An Optimized Energy Efficient Route Selection Algorithm for Mobile Ad hoc Networks based on LOA

P. Ramesh, Dr. M. Devapriya

Abstract: ***Due to the advancement of technology and the increased utilization of mobile sensors, Mobile Ad hoc Networks (MANET) has attracted the research attention of numerous researchers. Irrespective of the numerous advantages shown by MANET, there are several challenges confronted by it due to its mobility, unstable topology, energy efficiency and so on. Out of all the challenges, energy efficiency is the most crucial challenges being faced by MANET. The main reason for increased energy consumption of sensors in MANET is the mobility. Taking this challenge into account, this work intends to present an energy efficient routing solution for MANET that is based on the concept of trust and lion optimization algorithm. The lion optimization is a bio-inspired algorithm that helps in detecting the best possible route for the data transmission. The performance of the proposed approach is evaluated and compared against the existing approaches in terms of packet delivery rate, latency analysis, energy consumption and network lifetime.***

Keywords: MANET, energy efficiency, routing, lifetime enhancement.

I. INTRODUCTION

A Mobile Ad hoc Network (MANET) is a network with self-governing wireless sensor nodes [1, 2]. MANET requires no special infrastructure as the network is completely dynamic. The self-governance and the infrastructure-less characteristics are both the boon and curse of MANET. On the positive side, the self-governing sensor nodes overthrows the requirement of central governing authority, as in classic networks and the infrastructure-less nature supports in deploying the nodes without any special arrangements. On the flip side, numerous challenges are confronted by MANET, owing to its mobility and dynamic nature. The mobile nature of MANET makes the process of routing tougher and consumes more energy.

Hence, the energy of the sensor nodes must be utilized effectively to have a reasonable lifetime of the sensors. The greater the lifetime of the sensors, the better is the purpose fulfilment of the network. Though MANET is based on Wireless Sensor Networks (WSN), The routing protocols developed for WSN are unsuitable for MANET. The main reason for unsuitability is the dynamic nature of network topology and the dynamic mobility pattern of the sensor nodes [3,4]. The mobile nature of MANET is advantageous for several real time applications yet, the reliability of the network may get reduced.

Reliability is one of the most important performance metrics and it is mainly affected by the routing techniques employed by the network. For instance, the packets from the source node have to reach the destination node without any hassles. However in case of MANET, there are chances in which the forwarded packets fail to reach the destination due to different reasons such as mobility, congestion and so on. Hence, the reliability of the network can be enhanced, when the packet delivery rate with minimal latency is better. Better packet delivery rate can be achieved with the help of an efficient routing algorithm.

Basically, the routing protocols of MANET belong to one of three categories such as proactive, reactive and hybrid. The sensor nodes in proactive routing protocols maintain a routing table, which contains the existing routes between the source and destination. On the other hand, the reactive routing protocols attempt to establish routes whenever it is necessary and no routing table is maintained. The hybrid routing protocols are the combination of proactive and reactive routing protocols.

Recognizing the importance of routing policy, this work intends to present an energy efficient routing policy based on trust parameters and meta-heuristic algorithm. The standard Ad hoc On-demand Distance Vector (AODV) protocol is improvised with the help of Lion Optimization Algorithm (LOA). The AODV protocol is a popular reactive protocol for MANET, however it suffers from two critical issues and they are congestion, latency and packet loss. All these issues occur due to the route selection policy involved in AODV routing protocol. The proposed routing protocol attempts to route the packet by selecting the optimal route with the help of LOA. The work contributions are listed as follows.

- The proposed routing algorithm increases the reliability by selecting the optimal path from the source and destination.

Revised Version Manuscript Received on 22 December , 2018.
P. Ramesh, Asst.Professor, Department of Computer Science, Government Arts College, Udumalpet, Tirupur, Tamilnadu, India
Dr. M. Devapriya, PG and Research Department of Computer Science, Government Arts College (Autonomous), Coimbatore, Tamilnadu India.

- The choice of optimal path is done by computing the trust parameters such as residual energy, packet delivery rate and queue length of the node.
- The proposed routing algorithm encounters minimal packet loss and latency.
- The energy efficiency of the proposed approach is observed to be satisfactory.

The rest of this article is organized as follows. Section 2 discusses about the related review of literature with respect to routing and the proposed routing algorithm is elaborated in section 3. The performance of the proposed routing algorithm is evaluated in section 4. Section 5 concludes the article with possible future research directions.

II. REVIEW OF LITERATURE

This section reviews the related state-of-the-art literature with respect to routing algorithms in MANET.

In [5], a partially distributed dynamic model for secure and reliable routing approach is presented for MANET. This work utilizes a partially distributed model on all sensor nodes and the misbehaviour of the node is considered as additional information. This misbehaviour based information is circulated among the nodes, while forming the routes. This work makes decision in a dynamic fashion by considering the level of node's misbehaviour.

A novel opportunistic routing protocol is proposed in [6]. This work enhances the energy efficiency of routing protocols by employing candidate selection and coordination phases. This work is claimed to perform better than BATMAN routing protocol, when dealing with multimedia data. In [7], a dynamic connectivity factor based routing protocol that relies on neighbourhood nodes is presented for MANET. The protocol is named as neighbour based Dynamic Connectivity Factor routing Protocol (DCFP), which probes the status of the network by considering the network connectivity. The performance of the work is compared against AODV and proven to be better in terms of energy efficiency and packet delivery rate.

A self-adaptive proactive routing scheme is presented for MANET in [8]. This work includes a special indicator to check the mobility of nodes, such that the current status of the network can be assessed. The routing metric is switched between the expected transmission count or mobility factor, which increases the routing performance. This work claims to attain better packet delivery rates.

In [9], a smooth mobility and link reliability based optimized link state routing scheme is introduced for MANET. This work is based on markov smooth and complexity restricted mobility model, which aims to increase the reliability by selecting multi-point relay. This work claims that it can attain better lifetime with minimal control overhead. A dynamic cloudlet based energy saving routing mechanism is proposed for MANET in [10]. This work forms a temporary file that consists of node's identity and route information for a specific period of time. The cloudlets are the small data centres and by utilizing these cloudlets the mobile devices establish routes.

A security framework for MANET is introduced in [11], which is named as Security Using Pre-Existing Routing (SUPERMAN). This protocol focuses on secure routing by enabling the network and the routing protocols to carry out the functionality and the security mechanisms such as node authentication and access control. In [12], an ant based multipath backbone routing scheme with load balancing is presented for MANET. In this work, when a source node requires transmitting data, multiple routes are selected with the help of swarm based ant colony optimization technique by considering the maximum path preference probability. The path preference probability is computed by the availability of hops, delay and bandwidth. The load of the network is balanced with the help of backbone node for equal traffic distribution.

A multi-objective optimization model meant for presenting a secure routing scheme is proposed in [13]. This work presents a hybrid optimization algorithm based on M-lionwhale algorithm that incorporates both the lion and whale optimization algorithm by considering different quality of service parameters such as energy, distance, delay and so on. In [14], a new routing approach on the basis of fuzzy petri nets and ant system is presented for MANET. This work computes the minimal investment with reasonable capacities for routing traffic. The routing model is computed by the fuzzy synchronized petrinet and the routing decision is made with the help of synchronized fuzzy transition approach.

In [15], an attack pattern discovery based trusted routing scheme with pattern discovery is presented for MANET. This work analyses the sensitivity analysis of the routing scheme by varying the parameters with three different packet dropping attacks. An ACO look-ahead based approach is proposed for fault-tolerant routing in [16]. This work surveys different fault tolerant protocols and the ant colony based routing techniques for MANET. Additionally, a fault tolerant look-ahead routing algorithm that can detect suitable route and route pairs is presented. This technique helps in choosing the alternative path easily.

An evolutionary self-cooperative trust scheme is provided to withstand the routing disruptions in MANETs in [17]. The evolutionary self-cooperative trust mimics the cognitive process of humans and the trust information of nodes is taken into account to deal with different attacks. The trust information collected from the sensor nodes are interchanged between them and are analysed with the help of cognitive judgement.

In [18], a secure routing model is proposed on the basis of game theory model for MANET. This work analyses the profile of normal and malicious nodes with the help of dynamic Bayesian signalling game and the best actions of every node is notified. The Perfect Bayesian Equilibrium (PBE) offers the solution to signal games and the players are given pay-off. This work minimizes the malicious nodes and the cooperation of nodes is stated to be improved by means of reputation system. A constructive relay based cooperative technique is proposed for MANET in [19].

This work utilizes topological information being stored in the Cooperative table and relay table. This work manages itself by establishing relays to forward data. The routes are selected by considering the energy harvesting and link break probability.

Motivated by the above works, this work intends to present an energy efficient routing algorithm for MANET, which considers the trust parameters to select optimal routes. The proposed approach is elaborated in the following section.

III. PROPOSED ENERGY EFFICIENT ROUTING ALGORITHM FOR MANET

This section elaborates the proposed energy efficient routing algorithm for MANET based on trust parameters. The work overview is presented in the following subsection.

A. Work Overview

The objectives of this article are to present a routing algorithm for MANET that can establish optimal routes while conserving energy. The major challenges faced by MANET are mobility pattern and indefinite topology. This nature of MANET makes the process of routing tougher, as the mobility pattern of nodes cannot be predicted. Additionally, more energy is consumed for achieving routing, which reduces the network lifespan.

These issues can be addressed by an effective routing protocol, which can route the data without any hassles. This work presents a routing algorithm that forms the optimal routes between the source and destination nodes by considering the trust parameters. The optimal route from multiple routes is chosen by the LOA. The goal of this work is attained by three important phases which are route establishment phase, trust metrics computation and optimal route selection. The route establishment phase is based on standard AODV routing protocol, which detects multiple paths leading from the source and the destination nodes. The trust metrics are computed for all the nodes being present along every single route. Finally, the LOA is applied to choose the most optimal route out of all the possible routes. The following sub-sections elaborate all the phases involved in the proposed approach.

B. Route Establishment Phase

When the source node intends to transmit data to the destination node, then the source node broadcasts the route request (RREQ) message to all the neighbourhood nodes. The RREQ message is responded by the route reply (RREP) message by the neighbourhood nodes to the source node. This means that several routes from the source nodes leading to the destination node are returned. All these processes involved in route establishment are similar to the processes in AODV. Once the possible routes are established from the source to destination node, the trust metrics of the nodes involved in routes are computed as follows.

C. Trust Metric Computation Phase

The trust metrics utilized to determine the nature of nodes are energy backup, packet delivery rate and queue length of the node. The energy backup is one of the first and foremost requirements of any sensor node, as it is the life of sensor nodes. It is obvious that the sensor node with reasonable energy can render better service. The lesser the energy, the minimal is the lifetime of the sensor. Hence, when a route is occupied by nodes with minimal energy, the route may cut-off at any period of time. This may lead to packet loss or congestion. Hence, the energy is considered as one of the trust metrics.

Secondly, packet delivery rate is considered as another trust metric, which measures the rate of incoming and outgoing packets. When the count of incoming messages matches with the outgoing messages, then the node is considered to be reliable. When the route contains more of such nodes, then the route is reliable with better message delivery rates. Finally, the message queue length of a particular node is taken into account. The greater the queue length, the more is the wait time. This results in increased latency and degrades the performance of the routing algorithm. Additionally, lengthy message queues may cause congestion also. Considering these points, this work considers energy backup, packet delivery rate and message queue length of the nodes present in a specific route. The nodes with reasonable levels of trust metrics are trustworthy.

This work considers the above stated metrics instead of just considering shortest path alone. When the shortest path available is chosen for routing a message, the nodes involved in the route may not be trustworthy and this may lead to congestion and unnecessary latency. Hence, this work chooses the trust metrics to choose a reliable route which can make energy efficiency possible. The following part of the article presents the trust metric representation as follows.

The residual energy of the sensor node ranges from 0 to 1. The sensor nodes with full energy are denoted with the value 1 and nil energy are represented 0. The values between 0 and 1 represent the energy level of the node, which may be half, quarter and so on. The energy value assignment is presented in table 1. Similarly, the packet delivery rate is computed by taking the incoming and outgoing messages of the node. When a node forwards all the incoming messages, then the node is completely trustworthy. However, when the count of outgoing messages is half the incoming messages, then the nodes are considered as malicious or selfish. Such nodes are unsuitable for achieving reliable routing and hence, these routes are not chosen even when the route is the shortest among all routes. Table 2 presents the packet delivery rate value assignment of the nodes.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Table 1: Energy Value Assignment

Energy Table	
Energy value	**Node type**
0	Nodes with nil energy
0.5	Half energy
0.75	Three-fourth energy
1	Full energy

Table 2: Packet delivery rate Value Assignment

Packet delivery rate Table	
Value	**Node type**
0	$\emptyset = 0$
0.5	$\emptyset = \tau/2$
0.75	$\emptyset = 4\tau/3$
1	$\emptyset = \tau$

In table 2, $\emptyset$ is the outgoing packet and τ is the incoming packet. Based on these computations, the values are assigned to the node. When the sensor node forwards all the messages and none of the messages, then the node is assigned with value 1 and 0 respectively. The values between 0 and 1 indicate the message forwarding intention of the nodes. Hence, the nodes with greater packet forwarding ability are needed to be chosen for better reliability. Finally, the message queue length of the node is considered. The message queue length is computed by dividing the total count of messages in queue by the total number of nodes in the route, as represented by the following equation.

$$QL = \frac{M_c}{TN_R} \qquad (1)$$

In the above equation, M_c is the total count of messages in queue and TN_R is the total count of nodes along a route. By this way, the QL is computed and normalized by the following equation.

$$N = \frac{(QL - o_l) \times (n_h - n_l)}{o_h - o_l} \qquad (2)$$

In the above equation, o_l and o_h are the least and the highest values of the value. In this case, the least and the highest values are set to 0 to 3. The values of n_h *and* n_l denote the upper and the lower limits of the normalized value, which is 0 to 1. By this way, the values of all the trust metrics are computed and added together. The algorithm for route detection and trust metric computation is as follows.

Route detection and trust metric computation algorithm

Input : Sensor nodes
Output : Route detection and trust metric computation
Begin
For each source node
Broadcast RREQ to neighbourhood nodes;
Receive RREP from nodes;
Detect all possible routes from source to destination;
End for
For all routes returned
Do
Compute T_c by eqn.4 for all nodes involved in routes;
Save T_c;
End do
End for;
End;

$$T_c = \sum_{i=1}^{N} \frac{E + PDR + QL}{3} \qquad (3)$$

Hence, the trust metrics of nodes are computed by eqn.3. E, PDR, QL stands for energy, packet delivery rate and queue length. N is the total number of nodes along a route. As soon as the trust metrics of the nodes are computed, the LO algorithm is employed to select the optimal route from the available routes.

D. Optimal Route Selection

The optimal route out of all the possible routes from the source to destination is selected by the LO algorithm. The LO is a bio-inspired algorithm imitates the activities of lions. The lions are societal animals and they live in groups called pride. A pride of lions contain different classes of lions such as resident and nomadic lions [20,21]. Each and every pride consists of about four to five lions along with the cubs and adult lions. Once the young lions turned as adults, the young lions are dislodged from the pride and these lions become nomadic lions.

As the nomadic lions are mostly young, they target the adult lions living in the pride for attack in order to get inside the pride. The LO algorithm generates an initial population of lions that incudes pride and nomadic lions. The ratio of nomadic and resident lions is set in addition to the control region of the pride of lion. The gender ratio is also fixed, as the lionesses pay more attention towards hunting. This bio-inspired algorithm finds optimal solution by arranging the nomadic lions with respect to the fitness value. The lions with greater fitness value are allotted place in the pride and the resident lions with minimal fitness values are discarded. This operation continues till the no best solution can be further attained. The fitness value of the proposed approach is computed by the following equation.

$$F_v = \sum_{i=1}^{N} \frac{(T_{c_1}, T_{c_2}, \ldots, T_{c_N})}{N} \qquad (4)$$

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

The fitness value is computed by equation 4 and the optimal route is selected by means of the LO algorithm. This way of optimal route selection helps in attaining better reliability and energy efficiency. The proposed route selection algorithm based on LO is presented as follows.

Route selection algorithm

Input : Detected routes from source to destination
Output : Optimal route selection
Begin
For each resident lion
Do
Choose a lioness for hunting randomly;
Compute the fitness value of lions by eqn.4;
Sort the fitness value in ascending order;
Eliminate the lions with least F_v*;*
End do;
End for;
For each nomadic lion
Follow the same steps as that of resident lion;
Compute F_v*;*
If (F_v*(nomadic lion)<* F_v *(resident lion))*
Include the lion in pride;
Eliminate the lions with least F_v*;*
Compare the solutions and swap whenever necessary;
Store the best solution;
End if;
End for;
End;

By this way, the optimal route is selected from the available routes and this technique chooses better possible route rather than choosing just the shortest path. When the shortest path is chosen as the route, the quality of nodes available in the shortest route is not assessed. This may introduce unreliability and time delay for data transmission. Hence, instead of choosing the shortest path, it is better to choose the route by examining the nature of nodes along routes. This idea results in reliable and energy efficient routing. The performance of the proposed approach is evaluated in the following section.

IV. RESULTS AND DISCUSSION

The performance of the proposed approach is tested in terms of packet delivery rate, average delay, throughput, energy consumption and lifetime analysis. The results attained by the proposed approach are compared with the existing approaches such as ANT based routing [12], Ant system [14], self-adaptive routing [8]. The proposed algorithm is implemented in NS2 with a node count of 200 and the transmission radius is set as 250 m. The nodes are deployed in the area of $1000 \times 1000\, m^2$. Random waypoint mobility model is employed for simulation. The size of the packet is set as 512 bytes. The performance metrics are discussed in the following section.

A. Packet delivery rate analysis

Packet delivery rate is the most important performance metric of any routing algorithm. The packet delivery rate analyses the count of incoming and outgoing packets. The greater the packet delivery rate, the more reliable is the routing algorithm. The packet delivery rate of the routing algorithm is presented by the following equation.

$$PDR = \frac{Total\ count\ of\ packets\ delivered}{Total\ count\ of\ packets\ forwarded} \times 100 \qquad (5)$$

The packet delivery rate of the proposed approach is analysed and compared in the following graph.

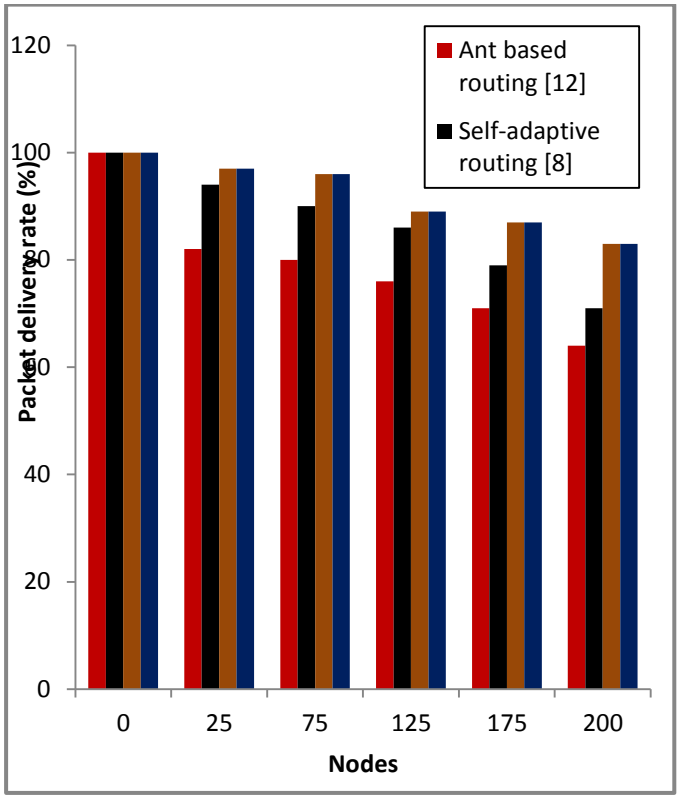

Fig.1. Packet delivery rate analysis

From the experimental results, it is evident that the proposed approach shows reasonable packet delivery rate. The main reason for the better performance of the proposed routing algorithm is the inclusion of significant trust metrics and the choice of optimal routes by LO algorithm. The following section presents the average latency rate of the proposed work.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

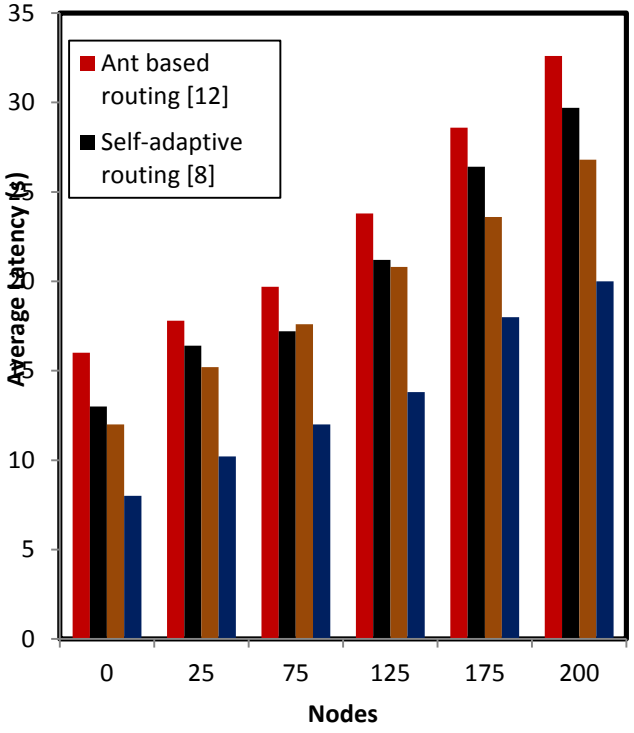

Fig.2. Average latency rate

The average latency rate of the proposed approach is depicted in figure 2. When the latency rate is minimal, the performance of the routing algorithm is better. The latency rate of the proposed routing algorithm is minimal, as the proposed approach selects the optimal route instead of shortest route. The shortest route may contain malicious node, whereas the optimal route is formed with the reliable nodes. The point here is that the best possible route among all the routes is selected to carry out packet forwarding. This idea reduces the latency. The following graph presents the energy consumption analysis of the proposed work

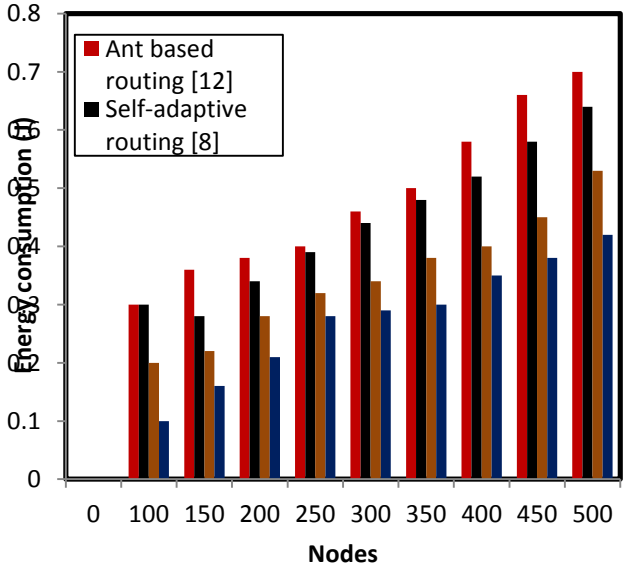

Fig.3. Energy consumption analysis

It is quite obvious that the lifetime of the network is better in case of the proposed routing algorithm. The lifetime of the network is computed by checking the count of alive nodes at a specific period of time. On analysis, it is found that the network with proposed routing algorithm shows more alive nodes with respect to the increasing simulation time, when compared to the existing techniques. Hence, the proposed routing algorithm better performs with respect to standard performance metrics and the following section presents the concluding points of the article. On analysis, it is observed that the energy consumption of the proposed approach is minimal than the comparative approaches. The energy consumption and lifetime of the network are inter-related with each other. When the energy consumption is lesser, the lifetime of the network can be improvised. The energy consumption can be reduced by employing different techniques and this work employs optimal route selection to conserve energy. The lifetime of the network is analysed and the results are presented in the following figure.

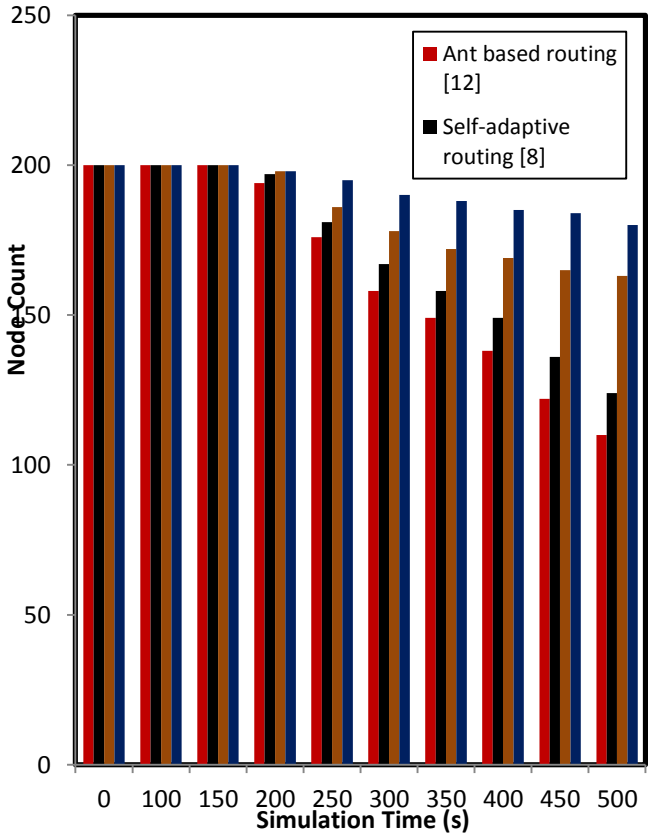

Fig.4. Network lifetime analysis

V. CONCLUSION

This article proposes a routing algorithm for MANET, which is reliable and optimal. The reliability is achieved by incorporating the trust metrics such as residual energy, packet delivery rate and message queue. These measures play a vital role in determining the optimal route for data forwarding. The optimal route out of all possible routes is selected by the LO algorithm, which is a bio-inspired algorithm. The proposed approach conserves reasonable energy, which contributes in increased lifetime of the network. The performance of the proposed work is analysed in terms of packet delivery rate, average latency, energy consumption and network lifetime. The results are then compared with the existing approaches and the proposed approach outperforms the existing routing approaches. In future, this work is planned to be extended to present a secured routing solution.

REFERENCES

1. Charles E. Perkins, Ad Hoc Networking, Addison-Wesley, 2001.
2. C.K. Toh, Ad Hoc Mobile Wireless Networks: Protocols and Systems, Prentice Hall, 2001.
3. R. Bhaskar, J. Herranz, and F. Laguillaumie, “Efficient authentication for reactive routing protocols,” in AINA „06: Proceedings of the 20th International Conference on Advanced Information Networking and Applications -Volume 2 (AINA 06). Washington, DC, USA: IEEE Computer Society, 2006, pp. 57–61.
4. M. Dorigo and C. Blum, “Ant colony optimization theory:a survey,” Theor. Comput. Sci., vol. 344, no. 2-3, pp. 243–278, 2005.
5. Anjali Anand ; Himanshu Aggarwal ; Rinkle Rani, "Partially distributed dynamic model for secure and reliable routing in mobile ad hoc networks", Journal of Communications and Networks, Vol.18, No.6, pp.938-947, 2016.
6. Ramon Sanchez-Iborra ; Maria-Dolores Cano, "JOKER: A Novel Opportunistic Routing Protocol", IEEE Journal on Selected Areas in Communications, Vol.34, No.5, pp.1690-1703, 2016.
7. Ali Mohamed E. Ejmaa ; Shamala Subramaniam ; Zuriati Ahmad Zukarnain ; Zurina Mohd Hanapi, "Neighbor-Based Dynamic Connectivity Factor Routing Protocol for Mobile Ad Hoc Network", IEEE Access, Vol.4, pp.8053-8064, 2016.
8. Tran The Son ; Hoa Le Minh ; Graham Sexton ; Nauman Aslam, "Self-adaptive proactive routing scheme for mobile ad-hoc networks", IET Networks, Vol.4, No.2, pp. 128-136, 2015.
9. Zhinan Li ; Yinfeng Wu, "Smooth Mobility and Link Reliability-Based Optimized Link State Routing Scheme for MANETs", IEEE Communications Letters, Vol.21, No.7, pp. 1529-1532, 2017.
10. Jirui Li ; Xiaoyong Li ; Yunquan Gao ; Yali Gao ; Rui Zhang, "Dynamic Cloudlet-Assisted Energy-Saving Routing Mechanism for Mobile Ad Hoc Networks", IEEE Access, Vol.5, pp.20908-20920, 2017.
11. Darren Hurley-Smith ; Jodie Wetherall ; Andrew Adekunle, "SUPERMAN: Security Using Pre-Existing Routing for Mobile Ad hoc Networks", IEEE Transactions on Mobile Computing, Vol.16, No.10, pp.2927-2940, 2017.
12. Pitchaimuthu Francis Antony Selvi ; Moola Seetharamaiyer Kasiviswanathan Manikandan, "Ant based multipath backbone routing for load balancing in MANET", IET Communications, Vol.11, No.1, pp. 136-141, 2016.
13. Ram Mohan Chintalapalli ; Venugopal Reddy Ananthula, "M-LionWhale: multi-objective optimisation model for secure routing in mobile ad-hoc network", IET Communications, Vol.12, No.12, pp.1406-1415, 2018.
14. Ibrahim Kacem ; Belkacem Sait ; Saad Mekhilef ; Nassereddine Sabeur, "A New Routing Approach for Mobile Ad Hoc Systems Based on Fuzzy Petri Nets and Ant System", IEEE Access, Vol.6, pp.65705-65720, 2018.
15. Rutvij H. Jhaveri ; Narendra M. Patel ; Yubin Zhong ; Arun Kumar Sangaiah, "Sensitivity Analysis of an Attack-Pattern Discovery Based Trusted Routing Scheme for Mobile Ad-Hoc Networks in Industrial IoT", IEEE Access, Vol.6, pp.20085-20103, 2018.
16. S. Surendran ; S. Prakash, "An ACO look-ahead approach to QOS enabled fault- tolerant routing in MANETs", China Communications, Vol.12, No.8, pp.93-110, 2015.
17. Ruo Jun Cai ; Xue Jun Li ; Peter Han Joo 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.
18. Balasubramanian Paramasivan ; Maria Johan Viju Prakash ; Madasamy Kaliappan, "Development of a secure routing protocol using game theory model in mobile ad hoc networks", Journal of Communications and Networks, Vol.17, No.1, pp.75-83, 2015.
19. Jingwen Bai ; Yan Sun ; Chris Phillips ; Yue Cao, "Toward Constructive Relay-Based Cooperative Routing in MANETs", IEEE Systems Journal, Vol.12, No.2, pp.1743-1754, 2018.
20. Mccomb, K, et al. Female lions can identify potentially infanticidal males from their roars. Proc. R. Soc. Lond. Ser B: Biol. Sci. 1993;252 (1333)59–64.
21. Schaller GB. The Serengeti lion: a study of predator–prey relations. Wildlife behavior and ecology series. Chicago, Illinois, USA: University of Chicago Press; 1972.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication