International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-1, November 2019

Mobility Aware Energy Efficient Cluster Based Secure Routing Protocol for Mobile Adhoc Networks

S. Murugan, M. Jeyakarthic

Abstract*: Mobile ad-hoc network (MANET) is an evolving technology which derives under the class of wireless networks. Due to the inherent characteristics of nodes in MANET, energy efficiency and security still remains a major design issue. This paper intends to develop a multi-objective optimization (MOO) model for effective load distribution and security in the network. The presented MOO technique operates on two main stages namely clustering and secure routing. In the first stage, fuzzy logic technique with multiple input parameters namely energy, distance, link duration, latency, and trust are used for effective cluster construction. In the next stage, Lion Whale optimization (LWO) algorithm is introduced for secure routing. Using the determined MOO variables, a fitness function is derived to select the optimal routes for secure routing in MANET. The effective performance of the presented FLWO model is tested using a set of validation parameters and the proposed model attains maximum performance over other methods in a considerable way.

Keywords*: MANET; Clustering; Security; Routing; Fuzzy logic.

I. INTRODUCTION

Mobile ad-hoc network (MANET)] is a self-directed model where many host nodes are linked to one another via multi-hop wireless connections as shown in Fig. 1. Based on the feature of MANET, it is necessary to add some safety measures that provide security like accessible at any time, avoid the repeated data, reliability, to maintain confidential information, as well as authorization. MANET protecting measure is divided into: protecting the routing operation and data transmission [1]. This routing model that involves in safety, offers the valid facility that protects over the changes occurred and repetition of routing control messages that utilizes various cryptographic fundamentals to avail safer routing. Some of the securing protocols are: fundamental approaches, detecting and isolating dependent methods, incentive based routing protocols, as well as trust based approaches [2]. The main aim of router is to transmit and distribute data which activates them to choose path among different nodes in the computer network, also to select the optimal root for communication of data.

Clustering is a better model that resolves several issues of MANET like scalability and improves the lifetime. In this case, the partitioning of network takes place into a set of clusters where a leader called cluster head (CH) is decided and rest of them are turned as cluster member (CM). The CHs has the role of getting data from CM, aggregating it and transmitting into the BS via other CHs or gateways. Routing protocol present in MANET is classified as follows: proactive, multicast and reactive. Proactive protocol is also called as table driven protocol, like destination sequenced distance vector and optimised link state routing technique (OLSR), every node present in the system is composed with the record of probable destinations and a path to transfer data. Reactive protocol includes dynamic source routing (DSR), and ad-hoc on-demand distance vector (AODV), the path is created only because of the requirement [3]. For ensuring the needed behaviour of the protocol, some security metrics are required.

Encryption and authentication are the 2 techniques that are helpful in achieving security while transmitting information in MANET. Sensor nodes in ad-hoc network are limited in battery usage and some sleeping mode to conserve the energy. Specified QoS is required for incorporating the routing protocol that helps in determining the consumption of network where it is used for realistic traffic support. Rather than this protocol, no other routing consists of these properties [4]. But the protocols used in MANET are prompt to many types of danger [5]. Therefore, several types of protocols are designed with the aim of eliminating the risk with specified safety metric such as, authentication, non-repeated data, accessibility of resource, integrity and confidentiality.

Revised Manuscript Received on November 30, 2019.
* Correspondence Author
S. Murugan*, Assistant Professor, Thiru Vi Ka Govt Arts College, Thiruvarur.
smuruganmpt79@gmail.com
M. Jeyakarthic, Assistant Director (Academic), Tamil Virtual Academy, Anna University Campus, Chennai-600025. jeya_karthic@yahoo.com

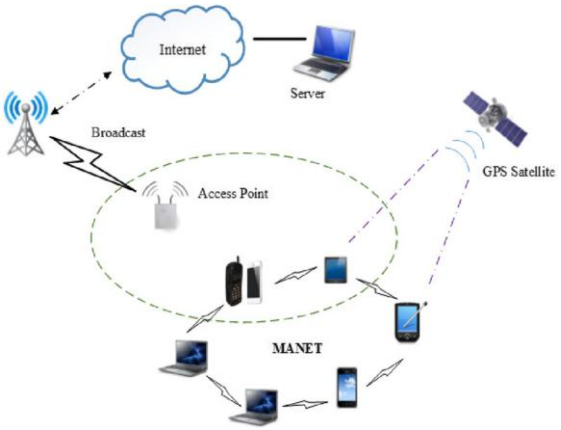

Fig. 1. MANET architecture

In MANET, a technique helps to generate constant and everlasting roots among each node [4]. This model uses some of the properties like stability function, that is based on value of mobility degree for the node, which acts as the criteria for the selecting the primary root. This technique is used in OLSR protocol to identify a balanced as well as retaining multipoint relays (MPRs) nodes and topology. This model is utilized to avoid the repeated operation of MPR and routing tables. Hence it assures in satisfying QoS, about packet loss as well as response time. Therefore, nodes in MPR are affected because of the speed that varies and problems related to path overload and residual energy is not taken into account.

[6] had been used the trust model and QoS measures to develop a trust-based QoS routing (TQR) technique. The trust degree would be calculated among the nodes by direct trust operation that depends upon direct observation whereas indirect trust computing process is done on the basis of neighbour nodes' implication. Assuming the nondeterministic polynomial time (NP)-completeness of many types of QoS issues, this technique takes only the delay in connecting since the QoS limitation is to be fulfilled. Consequently, the TQR technique had been developed for secured routing based on the trade-off among trust degree and delay in connecting. Though it provides security, this model is in need of retransmitting information due to increased data loss.

Hybrid genetic based optimizing model is developed for multicast routing [7]. It uses the benefits of both GA and PSO to provide an extended outcome with usage of Roulette wheel choosing model for selecting primary results. This operation is done by using different number of nodes and simulation outcome is compared with multicast AODV, PSO and GA based model. GA-PSO technique has improved PDR as well as minimized jitter, latency delay with quick convergence. At the same time, the influence of node pause time is concerned on routing outcome. [8] resolved a multi objective unicast routing optimization issue in MANET using diverse performance metrics. To solve the NP-hard problem, multi-objective version of traditional AODV and an ant-based routing protocol is utilized with the objective vector. Furthermore, much effort had been taken to select the routes which are stabilized and efficient with multi objective ant optimizing routing technique, yet the raise in packet loss is invariable.

[9] Designed a technique, multi objective PSO to resolve the multi-objectives present in routing. In this technique, many count of clusters in an ad-hoc network have undergone optimization and power dissipating to make an energy-efficient system and eliminating the network traffic. Cluster heads produced could handle inter-cluster and intra-cluster traffic. Additionally, it used the node degree, transmitting energy, and nodes' battery consumption. The main advantage in this model is, it offers collection of results concurrently. But many numbers of clusters raise the difficulty of computing operation. [10] Proposed an approach, Multi constrained and Multipath QoS Aware Routing Protocol (MMQARP) that uses QoS variables jointly with the path discovery so that it can utilize a consistent connectivity, and effective path for communicating. The protocol performance in better way regarding PDR, delay, and jitter compared with existing ad hoc on-demand multipath distance vector (AOMDV). The drawback in MMQARP is, it requires many numbers of QoS constraints for identifying the optimal paths.

Due to the inherent characteristics of nodes in MANET, energy efficiency and security still remains a major design issue. This paper intends to develop a multi-objective optimization (MOO) model for effective load distribution and security in the network. The presented MOO technique operates on two main stages namely clustering and secure routing. In the first stage, fuzzy logic technique with multiple input parameters namely energy, distance, link duration, latency, and trust are used for effective cluster construction. In the next stage, Lion Whale optimization (LWO) algorithm is introduced for secure routing. Using the determined MOO variables, a fitness function is derived to select the optimal routes for secure routing in MANET. The effective performance of the presented FLWO model is tested using a set of validation parameters and the proposed model attains maximum performance over other methods in a considerable way.

II. THE PRESENTED FLWO ALGORITHM

The presented FLWO technique operates on two main stages namely clustering and secure routing. In the first stage, fuzzy logic technique with multiple input parameters namely energy, distance, link duration, latency and trust are used for effective cluster construction. In the next stage, Lion Whale optimization (LWO) algorithm is introduced for secure routing. Using the determined MOO variables, a fitness function is derived to select the optimal routes for secure routing in MANET.

A. Fuzzy Based Clustering Scheme

Fuzzy model was developed by Zadeh which is mainly used for avoiding inaccuracy. Fuzzy set includes group of objectives with MFs that is allocated for all the objects lies in 0 to 1. A tilde character (~) present previous to the factor indicates fuzzy set. A triangular MF (TMF), $\tilde{M}F$is viewed as $p, q\ andr$ minimum, moderate and maximum values. Some details of fuzzy set are elaborated as follows.

Retrieval Number: A4621119119/2019©BEIESP
DOI: 10.35940/ijitee.A4621.119119
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Definition 1: If $\widetilde{MF_1} = (p_x, q_x, r_x)$ and $\widetilde{MF_2} = (p_b, q_b, r_b)$ are the 2 TMFs, then the basic operations such as add, sub, multiply, divide as well as reciprocal is computed as follows:

$$\widetilde{MF_1} - \widetilde{MF_2} = (p_x, q_x, r_x) - (p_y, q_y, r_y) \quad (1)$$

$$\widetilde{MF_1} + \widetilde{MF_2} = (p_x, q_x, r_x) + (p_y, q_y, r_y) \quad (2)$$

$$\widetilde{MF_1} \times \widetilde{MF_2} = (p_x, q_x, r_x) * (p_y, q_y, r_y) \quad (3)$$

$$\widetilde{MF_1} / \widetilde{MF_2} = (p_x, q_x, r_x) / (p_y, q_y, r_y) \quad (4)$$

$$\widetilde{M_{F1}}^{-1} = (p_x, q_x, r_x)^{-1} = \left(\frac{1}{p_x}, \frac{1}{q_x}, \frac{1}{q_x}\right) \quad (5)$$

Definition 2: Fuzzy set $\widetilde{MF}$ present inZ is viewed by a MF$\mu_{\widetilde{M}}(x) \in (0,1)$. It denotes the membership position z to $\widetilde{MF}$.

Definition 3: TMF of $\widetilde{MF_n}$ is computed in Eq. (6) and the level of membership is programmed in Eq. (7).

$$\mu_{\widetilde{M}}(z) = \begin{cases} \dfrac{z-p}{q-p}, & p \le z \le q \\ \dfrac{r-z}{r-q}, & q \le z \le r \\ 0, & otherwise \end{cases} \quad (6)$$

$$\widetilde{M} = (M^{L(y)}, M^{R(y)}) = (p + (q-p)y, r + (r-q)y), y \in [0,1] \quad (7)$$

where $M^{L(y)}$ and $M^{R(y)}$ indicates the fuzzy value.

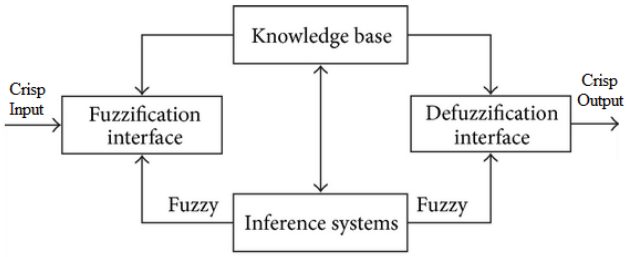

Fig. 2. Fuzzy logic system

When mobile nodes are placed in the sensing area, BS transmits a beacon signal for whole system. Based on RSSI, all mobile nodes get the beacon signal and compute the distance from BS. Mobile nodes transmit a handshaking message within its competition range to collect the information regarding its neighbour. The handshaking message comprises of node ID, connection superiority, residual energy and distance.

Usually, these variables are utilized during the process of clustering. Whenever the process is initiated, indefinite CHs are selected through a timer. The value of timer is not equal to the energy level of the node. All nodes must remain stable in prior to expiry of timer. If the CH advertisement packets received by a node in prior to the expiry of timer value, it could not participate in the competition of CH electing process and remains as a CM. If no CH advertisement message is sent to the node, then it considers itself as indefinite CH while the timer is zero. Hence, this model chooses the cluster head in an uncertain way. The timer values are low for nodes which has massive quantity of remaining energy whereas timer values are high for nodes with least number of residual energy. Hence the fuzzy logic is utilized to determine suitable CH as well as accurate selection of CHs.

Fuzzification

Some input variables of SFLC are energy, distance, link lifetime, delay, and trust. As a first step, the input value is provided to the fuzzy logic system and matches the value to the appropriate linguistic variables of the fuzzy variables.

MFs

Output variable member function is shown in Fig. 3. Trapezoidal MF is utilized for border values as well as triangular membership is used for the intermediate values.

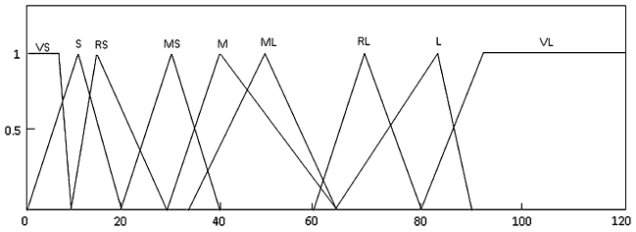

Fig. 3. Output MF

Fuzzy decision blocks/ Rule base

It consists of input and output variables under linguistic parameters which are interconnected by the collection of *if then* rules. Inference engine is used to compute these types of rules. *if-then* condition as defined in Eq. (8). When5 inputs are $A_1^i AND\ A_2^i\ AND\ A_3^i\ AND\ A_4^i\ AND\ A_5^i$, then the simulation outcome would be B_1^i and B_2^i.

$$Rule(i) IF\ x_1 is\ A_1^i\ AND\ x_2\ is\ A_2^i\ AND\ x_3 is\ A_3^i$$
$$AND\ x_4\ is\ A_4^i AND\ x_5 is\ A_5^i$$
$$THEN\ y_1 is\ B_1^i\ \ AND y_2 is B_2^i \quad (8)$$

where 'i' is the ith rule present in rule base table, A1, A2, A5 is the fuzzy set of x1, x2, ..., x5. As 5 input variables are deployed, the count of rules would be 243 totally. This is configured using Mamdami inference system which is very elegant and efficient.

Defuzzification

Centroid of Area (COA) is an approach used for defuzzification procedure which is shown in Eq. (9). This model is helpful in translating the fuzzified outcome variables to a crisp value that denotes the possibility for the node becoming a CH.

$$COA = \frac{\int \mu_A(x).x dx}{\int \mu_A(x).dx} \quad (9)$$

When PBCH is processed, each sensor node transmits a candidate to the various nodes present in its competition range. Candidate message comprises of node ID and PBCH number. A node with maximum possibilities is elected as CH by its own and forwards won to the closer nodes. Single node might receive many numbers of won from its neighboring node. In those cases, it sends join message to couple with beside CH. Receiving join message, the closer CH make sure of the cluster size in prior of considering CMs. The count of entire CMs is not superior when compared to the processed cluster head, it admits a novel CM by responding accept message, else, it would forward reject message.

When the sensor node gets a reject message, it resends the CM_JOIN message to nearby CH except the currently eliminated CH and this process is maintained unless it combines with new CH. In some cases, if the node fails to join with another CH within the coverage area 'R', it elects itself as CH. Consequently, all nodes belong to cluster and the nodes are not separated in WSN. The early death of CHs can be reduced by the rotation process in cluster head. When the remaining power of the CH goes below the threshold value (15% of initial value), CH rotation occurs.

B. LWO Based Secure Routing Scheme

The presented model combines the LA and WOA models to select the paths in an optimal way for secured communication. It assumes diverse QoS variables like energy, trust, distance as a major factor. When the method determines the QoS and security variables, a set of n probable routes are discovered between two nodes. The aim of this model is to choose the best route from the explored routes, fulfilling the many objectives assumed for a secure routing. It is developed using the incorporation of LA and WOA in the update rules. It makes use of an intended model which assumes a set of four QoS measures namely energy, delay, distance, link duration, and trust, as the objectives to select the optimal solutions to offer safety. LA is inspired from the social nature of lions include territorial defence, takeover, utilization of laggard lions, and prides. Next, WOA mimics the humpback whale nature of bubble net hunting. By applying the update rule of LA in WOA, the LWO model developed optimal solutions which offer secured routing paths. The processes involved in the LWO model are explained here.

Initialization

The LWO algorithm starts with the initialization stage where the population of the whales W_j having n solutions undergo initialization at an arbitrary way. Every solution W_j can be defined by

$$W_j = \{p_1, p_2, p_n\} \quad (10)$$

Where P_j is the jth solution in W_j. At the initialization stage, this technique undergo initialization of two vector coefficients *B* and *I*.

Fitness validation

The subsequent stage lies in the computation of fitness for searching the optimal solutions. The multi-objective fitness attained under the utilization of five objectives determines the fitness value of every solution present in population. As the location is not identified at the initial stage, the solution which has the optimal fitness in the present population is treated as the best search agent.

Estimating and updating location

Once the best agent is identified, the LWO model will update the location using the hunting nature like encircling prey, bubble-net attack, and searching prey as given below.

$$G = |I \cdot W^*(k) - W(k)| \quad (11)$$

where *G*is the distance vector, and $W^*(k)$is the location vector of the optimal search agent, in the initial round. The location vector of WOA at round $k+1$ can be represented by

$$Y(k+1) = Y^*(k) - B \cdot G \quad (12)$$

where B and I are vector coefficients as defined by

$$B = 2c * v - c \quad (13)$$

$$I = 2 * v \quad (14)$$

where c is a variables which gets reduced from 2 to 1 under several rounds and u is a vector generated in randomly in the range (0,1). At the attack or exploitation stage, the WOA uses a technique known as spiral bubble-net attacking process for updating the location. It depends upon the distance among the agent and preys. It then formulates a technique by the use of helix-shaped motion of the whales as

$$W(k+1) = G'.e^{q^f} \cdot \cos(2\pi f) + W^*(k) \quad (15)$$

Where $G' = |W^*(k) - W(k)|$ represents the distance of best search agents from prey, $and\ f$ indicates a chosen number from the range $[-1, 1]$. Therefore, the instantaneous spiral-shaped and surrounding nature of whales formulate the mathematical model by

$$W(k+1) = \begin{cases} \vec{w}^*(k) - B \cdot G; if h < 0.5 \\ G' \cdot e^{q^f} \cdot cos(2\pi f) + W^*(k); if h \geq 0.5 \end{cases} \quad (16)$$

where h is arbitrarily chosen in the range $[0, 1]$. For improving the search space, the presented model makes use of the update rule of LO as given below.

$$W(k+1) = W(k) + \left(0.1_{g_2} - 0.05\right)\left(W^*(k) - g_1 W(k)\right) \quad (17)$$

Where $g_1$and $g_2$are the arbitrarily created numbers in the range $[0, 1]$.

$$W^*(k) = W(k+1) + B \cdot G \quad (18)$$

Where $W(k+1)$ is the location vector at subsequent round and $W(k)$ is the location at present round.

Determining best search ages

When the location gets updated, this technique produces the solution of the subsequent population using the update of distance and coefficient vectors. Next, the fitness solution present in the present population is validated by the use of multi-objective function. The solution which holds the highest fitness will replace the solution that is considered as the best fit solution. At the end of every successive round, the value of k undergo incremented. i.e. k=k+1.

Stopping criteria

The steps 2-4 get iterated till the stopping condition is reached. It has the ability to select any stopping condition can choose any of the termination criteria as follows: (i) upon the discovery of optimal solution, (ii) outcome has no more important modification and (iii) when the round reach upto utmost count.

III. EXPERIMENTAL PHASE

A detailed experimental analysis takes place to validate the results of the FLWO algorithm. A simulation is carried out under the presence of 100 nodes as shown in Fig. 4. The nodes have the ability of transmitting and receiving the packets which lie in its communication region. So, the nodes stay away from the communication region and indicated in green color and the blue color indicates where the communication is carried out.

Retrieval Number: A4621119119/2019©BEIESP
DOI: 10.35940/ijitee.A4621.119119
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Without attack consideration

Fig. 5-7 illustrates the investigation of the performance without the existence of attacks under several measures. Fig. 5 states the results analyzed interms of energy. During the time period of 5s, the TQR model obtained a lower residual energy of around 31% whereas the LA and WOA achieved around 41% and 34% of remaining energy. In this case, the proposed approach could attain 55% remaining energy.

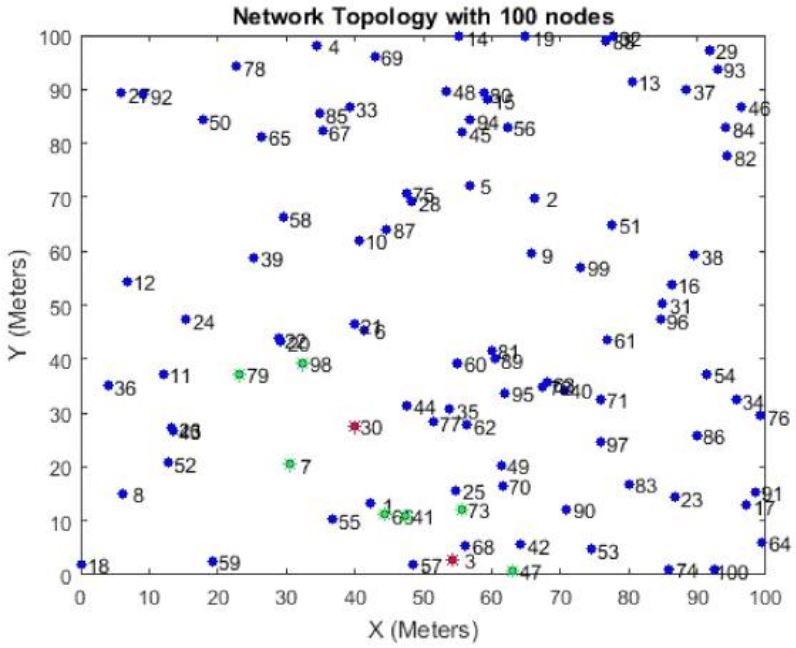

Fig. 4. Node deployment

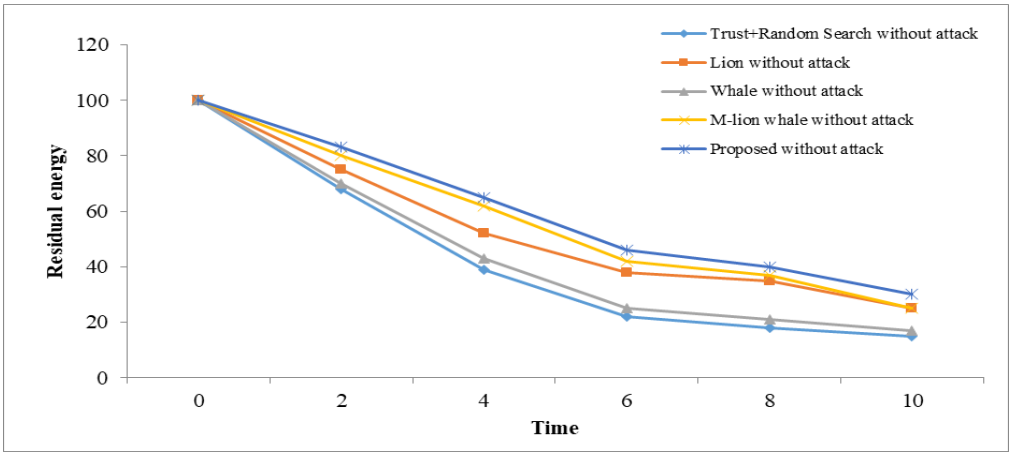

Fig. 5. Energy efficiency analysis without attack

From the figure, it is depicted that the TQR model is found to be inefficient and required maximum energy utilization over other methods. At the same time, the WOA showed slightly higher residual energy over TQR. However, it fails to show better results over the LA and MLW models. Then, the LA shows manageable results over TQR and WOA with moderate residual energy. But still, it shows inferior results over MLW and presented FLWO algorithms.

It is noted that the MLW manages well and attains high remaining energy. However, the presented FLWO algorithm obtains maximum remaining energy level over the other methods in a considerable way.

Fig. 6 states the results analyzed interms of throughput. During the time period of 5s, the TQR model obtained a throughput of around 0.128kbps whereas the LA and WOA achieved around 0.212kbps and 0.148kbps of throughput. From the figure, it is depicted that the TQR model is found to be inefficient and achieved minimum throughput utilization over other methods. At the same time, the WOA showed slightly higher throughput over TQR. However, it fails to show better results over the LA and MLW models. Then, the LA shows manageable results over TQR and WOA with moderate throughput. But still, it shows inferior results over MLW and presented FLWO algorithms. It is noted that the MLW manages well and attains high throughput. However, the presented FLWO algorithm obtains maximum throughput level over the other methods in a considerable way.

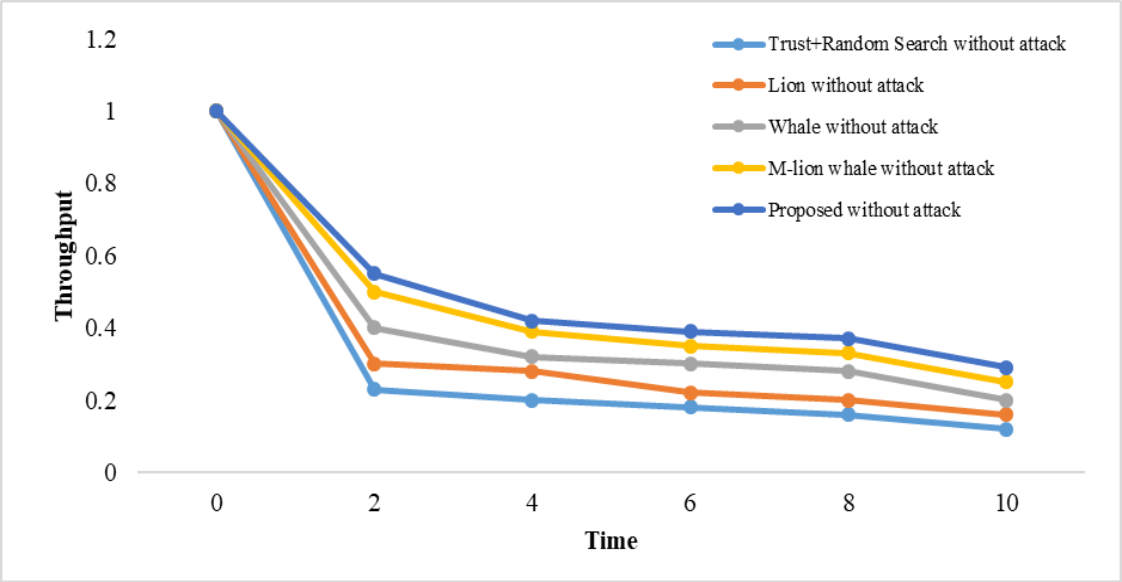

Fig. 6. Throughput analysis without attack

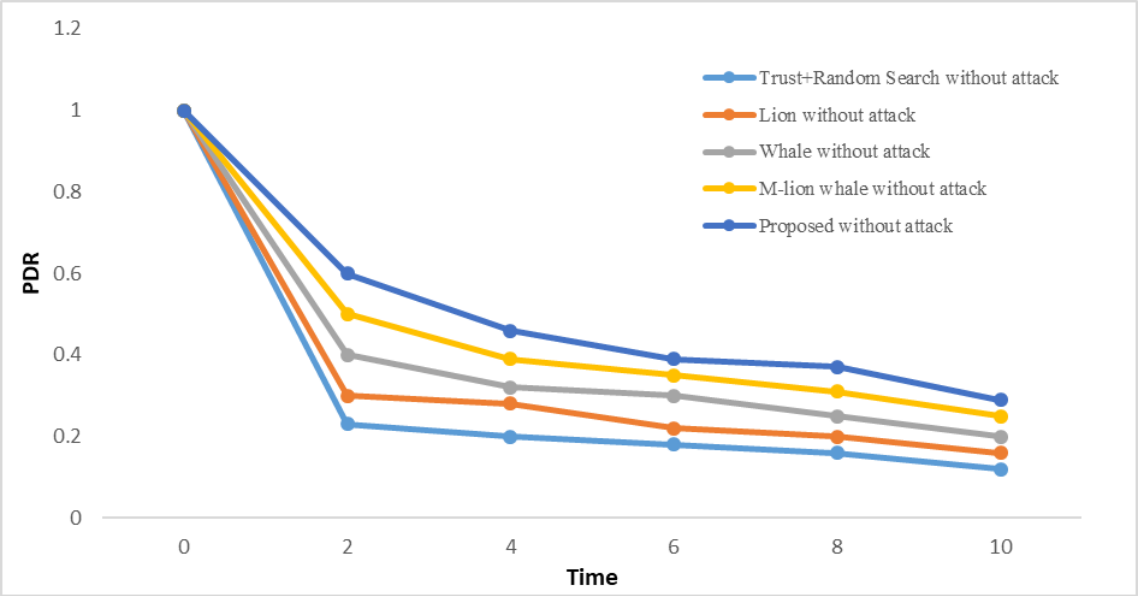

Fig. 7. PDR analysis without attack

Fig. 7 states the results analyzed interms of PDR. From the figure, it is depicted that the TQR model is found to be inefficient and achieved minimum PDR utilization over other methods. At the same time, the WOA showed slightly higher PDR over TQR. However, it fails to show better results over the LA and MLW models. Then, the LA shows manageable results over TQR and WOA with moderate PDR. But still, it shows inferior results over MLW and presented FLWO algorithms. It is noted that the MLW manages well and attains high PDR. However, the presented FLWO algorithm obtains maximum PDR level over the other methods in a considerable way.

With Attacks

Fig. 8-10 illustrates the investigation of the performance with the existence of attacks under several measures. From the analysis, it can be shown that the proposed algorithm attains maximum residual energy, throughput, and PDR than the existing methods. The cause of the effective results attained by the proposed method is due to the presence of fitness function. The solution with high trust, maximum energy, less delay, short distance, and maximum lifetime, makes the fitness maximum and thus, generates the optimal solution. In addition, the presented model utilizes the benefits of the LA as well as WOA algorithm.

Retrieval Number: A4621119119/2019©BEIESP
DOI: 10.35940/ijitee.A4621.119119
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

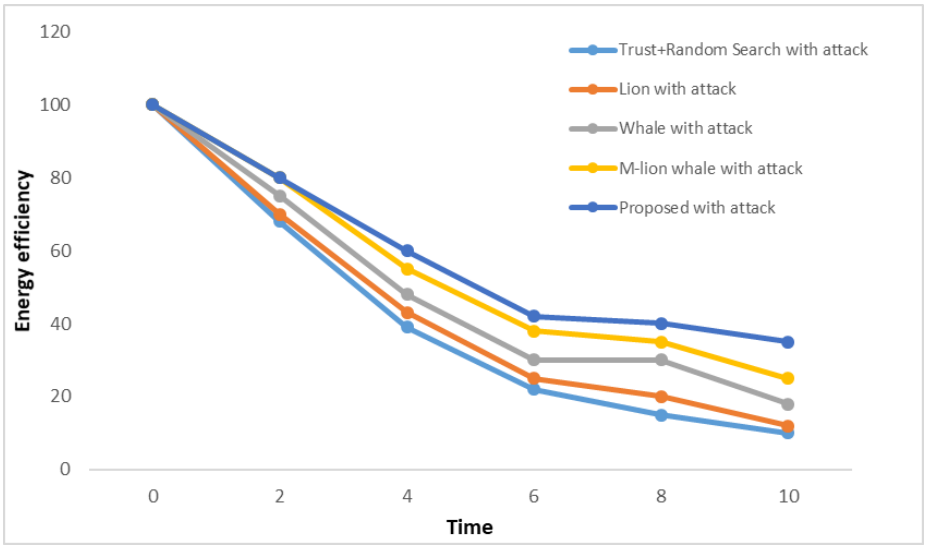

Fig. 8. Energy efficiency analysis without attack

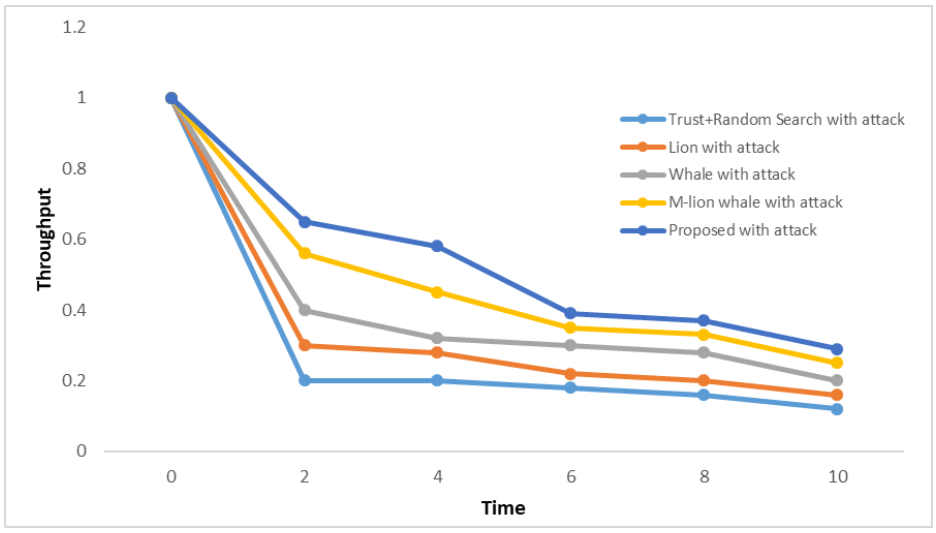

Fig. 9. Throughput analysis without attack

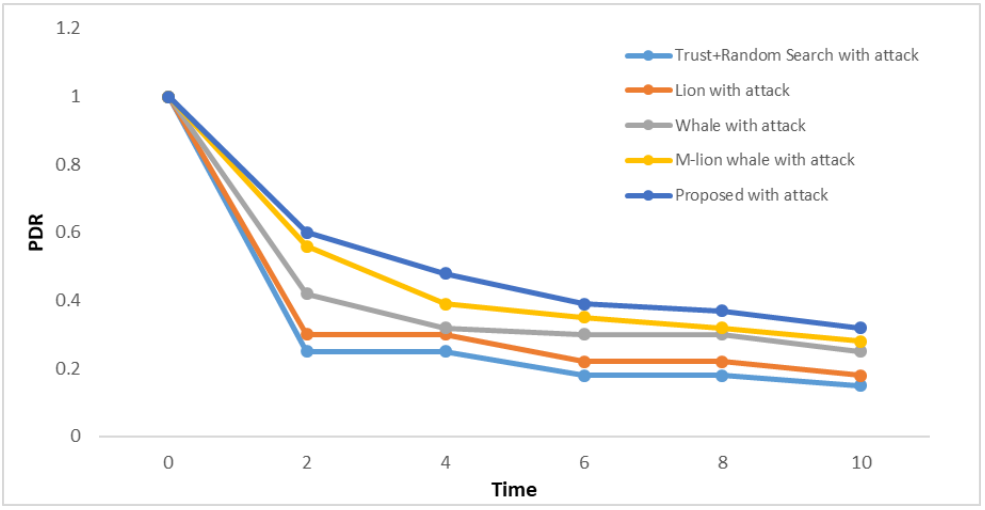

Fig. 10. PDR analysis without attack

IV. CONCLUSION

This paper has developed a MOO model for effective load distribution and security in the network. The presented FLWO technique operates on two main stages namely clustering and secure routing. In the first stage, fuzzy logic technique with multiple input parameters namely energy, distance, link duration, latency and trust are used for effective cluster construction. In the next stage, LWO algorithm is introduced for secure routing. The determined MOO variables, a fitness function is derived to select the optimal routes for secure routing in MANET. A detailed experimental analysis takes place to validate the results of the FLWO algorithm. The effective performance of the presented FLWO model is tested using a set of validation parameters and the proposed model attains maximum performance over other methods in a considerable way.

REFERENCES

1. Ertaul, L., Ibrahim, D.: 'Evaluation of secure routing protocols in mobile ad hoc networks (MANETs)', Security and Management, 2009, pp. 363–369
2. Dey, R, Saha, H.N.: 'Secure routing protocols for mobile ad-hoc network (MANETs) – a review', Int. J. Emerg. Trends Technol. Comput. Sci. (IJETTCS), 2016, 5, (1), pp. 74–79
3. Schweitzer, N., Stulman, A., Shabtai, A., et al.: 'Mitigating denial of service attacks in OLSR protocol using fictitious nodes', IEEE Trans. Mob. Comput., 2016, 15, (1), pp. 163–172
4. Hussain, Z., Balakrishna, R.: 'A survey on manets – types, characteristics, applications and protocols used'. National Conf. on Frontiers & Advances in Information Science and Technology, 2014
5. Muthusenthil, B., Murugavalli, S.: 'The impact of location based attacks on geographical routing protocols', J. Theor. Appl. Inf. Technol., 2014, 60, (2), pp. 189–199
6. Wang, B., Chen, X., Chang, W.: 'A light-weight trust-based QoS routing algorithm for ad hoc networks', Pervasive Mob. Comput., 2014, 13, pp. 164– 180
7. Rajan, C., Shanthi, N.: 'Genetic based optimization for multicast routing algorithm for MANET', Indian Acad. Sci., 2015, 40, (8), pp. 2341–2352
8. Persis, D.J., Robert, T.P.: 'Ant based multi-objective routing optimization in mobile AD-HOC network', Indian J. Sci. Technol., 2015, 8, (9), pp. 875–888
9. Ali, H., Shahzad, W., Khan, F.A.: 'Energy-efficient clustering in mobile adhoc networks using multi-objective particle swarm optimization', Appl. Soft Comput., 2012, 12, (7), pp. 1913–1928
10. Balachandra, M., Prema, K.V., Makkithaya, K.: 'Multiconstrained and multipath QoS aware routing protocol for MANETs', Wirel. Netw., 2014, 20, (8), pp. 2395–2408