ISSN 2278-3091
Volume 9, No.1, January – February 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse39912020.pdf
https://doi.org/10.30534/ijatcse/2020/39912020

An Improved Trusted On-Demand Multicast Routing with QoS for Wireless Networks

Jagadeesh Gopal[1], Vellingiri J[2], Gitanjali J[3],Arivuselvan K[4], Sudhakar S[5]
[1234]School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu-632 014, India.
vellingirijayagopal@gmail.com
[5]Dept. of CSE, Sree Sakthi Engineering College, Coimbatore, Tamil Nadu– 641 104, India.
sudhasengan@gmail.com[5]

ABSTRACT

Usage of Wireless networks increasing rapidly due to an increase in the usage of IoT devices. For the better utilization of wireless networks, Ad Hoc networks prepared than Infrastructure based networks. Quality of Service is the primary concern in Ad Hoc networks. QoS in a Multicast routing strategy is needed to adapt to provide better services in Ad Hoc networks. For network group communication On-Demand Multicast Routing Protocol (ODMRP) has a low control overhead. Many schemes have worked on the development of ODMRP, but very few have provided an aware quality mechanism. We propose a new method for reducing the control overhead and also a technique for supporting QoS routing in ODMRP by making an acceptable estimation of available bandwidth.

Key words: Ad hoc Networks, Infrastructure Networks, Multicast Routing Protocols, Control Overhead, Bandwidth.

1. INTRODUCTION

The disadvantages of wireless networks are, the need to set up an entire base station, centralized routing, and their static nature, i.e., they require the establishment of a connection for communication purposes. Ad hoc networks are a category of infrastructure-less wireless networks. They don't follow any centralized (cellular) structure, thereby exhibiting distributed routing. These networks enable the nodes to move around freely, resulting in frequent changes in the topology. This dynamic nature of Ad hoc networks makes them suitable for critical applications (military, collaborative, and distributed computing, emergency operations) where we can carry out our tasks without the need to set up an entire base station (centralized). Due to frequent topology changes, they fall under mesh topology. Mesh topology is nothing but the existence of multiple paths between the source and the destination. This method, in turn, results in multi-hop links between the sender and the receiver [1]. This, however, is an excellent advantage over the wired networks, but these do lead to certain critical disadvantages. These disadvantageous natures of Adhoc networks result in security issues, loss of packets due to path breakage, and QoS metrics aren't satisfied.

The advantage is that Ad hoc networks are more comfortable to deploy and are highly cost-effective, whereas wired networks are comparatively costlier. It is necessary to satisfy the quality parameters and make them highly efficient. We are concerned about the quality factors and are here to address a few issues. Since Ad hoc networks are truly infrastructure-less, they need control packets to broadcasted to know whether a link exists or not. Due to their change in topology, they will face link breaks quite often. This increases the control overhead in a network. The On-Demand-Multicast-Routing-Protocol reduces the control overhead as in [2]. This protocol performs multicasting. Multicasting is the sending of packets to many nodes. This protocol floods the network with Query packets. The ODMRP includes sending a join request to all the nodes by the source. The nodes will save the details and rebroadcast the join message until it reaches the receiver(s). The receiver, in turn, sends a join reply packet to the neighboring nodes. If there is an ID match, the intermediate node becomes a forwarding group member and rebroadcasts until the reply packet reaches the source. Taking the hop count as a parameter, the control overhead can be reduced even further. Due to the nature of these networks, we take into consideration the packet loss issue. This issue is minimized by calculating the available bandwidth in a network, and depending on this as well as the packet's data size, the packets will be transmitted.

Using the above two mechanisms (control overhead and bandwidth estimation), we improve efficiency by identifying the robust route, leading to the effectiveness of the packets being sent. We perform a comparison between the existing basic ODMRP and the proposed technique.

2. RELATED WORKS

Naveen Reddy et al. proposed a back-off mechanism is devised, which grants node access to the channel based on the rank of its highest priority packets. The source node is prioritizing the packets, and depending on its priority, packets [3] sent. The packets with minimum priority are submitted only at last. The disadvantage is that the receiver might want to receive packets in a different order. Xin Ming Zhang et al. found the EstD-Estimated Distance using two mechanisms: ETD-Estimated Topological Distance & EGD-Estimated Geographical Distance in the route discovery phase of the ODMRP protocol [4], EGD calculates the quality of a link and avoids weak links, and ETD is taken into consideration while EGD is inaccurate thereby reducing the control overhead in the network and improving accuracy. Alsheakhali et al. calculated the hop count is and compared it in [5] with the values in the routing table, and the route with minimum hop count is taken as the shortest route, and then packets are transmitted efficiently in the identified route resulting in low control overhead.YuanhuiNing et al. identified when a primary path is being over-utilized and is at its breakage point, the candidate paths are being maintained in a table, and the central path is given up well ahead of its breakage, and a new alternate path is made as primary path taking the quality of the alternative path considered. Only the paths which satisfy the QoS constraints [6] will be made as to the primary path, thereby creating a new TALORP protocol. Zhenhui Yuan et al. used two techniques the probing and the cross-layer for calculating the additional traffic [7] in a network. A combination of TCP & DCF models is taken, thereby reducing packet loss, and the available bandwidth is calculated efficiently. First, the size of the data to be sent is calculated, and then a path of required bandwidth for that particular data size of a packet is identified, and then that packet is transmitted. Barzuza et al. calculated the overutilization of Bandwidth in a network, and the real-time monitoring of the delay [8] is performed. Based on delay detection, bandwidth adaption is done to allocate bandwidth dynamically as and when needed. Yinzhe et al. proposed two approaches:

Testing the packets periodically ensuring that packets are not lost and maintaining the history of bandwidth in a table enabling the choosing of the candidate paths, which is, in turn, taken into consideration [9], when there is a breakage in the primary path resulting in a better estimation approach. Mingzhe et al. proposed a search algorithm used to detect the available bandwidth by statistically detecting the available fraction of the adequate capacity to mitigate estimation delay [10] and the impact of random wireless channel errors.

3. PROPOSED QOS MODEL

The disadvantage of existing ODMRP is that the packets are sent without knowing the capacity of the network (ABEST), which might lead to the loss of critical information. Prioritizing of packets will be of no use in case the chosen link doesn't meet the user's requirements, namely the size of data packets and traffic. The papers [10] [11] [12] take ABEST into consideration, but it also has certain disadvantages like for knowing the traffic in a network, the network is flooded with the probing packets thereby resulting increasing the cost incurred in a network. It is difficult to know whether a network is already being used by another set of nodes. So, to understand the AB in a network, we will have to forego the above control conditions.

The mechanism which we propose reduces the control overhead, and an estimation of the AB is also done, thereby increasing the efficiency of the network. The ODMRP protocol, which we use, has 2 phases: Route discovery and Route maintenance. In the Route discovery phase, the source will send JOIN_REQ packets to all the neighboring nodes. The adjacent nodes save the *lastHop_ID* and re-broadcasts to their neighbors. If the receiver's ID and the destination ID in the control packet sent matches, then broadcasting of the JOIN_REQ packet is suspended, and the receiving node creates a ROUTING_TABLE, which includes its *ID*, *nextHopAddr, sourceID, queueLength, hopCounter* and forwards to the neighboring nodes as JOIN_REP message. The nodes which receive the JOIN_REP message will crosscheck if it's ID and the *nextHopAddr* parameter matches or not. If it's a match, then the node will update the packet with its *queueLength, nodeID, nextHopAddr,* and increments the *hopCounter* by 1 and then forward it after setting the FG_FLAG to true. All the intermediate nodes which receive the JOIN_REP message will perform the same actions until it reaches the source node. Along with the hob count, the network congestion also takes into consideration to estimate the best available path.

After receiving the JOIN_REP message through multiple paths, the source finds the route with minimum *hopCount.* The Available Bandwidth Estimation (ABEST) in that particular route is done following which the transmission of data packets is performed. The algorithm for calculating the Available Bandwidth [13] is as given in Algorithm1.For calculating traffic in a link; we send back-to-back probe packets which estimate the load in a loop. The probeGap can be found out depending on the cross-traffic. Packet probing is done to perform capacity measurements. Taking the average of the return time of probes will be helpful in analyzing the Available Bandwidth of the particular link. We get accurate Available Bandwidth by sending of the probe packets with re-adjusted probeGaps. The returning speed and accuracy of the Gap search technique are modified by means of alpha, beta parameters.

$$availBandwidth = \frac{(probeSize * (trainLength - 1))}{sum(probe\,\mathrm{Re}\,turntime[])}$$

Where*probesize* is the size of the probing packet that we send, and *train length* is the length of the sequences of the packets.

The bandwidth available is hence calculated, and this is effective because there will be no data packet loss, which would incur more cost. As we now know, the available bandwidth of the link, the transmission of data packets is done without any bottleneck issue.

The problem we may face next is the path or link breakage. We address this issue by maintaining active neighbors of the primary path. The member node sends NEIGH_REQ to its neighbors. The neighbors will reply with their *nodeID* and *nodeTyp,* which will, in turn, be updated in the NEIGH_ROUTE_TABLE. The member sends its *group_ID* to the neighbor nodes. The FG_node gets to know if its neighbors are active or not depending on NEIGHBOR_CHECKOUT_TIME. If they are alive, they reply with their *group_ID*.

In case there is a path breakage detected in the primary path, then we perform checking of whether there exist active neighbors for source, FGnode, and receivers or not. If they are, then we broadcast JOIN_REQ packets asking the nodes to become the members of the primary path following which data transmission is carried out. The algorithm for detecting and recovering from link breakage [14] is as given in Algorithm 2.

3.1. Algorithm of Improved ABEST with ODMRP

```
Join Msg
A source sends JOIN_REQ message to neighbors
Nodes create ROUTING_INFO_TABLE and save last hop_ID
Nodes broadcast JOIN_REQ till it reaches receivers

Case Originator:
        On receiving JOIN_REP message
        Find minimum hopCount;
        Find maximum hopCount;
        Perform
                ProbeGap=probe Size/(2*Capacity);
                Beta = probeGap/4;
                Alpha = 0.01;
        Perform
        Perform
                SendprobePackets;
                Wait for probeGap;
        tilltrainLength is sent;
        readprobeReturntime[];
            err=(avg(probeReturntime[])-probeGap)/
            probeGap;
        probeGap = probeGap + beta;
        till |err|<alpha;
        availBandwidth=(probeSize*(trainLength-1))
        sum(probeReturntime[]);
        Send Data
        End
        End Case
        End

Case group_member:
        On receiving JOIN_REQ message
        Update the routing table and
                inform all other nodes in the network.

Case other nodes:
        On receiving JOIN-REP message
        Cross-check if (its ID==nextHopAddr)
        ThenUpdate Queuelength
        ++hopcounter
        Include ID, nextAddr,traffic_rateand forward
        Set FG_FLAG to TRUE

Case Receiver:
        On receiving JOIN_REQ message
        Perform
        Create ROUTING_TABLE
        Include its ID, nextHopAddr,node traffic,sourceID,
        queue length, Hopcounter
        Forward to neighbors as JOIN_REP
```

3.2. Algorithm of multicast routing with Path Breakage Recovery

```
LOCAL RECOVERY:
Each node:
        Send NEIGH_REQ to neighbor nodes and all
                reachable nodes of the network
        Neighbor nodes reply ID, node type and traffic
                information to the source
        Member node change ID, Type and update the traffic
                information along with its group address
        Store values in NEIGH_ROUTE_TABLE
        Send group_ID to neighbor nodes
        Send traffic information to neighbor nodes
        FG node sends HELLO PACKET to neighbor nodes
        Every NEIGHBOR_CHECKOUT_TIME seconds
        If(neighbor node available)
        Then
                replygroup_ID to FG node
        End

Case Traffic _Congestion nodes:
        If (Number of packets is > 1)  or
         (Number of source neighbors>1)    or
        (Number of packets>1)&&(Number of sender
        packet>1) then Do packets+1
        Else
                Send traffic_REQ to other nodes.

Case FG node:
        If (number of FG neighbors>1) or
                (Number of source neighbors>1)
        Or (number of FG neighbors>1 &&
                Number of receiver neighbors>1)
        Then    do nothing
        Else
                Send JOIN_REQ to neighbor nodes
End Case

Case group_member:
        If (number of FG neighbors>1)
                Or (number of source neighbors>1)
        Then
                Do nothing
        Else
                Send JOIN_REQ to neighbors
End Case
End Switch
```

The overall system design of the proposed mechanism is given in Fig.1. The system design clearly portrays the overall mechanisms such as control overhead, which includes minimum hop count calculation and then discovering the route. Bandwidth is estimated for the route, and then the data packets are sent accordingly. The recovery mechanism is also mentioned in the case of link breakage.

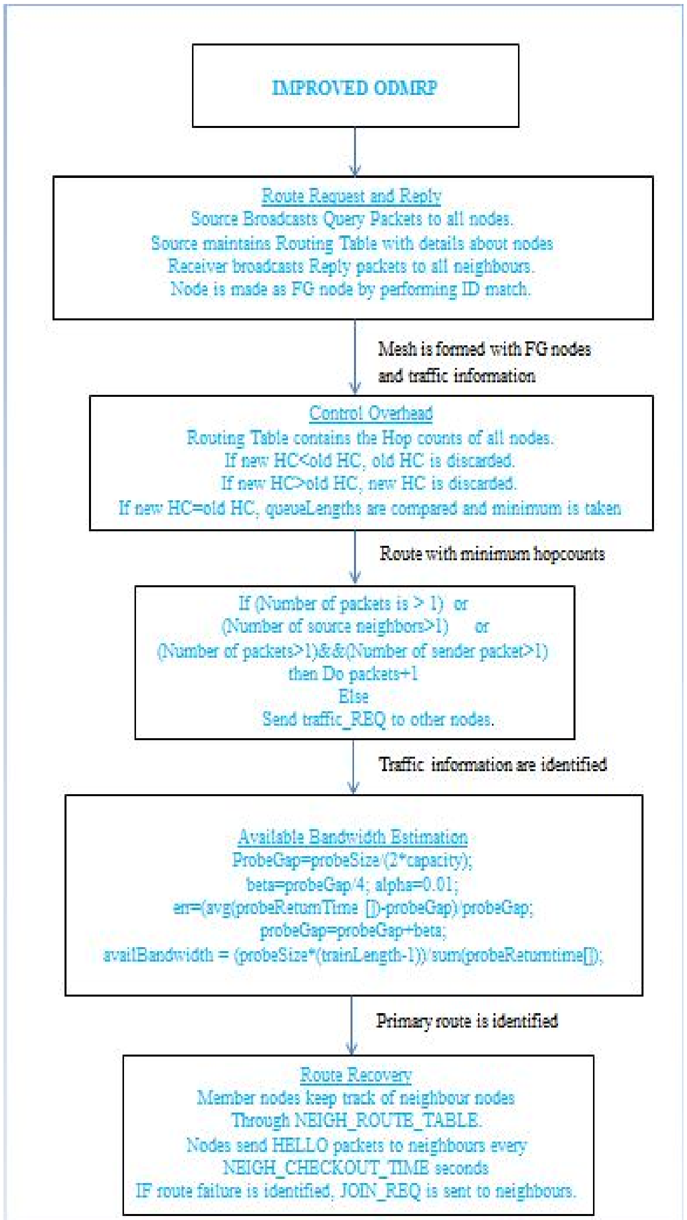

Figure 1: QoS Design for Multicast Routing

4. PERFORMANCE EVALUATION

We performed the simulation in C language, keeping some parameters constant, such as network traffic and the number of nodes in the network. When a source node wants to send data to some particular nodes in the mesh, it will send the JOIN_REQ packets through all identified paths and finds out the suitable way to the destination, and the data is sent. We performed our evaluation for various sets of nodes, and the respective values are made as graphs Fig 2 and Fig 3.

4.1. Packet Delivery Ratio

It is the ratio of the number of data packets delivered to the receivers versus the number of data packets that are to be received. It is used to find out the rate of loss of data packets. The higher the ratio is, the better is the delivery ratio.

In Fig 2, we have performed a comparison between the delivery ratio of the packets and the network size. The packet delivery ratio lets us know how reliable the network is for the delivery of the packet. From the graph, we can analyze that the delivery ratio of the enhanced system is comparatively higher than the basic ODMRP system. And we also find that the delivery ratio increases with an increase in the number of nodes in the group.

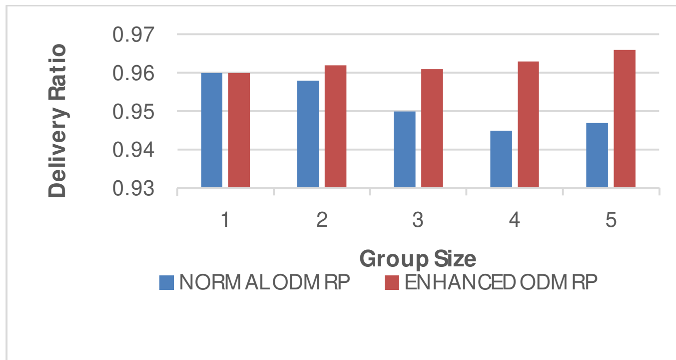

Figure 2: Packet Delivery Ratio vs. Network Size

4.2. Control Overhead

It is the ratio of the number of control bytes transmitted per delivered data byte. This ratio is evaluated to find out how many control packets are required to provide the data packets.

Fig 3 shows the overhead control metric of the enhanced system and the basic ODMRP. This ratio is evaluated to find out how many control packets are required to deliver the data packets. We can find that the overhead is reduced to minimal as compared with the underlying system. It is to be noted that the overhead is comparatively reduced as the group size increases.

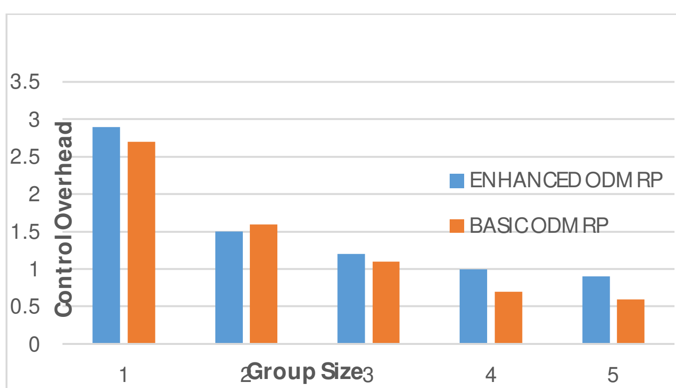

Figure 3: Control Overhead vs. Network Size

5. CONCLUSION

The proposed work supports QoS routing in ODMRP by appraising the available bandwidth of the paths and the congestion in the network nodes. The packet loss is reduced significantly by estimating the hop count, bandwidth, and congestion. In the proposed work, we have chosen the best route with minimum hob count and less congestion path. Reliable transmission of data packets supported by efficient recovery mechanism. According to user requirements, the Primary network path is identified among a group of feasible paths.

REFERENCES

1. Narsimha G, Reddy A.V, Kumar B.S, "QOS Multicast Routing Based on Bandwidth and Resource Availability in Mobile Adhoc Networks," Networking, 2008. ICN 2008. Seventh International Conference on, vol., no., pp.24-29, 13-18 April 2008 https://doi.org/10.1109/ICN.2008.118
2. Sung-Ju Lee; Gerla M, Ching-Chuan Chiang, "On-demand multicast routing protocol," Wireless Communications and Networking Conference, 1999. WCNC. 1999 IEEE, vol, no, pp.1298-1302 vol.3, 1999
3. RamMurthy G, Naveen Reddy G, Ravi Shankar Varma A. "Modified Distributed Laxity Based Priority Scheduling Scheme" Wireless Personal Communications Volume 58, Issue: 3 pp 627-636(2011)Springer Netherlands 2011-06-01 https://doi.org/10.1007/s11277-010-0126-1
4. Xin Ming Zhang, En Bo Wang, Jing Jing Xia, Dan Keun Sung, "An Estimated Distance-Based Routing Protocol for Mobile Ad hoc Networks," *Vehicular Technology, IEEE Transactions on*, vol.60, no.7, pp.3473-3484, Sept. 2011
5. Alsheakhali M, Awad F, "Traffic-Aware and Low-Overhead Routing Protocol for MANETs," *Wireless Days, 2008. WD '08. 1st IFIP*, vol., no., pp.1-5, 24-27 Nov. 2008 https://doi.org/10.1109/WD.2008.4812867
6. Yuanhui Ning, Guangxi Zhu, Gang Su, Li Tan, "A low overhead multipath routing based on feedback information for mobile Ad hoc networks," Intelligent Signal Processing and Communication Systems, 2007. ISPACS 2007. International Symposium on, vol., no., pp.333-336, Nov. 28 2007-Dec. 1 2007.
7. Sudhakar Sengan, Chenthur Pandian S, 2013,'Trustworthy Position-Based Routing to Mitigate against the Malicious Attacks to Signify Secured Data Packet using Geographic Routing Protocol in MANET', WSEAS Transactions on Communications, vol.12, no.11, pp. 584-2013.
8. Zhenhui Yuan, Venkataraman, H, Muntean, G.-M, "MBE: Model-Based Available Bandwidth Estimation for IEEE 802.11 Data Communications," Vehicular Technology, IEEE Transactions on, vol.61, no.5, pp.2158-2171, Jun 2012 https://doi.org/10.1109/TVT.2012.2190760
9. Barzuza T, Ben Zedeff S, Modai O, Vainbrand L, Wiener Y, Yellin, E, "Trend: A dynamic bandwidth estimation and adaptation algorithm for real-time video calling," Packet Video Workshop (PV), 2010 18th International, vol., no., pp.126-133, 13-14 Dec. 2010 https://doi.org/10.1109/PV.2010.5706829
10. Yinzhe Yu, Irene Cheng, Basu A, "Optimal adaptive bandwidth monitoring for QoS based retrieval," Multimedia, IEEE Transactions on, vol.5, no.3, pp. 466-472, Sept. 2003 DOI: 10.1109/TMM.2003.814725
11. Mingzhe Li, Claypool M, Kinicki, R, "WBest: A bandwidth estimation tool for IEEE 802.11 wireless networks," Local Computer Networks, 2008. LCN 2008. 33rd IEEE Conference on, vol., no., pp.374-381, 14-17 Oct. 2008
12. Sudhakar Sengan & Chenthur Pandian S, 2016, 'Hybrid Cluster-based Geographical Routing Protocol to Mitigate Malicious Nodes in Mobile Ad Hoc Network, International Journal of Ad Hoc and Ubiquitous Computing, ISSN online: 1743-8233; ISSN print: 1743-8225,Vol.21,No.4,pp:224-236. DOI: 10.1504/ijahuc.2016.076358
13. A.U. Priyadarshni, S.Sudhakar, 2015,"Cluster-Based Certificate Revocation by Cluster Head in Mobile Ad-Hoc Network," International Journal of Applied Engineering Research, ISSN 0973-4562 Vol. 10 No.20, pp: 16014-16018
14. Esmaeili T, Lari M, AkbariJahani E, Mohamadi S, "Proposing an approach for routing overhead reduction in mobile ad hoc networks," Electronic Computer Technology (ICECT), 2010 International Conference on , pp.161-164, 7-10 May 2010 https://doi.org/10.1109/ICECTECH.2010.5479965
15. Nianjun Zhou, Abouzeid A.A, "Information-Theoretic Analysis of Proactive Routing Overhead in Mobile Ad Hoc Networks," Information Theory, IEEE Transactions on , vol.55, no.10, pp.4608-4625, Oct. 2009
16. Mesut Ali Ergin, Marco Gruteser, Lin Luo, Dipankar Raychaudhuri, Hang Liu, "Available bandwidth estimation and admission control for QoS routing in wireless mesh network"s, Computer Communications, Volume 31, Issue 7, 9 May 2008, Pages 1301-1317, ISSN 0140-3664
17. Naderan-Tahan, M.; Darehshoorzadeh, A.; Dehghan, M.; "ODMRP-LR: ODMRP with Link Failure Detection and Local Recovery Mechanism," Computer and Information Science, 2009. ICIS 2009. Eighth IEEE/ACIS International Conference on , vol., no., pp.818-823, 1-3 June 2009. https://doi.org/10.1109/ICIS.2009.111
18. Sudhakar Sengan & Chenthur Pandian S, 2012, 'An Efficient Agent-Based Intrusion Detection System for Detecting Malicious Nodes in MANET Routing,' International Review on Computers and Software (I.RE.CO.S.), Vol. 7, No. 6, pp. 3037-304.