Enhanced QoS Multicast Routing Protocol in MANETs using Trust and Load Balance

Srinivasulu Sirisala, Rama Krishna. S

Abstract: ***Mobile ad-hoc network (MANET) is a wireless networks without fixed infrastructure, where each node can interact with its one hop distance neighbors only. Since the nodes are continuously moving from one location to another location, the network topology is not constant. Provisioning of Quality of Service (QoS) in MANETs is a challenging task because of its unstable nature. In multicast routing protocol, a sender node is sending the data to the group of members (multiple destination nodes), where the intermediate nodes resources are consumed at higher rate. In this paper, utilization of node resources (QoS parameters) is minimized by considering node attitude (trust) and load balancing. Here node energy and link bandwidth are considered as the QoS parameters. The proposed method "Enhanced QoS Multicast Routing Protocol in MANETs Using Trust and Load Balance-QMTL" identifies the intermediate nodes with higher trust values and constructs the multicast tree with optimized load balance. The performance of proposed method is analyzed theoretically (using asymptotic notations) and practically (using simulation tool-ns2)..***

Keywords: Quality of Service, Multicast tree, node energy, Bandwidth, trust.

I. INTRODUCTION

In MANETs, the applications are run with the collective effort and cooperation of nodes. Each node has to participate with unknown nodes for the completion of tasks. Hence the assessment of each node behavior definitely useful to improve the effectiveness of applications.

In multicast routing a source node will form the multicast tree, where it sits at root position and all the target nodes are at leaf level. In multicast routing, a source node simultaneously sends the same message to a group of targets. Here the source node keep sending same copies of messages to all destination nodes [16]. In QoS multicasting, the applications required certain level of quality end to end from source to destination nodes. Hence the routes from source to destination nodes should maintain the required level of quality while the applications are running in the network [10,15,17,25,26,27].

In MANETs high prioritized QoS Parameters are energy and bandwidth. Bandwidth calculation [9] at a node is a difficult job, bandwidth is a QoS parameter is assessed as a set of free time slots in TDMA process [29]. In [30] LajosHanzo II etc.. discussed admission control schemes for effective utilization of bandwidth. Admission control is a method assess the bandwidth availability and controls the data traffic accordingly. MANETs are decentralized wireless networks and nodes are provided with limited battery energy and the nature of MANETs is unstable topology, hop based delivery of packets and wireless communication, all these makes the nodes battery drains out fast. Nodes spent most of their energy not only in sending their packets but also forwarding packets of others. There was a lot of research was happen, many energy aware protocols [7,8,14] were proposed to reduce energy consumption in MANETs few of them dealt this issue by controlling the broadcast traffic and few suggested spanning tree and some other[28] do the collision prediction so that collision can be avoided as a result energy can be saved and etc. The multicast routing approach, nodes battery energy exhausts very quickly due to the jobs of multicast tree build up and to send the same data to several target nodes. [11].

Nodes in MANETs have inadequate quantity of resources where the complex algorithms can't be suggested. Hence the highly complicated encryption algorithms are not recommended to run the applications in secure environment. The alternate methods are soft security methods, i.e. trust mechanisms. In trust methods each node behavior is observed over the period of time and be rated with some trust value [1,2]. The applications in the MANETs select the nodes with good trust values to improve the performance. Here the node trust is evaluated based on it's packet forwarding ratio. The construction of multicast can greatly influence the performance of multicast protocol. Hence in the construction of tree, the intermediate nodes should not have more number of neighbor nodes so that the load can be balanced evenly along the multicast tree.

II. RELATED WORK

In the literature, there are many multicast routing protocols are proposed, which are classified into mesh based protocols [21] and tree based protocols [20, 23, 24]. Here the MAODV [19] and PMRP [12] multicast protocols are discussed.

A. Multicast Ad Hoc on-Demand Distances Vector Protocol (MAODV)

In MAODV, for establishing the path from source to destination, unlike AODV (unicast) it uses broadcast approach with same mechanism of route request (RREQ) and route reply(RREP) as it was referred in the AODV.

If a node suppose to be a part of multicast tree or wants to send a data to multicast group to which it has not available with route information in its routing table then it broadcasts a RREQ packet.

Any node on the path to target multicast group on receiving the join RREQ it rebroadcasts further until it reaches any one of the members of target multicast group and it gets RREP packet from a node with sequence number stored in it which is greater than the sequence number in stored in RREQ. For non join request any node having

Revised Manuscript Received on January 15, 2020.

Srinivasulu Sirisala *, Research Scholar, Department of Computer Science, SVU college of CM&CS, Tirupathi, India. Email: vasusirisala@gmail.com

Rama Krishna. S, Professor, Department of Computer Science, SVU College of CM&CS, Tirupathi, India. Email: drsramakrishna@yahoo.com

unexpired path to target node responds to the source in unicast mode with RRES packet by storing sequence number in it. In the journey of RREP packet each node on the path to the source will add routing table and multicast route table entry to the RREP packet as shown in Fig. 1. So that this information is useful for a source for data packet forwarding. Source on receiving many RREP packets from various nodes keeps the path with less hop count and highest sequence number and drops all other paths and unicasts to the next hop along that route a MACT message. This message set up the path. In multicast tree link status of next hop node is maintained by every node hence link failure easily detected and can be repaired using RREQ/RREP/MACT messages.

In multicast tree there is a specially designated node called group leader bear the responsibility of initializing and distribution of updated sequence number of multicast tree. It is useful in recovery process of multicast tree from the failures.

B. Power Aware Multicast Routing Protocol (PMRP)

PMRP is a multicast routing protocol in which data transmission is done by constructing multi cast tree. This protocol accomplishes the routing in two phases, route discovery phase and route maintenance phase.

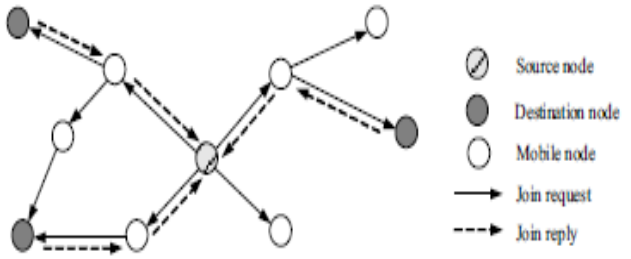

Fig. 1. Route discovery of MAODV protocol

B.1. Route discovery phase:

PMRP as it is on demand protocol, the multicast tree paths updated when ever source wants to send data. Path establishment is done using HELLO, RREQ and RREP packets. In PMRP, at the frequent intervals HELLO packets are exchanged between the neighbor nodes so that every node will come to know the distance to its neighbor nodes. In PMRP the node which wants to send the data treated as root of multicast tree and it broadcast the RREQ packet. The RREQ packet included with node's mobility information (location, velocity and direction).

In PMRP in selection of paths four parameters are considered, $P_{prediction}$, P_{remain} , link expiration time (LET) and the route expiration time (RET). $P_{prediction}$ is the estimation of the energy that each intermediate node should have to forward source data successfully, P_{remain} is the actual residual energy of the node, LET is the link existence time between two nodes and RET is equivalent to the least value of the set of LETs for the path which was set up.

Any intermediate node on receiving the RREQ it confirms itself whether it is a part of multicast tree or not using broad cast ID. If it is not, it computes $P_{prediction}$ if its $P_{prediction} < P_{remain}$ i.e node is not having sufficient energy to forwards the request so that it drops the RREQ. Otherwise node discriminates the RREQ packet to its neighbors. Each destination node after receiving RREQs from all its neighbors it will choose the path with minimum of LETs and maximum RET value .then each destination sends the RREP packet along the selected path.

B.2. Route maintenance phase:

In this phase PMRP handles the issues Multicast join, node pruning and link breakage.

Multicast Join:

Usually when a node send a join request packet, it gets response from a member node of multicast tree to which node wants be a member but if join request is received by a non member node of a target multicast tree then that node adds the reverse route entry and broadcast to the members of the targeted multicast tree. Each node of the multicast tree after receiving all join packets came from various paths select the path with highest RET and sends join reply packet stored with LET value along the selected path. On receiving the join reply packets the sender of the join request in its routing table do the entry of path which having minimum LET.

Node pruning:

When a node pruning was happened the pruned node sends the quit request packet to the upstream nodes. If the immediate upstream node is leaf node that node also gets pruned and discriminate quit request packet to its neighbors. This is how every node of multicast tree know about pruned node, accordingly they gets updated their routing tables.

Link breakage:

Link breakage is a frequent activity in MANETs due to the mobility of the nodes. In PMRP nodes' mobility is predicted and LETs and RETs is calculated accordingly. With this information link maintenance process will be initiated before link gets break. The upstream node of the link will send a route request repair (RREQ_R) to the downstream nodes. On receiving RREQ_R every downstream node computes $P_{prediction}$ and compares with $P_{remain.}$ If it is less than $P_{remain,}$ then it adds LET to the RREQ_R and do the broadcast. Otherwise drops the RREQ_R packet. After certain time every downstream node gather many RREQ_R packets and selects a route with high RET and send a reply repair(RREP_R) packet to the upstream node. So that upstream node will get an alternative path before link gets fail.

III. SYSTEM MODEL

In this section some of the metrics are discussed to make the understanding of proposed method easier to the reader. Here the QoS parameters bandwidth and energy evaluation is discussed. Trust computation of a node is explained. Which are used in the proposed method (QMTL) for the construction of multicast tree.

A. Energy calculation

The forwarding energy of an intermediate node is estimated based on the source data size and the distance between forwarding and receiving nodes [5,6,22]. The forwarding energy is the sum of transmission and receiving energies.

$$T_E(b,r) = E_{act} \times b + Amp_e \times b \times r \times r \quad (1)$$

In Eq. (1) $T_E()$ is the transmission energy, E_{act} is the node activation energy, Amp_e is the amplification energy, b is the data size in bits and r is the node's range of communication.

$$R_e(b) = E_{act} \times b \quad (2)$$

In Eq. (2) receiving energy- $R_e()$ is calculated.

$$Total_e = E_{tr} \times b + Amp_e \times b \times r \times r + E_{tr} \times b \quad (3)$$

In Eq. (3) the forwarding total energy is calculated.

B. Band width calculation using TDMA

According to Time Division Multiple Access-TDMA [11], the link band width between two nodes is estimated based on their available common free slots [13]. In TDMA the time slots are classified as transmission time slots and receiving time slots. If node n_i want to transmit the data to node n_j, then the current slot is not already allocated and not scheduled as the receiving slot of any neighbor(k) of node n_j as shown in Eq. (4).

$$T_i(t) = \{t \notin TransSlot_i, t \notin \text{Re}ceiveSlot_i, t \notin \text{Re}ceiveSlot_k\} \quad (4)$$

If node n_i want to receive the data from node n_j, then the current slot is not already allocated and not scheduled as the transmission slot of any neighbor(k) of node n_j as shown in Eq.(5).

$$R_i(t) = \{t \notin TransSlot_i, t \notin \text{Re}ceiveSlot_i, t \notin TransSlot_k\} \quad (5)$$

C. Node trust computation

In MANETs, a node trust computation is computed based on its packet forwarding ratio. i.e. how many packets a node received and among them how many packets its forwarded correctly. In MANETs trust computation methods broadly categorized into two types i.e. direct method and indirect method [3,4,18]. in direct method a node can asses all of it's one hop neighbor nodes through direct interactions. In indirect trust computation, a node can compute it's multi hop away neighbor node trust values considering recommendations of other nodes. In Eq. (6) the direct trust of node-i (DT(i)) is estimated based on packet forwarding ratio of different packets(i.e route reply-RREP, route request-RREQ and Data packets). Each packet is assigned some weightage using weightage functions where the sum of these functions are equal to 1 as shown in Eq. (10). The terminology that is used in Eq. (6,7,8) is discussed in Table I.

$$DT(i) = \left\{ \begin{matrix} f_1(RREP\_f) \times RREP\_f + f_2(RREQ\_f) \\ \times RREQ\_f + f_3(Data\_f) \times Data\_f \end{matrix} \right\} \quad (6)$$

Table- I: Trust computation terminology

$DT(i)$	Direct Trust of node-i
$f_1(RREP\_f)$	Weightage function of Route Reply packets
$RREP\_f$	Route Reply packets forwarding ratio
$f_2(RREQ\_f)$	Weightage function of Route Request packets
$RREQ\_f$	Route Request packets forwarding ratio
$f_3(Data\_f)$	Weightage function of Data packets
$Data\_f$	Data packets forwarding ratio

$$RREP\_f = \frac{RREP_s - RREP_f}{RREP_s + RREP_f} \quad (7)$$

In Eq(7) $RREP_s$ and $RREP_f$ refer the number of Route Reply packets that are forwarded and dropped respectively.

$$RREQ\_f = \frac{RREQ_s - RREQ_f}{RREQ_s + RREQ_f} \quad (8)$$

In Eq. (8) $RREQ_s$ and $RREQ_f$ refer the number of Route Request packets that are forwarded and dropped respectively

$$DATA\_f = \frac{DATA_s - DATA_f}{DATA_s + DATA_f} \quad (9)$$

In Eq. (9) $DATA_s$ and $DATA_f$ refer the amount of Data packets that are forwarded and dropped respectively.

$$f_1(RREP\_f) + f_2(RREQ\_f) + f_3(Data\_f) = 1 \quad (10)$$

IV. ENHANCED QOS MULTICAST ROUTING PROTOCOL IN MANETS USING TRUST AND LOAD BALANCE-QMTL

In this section, caveats in the classical multicast tree formation are discussed in terms of load balance. Which is considered as the motivation of proposed method. Next the the proposed routing protocol (QoS Multicast Routing Protocol in MANETs using Trust and Load Balance-QMTL) is discussed and explained over the example network. The performance of proposed method is discussed theoretically using asymptotic notations.

In Fig. 4. Proposed QMTL flows of actions are described.

A. Caveats in the classical multicast tree construction

In Fig. 2, the multicast tree is formed using classical multicast tree. Where S is the source node and (E,F,C) are destination nodes. Here the intermediate node B is the connecting node to all the destination nodes. Hence the node B is over burdened with data communication to all destination nodes. If any of the

links to it's neighbor nodes (i.e. D, F and C) are broken, then node B has to find out alternate paths through nodes X, Y and Z to the destination nodes E, F and C respectively. Hence the node along the multicast tree which has more number of downstream nodes as neighbor nodes is over burdened. This is the drawback of existing multicast trees.

The proposed method ensures that the intermediate node should not have more than threshold level of downstream nodes as neighbor nodes which can achieve the load balance in the network. In the further section the modified multicast routing route discovery process is explained

B. QMTL Route discovery process

Step 1: A source node sends the route request RREQ packets to all its neighbor nodes with its application requirements (i.e. energy, bandwidth and trust). On receiving request packet, each neighbor node verifies its residual energy is greater than required energy. (i.e. $P_{prediction} < P_{remain}$).

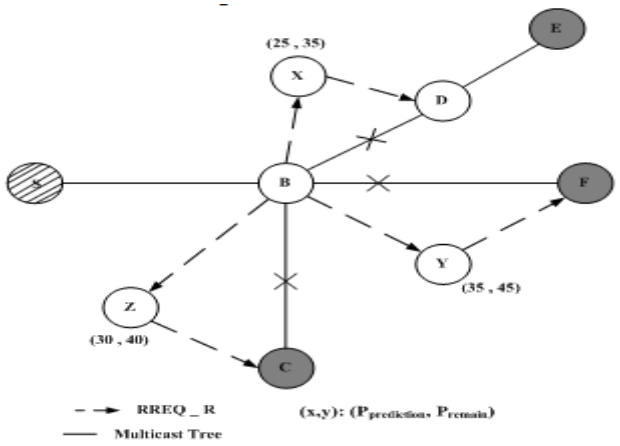

Fig. 2. Route Maintenance

.Step 2*:* If the node is capable to process the request, then it adds its trust value and residual energy to the request packet along with its id and forwards to the next hop node. If it is not capable then simply ignores the request packet.

Step 3*:* Each destination node collected with many request packets through multiple possible routes. For each route, it estimates the end-to-end route trust value and energy. Destination node selects the route which is trust wise and energy wise worthy and sends the reply RREP to the source node. if destination has alternative paths, then it sets the AP field in RREP as 1. Otherwise it remains as 0. In figure 3, (RREP packet structure is same as in [12] with extra field AP).

Step 4: Each intermediate node may receive multiple reply packet from its downstream nodes. If it has received single packet, simply forwards to upstream node or if it has received multiple packets, then it estimates the link band width with all its downstream nodes, from those it received reply packets.

Step 5: If the calculated bandwidth is higher than threshold band width, then it forwards all the reply packets. If the bandwidth is less then threshold value then it drops the reply packet with AP field value 1 and intimates concerned destination through route failure packet by adding its id as shown in Fig. 3.

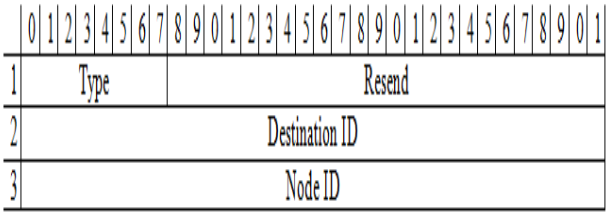

Fig. 3. RREP_F packet format

Step 6: On receiving route failure packet, the destination node chooses the alternative path to the source node and sends the reply packet.

Step 7: Always the proposed method can restrict on the count of branches at intermediate node and can achieve the load balance.

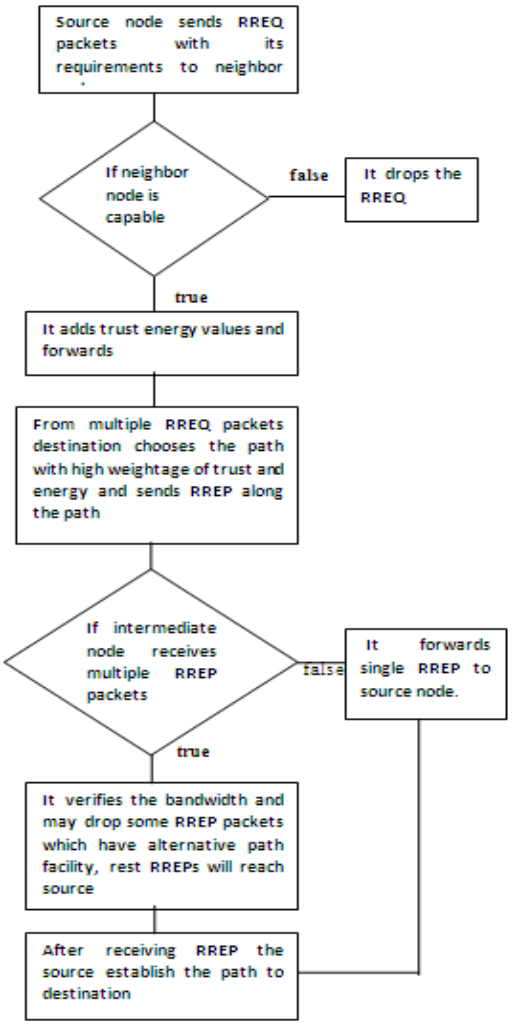

Fig. 4. Working model of proposed QMTL.

C. An Example of QMTL Multicast Routing

The proposed routing protocol is explained over the example network as shown in Fig. 5 and 6. In Fig. 5, source node S sends the route request packets to its one hop neighbors i.e. A, X and B with its requirements. On receiving request, all these nodes evaluates their ($P_{predict\ ion}$, P_{remain}) as (30, 40), (36, 30) and (25, 35) respectively. But the node X is not capable since its P-remain is less than P-prediction.

Now the capable nodes (A and B) adds its trust value to the request packet (evaluated by its upstream node) and forwards to the next hop nodes (i.e . 5 and 6 respectively).

The destination node E receives the request packets through (S, A, E) and (S, B, D, E). These routes trust values are 4, 5 respectively (minimum of all intermediate nodes trust value). Node E chooses the path (S, B, D, E) and sends the reply packet. in the same manner destination nodes F and C choose the routes (S,B,F) and (S,B,C) as with trust values as 5 and 5 respectively.

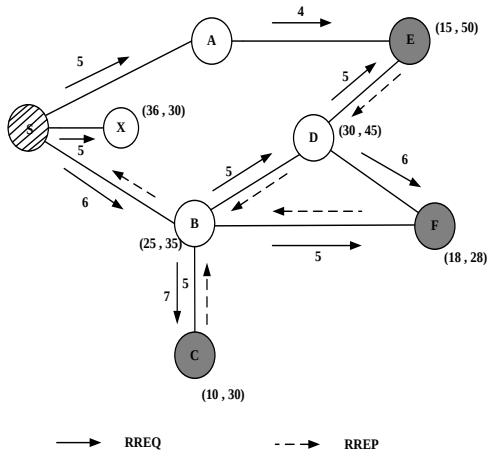

Fig. 5. Route Request in QMTL.

In Fig.6, all the destination nodes selects the routes through the common intermediate node i.e. node B, hence it is over loaded. But the node B should not allow all the reply packets. It drops the reply packet from node E, since node E has alternative path. The node E selects the alternative path through node A.

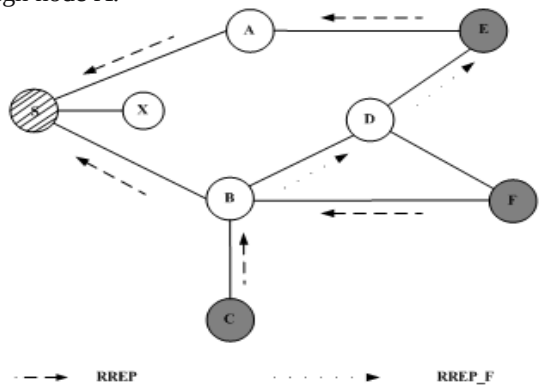

Fig. 6. Route Replay Phase in QMTL

In Fig. 7, after receiving reply packets, the source node construct the multicast tree where the paths to all destination nodes are trust worthy, have threshold energy and load is balanced.

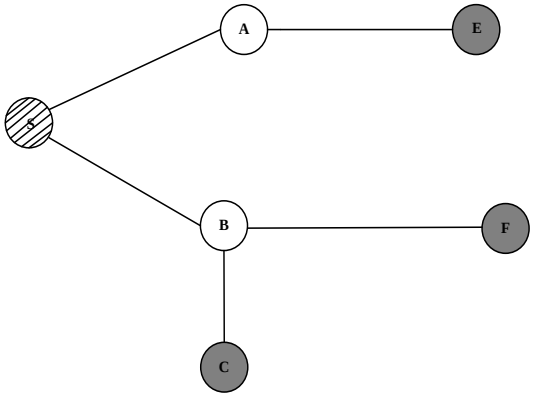

Fig. 7. Multicast Tree in QMTL.

D. Theatrical performance analysis of proposed method

The proposed doesn't use any additional packets over the classical protocols. In evaluation of link bandwidth it spends the time $O(m * t)$ where m is number of neighbor nodes and t is time slots. in trust evaluation it takes $O(n)$ time , where n is the number of nodes in network. in energy calculation it takes $O(m)$ time. Here RREPF packet is introduced but because of its small size doesn't have any impact on performance.

V. RESULTS

In this section, the simulation environment is introduced and simulation parameters are defined. The proposed method QMTL performance is compared with existing methods MAODV and PMRP.

A. Simulation environment

Here the network simulator ns2.34 is used to measure the performance of proposed method. The simulation is run over the area 1400×1400 and the simulation duration is 600sec. Each data packet size in the transmission is 0.3B and the transmission rate is 0.5 Mbps.

B. Simulation parameters

The performance of proposed method is compared with the existing methods MAODV and PMRP in terms of parameters delay, throughput and control overhead for the varying of network sizes and velocities. Here the number of nodes is taken from 10-50. The node velocity is considered from 0-40 m/sec.

Table- 2: Node velocity Vs Avg packet delay

	Average Packet Delay (Sec)		
Node Velocity (m/sec)	MAODV	PMRP	Proposed QMTL
0	0.446	0.412	**0.399**
5	0.458	0.428	**0.418**
10	0.498	0.478	**0.458**
15	0.518	0.499	**0.459**
20	0.608	0.541	**0.481**
25	0.667	0.591	**0.521**
30	0.690	0.611	**0.542**
35	0.704	0.647	**0.590**
40	0.708	0.677	**0.620**

In Table- 2, when the nodes are moving with higher velocities, then links will be broken and retransmission of data required. So the end to end packet delay is increased. But the QMTL can decrease the link breaks and reduce the delay.

Table- 3: Nodes Vs throughput.

	Throughput (mbps)		
Number of Nodes	MAODV	PMRP	Proposed QMTL
10	17.628	18.360	**18.003**
20	15.828	16.400	**17.428**
30	13.261	14.872	**16.264**
40	11.431	12.653	**14.286**
50	9.096	10.682	**13.763**
60	8.632	9.875	**12.347**

In Table- 3:., when nodes are increased then in the multicast tree, an intermediate node may have multiple branches which reduces the bandwidth and throughput. The QMTL can reduce these branches and improve the throughput and load balance.

Table 4: Nodes Vs Avg packet delay

	Packet Delay (Sec)		
Number of Nodes	MAODV	PMRP	Proposed QMTL
10	0.428	0.421	**0.408**
20	0.498	0.478	**0.458**
30	0.568	0.523	**0.513**
40	0.620	0.594	**0.556**
50	0.700	0.679	**0.620**
60	0.780	0.710	**0.650**

In Table 4, when network is with high density of nodes (more nodes) then the route maintenance work is increased. In case of path failure the routing protocol requires much time to find out the alternative path. Hence the packet delay is increases.

Table 5: Node velocity VS control over head

	Control packet overhead		
Node Velocity (m/sec)	MAODV	PMRP	Proposed QMTL
0	0.743	0.708	**0.708**
5	0.752	0.743	**0.717**
10	0.773	0.765	**0.739**
15	0.795	0.778	**0.752**
20	0.817	0.804	**0.769**
25	0.830	0.817	**0.791**
30	0.843	0.826	**0.800**
35	0.856	0.839	**0.821**
40	0.860	0.839	**0.826**

In Table 5, the results are depicting that when nodes are moving with increased velocity then path breaks occurs and the protocol has to use control packet to find out alternative path. Hence the COH is increased. But the QMTL is not deployed any additional control packets so the COH is inacceptable range.

VI. CONCLUSION AND FUTURE WORK

In the proposed method QMTL, the QoS routing is improved by considering node attitude (trust) and load balance in the network. The proposed method used the QoS parameters as energy and bandwidth. Here the conventional multicast routing protocols is enhanced to form the multicast tree, such that the total load is evenly distributed to all the intermediate nodes while the data is transferred. The QMTL considers energy, bandwidth and trust values of nodes. Hence it could improve the throughput and reduce the link breaks. The proposed method performance is analyzed theoretically and practically (simulation). Where it could outperforms the existing protocols MAODV and PMRP. Mobile Ad-hoc networks have common properties with social networks, where the entities participating with unknown other entities. Hence the trust model which is used in this work can also be used in social networks to identify and avoiding of malicious activities.

REFERENCES

1. Priya Sethuraman and N. Kannan , “Refined trust energy-ad hoc on demand distance vector (ReTE-AODV) routing algorithm for secured routing in MANET” *journal of wireless networks*, Vol 22, pp1-11,2016.
2. NageswaraRao Sirisala and C.Shoba Bindu.” A Novel QoS Trust Computation in MANETs Using Fuzzy Petri Nets”, *International Journal of Intelligent Engineering and Systems*, Vol.10, No.2, pp 116-125,2017.
3. NageswaraRao Sirisala and C.Shoba Bindu. “Recommendations Based QoS Trust Aggregation and Routing in Mobile Adhoc Networks”, *International Journal of Communication Networks and Information Security (IJCNIS)*, Vol 8, No 3, pp 215-220, 2016.
4. Muhammad Saleem Khan and Majid Iqbal Khan,“MATF: a multi-attribute trust frameworkfor MANETs”, *EURASIP Journal on Wireless Communications and Networking* , vol 2016,pp1-17, 2016.
5. Zijian Wang , Eyuphan Bulut, Boleslaw K. Szymanski .” Energy-efficient location services for mobile ad hoc networks”. Ad Hoc Networks 11. pp.273–287, 2013.
6. S.Sridhara, R.Baskaranb, P.Chandrasekarc,”The Energy supported AODV (EN-AODV) for QoS routing in MANET”, *2nd International Conference on Integrated Information*. Procedia - Social and Behavioral Sciences 73, pp.294 – 301, 2013.
7. Nicola Costagliola · Pedro Garçia López ·Francesco Oliviero · Simon Pietro Romano,” Energy- and Delay-Efficient Routing in Mobile Ad Hoc Networks”. *Mobile Network Applications* vol. 17 pp:281–297, 2012.
8. Ruifeng Zhang, Olivier Berder, Jean-Marie Gorce , Olivier Sentieys a “Energy–delay trade off in wireless multihop networks with unreliable links “, *Ad Hoc Networks 10* , pp: 1306–1321, 2012.
9. Chia-Cheng Hu, Eric Hsiao-Kuang Wu, Gen-Huey Chen, “bandwidth-Satisfied Multicast Trees in MANETs”. *IEEE Transactions On Mobile Computing*, Vol. 7, No. 6,pp:712-723, June 2008.
10. Mina Masoudifar, “A review and performance comparison of QoS multicast routing protocols for MANETs” *Ad Hoc Networks 7(6)*, pp:1150–1155, 2009.
11. Kuei-Ping Shih. "A TDMA-based bandwidth reservation protocol for QoS routing in a wireless mobile ad hoc network", *IEEE International Conference on Communications Conference Proceedings ICC 2002* (Cat No 02CH37333) ICC-02, 2002.
12. Nen-Chung Wang, Yung-Fa Huang · Yu-Li Su "A Power-Aware Multicast Routing Protocol for Mobile Ad Hoc Networks With Mobility Prediction", *Wireless Personal Communications* 43:pp.1479–1497,2007.
13. Zhu, C. and Corson, M. S., 2000, "BandwidthCalculation in a TDMA-based Ad Hoc Network," *Institute for Systems Research (ISR)*, Technical Reports: TR 2000-47, http://hdl.handle.net/1903/6173.
14. Guo, S.. "Energy-aware multicasting in wireless ad hoc networks: A survey and discussion", *Computer Communications*, Vol 30 Issue 9, , pp: 2129-2148, June 2007.
15. Huayi Wu, Xiaohua Jia,” QoS multicast routing by using multiple paths/trees in wireless ad hoc networks” *Ad Hoc Networks* Vol 5, Issue 5, pp: 600-612, July 2007.
16. Luo Junhai, Ye Danxia, Xue Liu, and Fan Mingyu, “A Survey of Multicast Routing Protocols for Mobile Ad-Hoc Networks”. Communications Surveys & Tutorials, IEEE Vol. 11 , Issue: 1 ,pp.78 - 91 ,2009.
17. “A Survey of Routing Protocols that Support QoS in Mobile Ad Hoc Networks”, *IEEE Network* • Vol. 21 , Issue: 6 , pp30-38, 2007.
18. NageswaraRao Sirisala and C.Shoba Bindu. Uncertain Rule Based Fuzzy Logic QoS Trust Model in MANETs, *International Conference on Advanced Computing and Communications -ADCOM, (IITM PhD forum)*,pp.55-60, 2015.
19. Royer, E.M. & Perkins, C. E. “Multicast AODV”, (1999). In Proceedings of the *ACM MOBICOM*, pp. 207–218, August 1999.
20. Baolin, S., & Layuan, L. “On the reliability of MAODV in ad hoc networks”. In Proceedings of the 2005 *IEEE international symposium on microwave, antenna, propagation and EMC technologies for wireless communications*, Vol. 2, pp. 1514–1517, August 2005.
21. Das, S. K., Manoj, B. S., & Murthy, C. S. R. “A dynamic core based multicast routing protocol for ad hoc wireless network”. In Proceedings of the *third ACM international symposium on mobile ad hoc networking and computing*, pp. 24–35, June 2002.

22. Heinzelman, W. R., Chandrakasan, A., & Baladrishnan, H. "Energy-efficient routing protocols for microsensor networks". Proceedings of the 33rd *Hawaii international conference on system sciences*, Vol. 8, pp. 1–10, January 2000.
23. Sirisala NageswaraRao, C. Shoba Bindu. "Weightage based trusted QoS protocol in Mobile Adhoc Networks", *IEEE Global Conference on Wireless Computing and Networking (GCWCN)*, pp.283-287, 2014.
24. 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 Vol. 10, Number 12 pp. 32175-32194, 2015.
25. Suneel Kumar Duvvuri and Dr. S. Rama Krishna, " Performance Evaluation of TCP alternatives in MANET using Reactive Routing Protocol" , *International Journal of Modern Computer Science* , Vol 4, Issue 4, , pp. 35-39, ISSN: 2320-7868, August 2016.
26. Suneel Kumar Duvvuri and Dr. S. Rama Krishna, " Comparative study on Fault tolerant routing Protocols in Mobile Ad hoc Networks" , *International Journal of Emerging Trends & Technology in Computer Science*, Vol. 5, Issue 4, pp. 121-126 , ISSN 2278-6856, July - August 2016.
27. Srinivasulu sirisala and Dr. S. Rama Krishna " Survey: Enhanced Trust Management for Improving QoS in Manets", *Advances in Intelligent Systems and Computing*,Vol.815, pp 255-263, ISSN 2194-5357,2018.
28. Allard G., Minet P., Nguyen DQ., Shrestha N. (2006) "Evaluation of the Energy Consumption in MANET", *Ad-Hoc, Mobile, and Wireless Networks. ADHOC-NOW 2006*. Vol. 4104,pp 170-183, ISBN :978-3-540-37248-6 Springer, Berlin, Heidelberg, 2006.
29. Espes, David & Mammeri, Zoubir."Delay and Bandwidth Constrained Routing with Throughput Optimization in TDMA-Based MANETs", *NIMS* 2009.5384774,pp.1-5.
30. Lajos Hanzo II. and Rahim Tafazolli., "Admission Control Schemes for 802.11-Based Multi-Hop Mobile Ad hoc Networks: A Survey", *IEEE communications surveys & tutorials*, Vol. 11, NO. 4,2009.

AUTHORS PROFILE

Srinivasulu Sirisala, received his M.Tech in Computer Science and Engineering from JNTUA,Anantapuramu in 2012 and pursuing Ph..D. in Computer Science from S V University, Tirupatiin 2015.His areas of interest are Computer Nerworks.

Dr. S Rama Krishna is a Professor, Department of Computer Science and Applications in Sri Venkateswara University. He has guided about 20 Ph.D students and 20 M.Phil Students so far. His areas of interests are Fluid Dynamics, Computer Networks and Data Mining.