Received: August 22, 2018

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Multi Objective ALO Based Energy Efficient and Secure Routing OLSR Protocol in MANET

Hamela Kanagasundaram[1*] **Kathirvel Ayyaswamy[2]**

[1]*Department of Computer Science, Mother Teresa Women's University, Kodaikanal, Tamil Nadu, India*
[2]*Department of Computer Science and Engineering, MNM Jain Engineering College, Chennai, India*
* Corresponding author's Email: hamela1229@gmail.com

Abstract: The routing protocol design with security and energy efficiency is a challenging task in mobile ad hoc network (MANET). To overcome this challenge, we propose an energy-efficient secured routing protocol. The objective of our work is to provide a secured routing protocol, which is energy efficient. To provide security the proposed technique allows each communicating node to monitor reputation factor, suspicion factor and contingency of threat to compute the degree of its vulnerability. The energy efficiency in optimized link state routing (OLSR) routing protocol is increased by generating new parameters and considering the energy of nodes. Based on the energy efficiency and security parameters the optimal route (multipoint relay) was selected. This approach uses less energy and secured compared to other energy models. The simulation result exhibits that the proposed multi objective Ant Lion Optimizer (MOALO) outperforms other state of art with respect to the performance metrics like energy consumption, Delay, throughput and network lifetime.

Keywords: MANET, Routing protocol, Multipoint relay, Multi objective ALO, Reputation, Suspicion, Delay, Throughput.

1. Introduction

Nowadays, one of the most popular emerging technologies is MANETS. It does not require any fixed infrastructure and rapidly deployed. In networking and interfaces capability the mobile devices consist of the adhoc wireless network are equipped with adaptive nature and are self-organizing [1]. On the fly the formed network can be de-formed and again formed without the help of system administration and is capable of router acting. For routing attacks MANETs are vulnerable, especially attacks launched by compromised or selfish network members and appear to be compliant of protocol [2]. In military communications, virtual classrooms, rescue operations and emergency search MANET are widely used, also hostile environments data acquisition, exhibitions and meetings in battle field and communications set up in conferences, [3, 4].

For secure communication MANETs offer a challenging environment among the participating nodes. All nodes can capture the packets within the signal reception range and random responses are generated. With the network's normal routing process the routing attacks are meant to interfere and thus the performance of protocol routing is degraded. The mobility node results in a changing network topology continuously [5, 6]. The limited resources are used in MANETs for example, the protocol used should not incur a large amount of computational or communication overheads or a large amount of energy not consume. The MANETs topology varies dynamically. So, a protocol design is difficult and about the security and energy desired by an application that is able to provide hard guarantees [7]. Energy efficiency is an important consideration in MANETs, since nodes are relies on limited battery power for their energy. Energy-saving techniques aimed at minimizing the total power consumption of all nodes in the multicast group and

at maximizing the multicast life span should be considered [8].

Various research works already carried out towards routing [9], energy efficiency [10], security, management of traffic [11], etc. in the MANET and in this regards significant improvement has also been observed. However, in research community studies towards proactive routing called as OLSR is recently gripping a good pace. Basically, some of the significant advantages are in OLSR e.g. destination before routing known information, routes availability, highly controlled communication over-head, easy to integrate with Internet etc. [12, 13]. Hence, such features are quite better than frequently used Ad-hoc On-Demand Distance Vector (AODV) [14]. From the security viewpoint, there is less number of research attempts towards investigating the robustness of OLSR against various types of adversaries. It was also seen that existing research work towards secure routing is quite specific to attack types and hence reduces the applicability on other attack types. For multipoint relay (MPR) selection [15] there has been some research used optimization to find MPR set but does not consider the quality metrics and not optimal. In the related work some optimization are developed to make an optimal MPR selection, but they are complex difficult to implement and consume more resources.

In MANET, it was found that there is less number of researches addressing the security and energy efficient problems in OLSR with optimization approaches. The main problems are wormhole attack addressing; attack of collusion, denial service, attack of replay, attack of link spoofing, attack of node capture, still OLSR is highly vulnerable. Never addressed such attacks and hence the scope of existing work applicability is too much limited and the attack scenario changes cause lacks of flexibility. Therefore the background of the paper is to design and develop a novel framework that offers energy and security solution by the malicious behavior of a mobile node in OLSR.

The fundamental goal of this paper is MPR selection with energy-efficient and secured routing OLSR protocol in MANET. To this end, we propose an optimization framework named multi objective ALO that prolonging network lifetime and reduce delay. For optimal routing ALO based optimization is used on each energy nodes in which, with the shortest routes the combination used weight factor. Of each node it integrated the energy factor into routing and selected the most optimal route. The rest of this paper is structured as follows: Section 2 briefly reviews the related works. The Section 3 states our proposed MPR selection parameter. The performance of our proposed algorithm is demonstrated in Section 4 and finally Section 5 includes the conclusion of the paper.

2. Relevant literature: A brief review

The most recent implementation work being carried out towards security and energy efficient problems in OLSR is discussed in this section.

The recent work carried out by Vallala Sowmya Devi and Nagaratna P Hegde [16] have presented a trust enhanced cluster based multipath routing algorithm (TECM). To create cluster formation and cluster head (CH) the energy efficient particle swarm optimization (PSO) algorithm was used and from trust values the super cluster head were selected, form TECM algorithm computation. With standard multipath OLSR protocol (TECM-OLSR) the introduced TECM algorithm performance was analyzed. The results show that when compare to fuzzy petri based trust inference model with OLSR protocol (FPNT-OLSR) in terms of loss and delivery rate, delay, routing overhead and network lifetime, the presented TECM-OLSR protocol was very effective. To achieve better throughput by securing end-to-end communication in MANETs Muhammad Usman et al. [17] introduced a novel scheme, known as QoS (Quality of Service)-Aware Secured End-to-End data Communication (QASEC). Through an optimal link selection the QoS was maintained from an available transmission links queue. By authentication, the end-to-end communication was secured. For node interaction symmetric encryption based simple secret-key was deployed. Between the source and destination QASEC scheme prevents the malicious nodes from data exchange with legitimate intermediate nodes on any path established.

S. Muthurajkumar et al. [18] introduced a new secured routing protocol called CEESRA (cluster based energy efficient secure routing algorithm) for efficient energy and uses the trust scores on nodes in cluster based routing to effectively detect the intruders. By using intelligent agents the routing algorithm reduces the denial of service attacks more efficiently for routing decision. With this trust based secured routing algorithm the experiments were conducted and observed that the introduced routing algorithm not only enhances the security but also reduces the energy consumption and delay in routing. The authors [19] presented an energy-efficient secured routing protocol to overcome the secure routing challenges. Amongst the set of one-hop neighbors each node chooses MPR nodes to

reach all neighbors with two-hop. From the network the access control entity authorizes nodes announcing the identification of node. Using generated keys the authors perform group key distribution with a small number of messages that helps to reduce energy consumption.

Based on a Markov chain Sajal Sarkar and Raja Datta [20] presented a secure and energy-efficient stochastic multipath routing protocol for MANETs. Between sources to destination pairs the routing protocol computes multiple paths and stochastically selects an energy-efficient path, from those paths the data packets was forward. The performance analysis and numerical results show that in terms of throughput, security, energy consumption, and delay of routing protocols the introduced protocol achieves significant performance gains. The authors [21] presented an ad hoc routing algorithm, for planetary exploration developed within the EU SWIPE (European Union's Space Wireless Sensor Networks for Planetary Exploration) project, applicable to wireless sensor networks (WSNs). The algorithm was able to assure with multiple data sinks in any-cast communication, for fault-tolerance and redundancy deployed purposes, for the maintenance of the routing paths the control overhead was minimized based on memory and computational requirements, in order to be installed into low-memory/processing and low-power devices, to be robust and in the presence of node failures rapid to reconfigure and to optimize the routes choice to achieve energy balancing and saving.

Seyed Hossein Hosseini Nazhad et al. [22] have presented a new HCAL (Hierarchical Clustering Algorithm) and corresponded protocol for hierarchical routing in LMANET. Based on a cost metric the HCAL was designed in the form of the link expiration time and node's relative degree. The presented algorithm performance and numerically evaluated protocol in average end- to-end delay, CH per round number, iteration count between the CHs, average keeping time of CH, normalized overhead routing, and delivery ratio of packet over a number of randomly generated benchmark scenarios. To increase the energy efficient zone based routing protocols P. Tamil Selvi and C. Suresh GhanaDhas [23] deals with a novel algorithm that control the network topology by estimating node die out rate. To improve QoS routing for MANET a game theory approach with energy efficient zone based routing protocol. The experimental outcomes proved the presented algorithm efficiency was compared with other routing algorithms.

For security in MANETs Hicham Amraoui et al. [24] has roused from ongoing advances gave in game theory by introducing a new model. With countless the displayed strategy was an intense device where on different occasions the co-operations were played. In addition, adapt to the practices, every hub (node) keeps a participation rate record of different hubs and mitigates different malignant gadgets aggregate impact. However, the cooperation rate is not a unique parameter to evaluate the node behaviour also it exhibits the limitation like overload of path and energy consumption of node. A new way to minimize the energy consumption called EM-OLSR (Energy Efficiency in MANET by enhancing OLSR protocol) was presented by Sofiane Hamrioui et al. [25]. The EM-OLSR depended on the OLSR routing protocol and include new parameter for energy decency to MPR strategy. In their mechanism for all the mobile nodes with low power were counteracted in the routing procedure in order to maintain comparable power esteems. Hence, it is noticed using OLSR only few works has been done for resisting adversaries in MANET. Some works like [24], [17] is adequate in terms of security, but weak in all aspects of providing efficient energy. Similarly the previous work like [21], [19] is adequate in terms of energy and security but weak in optimal MPR selection. To overcome these challenges an energy efficient and secure routing OLSR protocol with MOALO is presented in the following section.

3. Proposed energy efficient and secure routing for MPR selection

The main purpose of routing protocol in MANET is to route the data to any point in the network. By using minimum possible number of steps the prominent solution is routing to the destination. This technique greatly minimizes the routing time and it is significant. In order to achieve better performance, recently energy efficiency and security has been one of the main MANET concerns. Accordingly, in the proposed routing protocols it is very important to consider this issue. In this paper, for MANET a significant designing process with the least energy cost solutions and secure parameters was examined. By upgrading the OLSR routing algorithm the proposed approach provides MANET with efficient energy and security, also it aims at better energy conservation in MANET. The main approach of this paper is to use the multi objective ALO to select MPR for the OLSR promotion. Fig. 1 shows the schematic architecture of proposed system.

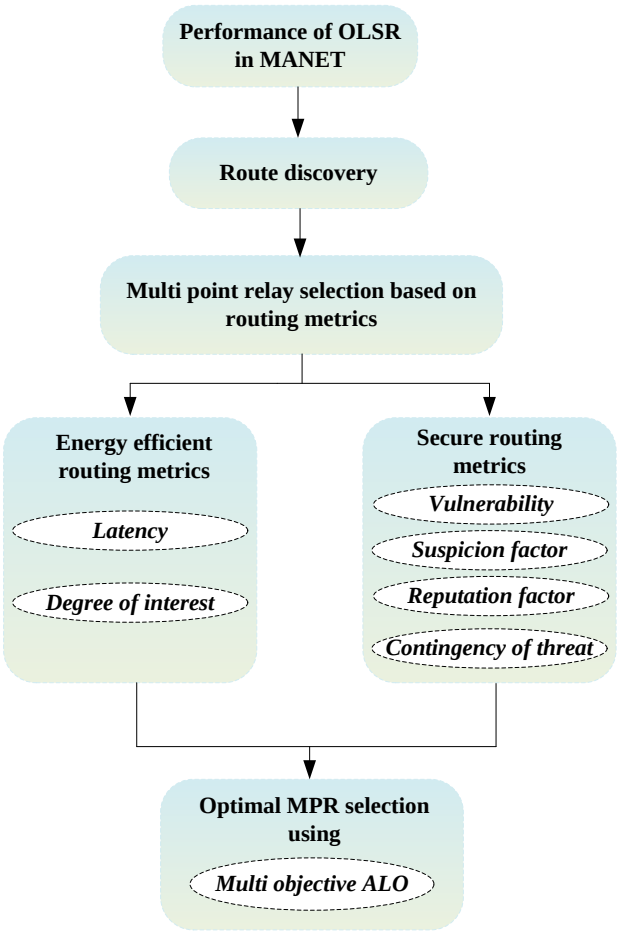

Figure. 1 Architecture of proposed MOALO based MPR selection

In MANET minimizing energy consumption and security is a very important issue. In order to achieve better energy conservation in MANET a secure routing protocol with reduced energy consumption is required to upgrading the OLSR routing algorithm. Here, the routing problem is considered as a multi objective problem. Based on the parameters of energy efficiency and security the multi objective problem is formulated. The research motivation is that a method for selecting the MPR, which is based on an multi objective ALO to find the appropriate problem space and to choose the optimal solution. The next section presents our routing metrics and proposed method to overcome the multi objective problem. The simulation results also indicate these approaches effectiveness in increasing and improving the OLSR routing algorithm efficiency.

3.1 Energy efficient routing metrics

Based on the quality of service parameters such as latency, the degree of interest of each node, the multi-point relays is selected. In OLSR, only MPR nodes are responsible to control traffic forward across the network with the intention of spreading. To control traffic flow an efficient mechanism is provide by MPR for reducing the number of required transmissions. In this paper, to help neighbors to find their own double-step and single-step through their answers OLSR used hi-res message. However, when the number of single-step neighbor is more than a number of similar uncovered double-step neighbors are covered by it. Thus, the neighbor who has a minimal delay and a high degree of interest in this node was chosen as a node of multiple relays.

(a) Latency

OLSR used the exchange of hi-res message to obtain information and to calculate latency. For efficient energy the packet delay (latency) was measured by the required average time it takes to send data packets from one node to another node or destination. The latency is calculated by subtracting the time for transmitted packet by source to destination.

$$latency = \frac{PD_{sum}}{PR_N} \quad (1)$$

Where, the sum of time spent to deliver packets for each destination is represented as PD_{sum},

PR_N is the number of packets received by destination nodes.

(b) Degree of Interest

The interest of the node to prioritize other nodes to send data to the network is indicated as the degree of interest. The degree of interest in the node's interest in wireless mesh networks is intended to provide a contribution or commitment to other nodes in the transmission of data on the network. In OLSR, the interest is based on the node energy state i.e., the node is selected to carry traffic from other nodes. Due to traffic power loss the node does not carry the other node traffic (interest will change).

3.2 Secure routing metrics

To optimize the OLSR protocol performance, for modeling node misbehavior in MANET by routing decision is the objective of the proposed method. For security the system computes the routing action such as assessment of vulnerability, suspicion factor, reputation, and contingency of threat using probability theory.

(c) Vulnerability

For both malicious and normal node the adoption of PF_i and PD_j could be applicable and to discretize there is no possibility PF_i and PD_j with vulnerability. Using the probability theory the vulnerability (V) is computed as

$$V = \frac{k(PF_i \times PD_j)}{(PF_i + PD_j)^2} \quad (2)$$

Where, PF_i represent the number of instances packet forwarding

PD_j represent the number of instances packet dropping and the network constant is k.

(d) Reputation and Suspicion Factor

The t_v variable corresponds to cumulative vulnerability is 1-V. For any cases of $PF_i = PD_j$ the formulation closer look will show that $PF_i/(PF_i+PD_j)$ is equal. The below equation is the only possibility from getting caught that an intruder will select to get itself avoided. Any possibility of $PF_i \neq PD_j$ is ignored

$$R_f = \left[\frac{PF_i}{(PF_i + PD_j)}\right] t_V \quad (3)$$

$$S_f = t_V - V \quad (4)$$

Therefore, both reputation and suspicion factor use t_v computing. Because, for two nodes $PF_i/(PF_i+PD_j)$ may be same. But the V value will differ in Eq. (2). In this case the change for identifying the possibility of misbehaving node is higher and this is considered as N to be malicious node best case.

(e) Contingency of Threat

Using the probability theory Eq. (5) is the best way to quantify the computations outcomes. The contingency of threat for communicating node is expressed as

$$C_T = \frac{PD_j}{(PF_i + PD_j)} \quad (5)$$

Where, C_T denote the contingency of threat.

3.3 MOALO based energy efficient and secure MPR selection algorithm

In OLSR, a hi-res message is periodically released by node. Through the information changes in neighborhood is discovered by these messages. The node address of publisher's and a neighbors list known to that node, for each neighbor including the link state (for example, non-symmetric or symmetric) are in hi-res message. Accordingly, a node informs its neighbors to communicate with which neighbor and in which communications direction is approved. A node can collect information by receiving a hi-res message that describes its neighbors and double-step neighbors. Besides, in its neighborhood it determined the quality of the links: the link from the node n to the neighbor m is symmetric if the n node in the hi-res message from no serves its own address (with any link state), otherwise it is asymmetric link. The multipoint relay selection process in the proposed method using ALO is shown in Fig2.

The ALO approximates the optimal solutions with utilizing a set of random solutions similarly to other algorithm for optimization problem. From the interaction between antlions and ants this set is enhanced based on the inspired principles. In the ALO there are two populations such as ants and antlions sets. To estimate the global optimum for a given optimization problem, these two sets are changed and the ALO general advances are as per the following steps:

- Ant move randomly around the hunt space and by antlions traps these move are influenced
- Antlions with highest fitness builds a larger pit.
- For catching ant an antlions is utilized, proportional to the fitness of ant lion.
- When iteration reached antlions can get an ant.
- Towards the antlions sliding ants are recreated; the range of random walk is diminished adaptively.
- If an ant becomes fitter than the antlions, that is caught and pulled under the soil by antlions
- The antlions repositions itself to the latest caught prey and after each hunt pit is constructed to enhance its chances of catching.

Step 1: Random walks

Around the hunt space utilizing random walks (position updating) at each iteration ant move based on condition (6).

$$Y(m) = [0, cumsum(2R(m_1) - 1), cumsum(2R(m_2) - 1), \cdots, cumsum(2R(m_t) - 1)] \quad (6)$$

Where, the cumulative sum is calculated by *comsum*, *t* is the maximum number of iteration, the step of random walk (iteration in this research) is *m* , the stochastic function is *R*(*m*){1 *if rand* > 0.5; 0 *if rand* ≤ 0.5} and the random number is *rand* generated with uniform distribution in [0,1] interval.

In search space to prevent ants from overshooting and to keep the random walk in boundaries, utilizing the eq. (7) the random walks are standardized.

$$Y_j^m = \left[\frac{\left(Y_j^m - a_{1_j}\right)\left(d_{1_j} - c_{1_j}^m\right)}{b_{1_j} - a_{1_j}}\right] + c_{1_j} \quad (7)$$

Where the maximum of j^{th} variable at m^{th} iteration is d_{1j}^m, the minimum of j^{th} variable at m^{th} iteration is c_{1j}^m, the maximum of random walk in j^{th} variable is indicated as b_{1j}, and a_{1j} represents minimum of random walk in j^{th} variable.

Step 2: Pits trapping of Antlions

By the antlions traps, the random walks of ants are influenced which is joined by accompanying Eqs. (8) and (9).

$$c_{1_j}^m = AL_i^m + c_1^m \quad (8)$$

$$d_{1_j}^m = AL_i^m + d_1^m \quad (9)$$

Here, the position of selected ith antlion at m^{th} iteration is denoted as $AL^m{}_i$, $c_1{}^m$ is the minimum vector and $d_1{}^m$ is the maximum vector that contains all the variables in m^{th} iteration.

Step 3: Trap constructing

To display the chasing capability of antlions the determination component ought to be utilized. With the high fitness the ant lion has a higher opportunity to get an ant. Here, based on their applied fitness value RWS (Roulette Wheel Selection) is utilized for choosing ant lions.

Step 4: Sliding ants toward antlion

The ant endeavors to escape when it slips into the pit. On the off chance that the ant lion acknowledges there is a prey in the pit and shoot the sand towards the pit focus. The random walk of ants range is diminished to display this behavior which is scientifically expressed in underneath Eqs. (10) and (11).

$$c_1^m = \frac{c_1^m}{r} \quad (10)$$

$$d_1^m = \frac{d_1^m}{r} \quad (11)$$

Where, the ratio is *r* is characterized as,

$$r = 10^{\alpha}\frac{m}{T_M} \quad (12)$$

Where the present iteration is *m*, T_M represents the maximum iteration, the accuracy level of exploitation is changed by parameter α, the parameter is characterized based on the present iteration.

Step 5: Prey catching and reconstructing the pit

In the final stage, at the pit base the prey reaches and caught the jaw of antlions. After that inside the sand the ant lion pulls the ant and expends its body. Here, the ant lion update its position to the chased ant position to raise its chasing ability of new ant by eq. (13).

$$AL_i^m = \begin{cases} ant_j^m; & if\ \ f\left(ant_j^m\right) < f(AL_i^m) \\ AL_i^m; & otherwise \end{cases} \quad (13)$$

Where, the position of j^{th} ant at m^{th} iteration is indicated as $ant_j{}^m$, and the current iteration is *m*,

Step 6: Fitness evaluation

The fitness function is evaluated based on delay, degree of interest, vulnerability, suspicion factor, reputation factor, and contingency of threat. A node with a minimal value of the fitness function is selected as the node of MPR. The fitness function is depicted as following Eq. (14).

$$fitness_{nm}(P) = min[delay_{nm}(P) + weight_{nm}(P) + V_{nm}(P)] \quad (14)$$

Where, $fitness_{mm}(P)$ represents the fitness function for packet *P* transfer from node *n* to node *m*, $delay_{nm}(P)$ represents the required time delay and $weight_{nm}(P)$ is the inverse degree of interest for packet *P* transfer from node *n* to node *m*, and $V_{nm}(P)$ represents the vulnerabilities of the security parameters such as suspicion factor, reputation factor, and contingency of threat.

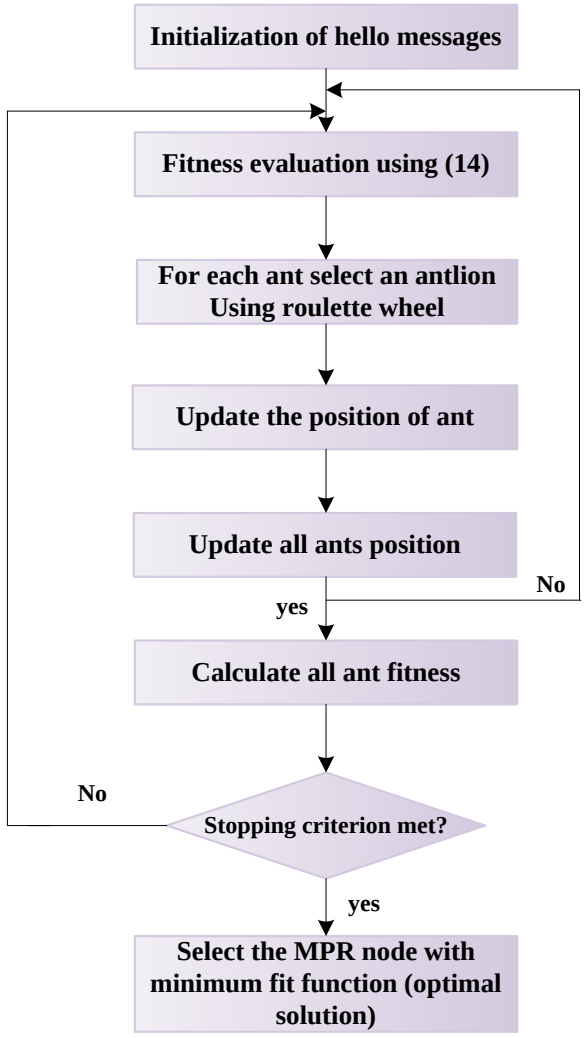

Figure. 2 Flow diagram of ALO based method in selection of MPR

Step 7: Elitism

In every iteration, the ant lion with the higher fitness is considered as elite. The selected and elite antlion utilized the selection mechanism to direct the random walk of ant and thus the given ant repositioning follows the following eq. (15).

$$ant_j^m = \frac{R_A^m + R_E^m}{2} \quad (15)$$

Where the random walk around the selected ant lion is represents as $R^m{}_A$ utilizing the roulette wheel mechanism and $R^m{}_E$ represents the elite random walk at m^{th} iteration.

4. Results and discussion

The performance of the proposed method to demonstrate its effects on energy consumption, and security in MANET is examined in this section. The proposed energy efficient and security protocol is simulated in NS 2 software with1000×1000 m^2 network area. In terms of delay, throughput, energy consumption and network lifetime the performance of proposed approach is compared with the existing OLSR [24] and EMOLSR [25]. In this paper three key performance measures like energy consumption, delay, network lifetime and throughput were investigated.

Table. 1 Simulation setup parameter

Parameter	Value
Network area	1000×1000 m^2
Routing protocol	OLSR
Number of nodes	20, 40, 60, 80, and 100
MAC protocol	IEEE 802.11
Transport layer	User datagram protocol (UDP)
Average node speed	20 ms
Mobility model	Random way model

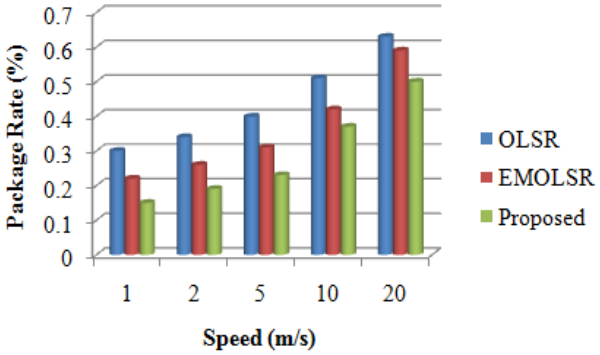

Figure. 3 Comparison of data loss rate with speed

4.1 Reliability of protocols

In this simulation, the network load is equal to 20 sources which in accordance with the comparison method. The stability is provided by the network is relatively high for weak mobility node and when compared to high mobility node the links failure is lower. Fig. 3 shows the package rate of the proposed and existing method with respect to speed. It is noticed from the figure the loss rates of packet for proposed method is very less of 15.25%, and 20.63% when compared with OLSR and EMOLSR. This is due to the optimal route selection for data transfer using the proposed method.

4.2 Delay and throughput performance

The proposed method effects are testified using the performance parameter of end-to-end delay and throughput along with a comparison of existing scheme. Fig. 4 shows the end-to-end delays of proposed method with different iterations. The result

show that the proposed scheme is better when compared to the existing techniques like OLSR and EM – OLSR. From the delay outcome it is noticed that, till 1000th round the delay rate increases and then till 1500th round decreases its delay rates. Again found to repeat the similar till 3000th round, due to proposed optimal routing parameters.

Fig. 5 shows the throughput of proposed method with different iterations. The result show that the proposed scheme is better when compared to the existing techniques like OLSR and EM – OLSR. It is because of the optimal MPR selection of secure routing metrics like vulnerability, initial computation of reputation factor and suspicion factor. The throughput of the proposed method is significantly increases from 0th to 5000th iteration round by 32.78%, 23.07%, 24.63%, 28.39% 29.07% and 21.27% when compared with standard OLSR, and 26.23%, 16.92%, 18.84%, 24.69%, 20.93% and 15.95% by EMOLSR. Hence, observed better delay compensation along with enhanced throughput.

4.3 Energy consumption and network lifetime

The total energy of network decreases faster before upgrade rather than after the upgrade period over a time of 601sec.

The consumption difference during this period is because of management intelligent energy by selecting the right multi-point relay through an ALO algorithm that reduces the energy consumption. During 600sec period it is determined that the level of grid energy before upgrade is fixed because of connection loss. Connection loss is due to the fact that the inappropriately used nodes energy which results in total node energy depletion by OLSR protocol. The failure of network connection thus stops the activity of network.

The energy consumption with time estimation is shown in Fig. 6. During the same time period, energy in the network began to decrease with the upgrade of the proposed method which proves that the nodes are communicating. While comparing with existing methods the proposed method saves 18% of total network energy. This indicates that the proposed achieves more network resources utilization by optimal MPR selection through MOALO to reduce energy consumption. On the other hand the existing methods select the metrics for route discovery with same intermediate nodes, which lead to high energy consumption. The network life time is shown in Fig. 7. Before upgrade the number of active nodes in network has reduced (at t=400sec). Due to connectivity loss only three nodes is stable at t=700sec. Thus, the proposed OLSR method the active node in the network is kept stable at 800sec and it rapidly started to slow down. This is because of consideration given to security and lifetime during the MPR selection. The simulation results showed that the approach improved the throughput and network life time of a network compared to existing method.

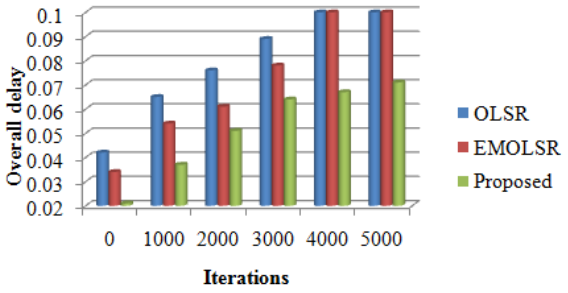

Figure. 4 Comparative delay analysis of proposed method

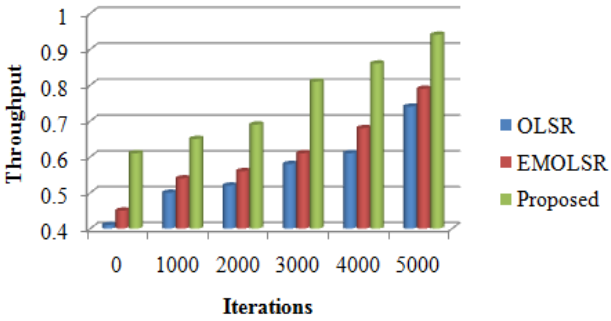

Figure. 5 Analysis of throughput with proposed method

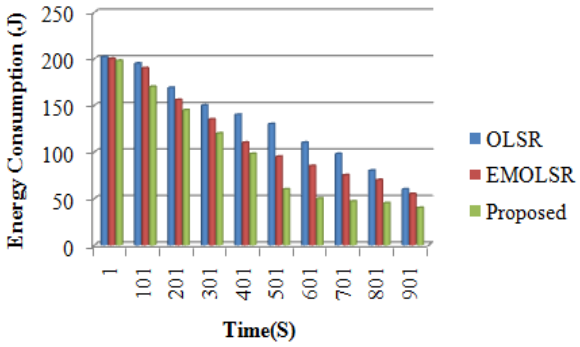

Figure. 6 Energy consumption versus estimation time

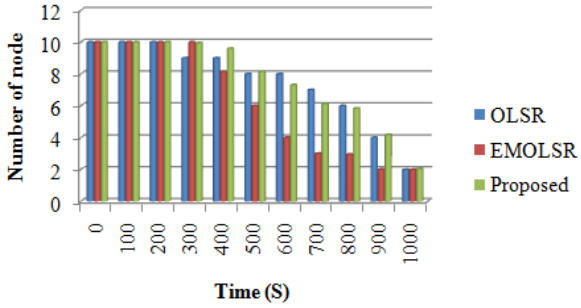

Figure. 7 Analysis of network lifetime

5. Conclusion

In this paper, a new approach in MANET is proposed by upgrading the OLSR based on energy efficiency and security which can be progression in OLSR for better energy conservation. The new approach is fundamentally based on the energy quality of mobile nodes and assists the node to compute vulnerability based on a number of the data packet being exchanged by the nodes. By this protocol another parameter is added to the multipoint relay method. The proposed method introduced the upgrading process for the selection of multipoint relay in OLSR protocol by using the ant lion optimization where the delay, degree of interest, and vulnerabilities are proposed as the fit function. The result show that the proposed method has a better performance rather than standard OLSR in terms operating power, energy consumption and security as well as lifetime of network. In terms of packet loss rates the proposed method is very less of 15.25%, and 20.63% when compared with OLSR and EMOLSR. The throughput of the proposed method is 26.54% superior to OLSR and 20.59% superior to EM-OLSR due to the optimal route selection using MOALO method.

References

[1] S. Ghasemnezhad and A. Ghaffari, "Fuzzy Logic Based Reliable and Real-Time Routing Protocol for Mobile Ad hoc Networks", *Wireless Personal Communications*, Vol. 98, No. 1, pp. 593-611, 2017.

[2] J. Kong, X. Hong, Y. Yi, J. Park, J. Liu, and M. Gerla, "A secure ad-hoc routing approach using localized self-healing communities", In: *Proc. of the 6th ACM international symposium on Mobile ad hoc networking and computing - MobiHoc '05*, Urbana-Champaign, pp. 254-265, 2005.

[3] C. Busch, R. Kannan, and A. Vasilakos, "Approximating Congestion + Dilation in Networks via "Quality of Routing" Games", *IEEE Transactions on Computers*, Vol. 61, No. 9, pp. 1270-1283, 2012.

[4] T. Meng, F. Wu, Z. Yang, G. Chen, and A. Vasilakos, "Spatial Reusability-Aware Routing in Multi-Hop Wireless Networks", *IEEE Transactions on Computers*, Vol. 65, No. 1, pp. 244-255, 2018.

[5] X. Zhang, Y. Zhang, F. Yan, and A. Vasilakos, "Interference-Based Topology Control Algorithm for Delay-Constrained Mobile Ad Hoc Networks", *IEEE Transactions on Mobile Computing*, Vol. 14, No. 4, pp. 742-754, 2015.

[6] G. Yao, J. Bi, and A. Vasilakos, "Passive IP Traceback: Disclosing the Locations of IP Spoofers From Path Backscatter", *IEEE Transactions on Information Forensics and Security*, Vol. 10, No. 3, pp. 471-484, 2015.

[7] N. Fernandes and O. Duarte, "An Efficient Group Key Management for Secure Routing in Ad Hoc Networks", In: *Proc. of International Conference on Global Telecommunications*, pp. 1-5, 2008.

[8] D. Karthikeyan and M. Dharmalingam, "Ant based intelligent routing protocol for MANET", In: *Proc. of the International Conference on Pattern Recognition, Informatics and Mobile Engineering*, pp. 11-16, 2013.

[9] D. Patel, S. Patel, H. Kothadiya, P. Jethwa, and R. Jhaveri, "A survey of reactive routing protocols in MANET", In: *Proc. of International Conf. on Information Communication and Embedded Systems*, pp. 27-28, 2014.

[10] K. Chawda and D. Gorana, "A survey of energy efficient routing protocol in MANET", In: *Proc. of International Conference on Electronics and Communication Systems*, pp. 953-957, 2015.

[11] H. Gupta and P. Pandey, "Survey of routing base congestion control techniques under MANET", In: *Proc. of IEEE International Conference ON Emerging Trends in Computing, Communication and Nanotechnology*, pp. 241-244, 2013.

[12] H. Zhan and Y. Zhou, "Comparison and Analysis AODV and OLSR Routing Protocols in Ad Hoc Network", In: *Proc. of International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 1-4, 2008.

[13] S. Gandhi, N. Chaubey, P. Shah, and M. Sadhwani, "Performance evaluation of DSR, OLSR and ZRP protocols in MANETs", In: *Proc. of International Conference on Computer Communication and Informatics*, pp. 1-5, 2012.

[14] A. Al-Maashri and M. Ould-Khaoua, "Performance Analysis of MANET Routing Protocols in the Presence of Self-Similar Traffic", In: *Proc. of IEEE Conference on Local Computer Networks*, pp. 801-807, 2006.

[15] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks", *IEEE Wireless Communications*, Vol. 14, No. 5, pp. 85-91, 2007.

[16] V. Devi and N. Hegde, "Multipath Security Aware Routing Protocol for MANET Based on Trust Enhanced Cluster Mechanism for

Lossless Multimedia Data Transfer", *Wireless Personal Communications*, Vol. 100, No. 3, pp. 923-940, 2018.

[17] M. Usman, M. Jan, X. He, and P. Nanda, "QASEC: A secured data communication scheme for mobile Ad-hoc networks", *Future Generation Computer Systems*, Vol. 45, No. 5, pp. 11-19, 2018,

[18] S. Muthurajkumar, S. Ganapathy, M. Vijayalakshmi, and A. Kannan, "An Intelligent Secured and Energy Efficient Routing Algorithm for MANETs", *Wireless Personal Communications*, Vol. 96, No. 2, pp. 1753-1769, 2017.

[19] T. Singh, J. Singh, and S. Sharma, "Energy efficient secured routing protocol for MANETs", *Wireless Networks*, Vol. 23, No. 4, pp. 1001-1009, 2016.

[20] S. Sarkar and R. Datta, "A secure and energy-efficient stochastic multipath routing for self-organized mobile ad hoc networks", *Ad Hoc Networks*, Vol. 37, No. 2, pp. 209-227, 2016.

[21] G. Oddi, A. Pietrabissa, F. Liberati, A. Di Giorgio, R. Gambuti, A. Lanna, V. Suraci, and F. Delli Priscoli, "An any-sink energy-efficient routing protocol in multi-hop wireless sensor networks for planetary exploration", *International Journal of Communication Systems*, Vol. 30, No. 7, pp. e3020, 2017.

[22] S. Nazhad, M. Shojafar, S. Shamshirband, and M. Conti, "An efficient routing protocol for the QoS support of large-scale MANETs", *International Journal of Communication Systems*, Vol. 31, No. 1, p. e3384, 2017.

[23] P. T. Selvi, and C. S. G. Dhas, "A Novel Algorithm for Enhancement of Energy Efficient Zone Based Routing Protocol for MANET", *Mobile Networks and Applications*, Vol. 1, No. 1, pp 1–11, 2018.

[24] H. Amraoui, A. Habbani, A. Hajami, and E. Bilal, "Security-Based Mechanism for Proactive Routing Schema Using Game Theory Model", *Mobile Information Systems*, Vol. 2016, No. 10, pp. 1-17, 2016.

[25] S. Hamrioui, M. Lalam, and P. Lorenz, "A new approach for energy efficiency in MANET based on the OLSR protocol", *International Journal of Wireless and Mobile Computing*, Vol. 5, No. 3, pp. 292, 2012.