IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501
Vol.6, No 4, July-August 2016

QoS Based Routing In MANETs

Usha Sree
Department of Computer Science and Engineering
Vardhaman College of Engineering
Hyderabad, India
alugubelli.usha@gmail.com

S.Nageshwara Rao
Department of Computer Science and Engineering
Vardhaman College of Engineering
Hyderabad, India
nagsirisila@gmail.com

Abstract**—** Provisioning of QoS in MANets gained researchers concentration in recent years. In this paper, multiple QoS parameters are aggregated to define a node trust value which reflects its competence in routing protocol. In this paper, Link-Bandwidth and Node energy are considered as QoS parameters in trust evaluation. In route discovery to the destination node, a source node selects an intermediate node with higher trust values. By considering node bandwidth and energy, source node establishes a path towards the destination. So the proposed method could reduce the path breaks and increase the throughput by establishing the path with potential nodes. In the simulation, the proposed method outperforms the existing protocols.

Keywords*-QoS,MANets,Bandwidth,Energy,throughput.*

I. INTRODUCTION

A Mobile Adhoc Network(MANet) is a peer-to-peer network where the nodes communicate with each other without using infrastructure. The nodes in the network change their position dynamically. A MANet is a self-configuring, dynamic, self-directed and infrastructure-less network. The nodes in the network communicate with each other to exchange information without any centralized administration. Information is exchanged between the nodes using other nodes in the network as intermediate nodes. Nodes cooperate with each other to forward the data. The primary goal of MANet routing protocols[4][5][6] is to provide a correct route to transfer the data efficiently. These networks are suitable for a dynamic environment where no infrastructure is used, which is cost-effective.

Due to the special characteristics such as dynamic in nature, self-configured and infrastructure less, MANets are vulnerable to attacks. Providing security in MANets has always been a complex issue. The dynamic nature of MANets results in network connections unreliable, as the nodes change their locations continually. MANets are implemented without any centralized administration, monitoring the behavior of nodes is difficult. The resource limitations and the difficulties made implementing QoS metrics[9] necessary.

The remaining sections of the paper are organized as follows. In Section 2, short discussions on related work are presented. Protocols used in QoS routing in MANets are described briefly. Section 3 describes the proposed work. The parameters of quality and trust are described along with the proposed algorithm. The proposed method is explained by using an example network. Simulation setup is explained in section 4.Section 5 describes the results of the proposed method and the paper is concluded in section 6.

II. RELATED WORK

The primary goal of QoS routing protocols is to find an optimal path from source to destination which satisfies the QoS metrics. Different protocols have been proposed for QoS based MANET such as QAODV,DSDV[10] to determine the routing information.

2.1.QAODV

QAODV is QoS enabled Adhoc on-demand routing protocol which is based on route message(RREQ and RREP). In this when a source node tries to send a message to a destination nodes, it broadcasts the RREQ(route request) packet to its neighbor nodes. The node which receives the RREQ packet verifies whether the node is able to meet the requirements if the requirements are satisfied an RREQ is broadcasted to the forwarding nodes, and so on until route to the destination node is located, destination node uni-castes RREP to the source node[1].

The QoS parameters can be *Maximum Delay, Minimum Available Bandwidth*, *Node Energy* and *Link Expiry Time.* The route which satisfies all the requirements and having the maximum quality is used for broadcasting the data among the network.

2.2.QoS Optimized Link State Routing

QOLSR is an extension of OLSR protocol. The QoS constraints considered by this protocol are delay and throughput. As a proactive routing protocol, this has the advantage of having the routes immediately when needed.[2] This protocol uses Dijkstra’s shortest path algorithm to provide optimal routes. This inherits the stability of link state routing and supports multiple-metric routing criteria.

2.3.QoS Multicast Routing Protocol with Dynamic Group Topology(QMRPD)

QMRPD is a hybrid protocol. By this protocol, the overhead of creating a multicast tree for multiple QoS constraints can be reduced. When a member of the multicast tree joins or leaves dynamically, there will be no effect on the topology. This is best fit when multiple constraints have to be satisfied. The overall cost of the tree is minimum by this protocol[3]. The main objective is to make effective usage of network resources with respect to performance-based constraints as minimum bandwidth, delay-jitter bound. By this protocol, the dynamic membership of group handles with minimum number of message processing

III. PROPOSED METHOD

The proposed method implements Quality and Trust Parameters to provide secure transmission of data from source to destination. The Quality and Trust Parameters[7][8] are aggregated to provide security in terms of capability and attitude of the nodes. The capability is calculated by Quality parameters as Energy, Bandwidth, Link Expiry Time and the attitude is verified by trust parameter[12].

3.1.Quality Parameters

In this paper, Energy and Link Bandwidth metrics are using as Quality Parameters which are briefly explained in the following section.

3.1.1. Node Energy

Energy Efficient protocol design has always been a major issue in MANets. Every node has to spend some energy to transfer a packet to the forwarding node and to receive from a sender. E is the total energy utilized by a node to transfer a packet. As MANets are multicasting the destination nodes can be more than one node. S be the number of destination nodes. The total energy is

$$E = m_{send} \times size + \sum_{n \in S} (m_{recv} \times size) \quad (1)$$

where m_{send} is the cost of sending a packet

m_{recv} is the cost of receiving a packet

size is the size of data transferring.

3.1.2. Link Bandwidth

In MANets, available bandwidth throughput the route must be known from source to the destination to transfer the packets. Bandwidth can be calculated by using the time gap between the arrival time of packets at the receiving end.

A pair of packets is transferred with a time gap Δ_{in} and reaches at the receiver end with a time gap Δ_{out} is the time taken by the second packet to reach at the receiver end. The rate of transmission is $\frac{\Delta_{out} - \Delta_{in}}{\Delta_{in}} \times C$, C is the capacity of the link. Available Bandwidth is

$$B = C \times \left[1 - \frac{(\Delta_{out} - \Delta_{in})}{\Delta_{in}} \right] \quad (2)$$

3.2. Trust Factor

Trust plays an important role in transferring the data among networks. Trust is calculated based on the previous transfers at a certain node. The node which has transferred data more accurately i.e., the difference between the number of received and the number of packets sent through a network is minimum is considered as a trusted node.

In this paper, the quality parameters such as Node Energy and Link Bandwidth are used to calculate the Trust Factor[11]. It is also known as Certainty Factor(C_F) by using a formula described in the algorithm. C_F ranges between 0 and 1. A node having high Certainty Factor is used to transfer the data.

3.3.Algorithm

Algorithm(Energy-Bandwidth efficient reliable multicast routing**)**

{

1) Source node n_s sets the RREQ packet with the group ID and sends to all neighbor nodes. The RREQ packet included with the predefined values like
   - Threshold Bandwidth(T_{BW})
   - Threshold Energy(T_E) (use energy eq)
   - Source node reliability [0 1] (r_s)
   - Threshold value(Th)
2) On receiving RREQ packet, an intermediate node verifies the group ID to determine whether the entry is its own ID(destination node). if not, it takes its residual energy (N_E) and estimates link bandwidth(L_{BW}) with the node from which it received the RREQ packet and estimates the certainty factor (C_F) [0 1]

$$C_F = \left(\frac{N_E}{T_E} + \frac{L_{BW}}{T_{BW}} \right) \Big/ 2 \quad (3)$$

If($C_F > Th$)
{
//calculate node reliability value r_i

$$r_i = C_F * r_{i-1} \quad (4)$$

// r_{i-1} is the previous node reliability from which it got the RREQ,
Forward the RREQ packet by adding and its node-ID.
}
Else
{
Discard the RREQ packet
}

Note: if an intermediate node receives multiple RREQs, then it forwards a packet with high r_i value.

3) If the intermediate node's ID matched with the group ID(i.e one of the destination node). Destination node collects the RREQ packets from possible different paths and chose the packet with high-reliability value. Sends back RREP packet in the path, through which it received selected RREQ. 3
4) After receiving the RREP packets from all the destination nodes, source node establishes the paths to all destination node and start data transmission.

3.4.Example of multicasting routing

Consider a network with S as source node, D as the destination node and some intermediate nodes. The network have some predefined values as Threshold Bandwidth(T_{BW}) 5 Mbps, Threshold Energy(T_E) 20 J, Source node reliability [0 1] (r_s) 0.98, Threshold value(Th) 0.50. The nodes which satisfy the above threshold values are only considered to transfer the data. For every node (C_F, r_i) is calculated where C_F is the certainty factor calculated by using formula(2) and reliability of the present node r_i.

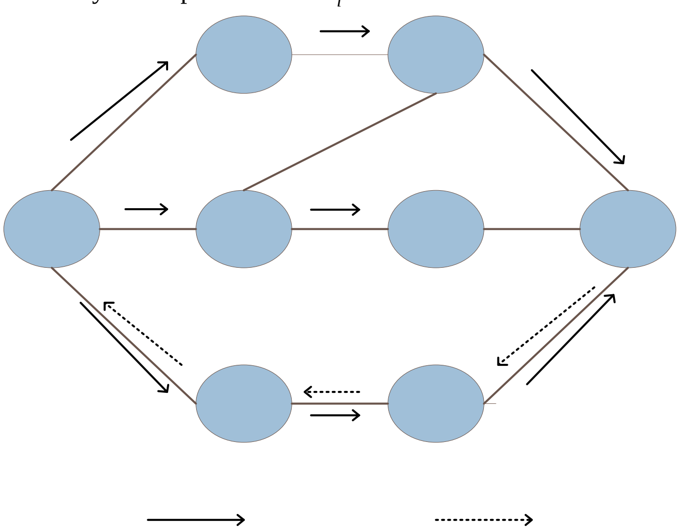

Figure 1.example network

When Source node S wants to share data with the destination node D, S sends an RREQ route request message to the neighboring nodes A, B, C with threshold values. On receiving the RREQ, the nodes A, B, C calculates their metrics as $(0.675, 0.66)$, $(0.6, 0.688)$, $(0.9, 0.882)$. All the nodes have enough metrics, so they update RREQ packets with their respective IDs and forward to next node. Nodes A, B, C forward the RREQ packets to X, Y, Z. On receiving RREQ packets they calculate their metrics as $(0.8, 0.528)$, $(0.4, \_)$, $(0.9, 0.79)$. But only X and Z are having enough QoS metrics, so the nodes X, Z update RREQ to the forwarding node D. Every destination node receives the RREQ packet with node IDs through which have come across. The destination node D receives RREQ packets through the paths (S, A, X), (S, B, X) and (S, C, Z). The route (S, C, Z) having high C_F, so the route is used to transfer the data from S to D.

IV. SIMULATION DETALS

Simulation is done in the NS-2 tool. In order to show the improvement in QoS paths(Network Size and Node Velocity) AODV and AQODV models were taken as the base for comparison. The proposed model hence forth referred as TBQM model.

5.1. Impact of node velocity:

Fig 2 describes the throughput for three protocols. Throughput reduced when nodes are moving with high velocity. The TBQM improves the throughput by considering the bandwidth in the estimation of node trust values.

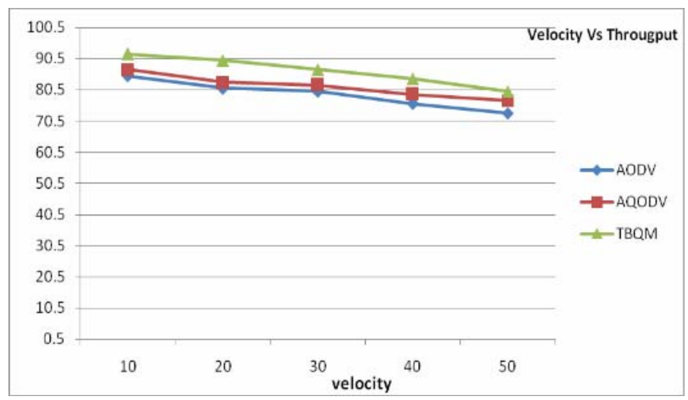

Figure 2:Throughput vs Node Velocity

5.2 Impact of Network Size:

In Fig 3, throughput parameter is evaluated. Throughput is reduced when network size is high.

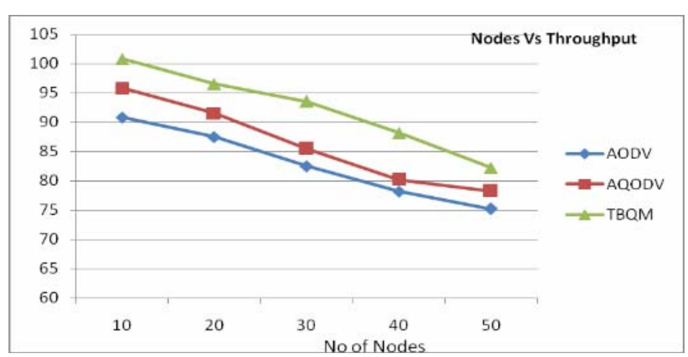

Figure 3: Throughput vs No of nodes

As depicted in Fig 4, Energy Consumption parameter is evaluated among three protocols AODV, AQODV and TBQM. There is a noteworthy change in the overall energy consumption for network size in all protocols. The TBQM(Trust Based QoS Model) uses low energy for different network sizes. As the network size increases the energy consumption is decreasing but TBQM using less energy compared to other two protocols. Hence, TBQM is better than other two protocols which are depicted through the results.

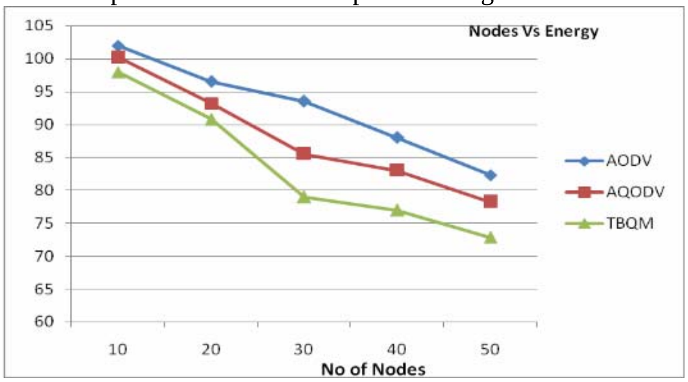

Figure 4: energy vs No of Nodes

V. CONCLUSION

Mobile Adhoc Network is infrastructure-less networks, due to which nodes mobility's provisioning of QoS is not an easy task. Here for every node in the network, a trust value is evaluated. Since the proposed method is the extension AODV protocol, does not require any packet changes in the experimental measures the performance is measured for the parameters bandwidth and energy. Comparison of AODV, AQODV and TBQM protocols is done by considering the performance metrics such as packet delivery ratio, energy consumption. Several simulations have performed under different network conditions to analyze the performance of modified protocol with TBQM. The analysis of results showed that there is a very slight change in packet delivery but a remarkable change in energy consumption. Packet delivery is low for highly dense network for all speed variations. The TBQM consumes less energy for the dense network . It is observed that overall energy consumption of the network is decreased. TBQM due to its energy efficient feature can be used for the energy constrained applications. The Proposed method measures better performance than the existing protocols.

REFERENCES

[1] Ruihui Mu and Wuqiang Zhang, "QAODV: Improved Security Routing Protocol of AODV", Journal of Networks, VOL. 8,pp.2400-2405,2013

[2] Hassan Sinky and Bechir Hamdaoui, "Optimized link state routing for quality-of-service provisioning: implementation, measurement, and performance evaluation",Wireless Communications and Mobile Computing, pp. 937-948, 2014

[3] Li Layuan, Li Chunlin," A QoS multicast routing protocol for dynamic group topology", Journal of Information sciences,VOL 169,pp. 113-130

[4] Sanjeev Gangwar1 , DR. Saurabh Pal1 and DR. Krishan Kumar, "Mobile Ad Hoc Networks: A Comparative Study of QoS Routing Protocols", IJCSET ,Vol 2, pp.771-775,2012

[5] G. Santhi1 and Alamelu Nachiappan," A Survey of QoS routing protocols for Mobile ADHOC Networks", International journal of computer science & information Technology (IJCSIT) Vol.2, No.4, August 2010

[6] CH. V. Raghavendran1 G. Naga Satish2 P. Suresh Varma3 K.N.S.L. Kumar," Challenges and Advances in QoS Routing Protocols for Mobile Ad Hoc Networks", ijarcsse,VOL 3, pp.121-127,2013

[7] S. R. Biradar, Subir Kumar Sarkar, Rajanna K M, Puttamadappa C, "Analysis QoS Parameters for MANETs Routing Protocols", IJCSE, VOL 2, pp.593-599

[8] D.Umuhoza, J.I.Agbinya, C.W.Omlin, "Estimation of Trust Metrices for Manet Using QoS parameters and source routing Alogorithms",IEEE,2007

[9] Evgeny Khorov, Alexander Safonov, "Multiple Metrics in MANET with End-to-End QoS Support for Unicast and Multicast Traffic", Third International Workshop, MACOM 2010, , pp 251-262,2010

[10] Prof. B.N. Jagdale1 , Prof. Pragati Patil2 , "Analysis and Comparison of Distance Vector, DSDV and AODV Protocol of MANET", International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.2,pp.121-131,2012.

[11] Sirisala, NageswaraRao.; C.Shoba Bindu. 2014 "Weightage based trusted QoS protocol in Mobile Adhoc Networks", IEEE Global Conference on Wireless Computing and Networking (GCWCN), pp.283-287.

[12] Sirisala, NageswaraRao.; C.Shoba Bindu " Fuzzy Based Quality of Service Trust Model for Multicast Routing in Mobile Adhoc Networks" International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 12 (2015) pp. 32175-32194