An Energy Efficient Trust Based Secure Routing Protocol for Wireless Sensor Network

Syed Mohd Ali
Research Scholar, ECE Department, JNTUH, India

Dr. Syed Abdul Sattar
Principal NSAKCET, Hyderabad, India

Dr. D. Srinivasa Rao
Professor ECE Department JNTUH India

Abstract- The rapid development in WSNs has encouraged the growth of less power-equipment and low-cost devices including sensing equipment and signal processing devices. This provides the capability to process WSN nodes for initiating wireless communication. One of the major drawbacks is the energy consumption in the WSN environment as the node consumes more energy to transmit the data. This evolves the representation of proper routing strategy while transmission. However, security becomes the most important criteria in routing, which must be critically ensured for secure data transmission. This paper aims to propose a novel energy efficient trust based secure routing protocol. Here, the optimal route selection is carried out by the new Improved Lion Algorithm (ILA). Thereby the considered constraints include energy, delay, link lifetime, trust model. Moreover, the trust model includes the parameters like integrity factors, direct trust, forwarding rate factor, and indirect trust to maintain the security of routing process.

Keywords – Wireless Sensor Network, Data Transmission, Optimal Route selection, Trust Model, Optimization.

Nomenclature

Abbreviation	Description
ACO	Ant Colony Optimization
ABC	Artificial Bee Colony
BS	Base Station
C-SSA	Cat Salp Swarm Algorithm
CH	Cluster Head
CCR	Congestion-aware Clustering and Routing
DT	Decision Tree
EATSRA	Energy Aware Trust based Secure Routing Algorithm
ER-SR	Energy efficient Region Source Routing
E-BEENISH	Enhanced Balanced Energy Efficient Network-Integrated Super-Heterogeneous
FCM	Fuzzy C-Means
GA	Genetic Algorithm
I-SEP	Improved -Stable Election Protocol
LEACH	Low Energy Adaptive Clustering Hierarchy

LA	Lion Algorithm
MOFPL	Multi-Objective Fractional Particle Lion
PSO	Particle Swarm Optimization
PCH	Primary Cluster Head
PDR	Packet Delivery Ratio
SEP	Stable Election Protocol
SCH	Secondary Cluster Head
WSN	Wireless Sensor Network

I. INTRODUCTION

WSN includes group of sensors linked in the wireless medium. Furthermore, the WSN system was powered through the BS that acted as the access point for the set of the sensor devices [9]. Some of the applications of WSN are field surveillance, weather monitoring, and the meteorological data collection, the real-time applications including commerce, industry, health-care, science, military, and transportation. Here, the WSNs efficiency directly depends on the present sensor quality [11]. However, WSN sensors do affect mainly by the different noise factors from both the external as well as the internal environments [12]. The noise present in the nearby hardware components of WSN mainly affects the performance of sensor nodes. Further, the sensor nodes were separated by maximum distances in WSN, and the communication among the sensor nodes are attained with low power in the wireless channels [13] [14].
Routing in the WSN is defined as the way of transmitting the packets among the BS and the sensor nodes by the wireless communication medium [15]. However, the major drawback is the energy consideration of every sensor nodes in the routing process. However, the WSNs lifetime depends on the every sensor nodes energy, and hence the routing protocol must increase the network lifetime by the proper routing of the nodes in the WSN [16] [17]. Based on the reception and the transmission of the message packets, the energy present in the nodes should be reduced in WSN [37] [38]. The routing protocols is divided on the basis of network parameters like network topology, working mode of the nodes, each node participation in the WSN, and the different clustering methods [18] [19]. Moreover, the implementation of the routing protocol depends mainly on the certain factors like scalability, security, node deployment, energy consumption, connectivity, and coverage, respectively.
For enhancing the life time of the sensor network, the energy aware routing protocols with optimization algorithms [41] [42] are used. Most of the researchers examined the biological species as an analogy used for the natural representation to solve the optimization problem. ACO algorithm simulating the ant colony manors and it is applied in different optimization problems of WSN routing [20] [39] [40]. In addition, other optimization algorithms like GA, PSO are used for multi-path routing. The main objective is to develop an energy efficient multi-hop routing protocol [21] [22] for WSN by the Meta heuristic algorithms. Moreover, cluster based routing is also a routing strategy that works with optimization concept for making the CH selection more optimal [23] [24].

The major contributions of the adopted methodology are given below:

- Proposes a new Energy Efficient trust based secure routing model considering various trust model along with energy consumption. These constraints are cumulatively considered as the single objective for selecting the optimal route.
- To solve this optimization issue, a new improved lion algorithm (ILA) is proposed in this work.

In this paper, Section 2 indicates the literature review on secure and energy efficient routing protocol in WSN. Section 3 signifies the proposed Energy efficient trust based secure routing model: step by step process flow. Section 4 depicts the identification of optimal route via improved lion algorithm. Section 5 depicts the results and their discussions. Finally, the conclusion to this proposed work is given in the section 6.

II. LITERATURE REVIEW

2.1. Related Works

In 2019, Vinitha *et al.* [1] have presented Taylor based C-SSA for addressing the energy problems and it offered an efficient WSN multi-hop routing. Moreover, the proposed method consists of two different stages to obtain the multi-hop routing that consists of data transmission and CH selection. The energy-efficient CHs were chosen by the LEACH protocol for transmitting the data effectively. In addition, the data transfers from the sensor node to the CH by the selected optimal hop and CH transmit it to BS.

Further, the selection of optimal hop was performed by the adopted Taylor C-SSA, and the trust model was done using the security aware multi-hop routing. Finally, the performance of the presented method have shown better throughput, high energy, less delay, and maximum alive node than other conventional models.

In 2019, Reeta *et al.* [2] have proposed the MOFPL algorithm for the energy-aware routing purpose. Moreover, the multi-objective fitness function was defined by the proposed model to select the optimal CH in the routing process with respect to the traffic rate, delay, distance, energy, and the cluster density. In the WSN, the optimal CH was identified from the different CH nodes by the adopted MOFPL algorithm, and the proposed multi-objective function would establish the optimal routing path. At last, the proposed MOFPL model have proven maximum number of alive nodes, less traffic rate, higher normalized network energy, and lower delay.

In 2019, Xu *et al.* [3] have introduced a new ER-SR protocol for enhancing the network lifetime in the WSN. Furthermore, the algorithm based on the distributed energy region was implemented in ER-SR for selecting the nodes with maximum residual energy. For each node, the optimal source routing path was calculated using the source routing nodes that balance the energy consumed in sensor nodes and allow some nodes to take part in the routing. Moreover, an effective distance-based ACO algorithm was implemented to search the optimal transmission path for reduced energy consumption. Finally, the experimental outcomes of the proposed model has achieved better consumption of energy, increased network lifetime, better PDR, and lower delay, respectively.

In 2019, Farsi *et al.* [4] have introduced the CCR protocol for alleviating the congestion problems in the network. Moreover, the adopted CCR protocol has included 2 major phases: transmission phase and the setup phase. Here, the feature includes reliability, stability, low overhead, scalability, fault tolerance and Load Distribution were considered. For improving the network lifetime and reducing the end-to-end delay time, the CCR protocol was implemented by selecting the appropriate SCH and the PCH. Finally, the simulation outcomes of the proposed model has attained maximum network lifetime, lower network bandwidth, minimum overflow of data, and higher number of packets.

In 2019, Zhang *et al.* [5] have suggested an E-BEENISH routing protocol to analyze the communication for the energy levels in heterogeneous WSNs and energy consumption of the clusters. In addition, the E-BEENISH was based on the weighted election probability of every node as a CH as per the distance and the residual energy from the sink to node. The heterogeneity parameters were captured the imbalanced energy in the network by learning the sensitivity of the stable election protocol, and then identified the longer stability region of E-BEENISH for the distance and the appropriate weight of energy. The performance of the proposed model has proven improved system lifetime, longer stability, largest throughput, increased residual energy, and better adaptability than other existing schemes.

In 2020, Behera *et al.* [6] have proposed an improved routing protocol known as I-SEP in the heterogeneous WSN for environmental monitoring. Further, the threshold energy value has decided the corresponding cluster and the CH continue or change the transmission at the next round. The distributed routing algorithm was suitable for the heterogeneous network in which the sensors were deployed with more energy levels. Moreover, the modified SEP was the proposed algorithm suitable for IOT based on environmental monitoring. The protocol has switched the energy levels among the member nodes and the CH nodes that save the energy in the network, and the threshold remains the uniform energy distribution. At last, the experimental outcomes of the adopted method have achieved better throughput improved network lifetime, and less number of dead nodes than other traditional schemes.

In 2020, Wang *et al.* [7] have introduced the clustering algorithm, which selects the CH by an improved ABC algorithm. For solving the clustering issues in WSNs, the CH location, CH density, network CH energy, and other similar factors were implemented in the proposed algorithm. In addition, each node has the similar energy level during the network initialization period, in which the improved ABC algorithm was used for optimizing the FCM clustering. Finally, the outcomes of the adopted model has proven with improved energy efficiency, better network throughput, maximum network life, and less energy consumption.

In 2019, Selvi *et al.* [8] have implemented a new secure routing algorithm known as EATSRA. In the proposed EATSRA, the trust score evaluation was determined in WSN for detecting the malicious users and the DT algorithm with the Spatio-temporal constraints for choosing the better routes. For making effective decisions, the spatio-temporal constraints were used in the proposed model. At last, the proposed model has shown low energy consumption, improved security, and better packet delivery ratio than other existing models.

2.2. Review

Table 1 show the review on secure and energy efficient routing protocol in WSN. Initially, Taylor based C-SSA was deployed in [1], which presents high energy, maximum alive node, less delay, and better throughput; however, needs to build a multi-hop routing technique for attaining the higher performance. MOFPL algorithm is exploited in [2] that offer higher network energy, maximum alive nodes, lower delay, and less traffic rate, but the energy of the nodes was not rechargeable in the radio model of WSN. Moreover, effective distance-based ACO algorithm was deployed in [3] that offer increased lower delay, network lifetime, maximum energy consumption, and better PDR. Nevertheless, the theoretical analysis based on the maximization of network lifetime was not provided for all the overloaded network using the routing protocol. Likewise, CCR protocol was exploited in [4], that lower bandwidth usage, higher number of packets, maximum network lifetime, and reduces the overflow of data. However, the CCR protocol was not constructed for transmitting the data only when it changed. E-BEENISH Algorithm was exploited in [5] that are longer stability, improved system lifetime, increased residual energy, largest throughput, and better adaptability; however, it needs need to extend the proposed work with the lower complexity algorithm. In addition, I-SEP Algorithm is introduced in [6], which offers less number of dead nodes, better throughput, and improved network lifetime. However, need to implement the modified algorithm for a mobile network that moves the node in a constant speed. An Improved ABC algorithm is suggested in [7] that offer improved energy efficiency, better network throughput, less energy consumption, and maximum network life; but, needs to extend the energy-efficient routing protocols in WSNs to the mobile networks. Finally, EATSRA was implemented in [8], which has low energy consumption, improved security, and better packet delivery ratio; however, the intrusion detection facility was not used as an additional feature by the fuzzy constraints. Such limitations have to be taken into account based on security and energy aware routing protocol in WSN in the present work effectively.

Table 1. Review on conventional models based secure and energy aware routing protocol in wsn: features and challenges

Author Reference	**Adopted scheme**	**Features**	**Challenges**
Vinitha *et al.* [1]	Taylor C-SSA	✓ High energy ✓ Maximum alive node ✓ Less delay ✓ Better throughput	❖ Needs to build a multi-hop routing technique for attaining the higher performance.
Reeta *et al.* [2]	MOFPL algorithm	✓ Higher normalized network energy ✓ Maximum alive nodes ✓ Lower delay ✓ Less traffic rate	❖ Less Convergence rate
Xu *et al.* [3]	Effective distance-based ACO algorithm	✓ Better PDR ✓ Maximum Energy consumption ✓ Increased Network lifetime ✓ Lower Delivery delay	❖ The theoretical analysis based on the maximization of network lifetime was not provided by the routing protocol.
Farsi *et al.* [4]	CCR protocol	✓ Reducing the overflow of data ✓ Lower network bandwidth usage ✓ Maximum network lifetime ✓ Higher number of packets	❖ Enhances the data transmission
Zhang *et al.* [5]	E-BEENISH Algorithm	✓ Longer stability ✓ Improved system lifetime ✓ Increased residual energy ✓ Largest throughput ✓ Better adaptability	❖ Needs to extend the proposed work with the lower complexity algorithm.

Behera *et al.* [6]	I-SEP Algorithm	✓ Improved network lifetime ✓ Less number of dead nodes ✓ Better throughput	❖ Needs to implement the modified algorithm for a mobile network that moves the node in a constant speed.
Wang *et al.* [7]	Improved ABC algorithm	✓ Improved energy efficiency ✓ Better network throughput ✓ Less energy consumption ✓ Maximum network life	❖ Needs to extend the energy-efficient routing protocols in WSNs to mobile networks.
Selvi *et al.* [8]	EATSRA	✓ Low energy consumption ✓ Improved security ✓ Better packet delivery ratio	❖ The intrusion detection facility was not used in the proposed model.

III. Proposed Energy efficient trust based secure routing Model: Step by Step Process Flow

This paper aims to introduce a novel energy efficient trust based secure routing protocol for WSN. Optimal route (path selection) is carried out by the Improved Lion algorithm. The proposed protocol not only considers the energy consumption but also the security (trust model) of the network to ensure the best secured route (path) for data transmission. The considered energy and security constraints are defined under single objective function, which includes energy, delay, link lifetime, trust model. Moreover, the trust model includes evaluation of forwarding rate factor, direct trust, integrity factors, and indirect trust for maintaining the energy efficiency in routing process. Figure 1 illustrates the architecture of the adopted methodology.

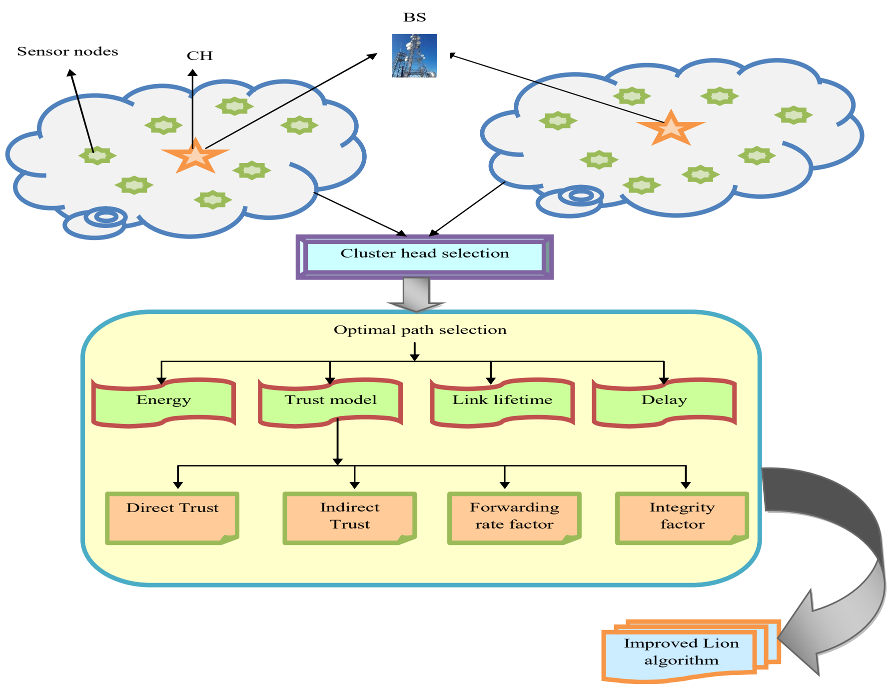


Figure 1. Architecture of the proposed energy efficient trust based secure routing protocol

The steps involved in the proposed scheme are (i) cluster head selection, (ii) optimal path selection based in trust factors and (iii) transmission of data.

3.1 Cluster Head Selection

Moreover, the LEACH protocol [1] has considered the dense sensor network that includes the nodes with similar energy and whose task is to transmit the data to the sink node. Moreover, the optimal CH is chosen to collect and broad cast the data to the sink node. Here, the leach protocol preceded $\frac{1}{b}$ rounds when the optimal percentage of CH is established. The set of CH is calculated for each round with size gb, here, g indicates the total number of rounds and b specifies the CH. Further, each round includes 2 phases, they are

✓ Steady-state phase
✓ Setup phase

The setup phase involves 3 phases (i.e.), sub phases

- Broadcast schedule
- Advertisement phase
- Cluster setup

Each node generates a random number of range 0 and 1 in the advertisement phase, and the predefined threshold is calculated. Moreover, the threshold is determined in Eq. (1).

$$Q(g)=\begin{cases}\dfrac{b}{1-b\times\left(e\bmod\dfrac{1}{b}\right)} & ;if\ \ c\in\theta\\ 0\ \ ;Otherwise\end{cases} \tag{1}$$

In Eq. (1), θ represents the node which is not the CH, e indicates the update interval of current topology, and b indicates the CH. Therefore, the CH produced by the LEACH protocol is given in Eq. (2).

$$B=\{B_1,B_2,....,B_n,....B_t\};1\le n\le t \tag{2}$$

In Eq. (2), t specifies the total CH.

IV. Identification of Optimal Route via improved lion algorithm

4.1 . Energy and Trust aware Parameters for optimal route selection

Energy: "The summation of energies of all hops which represents the energy present in the nodes is defined as the network energy". In Eq. (3), $E(P_l)$ denotes the energy of l^{th} hop, and d indicates the number of hops during multihop routing.

$$Energy=\frac{1}{d}\sum_{l=1}^{d}E(P_l) \tag{3}$$

Delay**:** "It is defined as the ratio of hop required for the total routing nodes present in the WSN".

$$Delay=\frac{d}{k} \tag{4}$$

In Eq. (4), k specifies the entire number of nodes.

Link Lifetime: "The network lifetime is derived from the link lifetime, and it should be higher for attaining the effective routing".

$$Linklifetime=\frac{1}{d}\times\sum_{l=1}^{d-1}\frac{C(P_l,P_{l+1})}{\alpha} \tag{5}$$

In Eq. (5), $C(P_l,P_{l+1})$ indicates the link lifetime of the l^{th} and $(l+1)^{th}$ hop and α indicates the regularization factor.

Trust model**:** In the WSN, each hop offers high trust degrees to evaluate the trust level among the particular hops as well as the nearby hops. Four parameters are used in the trust model are "(i) Direct trust, (ii) Indirect trust, (iii) Forwarding rate factor, and (iv) Integrity factor", and the parameters are given in Eq. (6).

$$L=\{L^D+L^I+L^F+L^J\} \tag{6}$$

4.1.1. Direct Trust (L^D)

"The direct trust is known as local trust and it presents the trust value as an agent to determine the familiarities with the target agent".

$$\left(L^D\right)_x^y(l,l+1)=fun_x^y(l,l+1) \tag{7}$$

In Eq. (7), fun specifies the satisfaction measure, and $\left(L^D\right)_x^y$ denotes the direct trust for y^{th} time interval and x^{th} transaction.

$$fun_x^y(l,l+1)=\omega+fun_{val}+(1-\omega)\times fun_{x-1}^y(l,l+1) \tag{8}$$

In Eq. (8), ω indicates the weight, and fun_{val} refers to the satisfaction value of recent transaction. Based on the accumulated deviation $O_x^y(l,l+1)$, the weight ω varies and it is given in Eq. (10).

$$fun_{val} = \begin{cases} 0; if\ transaction\ is\ fully\ unsatisfactory \\ 1; if\ transaction\ is\ fully\ satisfactory \\ \in (0,1); othewise \end{cases} \quad (9)$$

$$\omega = Z + h \times \frac{\beta_x^y(l,l+1)}{1+O_x^y(l,l+1)} \quad (10)$$

$$\beta_x^y(l,l+1) = \left| fun_{x-1}^y(l,l+1) - fun_{val} \right| \quad (11)$$

$$O_x^y(l,l+1) = h \times \beta_x^y(l,l+1) + (1-h) \times O_{x-1}^y(l,l+1) \quad (12)$$

In Eq. (10), Z indicates the threshold value (0.25), h specifies the constant factor, $\beta_x^y(l,l+1)$ denotes the recent error, and $O_x^y(l,l+1)$ denotes the accumulated deviation. Initially, $\omega = 1$ then it changes based on the Eq. (10).

4.1.2. Indirect Trust (L^I)

"It is determined from the knowledge obtained through other hops. The knowledge of other hops helps in decision making of each transaction". Therefore, the indirect trust of l^{th} hop in terms of $(l+1)^{th}$ hop is determined as in Eq. (13).

$$(L^I)_x^y(l,l+1) = \begin{cases} \dfrac{\sum_{q\in B-(l)} G_x^y(l,q) \times (L^D)_x^y(q,l+1)}{\sum_{q\in B-(l)} G_x^y(l,q)} & : if\ |B-\{l\}| = 0 \\ o;\ if\ |B-\{l\}| > 0 \end{cases} \quad (13)$$

In Eq. (13), B refers to the group of agents interact with $l+1$, and q indicates the hop that interacts with other hops. G_x^y Indicate the feedback creditability to make the prediction regarding the trust as in Eq. (14), where M_x^y indicates the similarity. The similarity measure is determined until the extent of two hops is similar Eq. (15).

$$G_x^y(l,l+1) = \begin{cases} \dfrac{1-\ln\left(M_x^y(l,l+1)\right)}{\ln \vartheta}; if\ M_x^y(l,+1) > \vartheta \\ 0; otherwise \end{cases} \quad (14)$$

$$M_x^y(l,l+1) = \begin{cases} M_{x-1}^y(l,l+1) + \dfrac{1-M_{x-1}^y(l,l+1)}{\chi} & ; if\ S_x^y(l,l+1) < f \\ M_{x-1}^y(l,l+1) - \dfrac{M_{x-1}^y(l,l+1)}{\sigma}; otherwise \end{cases} \quad (15)$$

In Eq. (15), f indicates the similarity deviation constant, χ denotes the reward factor, and σ specifies the punishment factor. Moreover, $S_x^y(l,l+1)$ is given in Eq. (16).

$$S_x^y(l,l+1) = \sqrt{\frac{\sum_{q\in K(l,l+1)} \left(fun_x^y(l,q) - fun_x^y(l+1,q)\right)^2}{|K(l,l+1)|}} \quad (16)$$

4.1.3. Forwarding Rate Factor

The nodes present in the WSN have minimum energy distributed for transferring and sensing the data. Therefore, the forwarding rate factor is calculated as in Eq. (17).

$$\left(L^{F}\right)^{y}(l,l+1)=\frac{X^{y}(l,l+1)}{Y^{y}(l,l+1)} \tag{17}$$

In Eq. (17), $X^{y}(l,l+1)$ indicates the counts of feedback packets, $Y^{y}(l,l+1)$ represents the count of packets to forward, l specifies the evaluation hop, and $l+1$ represents the hop evaluated.

4.1.4. Integrity factor

The integrity factor is given in Eq. (18), where $T^{y}(l,l+1)$ indicates the number of completely forwarded packets, and $K^{y}(l,l+1)$ represents the packets to forward.

$$L^{J}(l,l+1)=\frac{T^{y}(l,l+1)}{K^{y}(l,l+1)} \tag{18}$$

4.2. Solution Encoding and Fitness function

Moreover, the adopted ILA algorithm is used for determining the best path from source node. Figure 2 illustrates the solution encoding, where, s_1 is the source node and s_4 is the destination node, then the optimal route $s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow s_4$ is selected by the proposed ILA.

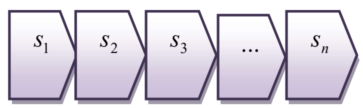


Figure 2. Solution Encoding

The fitness function of ILA is determined to find the optimal solution by the set of parameters, and it is given in Eq. (19). Here, the weights W_1, W_2, W_3, and W_4 are calculated using Eq. (20).

$$\begin{aligned} F &= W_1 \times Energy + W_2 \times (1 - Delay) \\ &+ W_3 \times Linklifetime + W_4 \times L \end{aligned} \tag{19}$$

$$W=\begin{cases} 0; \; if \;\; r<z \\ \dfrac{r-z}{a-z}; \; if \; z \le r \le a \\ \dfrac{w-r}{w-a}; \; if \;\; a \le r \le w \\ 0; \; if \; r \ge w \end{cases} \tag{20}$$

In Eq. (20), a, w, and r represents the membership function vertices $T(z)$ triangular. Here, w denotes the medium boundary with value 1, a indicates the lower boundary, and r refers to the upper boundary with value 0.

4.3 Proposed algorithm

Even though, the existing LA model are good in solving the complex optimization issues; it falls under local optima or global optima that does not provides better solutions and often stuck with low convergence. Consequently, some improvements are made in the adopted ILA algorithm to succeed the disadvantages of the existing LA [26] [27] [28] [29] [30] [31]. ILA developed within the motivation of lion's social behaviour through territorial takeover, territorial defence and territorial update. The algorithm includes different stages. Algorithm 1 explains the pseudo code of proposed Improved Lion algorithm and the flowchart is demonstrated in figure 3.

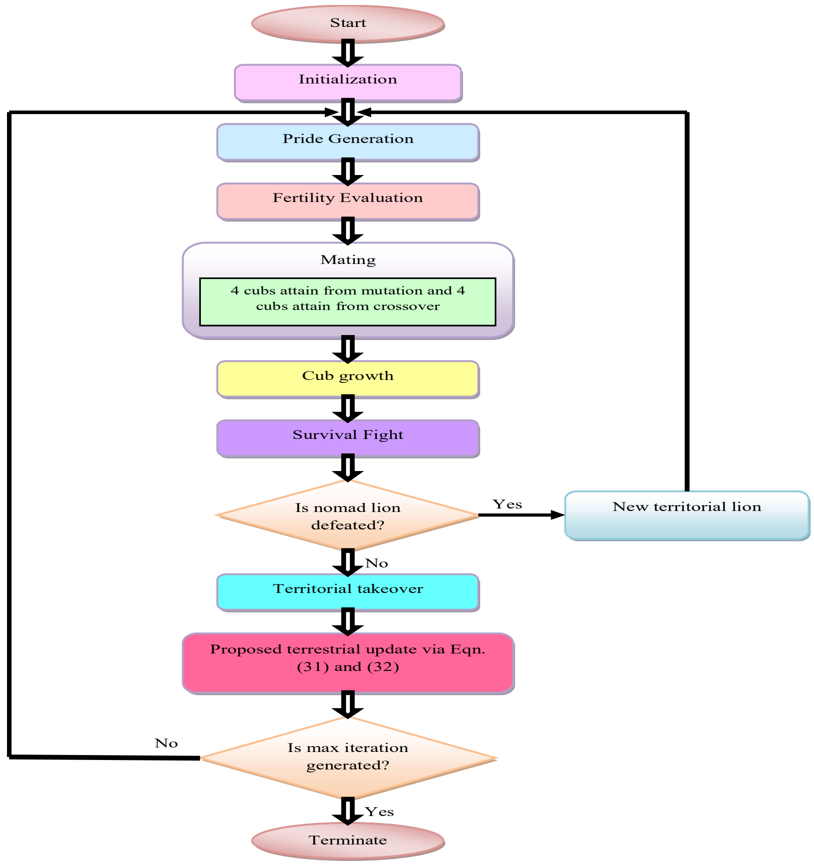


Figure 3. Flowchart of proposed ILA algorithm

4.3.1. Pride Generation

The pride generation is considered as the initialization phase. Moreover, the nomadic lion, female lion and male lion are initialized and it is represented as U^{nom}, U^{fem}, and U^{male}, correspondingly. Furthermore, the vector element of U^{male}, U^{fem} and U^{nom} are represented as u_m^{male}, u_m^{fem} and u_m^{nom}, respectively, that are the random integers in the maximum and the minimum limits as $i > 1$, and $m = 1,2..,LI$. Likewise, LI indicates the length of the lion given in Eq. (21), where, $\hat{i}$ and $\hat{j}$ are the integers for deciding the length of the lion. Further, when $\hat{i} = 1$, the search process continued with the vector elements and the binary-encoded lion are created as 1 or 0.

$$LI = \begin{cases} \hat{i}; & \hat{i} > 1 (genral\ case) \\ \hat{j}; & otherwise (special\ case) \end{cases} \tag{21}$$

$$A(u_m) \in \left(u_m^{\min}, u_m^{\max}\right) \tag{22}$$

$$j\%2 = 0 \tag{23}$$

Moreover, Eq. (22) and Eq. (24) indicates the obtained binary lion in the solution space, and Eq. (23) denotes the total binary bits used after and before the equal decimal point.

$$A(u_m)=\sum_{m=2}^{LI} 2^{\left(\frac{LI}{2}-m\right)} u_m \qquad (24)$$

4.3.2. Fertility evaluation

The lions become infertile or old and it makes the lions laggard in the terrestrial takeover or terrestrial defense. Moreover, U^{male} , and U^{fem} are saturated in terms of the fitness value, and it reach the local or global optimal. The fertility evaluation is employed for preserving the solution from being caught into the local optima. Additionally, the male lion U^{male} becomes laggard and the LI_R laggardness rate is raised by 1, when $V(U^{male}) > V^{ref}$, where, V^{ref} is denoted as the reference fitness. When $LI_R > LI_R^{\max}$, the terrestrial defence process is occurred.

The sterile rate ST_R ensures the U^{fem} fertility and at the end of crossover process, it is raised by 1. Eq. (25) indicates the update of U^{fem} with $U^{+(fem)}$, as $ST_R > ST_R^{\max}$. Further, the mating process is executed. This process of continues updating attains $OL_{ux}^{\max}$. Moreover, m^{th} and ux^{th} vector elements of $U^{+(fem)}$ is given as $U_m^{+(fem)}$ and $U_{ux}^{+(fem)}$, correspondingly. ux Indicates the random integer generated among the interval $[1, LI]$. In addition, ϕ represents the female update function and the random integers [0, 1] is indicated as $rand_2$ and $rand_1$. Eq. (26) and Eq. (27) specifies the female update function ϕ_{ux} .

$$U_m^{+(fem)}=\begin{cases} U_m^{+(fem)} & if\ m=ux \\ U_m^{fem} & otherwise \end{cases} \qquad (25)$$

$$U_{ux}^{+(fem)}=\min\left[U_{ux}^{\max}, \max\left(U_{ux}^{\min}, \phi_{ux}\right)\right] \qquad (26)$$

$$\phi_{ux}=\left\{U_{ux}^{fem}+\left[(0.1 rand_2-0.05)\left(U_{ux}^{male}-rand_1 . U_{ux}^{fem}\right)\right]\right\} \qquad (27)$$

4.3.3. Mating

During the process of mating, the 2 primary steps like mutation and crossover, and the supplementary step is done through the gender clustering. Moreover, the cubs are produced through U^{male} , and U^{fem} by the process of crossover and mutation. The cross over mask CS is different during the generation of each cub, and $U^{cubs}(R\hat{P})$ is produced in $R\hat{p}^{th}$ mask. U^{cubs} and U^{new} represents the cubs obtained from the crossover and mutation process. The generated 8 cubs fill the cub pool and they produce U^{j-cubs} and U^{V-cubs} through the gender clustering.

4.3.4. Lion operators

The territorial defense is arranged as the pride and nomad coalition, survival fights, and nomad coalition updates. The selection of $U^{\hat{e}i-nom}$ is chosen in Eq. (28) - Eq. (30). Territorial takeover make the algorithm for updating U^{male} and U^{fem} , and if U^{j-cubs} and U^{V-cubs} are matured when the age of cubs goes away from the maximum age for cub maturity $QB_{\max}$. QB_{cub} indicates the age of cubs.

$$V(U^{\hat{e}i-nom}) < U^{j-cubs} \qquad (28)$$

$$V(U^{\hat{e}i-nom}) < V(U^{male}) \qquad (29)$$

$$V(U^{\hat{e}i-nom}) < V(U^{V-cubs}) \qquad (30)$$

In the conventional LA model, there is no terrestrial update. But as per the implemented model, the terrestrial update is done in the LA. Eq. (31) and Eq. (32) represents the terrestrial update, where, $rand$ indicates the random variable, and $size$ denotes the size of male and female cubs.

$$U^{male} = \lfloor U^{male-cubs} + \left(U^{fem-cubs} \times rand\left(size\left(U^{fem-cubs}\right)\right)\right)\rfloor \quad (31)$$

$$U^{fem} = \lfloor U^{fem-cubs} + \left(U^{mal-cubs} \times rand\left(size\left(U^{mal-cubs}\right)\right)\right)\rfloor \quad (32)$$

Arithmetic crossover: The arithmetic crossover of the proposed algorithm is determined in Eq. (33) and Eq. (34), where WF indicates the weight factor ranges from 0to 1.

$$offspring1 = WF * parent1 + (1 - WF) * parent2 \quad (33)$$

$$offspring2 = (1 - WF) * parent1 + WF * parent2 \quad (34)$$

4.3.5. Termination

Eq. (35) and Eq. (36) specifies the termination of the algorithmic evaluation takes place while the termination criteria are met. Here, $NUM_{gen}^{\max}$, N and NUM_{gen}, indicates the the maximum number of generations, error threshold, and number of generations, respectively. The pseudo code of the proposed ILA is given in Algorithm 1.

$$NUM_{gen} > NUM_{gen}^{\max} \quad (35)$$

$$\lfloor V\left(U^{male}\right) - V\left(U^{optimal}\right)\rfloor \leq N \quad (36)$$

Algorithm 1: Improved Lion Algorithm (ILA)

Initialize U^{male}, U^{fem}, and U^{nom}

Calculate $V\left(U^{male}\right)$, $V\left(U^{fem}\right)$, and $V\left(U^{nom}\right)$

Set $V^{ref} = V\left(U^{male}\right)$ and $NUM_{gen} = 0$

Store U^{male} and $V\left(U^{male}\right)$

Execute fertility evaluation

Perform mating and attain cub pool

Execute gender clustering and achieve U^{j-cubs} and U^{V-cubs}

Initialize QB_{cub} as zero

Perform the cub growth function

Execute the territorial defense; if $(defense = 0)$

    Again store U^{male} and $V\left(U^{male}\right)$

        if $(QB_{cub} < QB_{MAX})$

        Again perform the cub growth function

        end

    Execute territorial takeover and attain updated U^{male} and U^{fem}

    Enhance NUM_{gen} by 1

    The terrestrial update is given in Eq. (31) and Eq. (32)

        If the termination criteria are not met

        Again store U^{male} and $V\left(U^{male}\right)$

Terminate the process
end
End

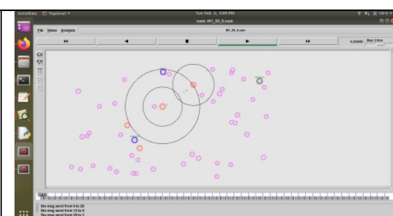
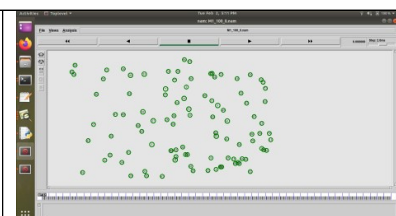
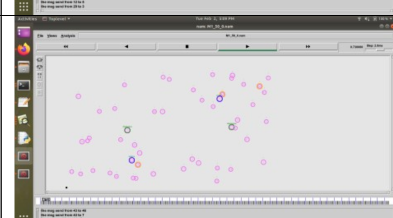
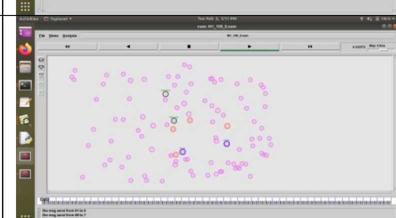
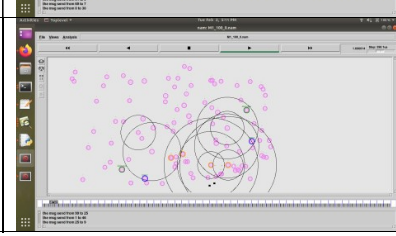
V. Results and discussions

5.1. Simulation Procedure

The adopted energy efficient trust based secure routing protocol in WSNs by ILA was implemented in NS-2 and the obtained results were analysed. The simulation parameters of the proposed work is summarized in Table 2. In addition, the analysis was done for two groups of nodes such as 50 nodes and 100 nodes. The analysis was carried out for two groups of nodes with respect to alive nodes, delay, residual energy, link lifetime, throughput and PDR. The adopted ILA scheme was compared to the traditional schemes such as LA [26], DU-WOA [36], FF [32], CSO[33], MFO [34], and ACO [35], respectively. Figure 4 represents the simulation outcomes of the adopted ILA scheme for two groups of nodes.

Table2. Simulation Parameters

Channel type	Wireless
Antenna	Omni Antenna
MAC type	MAC/802.11
Dimension Y	600
Packet size	50
Propagation model	Two ray ground
Dimension X	1501
Queue type	Queue/DropTail
Total Simulation time	100s
Initial Number of nodes	30
Network Interface type	wirelessPhy
Initial energy	3.4 J
Tx power	0.43
Rx power	0.2

Sample 1		
Sample 2		
Sample 3		

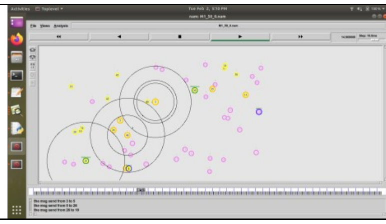
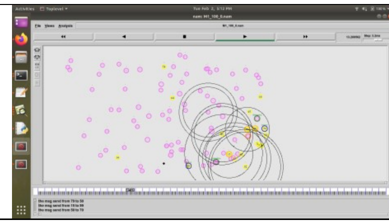
Sample 4		
	(a)	(b)

Figure 4. Simulation outcomes of proposed ILA model for (a) 50 nodes and (b) 100 nodes

5.2. Alive node Analysis

The alive node analysis of the adopted ILA method over other traditional models such as LA, ACO, FF, CSO, MFO, and DU-WOA models, respectively are illustrated in Figure 5 under two category: with and without security. From the graph, it is noted that as the simulation time increases the alive nodes get decreased. Though, the proposed ILA model obtains more alive nodes at simulation time (52sec) than other existing models like LA, ACO, FF, CSO, MFO, and DU-WOA for 50 nodes without security (in Figure 5 (a)). The count of alive node for both proposed and traditional models attains constant (i.e.), 50 alive nodes until the simulation time (30 sec) for all nodes under with and without security. In addition, in Figure 5 (b), the proposed ILA method at simulation time (58 sec) remains more alive nodes than other existing models like LA, ACO, FF, CSO, MFO, and DU-WOA models, respectively for 50 nodes with security. Furthermore, when the simulation time is 60 sec, the proposed ILA model is 71.42%, 57.14%, 42.85%, 80.955, 80.95%, and 47.61% better than the existing LA, ACO, FF, CSO, MFO, and DU-WOA scheme for 100 nodes without security in Figure 5(c) with more alive nodes. Moreover, the proposed ILA model exhibits maximum (59) alive nodes at simulation time (48 sec) than other traditional models for 100 nodes with security in Figure 5(d). Thus, the improvement of the proposed ILA model is proved with respect to maximal alive nodes.

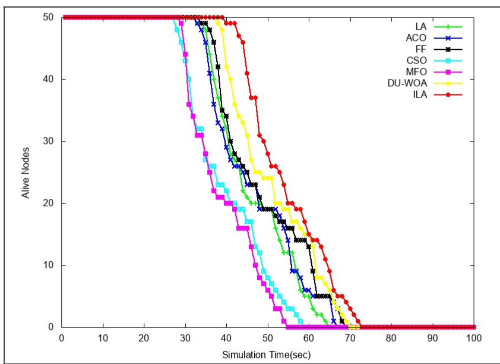
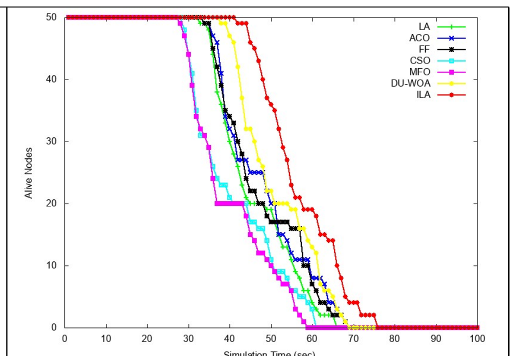
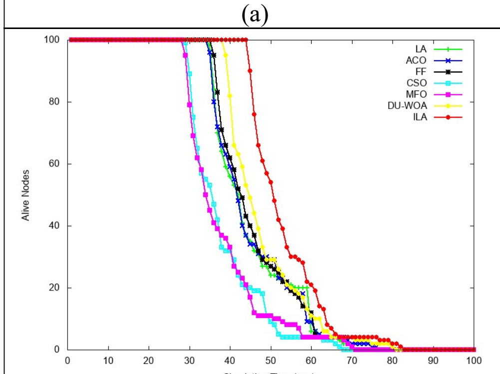
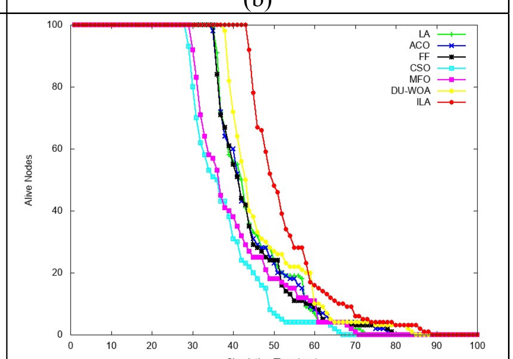
	
(a)	(b)
	
(c)	(d)

Figure 5. Alive node analysis of the proposed ILA method over other traditional models for (a) 50 nodes without security (b) 50 nodes with security (c) 100 nodes without security and (d) 100 nodes with security

5.3 Analysis on Delay

The analysis on delay of proposed ILA model over other existing schemes for two groups of nodes is illustrated in Figure 6. Nevertheless, the delay of the proposed model should be minimal for obtaining better performance. From the figure, the proposed method attains low delay almost for simulation time (0 sec to 100 sec) than other compared traditional models such as LA, ACO, FF, CSO, MFO, and DU-WOA models, respectively for 50 and 100 nodes with and without security. Moreover, the delay of the proposed ILA method at stimulation time 36 sec holds the minimal delay (0.237469); whereas, the traditional models hold highest delay value for LA (0.503923), ACO (0.500210), FF (0.338246), CSO (0.519730), MFO (0.533829) and DU-WOA (0.328499), respectively for 50 nodes without security in Figure 6(a). Similarly, the proposed ILA method at simulation time 21 sec remains with minimal delay than the existing schemes like LA, ACO, FF, CSO, MFO, and DU-WOA models for 100 nodes with security as per Figure 6(d). Thus, it is proved that the proposed routing model makes a delayless transmission with optimal route.

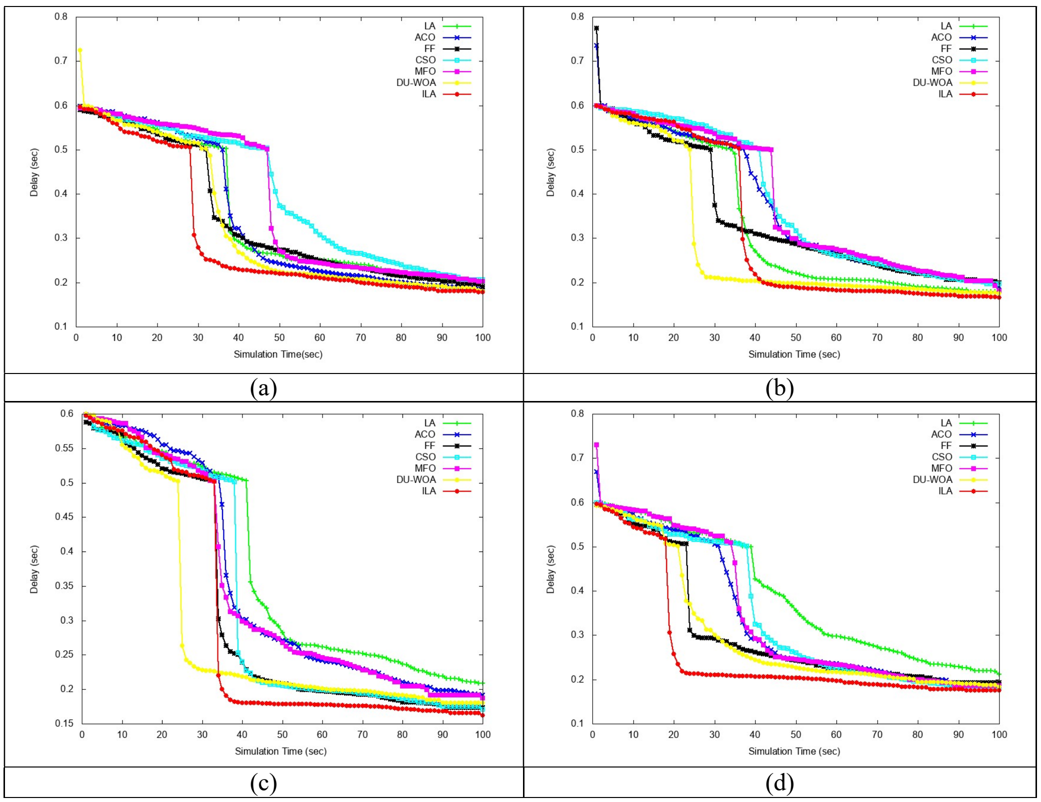


Figure 6. Analysis on delay: proposed ILA method over other traditional models for (a) 50 nodes without security (b) 50 nodes with security (c) 100 nodes without security and (d) 100 nodes with security

5.4. Residual Energy Analysis

The analysis on residual energy of the proposed ILA method was computed over other traditional schemes is given in Figure 7 Moreover, the residual energy decreases as the simulation time increases. Still, the proposed ILA model holds more residual energy for 2 groups of nodes with and without security than other existing models such as LA, ACO, FF, CSO, MFO, and DU-WOA models, correspondingly. In Figure 7(a), the residual energy of proposed ILA model at simulation time (25sec) is 19.93%, 23.81%, 20.97%, 49.23%, 41.11%, and 11.48% improved than other LA, ACO, FF, CSO, MFO, and DU-WOA models, correspondingly for 50 nodes without security. Likewise, the proposed ILA method attains higher residual energy at simulation time (40 sec) for 100 node with security; but the existing models has obtained lower energy values for LA, ACO, FF, CSO, MFO, and DU-WOA models, respectively in Figure 7(d). Similarly, the rest of the graphs prove that the proposed routing model ensures the minimal energy consumption, thereby more residual energy in nodes even at the last round.

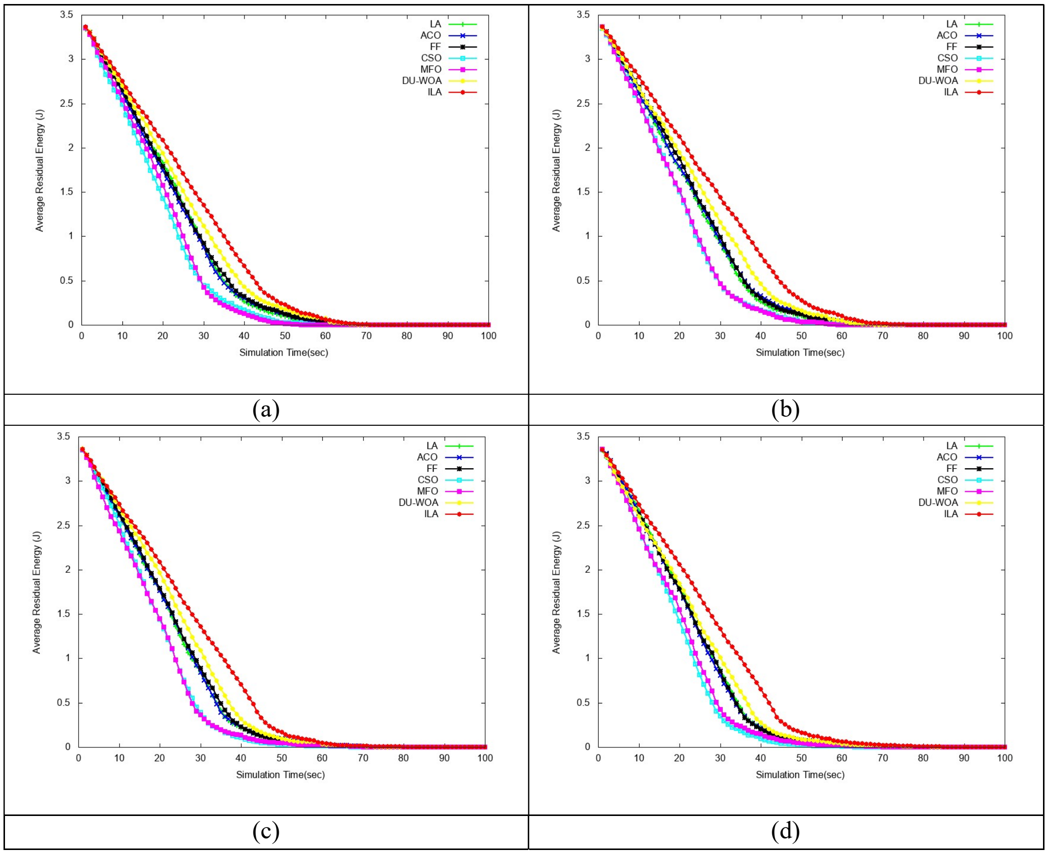


Figure 7. Analysis on residual energy of the proposed ILA method over other traditional models for (a) 50 nodes without security (b) 50 nodes with security (c) 100 nodes without security and (d) 100 nodes with security

5.5. Throughput Analysis

Figure 8 represents the throughput analysis of the adopted ILA model to the conventional methods. It is examined from the graph that 'as the simulation time increases, the throughput value also increases' for both the proposed and conventional models. Although, the throughput of proposed ILA model obtains higher values (8.590176 Mbps) at simulation time 68 sec than other existing schemes like LA (~8.048725 Mbps), ACO(~7.807357Mbps),FF(~7.472928Mbps), CSO(~7.390268 Mbps), MFO(~7.246543Mbps), and DU-WOA(~8.334558 Mbps) models, correspondingly in Figure 8(b), for 50 nodes with security. In addition, the adopted ILA model holds higher throughput values at stimulation time 60 sec; whereas, the traditional models such as LA, ACO, FF, CSO, MFO, and DU-WOA models holds lower throughput for 100 nodes without security in Figure 8(c). It is observed that the adopted ILA model obtains better throughput for two groups of nodes with and without security than other models. This obviously proves the assurance in performance (throughput) even with secured routing.

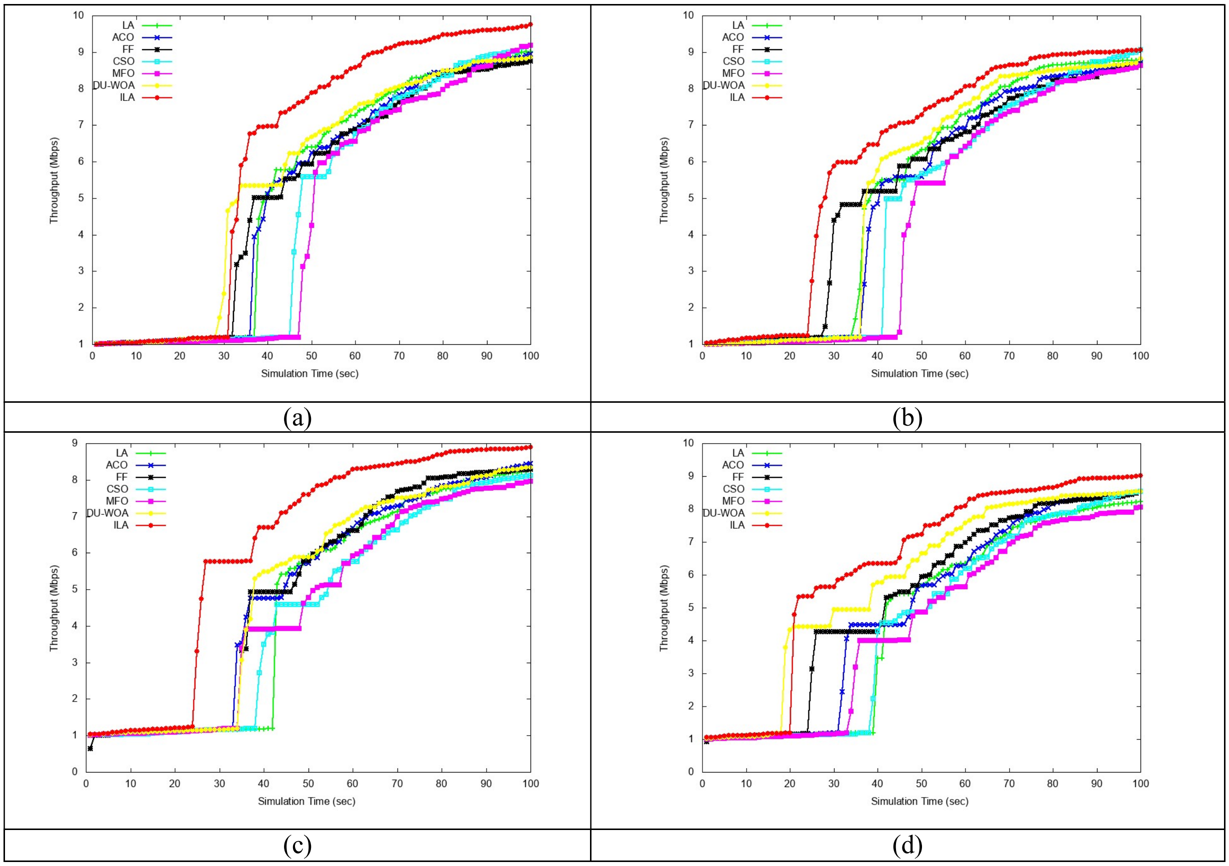
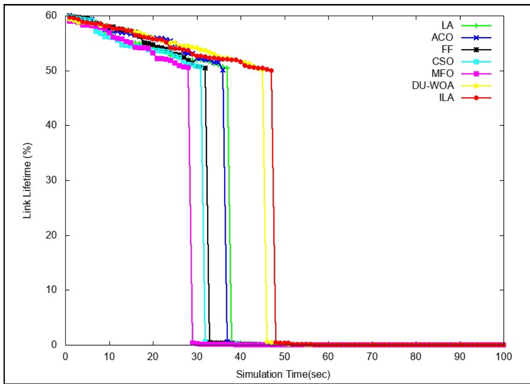


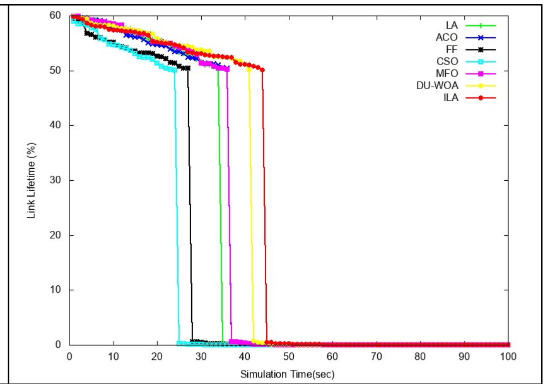
Figure 8. Throughput analysis of proposed ILA method over other traditional models for (a) 50 nodes without security (b) 50 nodes with security (c) 100 nodes without security and (d) 100 nodes with security

5.6. Analysis on link lifetime

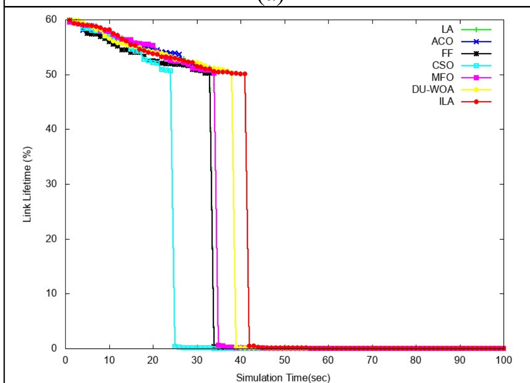
The analysis on link lifetime of adopted ILA model over other existing models is illustrated in Figure 9. From the graph, it is noted that the proposed ILA model is approximately constant (i.e.), low link lifetime for the simulation time 50 sec to 100. Moreover, the proposed ILA model holds higher link lifetime (50.172583) at simulation time 46 sec than the conventional models like LA (0.102779), ACO (0.051954), FF (0.048839), CSO (0.043146), MFO (0.033677), and DU-WOA (0.583342) models for 50 nodes without security in Fig. 9(a). Furthermore, the link lifetime of the adopted ILA model at stimulation time is seems to be high for 50 nodes with security; whereas, the existing models such as LA, ACO, FF, CSO, MFO, and DU-WOA models, respectively at simulation time (44sec) in Figure 9(b). An improvement of proposed ILA model at simulation time 40 sec is 98.07%, 99.93%, 99.91%, 99.92%, 99.75%, and 99.758% better than other traditional models like LA, ACO, FF, CSO, MFO, and DU-WOA models, respectively for 100 nodes without security in Figure 9(c). Therefore, the link life of the routing nodes becomes increased by the proposed routing strategy.



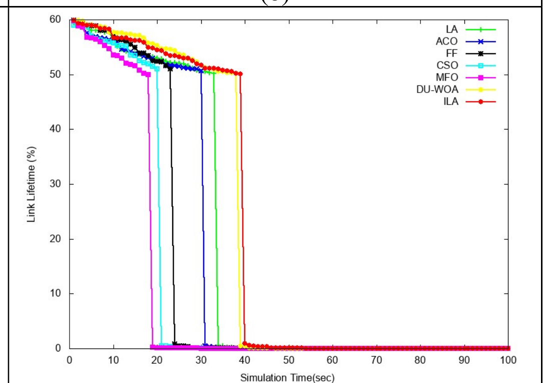
(a)



(b)



©

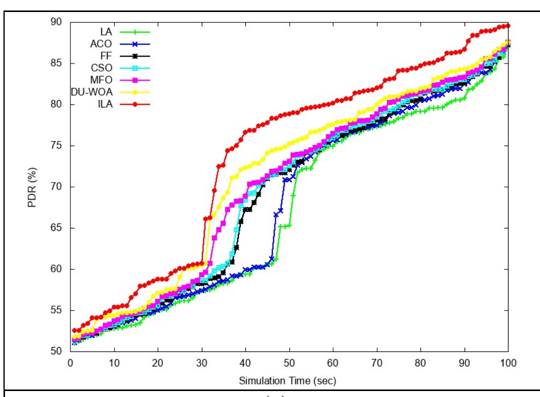


(d)

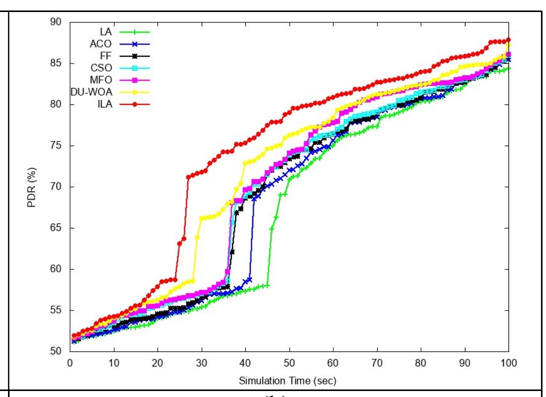
Figure 9. Analysis on link lifetime of proposed ILA method over other traditional models for (a) 50 nodes without security (b) 50 nodes with security (c) 100 nodes without security and (d) 100 nodes with security.

5.7. Analysis on PDR

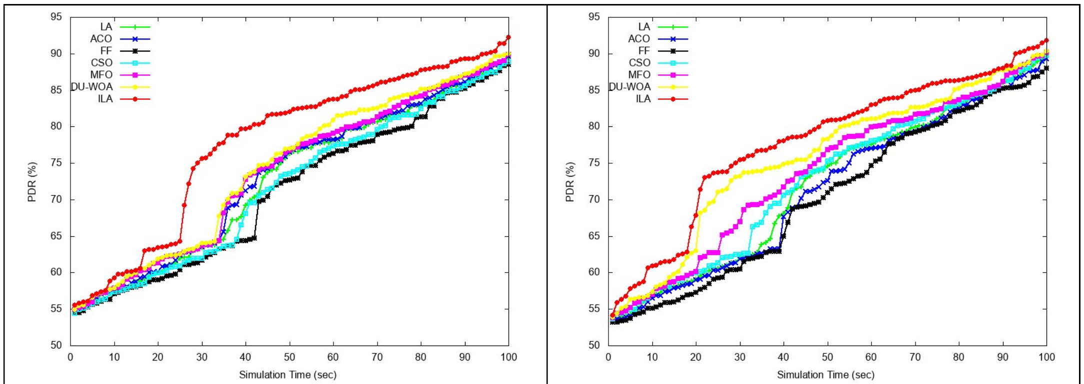
Figure 10 illustrates the analysis on PDR of adopted ILA model over other existing models. As the simulation time increases, the PDR obtains its maximum value. Further, the proposed ILA model is 2.86%, 2.590%, 2.43%, 2.389%, 2.27%, and 2.248% better than other traditional models like LA, ACO, FF, CSO, MFO, and DU-WOA, respectivetly for 50 node without security at simulation time (100sec) in Figure 10(a). Moreover, the the adopted model holds higher PDR(83.715367) at simulation time 60 sec than the conventional models like LA (78.140993), ACO (78.219332), FF (76.337396), CSO (77.314820), MFO (79.085321), and DU-WOA (80.877374) models for 100 nodes without security in Fig. 10(c). In addition, the PDR of the adopted ILA model at stimulation time 15 sec obtains higher values (~61.729571) for 100 nodes with security; whereas, the existing models such as LA, ACO, FF, CSO, MFO, and DU-WOA models, respectively holds minimum values in Figure 10(d). Thus, the PDR of the routing nodes attains high performance for the proposed model than the conventional models.



(a)



(b)



(c) (d)

Figure 10. Analysis on PDR of proposed ILA method over other traditional models for (a) 50 nodes without security (b) 50 nodes with security (c) 100 nodes without security and (d) 100 nodes with security.

VI. CONCLUSION

This paper has proposed a novel energy efficient Trust based secure routing protocol for wireless sensor network. Here, the optimal route selection was carried out by the new ILA. The proposed protocol not only considers the energy consumption but also the security (trust model) of the network for selecting the best route path and that was achieved by defining the single objective function. Finally, the performance of proposed model was evaluated over other conventional models with respect to different measures like alive nodes, delay, residual energy, link lifetime, throughput and PDR. On observing the graph, the proposed ILA method at simulation time (58 sec) remains more alive nodes than other existing models like LA, ACO, FF, CSO, MFO, and DU-WOA models, respectively for 50 nodes with security. Moreover, the delay of the proposed ILA method at stimulation time 36 sec holds the minimal delay (0.237469); whereas, the traditional models hold highest delay value for LA (0.503923), ACO (0.500210), FF (0.338246), CSO (0.519730), MFO (0.533829) and DU-WOA (0.328499), respectively for 50 nodes without security. The residual energy of proposed ILA model at simulation time (25sec) was 19.93%, 23.81%, 20.97%, 49.23%, 41.11%, and 11.48% improved than other LA, ACO, FF, CSO, MFO, and DU-WOA models, correspondingly for 50 nodes without security.

REFERENCES

[1] A. Vinitha, M. S. S. Rukmini, Dhirajsunehra, "Secure and energy aware multi-hop routing protocol in WSN using Taylor-based hybrid optimization algorithm" Journal of King Saud University - Computer and Information SciencesIn press, pp.1-12, corrected proof Available online 21 November 2019.

[2] Reeta Bhardwaj, Dinesh Kumar, "MOFPL: Multi-objective fractional particle lion algorithm for the energy aware routing in the WSN" Pervasive and Mobile Computing,vol. 58, Art.no. 101029, pp.1-16, August 2019.

[3] C. Xu, Z. Xiong, G. Zhao and S. Yu, "An Energy-Efficient Region Source Routing Protocol for Lifetime Maximization in WSN," IEEE Access, vol. 7, pp. 135277-135289, 2019, doi: 10.1109/ACCESS.2019.2942321.

[4] M. Farsi, M. Badawy, M. Moustafa, H. Arafat Ali and Y. Abdulazeem, "A Congestion-Aware Clustering and Routing (CCR) Protocol for Mitigating Congestion in WSN," IEEE Access, vol. 7, pp. 105402-105419, 2019, doi: 10.1109/ACCESS.2019.2932951.

[5] Y. Zhang, X. Zhang, S. Ning, J. Gao and Y. Liu, "Energy-Efficient Multilevel Heterogeneous Routing Protocol for Wireless Sensor Networks," IEEE Access, vol. 7, pp. 55873-55884, 2019, doi: 10.1109/ACCESS.2019.2900742.

[6] T. M. Behera, S. K. Mohapatra, U. C. Samal, M. S. Khan, M. Daneshmand and A. H. Gandomi, "I-SEP: An Improved Routing Protocol for Heterogeneous WSN for IoT-Based Environmental Monitoring," IEEE Internet of Things Journal, vol. 7, no. 1, pp. 710-717, Jan. 2020, doi: 10.1109/JIOT.2019.2940988.

[7] Z. Wang, H. Ding, B. Li, L. Bao and Z. Yang, "An Energy Efficient Routing Protocol Based on Improved Artificial Bee Colony Algorithm for Wireless Sensor Networks,"IEEE Access, vol. 8, pp. 133577-133596, 2020, doi: 10.1109/ACCESS.2020.3010313.

[8] Selvi. M, Thangaramya. K, Ganapathy. S, et al., “An Energy Aware Trust Based Secure Routing Algorithm for Effective Communication in Wireless Sensor Networks”, Wireless Pers Commun, vol. 105, pp. 1475–1490, 2019. https://doi.org/10.1007/s11277-019-06155-x

[9] Hema Kumar, M., Mohanraj, V., Suresh, Y. et al., "Trust aware localized routing and class based dynamic block chain encryption scheme for improved security in WSN", J Ambient Intell Human Comput, 2020. https://doi.org/10.1007/s12652-020-02007-w.

[10] Ganesh, D.R., Patil, K.K. & Suresh, L., "Q-FRPML: QoS-Centric Fault-Resilient Routing Protocol for Mobile-WSN Based Low Power Lossy Networks", Wireless Pers Commun, vol. 105, pp. 267–292, 2019. https://doi.org/10.1007/s11277-018-6112-8.

[11] Thangaramya, K., Kulothungan, K., Indira Gandhi, S. et al., "Intelligent fuzzy rule-based approach with outlier detection for secured routing in WSN", Soft Comput, vol. 24, pp. 16483–16497, 2020. https://doi.org/10.1007/s00500-020-04955-z.

[12] Chouhan, N., Jain, S.C., "Tunicate swarm Grey Wolf optimization for multi-path routing protocol in IoT assisted WSN networks", J Ambient Intell Human Comput, 2020. https://doi.org/10.1007/s12652-020-02657-w.

[13] Vijayalakshmi, V., Senthilkumar, A., "USCDRP: unequal secure cluster-based distributed routing protocol for wireless sensor networks", J Supercomput, vol. 76, pp. 989–1004, 2020. https://doi.org/10.1007/s11227-019-03040-z.

[14] Dhand, G., Tyagi, S.S., "SMEER: Secure Multi-tier Energy Efficient Routing Protocol for Hierarchical Wireless Sensor Networks" Wireless Pers Commun, vol. 105, pp. 17–35, 2019. https://doi.org/10.1007/s11277-018-6101-y.

[15] Vinodhini, R., Gomathy, C., "MOMHR: A Dynamic Multi-hop Routing Protocol for WSN Using Heuristic Based Multi-objective Function" Wireless Pers Commun, vol. 111, pp. 883–907, 2020. https://doi.org/10.1007/s11277-019-06891-0.

[16] Kavidha, V., Ananthakumaran, S., "Novel energy-efficient secure routing protocol for wireless sensor networks with Mobile sink" Peer-to-Peer Netw. Appl., vol. 12, pp. 881–892, 2019. https://doi.org/10.1007/s12083-018-0688-3.

[17] Sujanthi, S., Nithya Kalyani, S., "SecDL: QoS-Aware Secure Deep Learning Approach for Dynamic Cluster-Based Routing in WSN Assisted IoT", Wireless Pers Commun, vol. 114, pp. 2135–2169, 2020. https://doi.org/10.1007/s11277-020-07469-x.

[18] Shende, D.K., Sonavane, S.S, "CrowWhale-ETR: CrowWhale optimization algorithm for energy and trust aware multicast routing in WSN for IoT applications", Wireless Netw, vol. 26, pp. 4011–4029, 2020. https://doi.org/10.1007/s11276-020-02299-y.

[19] Kavitha, M., Geetha, B.G., "An efficient city energy management system with secure routing communication using WSN" Cluster Computing, vol. 22, pp. 13131–13142, 2019. https://doi.org/10.1007/s10586-017-1277-6.

[20] Revanesh, M., Sridhar, V. & Acken, J.M., "Secure Coronas Based Zone Clustering and Routing Model for Distributed Wireless Sensor Networks", Wireless Pers Commun, vol. 112, pp. 1829–1857, 2020. https://doi.org/10.1007/s11277-020-07129-0.

[21] Udhayavani, M., Chandrasekaran, M., "Design of TAREEN (trust aware routing with energy efficient network) and enactment of TARF: a trust-aware routing framework for wireless sensor networks" Cluster Computing, vol. 22, pp. 11919–11927, 2019. https://doi.org/10.1007/s10586-017-1512-1.

[22] Vidhya, S., Sasilatha, T., "Secure Data Transfer Using Multi Layer Security Protocol with Energy Power Consumption AODV in Wireless Sensor Networks" Wireless Pers Communication, vol. 103, pp. 3055–3077, 2018. https://doi.org/10.1007/s11277-018-5994-9.

[23] Deepa, C., Latha, B., "HHSRP: a cluster based hybrid hierarchical secure routing protocol for wireless sensor networks" Cluster Computing, vol. 22, pp. 10449–10465, 2019. https://doi.org/10.1007/s10586-017-1065-3.

[24] Kalidoss, T., Rajasekaran, L., Kanagasabai, K. et al., "QoS Aware Trust Based Routing Algorithm for Wireless Sensor Networks" Wireless Pers Commun, vol. 110, pp. 1637–1658, 2020. https://doi.org/10.1007/s11277-019-06788-y.

[25] Beheshtiasl, A., Ghaffari, A., "Secure and Trust-Aware Routing Scheme in Wireless Sensor Networks" Wireless Pers Commun, vol. 107, pp. 1799–1814, 2019. https://doi.org/10.1007/s11277-019-06357-3.

[26] Rajakumar B R, "Optimization using lion algorithm: a biological inspiration from lion's social behavior", Evolutionary Intelligence, Special Issue on Nature inspired algorithms for high performance computing in computer vision, vol. 11, no. 1-2, pp. 31-52, 2018, DOI: https://doi.org/10.1007/s12065-018-0168-y.

[27] B. R. Rajakumar, "Impact of Static and Adaptive Mutation Techniques on Genetic Algorithm", International Journal of Hybrid Intelligent Systems, vol. 10, no. 1, pp. 11-22, 2013, DOI: 10.3233/HIS-120161.

[28] B. R. Rajakumar, "Static and Adaptive Mutation Techniques for Genetic algorithm: A Systematic Comparative Analysis", International Journal of Computational Science and Engineering, vol. 8, no. 2, pp. 180-193, 2013, DOI: 10.1504/IJCSE.2013.053087.

[29] S. M. Swamy, B. R. Rajakumar and I. R. Valarmathi, "Design of Hybrid Wind and Photovoltaic Power System using Opposition-based Genetic Algorithm with Cauchy Mutation", IET Chennai Fourth International Conference on Sustainable Energy and Intelligent Systems (SEISCON 2013), Chennai, India, Dec. 2013, DOI: 10.1049/ic.2013.0361.

[30] Aloysius George and B. R. Rajakumar, "APOGA: An Adaptive Population Pool Size based Genetic Algorithm", AASRI Procedia - 2013 AASRI Conference on Intelligent Systems and Control (ISC 2013), vol. 4, pp. 288-296, 2013, DOI: https://doi.org/10.1016/j.aasri.2013.10.043.

[31] B. R. Rajakumar and Aloysius George, "A New Adaptive Mutation Technique for Genetic Algorithm", In proceedings of IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), pp. 1-7, Dec 18-20, India, 2012, DOI: 10.1109/ICCIC.2012.6510293.

[32] IztokFister, IztokFisterJr, Xin-SheYang and JanezBrest, "A comprehensive review of firefly algorithms", Swarm and Evolutionary Computation, vol. 13, pp. 34-46, 2013.

[33] Shu-Chuan Chu, Pei-wei Tsai, and Jeng-Shyang Pan, " Cat Swarm Optimization " International Conference on Artificial Intelligence, LNCS, volume 4099, pp. 854-858, 2006.

[34] SeyedaliMirjalili," Moth-flame optimization algorithm: A novel nature-inspired heuristic paradigm", Knowledge-Based Systems, vol. 89, pp. 228-249, November 2015.

[35] Christian Blum, "Ant colony optimization: Introduction and recent trends" Physics of Life Reviews, vol. 2, no. 4, pp. 353-373, Dec 2005.

[36] Syed Mohd Ali, Syed Abdul Sattar, D. Srinivasa Rao, "security aware routing for wireless sensor network using hybrid optimization algorithm", International Journal of Electronics and Communication Engineering and Technology (IJECET), Vol. 11, no. 3, pp. 1-21. Art. no. IJECET_11_03_001, Sept-Oct 2020.

[37] W.Brajula and Praveena S, "Energy Efficient Genetic Algorithm Based Clustering Technique for Prolonging the Life Time of Wireless Sensor Network", Journal of Networking and Communication Systems, Vol.1,No.1, pp.1-9,2018.

[38] Amit Kelotra and Prateek Pandey, "Energy-aware Cluster Head Selection in WSN using HPSOCS Algorithm", Journal of Networking and Communication Systems, Vol.2,No.1, pp.24-33,2019.

[39] Jacob John,Paul Rodrigues, "Multi-objective HSDE Algorithm for Energy-Aware Cluster Head Selection in WSN", Journal of Networking and Communication Systems, Vol.2,No.3, pp.20-29,2019.

[40] Sadanand L Shelgaonkar, "I-CSA based Cluster Head Selection Model in Wireless Sensor Network", Journal of Networking and Communication Systems, Vol 3, No 2, 2020.

[41] Santosh Kumar B. P,Venkata Ramanaiah K., "An Efficient Hybrid Optimization Algorithm for Image Compression", Multimedia Research, Vol.2,No.4, pp.1-11,2019.

[42] Gayathri Devi K.S, "Hybrid Genetic Algorithm and Particle Swarm Optimization Algorithm for Optimal Power Flow in Power System", Journal of Computational Mechanics, Power System and Control, Vol.2,No.2, pp.31-37,2019.

[43] Benjamín Barán, Rubén Sos, "AntNet: Routing Algorithm for Data Networks basedon Mobile Agents", Argentine Symposium on Artificial Intelligence, pp. 75-84, 2001.

[44] Yesy Diah Rosita, Erly Ekayanti Rosyida, Muhammad Adik Rudiyanto, "Implementation of Dijkstra Algorithm and Multi-Criteria Decision-Making for Optimal Route Distribution", Procedia Computer Science, vol. 161, pp. 378-385, 2019.