**JOURNAL OF ALGEBRAIC STATISTICS**
Volume 13, No. 2, 2022, p. 595 - 607
https://publishoa.com
ISSN: 1309-3452

# Optimal Route Selection for Mobile Ad-hoc Networks based on Cluster Head Selection and Energy Efficient Multicast Routing Protocol

**Dr. N. Sivapriya**

*Assistant Professor*
*Cauvery College for Women,*
*Trichy, Tamilnadu - 620018*
*nmsivapriya@gmail.com*

**Dr. R. Mohandas**

*Associate Professor*
*Balaji Institute of Technology & Science,*
*Narsampet, Warangal, Telangana - 506331*
*mohandasbe@gmail.com*

**ABSTRACT**

A mobile ad-hoc network is a self-organizing, fundamental structure-less, autonomous wireless mobile node that exists in the absence of any specified base station or federal organisation. MANET necessitates no unique infrastructure as the network is completely dynamic. Multicasting is the exigent issue in communication networks. In MANET, multicast is one of the competent approaches. In multicasting, data packets from one node are transmitted to a set of receiver nodes at a time, simultaneously. Multicasting reduces transmission costs. Cluster head selection is one of the challenges in MANET. Optimal Route Selection (ORS) is a proposed research paper that provides cluster head selection and alternate cluster head selection to avoid cluster head failure, as well as generation of the optimal path between the cluster head and member node based on reliability pair factor and node energy, and establishment of the path based on maximum energy and number of hops between the nodes. (minimum number of hops).

**Keywords:** Wireless Sensor Nodes, Quality of Service, Multicast Routing, Reliability Pair Factor, Cluster Head (CH*).*

## 1. Introduction

A mobile ad hoc network is a wireless network that may be formed on the fly to transport data from one point to another. It's a self-forming, peer-to-peer, and self-healing network. Mobile ad hoc networks (MANETs) are subject to security issues due to their intrinsic qualities, such as the open wireless medium and variable topology. The ability to afford trustworthy and secure communications in hostile contexts like war zones is difficult [1]. The fundamental goal of the multicast routing method is to find the most stable multicast route while taking into account of the host's mobility [2]. Unreliability, accidents, and energy consumption in mobile nodes are only a few of the security challenges that plague MANET data transfer. The secure transmission of data between source and destination is carried out using the trust-based protocol. Onion routing protects data during both forward and backward transport by encrypting and decrypting it with a key. End-to-end delays are reduced, throughput is increased, and energy consumption is reduced using the trust mechanism [3]. A single destination address identifies data packet transmission to a group of zero or more nodes who receive data packet when Multicast is used. In case of applications that require sending the same message to many recipients at the same time, (MQMR) Multi-path Qos Multicast Routing reduces the transmission cost. It's especially helpful in WiFi environments having limited storage mobile devices . As a result, in order to provide group communication, the nearby nodes must be linked securely. Multicast routing protocols such as MQMR[4] are examples of multicast routing technologies. Multicast routing protocols for MANET, such as QMRPCAH [5,6], SMR [6,7], and an energy-efficient ZBR [8] provide good performance in mobile ad-hoc networks. Mobile ad-hoc networks (MANETs) are used in a range of situations where quick exploitation and energetic reconfiguration are required.

Military battlegrounds, emergency search and rescue operations, liberating maneuvers, and online education systems are among them. It's also employed during natural disasters, when people can use their mobile devices to relay critical information. Several (QoS)Quality of Service multicast routing techniques for wireless mobile ad hoc networks have been developed in the literature. As a result of QoS, networks are capable of providing better service for certain types of network traffic than others. A path from a source to a set of destinations must have lower value for end-to-end delay and energy utilized, and higher value forthroughput[8–13]. When designing such networks, it takes into account factors like the remaining battery life and energy usage rate [14–17]. Various techniques for reducing energy usage in wireless ad-hoc networks have recently been developed [18–21]. The most prevalent characteristics of MANET are packet delay, channel bandwidth, loss, battery life time, jitter ,energy consumption and these have a significant impact on QoS. The following is the structure of the paper: The Literature Review in Section II focuses on multicast routing and sensor node clustering. The proposed scheme of Reliability Pair Factor based on multiple models (FRP) and the cluster head selection method based on energy, hop counting, and Reliability Pair Factor (CHSA), as well as the optimal path selection based on hop counting are explained in Section III (OPSH). The conclusion is established in Section IV.

**JOURNAL OF ALGEBRAIC STATISTICS**
Volume 13, No. 2, 2022, p. 595 - 607
https://publishoa.com
ISSN: 1309-3452

## 2. Literature Review

### 2.1 IN MOBILE ADHOC NETWORKS FOR TIME SENSITIVE APPLICATIONS, OPTIMAL PATH SELECTION:

In this study [22], we propose trust-based authentication for dynamically secured routing. This network-wide trust-based routing system uses a threshold value to identify rogue nodes. The trust node is the probability that a single node will provide anonymous routing in a hostile environment. The performance of nodes in the data, reputation, and commendation are all tied to node. An adversarial environment's trust nodes respond by minimising data packet transmission latency. Secure data is transmitted between the source and the destination via trust-based protocols. This protocol improves MANET performance in both RREQ and RREP scenarios, with the following goals: A public factor cannot access a specific node in a group, hence private keys are used. Secure networks can withstand an assault and destroy the attack's source if they can detect and eliminate it. The trusted process decreases the time it takes from start to finish. In order to encourage packet forwarding, each node keeps a trust counter. Lower trust values indicate a hostile intermediary node, while higher trust values indicate the opposite. The authorised node in this suggested method has a high throughput, and the packet delivery ratio can be significantly increased while decreasing the average end-to-end time by increasing the trust value.

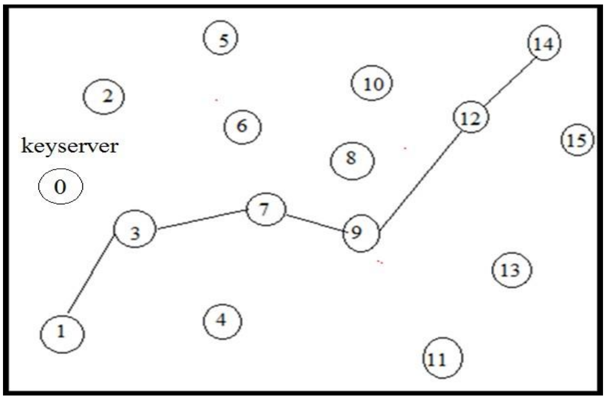


*Fig 1: Trust based Routing of MANET*

### 2.2 IN MOBILE AD-HOC NETWORKS, ENHANCED -ANT-AODV FOR OPTIMAL ROUTE SELECTION

To enhance MANET QoS, this study [23] integrates route selection and ad-hoc on-demand distance vector protocol with Ant Colony Optimization. This notion is based on the optimum method to communicate data utilising the path's pheromone value. The pheromone value is determined by the packet's end-to-end delivery, congestion, the number of nodes, and the node's leftover energy. The highest pheromone value of the path is chosen for data transmission. Packet Delivery Ratio, Throughput, and End-to-End Delay are all improved as a result of the ANT/AODV protocol's mechanism.

### 2.3 AN ENERGY EFFICIENT ROUTE SELECTION ALGORITHM BASED ON LOA FOR MOBILE AD HOC NETWORKS:

The purpose of this study [24] is to show how to use trust with the Lion Optimization Algorithm to create energy-efficient MANET routing. LOA is a bio-inspired algorithm that helps find the most effective data transmission method. The route establishment phase, trust metrics computations, and optimal route selection are the three phases. The AODV protocol is used to establish the route, which finds numerous paths between the destination and source. The sensor node's energy is concentrated and the sensor node's energy level is shown in Table 1.

| **Energy Table** | |
|---|---|
| **Energy Value** | **Node Type** |
| 0 | Nodes with nil energy |
| 0.5 | Half Energy |

| | |
|---|---|
| 0.75 | Three-fourth Energy |
| 1 | Full Energy |

**Table 1: Energy value and Node type**

Trust value is calculated by

$$\mathbf{Tc} = \sum_{i=1}^{n} \frac{E_i + PDR + QL_i}{3} \qquad - 1$$

Where E stands for Energy, PDR is for Packet Delivery Ratio, and QL stands for Message Queue Length.
The trust value is determined based on Energy, packet delivery rate, and queue duration in this study, and it is used to achieve reliability.
average delay, Packet delivery ratio, energy usage, and network lifetime are used to evaluate the work's performance.

**Choosing the Best Route**

This study selects optimal routes based on node fitness. As a result, the node became more dependable and efficient while also consuming less energy.

$$\text{FV} = \sum_{i=1}^{n} \frac{TC_i}{N} \qquad -2$$

**2.4 MANET's shortest and most energy-efficient routing protocol is:**

SEERP [25] proposes a protocol for determining the best route between a destination and a source based on residual energy and hop count. There is a routing protocol in place that uses the least amount of energy for nodes and the shortest possible distance between communication nodes. Table 2 demonstrates the power-saving approaches used in ad hoc networks, which are the most common type of power-saving protocol[26].

| **ProtocolLayer** | **PowerSavingTechniques** |
|---|---|
| ApplicationLayer | Espousean adaptive mobile quality of Service(QoS)framework. |
| TransportLayer | Avoidrepeatedretransmissions.<br>Handlepacketlossinalocalizedmanner. |
| NetworkLayer | Considerrouterelayingload.<br>Optimizesizeofcontrolheaders. |
| Data-LinkLayer | Avoid unnecessary retransmission.Turn radiooff(sleep)when not Transmittingorreceiving. |

**Table 2: Power saving Techniques**

| | | | | | |
|---|---|---|---|---|---|
| RREQID | Destination Address | Destination SequenceNumber | Source Address | Source SequenceNumber | Hop Count |

**Fig 2: RREQ Packet Structure**

**JOURNAL OF ALGEBRAIC STATISTICS**
Volume 13, No. 2, 2022, p. 595 - 607
https://publishoa.com
ISSN: 1309-3452

| Author | Work | Methodology | Advantages | Limitations |
|---|---|---|---|---|
| K.Sujatha et.al. | Choosing the best route in a MANET for time-sensitive applications | Trust Model Authenticated Anonymous Secure Routing | Decreases End-to-End Delay and Increases the trust value | small area and less number of nodes and Security is not achieved |
| Dipika,Swagata and Abhishek et.al. | Enhanced-Ant-AODV for Optimal route Selection in MANET | Pheromone value calculated based on ANT/AODV Protocol | Decreases End-to-End Delay and Increases the Throughput | Packet delivery ratio , Energy Consumption, Jitter and Security are not achieved |
| Dr.M.Devapriya and P.Ramesh | Based on LOA, an Optimal Energy Efficient Route Selection Algorithm for Mobile Ad-hoc Networks | Based on the trust value, the sensor node elected and based on the fitness value optimal path is calculated between source and destination | Better achievement of Packet delivery rate and Energy Consumption | Security is not achieved |
| Edwin Lawrence and LathaRamavel | Time-sensitive applications in MANET: Optimal Path Selection | It includes an algorithm for picking the lowest-energy node as well as a routing route with the fewest number of hops. | Minimum Energy Consumption and minimized hop counting | Security is not achieved |

*Table 3: Methodologies and Limitations of Exiting Research Methods*

## 3. Proposed Methodology

### 3.1 Cluster Head Selection Algorithm (CHSA)

In this algorithm, The cluster head is produced in this approach by calculating the Reliability Pair Factor and the node's maximal energy. When a node has the most energy, it is designated as the cluster head, with the following level of nodes designated as the alternate cluster head. In two circumstances, the alternate cluster heads are employed. When the energy of the cluster head is low, the alternate cluster head becomes the cluster head automatically. To handle cluster head failures, a second alternate cluster head is used.

**Cluster Head Selection Algorithm**

1. Compute the CH among the nodes based on the $N_E$ , $N_D$ and $F_{RP}$ between the base station and selected high energy node CH($N_E$.$N_D$,$F_{RP}$)
2. Send the REQ (Request Message) to all other nodes. When the nodes are on the same route, the REQ message is accepted and the cluster head is notified
3. FRP="max" (Eprem,Eqrem)/"d(p,q,t)" Calculate FRP="max" (Eprem,Eqrem)/"d(p,q,t)" where d is the distance between nodes p and q at timestampt.
4. 4. And, based on the computation CH>SCH>MN, cluster head determines the Substitute Cluster Head SCH.
5. Cluster head updates the cluster table in the base station
6. If the cluster head becomes dry, the cluster members' Energy, Distance, and Reliability Pair Factor are maintained by the replacement cluster head.Find the optimal path based on maximum available energy of the node and minimum hop count between base station to cluster head and cluster head to member nodes

### 3.2 The Algorithm for Optimal Path Selection

It is necessary to discover the shortest route between two points in order to get at a final destination. This algorithm, suggests the methodology based on maximum energy of the node and minimum hops between the nodes.

**JOURNAL OF ALGEBRAIC STATISTICS**
Volume 13, No. 2, 2022, p. 595 - 607
https://publishoa.com
ISSN: 1309-3452

**Optimal Path Selection Algorithm**

1. *Route request packet RREQ is generated by the source node.*
2. *The RREQ ID, destination address, destination, sequence number, source address, source sequence number, hop count, and NmaxE are all included in the RREQ.*
3. *If a node receiving the packet has a higher energy level than the current NmaxE, it updates NmaxE; otherwise, NmaxE stays unchanged.*
4. *Keep checking until the RREQ arrives at its destination.*
5. *The most energy efficient route is chosen from the numerous RREQ collected from several routes.*
6. *If (NmaxE=high &&hopcount=Low), choose a communication route.*
7. *A RREP (route reply) is created and returned.*
8. *Data is sent via the newly specified route.*

It is not necessary to determine the path using a distinct algorithm if the above algorithms are used. We may be able to locate multiple paths with the same high energy using this algorithm. If there are any crashes in the path, the alternate way must be chosen. As a result, computing time can be reduced. Figure 3 depicts an example of determining the shortest path with the highest energy node.

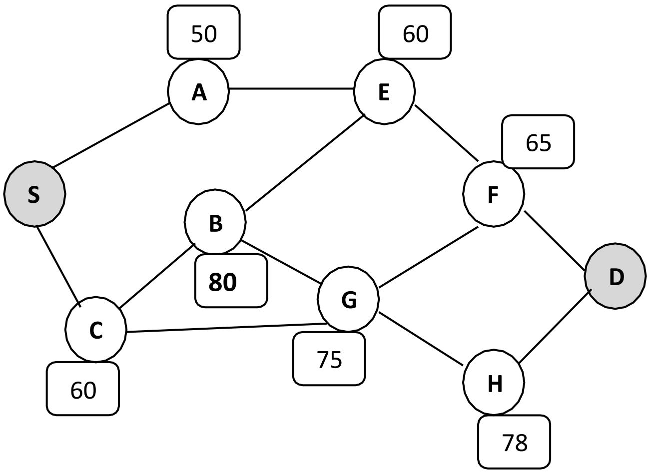


***Fig 3: Communication path between Source and Destination***

**4. Experimental Setup**

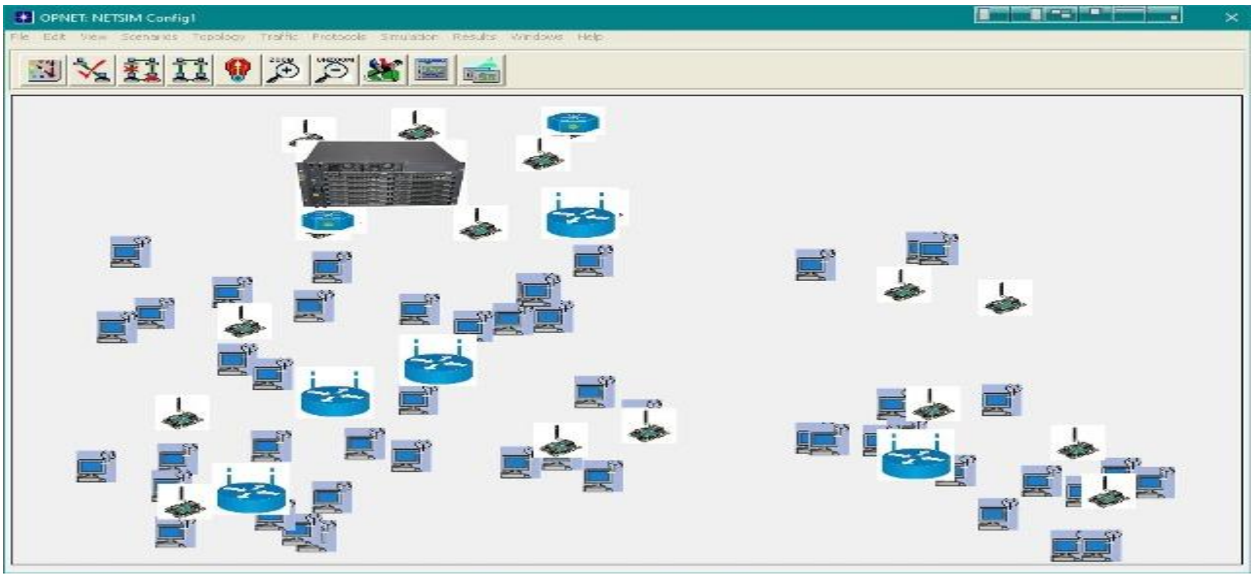


**Fig 4: Network Setup**

**JOURNAL OF ALGEBRAIC STATISTICS**
Volume 13, No. 2, 2022, p. 595 - 607
https://publishoa.com
ISSN: 1309-3452

OPNET is the latest network simulator from Riverbed Technology and it has the most up to date network simulation support available today. OPNET's graphical interface and scripting capabilities enable it to construct any legacy network architecture or protocol. It offers the ability to acquire real-world network environments by specifying latitude and longitude information. The usual network communication techniques network node types protocols, can all be defined and overridden with OPNET. OPNET has the ability to process C++ code to create network strategies, which is a unique feature. A customized user interface (UI) is built in Visual Studio to communicate with the network simulator and get analytical parameters from it. In Figure 5 you can see the user interface.

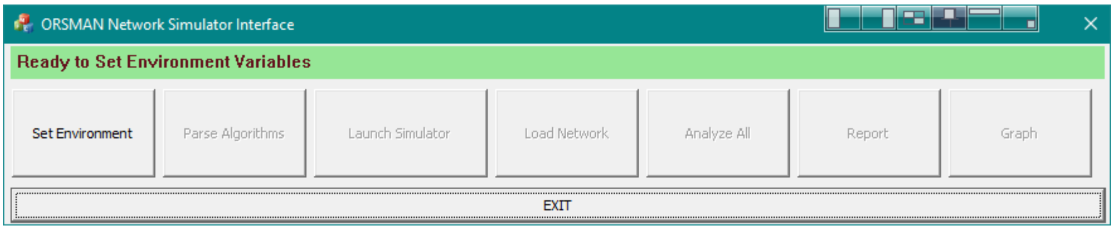


**Fig 5: Network Simulation Interface**

For current and planned approaches, experiments are carried out in OPNET with various numbers of nodes. Table 4 shows the specifics of the simulation setup..

| S.No. | Entity | Details |
|---|---|---|
| 1 | Simulation Area | 10000 Square meters |
| 2 | Number of Nodes | 100 to 1000 in step 100 |
| 3 | Node types | Mobile devices (Uniform Distribution) |
| 4 | Number of Routers | Automatic Selection |
| 5 | Node Placement | Random distribution |
| 6 | Network density | Default |
| 7 | RF Range of IoT-WSN Nodes | 500 meters |
| 8 | Frequency bands | GSM/4G |
| 9 | Simulation Time | 168 real-world hours |

**Table 4: Simulation Details**

## 5. Results and Analysis

Currently used methods MRP OPSTSA, EAAORS, MRP EMS and OEERS, as well as the suggested method MRP ORSMAN, have been tested and compared in this chapter. Throughput, end-to-end delay, latency, average energy, jitter, and packet delivery ratio are all measured and studied in the network.

### A. Throughput

The amount of data successfully transported from one location to another in a certain period of time is referred to as throughput. Bits per second are used to measure throughput. The highest possible throughput indicates the highest possible network quality. The measured throughput numbers are in table 5, and the comparison graph is in fig 6.

**JOURNAL OF ALGEBRAIC STATISTICS**
Volume 13, No. 2, 2022, p. 595 - 607
https://publishoa.com
ISSN: 1309-3452

| **Throughput (Kbps)** | | | | | |
|---|---|---|---|---|---|
| ***No. of Nodes*** | ***MRP_OPSTSA*** | ***MRP_EAAORS*** | ***MRP_EMS*** | ***MRP_OEERS*** | ***MRP_ORSMAN*** |
| 100 | 116.43 | 124.53 | 136.23 | 127.63 | 138.92 |
| 200 | 118.73 | 127.80 | 140.39 | 129.39 | 142.8 |
| 300 | 119.03 | 129.46 | 142.36 | 129.69 | 145.56 |
| 400 | 118.46 | 129.53 | 142.53 | 127.46 | 147.66 |
| 500 | 116.63 | 127.19 | 142.69 | 124.90 | 147.23 |
| 600 | 112.13 | 124.93 | 136.69 | 120.86 | 142.13 |
| 700 | 107.36 | 120.26 | 131.76 | 115.96 | 142.16 |
| 800 | 100.86 | 114.46 | 131.60 | 108.40 | 138.53 |
| 900 | 92.76 | 108.53 | 125.16 | 100.29 | 132.30 |
| 1000 | 83.73 | 99.13 | 117.53 | 91 | 125.26 |

***Table 5: Throughput***

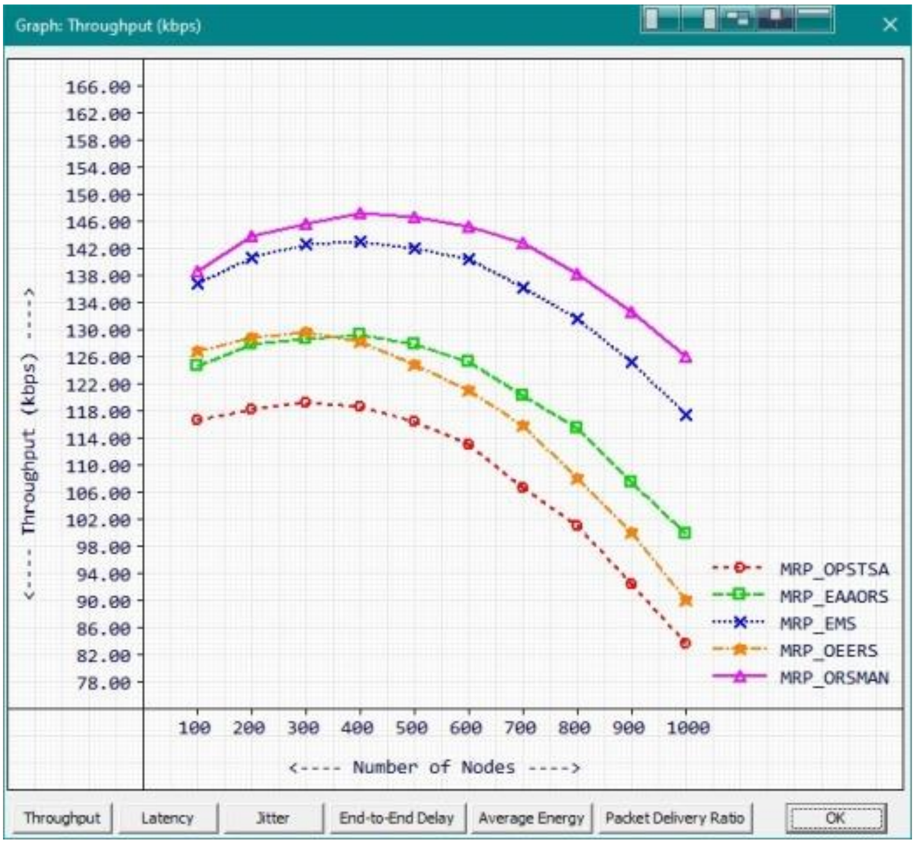


***Fig 6: Throughput***

***B. Latency***

Latency measures the time it takes for some data to get to its destination across the network. Latency is a measure of delay. It is measured in milliseconds (ms). The lower value of latency will be achieved by higher quality networks.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 595 - 607
https://publishoa.com
ISSN: 1309-3452

| **Latency (Ms)** | | | | | |
|---|---|---|---|---|---|
| ***No. of Nodes*** | ***MRP_OPSTSA*** | ***MRP_EAAORS*** | ***MRP_EMS*** | ***MRP_OEERS*** | ***MRP_ORSMAN*** |
| 100 | 135 | 129 | 116 | 123 | 114 |
| 200 | 136 | 130 | 117 | 125 | 115 |
| 300 | 138 | 133 | 118 | 127 | 116 |
| 400 | 141 | 137 | 119 | 131 | 117 |
| 500 | 144 | 140 | 122 | 133 | 119 |
| 600 | 147 | 145 | 124 | 137 | 121 |
| 700 | 151 | 150 | 126 | 143 | 122 |
| 800 | 156 | 155 | 127 | 147 | 122 |
| 900 | 163 | 161 | 130 | 153 | 124 |
| 1000 | 168 | 168 | 133 | 159 | 125 |

***Table 6: Latency***

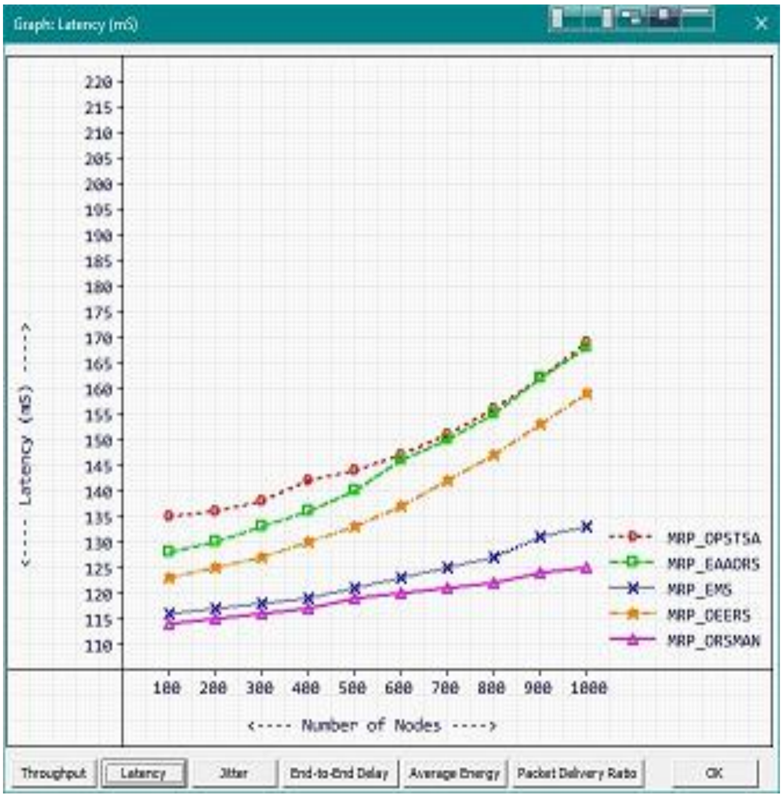


***Fig 7: Latency***

***C. Jitter***

Jitter is intermittent delays during data transfer. Due to the network congestion, improper queuing or delay between packet transfer are the causes of jitter. Minimum number of jitter will produce maximum quality of network performance.

**JOURNAL OF ALGEBRAIC STATISTICS**
Volume 13, No. 2, 2022, p. 595 - 607
https://publishoa.com
ISSN: 1309-3452

| ***Jitter*** **(Ms)** | | | | | |
|---|---|---|---|---|---|
| ***No. of Nodes*** | ***MRP_OPSTSA*** | ***MRP_EAAORS*** | ***MRP_EMS*** | ***MRP_OEERS*** | ***MRP_ORSMAN*** |
| 100 | 54 | 51 | 46 | 49 | 45 |
| 200 | 54 | 52 | 46 | 50 | 46 |
| 300 | 55 | 53 | 47 | 51 | 46 |
| 400 | 57 | 54 | 47 | 52 | 47 |
| 500 | 57 | 56 | 48 | 53 | 47 |
| 600 | 59 | 58 | 49 | 55 | 48 |
| 700 | 60 | 60 | 50 | 57 | 48 |
| 800 | 62 | 62 | 51 | 59 | 49 |
| 900 | 65 | 64 | 52 | 61 | 50 |
| 1000 | 67 | 67 | 53 | 63 | 50 |

***Table 7: Jitter***

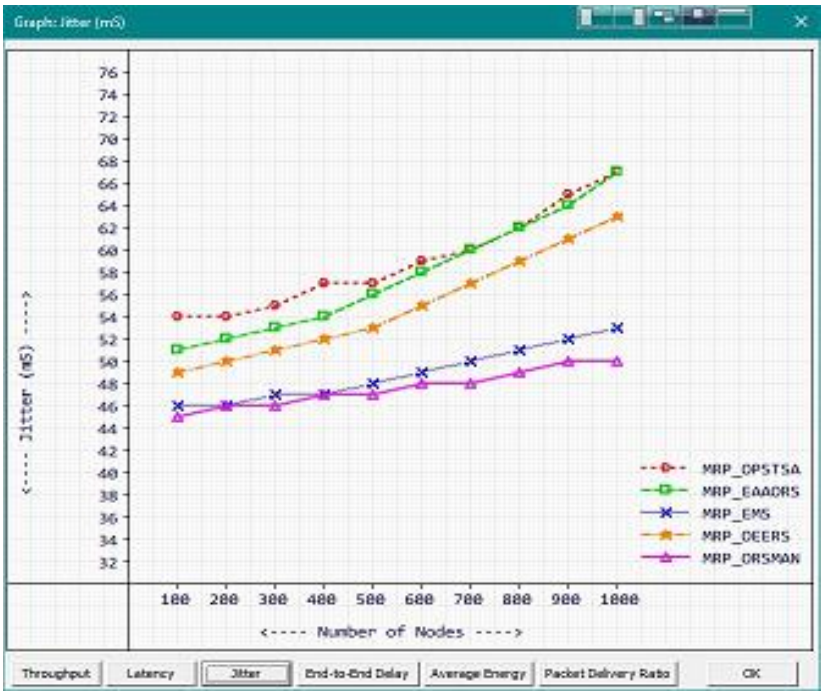


***Fig 8: Jitter***

### *D. End-to-End Delay*

End-to-end delay refers to the sum of all communication delays, such as jitter, IP-delay, and System delay. It describes how long a packet takes to travel from its origin to its destination. The end-to-end latency is significant since it has an impact on network quality. Figure 9 depicts a comparison graph of end-to-end delays for current and recommended ways, while Table 8 depicts end-to-end delays for existing and suggested approaches.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 595 - 607
https://publishoa.com
ISSN: 1309-3452

| ***End-to-End Delay* (Ms)** | | | | | |
|---|---|---|---|---|---|
| ***No. of Nodes*** | ***MRP_OPSTSA*** | ***MRP_EAAORS*** | ***MRP_EMS*** | ***MRP_OEERS*** | ***MRP_ORSMAN*** |
| 100 | 197 | 186 | 166 | 186 | 169 |
| 200 | 196 | 188 | 174 | 189 | 176 |
| 300 | 199 | 199 | 178 | 191 | 169 |
| 400 | 208 | 197 | 177 | 189 | 168 |
| 500 | 215 | 206 | 177 | 201 | 175 |
| 600 | 214 | 212 | 183 | 200 | 176 |
| 700 | 220 | 215 | 182 | 204 | 177 |
| 800 | 233 | 230 | 184 | 221 | 179 |
| 900 | 240 | 241 | 196 | 229 | 182 |
| 1000 | 249 | 244 | 196 | 229 | 187 |

***Table 8: End-to-End Delay***

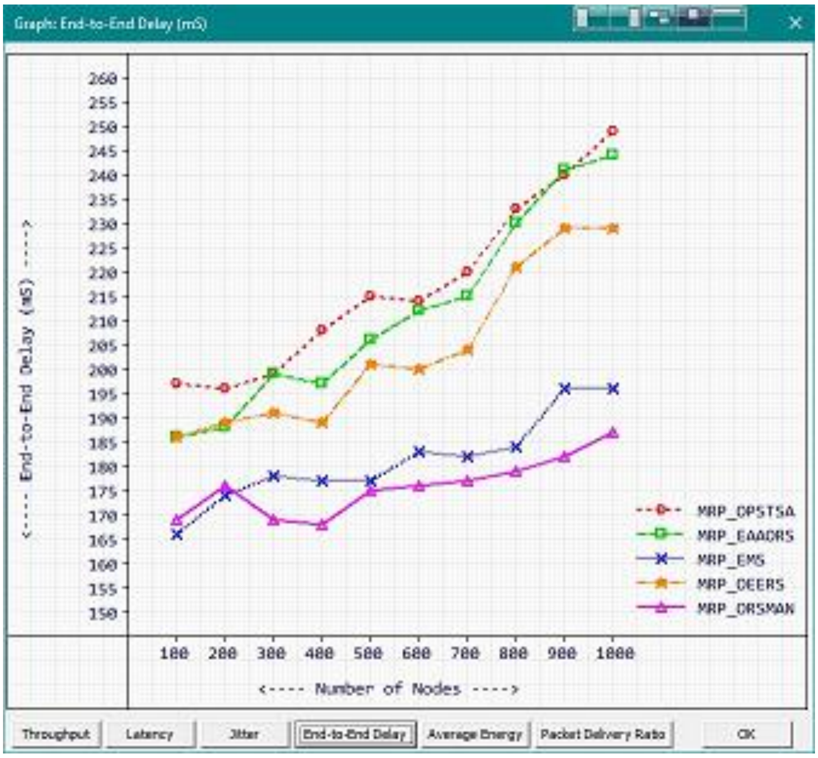


***Fig 9: End-to-End Delay***

### *E. Average Energy*

One of the features of network performance is its energy usage. It's challenging to keep the node's energy up throughout the transmission. When compared to existing approaches, the proposed ORS MAN method produced the best results in terms of energy consumption. Table 9 provides average energy measurements for known and suggested methodologies, while Figure 10 displays a comparison graph for the same.

**JOURNAL OF ALGEBRAIC STATISTICS**
Volume 13, No. 2, 2022, p. 595 - 607
https://publishoa.com
ISSN: 1309-3452

| *Average Energy* (UJ) | | | | | |
|---|---|---|---|---|---|
| ***No. of Nodes*** | ***MRP_OPSTSA*** | ***MRP_EAAORS*** | ***MRP_EMS*** | ***MRP_OEERS*** | ***MRP_ORSMAN*** |
| 100 | 457.36 | 489.02 | 537.33 | 508.56 | 490.63 |
| 200 | 464.06 | 492.65 | 542.13 | 514.46 | 495.26 |
| 300 | 469.23 | 498.54 | 548.53 | 521.23 | 495.23 |
| 400 | 476.26 | 504.04 | 554.53 | 527.93 | 503.73 |
| 500 | 484.43 | 510.86 | 561.53 | 535.16 | 508.7 |
| 600 | 492.73 | 517.56 | 569.33 | 543.13 | 514.66 |
| 700 | 501.23 | 525.12 | 577.66 | 552.03 | 520.36 |
| 800 | 510.4 | 532.68 | 586.13 | 561.13 | 526.66 |
| 900 | 519.83 | 541.97 | 595.26 | 571.43 | 533.36 |
| 1000 | 530.66 | 551.33 | 605.2 | 581.66 | 540.53 |

***Table 9: Average Energy***

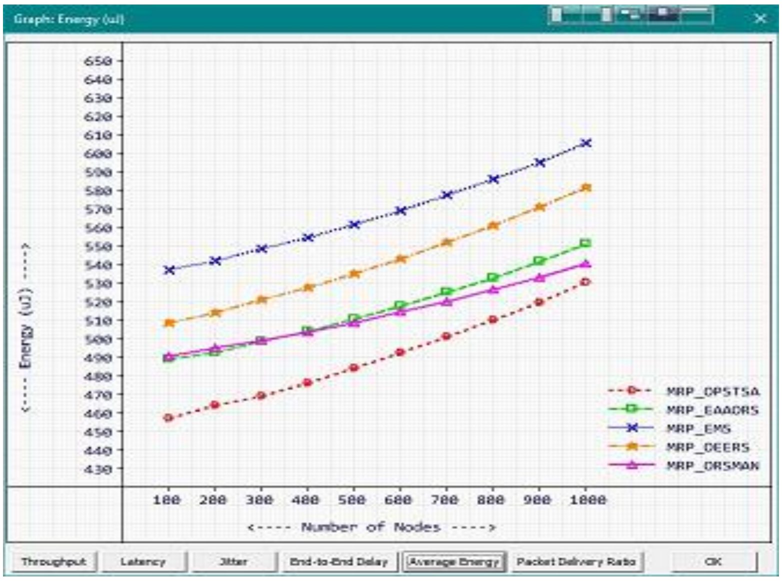


***Fig 10: Average Energy***

***F. Packet Delivery Ratio***

It is the ratio between the number of transmitted packets by the source and number of received packets by the destination and it is measured by %. The PDR values obtained from the simulations are tabulated as in table 10and comparison graph of the PDR is given in Fig 11.

| *Packet Delivery Ratio(%)* | | | | | |
|---|---|---|---|---|---|
| ***No. of Nodes*** | ***MRP_OPSTSA*** | ***MRP_EAAORS*** | ***MRP_EMS*** | ***MRP_OEERS*** | ***MRP_ORSMAN*** |
| 100 | 79.28 | 82.85 | 98 | 78.14 | 99.85 |
| 200 | 76.31 | 80.70 | 97.14 | 77.31 | 99.36 |

| | | | | | |
|---|---|---|---|---|---|
| 300 | 73.91 | 79.54 | 96.14 | 75.04 | 97.72 |
| 400 | 71.51 | 78.10 | 94.14 | 74.21 | 96.80 |
| 500 | 68.68 | 77.24 | 93.28 | 71.24 | 96.30 |
| 600 | 66.28 | 75.51 | 92.28 | 70.83 | 96.10 |
| 700 | 64.74 | 74.50 | 91.14 | 69.00 | 94.32 |
| 800 | 61.77 | 72.06 | 90.28 | 66.45 | 94.68 |
| 900 | 58.80 | 71.48 | 89.85 | 64.76 | 92.76 |
| 1000 | 56.68 | 69.32 | 89.85 | 63.79 | 92.26 |

***Table 10: Packet Delivery Ratio***

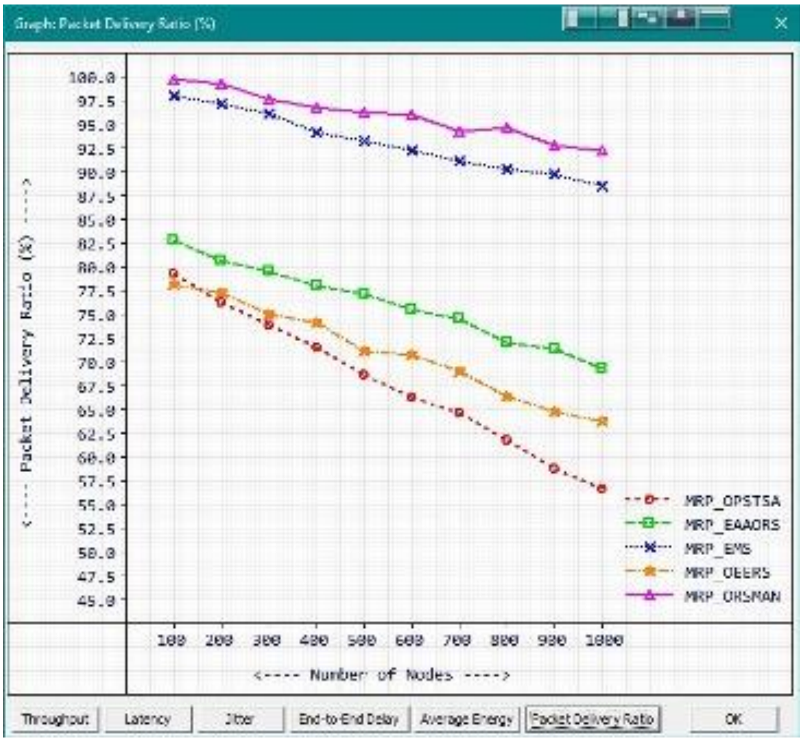


***Fig 11: Packet Delivery Ratio***

## 6. Conclusion

The suggested ORS approach implements an alternate path algorithm to reduce computational costs. When compared to other methods, ORS produces better outcomes. From the base station to the cluster head, and from the cluster head to the member node, ORS offers the most energy-efficient path. This research will eventually be expanded to include the development of a secure routing algorithm.

## References

[1]. Wei Liu and Ming Yu, “AASR:Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments,” IEEE Transaction On Vehicular Technology., vol. X, no. Y, March 2014.

[2]. Torkestani JA, Meybodi MR (2011) , A link stability-based multicast routing protocol for wireless mobile ad hoc networks. J NetwComputAppl 34(4):1429–1440

**JOURNAL OF ALGEBRAIC STATISTICS**
Volume 13, No. 2, 2022, p. 595 - 607
https://publishoa.com
ISSN: 1309-3452

[3]. A.Yashwanthreddy, M.RakeshChowdary and A.Krishna, “Authenticated Anonymous secure routing strategy for high speed networks”, International Journal of Applied and Advanced Scientific Research, ISSN:No-2456-3080, Volume-2,Issue:2, 2017
[4]. Wang N-C, Lee C-Y (2012) A multi-path qos multicast routing protocol with slot assignment for mobile ad hoc networks. Inform Sci 208:1–13
[5]. Li L, Li C (2007) A qos multicast routing protocol for clustering mobile ad hoc networks. Computer Commun 30(7):1641–1654
[6]. Xia H, Xia S, Jia Y, Jia Z, Sha EH-M (2014) Applying link stability estimation mechanism to multicast routing in manets. J SystArchit 60(5):467–480
[7]. Basurra SS, De Vos M, Padget J, Ji Y, Lewis T, Armour S (2015) Energy efficient zone based routing protocol for manets. Ad Hoc Netw 25:16–37
[8]. Hou R, Wang C, Zhu Q, Li J (2014) Interference-aware qos multicast routing for smart grid. Ad Hoc Netw 22:13–26
[9]. Wang X, Cheng H, Huang M (2014) Qos multicast routing protocol oriented to cognitive network using competitive coevolutionary algorithm. Expert SystAppl 41(10):4513–4528 Peer-to-Peer Netw. Appl.
[10]. Wang G, Peng Y, Feng P, Wang N (2014) An energy consumption minimization routing scheme based on rate adaptation with qos guarantee for the mobile environment. ComputNetw 74:48–57
[11]. Sahin D, Gungor VC, Kocak T, Tuna G (2014) Quality-of-service differentiation in single-path and multi-path routing for wireless sensor network-based smart grid applications. Ad Hoc Netw 22:43–60
[12]. Basarkod PI, Manvi SS (2015) Mobility and qos aware any cast routing in mobile ad hoc networks. ComputElectrEng
[13]. Alasaad A, Nicanfar H, Gopalakrishnan S, Leung VCM (2013) A ring-based multicast routing topology with qos support in wireless mesh networks. WirelNetw 19(7):1627–1651
[14]. Ivascu GI, Pierre S, Quintero A (2009) Qos routing with traffic distribution in mobile ad hoc networks. ComputCommun 32(2):305–316
[15]. Biradar RC, Manvi SS (2012) Ring mesh based multicast routing scheme in manet using bandwidth delay product. WirelPersCommun 66(1):117–146
[16]. Das SK, Tripathi S, Burnwal AP (2015) Fuzzy based energy efficient multicast routing for ad-hoc network. In: 2015 Third international conference on computer, communication, control and information technology (C3IT). IEEE, p 2015
[17]. Cadger F, Curran K, Santos J, Moffett S (2013) Towards a location and mobility-aware routing protocol for improving multimedia streaming performance in manets. Peer-to-Peer Networking and Applications 8(3):543–554
18]. Wang Gaocai, Peng Ying, Feng Peng, Wang Nao (2014) An energy consumption minimization routing scheme based on rate adaptation with qos guarantee for the mobile environment. Comput Netw 74:48–57
[19]. Yen Y-S, Chan Y-K, Chao H-C, Park JH (2008) A genetic algorithm for energy-efficient based multicast routing on manets. Comput Commun 31(4):858–869
[20]. Basurra SS, De Vos M, Padget J, Ji Y, Lewis T, Armour S (2015) Energy efficient zone based routing protocol for manets. Ad Hoc Netw 25:16–37
[21]. Liu Y, Wang Z (2012) Maximizing energy utilization routing scheme in wireless sensor networks based on minimum hops algorithm. Comput Electr Eng 38(3):703–721
[22]. Budyal VR, Manvi SS (2014) Agent driven delay and power constrained multicast routing in mobile ad hoc networks by using anfis. Wirel Pers Commun 75(1):531–556
[23]. Dipika Sarkar, Swagata Choudhury and Abhishek Majumder, “Enhanced-Ant-AODV for optimal route selection in mobile ad-hoc network”, Journal of King Saud University-Computer and Information Sciences,https://doi.org/10.1016/j.jksuci.2018.08.013 , August 2018.
*[24]. M.Devapriya and P.Ramesh, “An Optimized Energy Efficient Route Selection Algorithm for Mobile Ad hoc Networks based on LOA”, International Journal of Engineering and Advanced Technology, ISSN:NO-2249-8958,Volume-8, Issue-2S, December 2018*
[25]. E.Edwin Lawrence, R.Latha, “ Shortest and Energy Efficient Routing Protocol for MANET”,International Journal of Computer Sciences and Engineering, Volume-6, Issue-10, October 2018
[26]. Pradeep Chouksey,"Study of Routingin Adhoc network", International Journal of Scientific Research in Network SecurityandCommunication, Vol.5,Issue.2,pp.55-57,2017