An Approach to Improving Throughput of AODV Protocol by Classification of node's Power in MANET

[1]Pritesh Patel, [2]Kaushal Patel

Assistant Professor

Sigma Institute of Engineering and Technology, Vadodara, Gujarat, India

[1]patel.pritesh87@yahoo.com, [2]kaushalpatel15@gmail.com

***Abstract*---- AODV is very simple, effective and useful and efficient protocol in the Mobile Ad-hoc Network. It borrows the advantageous concept from DSR and DSDV algorithm. Obtain the routes purely on-demand makes AODV a very useful and desired algorithm for MANET. During the data transmission Between the nodes in the mobile ad-hoc network energy are used from the battery. so when the node will reach at the minimum power at that time they lost the packet data which are transmitted from the one node to another. So to overcome from this problem before the transmission of the packet data check the energy of the node. This paper shows how to improve the throughput of the AODV protocol**

***Keywords*-- Mobile AD-Hoc Network, AODV protocol, Routing table**

I. INTRODUCTION

Mobile Ad-hoc network is the self-configuring and self-healing wireless networks where the mobile nodes communicate without existence of infrastructure or centralized station. There is no stationary infrastructure. Each node act itself as a router. Node done the Forwarding and receiving packets to/from other nodes each wireless node can directly communicate with all nodes located within its range. In the mobile ad-hoc network each node act as a router and routing efficiency in MANETs. There is a lots of protocols are used for the transmission of the packet data. There is so much protocol for the completion of all tasks Like DSR, AODV, OLSR, DSDV, GPR etc. The goal of MANET is giving the mobility to user .In.-Ad-hoc networks nodes are communicate with each other using multi hop links. The communications between nodes is accomplished via other nodes and in this all task the energy of nodes are used. Nodes called intermediate or forwarding nodes. so there is a need of routing procedure between nodes. For this routing procedure very important thing is Node's energy for communication. And hence the routing protocol plays a major role in MANET. In this paper we are going to improve the throughput of AODV protocol.

II. MOBILE AD-HOC NETWORK

A Mobile ad-hoc network (MANET) consists of mobile hosts equipped with wireless communication devices. The transmission of a mobile host is received by all hosts within its transmission range due to the broadcast nature of wireless communication and omni-directional antennae. If two wireless hosts are out of their transmission ranges in the ad hoc networks, other mobile hosts located between them can forward their message which effectively builds connected networks among the mobile hosts in the deployed area. Due to the mobility of wireless hosts, each host needs to be equipped with the capability of an autonomous system or a routing function without any statically established infrastructure or centralized administration. The mobile hosts can move arbitrarily and can be turned on or off without notifying other hosts. The mobility and autonomy introduces a dynamic topology of the networks not only because end-hosts are transient but also because intermediate hosts on a communication path are transient.

III. WHY AODV PROTOCOL?

AODV is a very simple, efficient, and effective routing protocol for Mobile Ad-hoc Networks which do not have fixed topology. This algorithm was motivated by the limited bandwidth that is available in the media that are used for wireless communications. It borrows most of the advantageous concepts from DSR and DSDV algorithms. The on demand route discovery and route maintenance from DSR and hop-by-hop routing, usage of node sequence numbers from DSDV make the algorithm cope up with topology and routing information. Obtaining the routes purely on-demand makes AODV a very useful and desired algorithm for MANETs.

A. AODV Terminology

- Active route - A route towards a destination that has a routing table entry that is marked as valid. Only active routes can be used to forward data packets.
- Broadcast - Broadcasting means transmitting to the IP Limited Broadcast address, 255.255.255.255. A broadcast packet may not be blindly forwarded, but Broadcasting is useful to enable dissemination of AODV messages throughout the ad hoc network.

- Destination - An IP address to which data packets are to be transmitted. Same as "destination node". A node knows it is the destination node for a typical data packet when its address appears in the appropriate field of the IP header. Routes for destination. Nodes are supplied by action of the AODV protocol, which carries the IP address of the desired destination node in route discovery messages.
- Forwarding node - A node that agrees to forward packets destined for another node, by retransmitting them to a next hop that is closer to the unicast destination along a path that has been set up using routing control messages.
- Forward route - A route set up to send data packets from a node originating a Route Discovery operation towards its desired destination.
- Invalid route - A route that has expired, denoted by a state of invalid in the routing table entry. An invalid route is used to store previously valid route information for an extended period time. An invalid route cannot be used to forward data packets, but it can provide information useful for route repairs, and also for future RREQ messages
- Originating node - A node that initiates an AODV route discovery message to be processed and possibly retransmitted by other nodes in the ad hoc network. For instance, the node initiating a Route Discovery process and broadcasting the RREQ message is called the originating node of the RREQ message.
- Reverse route - A route set up to forward a reply (RREP) packet back to the originator from the destination or from an intermediate node having a route to the destination.
- sequence number - A monotonically increasing number maintained by each originating node. In AODV routing protocol messages, it is used by other nodes to determine the freshness of the information contained from the originating node.

B. *Routing tables*

Each routing table entry contains the following information

- Destination
- Next Hop
- Number of Hops
- Destination Sequence Number
- Active Neighbours for this Route
- Expiration time for this route table entry
- Request buffer: Makes sure that a request is only processed once.

Expiration time, also called lifetime, is reset each time the route has been used. The new expiration time is the sum of the current time and a parameter called active route timeout. This parameter, also called route caching timeout, is the time after which the route is considered as invalid, and so the nodes not lying on the route determined by RREPs delete their reverse entries. If active route timeout is big enough route repair will maintain routes RFC 3561 defines it to 3 seconds.

C. *AODV operations*

- *Route discovery*

When a node needs to determine a route to a destination node, it floods the network with a *Route Request (RREQ) message*. The originating node broadcasts a RREQ message to its neighboring nodes, which broadcast the message to their neighbors, and so on. To prevent cycles, each node remembers recently forwarded route requests in a route request buffer (see next section). As these requests spread through the network, intermediate nodes store reverse routes back to the originating node. Since an intermediate node could have many reverse routes, it always picks the route with the smallest hop count. When a node receiving the request either knows of a “fresh enough” route to the destination (see section on sequence numbers), or is itself the destination, the node generates a *Route Reply (RREP) message*, and sends this message along the reverse path back towards the originating node. As the RREP message passes through intermediate nodes, these nodes update their routing tables, so that in the future, messages can be routed though these nodes to the destination. Notice that it is possible for the RREQ originator to receive a RREP message from more than one node. In this case, the RREQ originator will update its routing table with the most “recent” routing information; that is, it uses the route with the greatest destination sequence number.

Whenever an AODV router receives a request to send a message, it checks its *routing table* to see if a route exists. Each routing table entry consists of the following fields:

- Destination address
- Next hop address
- Destination sequence number
- Hop count

If a route exists, the router simply forwards the message to the next hop. Otherwise, it saves the message in a *message queue*, and then it initiates a route request to determine a route.

- *Link Monitoring & Route Maintenance*

Each node keeps track of a *precursor list*, and an *outgoing list*. A precursor list is a set of nodes that route through the given node. The outgoing list is the set of next-hops that this node routes through. In networks where all routes are bi-directional, these lists are essentially the same. Each node periodically sends HELLO messages to its precursors. A node decides to send a HELLO message to a given precursor only if no message has been sent to that precursor recently. Correspondingly, each node expects to periodically receive messages (not limited to HELLO messages) from each of its outgoing nodes. If a node has received no messages from some outgoing from some outgoing node for an extended period of time, then that node is presumed to be no longer reachable whenever a node determine one of its next- hops to be unreachable, it removes all affected route entries and generates a Route Error (RERR) message. This RERR message contains a list of all destinations that have become unreachable as a result of the broken link. The node sends the RERR to each of its precursors these precursors update their routing tables, and in turn forward the RERR to their precursors, and so on. To prevent RERR message loops, a node only forwards a RERR message if at least one route has been removed.

IV. ANALYSIS OF PACKET TRANSMISSION

After the study of the MANET and AODV protocol the next step of our research work is how to increase the through put of AODV protocol. So first of all we have to know that how the packet does was lost in the transmission and we cannot get the desired output. In the Mobile ad-hoc network node send the packet data to another packet .in this transmission of packet and also receiving the packet which are sent by other require the battery power or we can say node are able to transmit and received the packet .the node are able which have enough power or enough battery power to handle the task. In the transmission the power are consumed from the battery and the power of the battery will decrease and decrease as per the transmission will going on. It will affect on the transmission because if the node have not enough power the node cannot transmit or receive the packet as per our requirement and so packet drop ratio will arise which are not reliable. So from the analysis of the packet transmission I conclude that if the node have not enough power the node cannot send or received the packet so I proposed the technique to improve the transmission and to make the minimum loss of packet during the communication.

V. PROPOSED SYSTEM

By analysis i conclude that packet was drop by the node because the node have not sufficient energy for the transmission so I proposed the technique for this problem. We have to calculate the energy of the node before the packet transmission. AODV Protocol has not any improved mechanism regarding Energy of nodes that why my main aim of dissertation is to identify node with less power node and discard this node from the route and improve data drop ratio and throughput.
For improve data drop ratio we have categorize the node state in three state.

- Node reception power < **X%** = Dangerous Node
- **X%**>node reception power < **Y%**=Critical Node
- Node reception power > **Y%**= active node

Here we have declare X% for safe energy point when node reception power is reached at X% level node will do not transmit or forward data packet to other node, it will only transmit only important control message which are generated in Current Route which node is leaving. Critical node is which type of node which has reception power in between X% to Y% .During transmission this type of nodes are losing its energy and move toward to Dangerous node state. Active node has maximum reception power means it will give maximum throughputs and data drop is also very low.

VI. SIMULATION AND RESULT ANALYSIS

Simulate the proposed work in ns2 by the parameter which are Define at below and take the result which are given at After the simulation get the trace file for both AODV and also for Proposed_AODV .So get the result from the trace file by using perl script .and then create the graph for them to well understand. Here compared the existing AODV and MY_AODV in the term of the Throughput, packet dropped and packet delivery ratio.

Table 1 Throughput

Throughput	**Throughput(bit/sec)**	
Pause time	**AODV**	**Proposed_AODV**
10	10328	10330
20	10336	10340
30	10337	10338
40	10370	10372
100	10380	10385

Table 2 Packet Dropped

Packets dropped	**PROTOCOLS**	
TIME	**AODV**	**Proposed_AODV**
10	95	30
20	97	55
30	122	52
40	110	57
100	130	70

Table 3 Packets Delivery Ratio

Packets delivery ratio	**PROTOCOLS**	
TIME	**AODV**	**Proposed_AODV**
10	0.99080	0.99930

20	0.97420	0.99370
30	0.97112	0.99418
40	0.96420	0.99475
100	0.96890	0.99640

VII. CONCLUSION AND FUTURE WORK

In this mechanism i have define three node type like if node energy lower than 25% will called Dangerous node, node energy between 25% to 50% will called Critical node and node energy with more than 50% energy will called active node. I have use existing control message with different mechanism, when node has 25% reception power remain it will drop messages like RREQ,RREP and If it will Data Packet or RERR then It will generate and send RERR to source. If node has more than 25% node will do as usual work. For Route maintenance node will check its own remain residual energy, if energy is lower than predefine energy level mean 25% then node will check whether node is Intermediate node if it is then node will Drop next packet and Generates RERR, if node is Destination then It will Generate Stop Traffic Signal message to Source.

VIII. FUTURE WORK

We have use simple mechanism for Load transfer from one node to another node which doesn't have enough node energy to transfer packet. In future we can make own Control message which will store the no of nodes which have lower energy and this will be send to source from any node which have low energy. We can also mechanism to calculate whole forward path energy cost and using this source will chose higher energy cost for more reliable packet transfer.

REFERENCES

[1] Energy-Aware Algorithms for AODV in Ad Hoc Networks, Department of Electrical Engineering Graduate Center and City College of City University of New York New York, NY 10031, USA.
[2] Design of an Energy Efficient Routing Protocol for MANETs based on AODV, IJCSI july 2011
[3] SNR/RP Aware Routing Model for MANETs, JSAT, march 2011.
[4] C. E. Perkins, E. M. Royer and S. R. Das, "Ad hoc On-Demand Distance Vector(AODV) Routing," IETF RFC-3561, MANET Working group, 2003.
[5] Sanjay K. Dhurandher, Mohammad S. Obaidat, Fellow FACES: Friend-Based Ad Hoc Routing Using Challenges to Establish Security in MANETs Systems IEEE SYSTEMS JOURNAL, VOL. 5, NO. 2, JUNE 2011.
[6] Ramanathan and Rosales-Hain, "Topology control of multi hop wireless networks usingtransmit power adjustment," IEEE Infocom 2000.
[7] Radika D Joshi, Priti P Rege, "Energy Aware Routing in Ad Hoc Networks", WSEAS, 2007
[8] Natalia Vassileva, Francisco Barcelo-Arroyo, "A Survey of Routing Protocols for Energy Constrained Ad Hoc Wireless Networks", International Journal of Software Engineering and Its Applications 2008.
[9] Fuad Alnajjar, Tarek Saadawi, "Social-stratification Probabilistic Routing Algorithm in Delay- Tolerant Networks", The International Conference on Wireless Algorithms, Systems and Applications (WASA'09), Boston, MA, August 2009, Pages: 579–591.
[10] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," inMobile Computing, 1996.
[11] Elizabeth M.Royer and C.K.Toh,"A Review of current Routing Protocol for Ad-HocMobile Wireless Networks ", 2003.
[12] D. P. Agrawal and Q.-A. Zeng,"Introduction to Wireless and Mobile Systems. Pacific Grove, CA: Brooks/Cole, Thomson, 2002.
[13] Chai K. Toh, A. Le and Y. Cho "Load Balanced Routing Protocols for Ad Hoc"Mobile Wireless Networks Pros " In IEEE Communications Magazine August 2009.
[14] C. Perkins, E. Royer, "Ad-hoc on-demand distance vector routing", in: Second IEEE Workshop on Mobile Computing Systems and Applications, pp. 90– 100, 1999.
[15] Dube, R., Rais, C.D., Wang, K.-Y., Tripathi, S.K.,"Signal stability based adaptiverouting (SSA) for adhoc networks "IEEE Personal Communications 4, pp.36–45, February 1997.
[16] S.Preethi B. Ramachandran "Energy Efficient Routing Protocols for Mobile Ad Hoc Networks" @ 2011 IEEE