Computers, Materials & Continua
DOI: 10.32604/cmc.2022.021857
Article

Tech Science Press

Efficient Load Balancing with MANET Propagation of Least Common Multiple Routing and Fuzzy Logic

V. Gayatri* and M. Senthil Kumaran

Department of Computer Science and Engineering, SCSVMV University, Enathur, Kanchipuram, 631561, India
*Corresponding Author: V. Gayatri. Email: 5678gayathri@gmail.com
Received: 17 July 2021; Accepted: 14 October 2021

Abstract: Mobile Ad Hoc Network **(**MANET) is a group of node that would interrelate among each other through one multi-hop wireless link, wherein the nodes were able to move in response to sudden modifications. The objective of MANET routing protocol is to quantify the route and compute the best path, but there exists a major decrease in energy efficiency, difficulty in hop selection, cost estimation, and efficient load-balancing. In this paper, a novel least common multipath-based routing has been proposed. Multipath routing is used to find a multipath route from source and destination. Load balancing is of primary importance in the mobile ad-hoc networks, due to limited bandwidth among the nodes and the initiator of the load routing discovery phase in the multipath routing protocol. Fuzzy logic for load balancing multipath routing in MANETs is proposed, which ensures the data packets are sent through a path with the variance of binary sets to predict the original transformation of the data to be received in the system. The main objective of the proposed system is to reduce the routing time of data packets and avoid the traffic based on multipath source and destination. The experimental results have to verify 96.7% efficiency in balancing the load.

Keywords: MANETs; multipath routing; least common multiple routing (LCMR) and fuzzy logic; route requests (RREQs); route replies (RREPs)

1 Introduction

Mobile Ad-hoc Networks (MANETs) are cellular, infrastructure-free, and self-organizing networks that can be implemented on-the-fly. The mobility factor in these networks leads to dynamic topological changes that make the routing task very challenging. Initial attempts to establish routing protocols imitated the ideas that predominate in wired networks. They did not perform satisfactorily well, because of the complexity of the mediums used in both the networks [1]. For wireless networks, the quality of the connection is determined by quality metrics that regulate the quality of communication over a link. MANET is known as the network of Wireless Ad Hoc (WAN). They include collecting nodes that are wirelessly connected to a self-configured, self-healing network without requiring fixed infrastructure, and nodes traveling freely within the rapidly changing network topology. A centralized

network due to multi-hop, in which data is comfortable [2]. A single node has to move through the router in those networks. Due to the limited node bandwidth, the intermediate node interacts with the source and destination nodes. The main routing problem noticed are interference, asymmetric links, overhead and Complex Topology. Some of the routing protocols used in MANETs are proactive such as DSDV, OLSR, and reactive as DSR, AOMDV and some are hybrid as ZRP.

Three AODV messages are route requests (RREQs). They commence as source node S is sent throughout the transitional in order to receive one route to destination Node D. Route Replies (RREPs), are undertaken, either by destination node or by the shortest path with a route to the appropriate destination [3]. Using the Fibonacci series, the transmit packet can be distributed in the load balancing protocol via mobile nodes. Routing was selecting and sorting between the numbers of hops in growing order [4]. FMLB has the following advantages: it uses the shortest path and enhances the effect of network congestion, and it achieves load balancing by using a Fibonacci sequence FMLB routing protocol. Fuzzy logic with multiple AODV properties, works based on distance vector routing and transmits the data hop through hop transfer packets [5,6], using a route discovery approach on routes of traffic aware links multipath that results in a reduction of delays and load distribution on multiple paths.

1.1 Contribution

The contribution of the proposed research includes:

- A Least Common Multiple Routing with Fuzzy Logic is proposed for balancing the load and incorporation of multipath while transmitting the data among the nodes.
- The initiator of node specification enables the multipath load balancing. The novelty of the research phase is the initiator with Least Common Multiple Routing (LCM) that enables the data packets to be distributed based on the node specification generated by the Initiator. By this, the routing time is enhanced and secure forwarding of data occurs.
- Fuzzy logic is implemented to verify the perspective in terms of authentication.
- The proposed scheme enables multipath through this traffic and network delay degrades.
- In this scheme, the efficiency of the system is improved with reduced time, with the aid of Least Common Multiple Routing (LCMR).

1.2 Paper Organization

The paper is organized as follows: A literature survey is given in section II. The proposed methodology is explained in section III. Section IV presents the results and discussions and the comparative analysis with state-of-art methods. The conclusion is given in section V.

2 Literature Survey

Increase the power of the battery in MANET to provide higher efficiency in the transmission of packets. This is ensured by the use of the AODV protocol to enhance the routing strategy in a packet transfer. This makes the power consumption in MANET become an integral factor in ensuring stable contact without power loss. But this approach does not have a proper accuracy [7]. To safeguard data from attackers, a fuzzy-based secure multicast routing strategy is developed to achieve more security among mobile nodes [8]. The fuzzy decision mechanism decides the authentication of nodes, i.e., normal or abnormal nodes. Sign encryption and key generation concepts are deployed

in a multicast zone to improve authentication. The FTBSMIAM (Fuzzy Trust-Based secure multicast routing for improving authentication in MANET) establishes clustering comprising cluster heads. The FTBCGKM (Fibonacci Time Based Cluster Group Key Management) has been evaluated for various ECGKM (Energy-aware Clustering-based Group Key Management) based on several parameters, along with delay, delivery ratio, and drop [9]. As the viability of FTBCGKM is accessed, node capture intruders will be penetrated. The computation analysis reveals that FTBCGKM does not outperform the existing ECGKM [10,11]. An enhanced ABC (Artificial Bee Colony) method that was augmented with the use of a 2-Opt local search, applied to small, medium, or large symmetric and asymmetrical networks. The network paths are chosen based on the loyalty benefits [12–14]. The routing protocol is of OLSR (Optimized Link State Routing). On-demand, pathways are enabled for this OSLR protocol. Relevant load specifications and distributions with the identification of any anomalies in functionality. MANET was successfully implemented in the load balancing routing protocol.

NDM (N-Decision Making)-based MANET congestion management system, specifically integrated for improving NDM-based MANET energy efficiency [15]. As a suggestion for further research, they have suggested two approaches for previous NDN-based MANET congestion management studies to address energy efficiency issues, congestion detection for NDN-based MANET [16,17]. A route may lose its connection quality after a number of transmissions. The energy consumption of the proposed routing protocol is very low compared with earlier energy-aware routing protocols [18]. An effective FL-EPDDA is a packet-dropping detection approach based on fuzzy logic that uses MANET's Fuzzy Inference System (FIS) to handle the issues of MANET malicious nodes. FL-EPDDA is far more experienced than attackers and has obtained negative outcomes [19]. The AODV routing protocol used to protect against wormhole attacks (DAWA) utilizes a fuzzy logic conceptual model or even an artificial immune system [20]. The SFLC (Security aware Fuzzy Logic Connection) methodology is used to safeguard the network. The SFLC model is validated in the MANET, which uses a random deployment in the $100 * 100$ m region [21]. An effective safe route analysis algorithm for real-time is provided. A single route has been chosen to carry out data forwarding, based on the importance of FMLB (Fibonacci Multipath Load Balancing).

To analyze the hidden traffic patterns in MANETs, the concept of a relative traffic relation matrix was adopted [22]. The simulation results suggest that the local traffic link matrix method is better for managing network congestion in MANETs [23]. In the fuzzy-based clustering approach, the server produces the distributed keys using RSA to ensure safe storage allocation. KNN is employed as a pathfinder for efficient storage allocation that ensures efficient load balancing between available clusters. This approach can be used to have a fair time to wash different fabrics. The layout of the fluffy reasoning controller, which has three contributions to the correct wash time of the clothes washer. The procedure entirely depends on the contribution of flourishing members and wastage of time.

3 Proposed Methodology

The network system in which MANET manages and distributes nodes in assemblage, utilizing load-balanced algorithm such as LCMR, permits LCM numbers to be sent to every node based upon this computation. The intermediate node should send relevant data to the destination node, after the transition process. Fuzzy logic ensures that data is sent in the correct direction with the node's processed lcm values. The RREQ message from the source to the destination by intermediate node is prepared to receive the ACK of the data concerned. If it receives then the logical value is set to 1. If not, repeat the process. Then, output Node rate estimation is verified by the lowest end-to-end delay point as shown in Fig. 1. Upon acquiring the RREP upgrade, the source node often describes the route, and

the time required for a forward hop on this route by a packet from source to destination. The source node may maintain for potential paths to set limits. RREQ sequence number, RREQ generation time set of intermediate nodes navigated are shown in Fig. 2. The destination node delegates RREP to a source node whenever the RREQ packet is acquired.

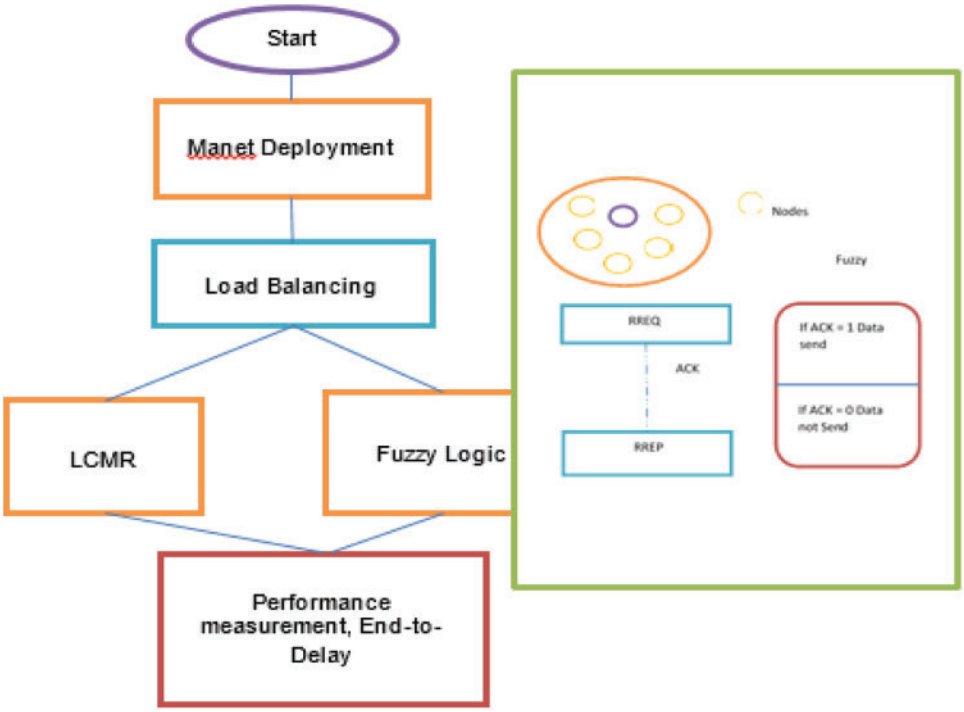

Figure 1: Flowchart of the proposed least common multiple routing (LCMR) scheme

3.1 Load Balancing

Forwarding responses to only one server online greatly enhances performance and reliability. Interfaces optimize application quality by reducing the effort on nodes involved with managing and sustaining network sessions, such as completing certain tasks. Rt(ni) and Rc(ni) are the transfer and carry sensing limits, respectively. When ni V and 1I N, if ni is in NJ's transmission range and nj is within ni's transmission range, the edge eij E.

3.1.1 Least Common Multiple

Identification of route time across each of the directions is required. The number of data packets forwarded through each such path is inversely proportional to the time they are redirected along that path. This routing technique keeps the load balanced along all routes to ensure that the total routing time is balanced.

3.1.2 Multipath

In order to guarantee consistent network operation, load balancing is the major characteristic which a routing protocol must possess. In every condition, a deviation throughout the path due to

such a sensor failure, i.e., a structural failure or a lack of energy, doesn't cause a transmission problem between the source and the destination.

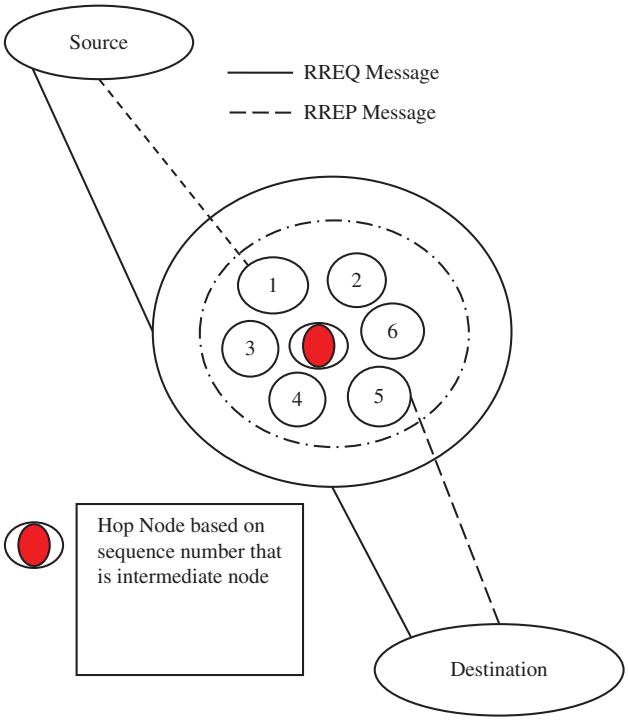

Figure 2: Architecture of the proposed

3.1.3 Definition

Path Lij denotes a sequence of edges from a source node ni to a destination node nj, and Lij includes all successive links on ni to nj. If there are M paths from node ni to nj, then the multipath can be represented as Lij = {Lmij, $1 \leq m \leq M$}.

3.2 Least Common Multiple Routing

Across such different destinations, the data packets are indeed spread from the other source to the endpoint in such a way that the number of data packets distributed through each path becomes inversely proportional to the forwarding time along the entire route. To compute the least common routing time multiple (L) in specific source-destination pair connections and calculate the distribution of packets sent to a route Splitting L perhaps enhances the routing time. Such a phase usually between a source S and destination D node pairs is being used to counteract the Ad hoc network's complex and complicated existence. X = (n1, n2, ... xn) finite positive integers, n > 1. The mechanism worked in the following steps: for each transition m, it searches and restores the pattern X(m) = (n1 (m), n2 (m), ... Nm (m)), X (1) = X. An evaluation designed to select the fewest elements from the X(m) sequence. If the retrieved element is XK0(m), the X(m+1) sequence is specified by Eqs. (1) and (2).

$$x_k^{(m+1)} = x_k^{(m)}, \quad k \neq K_0 \tag{1}$$

$$x_{k0}^{(m+1)} = x_{k0}^{(m)} + x_{k0} \tag{2}$$

The smallest parameters are augmented with succeeding x, while a mass of the components move unrecognized from X(m) to X(m+1). with a positive integer and L $\neq$ s·x1 $\leq$ x2(m) $\leq$ ... $\leq$ xn(m) = Mm $\leq$ L. Now, (s+l) x1 L suggests that Mm+1 L is not possible due to the maximality of m. Hence

$$r \cdot x_1 \ < \ L \ < \ (s+1) \cdot x_1. \tag{3}$$

But this contradicts in above Eq. (3) the fact that L is a multiple of x_1. Hence the assumption that m^z is not the false one, then the last step as proceeds:

$$X^{(m)} = (M^m, \ M^m, \ldots, \ M^{(m)}) \tag{4}$$

But then M^m is a common multiple of all the x_i, i = 1, 2, ..., n, as shown in above Eq. (4) and L $\geq M^m$, at that. However, since L is the least common multiple, L $\leq M^m$. Hence

$$L = M^m \tag{5}$$

The Least Common Multiple Routing (LCMR) that enables a node to set up a path for the transmission of data packets within the network, for this the main set up is the initiator. This process sends a data packetto the source, which permits a series based on the nearest among the source nodes that verifies the authentication. Through this series, a common value is chosen. This process continues till it reaches the destination. When the series defines an LCM value the data load is also allotted in the specified path is to be defined. After this specification of Authentication and time is enhanced, then the Fuzzy validates the load balancing with the help of the inference rules allowing the regulation of the Least Common Multiple Routing (LCMR), as the verification is similar to the LCMR Protocol. For example, let the source-sink out like three paths P_1, P_2, and P_3 possess routing times of 30, 20, and 10 units, etc. Assume the LCMs as 30, 20, and 10; each number is also separated by path value, so 60 dividing the 10 equals 6; meanwhile, the other two pathways are 2 and 3, respectively. Furthermore, with every 2 + 3 + 6 = 11 data packet, they send. Two data packets along these route, three data packets forward into P_2, and six data packets at P_3, thus generating 60 units of time to those pathways. A total of k plausible pathways P_1, P_2, P_k, are investigated., and that routing time is scheduled as T_1, T_2, ... T_k, respectively. Let L = T_1, T_2, · · · · and LCM (Least Common Multiple) T_k,. Assume that either the data transmission along routes P_1, P_2, P_3. P_4.P_5 and P_6. As a result, packets on other routes will be redistributed 251 as in the ratio of 1:1:2:3:4, accordingly. Each intermediate node securing a path disclosure packet estimates its present overall outstanding task at hand while adding the width of the movement between this node and its neighboring hubs.

Balancing ensures optimal delivery of data by raising the overhead tests during data transmission. Its preference for the path may impact on the speed limit. Unless the direction has the minimum speed limit, it will be chosen as the path. The regulating node inside the hub to be stated in Tab. 1, where the data flow way and data flow route improves the exactness dependent on the least LCM Values of each hub and afterward, the deactivate node way.

Table 1: Specifies parameters in the load

Parameters	Use
$DF_P + DF_R$	Data flow path and data flow request (least LCM)
Delivery count	Data pass through the nodes (hop count)
DN_P	deactivate node path

3.2.1 Algorithm of Find Route Source Node

Input: DA
Output: RREQ, Data packets
if SA = its own id then
/∗ Path initialization ∗/
Initialize a real time clock T to 0;
Broadcast RREQ message with its SA and DA;
while (T < T_max) do // is
the time-out period
Hop selection
if RREP message received then
Collect the RREP messages and create
a path list with P_i and T_i
T = T + 1;
if Path list is created then
Calculate L from all T_i ;
/∗ Data Transmission ∗/
while all data packets are not sent do
Send Data packet and wait for δT time; // according to ratio of n_i values
if ACK received within δT time then
Send next Data packet;
else
Resend Data packet;

Let n_i = LT_i, pervasive, 1 I prevalent k, and $n = P_K\ i = 1\ ni$. They attempt to schedule n_i data across the P_i path, through n subsequent packets of data. In many words, data packets are sent 32 along paths $P_1, P_2, \cdots, P_k$ throughout the ratio of $n_1 : n_2 : \cdots : N_k$ Then max $(n_i T_i) = L$ determines the total routing time for n data packets across these k routes. Instead, every hop node involves separating packets to transmit and establishing the Initiator, Cluster Head or Hop node, as well as cluster centers.

3.2.2 Algorithm of Find Route Intermediate Node

Input: Routing messages received
Output: Routing messages transmitted
if both SA and DA not equal to its own id then if RREQ received then
Send RREQ message

3.2.3 Algorithm of Find Route Destination Node

Input: RREQ, Data packet

Output: RREP, ACK, NACK

if DA = its own id then

/∗ Path initialization ∗/

if RREQ received then

Send RREP message from which RREQ

received;

3.3 Fuzzy Logic

Fuzzy logic is a much-coveted line of logic. Binary ranges include two-valued, true, or false logic. This was generalized to accommodate partial truth, in which the significance of truth may vary from one true to the next to another. It is capable of exploiting, missing confirmation, blurry, reflecting, and interpreting information.

- Fuzzy all input values into fuzzy membership fn.
- Execute all valid set rules in the rule base to compute the fuzzy output fn.
- De-fuzzily the fuzzy output functions to get "crisp" output values.

3.3.1 Fuzzy Logic Algorithms

If S message D received then

Source A from neighbor list Compute the network topology

If source (p) = T (traffic) then,

Reset parent (A<=Received) Reset Data

Broadcast FUZZY LOGIC message Enter neighbor discovery phase

End if

End if

If CSPR message AP received then If source (p) = D (destination) then

Reset parent (p <= Received) Packet received

Broadcast FUZZY-SET logic Enter Route discovery

Else If P = loss then

Broadcast FUZZY-Operator logic

End if

End if End if

If P not equal loss, then

Broadcast set Defuzzification Logic

End if

3.3.2 Fuzzy Logic Rules

On rendering the crisp input into fuzzy input, the collection of the rule base and index is created. The fuzzy feedback from the defuzzification unit is finally, through fuzzy rule-based sets used to predict an output associated with the input variables. The most important principles of inference and the scheme of fuzzy rules are mentioned in Tab. 2.

Table 2: Fuzzy rules scheme

Rules			
0(IF ACK not receives)	False	0	0
1(IF ACK receives)	True	0	1
If any CH values based on LCMR	True	1	0
If any LCMR with CH Not with path	False	1	1

The sender sends a packet to the destination, if any Ack receives based on the FIS, it will be set to 1.

If it is not received then it will be set to 0.

Various steps involved in the fuzzy logic routing

1. The data packet is forwarded from source node to the destination node through the network topology.
2. The neighbor node list is gathered from the source node and transmits data through the access point (AP) to the destination intermediately.
3. APs perform together until the cycle of sending and receiving data is undertaken within the network. At this access point the traffic conditions are to be tested.
4. It will be assigned to an AP at that level, and if there is any traffic on that network path, it will use alternate shortest way path to send data. For instance, conditional shortest path navigation is used in the network.
5. If a packet loss arises, a fuzzy operator is executed. Instead, the defuzzification method is carried out. Once information gets sent from source to destination. It assigns a R_{out}. Suppose i-th path among s number of selected paths, carry $pckt\_prt_i$ and each packet takes $delay_i$ unit time to reach destination where $1 \leq i \leq s$. Therefore, the ideal condition to finish almost the same time as follows:

$$Pckt_{Delvi} = PCKTR + PCKTP = PCKTI = PCKTS;\ 1 < i \tag{6}$$

4 Experimental Results

There are many metrics they can use for the performance comparison of proposed routing protocols with the existing routing protocols, The Least Common Multiple Routing (LCMR) routing protocol is implemented in Matlab Simulation with the help of Initiator and the lcm values. First, the initiator enables the node specification from the source to the destination. Then, based on the nearest security parameter, Least Common Multiple (LCM) Values are calculated as well as the node range for data transmission, the value generated, along with the initiator node specification. Network setup are obtained using MATLAB 2016 installed in Intel core i5 processor.

4.1 Packet Delivery Ratio

It is the ratio between the total packets are received at the destination node to the total data packet sent by the source node, when a network has to reach a destination and it has no active route as shown in Fig. 3, as it broadcasts a new path. The route runs out after a defined duration. Our proposed scheme receives 50% under higher traffic load at 7 packets/Sec.

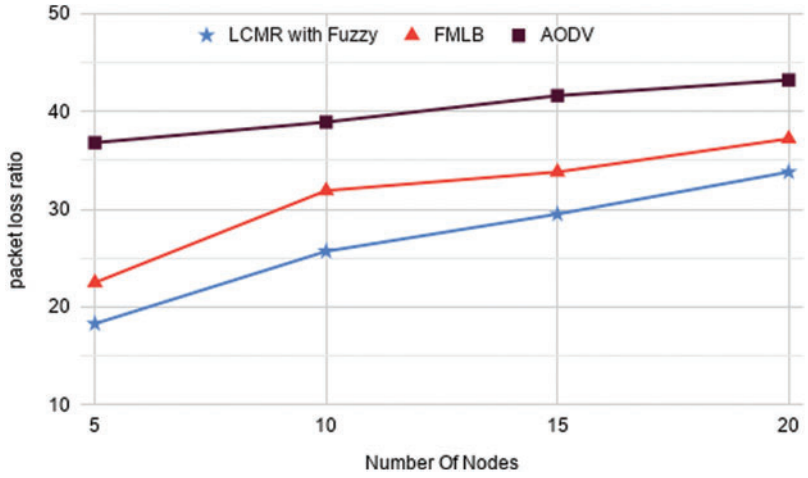

Figure 3: Packet loss

4.2 Routing Time

Fig. 4 demonstrates that the forwarding load is set to the amount of route packets transmitted to receivers of the network to attach for establishment. It seems to be time to interact with information about a path assisted by cluster head address, including network delay, hop count, and path cost, load, maximum transmission, reliability, and transmission range to the hop count of nodes as an intermediator.

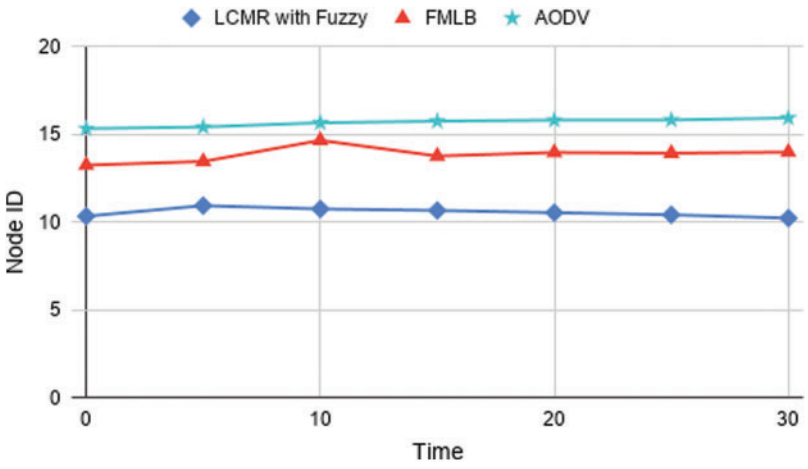

Figure 4: Routing time of the node within time

4.3 Delay Variation in Node

Hop-count is below the routing l cm hop-count; therefore, the consequent node updates the route entry and sends an RREP or retransmission of its packet based on the delay rate to the intermediate nodes to check the route as shown in Fig. 5.

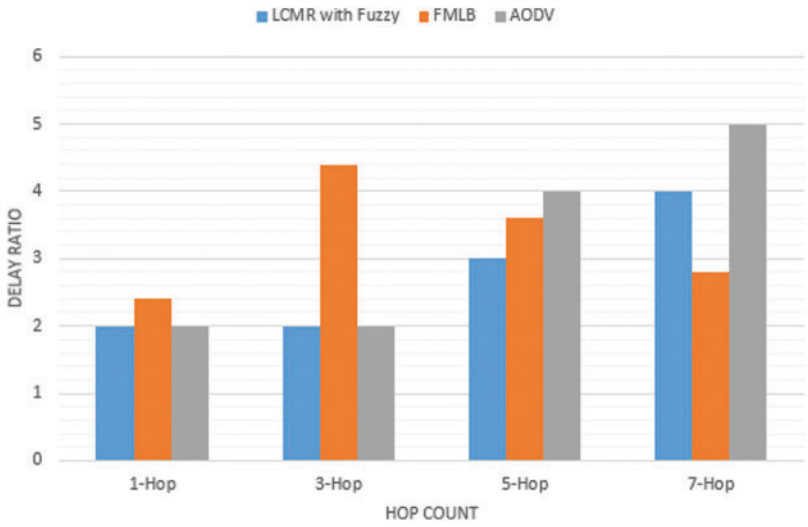

Figure 5: Delay variation in node

However, it is due to the fact that, as its network load increases, the number of data packets arriving at the node's midway often increases due to network blocking where hop count specifies (no of nodes).

4.4 Load Balancing Comparison

Least common multiple routing (LCMR) load balancing has multiple routing packets supplied per destination, Each data packet, as compared to existing protocols as shown in Fig. 6, suggests choosing routes that are relatively short, but created by nodes that are the farthest possible.

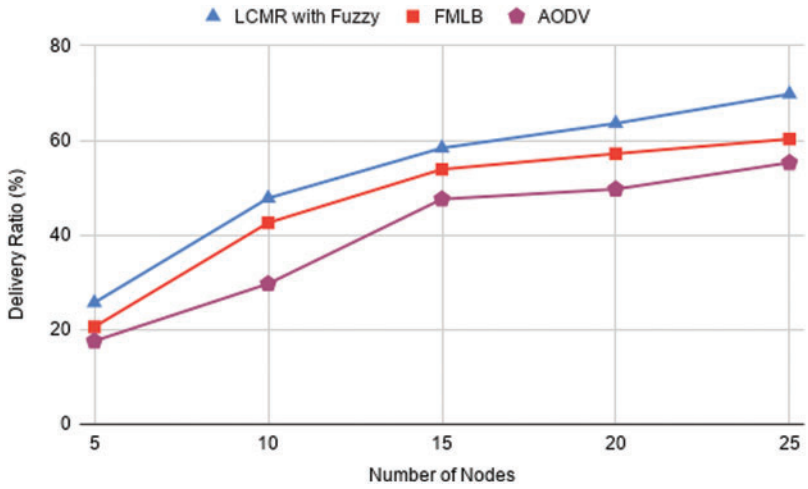

Figure 6: Comparison of load balancing techniques

4.5 Fuzzy Membership Function

The Rule consequent denotes the rules specifications of Rrep, Rreq, Ack, Send, Receive, Data packet, Node number, and Hop, Rule weight denotes the learning of a several parameter values of each membership function as shown in Fig. 7. Rule Connection denotes the value mapped as 0 or 1, the data to be sent is verified right as 1.

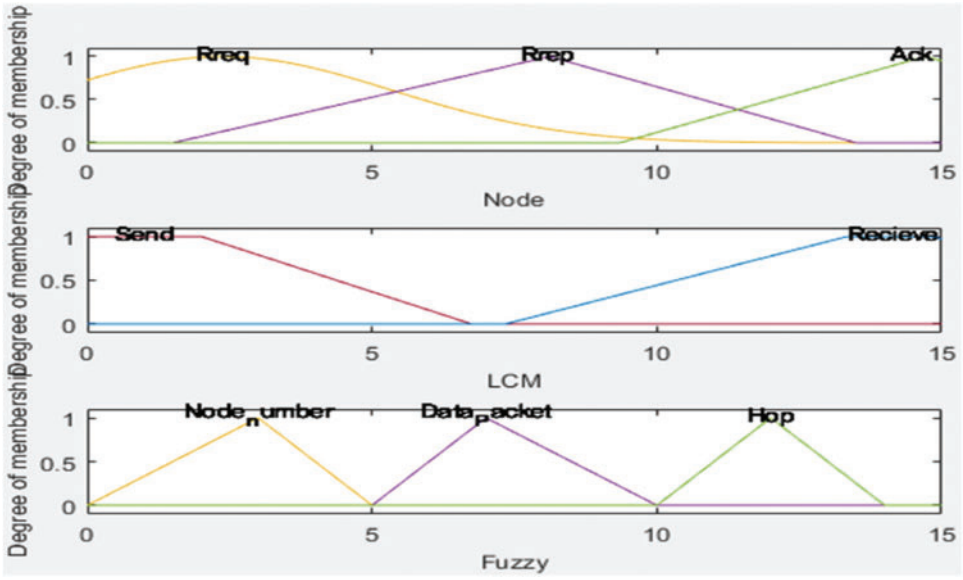

Figure 7: Membership function of fuzzy logic

4.6 Surface Membership Functions

Fig. 8 specifies that the fuzzy rules set assigned, each membership functions denotes elements in fuzzy that are discrete or continuous, where each element of X is mapped to a value between 0 and 1.

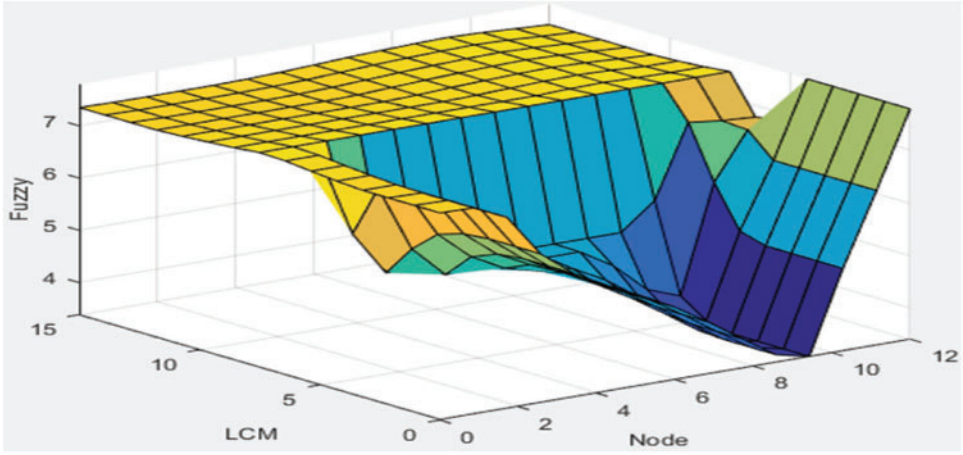

Figure 8: Surface viewer of the membership functions

4.7 Comparison Between the Proposed and Existing

The design and implementation of dual destination points throughout this process requires finding multiple paths between the nodes disrupted by the failure of the link, but also finding the path between the upstream node as well as the receiver at each time of failure with the time. The load to be balanced with avoidance of complexity as shown in Fig. 9.

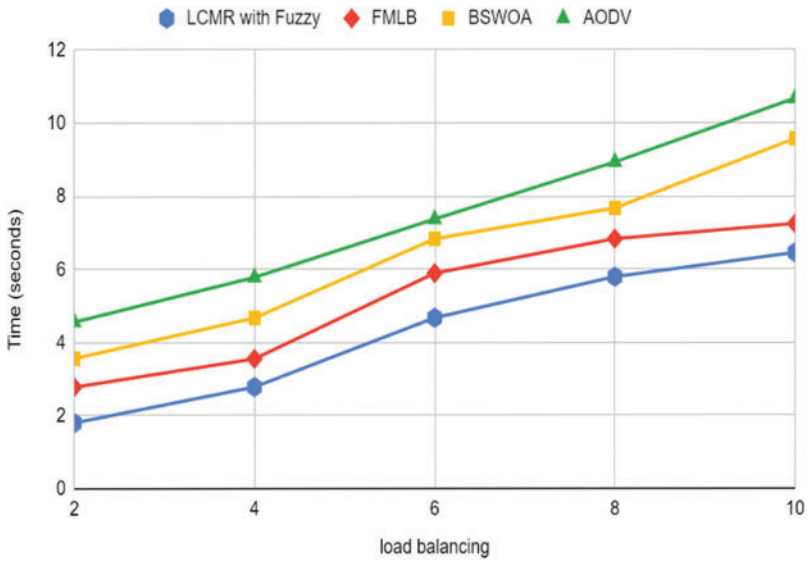

Figure 9: Comparison between the proposed least common multiple routing (LCMR) and existing approaches

Tab. 3 specifies the values of the proposed along with the existing system, the total time required to transfer packet to its destination on random networks multipaths, respectively and the complexity of the routing time variance.

Table 3: Comparative analysis

Load balancing	Least common multiple routing (LCMR) with fuzzy	FMLB	BSWOA	AODV
2	1.8	2.78	3.56	4.56
4	2.78	3.55	4.67	5.78
6	4.67	5.89	6.83	7.37
8	5.79	6.83	7.67	8.93

5 Conclusion

Routing time and traffic on the multipath between the source and destination and the best cost estimation are major problems. In this paper, Least Common Multiple Routing (LCMR) is proposed for multipath routes that will find the source to destination through the nodes, calculate the routing time on each path from source to destination and also find several possible routes. The routing time

throughout distinct paths is adequately employed for estimating the amount of data. Fuzzy logic that interprets the data packets over different routes ensures the packets originated from source to sink are authenticated with binary sets. The simulation results show 86.8% of overall performance, improvement in the end-to-end delay, packet delivery ratio, reducing the routing time, and avoiding traffic in the multipath between sources and destinations.

Acknowledgement: The authors would like to thank Anna University and also we like to thank Anonymous reviewers for their so-called insights.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] D. Bisen and S. Sharma, "Fuzzy based detection of malicious activity for security assessment of MANET," *National Academy Science Letters*, vol. 41, no. 1, pp. 23–28, 2017.

[2] M. A. Gawas, K. Modi, P. Hurkat and L. J. Gudino, "QoS based multipath routing in MANET: A cross layer approach," in *Proc. ICCSP*, IEEE, Chennai, India, pp. 1806–1812, 2017.

[3] J. Shahram and R. Fotohi, "DAWA: Defending against wormhole attack in MANETs by using fuzzy logic and artificial immune system," *The Journal of Supercomputing*, vol. 73, no. 12, pp. 5173–5196, 2017.

[4] D. Bisen and S. Sharma, "An energy-efficient routing approach for performance enhancement of MANET through adaptive neuro-fuzzy inference system," *International Journal of Fuzzy Systems*, vol. 20, pp. 2693–2708, 2018.

[5] N. C. Krishna and S. Varadarajan, "Traffic aware congestion control priority based efficient adaptive multipath routing in wired networks with new queuing technique," *Wireless Personal Communications*, vol. 103, no. 4, pp. 3209–3220, 2018.

[6] H. Rajadurai and U. D. Gandhi, "Fuzzy based collaborative verification system for sybil attack detection in MANET," *Wireless Personal Communications*, vol. 110, no. 4, pp. 2179–2193, 2020.

[7] V. Brindha, T. Karthikeyan and P. Manimegalai, "Fuzzy enhanced secure multicast routing for improving authentication in MANET," *Cluster Computing*, vol. 22, pp. 9615–9623, 2018.

[8] G. Krishnasamy, "An energy-aware fuzzy trust based clustering with group key management in MANET multicasting," in *Proc. ICTCS*, IEEE, Amman, Jordan, pp. 557–571, 2019.

[9] R. B. Logesh and P. Balasubramanian, "Fuzzy rule selection using hybrid artificial bee colony with 2-opt algorithm for MANET," *Mobile Networks and Applications*, vol. 6, pp. 1–11, 2019.

[10] M. Rajashanthi and K. Valarmathi, "A secure trusted multipath routing and optimal fuzzy logic for enhancing QoS in MANETs," *Wireless Personal Communications*, vol. 112, no. 1, pp. 1–16, 2019.

[11] N. Veeraiah and B. T. Krishna, "Trust-aware fuzzy clus-fuzzy NB: Intrusion detection scheme based on fuzzy clustering and Bayesian rule," *Wireless Networks*, vol. 25, no. 7, pp. 4021–4035, 2019.

[12] C. Chaitanya, N. Krishna and S. Varadarajan, "Load distribution using multipath-routing in wired packet networks: A comparative study," *Perspectives in Science*, vol. 8, pp. 234–236, 2016.

[13] M. V. T. Lokare, M. P. M. Jadhav and M. B. K. Ugale, "QoS based routing using the fuzzy TOPSIS MCDM method to enhance the performance of the MANET," in *Proc. I2CT*, IEEE, Bombay, India, pp. 342–347, 2019.

[14] F. Muchtar, A. H. Abdullah, M. A. Adhaileh and K. Z. Zamli, "Energy conservation strategies in named data networking based MANET using congestion control: A review," *Journal of Network and Computer Applications*, vol. 3, pp. 102511(1–18), 2019.

[15] P. Madhavan, "Framework for QOS optimization in MANET using GA-ACO techniques," in *Proc. ICACCS*, IEEE, Coimbatore, India, pp. 44–49, 2019.

[16] S. Singh, I. Sharma, P. Saurabh and R. Prasad, "Fuzzy logic based packet dropping detection approach for mobile Ad-Hoc wireless network," in *Soft Computing for Problem Solving*, Springer, Singapore, vol. 1057, pp. 263–273, 2020.
[17] N. Veeraiah and B. T. Krishna, "An approach for optimal-secure multi-path routing and intrusion detection in MANET," *Evolutionary Intelligence*, vol. 2, pp. 44–50, 2020.
[18] S. Murugan and M. Jeyakarthic, "An energy-efficient security aware clustering approach using fuzzy logic for mobile adhoc networks," in *Proc. ICCMC*, IEEE, Erode, India, pp. 221–229, 2020.
[19] P. Sathyaraj and D. R. Devi, "Designing the routing protocol with secured IoT devices and QoS over MANET using trust-based performance evaluation method," *Journal of Ambient Intelligence and Humanized Computing*, vol. 6, pp. 1–9, 2020.
[20] D. Krishnamoorthy, P. Vaiyapuri, A. Ayyanar, Y. Harold Robinson, R. Kumar *et al.,* "An effective congestion control scheme for MANET with relative traffic link matrix routing," *Arabian Journal for Science and Engineering*, vol. 12, no. 8, pp. 6171–6181, 2020.
[21] M. Sivaram, M. Kaliappan, S. J. Shobana, M. V. Prakash, V. Porkodi *et al.,* "Secure storage allocation scheme using fuzzy based heuristic algorithm for cloud," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, pp. 1–9, 2021.
[22] A. H. Mohammed, M. M. Hamdi, S. A. Rashid and A. M. Shantaf, "An optimum design of square microstrip patch antenna based on fuzzy logic rules," in *Proc. HORA*, Ankara, Turkey, pp. 221–228, 2020.
[23] N. Fareena and S. S. Kumari, "A distributed fuzzy multicast routing protocol (DFMCRP) for maximizing the network lifetime in mobile ad-hoc networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, pp. 4967–4978, 2020.