ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Special Issue 7, October 2015

A Novel AODV Routing protocol for Delay Sensitive Applications in MANET

Ravi.V, Vedamurthy H K, Dr. Pallapa Venkataram

Assistant Professor, Dept. of CSE, SIT, Tumkur, Karnataka, India[1,2]

Professor, Dept. of ECE, IISc, Bangalore, Karnataka, India[3]

ABSTRACT: Manet is a heterogeneous collection of mobile nodes communicating without fixed infrastructure. The nodes in these networks are constrained by transmission power, bandwidth and processing capability. The most important parameter is every node is battery powered which makes it difficult to enable the delivery of sensitive data reliably and timely to the destination. Traditional AODV routing algorithm does not consider the bandwidth available at the node and also traffic available to transmit data between source and receiver. This paper proposes a simple approach for QoS enabled routing between nodes by considering the bandwidth available at the neighboring nodes by dynamically constructing the path to the destination. The proposed scheme modifies the entries in AODV-RREQ and RREP packet formats to satisfy the QoS requirements of the delay sensitive applications. The result show a reasonable improvement in the Packet Delivery Ratio in transmission of CBR data transfer between source and receiver by maintaining the network life time by managing the battery power. The proposed scheme can be effectively used in various applications such as multimedia applications, emergency applications and military applications.

KEYWORDS: Manet; Delay sensitive application; Bandwidth aware routing

I. INTRODUCTION

Mobile Ad hoc Network (MANET) [1-2] is a flexible heterogeneous network of mobile nodes that can be deployed and setup anytime and anywhere without any pre-installed infrastructure. Since the deployment is dynamically constructed by battery powered nodes and limited bandwidth, routing algorithms designed earlier for Manet constructs dynamic paths to destination as and when required without considering the QoS parameters of application. Routing algorithms designed earlier are designed to be on demand, but does not dynamically handle the path failures and path negotiation for timely delivery of delay sensitive data. Many applications such as defence and disaster management applications, alarm detection and notification systems require messages to be delivered reliably and timely even in bandwidth constrained networks.

Traditional on demand routing algorithm such as Dynamic Source Routing (DSR)[3] helps in constructing the dynamic routes by the help of route cache which maintains a list of possible paths to destination during route discovery phase. The main drawback of DSR is every node needs to maintain route cache and DSR uses exponential back off method for detecting route breaks and dynamically deciding for route maintenance. DSR routing algorithm is less suitable for delay sensitive applications since the path discovery, path maintenance phase and path recovery phase does not consider the available bandwidth at each node, delay that can occur at each node due to propagation and queuing delay. The DSR routing algorithm can be enhanced in various phases such as Route discovery and Route maintenance phase.

- Each node can set route request hop limit in RREQ for deciding the life time of RREQ.
- Each node can check the route cache for unique path to source and destination before generating RREP for each RREQ.
- Nodes can decide upon receiving the RREQ for shortening the path between source and destination.
- Nodes can avoid sending the RERR messages back to the node which generated RERR message when ever a path is broken, this avoids overhead of flooding RERR message.

Delay sensitive applications require new extensions in RREQ packet format to satisfy the dynamic requirements of the application. Adhoc on Demand Routing (AODV) routing algorithm is well suited for these kind of applications, since AODV provides loop free paths to destination, utilizes only symmetric links between neighbouring nodes, routing tables can be used to store pertinent routing information. AODV is able to provide routing for unicast and multicast routes even in stringent resources.

AODV uses expanding ring search, the source node sets the Time to Live (TTL) value of the RREQ to an initial TTL start value. If no reply is received within the discovery period, the next RREQ is broadcast with a TTL value increased by an increment value. TTL value is incremented until threshold value is reached, beyond which RREQ packets are generated based on increment value. The rest of the paper is ordered as follows, Section 2 gives the working of standard AODV protocol. Section 3 describes the working of the proposed AODV protocol for delay sensitive application. Section 4 gives the detail of simulation setup and results of the proposed system are being discussed in section 5 followed by concluding remarks.

II. RELATED WORK

This section elaborates on the conventional AODV [3][4][5][6] protocol that is used on-demand routing protocol for mobile Adhoc networks. AODV is a reactive on demand routing protocol is well suited to any of the Adhoc applications in Manet, But to support Quality of Service (QoS) [7][8][9][10][11] based routing requires extensions to RREQ and RREP packet format and also require modification to routing table entries of AODV protocol. The working of the AODV protocol has different phases such as Route Discovery, Route Reply and Route Maintenance phase.

A. Route Request phase (RREQ)

AODV protocol uses on demand approach for finding routes; with these result the route is constructed on demand by the source node. The source node generates a RREQ packet and floods this route request packet to the neighboring nodes which intern update the sequence number and Time to live values before forwarding the RREQ to the next nodes. Whenever intermediate nodes receive the RREQ packet, if it has a route to the destination it intern replies unicast message, Route Reply (RREP) back to the source. If the route does not exists, intermediate node increments the broadcast ID and sequence number before forwarding to next node. The sequence number helps to avoid forwarding the same packet more than once. The figure 1. show node 1 generating a RREQ for node 3 which is destination.

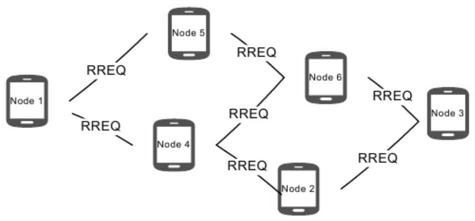

Fig. 1: Node 1 generates RREQ

Figure 1. Node 1 generates RREQ

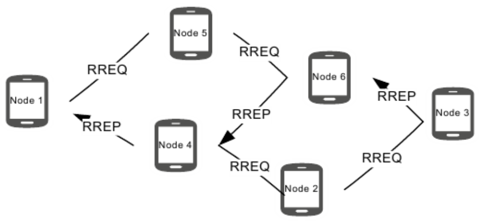

Fig. 2: RREQ and RREP

Fig. 2: RREQ and RREP

B. Route Reply phase (RREP)

Whenever an intermediate node receives a RREQ it updates the routing table entries with the node identifiers and also other information in its local routing table and later floods the same to neighboring nodes. The routing table entries now consist of Source IP address, Source seq. number, number of hops to source node, IP address of node from which RREQ was received.

If the RREQ reaches destination, it has to reply back to the source by sending the RREP packet. In this process the nodes verify whether there exists a better path by comparing the sequence numbers present in the routing table entries.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Special Issue 7, October 2015

The sequence number serves as a parameter to determine the freshness of the RREP packet. To conclude, it is the characteristic of AODV protocol that out of various route reply messages received by the source node from destination side, the source node considers the last RREP message which is fresh enough having higher sequence number is being selected for further route to be followed or a smaller hop count in RREP can be considered for data transmission. The figure 2. Shows the RREP from node 3 to node 1.

C. Path Maintenance phase

AODV protocol does not repair a broken route locally, the route error (RERR) message is sent whenever a link breaks which is determined by the periodically link level acknowledgements observed by source and destination nodes. Whenever a source node receives RERR message it has to retransmit the RREQ message to the neighboring nodes. Consider the example shown in figure 3, here as the path between node 6 and node 3 breaks, the node 4 checks for the existence of node 6 by sending the HELLO message, if it doesn't receive the HELLO message, node 4 initiates the oute error (RERR) message to inform their end nodes about the path break. After getting the RERR message end nodes of both sides delete the related information from their tables (buffer memory). The source node re-instantiate the route finding with new broadcast ID and prior destination sequence number.

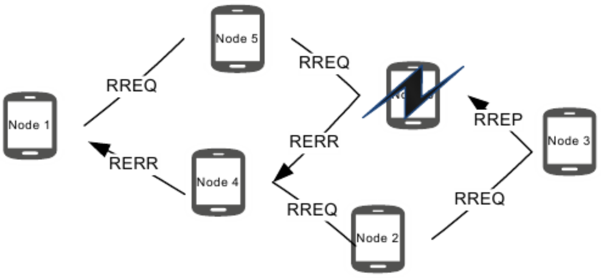

Fig. 3: RERR message for Path break

III. PROPOSED MODEL

Before discussing our proposal we would like to review the traditional RREQ format [3] of the conventional AODV protocol as shown in the Figure 4. These will enable us to understand the proposed routing scheme. he figure 4 shows the basic RREQ packet format which does not consider the QoS requirements of the applications. The RREQ packet is generated at the source as and when it requires sending data to destination, the RREQ is flooded to the neighboring nodes without considering the Bandwidth availability, Energy constraints at the neighboring nodes. The traditional AODV generates RERR message only when the path between the nodes brake due to mobility and out of range communication.

<table>
<tr><td>0 1 2 3 4 5 6 7</td><td colspan="3">0 1 2 3 4 5 6 7</td><td>0 1 2 3 4 5 6 7</td><td>0 1 2 3 4 5 6 7</td></tr>
<tr><td>Type</td><td>D</td><td>G</td><td colspan="2">Reserved</td><td>Hop Count</td></tr>
<tr><td colspan="6">RREQ ID</td></tr>
<tr><td>X_s</td><td colspan="3">Y_s</td><td>X_d</td><td>Y_d</td></tr>
<tr><td colspan="6">Destination IP Address</td></tr>
<tr><td colspan="6">Destination Sequence Number</td></tr>
<tr><td colspan="6">Originator IP Address</td></tr>
<tr><td colspan="6">Originator Sequence Number</td></tr>
<tr><td colspan="6">Path Node IP Address</td></tr>
<tr><td colspan="6">Path Node Sequence Number</td></tr>
<tr><td colspan="6">(additional path node IP address and sequence number pairs) ...</td></tr>
</table>

Fig. 4: RREQ packet format

In the proposed model we assume that every node is having adequate amount of energy to transfer the data from source to destination. The bandwidth availability at the node [8] is calculated by every node and whenever a request for QoS path arrives it has to be satisfied. The proposed system considers the basic AODV protocol packet formats and extends the RREQ and RREP packet formats to support delay sensitive applications. Perkins et al. [9] have extended the AODV RREQ and RREP packet formats for QoS support. RREQ and RREP can be extended to include QoS object extension formats such as Maximum Delay extension, Maximum Jitter extension, ICMP QoS Lost Message formats. The proposed model considers inclusion of two new field such as Ipr- Priority of the RREQ request and P- energy level of each node in the RREQ packet. The priority field Ipr can take either 0 or 1 values indicating less and high priority data transfer request. The energy field P indicates the available energy at each node.

IV. WORKING OF PROPOSED AODV PROTOCOL

During the route discovery process the source node that wants to find QoS route to the destination floods a QoS route request (RREQ) packet. The modified RREQ packet contains the following fields: packet type, source ID, destination ID, and sequence number, lpr- priority of data to be transmitted, P- energy level required at each node, route list, slot array list, data, and TTL. For each RREQ packet, the source node uses a new sequence number in order to avoid multiple forwarding of the same packet by intermediate nodes. The route list records the nodes that have been visited by the RREQ packet, where the slot array list records free slots available at each of these nodes. The TTL field limits the maximum length of the path to be found.

A. Route Discovery: The algorithm in Figure 5. show the working of Route Discovery in proposed system.

```
Ipr = Priority of the RREQ request
P = Energy level at the node
$Node_i$ = Intermediate node i
$A_i$ = Available Bandwidth at the node i.
Routelist- list of nodes that have been visited by RREQ
TTL- Time to Live value.
Slotarraylist- Nodes which satisfies the lpr and P.

For Every RREQ received at the node $Node_i$ perform the
following steps:

If ($Node_i$ is not the destination node)
{
        If ( $Ipr = 0$ and $P <$ threshold at $Node_i$)
        {
        Discard the RREQ
        }
        Else
        If ( $Ipr = 0$ and $P >$ threshold at $Node_i$)
        {
        Send the RREQ to next hop and also record the
        address of $Node_i$ in the Routelist.
        Decrement TTL
        }
        If ( $Ipr = 1$ and $P <$ threshold at $Node_i$)
        {
        Send the RREQ to next hop and also record the
        address of $Node_i$ in the Routelist and Slotarraylist.
        Decrement TTL
        }
        If ( $Ipr = 1$ and $P >$ threshold)
```

```
            {
            Send the RREQ to next hop and also record the
            address of $Node_i$ in the Routelist.
            Decrement TTL
            }
            Else
            Send generate Route Reply (RREP) back to source (if
            $Node_i$ is Destination )
}
```

Fig. 5: Algorithm for Route Discovery

Intermediate nodes forward the RREQ packet only if it has adequate bandwidth and energy level available just below the threshold value also the node addresses are updated in to Slot arraylist and Route list. If not the node address is only updated to Route ist which can be used later for path maintenance. In the proposed model, every routing table also has Slot arraylist which can be used by intermediate node to generate RREQ when it receives RERR message during path break. The Intermediate power (P) is of one bit and is used for representing low/high residual battery power of the node. Each node before Broadcasting a RREQ packet must check its residual battery power (defined as threshold value of battery) status for taking further action as either it is low or high, if low no broadcast else broadcast.

Another field for bandwidth estimation for high or low priority data (lpr) in the form of 0/1 for representing low/high is also being added to next reserved bit of RREQ, which shows that the RREQ should not be dropped if its available bandwidth is less than that of the requested level and if available bandwidth is already in use for data transfer of some other node, then intermediate node cannot afford for data transfer of high priority data so it does not forward the RREQ. All other nodes which has capacity equal to the requested should be allocated in path discovery and only those nodes are used for sending the delay sensitive data.

B. Modification in RREQ

Type	J	R	G	U	P	Lpr	Resereved	Hop count
RREQ ID								
Destination IP address								
Destination Sequence Number								
Originator IP address								
Originator Sequence Number								
Route List								
Slottedarraylist								

Fig. 6: Proposed RREQ packet format

Figure 6. Shows the RREQ format of the base protocol. Various fields related to the RREQ format are as follows:

- Type: 1 (It give the packet format type).
- J: Join flag; reserved for multicast.
- R: Repair flag; reserved for multicast.
- G: Gratuitous RREP flag; indicates whether a gratuitous RREP should be unicast to the node specified in the Destination IP Address field.
- D: Destination only flag; indicates only the destination may respond to this RREQ.
- U: Unknown sequence number; indicates the destination sequence number is Unknown.
- Reserved: Sent as 0; ignored on reception.

- Hop Count: The number of hops from the Originator
- P- energy level threshold
- lpr - priority of the data sent by source.
- Routelist - list of nodes visited by RREQ
- SlotArrayList- list of nodes satisfying the QoS requirements

C. Path Maintenance

In the proposed model, the path maintenance is achieved through dynamic generation of RREQ at the intermediate node level instead of source node reinstantiating RREQ for every path break. The figure 3. Shows Node 6 not able to send HELLO messages periodically to its neighbor nodes 4, 5, and node 2 to reinstantiate RREQ request for reaching destination node. The intermediate node 4. Removes the entry of node 6 from its routing table and immediately generates a fresh RREQ using the Slot arraylist stored in its routing table. Figure 7. shows the path maintenance phase where path between node 6 and node 3 breaks, the node 4 checks for the existence of node 6 by sending the HELLO message, if it doesn't receive the HELLO message, node 4 initiates the route error (RERR) message to inform their end nodes about the path break.

Instead of source resending the RREQ packet again, we can also modify the route discovery phase to fix the path break where it has happened, this can be done by using the Slot arraylist entry stored at node 4 for immediate path selection in the neighborhood and send RREQ to find path which satisfies the QoS requirements. Random selection of nodes from the neighborhood set increases the chance of full network coverage. Greater savings could be achieve by using a range dependent technique to select nodes for transmission but this can only be achieved at the cost of greater complexity at routing table entries.

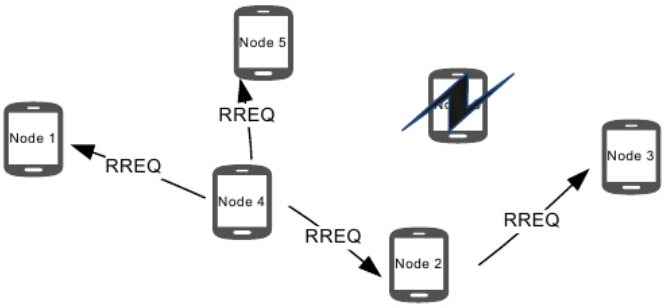

Fig. 7: Node 4 sending RREQ after path breakup

IV. Simulation Setup

In order to evaluate the performance of our QoS routing protocol, we simulated the proposed mechanism using Network Simulator NS-2.34[12]. The setup consists of following setup values

- Channel = Wireless channel
- Propagation = TwoRayGround
- MAC= 802.11
- Antenna = OmniAntenna
- Number of nodes = 50 nodes
- Area = 500500m
- Movement at a random destination every 30s
- Simulations run = 300s.

The proposed model has uses the newly added fields for bandwidth and delay sensitive routing operation by modifying the AODV.cc source file and also corresponding entries are modified in various files such as aodv-packet.h, aodv-rtable.h, aodv.h files for incorporating the Route list and Slot arraylist entries at each node. Performance Metrics In order to investigate the performance of these protocols, we used the following performance metrics:

• Packet Delivery Ratio (PDR): It is the ratio between the packets received at the destination and the packets generated by the sources.
• Routing Overhead: It is defined as the percentage of control packets with respect to the received data packets. Each hop of any control packets is computed as a new control packet.
• End-to-End Delay: It is the delay in transmitting data packets through wireless links plus the delay in the network interface queues due to network congestion.

The results obtained from simulation have significant improvement in the packet delivery ration and throughput with lesser end to end delay. The time taken for Route discovery in modified AODV is also less against traditional AODV, The time taken to re-establish the path whenever a path break happens is significant reduction, the number of packets delivered for a CBR data is increased along with improvements in throughput.

V. CONCLUSION AND FUTURE WORK

The proposed work extends the RREQ packet format for satisfying the requirements of delay sensitive applications, there is a significant improvement in packet delivery ratio, end-end delay and throughput. In the future work, we consider reducing the overhead of updating the Route list and slot arraylist for larger set of nodes and dynamic nature of network. Whenever a path is broken we can also have path re-negotiation at intermediate nodes which can significantly help in Delivery Ratio and throughput improvements for Manets.

REFERENCES

[1] C. Shiv Ram Murthy and B. S. Manoj, AdHoc Wireless Networks, Architectures and Protocols, Prentice Hall, 2004.
[2] Krishna Gorantala , ”Routing Protocols in Mobile Ad- hoc Networks ” Master’s Thesis in Computing Science, Umea University, SE-901 87 Umea, Sweden.
[3] Djamel Djenourix, Abdelouahid Derhabx, and Nadjib Badache, Ad hoc Networks Routing Protocols and Mobility, The International Arab Journal of InformationTechnology, April 2006, Vol 3, No. 2.
[4] S. Ramanathan and M. E. Steenstrup. 1996. A survey of routing techniques for mobile communications networks. MobileNetworks and Applications 1:98- 104.
[5] Juan Carlos Cano, Pietro Manzoni, A Performance Comparison of Energy Consumption for Mobile Ad Hoc Networks Routing Protocols, Proceedings of the 8th International Symposium on Modeling, analysis and Simulation of Computer and Telecommunication Systems, 2000, pp. 57 64.
[6] Krishna Gorantala, Routing Protocols in Mobile Ad-hoc Networks, Masters Thesis in Computing Science, Umea University, Sweden Department of Computing Science June 15, 2006.
[7] V. Kanakaris, D. Ndzi and D. Azzi, Ad-hoc Networks Energy Consumption: A review of the Ad-Hoc Routing Protocols, Journal of Engineering Science and Technology Review 3 (1) 162-167, 2010.
[8] C.R. Lin, J. Liu, QoS routing in ad hoc wireless networks, IEEE Journal on Selected Areas in Communications 17 (8) (1999) 14261438.
[9] C. E. Perkins, S.R. Das, and E. Royer, Ad-hoc on Demand Distance Vector (AODV). March 2000, http://www.ietf.org/internal-drafts/draft-ietf-manet- aodv-05.txt
[10] Abdullah, J., Parish, D., 2007, Impact of QoS Routing Metrics for MANETs in the Pervasive Computing Environment; International Conference on Wireless and Optical Communications Networks 2007, 2-4 July, 1-5.
[11] Qi Xue and Aura Ganz, Adhoc QoS in mobile adhoc networks, Journal of parallel and Distributed Computing, 2002.
[12] https://ns2 simulator - www.isi.edu/nsnam/ns