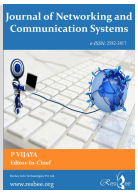
Vol.4 No.3 July 2021

Journal of Networking and Communication Systems

Received 8 May, Revised 26 June, Accepted 10 July



# Route Maintenance and Multi-Hop Routing in IoT using Optimization Algorithm

**G.Shyama Chandra Prasad**
*Associate Professor, Department of CSE,*
*Matrusri Engineering College, Saidabad, Telangana, India*
*chandrashyama6@gmail.com*

**Abstract:** In various Internet of Things (IoT) applications, messages are distributed to a few nodes or objects, based on the multicast transmissions. Nevertheless, in IoT, preceding multicast routing models are mainly concentrated on adhoc sensor networks; however, they are not robust and receptive in IoT environment. Therefore, this work develops a multicast routing protocol on the basis of the adopted optimization technique named Enhanced Shark Smell Optimization (ESSO) Algorithm on the basis of World Cup Optimization (WCO) Algorithm in the IoT network. From the multicast source node, the multicast path is modeled to several destinations using the multicast routing protocol. To multiple destinations, the multicast source node forwards the packet concurrently. At first, by adopting the adopted optimization model, the nodes are experimented with together in the IoT network and carry out the multi-cast routing model in an efficient way. The multicast routing model is performed by the multicast routing protocol by exploiting the multi-objective parameters namely delay, distance, link quality factors, energy, and trust. Moreover, using the fitness measure, the multicast routing path is effectually selected on the basis of the proposed method. By exploiting various fitness parameters, the path with the least distance is chosen as the optimal path. The multicast routing model is performed efficiently by the developed optimization approach by combining the parametric features.

**Keywords:** Fitness Parameters, IoT Network, Multicast, Path, Routing

***Nomenclature***

| Abbreviations | Descriptions |
|---|---|
| **ESSO** | Enhanced Shark Smell Optimization |
| **WSNs** | Wireless Sensor Network |
| **WCO** | World Cup Optimization Algorithm |
| **RPL** | Routing Protocol for Low Power and Lossy Networks |
| **ITS** | Intelligent Transportation System |
| **DHSSRP** | Dynamic hop selection static routing protocol |
| **PEERP** | Priority-based Energy-Efficient Routing Protocol |

## 1.Introduction

IoT is considered a novel topic that allows billions of minute machines such as sensors to be linked to the internet. Generally, IoT is exploited in many fields namely smart city, smart home, developed manufacturing, and environmental monitoring. In particular, to enable a huge number of cases on IoTs, the WSNs are considered as most hopeful technology. WSN comprises a huge amount of sensor nodes, and it has the ability to compute, sensing and communicating with restricted energy [1].In the concerned equipment or environmental field, they are generally used to sense and gather information for several IoT applications. WSNs must fulfill a requirements diversity namely reliability, real-time, and energy effectuality to attain their objectives. Nevertheless, because of several reasons in real-world test beds, the ratio of packet delivery is degraded. About 50%, the delivery ratio was minimized, and the test was modeled in a city environment packed with three as well a four stories. In the real world, the reliability is degraded, since wireless medium characteristics namely collision, fading, and interference [2].

Conversely, the main aim of IoT communication concentrated on the usage of minimum network resources and power with efficient QoS. The IoT growth finds its valuable application in IoT mostly, in the numerous applications. The network optimization lead to the power conservation and energy conservation is assisted through the routing effectuality. The ad hoc mode is extensively exploited in various IoT cases

© Resbee Info Technologies Pvt Ltd

https://doi.org/10.46253/jnacs.v4i3.a5

like ITS or environment sensing. The Ad-hoc network possesses various advantages such as impulsive deployment, infrastructure less as well as the chance to enable impermanent as well as dynamic networks cost-efficiently. Nevertheless, a few of their characteristics like the wireless links unreliability, resource constraints, dynamic topology and in energy as well as objects power processing, create novel protocols' expansion ignores security needs of applications to fulfills few quality of service. As a result, amid IoT devices, standardization works are needed in secure routing areas. Moreover, secure routing methods are currently developed which does not convene the present requirements for secure routing in IoT applications [3].

Numerous multi-path routing protocols are developed to overwhelm the need for reliability. By generating multi-paths to the destination, the multipath routing protocol is a general model which can attain the needed packet delivery ratio as well as concurrently it can transmit the packets on every path. Even though it could enhance the reliability considerably, they experience additional energy exhaust as well as a huge number of scale networks is needed due to the contribution of the huge amount of nodes to preserve the paths. For IoT environments, these disadvantages might lead to several issues. For the IoT services, as the environment which is diverse from the environment of conventional WSNs, it comprises of numerous few limited networks rather than one huge network. In a variety of forms, the network can be deployed, which comprises a comparatively huge number of nodes. Hence, conventional multipath routing protocols cannot be fulfilling needed the ratio of packet delivery due to they cannot model an adequate amount of paths. Additionally, unwanted energy utilization on the network involved a few amount of nodes that tends to possess a reduction of the lifetime of the network. Hence, for the several applications of IoT, the conventional multipath routing protocols are not appropriate [5].

A bridge node between the paths is exploited to model the multipath for IoT services. The bridge cannot attain information like the ratio of packet delay and delivery ratio via eavesdrop transmission of the packet for its perimeter paths. The issues such as delay and transmission failures occur at any one path, bridge node helps transmission using the relaying packet it attained from another path.

The main contribution of the paper is to develop an optimization technique for the secure multicast routing protocol to setup secure communication. In addition, to assure the maintenance of the route, the link lifespan is calculated. Here, the main objective is to choose the appropriate path for the secure multicast routing in order to transmit the packets to the multipath destination in a safe manner. Therefore, the proposed enhanced SSO method with WCO is used to perform for the multicast routing. It is used to discover the optimal path with the aid of the fitness parameters namely trust, delay, link quality factor, energy, as well as distance. Subsequent to optimal routes finding, for the path breakage recovery the route maintenance is performed.

## 2. Literature Survey

In 2021, Muhammad Adil [1], worked on DHSSRP to solve the load balancing problem of IoT networks priority-based communication infrastructure and in congestion-free. For the DHSSRP routing protocol, the traffic management on the basis of the priority-based information balances energy utilization with a balanced traffic environment that increases deployed IoT devices lifetime. In 2020, Sangdae Kim et al [2], a routing model were proposed in order to setup the collaboration between the paths with a bridge node. The real-time reliability in WSN had been achieved by the proposed model when it solves the limitations on energy utilization by exploiting the minimum amount of paths. In 2020, Badis Hammi et al [3], a probabilistic model was developed that contemplates two types of events that affect routing performance if a present node such as uncooperative and mobility behavior. In 2019, Mauro Conti et al [4], developed a new model named SARP for IoT networks, that was an attestation-helped secure and scalable routing protocol. By exploiting the RPL model and using the inherent features of RPL performance of the proposed model attestation in large-scale IoT networks. In 2020, Ben othman soufiene et al [5], developed PEERP by exploiting the IoT for Reliable Data Transmission in Healthcare. The health information was classified into two classifications which were related to the priorities. They are Vital Health data and emergency circumstances. For critical data, direct communication was exploited and the vital health data delivery exploits multihop communication.

## 3. IoT Model

IoT comprises of smart device which is interlinked with each other in order to swap the collected data network is exploited. In IoT, various smart devices are resource-constrained that encompass processing abilities as well as communication in order to swap the data. Fig 1 demonstrates the IoT network model in that numerous nodes in the network is inaccessible to transfer data packets by exploiting the effectual paths to the BS. Moreover, IoT is spotted amid various minimum power networking protocols namely

ZigBee, ZWave, as well as Bluetooth. For domain-specific applications aforesaid protocols are developed with inimitable characteristics. Additionally, the mart objects are energy-constrained and resource. Therefore, for management the gateway is responsible.

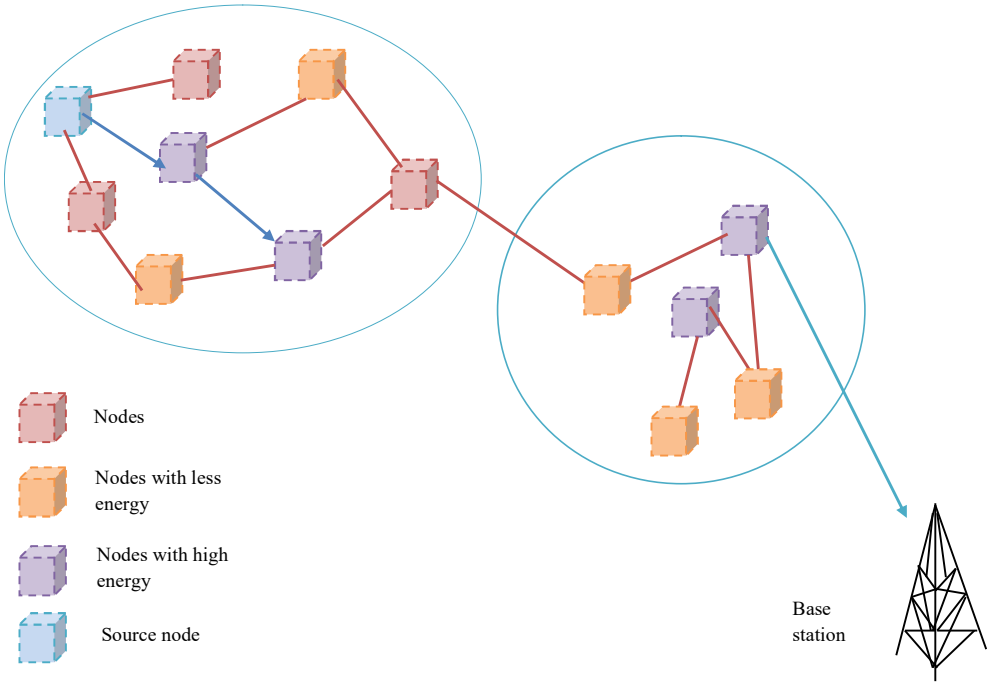



***Fig. 1.*** *System model of IoT network*

## 3.1 Energy model

By exploiting nodes' energy, the lifetime of the network is increased; the battery power is exploited by the source nodes [6].Several operations are performed by the IoT energy model, such as sleeping, transmitting idle as well as the receiving mode. To identify the path, the nodes with maximum energy are selected. Additionally, to transfer the data, the routing path with the minimum energy is used hence the route is achieved in the routing table. Hence, each node value of energy is calculated at a specific time interval. So, the node with the utilized energy is stated as follows

$$Q^{b}(s) = D_{h}^{b} * Q_{h}^{b} + D_{g}^{b} * Q_{g}^{b} \quad (1)$$

In eq. (1), $D_{h}^{b}$ symbolizes the forwarded data packets using $b^{th}$ node, $Q^{b}(s)$ symbolizes utilized energy using $b^{th}$ node at a time $s$, $D_{g}^{b}$ symbolizes received data packets using $b^{th}$ node, and $Q_{h}^{b}$ symbolizes required energy for transmitting packets and $Q_{g}^{b}$ symbolizes the required energy for receiving packets. Nevertheless, $Q_{g}^{b}$ and $Q_{h}^{b}$ is computed as,

$$Q_{h}^{b} = D * \kappa \quad (2)$$

$$Q_{g}^{b} = \alpha * \tau \quad (3)$$

$\kappa$ symbolizes the needed power to transmit data packets, $D$ symbolizes a needed time to transmit packets, $\tau$ symbolizes the needed power to receive packets and the $\alpha$ symbolizes the needed time to receive packets. Consequently, the remaining energy is stated as below,

$$Q_{\gamma} = QQ - Q^{b}(s) \quad (4)$$

$Q_{\gamma}$ is calculated and nodes energy is examined by means of the threshold value hence nodes with the minimum energy is to transmit the data, and $QQ$ indicates the sensor nodes' initial energy for every node.

## 3.2Mobility Model

In [7], the movement of the nodes is explained with the mobility model in the network. The routing process is performed by the mobility patterns of IoT in the transmission of data.

In addition, in real-time applications, the mobility model emulates the movements of the nodes. Hence, to examine the network's optimal performance due to the wide availability and ease the arbitrary mobility technique is developed.

Let two nodes as $b$ and $c$ with starting position as $(p_1,q_1)$ and $(p_2,q_2)$, correspondingly. Additionally, the nodes $b$ and $c$ moves in-network with diverse velocity on the basis of the angle $\theta_1$ and $\theta_2$ associated with the x-axis at a certain direction. Moreover, $b^{th}$ node travel by means of distance $d_1$ and $c^{th}$ node move by means of $d_2{}^{th}$ distance at $s$ time interval. Here, $b$ as well as $c$ nodes travel to the novel location at the time $s$ formerly the mobility procedure is finished. Therefore, the distance between nodes $b(p_1,q_1)$ and $c(p_2,q_2)$ is stated as,

$$\beta_{(b,c)} = \sqrt{|p_1 - q_2|^2 + |p_1 - q_2|^2} \tag{5}$$

$\beta_{(b,c)}$ indicates the distance between the nodes $b(p_1,q_1)$ and $c(p_2,q_2)$.

## 3.3 Link Lifetime Model

In [6], calculating the lifetime of the path is very important because of the alterations in dynamic topology in IoT. During the path travel of the demanding route, the link lifetime is calculated at each hop. Let $b$ as well as $c$ nodes are relied on transmission range. Therefore, the formulation of link lifespan is stated as below:

$$H = \frac{-\left(uv + yz + \sqrt{\left(u^2 + y^2\right)k^2 - (uz - yv)^2}\right)}{\left(u^2 + y^2\right)} \tag{6}$$

where, $u = R_b \cos\theta_b - R_c \cos\theta_c$

$v = x_b - x_c$

$y = R_b \sin\theta_b - R_c \sin\theta_c$

$z = r_b - r_c$

$(x_b,r_b)$ simplifies node coordinate $b$, $(x_c,r_c)$ simplifies node coordinate $c$, $R_c$ simplifies $c^{th}$ mobility node of speed, $R_b$ simplifies the $b^{th}$ node mobility speed, motion direction of $b^{th}$ node is simplified as $\theta_b$, and $\theta_c$ simplifies motion direction at $c^{th}$ node, and the $k$ indicated as transmission.

### 3.3.1 Trust model

The major contribution of this technique is to develop a trust model in the IoT for multicast routing. Here, to mitigate mistrustful nodes, the trust model is used by Cluster Heads (CHs). To ascertain the trust enable CHs, the CHs are formulated by exploiting the trust parameters [8], such as integrity factor, forwarding rate factor, consistency factors, as well as availability factors.

In this scenario, on the basis of the internet and function in a particular mode, each and every node is communicated. Additionally, for IoT, the trust model is appropriate due to the computational necessity and the minimum energy. The trust model is stated as follows:

$$T = \frac{1}{4}\left[B_{i,j} + E_{i,j} + U_{i,j} + G_{i,j}\right] \tag{7}$$

$B_{i,j}$ simplifies integrity factor, normal node to be calculated is simplified as $j$, $G_{i,j}$ simplifies availability factor, $i$ simplifies CH to calculate, and constancy factor is simplified as $U_{i,j}$, and $E_{i,j}$ simplifies the forwarding rate factor.

**i) Integrity factor:** When data is transmitted to a neighboring node, source nodes are verified the interfered data as well as recognizes if the packet data is transferred with the particular time as well as set up data as well as integrity.

The integrity factor [8] is stated as,

$$B_{i,j}(e) = \frac{m_{i,j}(e)}{n_{i,j}(e)} \tag{8}$$

$n_{i,j}(e)$ simplifies the total packets so far for forwarding and $m_{i,j}(e)$ simplifies entirely forwarded total packets.

**ii) Forwarding rate factor:** In IoT, nodes comprising restricted-energy that is communicated while sending and transmitting data. Therefore, forwarding rate factor [8] is devised as,

$$E_{i,j}(e) = \frac{C_{i,j}(e)}{J_{i,j}(e)} \tag{9}$$

$C_{i,j}(e)$ simplifies total feedback packets, as well as $J_{i,j}(e)$ simplifies total packets for forwarding.

**iii) Consistency factor:**

In IoT, the consistency factor is employed to protect the behavior of the sensor nodes by recognizing recognized nodes. Additionally, the consistency factor discovers suspicious nodes as well as riddles network data which is indicated as,

$$U_{i,j} = \chi II_{p-1}^{i,j} + \eta II_{p-2}^{i,j} + \nu II_{p-3}^{i,j} \tag{10}$$

$II_{p-1}^{i,j}$, $IL_{p-2}^{i,j}$, $II_{p-3}^{i,j}$ symbolizes JointTrust at the iteration $(p-1), (p-2)$, as well as $(p-3)$ and $\chi$, $\eta$ and $\nu$ symbolizes constants, correspondingly.

**iv) Availability factor:** Because of the elevated channel interface, directly the node is used in the network as well as the insensitive environment enormously and therefore, it is suitable to examine calculated node by verifying as well as transmitting the data. In [8], the availability factor is calculated as

$$G_{i,j}(e) = \frac{C_{i,j}(e)}{C_{i,j}(e) + fC_{i,j}(e)} \tag{11}$$

$fC_{i,j}(e)$ symbolizes the un-responded packets, and $C_{i,j}(e)$ symbolizes responded packets.

### 3.3.2 Multicast routing using the proposed model in IoT

The proposed enhanced SSO algorithm with WCO is explained to attain secure multicast routing in the IoT. At first, in a distributed environment, IoT nodes have experimented with, as a point of promising safe routing, trust, the energy, mobility, as well as link lifetime is being calculated. To make possible safe communication, the trust is calculated for each and every experimented node in the network. Moreover, consistency metrics like availability factor, integrity factor, and forwarding rate factor is calculated for all IoT nodes experimented.

The nodes are calculated amid the mobility, trust, energy, and lifetime of the link, subsequently, the secure multicast routing model is set up by exploiting the secure nodes. On basis of the developed model, a secure routing model is developed. Hence, the best manner of multicast routing is developed in an IoT environment. Fig 2 exhibits the systematic model of the proposed method for multicast routing.

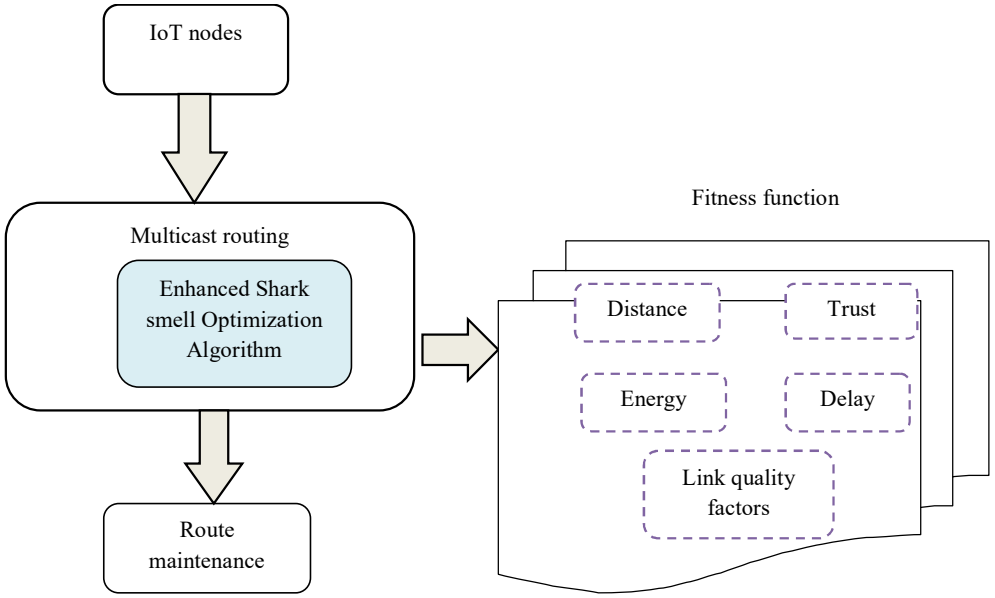



***Fig2.****Architecture model for multicast routing using the developed model*

Based on the proposed method, optimal paths are chosen by exploiting the fitness function that is executed. Moreover, the solution vector is used to estimate the optimal paths in order to transfer the data amid the sender node to the receiver node as well as this process is the same for all other probable paths produced for routing.

### 3.3.3 Fitness model

On basis of several parameters namely, delay, distance, trust link quality factors as well as energy fitness function is computed. Nevertheless, the function with maximum fitness is represented as an optimal solution that is calculated by representing minimum distance. Therefore, the fitness function is represented as,

$$\text{Fitness} = \sum_{h=1}^{N}\sum_{j=1}^{n}\left(1-E_{jh}\right)+\left(1-D_{jh}\right)+\left(1-Y_{jh}\right)+H_{jh}+T_{jh} \tag{12}$$

$E_{jh}$ indicates the energy of $j^{th}$ node of $h^{th}$ path, $H_{jh}$ symbolizes link quality of factor of a node $j$ of the path $h$, $D_{jh}$ indicates the distance of node $j$ of the path $h$, delay of $j^{th}$ node of $h^{th}$ path indicates as $Y_{jh}$, and the trust of $j^{th}$ node of $h^{th}$ path is symbolized as $T_{jh}$.

**i) Distance:** To calculate distance amid the cluster members and CHs the distance [9] model is used, whereas the minimum value is indicated as optimal CH. The distance is computed on the basis of eq. (13).

$$M_n^{\lambda} = \frac{\sum_{h=1}^{d}\sum_{\substack{i=1 \\ i\in h}}^{Q}\left\|R_j^L - R_i^A\right\| + \left\|R_i^A - R^o\right\|}{\sum_{j=1}^{d}\sum_{i=1}^{d}\left\|R_j^L - R_i^A\right\|} \tag{13}$$

The total nodes are indicated as $d$, CH is denoted as $R^A$, total CHs is symbolized as $Q$. The normal node is symbolized as, $R^L$, $R^o$ symbolizes sink node. $R_i^A$ symbolizes CH $i$, as well as the term $R_j^L$ signifies the $j^{th}$ normal node.

**ii) Delay:** By exploiting total nodes the delay [9] is calculated. If total nodes are maximumsubsequently, the delay is maximized, as well as delay formulation is stated as,

$$M_n^{\lambda} = \frac{\underset{i=1}{\overset{Q}{\text{Max}}}\left(X_{d,h}^A\right)}{d} \tag{14}$$

$X_{d,h}^A$ symbolizes cluster nodes subsist in $h^{th}$ cluster.

**iii) Energy:** The energy [9] is important to transfer data amid nodes therefore, it must be maintained maximum. By exploiting the cluster's cumulative energy the energy is calculated and summed to all energy cluster, and is formulated using,

$$M_n^{\mu} = \frac{\sum_{i=1}^{Q} R_{\mu}^A(i)}{Q \times \underset{i=1}{\overset{Q}{\text{Max}}}\left[\mu\left(R_i^L\right)\right] \times \underset{i=1}{\overset{Q}{\text{Max}}}\left[\mu\left(R_i^A\right)\right]} \tag{15}$$

$$R_{\mu}^A(h) = \sum_{\substack{h=1 \\ h\in i}}^{Q}\left[1-\mu\left(E_h^L\right)*\mu\left(R_h^A\right)\right];\ (1 \le i \le Q) \tag{16}$$

CH energy is expressed as $R_{\mu}^A(h)$, $\sum_{i=1}^{Q} R_{\mu}^A(i)$ indicates cumulative energy of whole CH and the product of total CHs with maximum energy is expressed as $Q \times \underset{i=1}{\overset{Q}{\text{Max}}}\left[\mu\left(R_i^L\right)\right] \times \underset{i=1}{\overset{Q}{\text{Max}}}\left[\mu\left(R_i^A\right)\right]$.

## 4 Proposed Enhanced Shark Smell Optimization (ESSO) Algorithm - World Cup Optimization (WCO) Algorithm

In the SSO algorithm [11], animmenseissue is its frailtytofind the global solution in some issues. Here,to resolve this issue, a hybrid model is developed. Thedisadvantage of SSO is free parameters of SSOsuch as $R_1$, $R_2$, $R_3$, $\mu_m$, as well as $\alpha_m$. Here, the WCO method [12] is developedtoenhance the global capability of SSO. This the enhancement will maximizethe utilized time of the methodas well

asconvergence speed that has the ability to enhance population diversityto evade from the local optimal point. Here, the WCO method isused to generate the free parameters of SSO such as $R_1$, $R_2$, $R_3$, $\mu_m$, and $\alpha_m$ that are restricted in the interval (0,1],i.e.

$$0 < \mu_m \le 1 \tag{17}$$

$$0 < \alpha_m \le 1$$

$$0 < R_1, R_2, R_3 \le 1$$

.

In this scenario, the WCO input population will be a $5 \times N$ population whereas those five parameters for optimizing are:

$$\left[x_1^m, x_2^m, x_3^m, x_4^m, x_5^m\right] = \left[\mu_m, \alpha_m, R_1, R_2, R_3\right] \tag{18}$$

$$C = \begin{bmatrix} x_{c1,1} & x_{c2,1} & x_{c3,1} & \cdots & x_{cM,1} \\ x_{c1,2} & x_{c2,2} & x_{c3,2} & \cdots & x_{cM,2} \\ x_{c1,3} & x_{c2,3} & x_{c3,3} & \cdots & x_{cM,3} \\ x_{c1,4} & x_{c2,4} & x_{c3,4} & \cdots & x_{cM,4} \\ x_{c1,5} & x_{c2,5} & x_{c3,5} & \cdots & x_{cM,5} \end{bmatrix} \tag{19}$$

where $N_{var}$ symbolizes the number of variable dimensions, $x_i^m$ symbolizes the system variables, C symbolizes the

continent, and $x_{i,j}$ symbolizes the $i^{th}$ team of the $j^{th}$ country. WCO M symbolizes the continents quantity, such as other population-based techniques, initiates by means of an arbitrary vector of solution. The rating parameter in this approach is attained by Rank as below:

$$\text{Rank} = \frac{\left(\beta \times \sigma + \overline{X}\right)}{2} \tag{20}$$

$$\overline{X} = \frac{1}{n} \sum_{i=1n}^{n} X_i \tag{21}$$

$$\sigma = \sqrt{\frac{1}{n-1} \sum_{i=1n}^{n} \left(X_i - \overline{X}\right)^2} \tag{22}$$

$\beta$ symbolizes a tunable parameter among 0 as well as 1, $\overline{X}$ and $\sigma$ symbolizes average as well as the standard deviation of $X$, $n$ symbolizes the team's quantity, and correspondingly. Play-Off is considered as a significant parameter in WCO that makes the global optimization which is the exploration part of the technique stronger.

$$\text{Pop} = \left[X_{best}, X_{Rand}\right] \tag{23},$$

$X_{Rand}$ symbolizes an arbitrary quantity, Pop symbolizes subsequent population of the algorithm by the $_{\text{Size}\ \ N \times M}$,

$$\frac{1}{2} \times ac \times \left(Ub - lb\right) < X_{best} < \frac{1}{2} \times ac \times \left(Ub - lb\right) \tag{24}$$

lb and Ub indicates lower as well as upper restrictions of the problem as well as ac indicates free parameter between Lb and Ub.

## 5.Result and Discussion

The outcomes of the proposed model for secure multicast routing in IoT were discussed in this section. The performance algorithm exhibited using the proposed model was calculated on basis of distance, energy, delay, trust, as well as throughput by varying the rounds such as 50 and 100. The proposed method is compared with the conventional models such as Particle Swarm Optimization Algorithm (PSO), Artificial Bee Colony (ABC), Genetic Algorithm (GA) and Grey Wolf Optimization (GWO) algorithms.

Table 1 explains the performance of techniques by exploiting measures using 50 nodes by varying the rounds. Here, it summarizes the analysis using delay metric with different number of rounds. The minimum delay is attained by the proposed model and also the minimum average routing distance is calculated by the developed algorithm. Table 2 summarizes the analysis of the proposed BSWO model

using 100 nodes. The maximum throughput value is obtained by the proposed methods. Here, the overall analysis states the performance of the proposed model is better than the conventional models.

***Table 1****Performance analysis of a proposed model and the conventional models for 50 nodes*

| Node | Metrics | PSO | ABC | GA | GWO | Proposed Model |
|---|---|---|---|---|---|---|
| 50 | ***Average Routing Distance (m)*** | 300.8 | 330.8 | 303.7 | 183.31 | 178.4 |
| | ***Delay (sec)*** | 0.0811 | 0.0835 | 0.0853 | 0.0738 | 0.0583 |
| | ***Residual energy (J)*** | 35.55 | 35.38 | 35.71 | 35.83 | 38.83 |
| | ***Trust (%)*** | 80 | 80 | 70 | 80 | 80 |
| | ***Throughput (%)*** | 50.8 | 58.54 | 75.51 | 78.11 | 87.75 |

***Table 2****Performance analysis of a proposed model and the conventional models for 100 nodes*

| Node | Metrics | PSO | ABC | GA | GWO | Proposed Model |
|---|---|---|---|---|---|---|
| 100 | ***Delay (sec)*** | 0.0813 | 0.0815 | 0.0817 | 0.0775 | 0.0753 |
| | ***Average Routing Distance (m)*** | 110.3 | 117.3 | 110.8 | 181.8 | 183.7 |
| | ***Residual energy (J)*** | 37.15 | 35.8 | 37.44 | 37.711 | 38.58 |
| | ***Throughput (%)*** | 57.75 | 77.05 | 73.04 | 75.054 | 87.75 |
| | ***Trust (%)*** | 80 | 70 | 70 | 80 | 80 |

## 6. Conclusion

In this paper, to enable the optimal multicast routing an optimal multicast routing was performed using an effectual optimization algorithm in IoT. Finally, using the communication process, the route was maintained for effectual network lifetime. On the basis of the fitness parametric metrics like distance, delay, energy, trust, and link quality factors, the optimal path was calculated. Moreover, the optimal path assures the routing model in a robust and effective way. By exploiting the developed method, the multicast routing procedure was efficiently attained. Nevertheless, the adopted model efficiently recognizes the safe multicast path by exploiting the fitness measure. Consequently, to transmit the data packets, the function with utmost fitness value was received as the best route. Subsequent to that, by exploiting experimented IoT network, the maintenance of the route was carried out. Finally, the proposed model performance was verified by means of a number of nodes. Also, these measures exhibit that the adopted model obtained maximum energy, throughput and trust, and minimum delay, and average routing distance.

## Compliance with Ethical Standards

**Conflicts of interest:** Authors declared that they have no conflict of interest.

**Human participants:** The conducted research follows the ethical standards and the authors ensured that they have not conducted any studies with human participants or animals.

## References

[1] Muhammad Adil,"Congestion free opportunistic multipath routing load balancing scheme for Internet of Things (IoT)", Computer Networks, 23 November 2020.
[2] Sangdae KimCheonyong KimKwansoo Jung,"Cooperative multipath routing with path bridging in wireless sensor network toward IoTs service",Ad Hoc Networks, 18 June 2020.
[3] Badis HammiSherali ZeadallyLyes Khoukhi,"A secure multipath reactive protocol for routing in IoT and HANETs", Ad Hoc Networks, 28 February 2020...
[4] Mauro ContiPallavi KaliyarSilvio Ranise,"Attestation-enabled secure and scalable routing protocol for IoT networks", Ad Hoc Networks, 6 December 2019.
[5] Ben othman soufieneAbdullah Ali BahattabHabib Youssef,"PEERP: An Priority-Based Energy-Efficient Routing Protocol for Reliable Data Transmission in Healthcare using the IoT",Procedia Computer Science6 August 2020.
[6] 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.
[7] 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.
[8] Zhu, J., "Wireless Sensor Network Technology Based on Security Trust Evaluation Model," International Journal of Online Engineering, vol.14, no.4, pp.211-226, 2018.

[9] Rajeev Kumar and Dilip Kumar, “Multi-objective fractional artificial bee colony algorithm to energy aware routing protocol in wireless sensor network," Wireless Networks, vol. 22, no. 5, pp 1461–1474, July 2016.

[10] Y. Rao, Z. Shao, A.H. Ahangarnejad, E. Gholamalizadeh, B. Sobhani, Shark Smell Optimizer applied to identify the optimal parameters of the proton exchange membrane fuel cell model, Energy Convers. Manage. vo1. 82 ,pp. 1–8, 2019.

[11] O. Abedinia, N. Amjady, A. Ghasemi, A new metaheuristic algorithm based on shark smell optimization, Complexity,vo1 21,no. 5, pp. 97–116, 2016.

[12] N. Razmjooy, M. Khalilpour, M. Ramezani, A New Meta-Heuristic Optimization Algorithm Inspired by FIFA World Cup Competitions: Theory and Its Application in PID Designing for AVR System, J. Control Autom. Elect. Syst. vol.27, no.4, 419–440, 2016.

[13] Dr.Sivaram Rajeyyagari,"Automatic Speaker Diarization using Deep LSTM in Audio Lecturing of e-Khool Platform",vol. 3, no. 4, October 2020.

[14] Amol V Dhumane,"Examining User Experience of eLearning Systems using EKhool Learners", vol. 3, no. 4, October 2020