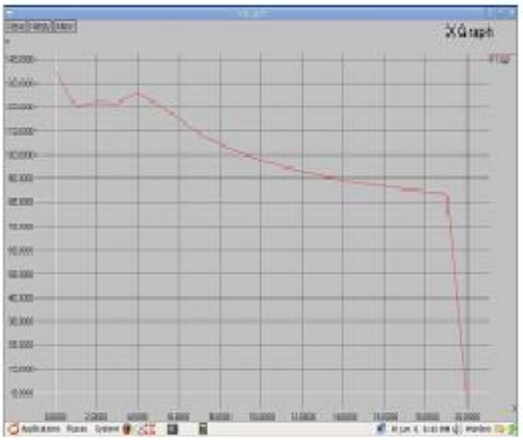

Fig. 6. Packet Delivery Ratio for node 1 (PDR more than 100 shows abnormality)

VI CONCLUSION

We proposed reliable AODV routing protocol which enhances network performance by selecting stable nodes (i.e, only good neighbour nodes) for network formation. All information related to reliable nodes are stored in routing table which improves performance of routing protocol in terms of good communication and stable route. Simulation results shows that our proposed solution improves network stability and signal strength.

REFERENCES

[1] M. Usha, S. Jayabharathi, Wahida Banu R, "RE-AODV: An enhanced routing algorithm for QoS Support in Wireless Ad-hoc Sensor Networks" ,2011, IEEE International conference on Recent trends in Information Technology.

[2] Che-Aron, Al-Khateeb, Anwar, "An Enhancement of Fault-Tolerant routing protocol for wireless sensor network", 2010, IEEE International conference on computer and communication engineering.

[3] Wang N, Cao Yewen, "An Improved AODV protocol with lower route cost and smaller delay", 2011, IEEE fourth international conference on intelligent computation technology and automation.

[4] C. E. Perkins and E. M. Royer, "Ad hoc on demand distance vector (AODV) routing," Internet-Draft, draft-ietf-manet-aodv-02.txt, Nov.1998.

[5] www.isi.edu/nsnam

[6] P.Santi, "Topological Control in Wireless Adhoc and Sensor Networks", John Wiley & Sons Ltd.,2005

[7] Srdjan Krco and Marina Dupcinov, " Improved Neighbor Detection Algorithm for AODV Routing Protocol", IEEE COMMUNICATIONS LETTERS, VOL. 7, NO. 12, DECEMBER 2003

[8] Rudolf Ahlswede, Ning Cai, Shuo-Yen Robert Li, and Raymond W.Yeung,"Network Information Flow, IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 46, NO. 4, JULY 2000, 0018– 9448/00$10.00 © 2000 IEEE

[9] Cao Minh Trang, Hyung- Yun Kong, Hong Hee Lee, "A Distributed Intrusion Detedtion System For AODV", 2006, IEEE, 1-4244-0574— 2/06