International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-2, December 2019

Link breakage maintenance and power-aware secure routing in MANET based on the Fuzzy Krill Herd-based Grasshopper optimization

Nukam Reddy Srinadh, B. Satyanarayana

Abstract: ***As Mobile Ad hoc Networks (MANETs) are established using battery-powered nodes, the major concern to minimize the power consumption of the nodes is still a challenge while the lifetime of the network is taken into account. Thus, power-aware routing is the effective way to handle the situation that aims at minimizing the power consumption and network overhead in order to increase the network lifespan. Therefore, an effective power-aware secure routing protocol is designed using the proposed Fuzzy Krill Herd-based Grasshopper Optimization Algorithm (Fuzzy KH-GOA) such that the secure path is determined. Hence, it is evident that the routing path for transmitting the data packets is effectively decided using the proposed algorithm, which is based on the fitness parameters, such as fuzzy function, delay, distance, and power consumed by the path. The significance of this research relies on the link lifetime estimation for which the lifetime of the routes is detected in order to measure the link failure. The performance of the proposed Fuzzy KH-GOA reported the values of 23.858 J, 0.016 sec, 0.783, 0.840, and 10.908 sec, respectively in the absence of the attack and 22.624J, 22.624sec, 0.773, 0.812, and 9.862sec, respectively in the presence of attack for the measures, such as power, delay, Detection Rate (DR), throughput, and average Link Life Time.***

Keywords: Grasshopper Optimization Algorithm (GOA), Krill Herd algorithm, MANET, routing protocol, link breakage.

I. INTRODUCTION

MANET is an infrastructure-less network, which contains self organizing nodes such that each node acts a router in the ad hoc network. The mobile nodes operate independently as they do not require any centralized base station [1] [20] [21]. Hence, the ad hoc network is termed as "for this purpose" [4] [16] [17] [18]. The communication link used in the ad hoc network is broadcast, which is different from multicast, where the messages are broadcasted from the source node to the destination node [5] [12] [14] [15]. The malicious mobile nodes often misroute the data packets so that the high nodes having high mobility may damage and interrupt the data transmission. To protect the ad hoc network from the external and internal attacks is the basic need to be addressed properly [3] [22].

Revised Manuscript Received on December 30, 2019.
***** Correspondence Author
Nukam Reddy Srinadh*, Research Scholar, Rayalaseema University, Kurnool. & Assoc. Professor, Dept of CSE, VEC, Kavali, A.P, India. E-Mail : reddynsrs@gmail.com
Dr. B. Satyanarayana, Professor in Computer Science &Technology., Sri Krishnadevaraya University, Anantapur ,A.P , India. E-Mail : bachalasatya@yahoo.com

As the ad hoc networks are deployed easily, they are widely used in various applications, such as disaster relief operations, and military [1] [23].

When the mobile nodes lie in the same communication range then, each node communicates with other node through single-hop or multi-hop network. When the node in the ad hoc network moves out of the transmission range then, the link between the nodes will break. To solve the node failure and link breakage problem, the energy-efficient methods are introduced in MANET. When the power of mobile node decreases, the node moves to die and this problem can be controlled using the efficient power-aware routing (EPAR) approach. EPAR minimizes the consumption of power and eliminate the packet loss in single mobile node by selecting the path with maximum power [4] [19]. Most of the proposed routing protocols in MANET are based on the hop count metric such that it concerns only the shortest path and eliminate the solidity concerns. The link stability may affect due to the nodes mobility, residual energy, available bandwidth, and so on. These factors lead to route reconfiguration and link breakage in MANET. Hence, it is required to prefer stable path rather than selecting shortest path [6].Stability-based routing protocol is used to select the long-lasting path. Moreover, the parameters, such as pilot signals, relative speed, and signal strength are used for computing the link stability [7].

The research intends to concentrate on developing a power-aware secure routing protocol based on the proposed Fuzzy KH-GOA algorithm in order to enable the secure communication and in addition, the lifetime of the nodes are evaluated for ensuring the link breakage maintenance. The proposed Fuzzy KH-GOA algorithm selects the optimal path based on the maximization fitness function and the fitness parameters include delay, distance, fuzzy, and power consumed by the individual nodes in the path. The role of the fuzzy function in the proposed algorithm is that the fuzzy function boosts the performance through evaluating the mobility of the node, capability of the node, previous records, and reputation among the neighbors. Moreover, the link breakage mechanism is activated in the network using the lifetime parameters in order to maintain the communication link in the network. Thus, the proposed method concentrates in enabling the power and secure-aware communication in MANETs thereby, assuring the smooth communication with the help of the link breakage mechanism in MANETs.

The major contribution of this research is as follows:

The first contribution is regarding the power-aware secure routing protocol named as the proposed Fuzzy KH-GOA algorithm, which finds the route optimally for data transmission between the source and the target nodes. The path with less delay, minimum power consumption, less distance, and maximum fuzzy function is selected as the best path based on the maximization fitness objective. The proposed fuzzy KH-GOA is the integration of the fuzzy principle in the KH-GOA, which inherits the characteristics of Krill Herd (KH) and Grasshopper Optimization Algorithm (GOA).

The second contribution of the research is regarding the link breakage maintenance mechanism in MANET, which is activated in the network based on the lifetime parameters in order to assure the smooth performance of the network.

The rest of this paper is organized as: section 2 describes the existing methods of power-aware routing, and section 3 explains the mobility model of MANET. Section 4 elaborates the proposed optimization algorithm along with the link break maintenance. Section 5 discusses the results and discussion of the proposed algorithm, and finally, section 6 concludes the paper.

II. MOTIVATION

In this section, various existing routing protocols are discussed along with their merits and demerits. Moreover, the challenges associated with the routing techniques are explained.

2.1 Literature survey

Various existing power secure routing protocols are reviewed in this section. ChrispenMafirabadza and PallaviKhatri [1] developed an efficient power-aware AODV routing protocol to maximize the lifespan of network. It saved the nodes energy and attained better throughput and packet delivery ratio by reducing the dead nodes. This protocol was highly suitable in the high dense network and their performance was evaluated in terms of 100 and 300 nodes, but it consumed more battery power. Md. MahbuburRahman and Md. Akhtaruzzaman [2] introduced a power-aware routing approach to determine the network path in MANET. It used the combination of weighted metrics, like battery power, velocity, and distance to select the route. It effectively maximized the performance and lifespan of network. However, it failed to consider the packet loss. Mukherjee, S *et al.* [3] developed an enhanced average encounter rate AODV (EAER-AODV) protocol to select the optimal path in ad hoc network. The trust model in the routing protocol used the nodes opinion that contains distrust, uncertainty, and trust components. The source mobile node selected the reliable route by eliminating the malicious node. It attained better delivery ratio, but failed to consider the energy consumption. Femila, L. and Beno [4] modeled an efficient power-aware routing (EPAR) approach to distinguish the capacity of nodes by considering the battery power. The path with less cost was selected and the data rate was effectively controlled using this protocol. Moreover, the lifetime of the node was maximized and the energy consumption was reduced, but failed to consider the energy cost.

Gopinath, S *et al.* [5] developed a secure location-aware routing protocol in MANET. The key role of this approach was to select the multicast group in a secure manner. Moreover, the public key decryption and the encryption model were considered by deploying the security to protect the node from attackers. The parent or the source node broadcasted the data packet once it received the plain text. It attained better packet delivery, but failed to use the signcryption through certificateless routing. Singal, G *et al.* [6] developed a link stable multicast routing protocol to determine the lifespan of network. It computed the link stability factor and considered the path having maximum lifetime. The efficiency of protocol was enhanced by reducing the path length. Palaniappan, S. and Chellan, K [7] introduced an energy efficient routing protocol to provide reliable and stable route. The monitoring agents computed the link reliability factors to find the path with more reliability. It increased the delivery ratio of packet and decreased the energy consumption, but failed to reduce the delay. Jayalakshmi, V. and Razak, T.A [8] introduced a trust-based source routing protocol to find the route to meet the security requirement of packet transmission. It achieved significant enhancement in terms of packet delivery ratio. However, the trust decision attributes failed to incorporate the trust value.

2.2 Challenges

Some of the challenges associated with the existing power-aware secure routing protocols are discussed.

In the perspective of multihop ad hoc networks, selecting the optimal route among various routes in an effective and efficient way, poses a challenging issue in MANET [10].

Due to the characteristics, like unreservedly freely and dynamic topology, the link breakage arise frequently in MANET, which is the major complex issue in wireless network [9].

To ensure security in the ad hoc environment is a major challenge. Moreover, to implement end-to-end reliability, limited resources, and QoS mechanism were the challenging issues in MANET.

III. PROPOSED FUZZY KRILL HERD-BASED GRASSHOPPER OPTIMIZATION ALGORITHM FOR SECURE ROUTING IN MANET

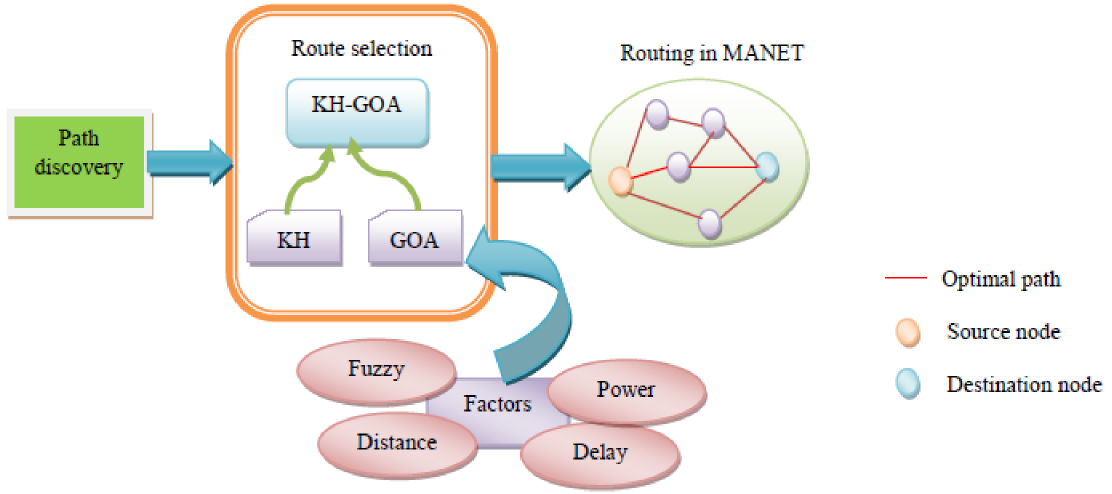

Figure 1. Block diagram of the proposed Fuzzy KH-GOA based secure routing in MANET

To transmit the data securely and to prevent the packet loss in MANET, it is necessary to have the secure routing mechanism in order to find the secure route to transmit the packet without any path conjunction. The link used to transmit the data packets can enable secure communication, which is

decided using the optimization algorithm. In this section, the secure routing initiated from the source

node to the target node is elaborated. Figure 1 shows the secure MANET routing.

The secure routing phenomenon involves three major steps, such as path discovery, optimization model, and optimal path discovery. Accordingly, the total number of the possible paths is discovered and then, the optimal route is selected using the proposed Fuzzy KH-GOA algorithm based on the fitness measure, such as delay, distance, power, and fuzzy factor. Once the optimal route is selected, the nodes communicate the data through the selected optimal path.

3.1 Solution encoding

The solution encoding is the representation of the solution to be determined using proposed algorithm. Let us consider w number of paths in MANET, among which the optimal path s is selected using the proposed Fuzzy KH-GOA approach such that s lies in the range of $1 \le s \le w$, respectively. The solution specifies w paths from which s optimal route is selected by the proposed algorithm based on the fitness value.

3.2 Fitness function

The fitness function is computed for all the possible w paths and the optimal route is selected based on the maximal value of the fitness using the proposed fuzzy KH-GOA. The path contributing towards less delay, maximum fuzzy function, minimum distance, and less power consumption is selected as the optimal path. The fitness measure is determined using the following equation.

$$F = \sum_{z=1}^{|k|} J_z \qquad (6)$$

where, z represents the total number of intermediate nodes in the selected path, k denotes the total nodes, and J_z indicates the node factor. The node factor is used to generate the secure path to transmit the information from source to target nodes. During path discovery, the stability of the nodes is evaluated based on the node factors, such as power, delay, distance, and fuzzy function. The node factor is represented as,

$$J_z = \frac{1}{4} \times \left[X_i^x + (1 - S_i) + (1 - \alpha_i) + (1 - \beta_i) \right] \qquad (7)$$

where, X_i^x denotes the fuzzy function, S_i represents the power consumed by i^{th} node, β_i indicates the delay of i^{th} node, and α_i represents the distance between i^{th} node and the previous node.

3.2.1 Fuzzy system

The fuzzy system [25] assists the selection of the optimal path in order to perform the data transmission in MANET by considering the input factors, such as previous record, node capability, node mobility, and reputation neighborhood. The input factors are fuzzified to select the optimal path for routing the packets. The steps involved in the fuzzy system are explained as follows:

i) Fuzzification: It receives the crisp input from the input variables and estimates a degree to which the input belongs to the specific fuzzy sets is called as fuzzification.

ii) Inference system: The fuzzified inputs are fed to the antecedents of fuzzy rule, which is further passed to the membership function. Finally, the outputs obtained from all the rules are combined.

ii) Defuzzification: The combined output of fuzzy set is fed as input to the Defuzzification, where the single crisp number is generated as output. The fuzzy function used to select the routing path is expressed as,

$$X_i^x = f\left(K_i^x, L_i^x, I_i^x, R_i^x\right) \tag{8}$$

where, X_i^x denotes the fuzzy function, x indicates current time, K_i^x indicates previous record, which means the history of i^{th} node at time x, L_i^x represents the mobility of node i at time x, I_i^x specifies the actual capability of i^{th} node at time x, R_i^x represents the reputation among neighbors of i^{th} node at time x, and f denotes fuzzy operator, respectively.

Previous records: To make the data transmission, the reputation system takes the input from the previous record, which is given as,

$$K_i^x = \frac{1}{2}\left[X_i^{x-1} + \frac{1}{2} \times X_i^{x-2}\right] \tag{9}$$

where, X_i^{x-1} denotes reputation value at time $x-1$, and X_i^{x-2} indicates reputation value at time $x-2$, respectively.

Node capability: It is defined as the ratio of total transmitted bytes to total capacity, which is expressed as,

$$I_i^x = \frac{H}{\gamma} \tag{10}$$

where, H is the total transmitted bytes, and γ is the total capacity.

Node mobility: The movement nodes specified as node mobility, where some node uses predefined path and some node moves randomly. Based on their responsibilities, the mobility of nodes is discovered, and is specified as arbitrary. When the nodes move fast, it affect the selection process of nodes, and when the movement of nodes is slow, it is easy to manage the neighborhood nodes. The mobility values obtain medium, low, and high value based on the movement of nodes as fast and steady. Based on the nodes location, the mobility factor is calculated as,

$$L_i^x = \frac{dist\left(Z_i^{x-1}, Z_i^x\right)}{\kappa} \tag{11}$$

where, $dist\left(Z_i^{x-1}, Z_i^x\right)$ indicates the difference between the location of i^{th} node at time $(x-1)$ and x, and κ represents normalization factor.

Reputation neighborhood: The total number of neighbor nodes situated close to the node is termed as reputation neighborhood. It is calculated using the below equation as,

$$R_i^x = \frac{1}{|J|}\sum_{r=1}^{|J|} J_{r,i} \tag{12}$$

where, $|J|$ denotes number of neighbors, and r is the neighboring node.

3.2.2 Power

The less power consumed by the mobile node is responsible to transmit the packets, which is computed using the Eq. (1)

3.2.3 Delay

The delay factor is computed based on the nodes available in the path, and the delay must be minimal for the optimal path. The delay is given as the ratio of number of nodes in the path to the total nodes, which is represented as,

$$\beta_i = \frac{\tau}{k} \tag{13}$$

where, τ represents the total number of nodes exist in the corresponding path, and k is the total nodes.

3.2.4 Distance

The distance is computed using the difference of distances between the i^{th} node and $(i-1)^{th}$ node with the normalization factor, which is expressed as,

$$\alpha_i = \frac{dist(i, i-1)}{\kappa} \tag{14}$$

where, κ denotes the normalization factor. The above factors are used to evaluate the fitness of the route to forward the data packets, such that the optimal fitness is computed to determine the optimal route using the proposed optimization algorithm.

3.3 Proposed Fuzzy Krill Herd-based Grasshopper Optimization Algorithm

The proposed Fuzzy KH-GOA is the integration of Grasshopper Optimization Algorithm (GOA) [28] and Krill Herd (KH) algorithm [27] to select the optimal path for data transmission in MANET. The proposed algorithm is effectively suitable in determining the optimal path for effective power-aware routing. KH algorithm simulates herding behavior of the krill individuals and the minimum distance of the krill towards the food source is considered as the objective function of the krill movement. The position of krill individuals are updated based on the factors, like foraging activity, random diffusion, and of movement other krill individuals. Here, the behavior of the krill is modeled using the adaptive genetic operators. Here, the individual krill move towards the optimal solution when it searches the food with high density. The swarming behavior of GOA enables the optimization algorithm to achieve effective performance in route selection. Due to the fine tuning of parameter, the proposed algorithm is considered as more effective than the nature-inspired optimization algorithms.

GOA balances the exploration and exploitation phase by changing the zone coefficient, which provides the GOA to be accurate in global medium rather than the local optima. GOA has the tendency to solve the optimization problems in the unknown search space. The integration of GOA with the KH algorithm is offered to select the optimal route effectively to increase the performance of optimization. The update equation of KH is modified with the GOA to compute the optimal solution. The algorithmic steps involved in the proposed KH-GOA algorithm are explained as follows:

i) Initialization: Initially, the algorithmic parameters, set of solution, and the termination criteria are defined. In the initialization phase, the solution size V with U solutions is randomly initialized. Each solution in the solution size V is specified as,

$$V = \{V_1, V_2, ..., V_g, ... V_U\} \tag{15}$$

where, U denotes the total population size that lies in the range of $1 \leq g \leq U$.

ii) Fitness evaluation: The fitness function is evaluated in the optimization algorithm to find the optimal solution. Here, the fitness function is computed based on the factors, like delay, power, distance, and fuzzy function using the Eq. (6). The solution with the best fitness value is accepted as the optimal solution.

iii) Update the solution: Let us consider the U number of solutions, which are generated in $w_{\max}$ iterations such that the best and worst solutions are generated. The updated solution contains the parameter that has the affinity to move towards the best solution by discarding the worst solution. According to KH algorithm, the position vector of the krill at the interval w and Δw is represented as,

$$V_g(w + \Delta w) = V_g(w) + \Delta w \frac{dV_g}{dw} \tag{16}$$

$$V_g(w) = V_g(w + \Delta w) - \Delta w \frac{dV_g}{dw} \tag{17}$$

where, $V_g(w)$ denotes g^{th} solution at w^{th} interval. However, the parameter Δw is carefully set in the optimization problem as this parameter acts as a scale factor. GOA updates the position based on the grasshopper position, target location, and current position. The location of search agent is describes through the grasshopper status with respect to the target position. Hence, the update equation of grasshopper is represented as,

$$V_g^p(w + \Delta w) = y\left(\sum_{\substack{k=1 \\ k \neq g}}^{U} y \frac{W_p - Y_p}{2} h\left(\left|V_k^p - V_g^p\right|\right) \frac{V_k - V_g}{m_{gk}}\right) + \hat{Q}_p^* \tag{18}$$

where, y represents decreasing coefficient, p indicates dimension, U is the total number of grasshoppers with the dimension p, k and g indicates the location of grasshopper. W_p and Y_p are the upper and lower bound at dimension p. h indicates the strength of social forces, m_{gk} denotes the distance between two grasshoppers, and Q_p^* is the best solution. Let us assume $U = 1$,

$$V_g^p(w + \Delta w) = y^2 \frac{W_p - Y_p}{2} h\left(\left|V_1^p - V_g^p\right|\right) \frac{V_1(w) - V_g(w)}{m_{g1}} + \hat{Q}_p^* \tag{19}$$

By substituting the Eq. (17) in Eq. (19), the resulted updated equation is expressed as,

$$V_g^p(w + \Delta w) = y^2 \frac{W_p - Y_p}{2} h\left(\left|V_1^p - V_g^p\right|\right) \frac{V_1(w) - V_g(w + \Delta w) + \Delta w \frac{dV_g}{dw}}{m_{g1}} + \hat{Q}_p^* \tag{20}$$

After rearranging the above equation is represented as,S

$$V_g^p(w + \Delta w) + y^2 \frac{W_p - Y_p}{2} h\left(\left|V_1^p - V_g^p\right|\right) \frac{V_g(w + \Delta w)}{m_{g1}} = y^2 \frac{W_p - Y_p}{2m_{g1}} h\left(\left|V_1^p - V_g^p\right|\right)\left[V_1(w) + \Delta w \frac{dV_g}{dw}\right] + \hat{Q}_p^* \tag{21}$$

$$V_g^p(w + \Delta w)\left[1 + y^2 \frac{W_p - Y_p}{2m_{g1}} h\left(\left|V_1^p - V_g^p\right|\right)\right] = y^2 \frac{W_p - Y_p}{2m_{g1}} h\left(\left|V_1^p - V_g^p\right|\right)\left[V_1(w) + \Delta w \frac{dV_g}{dw}\right] + \hat{Q}_p^* \tag{22}$$

$$V_g^p(w + \Delta w) = \frac{2m_{g1}}{2m_{g1} + y^2 W_p - Y_p h\left(\left|V_1^p - V_g^p\right|\right)} \left\{y^2 \frac{W_p - Y_p}{2m_{g1}} h\left(\left|V_1^p - V_g^p\right|\right)\left[V_1(w) + \Delta w \frac{dV_g}{dw}\right] + \hat{Q}_p^*\right\} \tag{23}$$

iv) Replace the best solution: Once the position is updated based on the fitness value, the solution that yields the maximum fitness is replaced as the optimal solution.

v) Termination: The above steps are repeated until the best solution is obtained until the maximum iteration $w_{\max}$. Algorithm 1 shows the pseudo code of the proposed Fuzzy KH-GOA algorithm.

Algorithm 1. Pseudo code of the proposed Fuzzy KH-GOA algorithm

Sl. No	Pseudo code of proposed Fuzzy KH-GOA
1	**Input:** Population V
2	Determine the optimal solution Q_p^*
3	Begin
4	Population initialization
5	Update W_p, Y_p, y, h, and m

while $w < w_{\max}$	
for $[1 \le g \le U]$	
Compute F using the Eq. (6)	
Update $V_g^p(w+\Delta w)$ using Eq. (23)	
Generate new solution	
Reevaluate F	
Compute Q_p^*	
$w = w+1$	
end while	
return Q_p^*	
Terminate	

3.4 Link breakage Maintenance

After selecting the secure route using the proposed Fuzzy KH-GOA, the lifetime of the nodes is calculated. While transmitting the data to the neighboring hop, it is required to detect if its link to the neighboring hop is broken. When the node considered that the link is broken then, the link breakage maintenance process is carried out by calculating the lifetime of the routes. During the route traversal of data packet, the lifetime of the route is computed at each hop. Each node computes the lifetime of the route between itself and the previous hop. However, the LLT of the node is calculated as,

$$\xi = \frac{-(\tau\mu + \vartheta\omega) + \sqrt{(\tau^2 + \vartheta^2)r^2 - (\tau\omega - \vartheta\mu)^2}}{(\tau^2 + \vartheta^2)} \quad (24)$$

where, $\tau = a_u^s \cos\theta_{a_u} - a_v^s \cos\theta_{a_v}$, $\mu = a_u^{c_1} - a_v^{c_1}$, $\vartheta = a_u^s \sin\theta_{a_u} - a_v^s c \sin\theta_{a_v}$, and $\omega = a_u^{c_2} - a_v^{c_2}$, respectively. Here, $(a_u^{c_1}, a_u^{c_2})$ denotes the coordinate of node a_u, $(a_v^{c_1}, a_v^{c_2})$ represents the coordinate the node a_v, θ_{a_u} represents the direction of motion of node a_u, θ_{a_v} indicates the direction of motion of node a_v, a_u^s denotes the mobility speed of node a_u, a_v^s indicates the mobility speed of node a_v, respectively. Based on the rate of link failure, the link breakage is identified [25] [24]. The link reliability is computed using the below equation as,

$$\mathrm{P}(q) = e^{-\lambda q} \quad (25)$$

where, P is the probability, q denotes the time at which the link is work, and λ represents the average link failure rate. Average link failure rate is the inverse of lifetime of the route, which is specified as,

$$\lambda = \frac{1}{s} \quad (26)$$

where, s denotes the link lifetime. The average link failure rate is compared with the threshold τ in order to decide to transmit the data using the selected route or to perform the re-routing process. When $\lambda > \tau$, re-routing is done to transmit the data from the source node to the target node, and if $\lambda < \tau$, then the node transmit the data in the selected route.

IV. RESULTS AND DISCUSSION

The results and discussion made using the proposed algorithm is explained in this section with respect to the evaluation metrics.

4.1 Experimental setup

The implementation of the proposed Fuzzy KH-GOA algorithm is carried out in the NS2 simulator using windows 10 OS with 2 GB Ram, and Intel processor.

4.2 Evaluation metrics

The performance achieved by the proposed algorithm is analyzed and evaluated using the metrics, like power, delay, detection rate, LLT and throughput.

Power: The node used to transmit the data requires high power and the power consumed by the proposed algorithm is specified using the Eq. (1)

Delay: It is the time taken by the packet to travel from source to destination, which is computed using the Eq. (13).

Throughput: It is the amount of data packets received by the destination at a specific time, which is calculated as,

$$\eta = \frac{\nu}{\mu} \quad (27)$$

where, ν is the number of packets received at time μ.

Link Life Time (LLT): It defines the lifetime of the link in network, which is calculated at each hop while traversing the route request. Each node computes the lifetime of the route between itself and the previous hop.

Detection rate: It is defined as the ratio of number of malicious nodes detected accurately to the total number of nodes in network.

4.3 Comparative methods

The performance enhancement of the proposed algorithm is revealed by comparing the proposed with the existing methods, like Fuzzy Reputation dynamic source routing (FR-DSR) [30], Ad hoc On-demand Multi-path Distance Vector protocol-Secure Adjacent Position Trust Verification (AOMDV-SAPTV) [29], and secure reputation based routing [31], respectively.

and KH-GOA based routing is 0.7125, 0.714, 0.704, and 0.753, while the proposed Fuzzy KH-GOA obtained better throughput rate of 0.801, respectively.

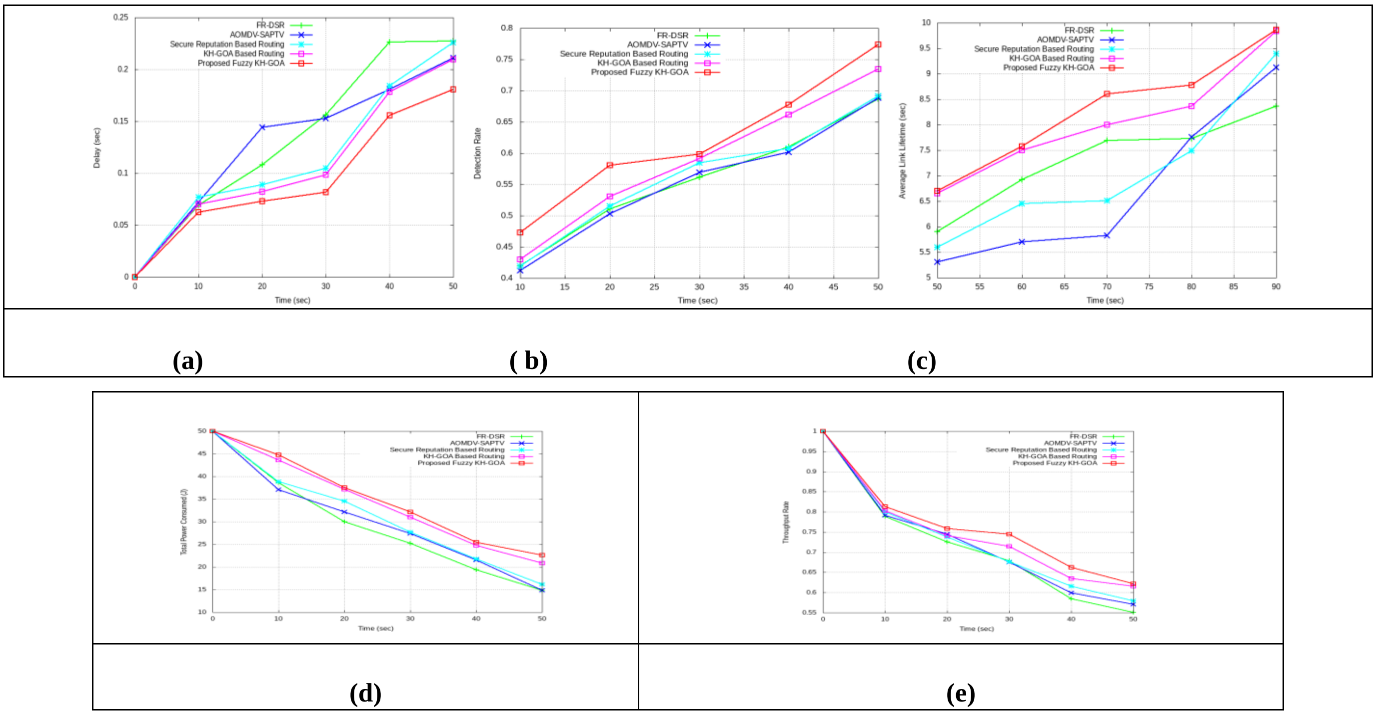

Figure 2. Comparative analysis with attack, a) delay, b) DR, c) average LLT, d) total power consumed, e) throughput rate

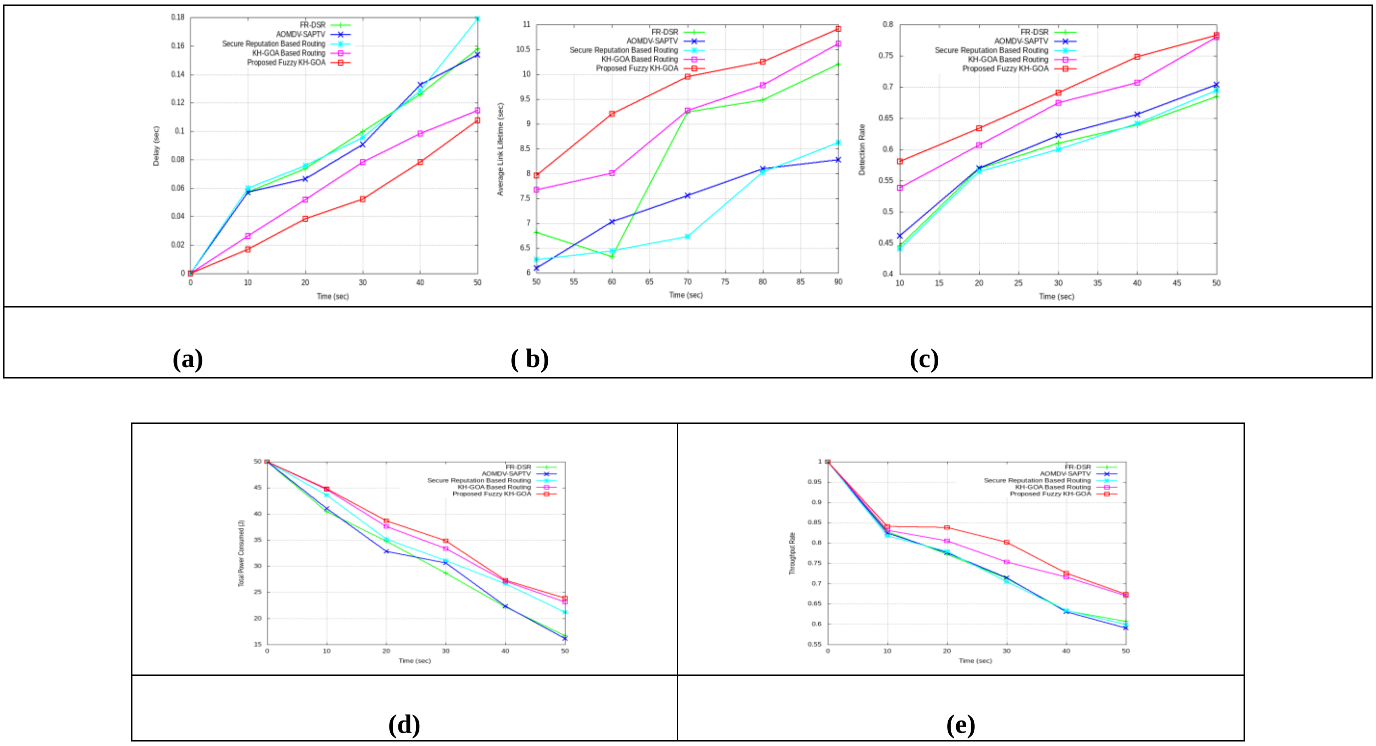

Figure 3. Comparative analysis without attack, a) delay, b) DR, c) average LLT, d) total power consumed, e) throughput rate

4.4 Comparative discussion

Table 1 represents the comparative discussion of the proposed algorithm. It is clearly depicted that the proposed obtained significantly better performance in the presence/absence of network attack. The delay obtained by the existing methods, like FR-DSR, AOMDV-SAPTV, Secure reputation based routing, and KH-GOA based routing is 0.069sec, 0.071sec, 0.076sec, and 0.070sec, while the proposed Fuzzy KH-GOA obtained lower delay of 0.062sec for 10sec in the presence of the attack. The average LLT obtained by the existing methods, like FR-DSR, AOMDV-SAPTV, Secure reputation based routing, and KH-GOA based routing is 8.369sec, 9.127sec, 9.391sec, and 9.837sec, while the proposed Fuzzy KH-GOA obtained the average LLT of 9.862sec for 90sec in the presence of the attack. The throughput rate obtained by the existing methods, like FR-DSR, AOMDV-SAPTV, Secure reputation based routing, and KH-GOA based routing is 0.827, 0.824, 0.817, and 0.831, while the proposed Fuzzy KH-GOA obtained better throughput of 0.840 for 10sec in the absence of the attack.

Table 1. Comparative discussion

Metrics/Methods			FR-DSR	AOMDV-SAPTV	Secure reputation based routing	KH-GOA based routing	proposed Fuzzy KH-GOA
With attack	time=10sec	*Delay*	0.069	0.071	0.076	0.070	0.062
	time=50sec	*DR*	0.686	0.688	0.691	0.734	0.773
	time=90sec	*Average LLT*	8.369	9.127	9.391	9.837	9.862
	time=50sec	*Power*	14.849	14.842	16.156	20.869	22.624
	time=10sec	*Throughput rate*	0.7891	0.791	0.799	0.802	0.812
Without attack	time=10sec	*Delay*	0.057	0.057	0.059	0.026	0.016
	time=50sec	*DR*	0.684	0.704	0.694	0.780	0.783
	time=90sec	*Average LLT*	10.198	8.277	8.628	10.619	10.908
	time=50sec	*Power*	16.713	16.127	21.223	23.160	23.858
	time=10sec	*Throughput rate*	0.827	0.824	0.817	0.831	0.840

V. CONCLUSION

In this research, an effective Fuzzy Krill Herd-based Grasshopper Optimization Algorithm is proposed to enable the optimal power-aware secure routing in MANET and finally, the link breakage maintenance mechanism is initiated in the research in order to sustain the effective lifetime of the network throughout the communication process. The optimal path is computed based on the fitness measures particularly, with minimum delay and energy. The optimal path ensures the routing mechanism in a robust and efficient manner. Hence, the secure power-aware routing protocol developed and the link breakage maintenance phenomenon initiated in the research is reported as the remarkable point of attraction to extend the lifetime of the network. The analysis of the methods reveal that the proposed Fuzzy Krill Herd-based Grasshopper Optimization Algorithm attained better performance with values of 23.858 J, 0.016 sec, 0.783, 0.840, and 10.908 sec for the metrics, like power, delay, Detection Rate, throughput, and average Link Life Time (LLT) in the absence of the attack scenario, and 22.624J, 22.624sec, 0.773, 0.812, and 9.862sec in the presence of attack scenario. In future, the performance of routing and lifetime maintenance shall be enhanced through any other hybrid algorithms of optimization and immune computing algorithms.

REFERENCES

1. ChrispenMafirabadza and PallaviKhatri, "Efficient Power-aware AODV Routing Protocol for MANET," Wireless Personal Communications, vol. 97, no. 4, pp. 5707-5717, 2017.
2. Md. MahbuburRahman and Md. Akhtaruzzaman, "An Efficient Position based Power-aware Routing Algorithm in Mobile Ad-hoc Networks," International Journal of Computer Network and Information Security, vol. 7, pp. 43-49, 2016.
3. Mukherjee, S., Chattopadhyay, M., Chattopadhyay, S. and Kar, P., "EAER-AODV: Enhanced Trust Model Based on Average Encounter Rate for Secure Routing in MANET," in Advanced Computing and Systems for Security, pp. 135-151, May 2018.
4. Femila, L. and Beno, M.M., “Optimizing Transmission Power and Energy Efficient Routing Protocol in MANETs”, Wireless Personal Communications, vol. 106, no. 3, pp.1041-1056, 2019.
5. Gopinath, S., Kumar, K.V. and Sankar, T.J., “Secure location aware routing protocol with authentication for data integrity”, Cluster Computing, pp.1-10, 2018.
6. Singal, G., Laxmi, V., Gaur, M.S., Todi, S., Rao, V., Tripathi, M. and Kushwaha, R., “Multi-constraints link stable multicast routing protocol in MANETs”, Ad Hoc Networks, vol. 63, pp.115-128, 2017.
7. Palaniappan, S. and Chellan, K., “Energy-efficient stable routing using QoS monitoring agents in MANET”, EURASIP Journal on Wireless Communications and Networking, no. 1, p.13, 2015.
8. Jayalakshmi, V. and Razak, T.A., “Trust based power-aware secure source routing protocol using fuzzy logic for mobile adhoc networks”, IAENG International Journal of Computer Science, vol. 43, no. 1, pp.98-107, 2016.
9. Choksi, Y., Tandel, P. and Khatri, T., “AODV modification to address link breakage issue: A review”, IEEE International Conference on Trends in Electronics and Informatics (ICEI), pp. 576-578, May 2017.
10. Shin, H.H., Lee, S. and Kim, B.S., “Performance Improvement Using Self-Link-Breakage Announcement in Wireless Ad-hoc Networks”, IEEE International Conference on Computational Science and Engineering, pp. 208-212, December 2013.
11. Malathi, M. and Jayashri, S., “Robust against route failure using power proficient reliable routing in MANET”, Alexandria Engineering Journal, vol. 57, no. 1, pp.11-21, 2018.
12. Patel, V.H., Zaveri, M.A. and Rath, H.K., “Trust based routing in mobile ad-hoc networks. Lecture Notes on Software Engineering, vol. 3, no. 4, p.318, 2015.
13. Maleki, M., Dantu, K. and Pedram, M., “Power-aware source routing protocol for mobile ad hoc networks”, ACM Proceedings of the international symposium on Low power electronics and design, pp. 72-75, August 2002.
14. Singh, P. and Singh, G., “Security issues and link expiration in secure routing protocols in MANET: a review”, International Journal of Advanced Research in Computer and Communication Engineering, vol. 3, no. 7, 2014.
15. Maxa, J.A., Mahmoud, M.S.B. and Larrieu, N., “Secure routing protocol design for uav ad hoc networks”, IEEE/AIAA 34th Digital Avionics Systems Conference (DASC), pp. 4A5-1, September 2015.
16. Akhtar, A.M., Nakhai, M.R. and Aghvami, A.H., “Adaptive power-aware routing in wireless mesh networks”, IEEE 73rd vehicular technology conference (VTC Spring), pp. 1-5, May 2011.
17. Bhople, N.B. and Waghmare, J.M., “Energy routing protocol with power utilization optimization in MANET”, IEEE international conference on recent trends in electronics, information & communication technology (RTEICT), pp. 1371-1374, May 2016.
18. Zhu, J. and Wang, X., “Model and protocol for energy-efficient routing over mobile ad hoc networks”, IEEE Transactions on Mobile Computing, vol. 10, no. 11, pp.1546-1557, 2010.

19. Rishiwal, V., Verma, S. and Bajpai, S.K., "QoS based power-aware routing in MANETs", International Journal of Computer Theory and Engineering, vol. 1, no. 1, p.49, 2009.
20. Vijayakumar, P. and Poongkuzhali, T., "Efficient power-aware broadcasting technique for mobile ad hoc network", Procedia Engineering, vol. 30, pp.782-789, 2012.
21. Yitayal, E., Pierson, J.M. and Ejigu, D., "A balanced battery usage routing protocol to maximize network lifetime of MANET based on AODV", In International Conference on Next Generation Wired/Wireless Networking, Springer, Cham, pp. 266-279, August 2014.
22. Feng, R., Che, S., Wang, X. and Yu, N., "A credible routing based on a novel trust mechanism in ad hoc networks", International Journal of Distributed Sensor Networks, vol. 9, no. 4, p.652051, 2013.
23. Raza, I. and Hussain, S.A., "Identification of malicious nodes in an AODV pure ad hoc network through guard nodes", Computer Communications, vol. 31, no. 9, pp.1796-1802, 2008.
24. Balachandra, M., Prema, K.V. and Makkithaya, K., "Multiconstrained and multipath QoS aware routing protocol for MANETs", Wireless networks, vol. 20, no. 8, pp.2395-2408, 2014
25. Palaniappan, S. and Chellan, K., "Energy-efficient stable routing using QoS monitoring agents in MANET", EURASIP Journal on Wireless Communications and Networking, no. 1, p.13, 2015.
26. Tantubay, N., Gautam, D.R. and Dhariwal, M.K., "A review of power conservation in wireless mobile adhoc network (MANET)", International Journal of Computer Science Issues (IJCSI), vol. 8, no. 4, p.378, 2011.
27. Gandomi, A.H. and Alavi, A.H., "Krill herd: a new bio-inspired optimization algorithm", Communications in nonlinear science and numerical simulation, vol. 17, no. 12, pp.4831-4845, 2012.
28. Saremi, S., Mirjalili, S. and Lewis, A., "Grasshopper optimisation algorithm: theory and application", Advances in Engineering Software, vol. 105, pp.30-47, 2017.
29. Borkar, G.M. and Mahajan, A.R., "A secure and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks," Wireless Networks, vol. 23, no.8, pp.2455-2472, 2017.
30. Menaka, R., V. Ranganathan, and B. Sowmya, "Improving Performance Through Reputation Based Routing Protocol for MANET," Wireless Personal Communications, Vol. 94, No. 4, pp. 2275–2290, 2017.
31. S. Sharma, "A secure reputation based architecture for MANET routing," in proceedings of 4th International Conference on Electronics and Communication Systems (ICECS), Coimbatore, pp. 106-110, 2017.
32. Yadav, A.K. and Tripathi, S., "QMRPRNS: Design of QoS multicast routing protocol using reliable node selection scheme for MANETs", Peer-to-Peer Networking and Applications, vol. 10, no. 4, pp.897-909, 2017.

AUTHORS PROFILE

Mr. Nukam Reddy Srinadh received his B.Sc Degree in Mathematics, Physics and Chemistry from Sri Venkateswara University,Tirupti, A.P , India in 1997, Master of Computer Applications from Sri Venkateswara University in 2000,Master Of Technology in computer science Engineering From AAIDU in 2006. Now He is pursuing Ph.D. from Rayalaseema University, Kurnool , AndhraPradesh, India. His research areas include Computer Networks/Secure Routing in MANET.

Prof. B. Sathyanarayana received his B.Sc Degree in Mathematics, Economics and Statistics from Madras University, India in 1985, Master of Computer Applications from Madurai Kamaraj University in 1988. He did his Ph.D in Computer Networks from Sri Krishnadevaraya University, Anantapur, A.P. India. He has 24 years of teaching experience. His Current Research Interest includes Computer Networks, Network Security and Intrusion Detection. He has published 30 research papers in National and International journals.