Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 5318136, 12 pages
https://doi.org/10.1155/2022/5318136

Research Article

Cluster Head Selection and Energy Efficient Multicast Routing Protocol-Based Optimal Route Selection for Mobile Ad Hoc Networks

R. Suresh Kumar,[1] **P. Manimegalai**,[2] **P. T. Vasanth Raj**,[1] **R. Dhanagopal**,[1] **and A. Johnson Santhosh**[3]

[1] *Center for System Design, Chennai Institute of Technology, Chennai, India*
[2] *Department of Biomedical Engineering, Karunya Institute of Technology and Sciences, Coimbatore, India*
[3] *Faculty of Mechanical Engineering, Jimma Institute of Technology, Jimma University, Jimma, Ethiopia*

Correspondence should be addressed to A. Johnson Santhosh; johnson.antony@ju.edu.et

Received 8 April 2022; Revised 28 May 2022; Accepted 31 May 2022; Published 9 June 2022

Academic Editor: Kalidoss Rajakani

Wireless networks with a large number of peer nodes are known as mobile ad hoc networks (MANETs). In MANETs, the mobility of nodes causes a number of challenges, including path preservation, battery life, safety, dependability, and unexpected connection characteristics. As a result, the network's quality of service (QoS) would be compromised (QoS). For the discovery and maintenance of pathways in MANETs, the routing protocol is critical. By implementing the multicast routing protocol, the MANET network's reliability may be improved significantly. Evaluation of multicast routing for quality of service (QoS) is the primary goal of this study. 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. This proposed research paper optimal route selection (ORS) provides the cluster head selection and alternate cluster head selection for avoiding the failure of the cluster head, generation of the optimal path between the cluster head and member node based on reliability pair factor and node's energy, and establishment of the path based on maximum energy and number of hops between the nodes (minimum number of hops). In comparison to existing methods, ORS is more effective in the energy-efficient path between base station and cluster head, and member node is provided by an ORS route. Results show that the proposed ORSMAN has higher throughput, minimum latency, minimum jitter, and maximum packet delivery ratio, when compared to the existing methodologies.

1. Introduction

MANETs, or mobile ad hoc networks, are used by a diverse variety of computer devices, including laptops, smart phones, and other computing solutions. Mobile devices' network connections take the form of node connections and are mostly a term that is being utilized in the present circumstances. Additionally, the defined range of communication, even in regular conversation, has a significant impact. Mobile communication has become a necessary component. A network partition as a component of the network topology was categorized in MANET [1]. For MANETs, energy-efficient multicast is one of the most important criteria in determining the system's success. In this process, it was anticipated that the restricted battery capacity of mobile nodes would lead to increased power consumption, which in turn might have a substantial influence on the nodes' ability to transmit data, potentially creating new problems.

For MANET nodes, access and usage are limited, and security and privacy concerns arise because of the wireless communication channel. Interoperability and data exchange are made possible by the open nature of wireless mediums. There is security issues associated with open-access media since an attacker may break through the nodes' communication [2]. Intruders

Table 1: Methodologies and limitations of exiting methods.

Reference	Work	Methodology	Advantages	Limitations
[28]	Optimal path selection in MANET for time sensitive applications (OPSTSA)	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
[29]	Enhanced-ant-AODV for optimal route selection in MANET(EAAORS)	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
[30]	An optimal energy efficient route selection algorithm for mobile ad hoc networks based on LOA (OEERS)	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
[31]	Shortest and energy efficient routing protocol for MANET (EMS)	It provides the algorithm for selecting the minimum energy node and provides the routing path based on minimum number of hops	Minimum energy consumption and minimized hop counting	Security is not achieved

```
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 ($N_E.N_D$, $F_{RP}$)
Broadcast the request message (REQ) to all other nodes. When the nodes are in the same path which accepts the REQ message and it replied to the cluster head
Calculate $F_{RP} = \max((\mathrm{Ep}^{rem}, \mathrm{Eq}^{rem})/(d(p, q, t)))$, where $d$ is the distance between node $p$ and node $q$ at time stamp
And cluster head finds the substitute cluster head (SCH) based on the calculation of CH>SCH>MN
Cluster head updates the cluster table in the base station
When the cluster head become arid, then the substitution cluster head maintains the cluster members energy, distance, and reliability pair factor
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
```

Algorithm 1: Cluster Head Selection Algorithm

or adversaries may get access to a network's communications by exploiting network dynamics, node mobility, and the absence of centralized administrative assistance. A malicious user or node that interrupts itself into the network's transmission is able to gather data about the other nodes. A further battering is then launched to limit resources, route failure, and packet loss, as well as the spoofing of others [3]. This kind of attack is determined by the nature and aim of the intrusion into the network by the adversary. As a consequence, network performance degrades, resources are wasted, and the privacy of users is jeopardized. This is why a MANET's cooperative routing and attack mitigation technologies are built [4]. Numerous research has already been done on the routing protocol for MANETs to find solutions for nodes that are conscious of their energy usage [5].In order to identify decentralized recognition in a quick reaction time by utilizing the distinctive highlights of power flow in the independence of diverse groups, graph-theory-based network partitioning algorithms have been provided thus far [6]. In one such application, sensors installed in the pipeline network are used to solve a data-driven detection issue caused by device failure or a network disruption, which impedes pipeline status monitoring in its turn. This problem may be resolved to prevent the leakage of data [7].

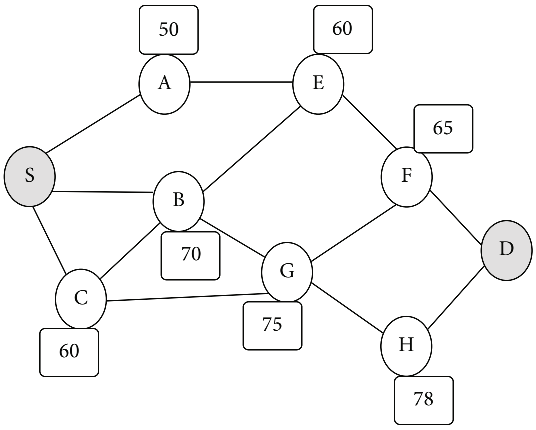
To advance packages from one node to another, the MANET hub serves as both host and switch [8, 9]. Applications where there is no precedent, such as military [10], disaster relief [11], and mining activities [12], benefit from this. Zaghal et al. have proposed a novel strategy for enhancing QoS in MANET multipath routing systems [13]. The principle of this strategy is to increase load balancing and hence reduce congestion on overcrowded lines. As a result, the most critical applications get top priority when packets are routed over the network. Then, the link failures and packet losses may be reduced by a more efficient management of continual connections and delinking. According to [14–16], the quality of service (QoS) in an AODV routing protocol variation has been proposed. Using the Moving Picture Experts Group (MPEG)-4 compressions, the proposed method may improve routing performance and data transmission throughput in a variety of network settings. To assess the AOMDV, variables such as data packet size and time duration are taken into account. Using sensors

```
The source node initiates the creation of a route request packet RREQ
RREQ contains the following information: the RREQ ID, the destination address, the source address, the destination sequence number, the source sequence number, the NmaxE, and the hop count
NmaxE is updated by a node receiving the packet only if its energy level is greater than the current NmaxE; otherwise, NmaxE stays constant
Continue checking until RREQ reaches its target
The most energy efficient route is chosen from the numerous RREQ collected from several routes
If (NmaxE=high &&hopcount=low), choose the communication route
A route response RREP is created and returned
Data is sent through the newly specified route
```

Algorithm 2: Optimal Path Selection Algorithm

installed in pipeline networks, a data-driven detection issue occurs when a device fails or the network is disrupted, which prevents the deployment of pipeline monitoring. It is possible to avoid data leaking by solving this problem [17].

The following is the structure of the paper: The Literature Review in Section 2 focuses on multicast routing and sensor node clustering. The proposed scheme of reliability pair factor based on multiple models and the cluster head selection method based on energy, hop counting, and reliability pair factor, as well as the optimal path selection based on hop counting, are explained in Section 3. The conclusion is established in Section 6.



S – A – E – F – D	Hopcount = 3, N_{maxE} = 65
S – B – E – F – D	Hopcount = 3, N_{maxE} = 80
S – B – G – F– D	Hopcount = 3, N_{maxE} = 80
S – B – G – H – D	Hopcount = 3, N_{maxE} = 80
S – C – B – E – F – D	Hopcount = 4, N_{maxE} = 80

Figure 1: Communication path between source and destination.

2. Related Works

Li et al. [18] proposed the DAPV approach for identifying abnormalities in MANETs and enhancing their routing efficiency. Direct and indirect route adversaries may be detected by DAPV, which is valid. A Merkle-based hash tree is used to identify and authenticate neighbors in DAPV's peer logs. Using this approach, it is possible to identify more targets with less effort and at a lower cost. Cai et al. [19] present evolutionary self-cooperative trust (ESCT) to reduce MANET routing distraction. The human intervention process is replicated, and the confidence of the route nodes is evaluated at multiple stages in this safe routing approach. The scheme's most dependable feature is its ability to withstand known assaults. Each stage of assault detection has its own unique decision-making process. In terms of energy consumption, latency, and packet delivery ratio, this strategy produces a reliable network output.

A behavior-based analysis technique was presented by Zhang et al. [20] as a defense against various types of attacks. Based on the nodes' activities and reactions to their neighbors, various attacks are detected. This response confirms that the nodes are capable of processing and forwarding data packets effectively. With the use of layer 4 transport protocols and typical ad hoc routing, the authors confirmed the algorithm's consistency in terms of latency and packet delivery ratio. Wang et al. [21] provide a trust-based multiobjective optimization (MOO) for enhancing MANET service outcomes. Multidimensional trust is aided by this optimization when network resources and communication are allocated and communicated. To put it another way, this trust optimization strategy reduces the cost of service and increases the quality of service between service providers and nodes. Vaseer et al. [22] used energy, communication, and recommendation-based trust assessment in the MANET scenario to enhance its flexibility and dispersed nature. Distance, packet transmission rate, dependability, and familiarity of the nodes are used to assess the trust model's adaptive quality. One-to-one validation reduces the effect of attackers by using the trust concept. As a result, the node's trustworthiness may be verified for subsequent transmissions using mean trust alone. To improve the detection rate, we need to figure out how trustworthy each node is.

In order to avoid black hole attacks in MANET, Keerthika and Malarvizhi [23] created a trust-based artificial bee colony 2-opt method with a weighted trust component. Finding the most direct route to a given location is done by using the artificial bee colony method, while the fitness function evaluation in the 2-opt algorithm determines how trustworthy the nodes are. Two algorithms are combined

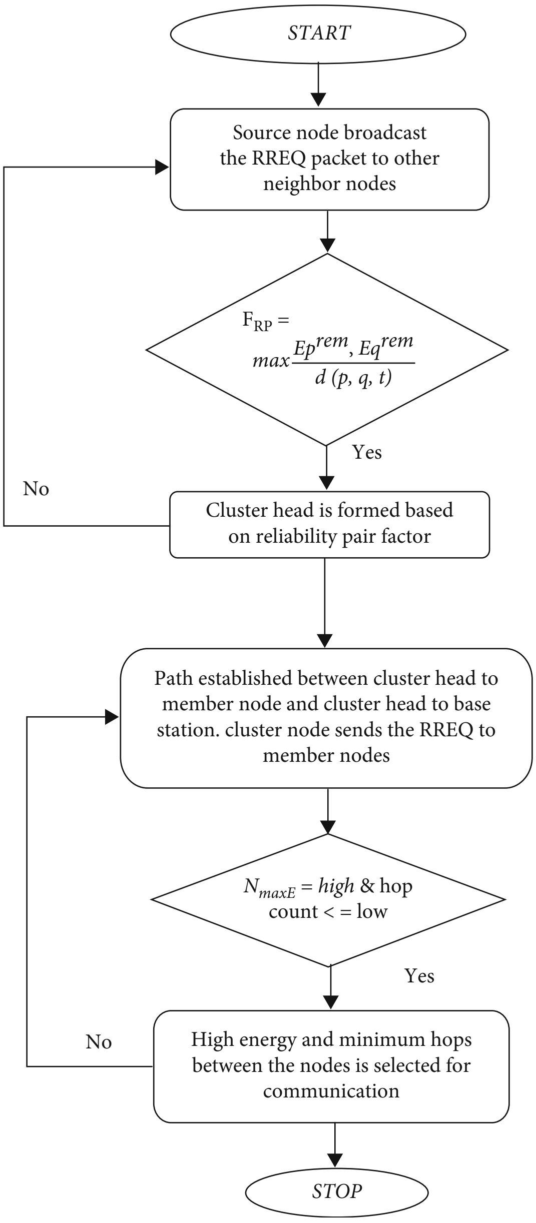

START
Source node broadcast the RREQ packet to other neighbor nodes
$F_{RP} = \max \frac{Ep^{rem}, Eq^{rem}}{d\,(p, q, t)}$
Yes
No
Cluster head is formed based on reliability pair factor
Path established between cluster head to member node and cluster head to base station. cluster node sends the RREQ to member nodes
$N_{maxE} = high$ & hop count < = low
Yes
No
High energy and minimum hops between the nodes is selected for communication
STOP

Figure 2: Flow chart of ORSA.

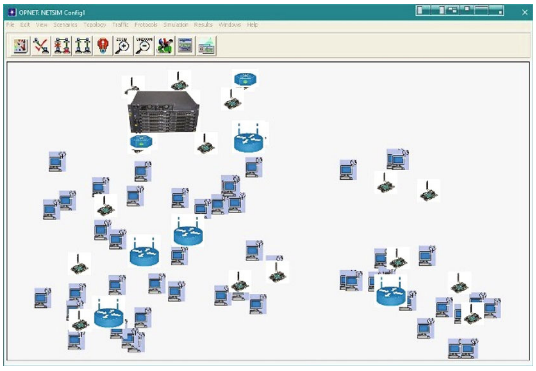
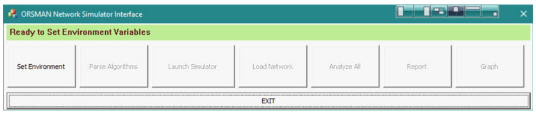

OPNET: NETSIM Config1
File Edit View Scenarios Topology Traffic Protocols Simulation Results Windows Help

Figure 3: Network setup.



Ready to Set Environment Variables

Figure 4: Network simulation interface.

to create a trust model that decreases the distance to the sink and delays while delivering more reliable packets. This method was established by Mechtri et al. [24] as a measure of how well an attack may be evaded. Adversaries in the routing route are notified to source nodes so that they may make better routing decisions. This reduces the number of false alarms in the network, regardless of the number of attacks on the MANET. Improved packet delivery and reduced latency may be achieved with this strategy by limiting the false detection rate.

Demidov et al. [25] examined the difficulty in identification and mitigation of cyber security risks in ad hoc wireless networks. A neural network has been used to analyze the issues in ad hoc networks more accurately. In order to improve the security of ad hoc networks, this neural network training makes use of probability maximization and recurrent graph analysis models. The particle swarm optimization (PSO) and adaptive neuro fuzzy inference system (ANFIS) were proposed by Moudni et al. [26] to identify and mitigate black hole hazards in MANET routing. Packet forwarding percentage and destination concentric sequence number are used to create fuzzy rules for a network. PSO is used to identify conditional routes that meet the requirements of the fulfilled criteria.

The combined strategy eliminates false alarms by removing nodes that break the rules from the transmission process. Vigenesh and Santhosh [27] develop an efficient stream region sink position analysis (ESRSPA) to improve the detection of attacks in the MANET routing process. The existence of an attack is discovered in the stream area analysis by obtaining the position of the sink and other authorized nodes. The transmission route is dictated by the sink's location. An attacker is a node that is unable to meet the weight limits in a stream. The routes that include such nodes are rejected. Reliable network speed and packet delivery are the hallmarks of this approach's low overhead. In order to make MANETs more resistant to attacks, Zhang et al. [28] proposed a reputation management system. Adapting reputable neighbors for route finding and communication improves network performance. Transmission pathways are chosen based on the sum of the reputations of the nodes in the network. In order to enhance detection, the reputation of the nodes is evaluated based on subjective and recommendation-based trust.

This study [29] proposes trust-based authentication for dynamically secured routing. This network-wide trust-based routing system uses a threshold value to identify the 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 the node. An adversarial environment's trust nodes respond by minimizing the data packet

Table 2: Simulation details.

S. no.	Entity	Details
1	Area required for simulation	10,000 square meters
2	Node counts	In step 100, go from 100 to 1,000
3	Types of nodes	Mobile devices
4	Router specification	Selecting automatically
5	Placement of nodes	Distribution at random
6	Density of the network	Default
7	Radio frequency range	0.5 km
8	Frequency spectrum	4G
9	Time required for simulation	168 hours

Table 3: Throughput.

No. of nodes	OPSTSA [29]	EAAORS [30]	EMS [35]	OEERS [34]	ORSMAN (proposed method)
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

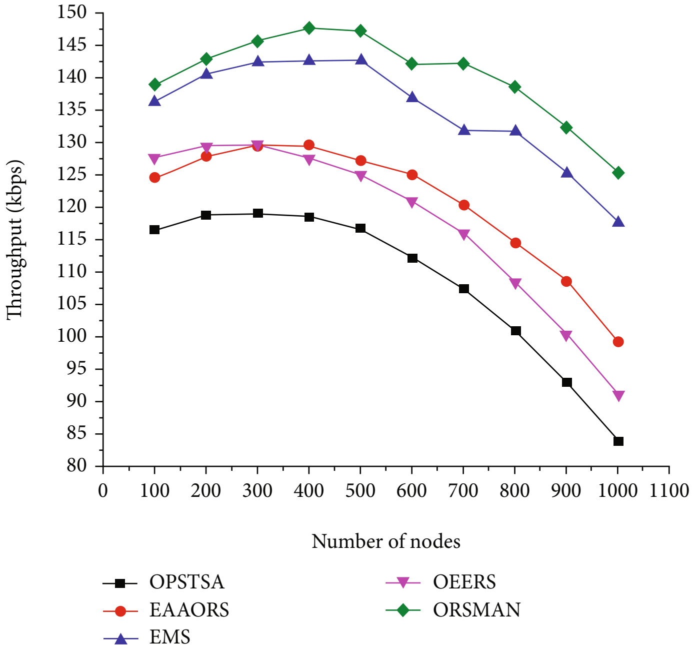


Figure 5: Throughput.

Table 4: Latency for the proposed ORSMAN.

No. of nodes	OPSTSA [29]	EAAORS [30]	EMS [35]	OEERS [34]	ORSMAN (proposed method)
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

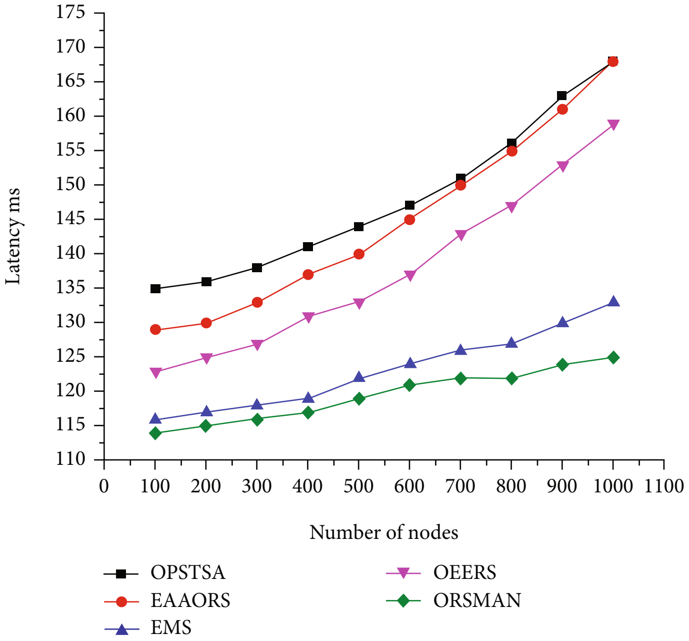


Figure 6: Latency for the proposed ORSMAN.

Table 5: Jitter for the proposed ORSMAN.

No. of nodes	OPSTSA [29]	EAAORS [30]	EMS [35]	OEERS [34]	ORSMAN (proposed method)
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

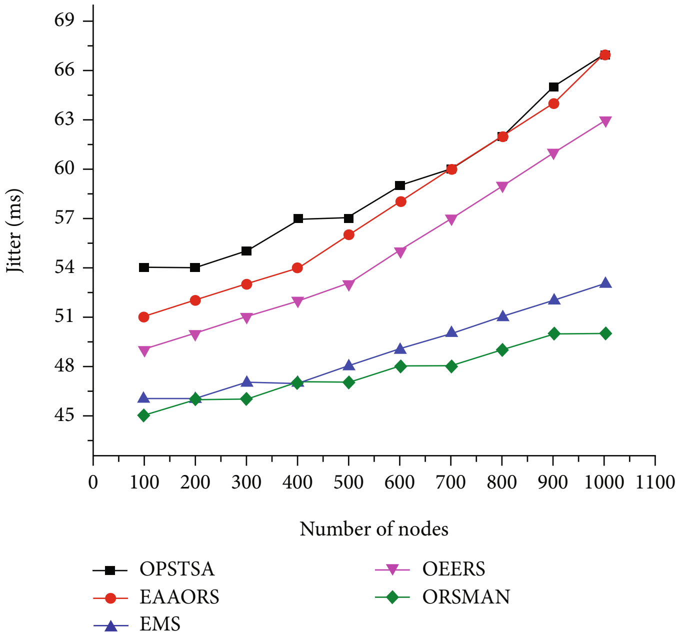


Figure 7: Jitter for the proposed ORSMAN.

Table 6: End-to-end delay for the proposed ORSMAN.

No. of nodes	OPSTSA [29]	EAAORS [30]	EMS [35]	OEERS [34]	ORSMAN (proposed method)
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

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 attack 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. Throughput may be enhanced greatly, while the average end-to-end time is decreased by raising the trust value of the authorized node in this technique.

Using route selection and an Ad Hoc On-Demand Distance Vector protocol, this study [30] improves MANET QoS. A pheromone value of the route is the greatest approach to communicate information. Congestion, number of nodes, and energy left over from previous nodes are all factor towards pheromone value. The route with the greatest pheromone value is used to transmit data. The ANT/AODV protocol's technique improves packet delivery ratio, throughput, and end-to-end delay. Traditional routing and clever machine learning paradigms are inherited by Sankaran et al. in the classification of nodes based on their communication patterns. It is possible to build reliable and secure pathways to a destination by thoroughly studying the behavior of the nodes at various communication hop levels [31]. In order to help the optimization process, intelligent computing and decision-making algorithms use present and previous behavior of nodes to identify the adversary. To ensure reliable communication in MANET, certain decision-making systems combine sensing properties and location, which need the use of external networks like the cloud

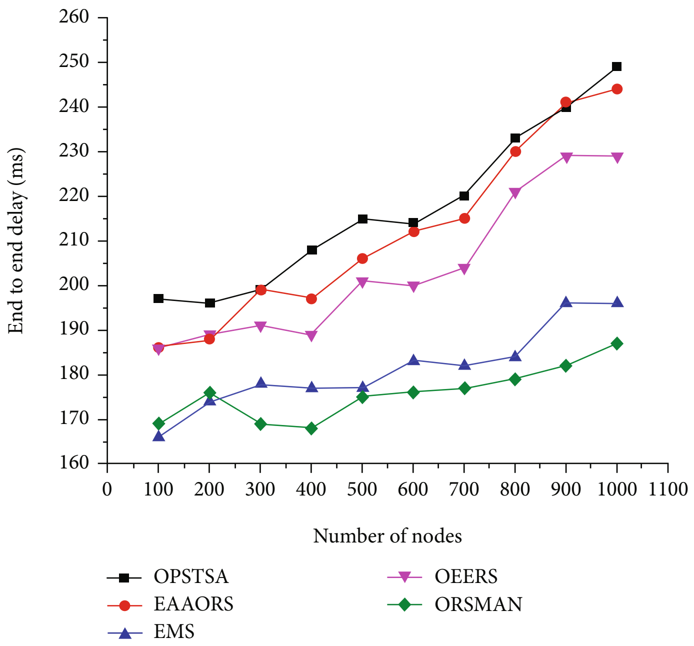


Figure 8: End-to-end delay for the proposed ORSMAN.

Table 7: Average energy for the proposed ORSMAN.

No. of nodes	OPSTSA [29]	EAAORS [30]	EMS [35]	OEERS [34]	ORSMAN (proposed method)
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

[32]. Yushuai et al. [33] investigated one of these multibodies, as well as the optimum energy consideration or production of all participants in the single bodies, as well as the optimal distribution of energy at the lines that were connected between any two energy entities.

The purpose of this research [34] is to show that trust and the Lion Optimization Algorithm (LOA) may be used to achieve energy-efficient MANET routing. Bioinspired LOA is used to choose the most effective data transmission route. The three processes are route establishment, trust metrics calculations, and optimum route selection. It is possible to discover various pathways between the source and the destination using the AODV protocol. In this research, the trust value was calculated based on energy, packet delivery rate, and queue time [35]. The work's efficiency is gauged by a variety of metrics, including packet delivery ratio, energy consumption, average latency, and network lifespan. Node fitness is used to determine the best paths in this investigation. Node reliability and efficiency improved, while energy consumption decreased as a consequence. Table 1 shows the comparison for various methodologies and limitations of the existing 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 maximum 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.

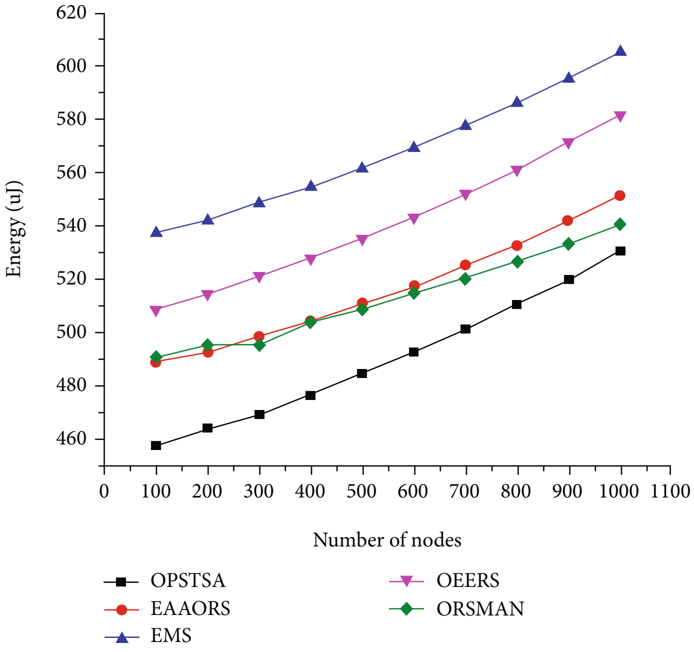


Figure 9: Average energy for the proposed ORSMAN.

Table 8: Packet delivery ratio for the proposed ORSMAN.

No. of nodes	OPSTSA [29]	EAAORS [30]	EMS [35]	OEERS [34]	ORSMAN (proposed method)
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

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.

3.2. Optimal Path Selection Algorithm. Optimal path selection algorithm is used to find the path between sources and destination. This algorithm, suggests the methodology based on maximum energy of the node and minimum hops between the nodes.

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 1 depicts an example of determining the shortest path with the highest energy node, and Figure 2 shows the flow chart of optimal path selection algorithm (OPSA).

4. Experimental Setup

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 node

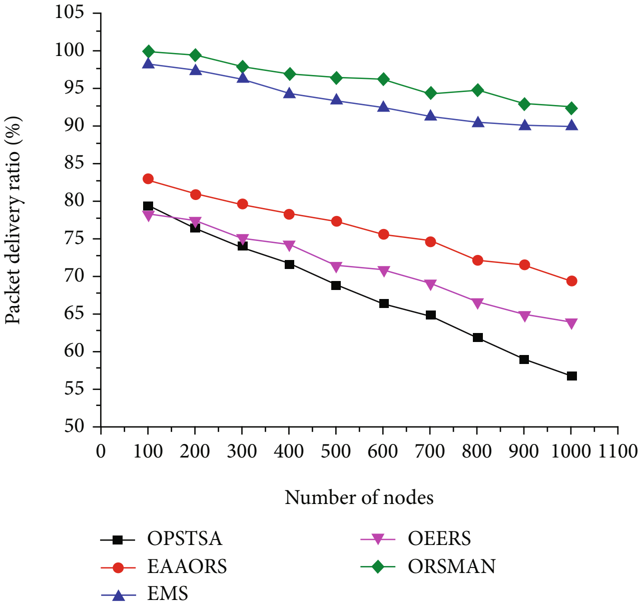


Figure 10: Packet delivery ratio for the proposed ORSMAN.

types, protocols, and network communication techniques can all be defined and overridden with OPNET as shown in Figure 3. 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. The user interface was shown in Figure 4.

Existing and proposed methods are tested in OPNET by varying the numbers of nodes. Table 2 provides the simulation setup information.

5. Results and Analysis

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

5.1. 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 3, and the comparison graph is in Figure 5.

5.2. 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. Table 4 and Figure 6 shows the latency in terms of milliseconds.

5.3. Jitter. Jitter is intermittent delays during data transfer. Due to the network congestion, improper queuing or delays between packet transfers are the causes of jitter. Minimum number of jitter will produce maximum quality of network performance. Table 5 and Figure 7 show the jitter in terms of milliseconds.

5.4. End-to-End Delay. The entire amount of all communication delays, such as jitter, IP delay, and system delay, is called end-to-end delay. It specifies the overall time taken for a packet to travel from its origin to its destination. End-to-end delay is important since it affects network quality. Table 6 shows end-to-end delays for existing and suggested approaches, whereas Figure 8 shows a comparison graph.

5.5. Average Energy. One of the features of network performance is its energy usage. It is 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 7 provides average energy measurements for proposed and existing methodologies, while Figure 9 displays a comparison graph for the same.

5.6. 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 8, and comparison graph of the PDR is given in Figure 10.

6. Conclusion

The proposed ORS method implements an alternate path algorithm to reduce computational costs. When compared to existing approaches, ORS provides superior results. ORS provides the most energy-efficient route from the base station to the cluster head and from the cluster head to the member node. Results show that the proposed ORSMAN has higher throughput at 400 nodes by 29.2 Kbps, by 18.13 Kbps, by 5.13 Kbps, and by 20.2 Kbps for OPSTSA, EAAORS, EMS and OEERS, respectively. The proposed ORSMAN has minimum latency at 1000 nodes by 43 ms, 43 ms, 8 ms, and 34 ms when compared to OPSTSA, EAAORS, EMS, and OEERS, respectively. Also the proposed ORSMAN achieved minimum jitter at 1000 nodes by 17 ms, 17 ms, 3 ms, and 13 ms when compared to OPSTSA, EAAORS, EMS, and OEERS, respectively. Maximum packet delivery ratio is achieved at 100 nodes by 20.57%, 17%, 1.85%, and 21.71% when compared to OPSTSA, EAAORS, EMS, and OEERS, respectively. As a future project, this protocol may be tested in a variety of network topologies and settings. We may also evaluate the performance of different cluster-based protocols by taking into account the mobility, traffic, and transmission range of the nodes.

Data Availability

The data are available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work is funded by the Centre for System Design, Chennai Institute of Technology, Chennai, vide funding number CIT/CSD/2022/006.

References

[1] M. Cagalj, J.-P. Hubaux, and C. Enz, *Minimum-Energy Broadcasting All-Wireless Networks: Np-Completeness and Distribution Issues*, Proceedings of the 8th Annual International Conference on Mobile Computing and Networking, ACM, 2002.

[2] Z. Ali Zardari, J. He, N. Zhu et al., "A dual attack detection technique to identify blackand gray hole attacks using an intrusion detection system and a connected dominating set in MANETs," *Future Internet*, vol. 11, no. 3, p. 61, 2019.

[3] A. Yasin and M. Abu Zant, "Detecting and isolating black-hole attacks in MANET using timer based baited technique," *Wireless Commun. MobileComput*, vol. 2018, pp. 1–10, 2018.

[4] M. Rmayti, R. Khatoun, Y. Begriche, L. Khoukhi, and D. Gaiti, "A stochastic approach for packet dropping attacks detection in mobile Ad hoc networks," *Computer Networks*, vol. 121, pp. 53–64, 2017.

[5] I. Kang and R. Poovendran, "Maximizing static network lifetime of wireless broadcast ad hoc networks," in *IEEE International Conference on Communications, 2003, ICC'03, vol. 3*, IEEE, 2003.

[6] D. Ma, X. Hu, H. Zhang, Q. Sun, and X. Xie, "A hierarchical event detection method based on spectral theory of multidimensional matrix for power system," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 4, pp. 2173–2186, 2021.

[7] X. Hu, H. Zhang, D. Ma, and R. Wang, "A tnGAN-based leak detection method for pipeline network considering incomplete sensor data," *IEEE Transactions on Instrumentation and Measurement*, vol. 70, pp. 1–10, 2021.

[8] D. N. Shashidhara, D. N. Chandrappa, and C. Puttamadappa, "A novel location aware content prefetching technique for mobile adhoc network," *Procedia Computer Science*, vol. 171, pp. 1970–1978, 2020.

[9] H. Zemrane, Y. Baddi, and A. Hasbi, "Mobile adhoc networks for intelligent transportation system: comparative analysis of the routing protocols," *Procedia Computer Science*, vol. 160, pp. 758–765, 2019.

[10] S. Manohar, V. Rajasekar, and N. Muthurasu, "Energy optimization and reliable message communication in mobile adhoc networks using packet shifting," *Materials today: Proceedings.*, vol. 70, pp. 1–10, 2020.

[11] V. Alappatt and P. J. Prathap, "Hybrid cryptographic algorithm based key management scheme in MANET," *Materials today: Proceedings*, 2020.

[12] D. Gautam and V. Tokekar, "A novel approach for detecting DDoS attack in MANET," *Materials Today: Proceedings*, vol. 29, pp. 674–677, 2020.

[13] R. Zaghal, S. Salah, and M. Ismail, "An InfniBand-based mechanism to enhance QoS in multipath routing protocols in MANETs," in *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pp. 1–5, IEEE, 2018.

[14] S. Gupta, S. R. Sinha, and P. Khatri, "Effect of varying pause time on performance of QoS parameters in MANET," *Proceedings of International Conference on Recent Advancement on Computer and Communication*, , pp. 105–113, Springer, Singapore, 2018.

[15] T. Pandikumar, B. Zewdie, and C. Z. Haile, "Mitigating black hole attack on MANET with AOMDV protocol," *International Journal of Engineering Science*, vol. 12666, 2017.

[16] T. R. Sheltami, E. Q. Shahra, and E. M. Shakshuki, "Performance comparison of three localization protocols in WSN using cooja," *J AmbIntellHumanizComput*, vol. 8, pp. 373–382, 2017.

[17] X. Hu, H. Zhang, D. Ma, and R. Wang, "A tnGAN-based leak detection method for pipeline network considering incomplete sensor data," *IEEE Transactions on Instrumentation and Measurement*, 2021.

[18] T. Li, J. Ma, Q. Pei, H. Song, Y. Shen, and C. Sun, "DAPV: Diagnosing anomalies in MANETs routing with provenance and verification," *IEEEAccess*, vol. 7, pp. 35302–35316, 2019.

[19] R. J. Cai, X. J. Li, and P. H. J. Chong, "An evolutionary self-cooperative trust scheme against routing disruptions in MANETs," *IEEE Transactions on Mobile Computing*, vol. 18, no. 1, pp. 42–55, 2019.

[20] D. G. Zhang, J.-X. Gao, X.-H. Liu, T. Zhang, and D.-X. Zhao, "Novel approach of distributed & adaptive trust metrics for MANET," *Wireless Networks*, vol. 25, no. 6, pp. 3587–3603, 2019.

[21] Y. Wang, I.-R. Chen, J.-H. Cho, A. Swami, and K. S. Chan, "Trust-based service composition and binding with multiple objective optimization in service-oriented mobile ad hoc networks," *IEEE Transactions on Services Computing*, vol. 10, no. 4, pp. 660–672, 2017.

[22] G. Vaseer, G. Ghai, and D. Ghai, "Novel intrusion detection and Prevention for mobile ad hoc networks: a single- and multiattack case study," *IEEE Consumer Electronics Magazine*, vol. 8, no. 3, pp. 35–39, 2019.

[23] V. Keerthika and N. Malarvizhi, "Mitigate black hole attack using hybrid bee optimized weighted trust with 2-Opt AODV in MANET," *Wireless Personal Communications*, vol. 106, no. 2, pp. 621–632, 2019.

[24] L. Mechtri, F. D. Tolba, and S. Ghanemi, "An optimized intrusion response system for MANET," *Peer-to-Peer Networking and Applications*, vol. 11, no. 3, pp. 602–618, 2018.

[25] R. A. Demidov, P. D. Zegzhda, and M. O. Kalinin, "Threat analysis of cyber security in wireless adhoc networks using hybrid neural network model," *Automatic Control and Computer Sciences*, vol. 52, no. 8, pp. 971–976, 2018.

[26] H. Moudni, M. Er-rouidi, H. Mouncif, and B. E. Hadadi, "Black hole attack detection using fuzzy based intrusion detection systems in MANET," *Procedia Computer Science*, vol. 151, pp. 1176–1181, 2019.

[27] M. Vigenesh and R. Santhosh, "An efficient stream region sink position analysis model for routing attack detection in mobile ad hoc networks," *Computers and Electrical Engineering*, vol. 74, pp. 273–280, 2019.

[28] S.-S. Zhang, S.-W. Wang, H. Xia, and X.-G. Cheng, "An attack-resistant reputation management system for mobile ad hoc networks," *Procedia Computer Science*, vol. 147, pp. 473–479, 2019.

[29] K. Sujatha, "Optimal path selection in mobile adhoc networks for time sensitive applications," *International Journal of Current Engineering and Scientific Research*, vol. 4, no. 9, 2017.

[30] D. Sarkar, S. Choudhury, and A. Majumder, "Enhanced-Ant-AODV for optimal route selection in mobile ad-hoc network," *Journal of King Saud University - Computer and Information Sciences*, vol. 33, no. 10, pp. 1186–1201, 2021.

[31] K. S. Sankaran, N. Vasudevan, K. R. Devabalaji, T. S. Babu, H. H. Alhelou, and T. Yuvaraj, "A recurrent reward based learning technique for secure neighbor selection in mobile AD-HOC networks," *IEEE Access*, vol. 9, pp. 21735–21745, 2021.

[32] F. Xia, S.-S. Xiao, X.-G. C. Zhang, and Z.-K. Pan, "A reputation-based model for trust evaluation in social cyber-physical systems," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 2, pp. 792–804, 2020.

[33] L. Yushuai, W. Gao, W. Gao, H. Zhang, and J. Zhou, "A distributed Newton descent algorithm for cooperative energy management of multiple energy bodies in energy Internet," *IEEE Transactions on Industrial Informatics*, vol. 17, pp. 5993–6003, 2021.

[34] 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*, vol. 8, no. 2S, 2018.

[35] E. Edwin Lawrence and R. Latha, "Shortest and energy efficient routing protocol for MANET," *International Journal of Computer Sciences and Engineering*, vol. 6, no. 10, p. 54, 2018.