Received: May 26, 2019

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Energy Preserving Secured Route Selection Algorithm Based on Hybrid Metaheuristic Algorithms for MANET

Kokila Subramanian Surampatti[1]* **Brindha Devi Cinniyampalayam Lakshmanan[2]**

[1]Research and Development Centre, Bharathiar University, Coimbatore-46, India
[2]Department of Computer Science, Queen Mary's college, Chennai-04, India
* Corresponding author's Email: kokilaresearchbu@gmail.com

Abstract: MANET is severely energy constrained, due to the capricious mobility rate and the deployed hostile environment. The most energy consuming activity of mobile sensors is the process of routing. Hence, the energy efficient routing is an evergreen research topic for MANET. Additionally, the energy efficient routing algorithm must be as lightweight as possible to conserve the energy. Considering these points, this work aims to present an energy efficient, trustworthy route selection algorithm based on trust index. The trust index is formed by considering the trust metrics such as energy backup, packet forwarding rate and node loyalty. The trust index is considered as the fitness value for the route selection algorithm. The route selection algorithm is based on the metaheuristic algorithms such as Artificial Bee Colony (ABC) and Whale Optimization (WO) algorithms. The performance of the proposed work is analysed in terms of packet delivery rate, average loyalty, energy efficiency and network lifetime. The proposed work shows better performance than the comparative approaches with increased energy efficiency and thereby network lifetime.

Keywords: Energy efficiency, Route selection, Metaheuristic algorithms, Trust index.

1. Introduction

A Mobile Ad hoc NETwork (MANET) is a network with numerous movable nodes, which is based on the concept of Wireless Sensor Networks (WSN). In MANET, the mobile nodes are movable with no restrictions on the degree of mobility. Additionally, the MANET is completely free from the concept of Base Station (BS) and the mobile sensor nodes perform the functionality of the normal sensor node and router as well. The major activities performed by the sensor nodes are sensing, processing and transmission. Sensing is the most important task of the mobile sensors and it is the base for several real-time applications. The data transmission is the second important activity performed by the mobile sensors, in which the gathered information is forwarded to the neighbourhood nodes as such or with minimal processing [1,2].

The data transmission is the most crucial activity of the MANET, as the purpose of any application is satisfied by this data exchange. However, the major challenges encountered by the MANET are the mobility and energy efficiency. The mobility pattern of the mobile sensors can vary from each other and need not be static. Additionally, it is obvious that the wireless sensors are severely constrained to energy and hence, balanced energy utilization is the wise idea to prolong the lifetime of the sensor and in turn the network itself.

Though MANET is based on Wireless Sensor Networks (WSN), the routing algorithms meant for WSN cannot serve well for MANET, as a result of the infrastructure-less nature and the dynamic mobility pattern of the mobile sensors [3]. Yet, these reasons are advantageous that makes the quicker establishment of MANET possible. On the flip side, these points make the networks susceptible to security threats. As mentioned, the mobile sensors involve in three significant operations, which are sensing, data transmission and local processing of data. Among all these basic activities of sensors, data transmission consumes more energy, however it is the most vital action of the network. Hence, there is a constant demand for secure, energy efficient routing algorithm for MANET.

The routing protocols can be classified into two brad categories and they are proactive and reactive protocols. The proactive routing protocols attempt to maintain all the possible routes from a corresponding node to all the other nodes throughout the lifetime of the network. This consumes more memory space and suffers from computational complexity as well. As the proactive protocols attempt to maintain all the routes, continuous tracking of nodes irrespective of the varying mobility degree is quintessential, but it is quite difficult to manage, achieve and may involve inefficiency (in certain cases due to poor tracking) also. On the other hand, reactive routing protocols need not to manage any routing information unless it is demanded by the node. Thus, the reactive routing protocols are free from routing information management and periodic modification. However, reactive routing protocols suffer from time complexity [4].

Energy efficiency is the primary requirement of any routing algorithm meant for MANET, as the energy depletion paves way for poor connectivity between the sensor nodes. This in turn degrades the performance of the network. Understanding the current need, this article intends to present a trustworthy, energy efficient and secure routing algorithm for MANET by clubbing the metaheuristic algorithms. This work considers the trust parameters of every sensor node such as energy backup, packet forwarding rate and loyalty. The routes are detected and the most optimal route is selected by clubbing the metaheuristic algorithms such as Artificial Bee Colony (ABC) and Whale Optimization (WO) algorithm. This idea helps in choosing the best possible route for every data transmission and ensures security, energy efficiency. Some of the work contributions are listed below.

- Energy efficiency is the most crucial issue being faced by the mobile sensor network, as the sensor nodes are movable with varying speed. Considering this fact, this work presents an energy efficient route selection algorithm.
- This article presents an energy efficient and secure routing policy for MANET by incorporating the hybrid metaheuristic ABC and WO algorithms.
- The fitness values of the metaheuristic algorithms are computed by the trust metrics of the sensor nodes. This idea helps in detecting the best possible route from the source to the destination node.
- The proposed approach proves better Packet Delivery Rate (PDR), average latency, throughput, energy efficiency, network lifetime, which are discussed in the results section.

The remainder of this article is organized as follows. Section 2 discusses the related literature with respect to routing meant for MANET. The proposed routing algorithm is elaborated in section 3 and section 4 evaluates the performance of the proposed approach. Finally, the article is concluded by section 5.

2. Review of literature

This section reviews the recent existing literature related to the routing algorithms for MANET.

In [5], a new routing approach based on fuzzy petrinet and ant system is proposed for MANET. This work employs fuzzy synchronized petrinets for modelling the routing framework. The ant system is utilized for detecting the solutions for uncertainty problems. The performance of the work is tested in terms of packet delivery rate, throughput and end-to-end delay. However, this work suffers from computational overhead.

A multi-criteria based hybrid multipath routing protocol is proposed for MANET in [6]. This work computes multicriteria node rank metric by aggregating several parameters that are associated with energy and Quality of Service (QoS) for reducing the control overhead. Based on the computed metric, the multipoint relay nodes are selected by considering the energy and QoS metric. This work focuses on control overhead that results in memory overhead.

In [7], the Ant Colony Optimization (ACO) algorithm based routing protocols meant for MANET are discussed. This work states that the swarm intelligence based algorithms provide better solutions with robustness, flexibility and efficiency. An energy efficient multipath routing protocol is proposed for MANET in [8]. This work optimizes the energy consumption model by employing Ad hoc On Demand Multipath Distance Vector (AOMDV) routing protocol. This work proposes a fitness function and applied it over AOMDV. The experimental results of this work show that the fitness function based AOMDV performs better than the standard AOMDV protocol. This work gives an idea that metaheuristic algorithms perform better with the help of fitness functions.

In [9], a Smooth Mobility and Link Reliability (SMLR) based optimized link state routing scheme is proposed for MANET. This work proposes a novel Optimized Link State Routing (OLSR) scheme by exploiting semi-markov smooth and complexity restricted mobility model. The reliability of the work is tackled by the multi-point relay selection technique. Yet, this work involves complex mechanisms and the energy efficiency can still be enhanced.

A dynamic cloudlet assisted energy saving routing mechanism is proposed for MANET in [10]. This work forms a temporary file to keep the identity and route information of nodes for a specific period of time. The cloudlets are the small data centers and the relation table is formed. With these elements, the mobile sensors detect routes and perform data transmission. The incorporation of temporary files introduces issues such as temporary file management and updations. Additionally, memory overhead is also observed.

In [11], an ACO look-ahead approach is proposed to achieve a QoS aware fault tolerant routing in MANET. This work studies and reviews the fault tolerant protocols in addition to ACO algorithms for MANET. The proposed look-ahead routing algorithm attempts to detect the valid route and the route pairs are look-ahead for selecting the alternate path. This work consumes more time for route selection.

A partially distributed dynamic model to achieve secure and reliable routing for MANET is proposed in [12]. This work employs a partially distributed dynamic model on all the sensor nodes to improve the security of the network. The misbehaviours of the sensor nodes are passed as additional information to other sensor nodes in the network. Hence, the decision making process of the work is dynamic as the route is chosen by considering the misbehaviour of the nodes. Though this work shows better security, the time consumption and computational complexity are improved.

In [13], a neighbour based Dynamic Connectivity Factor based routing Protocol (DCFP) is proposed for MANET. This protocol forwards the status of the network on its own and no central management is required. This work claims itself with reduced routing overhead but, the efficiency of the work is based on the trustworthiness of the neighbourhood nodes. A secure routing protocol is developed for MANET in [14] by employing game theory model. This work analyses the profile of all the sensor nodes for distinguishing between the normal and malicious nodes with the help of dynamic Bayesian signalling game. The incomplete information of the problem is tackled by uniting the strategies and the players are payed off with the help of Perfect Bayesian Equilibrium (PBE). This work shows computational complexity.

A self-adaptive proactive routing scheme for MANET is proposed in [15]. This work is based on the mobility indicator, which is utilized for detecting whether the network is static or mobile. The routing metric is fixed on the basis of Expected Transmission Count (ETX) or the Mobility Factor (MF). The performance of this approach is analysed by varying the mobility states of the sensor nodes. The energy efficiency of the work can still be improved. An evolutionary self-cooperative trust scheme is presented against route disruptions for MANET in [16]. This work is based on human cognitive process and based on the trust information, which is exchanged between nodes. This work is claimed to be resilient to internal attacks also. However, this work suffers from memory overhead.

In [17], a MANET routing scheme is proposed by Diagnosing the Anomalies with Provenance and Verification (DAPV). The DAPV detects the single and collaborative malicious nodes in case of both direct and indirect attacks. Initially, the provenance tracking is carried out and the log information of the peers is collected. The privacy preservation is verified with the help of Merkle hash tree. This work maintains so much supplementary data, such that it suffers from memory overhead.

In [18], an energy efficient and security based model for OLSR routing protocol is proposed for MANET. This work makes use of Enhanced Intellects-Masses Optimizer (EIMO) and considers two different factors such as willingness nodes and Composite Eligibility Index (CEI). Finally, this work concludes that the energy consumption is quite minimal when compared to the existing approaches, however at the cost of reliability.

Motivated by the recent related literature, this paper aims to present an energy efficient, secure and trustworthy routing algorithm for MANET, while considering the crucial challenges such as energy restriction, security threats and network lifetime. The following section elaborates the proposed routing algorithm for MANET.

3. Proposed energy efficient, secure and trustworthy routing (EESTR) algorithm

The main objective of the paper is to ensure energy efficiency while providing trustworthy route

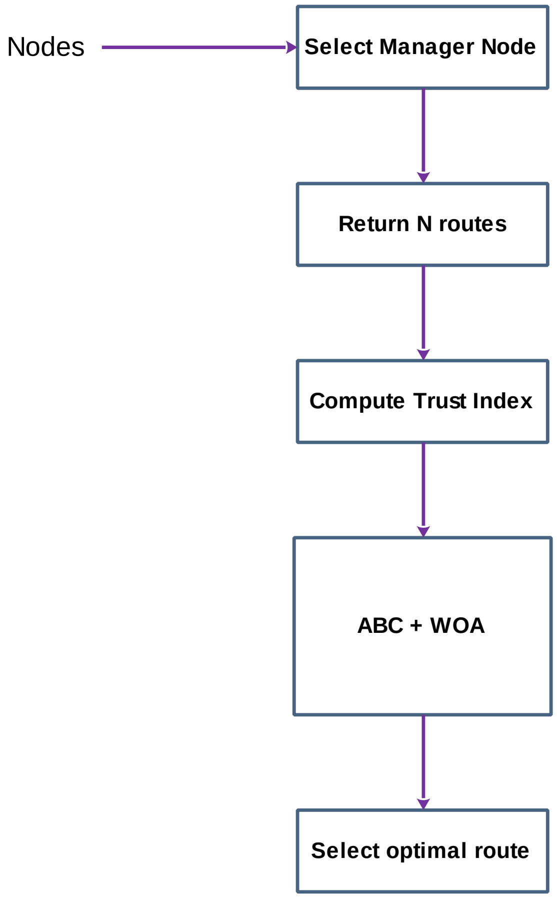

Figure.1 Overall flow of the proposed algorithm

between the source and destination. MANET is highly susceptible to security threats due to the varying degree of mobility and the absence of central managing authority. However due to the numerous advantages of MANET, several real-time applications employ MANET and hence, security is given utmost importance which is par equivalent to the energy efficiency. Understanding this scenario, the proposed routing algorithm focuses both on energy efficiency and security. The overall flow of the work is depicted in Fig. 1.

This work is based on the idea that the energy efficiency can be achieved by utilizing the available power source effectively, such that the lifetime of the network is enhanced. On the other hand, security can be ensured by figuring out the trustworthy route, which can be framed by considering the trustworthiness of the nodes being present in the route. The proposed routing algorithm works by dividing the work into three phases such as network area segregation, trust index computation, route formation and optimal route selection. This work is carried out on the assumption that all the sensor nodes are aware of the neighbours and their current location. All these phases are described in the forthcoming subsections.

3.1 Network area segregation

As MANET involves mobile sensors with unpredictable motion pattern, inclusion of centralized management authority is impossible. However, the proposed work is based on the trust metrics, which are needed to be computed by a trustworthy node and this scenario is not possible in the case of MANET. Hence, this work segregates the complete network area into several zones and the trust metrics are exchanged among the nodes. For every zone, the node with the greatest trust index is declared as the ‘manager node’ and it supports the fellow nodes in the process of routing for a limited period of time. However as the node is mobile, the functionalities that can be performed by the manager node is limited. Yet this idea is effective, as the manager node helps in managing the process of routing and monitoring the behaviour of the nodes. The following section presents the process of manager node selection.

3.2 Manager node selection

The complete network area is divided into equal areas and encloses the sensor nodes being present in that specific area. In every separate area, the node with maximal energy is considered as the manager node. Initially, all the nodes present in a specific geographical area exchange the unique identifiers and the current energy backup of the node. When the energy is completely loaded in the sensor, then it is indicated by the value 1. On the other hand, a node with completely drained energy is represented by 0.1 or 0 itself. The nodes exchange the message as follows <ID,CUR_ENR> and circulate this message to the neighbourhood nodes.

The nodes compare the received energy of the neighbourhood node with its current energy. When the energy of the neighbourhood node is greater than the energy of the corresponding node, the current node forwards the message of the neighbourhood node to its own neighbourhood node. In case, if the energy of the corresponding node is greater than the energy of the neighbourhood node, then the corresponding node sends its message to the neighbourhood node. This idea saves more energy, as the sensor nodes do not involve in the process of flooding the energy information to all the sensor nodes. The algorithm for manager node selection is as follows.

```
Manager node selection
Input : Sensor nodes;
```

```
Output : Manager node selection
Begin
Divide the network area into several regions;
For each region
  For every node
    Do
      Send <ID,CUR_ENR> to the neighbourhood node (N1);
      Neighbourhood node checks the message;
      If (CUR_ENR (C1) < CUR_ENR (N1))
        Transmit CUR_ENR (N1) to the neighbourhood node of C1;
        Else
        Transmit CUR_ENR (C1) to the neighbourhood node of C1;
      End if;
       Declare the node with maximum CUR_ENR as manager node;
   End for;
End for;
If manager node exits the region1
  Declare the node with greatest energy at time T1;
End if;
End;
```

The manager node is selected by the mentioned algorithm and this idea conserves energy while ensuring better manageability. The manager node then computes the trust index for all the fellow nodes. The following section explains the trust metrics and the procedure for trust index computation.

3.3 Trust index computation

The trust index of the node is computed by considering three simple yet powerful trust metrics such as energy backup, packet forwarding rate and loyalty. These trust metrics are simple to compute and can determine the nature of the node effectively. The details of the trust metrics are presented as follows.

3.3.1. Energy backup (EB)

Energy is the main life source of the sensor node and hence, it is one of the most important trust metrics. A node with minimal energy backup cannot perform well in the network and the performance of the network may go down with these kinds of nodes. As mentioned already, a node with full energy backup is denoted by value 1 and nil energy is denoted by 0. Hence, the values meant for energy backup lies between 0 and 1.

3.3.2. Packet forwarding rate (PFR)

The PFR is meant for analysing the nature of the node, by considering the flow of packets. A normal node must forward all the packets that are intended to be forwarded. However in certain cases, the malicious nodes neglect the task of routing and it leads to a serious issue. A node can be considered as trustworthy, when it shows interest in forwarding packets. Hence, it is always preferable to choose a route with multiple trustworthy nodes.

To measure the PDR, the packet inflow and outflow are taken into account. Let the inflow and the outflow are denoted by α and β respectively. The normal node satisfies the following condition.

$$\alpha = \beta \tag{1}$$

Suppose, when the packet outflow of the node is half the packet inflow or a little plus or minus to that indicates that the node doesn't show interest to forward packets. This can be indicated by the following condition.

$$\alpha = \frac{\beta}{2} \tag{2}$$

When the β rate is lower than the half of α, then the node is completely untrustworthy and is not fit to be a part of the network. When the route is chosen by considering these kinds of nodes, then the data routing is made risk free and secure. Hence, PFR is another important trust metric of a node, which can help in increasing the reliability of the route.

3.3.3. Node loyalty (NL)

Node loyalty is another significant trust metric that checks the original behaviour of the node while forwarding data. For instance, a malicious node participates in several meaningless activities just to overhear or to collapse the security of the network. This is achieved by modifying or deleting the packets being forwarded. These behaviours of the nodes are computed by tracking the node's behaviour constantly. A node with value 1 as loyalty is considered to be completely loyal, which does not involve in any unwanted activity. Hence, these three trust metrics are employed to compute the trust index, which is as follows.

$$TI = \frac{EB+PFR+NL}{3} \tag{3}$$

By this way, the trust index is computed and is utilized as the fitness value of the proposed routing algorithm. The route formation and selection phases are presented in the following section.

3.4 Route formation and selection

When a source node intends to transmit packet to the destination node, then the multiple routes are returned, from which the most feasible and trustworthy route needs to be selected. Hence, this work chooses the best available route that ranges from the source and the destination. This work clubs the ABC and WO algorithms for choosing the optimal route. The following section presents a short note on ABC and WO algorithms.

3.4.1. ABC algorithm

ABC is a metaheuristic algorithm, which mimics the original nature of honey bees and the algorithm is discussed in [19]. The three basic components of ABC algorithm are the food source, employed and unemployed bees. The objective of the ABC algorithm is to detect the best food source available in the space.

The food source is considered to be good, when the distance of the food from the bee-hive is minimal, quality of food and so on. The employed bees exchange the important details about the food source such as location, distance between the food source and the bee-hive. The unemployed bees can be categorised into two kinds and they are scout and onlooker bees. The scout bees search the new source of food in the surrounding area of the bee-hive. The onlooker bees stay in the hive and make final decision about the food source with the help of the information fed by the employed bees.

Fundamentally, the ABC algorithm relies on three phases and they are initialization, employed, onlooker and scout bees phase. Each phase is repeated till the greatest count of iterations is reached. Initially, the control parameters are fixed. The employed bees search for new high quality food sources in surrounding area of older food source. The new food source is then assessed for its fitness, and compared with the older food source by applying greedy selection.

The information about the food source is then passed among the onlooker bees in the beehive. Finally, the employed bees change as scout bees, as their solutions could not be improved anymore. In this point, the scout bees again search for new food source and the poor solutions are removed. This process is repeated until the termination condition is reached [20,21].

3.4.2. WO algorithm

WOA is a bio-inspired algorithm that imitates the real nature of whales [22]. Basically, the whales target a school of fish by circling them and bubble formation. The whales hunt the fish in two steps, which are denoted by the terms exploitation and exploration. The exploitation step circles the fish, while the exploration step checks the fish in a random fashion. Based on these concepts, the proposed work clubs these two metaheuristic algorithms for selecting the best optimal route. The proposed algorithm is presented as follows.

Proposed Optimal Route Selection Algorithm

```
Input : Possible routes;
Output : Optimal selection
Begin
Randomly allot the food source population;
For each employed bee
  Do
    Generate new food source;
    Compute the TI by Eq.(3);
   Employ WOA;
  Calculate the food source probability by Eq.(4);
For each onlooker bee
  Choose food source;
  Generate food source and compute TI by Eq.(3);
 Employ WOA;
Compare the results and swap if the recent result is better;
Store the best source and return the result;
End do;
End for;
End;
```

The probability of the food source is computed by the Eq. (4), which is as follows.

$$prob_i = \frac{TI_i}{\sum_{n=1}^{TIs} TI_n} \quad (4)$$

In the above equation, TI_i is the trust index of the i^{th} route and n is the total number of available routes between the source and destination. By this way the TI, which is considered as the fitness value is computed. The fitness values for all the routes are computed, which are based on the trust index. It is obvious that the trust index of the route depends on the trust index of the nodes available in a specific route.

As the trust index is employed as the fitness value, the selected route enjoys the highest fitness

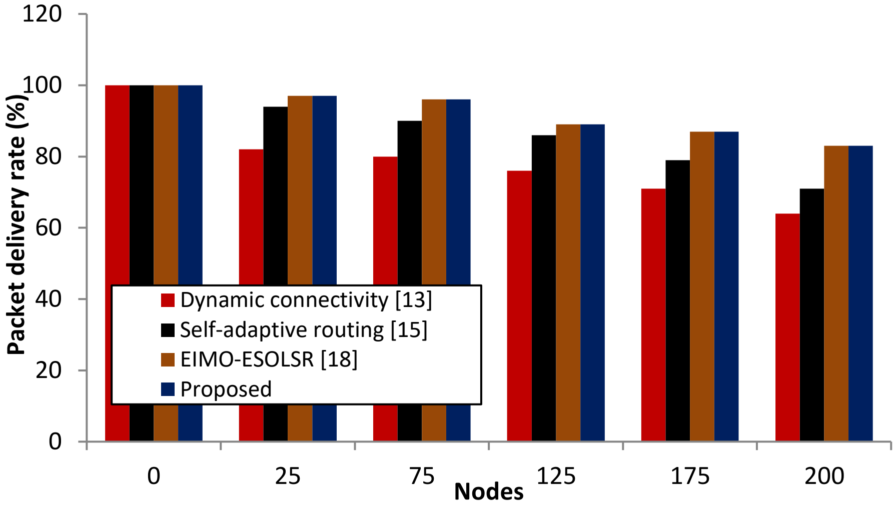

Figure.2 Packet delivery rate analysis

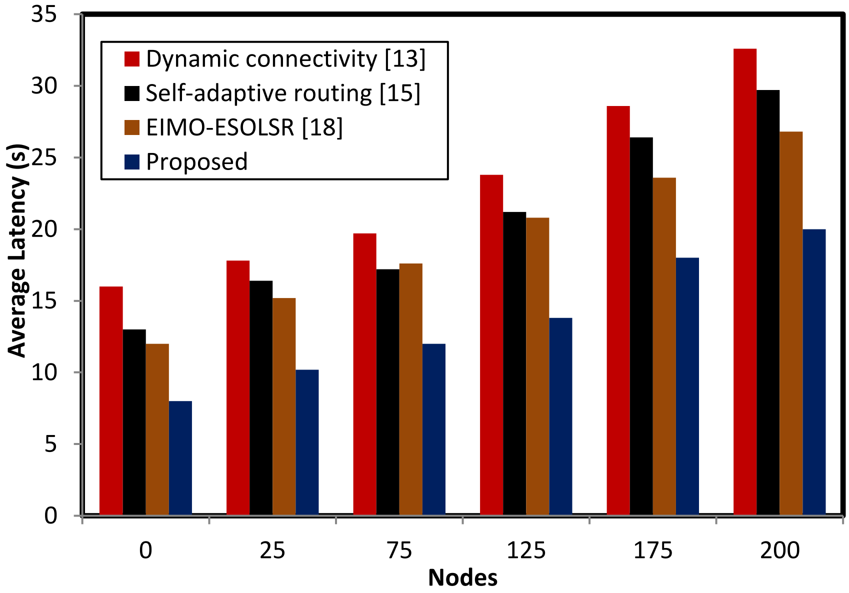

Figure.3 Average latency analysis

value. This makes sense that the most feasible route is chosen as the route for packet transmission. As the route is chosen on the basis of trust index, the route is secure, trustworthy and energy efficient. The following section analyses the performance of the proposed routing algorithm.

4. Result and discussion

The performance of the proposed approach is analysed by setting the network size as $1000 \times 1000\,m^2$. The wireless bandwidth of the proposed work is set as 2 MB/Sec. The transmission range of the mobile node is set to 100 meters. The mobile sensor nodes play the roles of both the node and router. The random waypoint mobility model is utilized to carry out the simulation, which means that a mobile node stays in a specific location for a certain period of time known as ‘pause’. When the pause time gets over, the mobile node initiates the process of choosing the speed. The node moves to reach the destination node at a specific speed and the node is paused again. This work sets the maximum speed of the node as 10m/sec and the node pause time is 20 seconds.

The proposed work is simulated in NS2 and the total number of nodes is set as 200. The performance of the proposed work is analysed in terms of PFR, average latency, throughput, energy efficiency and network lifetime. The experimental results of the proposed work are compared with the existing approaches such as dynamic connectivity [13], self-adaptive routing [15] and EIMO-ESOLSR [18].

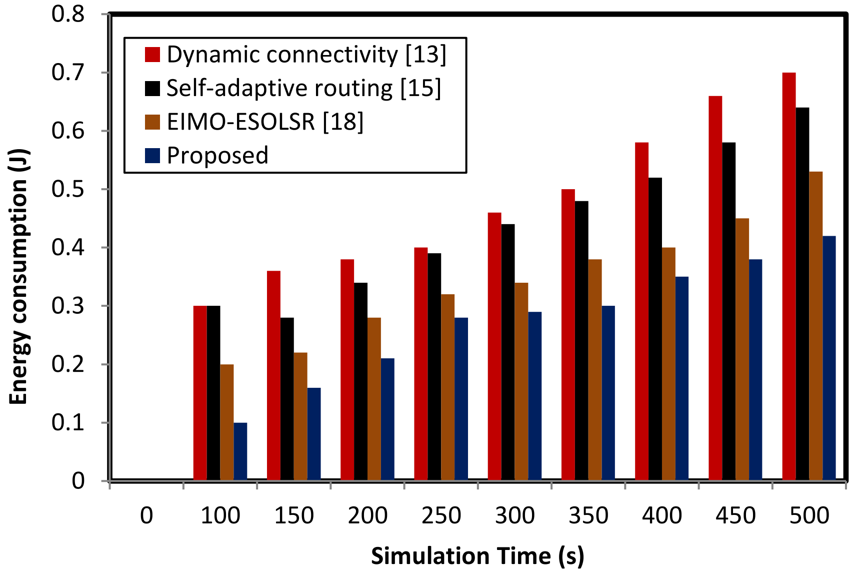

Figure.4 Energy consumption analysis

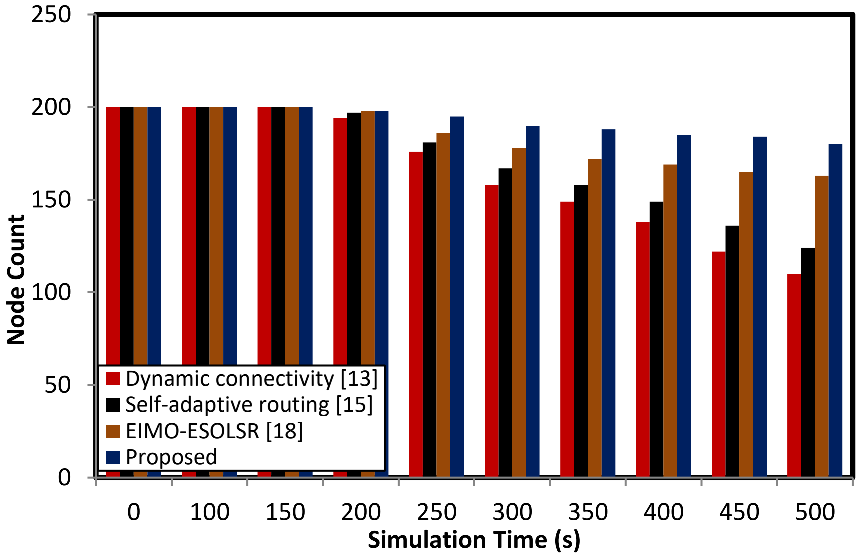

Figure.5 Network lifetime analysis

The packet delivery rate of the proposed approach is presented and the attained results are compared with the existing approaches. The number of nodes is varied and the packet delivery rate of the work is computed. On analysis, it is found that the proposed approach proves better packet delivery rate than the existing approaches. The packet delivery rate starts to diminish, as the count of nodes increases. The main reason for achieving better packet delivery rates is the effective choice of routes. The route is selected by the hybrid of ABC and WO algorithms and is completely based on the trust index. The route selection is performed by considering the trust measures such as packet delivery rate, energy and node's loyalty. The route is selected only when the energy, packet delivery rate and packet loyalty is greater. As the most trustworthy route is selected, the packet delivery rate is increased. The proposed approach shows an initial PDR of 97 percent for 25 nodes and the PDR diminishes to 83 percent for 200 nodes. The second better performer in the analysis is the EIMO-ESOLSR [18], which starts from 94 percent and reduced to 71 percent for 200 nodes.

Fig. 3 shows the average latency of the proposed approach, which is minimal than the comparative approaches. The average latency increases with the increase in nodes. The The proposed work shows the maximal latency with 20 seconds for 200 nodes and the EIMO-SOLSR proves second better performance with 26.8 seconds for 200 nodes. The proposed approach proves this latency, owing to the choice of the trustworthy route that promises the packet delivery on time.

Energy conservation is the major goal of any routing algorithm for MANET, as the mobile nodes are severely energy constrained. The proposed work conserves as much energy as possible by choosing the trustworthy route out of all the possible routes. The computation of trust index is made simpler with three basic yet powerful trust metrics. All these points help in achieving energy efficiency. The energy consumption of the proposed approach is lower than the other existing approaches.

The network lifetime and energy consumption are indirectly proportional to each other. As the energy consumption of the proposed approach is minimal, it is obvious that the proposed work shows better network lifetime than the comparative approaches. The network lifetime of the work is measured with respect to the count of active nodes in a specific simulation time. The proposed work shows the count of 180 nodes at 500th second, whereas the second better performer EIMO-ESOLSR proves itself with 163 nodes. Hence, the objective of the proposed algorithm is met and the following part concludes the paper.

5. Conclusions

This article proposes a trustworthy and secure route selection algorithm for MANET, which is proven to be energy efficient. The goal of this work is attained by employing trust metrics through which the trust index is computed. The process of trust index computation is taken care of by the manager node. The trust index is computed by considering three powerful trust metrics such as energy backup, packet forwarding rate and loyalty. The so computed trust index is treated as the fitness value for the route selection algorithm, which is the combination of ABC and WO algorithms. The performance of the proposed work is better than the comparative approaches in terms of PDR, latency, energy efficiency and network lifetime. In future, this work can be extended by investigating several other bio-inspired algorithms and trust metrics.

References

[1] G.V. Kumar, Y.V. Reddyr, and D.M. Nagendra, "Current research work on routing protocols for MANET: a literature survey", *International Journal on Computer Science and Engineering*, Vol.2, No.3, pp.706-713, 2010.

[2] W.A. Jabbar, M. Ismail, R. Nordin, and S. Arif, "Power-efficient routing schemes for MANETs: a survey and open issues", *Wireless Networks*, Vol.23, No.6, pp. 1917-1952, 2017.

[3] V.B. Reddy, A. Negi, and S.Venkataraman, "A Comparison of Trust in MANETs and WSNs", In: *Proc. of IEEE 6th International Conference on Advanced Computing (IACC),* pp. 577-581, 2016.

[4] Y. Bai, Y.Mai, and N. Wang, "Performance comparison and evaluation of the proactive and reactive routing protocols for MANETs", In: *Proc. of Wireless Telecommunications Symposium (WTS),* pp. 1-5, 2017.

[5] I. Kacem, B. Sait, S. Mekhilef, and N. 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.

[6] W.A. Jabbar, W.K. Saad, and M. Ismail, "MEQSA-OLSRv2: A Multicriteria-Based Hybrid Multipath Protocol for Energy-Efficient and QoS-Aware Data Routing in MANET-WSN Convergence Scenarios of IoT", *IEEE Access*, Vol.6, pp.76546-76572, 2018.

[7] H. Zhang, X. Wang, P. Memarmoshrefi, and D. Hogrefe, "A survey of ant colony optimization based routing protocols for mobile ad hoc networks", *IEEE Access,* Vol.5, pp.24139-24161, 2017.

[8] A. Taha, R. Alsaqour, M. Uddin, M. Abdelhaq, and T. Saba, "Energy efficient multipath routing protocol for mobile ad-hoc network using the fitness function", *IEEE Access*, Vol.5, pp.10369-10381, 2017.

[9] Z. Li and Y. 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] J. Li, X. Li, Y. Gao, Y. Gao, and R. Zhang, "Dynamic cloudlet-assisted energy-saving routing mechanism for mobile ad hoc networks", *IEEE Access*, Vol.5, pp.20908-20920, 2017.

[11] S. Surendran and 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.

[12] A. Anand, H. Aggarwal, and R. 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.

[13] A.M.E. Ejmaa, S. Subramaniam, Z.A. Zukarnain, and Z.M. Hanapi, "Neighbor-based dynamic connectivity factor routing protocol

for mobile ad hoc network", *IEEE Access*, Vol.4, pp.8053-8064, 2016.

[14] B. Paramasivan, M.J.V. Prakash, and M. 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.

[15] H. Le Minh, G. Sexton, and N. Aslam, "Self-adaptive proactive routing scheme for mobile ad-hoc networks", *IET Networks*, Vol.4, No.2, pp.128-136, 2014.

[16] 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.

[17] T. Li, J. Ma, Q. Pei, H. Song, Y. Shen, and C. Sun, "DAPV: Diagnosing Anomalies in MANETs Routing With Provenance and Verification", *IEEE Access*, Vol.7, pp.35302-35316, 2019.

[18] H. Kanagasundaram, and A. Kathirvel, "EIMO-ESOLSR: energy efficient and security-based model for OLSR routing protocol in mobile ad-hoc network", *IET Communications*, Vol.13, No.5, pp. 553-559, 2018.

[19] D. Karaboga and B. Basturk, "On the performance of artificial bee colony (ABC) algorithm", *Applied Soft Computing*, Vol.8, No.1, pp. 687-697, 2008.

[20] D. Karaboga, B. Gorkemli, C. Ozturk, and N. Karaboga, "A comprehensive survey: artificial bee colony (ABC) algorithm and applications", *Artif. Intell. Rev.*, 2012.

[21] D. Karaboga and C. Ozturk, "A novel clustering approach: Artificial Bee Colony (ABC) algorithm", *Applied Soft Computing,* Vol.11, pp. 652–657, 2011.

[22] S. Mirjalili and A. Lewis, "The whale optimization algorithm", *Advances in Engineering Software*, Vol.95, pp.51-67, 2016.