Energy Efficient with Trust and Qos-Aware Optimal Multipath Routing Protocol Based on Elephant Herding Optimization for Iot Based Wireless Sensor Networks

R. Lavanya [a] and Dr.N.Shanmugapriya[b]

[a] Assistant Professor, Department of Computer Science, Dr.SNS Rajalakshmi College of Arts and Science, Coimbatore

[b] Assistant professor and Head, Department of Computer Applications, Dr.SNS Rajalakshmi College of Arts and Science, Coimbatore.

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 20 April 2021

Abstract: RPs (Routing Protocols) fail to consider node statuses like a node's lifetime or congestions in networks in during transmissions. Node's lifetime plays an important role as it needs sufficient energy to route or transmit information. However, QoS (Quality of Services) can improve network lifetimes specically in selections of multi-paths in routing information. This work proposes an energy efficient and optimal QoS aware multi-path routing protocol based on EHO (Elephant Herding Optimization) algorithm and trust called EHO-ETQRP for IoT (Internet of Things) based WSNs (Wireless Sensor Networks). This work's objective function targets QoS parameters of trust and energy. The proposed protocol identified an optimal path for routing by computing costs involving congestion and lifetimes of nodes. The protocol is evaluated for its suitability where it produces satisfactory results.

Keywords: Internet of Things (IoT), Wireless Sensor Networks (WSN), Multicast Routing, Energy, Trust, QoS, Elephant Herding Optimization (EHO).

1. Introduction

IoTs are gaining importance both industrially and academically. These devices fulfil visions of plug-and-play in devices for deployments in environments and for collaborative communications between smart devices (Shende et al., 2020). Evolutions in smart sensing devices, internet protocols, big data analytics, and machine to machine (M2M) communications have made IoTs a reality. IoTs can be viewed as two elements namely internet and things. IoTs allow non-computer devices to communicate, listen, think and compute by collaborative communications and decision making. Alternatively, they are smart devices that can benefit applications by their consensus decisions (Reddy & Babu, 2017). IoTs transform passive devices to active devices with the abilities of computations, communications, collaborations and decisions. Embedded sensors, evolving computing paradigms in technology, light weight communication, data analytics and internet protocols have led to the birth of new smart applications though there are gaps in communication protocol standards resulting in many challenges (Kharrufa et al., 2019). Scores of applications based on IoTs have erupted in the domains of healthcare, transportation, automation, agriculture, disaster management. IoTs can also play significant roles in improving the quality of business applications and life (smart homes).

WSNs have become an effective medium for integrations with IOTs. These networks encompass a number of micro-sensors with limited energy in IOT (Haseeb et al., 2020). WSNs sensors are autonomous, spatially distributed and monitor environmental changes co-operatively, examples being temperature changes, sound vibrations, pollution levels, atmospheric pressure and motion changes. MCSs (Multi-Cast Services) is an efficient model that optimize network resources with the ability of adapting changes in WSN bandwidths and can be used to enhance IoT performances (Wong & Wan, 2019). MCRPs (Multi-Cast Routing Protocols) establish different paths for transmitting data packets between a source and a destination. For Example, an IoT application using MCRPs can dynamically update commodity prices having electronic labels. RPs (Routing Protocols) can be categorised as geographic or non- geographic where in the latter packets flood all destination nodes from multi-cast sources. In geographic-based multicast routing, the nodes are aware of GPS (Global Positioning System) device locations (Jabbar et al., 2018). Multi-channel routings reduce congestions and interferences and thus increase data transfers with minimized power consumption while guaranteeing QoS constraints.

In network topologies, dynamic topologies help IoT operations better than in terms of multimedia communications. This implies that highly efficient MCRPs g that address multimedia communications need IoT applications are a need (Johnson et al., 2001). The bottom-line of any MCRP is to increase resource utilizations while reducing network's energy consumptions and hence do not cater to QoS in multimedia communications. MCRPs routing involving a BS (Base Station) in terms of secure transmissions (Kyasanur & Vaidya, 2006). WSN challenges in efficient routing are detailed below:

- IoT nodes have heterogeneity in terms of memory or effective sensors/actuators with limited memory though they are termed eligible for reliable transport using establishing routes (Biswas & Morris, 2005). This constraint in memory affects link reliability and result in higher end-to end errors.
- Communication channels using these nodes with greater mobility impose security threats in IoT based networks. Self organization of IoT nodes also leads to challenges in security in application.
- WSNs demerits include (Mo et al., 2006) environmental dynamism and random positioning of nodes.

- Restriction of power and limitation in processing abilities, limit their ranges culminating in unreliable communications.
- MCRPs are dependent on priority assignments to select routes which can be computationally intensive and untrustworthy and are generally not considered.

Thus, it is evident from the aforesaid problems that MCRPs fail to consider the status of nodes and specifically their lifetime or congestion (Cengiz & Dag, 2017). A network should have sufficient energy and routing information to transmit between a source and destination where enhancing network lifetimes and catering to QoS parameters in MCRPs is an exceedingly challenging issue. This work attempts to overcome this issue by proposing an energy efficient and optimal QoS aware multi-path routing protocol based on EHO, EHO-ETQRP for IoT based WSN applications

Following this introductory section, an exhaustive review of literature related to the study is in section two. The proposed MCRP methodology is detailed in section three followed by its simulation results in section four. This paper concludes with future scope in section five.

2. Literature Review

This section discusses a select few recent techniques that deal with MCRPs for WSNs.

DLTs (Deep Learning Techniques) were used by Sujanthi & Kalyani, (2020) in their study to improve energy efficiency. The scheme called SecDL (Secure Deep Learning) targeted dynamically clustered WSN-IoT networks. The scheme used Bi-Concentric Hexagons in Mobile Sinks to improve energy efficiency. The scheme formed dynamic clusters in Bi-Hex networks and selected CHs (Cluster Heads) optimally using QP^2 (Quality Prediction) Phenomenon for ensuring energy efficiency and QoS. The study used Co-FitDNN (Crossover based Fitted Deep Neural Network) for its optimal selection of routes. The study also addressed IoT in terms of user security by using DMTs (Data Mining Techniques) for authenticating users where authentications were based on Apriori based Robust Multi-factor Validation algorithm which mapped validations to an authentication feature set of the user.

CSA (Crow Search Algorithm) was used by Islam et al., (2019) in their study. They modified the original CSA for their objectives. Primitive CSA is based on population and gained research attention due to its tuning of only one parameter. In spite of its easy implementations, CSA exhibits weakness in finding global optimum and slow convergence rates in multi-modal optimizations. CSA's search agent does not necessarily produce the best solution. The location updates of the agent are also random adding to its disadvantages. This study used a global search operator to overcome CSA disadvantages. Their scheme also used a modified search by incorporating a niching method for increased explorations. The study was tested benchmarked with 23 functions.

BSWO (Brain Storm Water Optimisation) was used by John & Sakthivel, (2021) in their MCRP scheme for optimisations in IoT networks. The proposed MCRP functioned on multiple objective factors including distances, delays, energies, link-qualities and trust. The MCRP routing path selection was based on BSWO fitness measures which integrated BSO (Brain Storm Optimisation) and WWO (Wave Optimisation). Once multicast, routes were maintained in IoT networks to normalize link breakages. The scheme proposed BSWO outperformed other methods in simulations with minimal delay (0.0682s), average routing (178.4m), maximal energy (39.59J), maximal throughput (87.75%) and trust (90%).

The scheme QoSMIC was poroposed by Yan et al., (2002) for MCRPs in Internet. Their scheme provided QoS-sensitive paths that were flexible, scalable and resource-efficient. The proposed QoSMIC differed from other MCRPs in identifying multiple paths and selecting only paths that catered to QoS. Main advantages of QoSMIC was in its adaptivity and flexibility. Their exhaustive simulations showed that their protocol improved end-to-end performance and resources utilization in comparison to other protocols. The proposal specifically, reduced call blocking probabilities by a factor of six while reducing end-to-end delays by 90% of PIM protocol.

A complete solution for QoS based routing was proposed by Baolin & Layuan (2006). Their proposal was an extension MAODV (Multicast Ad hoc on demand Distance Vector) routing protocol and catered to delays, bandwidths while measuring packet losses. The study's solution was based on lower layer specifications. Their simulation proved that using QoS constraints, MCRPs could improve end-to-end delays, bandwidths and reduce packet losses in a rout.

Unicast routing was also used for MCRPs by Layuan & Chunlin, (2003) in their study. Their proposed scheme was a distributed QMRP (QoS-aware multicast routing protocol) which operated on top of unicast routing protocols. Their scheme gathered only local state of a link/node and did not require any global state. QMRP significantly reduced its overhead while constructing a multicast tree with QoS constraints. QMRP supported dynamic membership by allowing a multicast group member to join or leave sessions dynamically. The protocol exhibited its ability to search multiple feasible tree branches for selecting optimal/near-optimal branches while connecting new receivers to existing multicast trees thus demonstrating their QMRP's novelty in MCRPs QoS routing with dynamic membership support.

QMRP was also proposed in the study by Promkotwong & Sornil (2007). Their MCRP was based on mesh architecture which offers bandwidth guarantees for MANET applications. Their simulation experiments showed their QMRP outperformed other mesh-based MCRPs under a variety of environments.

Resource allocation figured in the study of Neto et al., (2007). Their scheme called MIRA (Multi-service Resource Allocation) was a multicast resource reservation protocol for class-based networks that addressed asymmetric routings. Their proposed MIRA controlled network resources in multicast sessions with QoS parameters of class network characteristics and availability of classes routing paths. The study also conceptually detailed on RSVP, RMD-QoSM and their proposed scheme. The study assessed session setup times, signal parameters and state overheads of MIRA with RSVP in simulations.

QMRP was again proposed by Chen et al., (2000) in their study. The proposal a QoS-aware MCRP achieved scalability by reducing communication overheads in multicast tree constructions significantly and maintaining higher level of success. The scheme achieved this by alternating between single-path and multiple-path routing based on network environments. The scheme's high level design made it operable on top of any unicast routing algorithm in intra and inter networks. The scheme has higher responsiveness by its termination mechanism based on a timeout period and detected success/failures in routing. Moreover their QMRP constructed multicast trees that were free of loops.

Network loads were balanced in the study of Zhao et al., (2010). The scheme balanced loads with a multicast algorithm that enhanced QoS in multicast communications of WMNs. The study's experimental showed that their multicast algorithm performed better than most multicast algorithms in terms of lower delays, jitter and better throughputs.

The study by Shende et al., (2020) optimized energy of MCRPs. Their proposal based on CSA and CSA and WOA (Wolf Optimization Algorithm) used an objective function for evaluating energy and trust of nodes. The initial part assessed energy and trust of nodes for establishing optimal routes chosen by their CWOA scheme which was then used as the data transmission route. The energy status of nodes was updated along with trust values towards the end of each individual transmission. This outlines the choice of secure nodes and improved secure communications in the network. Their simulation analysis using 50 and 100 nodes evaluated their scheme's performances. Their scheme achieved minimal delays (0.2729 and 0.3491), maximum detections (0.6726), high energies (66.4275 and 71.0567), and maximum throughputs (0.4625 and 0.8649) for 50 nodes in an attacked/normal state.

This literature review has summarized overall issues and challenges of MCRPs in WSNs as it is significant to understand implicit technical issues. Networks need sufficient energy to carry on transmissions with proper routing information. Moreover, the status of individual nodes like estimated lifetimes and congestion need to be considered by routing protocols for improving network lifetimes. Also, QoS parameter consideration in multipath selections is an exceedingly challenging task. Hence, this work aims to improve routing paths with QoS criteria.

3. Proposed Methodology

This research work proposes an optimal trust based energy saving QoS aware MCRP protocol for IoT based WSNs. The proposed scheme determines the path from source a to a destination using the afore said parameters. The proposed technique EHO-ETQRP is an enhancement of multicast routing based on EHO for IoT based WSNs. EHO-ETQRP mainly considers three parameters including energy consumptions, node trust values and QoS parameters. EHO-ETQRP‘s important steps are detailed below.

- Primarily network node's trust level and energy are computed mathematically.
- QoS criteria are used in optimality of cost calculations on lifetime energy and congestion in nodes.
- Based on the above two factors route are discovered by EHO.

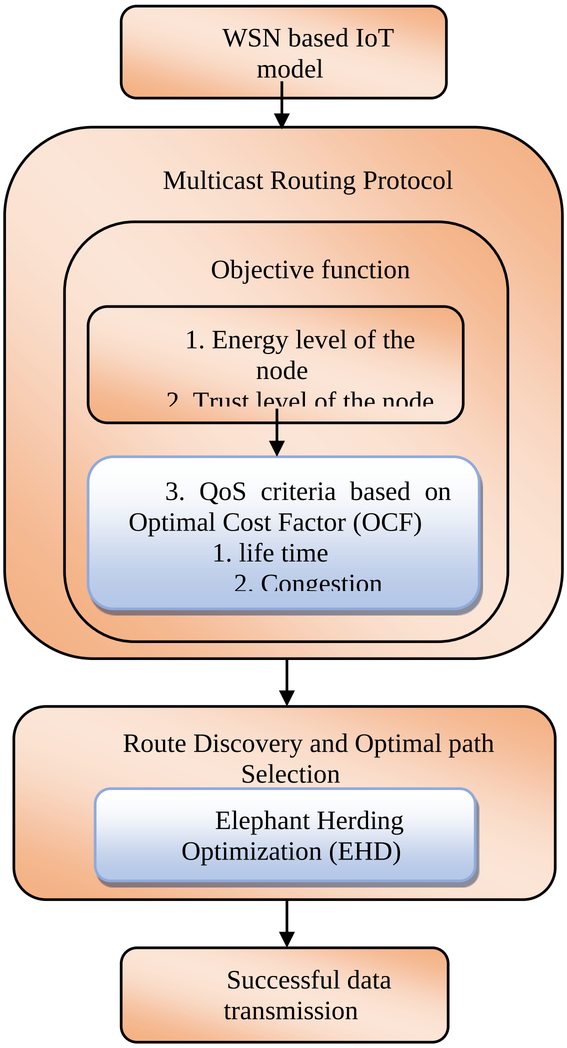

WSN based IoT model
Multicast Routing Protocol
Objective function
1. Energy level of the node
2. Trust level of the node
3. QoS criteria based on Optimal Cost Factor (OCF)
1. life time
2. Congestion
Route Discovery and Optimal path Selection
Elephant Herding Optimization (EHD)
Successful data transmission

Figure 1. Proposed Methodology of EHO-ETQRP

3.1 Proposed Protocol

The main aim of MCRPs is to distribute data to multiple destinations where this work displays an optimal performance using EHO-ETQRP. Mobile nodes in IoT networks are evaluated for their trust, energy and QoS parameters. On selection of secure nodes, routes are framed using EHO. An optimal path is then chosen for data transmissions and nodes are updated with trust/energy/QoS values at the end of transmission. This helps in assessing secure nodes in further selections. Figure 2 is the block diagram of the proposed optimized MCRP in an IoT environment with mobile nodes as forwarding agents.

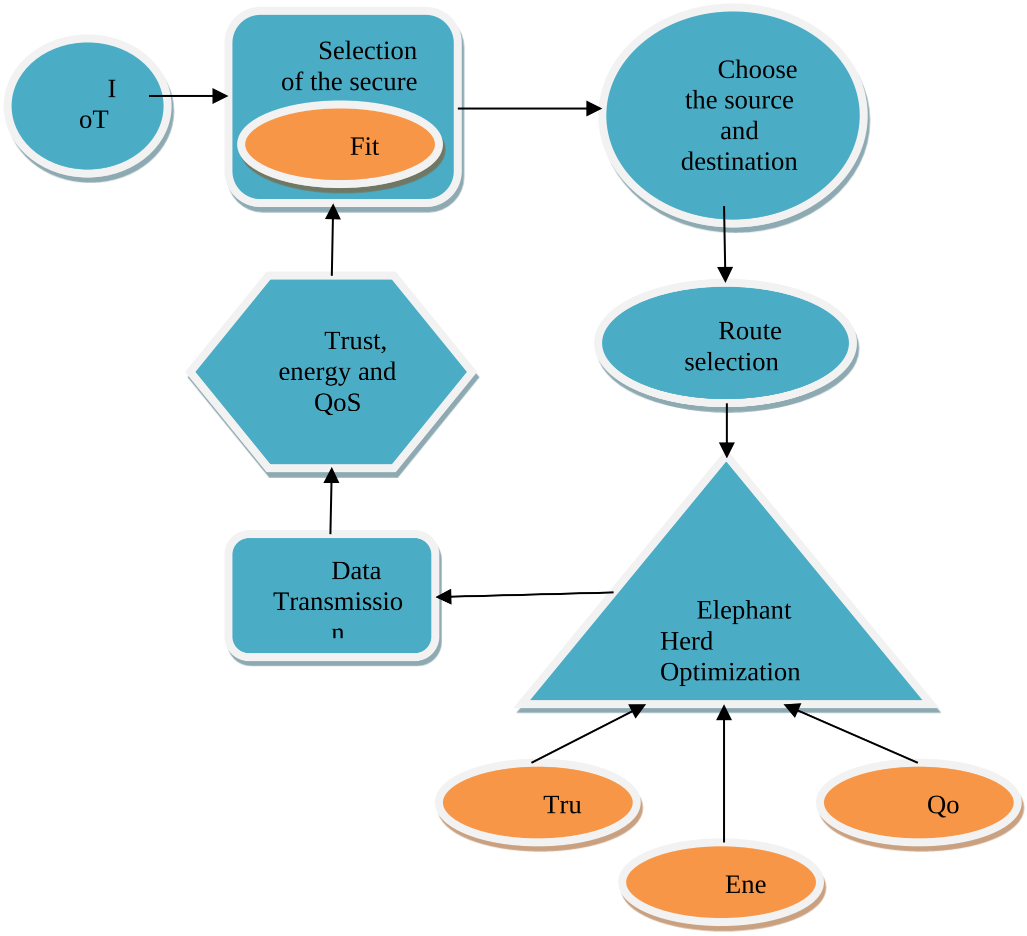


Figure 2. Proposed MCRP using EHO

Mobility of WSN nodes: Node mobility in WSNs can be described in terms of position, velocity, and acceleration and hence the performance of routing protocols in mobility models depend on their distances (Shende & Sonavane, 2020). Assuming N_i and N_j are 2 nodes placed at locations (u_i, v_i) and (u_j, v_j) such that $\Omega^i \epsilon(u_i, v_i) and\ \Omega^j \epsilon(u_j, v_j)$. N$_i$ and N$_k$ traverses in a direction with variable velocity at angles θ_1 and θ_2. The nodes N$_i$ and N$_k$ travel a distance ∂_1 and ∂_2, and after movement attain new positions (u_i^{new}, v_i^{new}) and (u_j^{new}, v_j^{new}).

Initially, the Euclidean distance of the nodes at positions $N_i(u_i, v_i)$ and $N_j(u_j, v_j)$ is given as,

$$\partial_{(uv,0)} = \sqrt{|u_i - u_j|^2 + |v_i - v_j|^2} \qquad (1)$$

The velocity of the nodes N_i and N_k is v_{Ni} and v_{Nj} making an angle θ_1 and θ_2 to travel the distances ∂_1 and ∂_2 that is represented as,

$$\partial_1 = v_{Ni} \times t \qquad (2)$$

$$\partial_2 = v_{Nj} \times t \qquad (3)$$

At t, the node acquire a new position, which is given by,

$$u_i^{t+1} = u_i^t + v_{Ni} \times t \times cos\theta \qquad (4)$$

$$v_i^{new} = v_i^{old} + v_{Ni} \times t \times cos\varphi \qquad (5)$$

When the node $N_k(u_k, v_k)$ travel a distance ∂_2 making an angle θ_2, the node v_j acquire a new position as given as,

$$u_j^{t+1} = u_j^t + v_{Nj} \times t \times cos\theta \qquad (6)$$

$$u_j^{t+1} = u_j^t + v_{Nj} \times t \times cos\theta \qquad (7)$$

After the nodes attain a new position, the distance between the nodes is computed as given by,

$$\partial_{(u^{t+1} v^{t+1},t)} = \sqrt{|u_i^{t+1} - u_j^{t+1}|^2 + |v_i^{t+1} - v_j^{t+1}|^2} \qquad (8)$$

3.2 Fit Factor Computations for Secure Node Selection

This work's fit factor is very important in selecting secure nodes for its communication security in the network and helps enhancements in data integrity and confidentiality. The used fit factor is computed for network node's trust and energy where maximal trust and energy are the criteria for node selections. Fit factor is computed as follows,

$$Fit_{ij} = D = \frac{1}{2} \times \left[\varepsilon_i + \frac{1}{N} \times \sum_{\substack{j=1 \\ i \in j}}^{N} T_{ij} \right] \quad (9)$$

Where, N – count of neighbors, e_i - i^{th} node's energy and T_{ij} - i^{th} node's j^{th} neighbour's rust value. Only genuine nodes in the IoT network are selected based on the results of the above equation which then participate in the proposed selected optimized routes.

3.2.1 Trust Calculations

The trust/energy of IoT network's nodes are computed using Equations given below:

$$T_{ij} = T_{ij}^{direct} + T_{ij}^{indirect} + T_{ij}^{recent} + T_{ij}^{bytes} \quad (10)$$

Node trusts are evaluated using trust values and bytes transferred. Initial value of node's trust is set to a maximum of 1 and includes: T_{ij}^{direct}, $T_{ij}^{indirect}$, T_{ij}^{recent} , T_{ij}^{bytes}.

3.2.2 Direct Trust

Direct trust is based on actual and estimated time deviations computed on a witness factor which demarcates nodal trust enhancements. This factor is based on the ith node's receipt of a public key from the sth sink node in the IoT network. It is used to authenticate the nodes and hence trust value is based on the approximate time of nodes. Direct trust is formulated as,

$$T_{ij}^{direct}(t) = \frac{1}{3} \left[T_{ij}^{direct}(t-1) - \left[\frac{T^{key} - E^{key}}{T^{key}} \right] + \omega \right] \quad (11)$$

Where, T^{key} - Fitting time to send the key, E^{key} – Anticipated time for receiving the key, and x - witness factor of jth destination.

3.2.3 Indirect Trust

Indirect trust is equally important to nodes receiving public keys for authenticating nodes without a witness value. This parameter specifies nodes trust worthiness and computed using

$$T_{ij}^{indirect}(t) = \frac{1}{N} \sum_{i=1}^{N} T_{i,x}^{direct}(x) \quad (12)$$

Where, N – count of neighbors of the i^{th} node

3.2.4 Recent Trust

Recent trust is a regression value of node's direct and indirect trusts, key authenticity, sink's acknowledgment and computed using

$$T_{ij}^{recent}(t) = \alpha * T_{ij}^{direct}(t) + (1-\alpha) \times T_{ij}^{direct}(t) \quad (13)$$

With an α value equal to 3.

3.2.5 Trust based on the Bytes Transferred

Robustness of routing is enhanced by including trust factor based on the count of bytes transferred between a source and destination in transmissions. The trust factor is computed as

$$T_{i,j}^{\partial} = \frac{1}{2} \times \left[\frac{\partial_{i,j}^{i}}{d} + \frac{\partial_{i,j}^{j}}{d} \right] \quad (14)$$

Where, $\partial_{i,j}^{i}$ - count of bytes forwarded from the source and $\partial_{i,j}^{j}$ - bytes received at the destination. d. data sent/received constraint.

3.2.6. Energy Model of the Network

IoT sensors are powered by batteries limiting their energies. The energy depletions need to be controlled as it is essential to extend their IoT network life-times. Assuming battery energy in the beginning of communications is e0. In communications, energy is lost and its intensity is dependent on the nature of the node and distance of transmission. The receiving node can be a CH or normal node in a cluster. Transmissions are also dependent on routing protocol's dissipation of energy which use radio frequencies and power amplifier. Energy dissipations occur in node's data transmissions and based on the following equation,

$$\varepsilon_{dis}(K_i) = \varepsilon_{elec} \times l_i + \varepsilon_{pa} \times l_i \times \left\| K_i - H_j \right\|^4; if \left\| K_i - H_j \right\| \geq \beta_0 \quad (15)$$

Where, ε_{elec} is electrical energy and $\varepsilon_{dis}(K_i)$ is i^{th} node's dissipation of energy. The bytes sent by the i^{th} node is i while epa is the power amplifiers energy. Energy dissipation parameter b0 is compared with the computed distance between the i^{th} sensor node and j^{th} head. Whenever distance (Ki, Hj) s < b0, energy dissipation can be computed using Equation (15) else energy dissipation of Ki is computed using Equation (16).

$$\varepsilon_{dis}(K_i) = \varepsilon_{elec} \times l_i + \varepsilon_{fs} \times l_i \times \left\| K_i - H_j \right\|^2; if \left\| K_i - H_j \right\| < \beta_0 \quad (16)$$

and $$L_{D0} = \sqrt{\frac{\varepsilon_{fs}}{\varepsilon_{pa}}} \quad (17)$$

Where, ε_{fs} - free space energy. Electrical energies are dependent on modulations, filtering, coding, and other transmitter related elements. The data aggregation can be given as,

$$\varepsilon_{elec} = \varepsilon_{tx} + \varepsilon_{agg} \quad (18)$$

Where, ε_{tx} - transmitter energy and ε_{agg} - data aggregation energy. $\left\| K_i - H_j \right\|$ - distance between i^{th} node and j^{th} CH. In a normal mode K_i attempts to communicate with Hjand CH loses energy while receiving the transmitted data bytes received. This energy dissipation of the CH is,

$$\varepsilon_{dis}(H_j) = \varepsilon_{elec} \times l_i \quad (19)$$

At the end of transmission nodes and CHs are updated based on dissipated energy given by

$\varepsilon_{t+1}(K_i) = \varepsilon_t(K_i) - \varepsilon_{dis}(K_i)$ (20)

$\varepsilon_{t+1}(H_i) = \varepsilon_t(H_i) - \varepsilon_{dis}(H_i)$ (21)

Where, H_i – CH's energy dissipation or receiver node in transmissions The energy updates are followed till the node energy becomes zero or dead.

3.3 QoS Criteria for Selecting Route Paths

Intermediate nodes find their next hop neighbour optimal paths. OCFs (Optimal Cost Factors) choose best 1-hop neighbour by evaluating two parameters namely estimated lifetimes and congestion levels of nodes. The computations of maximum Lifetimes and minimized congestion levels progressively lead to optimal paths towards destinations for successful data transfers. The protocol follows steps detailed below:

Initialization Phase: Each sensor node computes its OCF and also acquire its neighbour information for storing it in a routing table. This table is the base for identifying next best hop-node in the destination route.

Establishing routes: In the absence of known paths source nodes initiate a route finding process by distributing PDReq (Path discover request) packets to its one-hop neighbors. Intermediate nodes rebroadcast these packets based on OCF values of their neighbouring 1-hop nodes and stored in routing tables till a destination node is found. On receipt of the PDReq packet, destination node acknowledges with PDRep (Path discover reply) packets. The path followed by these packets is the reverse of PDReq packet path. The process is terminated when the PDReq packet reaches the destination.

Data Forwarding Phase: Multiple paths from a source to a destination are generated in the route discovery phase. The OCFs of the paths are compared to forward the best path for data to follow.

Route Maintenance Phase: This is the update phase where network Lifetime and congestion level of neighboring nodes get updated in the routing table after each round's completion. The OCF considered by the protocol in each node is based on the following equation.

$OCF = \delta L_E + (1 - \delta)C_L$ (22)

Where. OCF - optimal cost factor, L_E - estimated life time of node, C_L - node's congestion level and δ - coefficient of proportionality = 0.7 in this work. Nodes with higher OCF have higher chance of being selected as a middle node where OCF is determined by computations following parameters influences.

3.3.1 Estimated Life Time of Node

A node's Life time can be estimated using the following equation:

$L_E =$ (23)

Where, R_E - node's residual energy, T_r - node traffic rate and T_p - node's transmission Routing protocols should prioritize network connectivity and acquire equal amount of energy in the topology.

3.3.2 Congestion Level

Node congestion is evaluated using:

$C_L = T_r/S_r$ (24)

Where, T_r- traffic rate and count of packets arriving at a node in unit time, S_r - service rate or count of packets sent in unit time. When the arrivals and departures match it implies the absence of congestion and thus ensures that the node can process packets in unit time.

3.4 Generation and Selection of the Optimal Routes based on the Proposed EHO-ETR Protocol

After the selection of genuine nodes in the IoT network, sources and destinations are fixed. The proposed EHO-ETR uses random generation of routing paths and then selects the optimal path using an optimization objective function based on fit factor of IoT nodes. The steps followed in optimal route selections are detailed below:

3.4.1 Solution Encoding

An encoding solution signifies node participation in routing. In multicast routing, the source is fixed but have multiple destinations with involvement of intermediate nodes. The dimension of the solution vector is given as, $(m \times k)$, where, m stands for multicast destinations while k indicates the maximum count of intermediate nodes.

3.4.2 Optimization Steps in EHO

Optimal routes in this work are determined using EHO, a novel nature-inspired optimization metaheuristic algorithm illustrated in (Ismaeel et al., 2019):

- **Clan Operator**

Elephants live together in clans under a matriarch leader. Each elephant clan has its next position influenced by the matriarch ci. For an elephant j in clan ci can be updated using the following Equation:

$x_{new,ci,j} = x_{ci,j} + \alpha \times (x_{best,ci} - x_{ci,j}) \times r$ (25)

Where, $x_{new,ci,j}$ and $x_{ci,j}$ - updated and old positions of elephant j in clan ci, α ∈ [0, 1] – scaling factor influenced by the matriarch on $x_{ci,j}$. $x_{best,ci}$ implie the fittest individual elephant in the clan and r ∈ [0, 1]. The fittest elephant in each clan is updated using the following Equation:

$x_{new,ci,j} = \beta \times (x_{center,ci})$ (26)

Where 1 ≤ d ≤ D implies the dth dimension, D - total dimension. nci – count of elephants in clan ci. $x_{ci,j}$, d - dth individual elephant in $x_{ci,j}$. The center of clan ci, $x_{center,ci}$ can be computed through D calculations as given in the defined Equation.

- **Separating Operator**

Generations of elephants using the separation operator is given by the Equation:

$$x_{worst,ci} = x_{min} + (x_{max} - x_{min} + 1) \times rand \qquad (27)$$

Where, x_{max} and x_{min} are individual elephant's upper and lower bounds, $x_{worst,ci}$ is the worst elephant in the clan ci and rand ∈ [0, 1] is a stochastic and uniform distribution in the interval [0, 1].

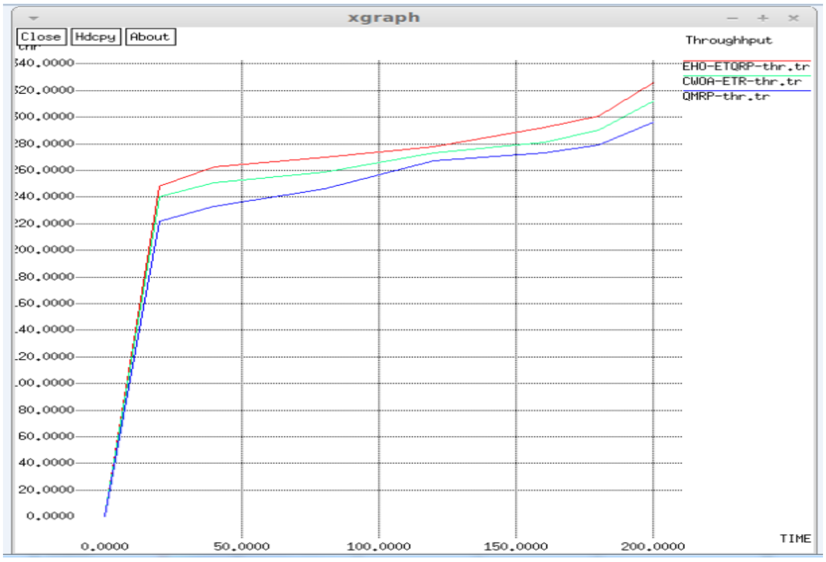
4. Results and Discussion

This section deliberates the experimental analysis and discussion of the IoTs based on the proposed multicast routing algorithm. The evaluation of the results is deeply elaborated in this section. The experiment is analyzed in MATLAB and the simulation is developed with 200 nodes for analysis. The metrics employed for the analysis include: delay, energy, and throughput of the network. The network energy refers to the energy remaining in the nodes after the end of the transmission and it should be a maximum value in order to extend the lifetime of the network. The throughput of the network is the total data rates transmitted over the network within a particular time and delay refers to the time taken for the transmission of the data. The effective method contributes with the maximal energy, throughput but with minimal delay.

Table 1. Performance Comparison Results for Throughput

No.of nodes	QMRP	CWOA-ETR	EHO-ETQRP
20	222	240	248
40	233	251	263
80	246	259	270
120	267	273	278
160	273	281	292
180	279	290	301
200	296	312	326

Table 1. illustrate the performance comparison results for throughput between the proposed and existing methods.



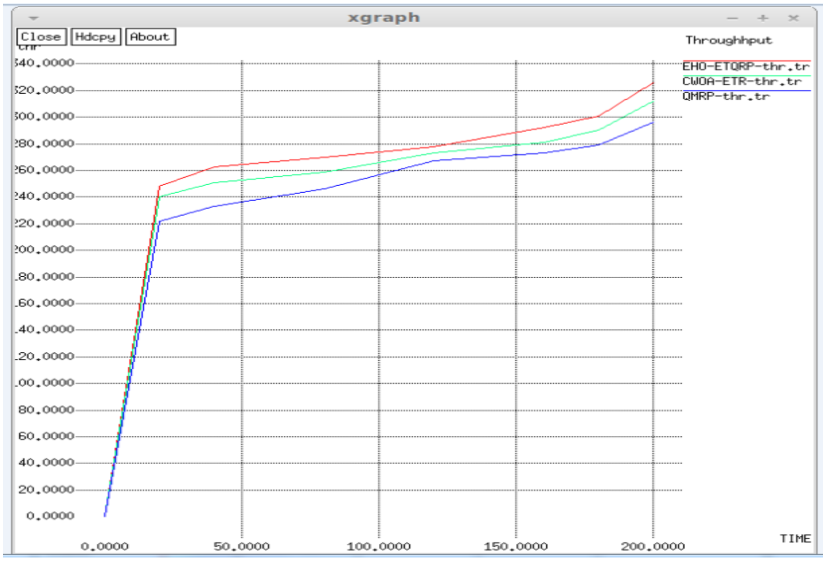


Figure 3. Comparison of Throughput between the Proposed EHO-ETQRP and Existing Methods

In the figure 3 shows the throughput of the proposed EHO-ETQRP is better performance than the existing methods. The proposed EHO-ETQRP produce higher throughput. It concludes that the proposed method produces higher throughput when compare to the existing routing protocol methods.

Table 2. Performance Comparison Results for Consumed Energy

No.of nodes	QMRP	CWOA-ETR	EHO-ETQRP
20	2.87	2.70	2.61
40	2.96	2.83	2.76
80	3.01	2.92	2.81
120	3.1	3.05	2.90
160	3.21	3.15	3.02
200	3.46	3.26	3.11

Table 2. illustrate the performance comparison results for Consumed energy between the proposed and existing methods.

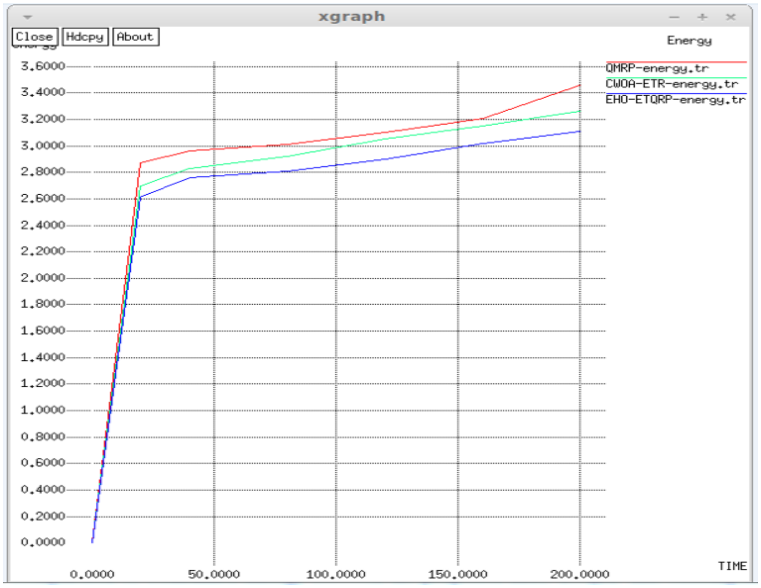


Figure 4. Comparison of Consumed Energy between the Proposed EHO-ETQRP and Existing Methods

In the figure 4 shows the Consumed Energy of the proposed EHO-ETQRP is better performance than the existing methods. The proposed EHO-ETQRP consume less energy. It concludes that the proposed method consumes less energy when compare to the existing routing protocols.

Table 3. Performance Comparison Results for Delay

No.of nodes	QMRP	CWOA-ETR	EHO-ETQRP
20	0.3	0.24	0.18
40	0.33	0.29	0.20
80	0.40	0.31	0.26
120	0.49	0.36	0.29
160	0.49	0.40	0.32
200	0.51	0.43	0.33

Table 3. illustrate the performance comparison results for delay between the proposed and existing methods.

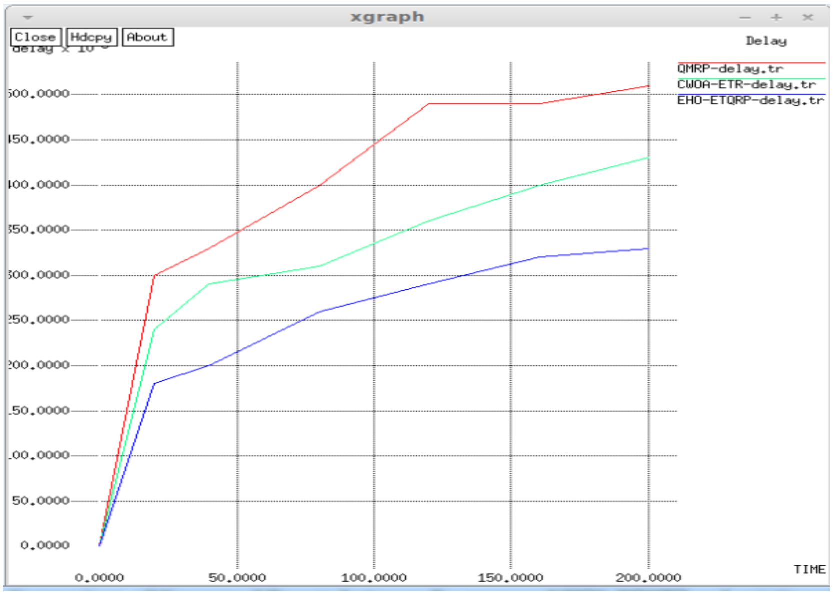


Figure 5. Comparison of Delay between the Proposed EHO-ETQRP and Existing Methods

In the figure 5 shows the delay comparison between the proposed EHO-ETQRP is better performance than the existing methods. The proposed EHO-ETQRP has less delay. It concludes that the proposed method gives less delay when compare to the existing routing protocols.

5. Conclusion

This research work proposes a new optimal path section protocol for IoT based wireless sensor network. In this energy with trust and QoS-aware multicast routing is essential in IoT applications, which is performed using the proposed optimization, EHO. The optimal selection of the routes for multicast routing is enabled using the objective function depending on the trust and energy and QoS factors that chooses the effective nodes for establishing the routes for data transmission. Based on the energy and trust update, the secure nodes are selected and which improves the secure communication. The analysis using 50 and 100 nodes in the simulation environment reveals that the proposed method acquired better performance in comparison with the existing methods. The simulations are performed using NS2 simulator under various conditions of operation. The proposed protocol is compared with the standard state of the art strategies. The different parameters considered for comparison are throughput, energy consumption and delay. The simulation result proves that the proposed routing protocol used to increase the delivery ratio, energy efficiency and network lifetime, which are the network related QoS parameters. The future direction of the proposed work includes the implementation of cluster-based routing protocol for increasing the network performance.

References

1. Shende, D. K., Sonavane, S. S., & Angal, Y. (2020). A Comprehensive Survey of the Routing Schemes for IoT applications. *Scalable Computing: Practice and Experience*, *21*(2), 203-216.

2. Reddy, P. K., & Babu, R. (2017). An evolutionary secure energy efficient routing protocol in Internet of Things. *Int. J. Intell. Eng. Syst*, *10*(3), 337-346.
3. Kharrufa, H., Al-Kashoash, H. A., & Kemp, A. H. (2019). RPL-based routing protocols in IoT applications: A Review. *IEEE Sensors Journal*, *19*(15), 5952-5967.
4. Haseeb, K., Ud Din, I., Almogren, A., & Islam, N. (2020). An energy efficient and secure IoT-based WSN framework: An application to smart agriculture. *Sensors*, *20*(7), 1-14.
5. Wong, K. S., & Wan, T. C. (2019). Current state of multicast routing protocols for disruption tolerant networks: Survey and open issues. *Electronics*, *8*(2), 1-28.
6. Jabbar, W. A., Saad, W. K., & Ismail, M. (2018). MEQSA-OLSRv2: A multicriteria-based hybrid multipath protocol for energy-efficient and QoS-aware data routing in MANET-WSN convergence scenarios of IoT. *IEEE Access*, 76546-76572.
7. Johnson, D. B., Maltz, D. A., & Broch, J. (2001). DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks. *Ad hoc networking*, *5*(1), 139-172.
8. Kyasanur, P., & Vaidya, N. H. (2006). Routing and link-layer protocols for multi-channel multi-interface ad hoc wireless networks. *ACM SIGMOBILE Mobile Computing and Communications Review*, *10*(1), 31-43.
9. Biswas, S., & Morris, R. (2005). ExOR: Opportunistic multi-hop routing for wireless networks. In *Proceedings of the 2005 conference on Applications, technologies, architectures, and protocols for computer communications*, pp. 133-144.
10. Mo, Z., Zhu, H., Makki, K., & Pissinou, N. (2006). MURU: A multi-hop routing protocol for urban vehicular ad hoc networks. *Third Annual International Conference on Mobile And Ubiquitous Systems: Networking & Services*, pp. 1-8.
11. Cengiz, K., & Dag, T. (2017). Energy aware multi-hop routing protocol for WSNs. *IEEE Access*, *6*, 2622-2633.
12. Sujanthi, S., & Kalyani, S. N. (2020). SecDL: QoS-Aware Secure Deep Learning Approach for Dynamic Cluster-Based Routing in WSN Assisted IoT. *Wireless Personal Communications*, *114*(3), 2135-2169.
13. Islam, J., Vasant, P. M., Negash, B. M., & Watada, J. (2019). A modified crow search algorithm with niching technique for numerical optimization. *IEEE Student Conference on Research and Development (SCOReD)*, pp. 170-175.
14. John, J., & Sakthivel, S. (2021). Brain Storm Water Optimisation-Driven Secure Multicast Routing and Route Maintenance in IoT. *Journal of Information & Knowledge Management*,
15. Yan, S., Faloutsos, M., & Banerjea, A. (2002). Qos-aware multicast routing for the Internet: The design and evaluation of Qosmic. *IEEE/ACM Transactions on networking*, *10*(1), 54-66.
16. Baolin, S., & Layuan, L. (2006). QoS-aware multicast routing protocol for Ad hoc networks. *Journal of Systems Engineering and Electronics*, *17*(2), 417-422.
17. Layuan, L., & Chunlin, L. (2003). A distributed QoS-Aware multicast routing protocol. *Acta Informatica*, *40*(3), 211-233.
18. Promkotwong, D., & Sornil, O. (2007). A Mesh-based QoS aware multicast routing protocol. In *Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD 2007)*, pp. 1046-1051.
19. Neto, A., Cerqueira, E., Rissato, A., Monteiro, E., & Mendes, P. (2007). A resource reservation protocol supporting QoS-aware multicast trees for next generation networks. *IEEE Symposium on Computers and Communications*, pp. 707-714.
20. Chen, S., Nahrstedt, K., & Shavitt, Y. (2000). A QoS-aware multicast routing protocol. *IEEE Journal on selected areas in communications*, *18*(12), 2580-2592.

21. Zhao, L., Al-Dubai, A. Y., & Min, G. (2010). GLBM: A new QoS aware multicast scheme for wireless mesh networks. *Journal of Systems and Software*, *83*(8), 1318-1326.
22. Shende, D. K., & Sonavane, S. S. (2020). Crow Whale-ETR: Crow Whale optimization algorithm for energy and trust aware multicast routing in WSN for IoT applications. *Wireless Networks*, 1-19.
23. Ismaeel, A. A., Elshaarawy, I. A., Houssein, E. H., Ismail, F. H., & Hassanien, A. E. (2019). Enhanced elephant herding optimization for global optimization. *IEEE Access*, *7*, 34738-34752.