Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2022.020551
Article

Tech Science Press

Quantum Firefly Secure Routing for Fog Based Wireless Sensor Networks

R. Dayana[1,*] and G. Maria Kalavathy[2]

[1]Department of Computer Science and Engineering, Jeppiaar Institute of Technology, Chennai, 631604, Tamil Nadu, India
[2]Department of Computer Science and Engineering, St. Joseph's College of Engineering, Chennai, 600119, Tamil Nadu, India
*Corresponding Author: R. Dayana. Email: dayanacse006@gmail.com

Received: 29 May 2021; Accepted: 20 July 2021

Abstract: Wireless Sensor Networks (WSNs) become an integral part of Internet of Things (IoT) and finds their applicability in several domains. As classical WSN faces several issues in service-based IoT applications, fog computing has been introduced in real-time, enabling local data processing and avoid raw data transmission to cloud servers. The Fog-based WSN generally involves advanced nodes, normal nodes, and some Fog Nodes (FN). Though the Fog-based WSN offers several benefits, there is a need to develop an effective trust-based secure routing protocol for data transmission among Cluster Heads (CHs) and FNs. In this view, this paper presents a Quantum Firefly Optimization based Multi-Objective Secure Routing (QFO-MOSR) protocol for Fog-based WSN. The main intention of the QFO-MOSR technique is to derive an optimal selection of routes between CHs and FNs in the network. The QFO-MOSR technique has incorporated the concepts of quantum computing and Firefly (FF) optimization algorithm inspired by the flashing behaviour of FFs. In addition, a multi-objective fitness function is derived by the QFO-MOSR technique using seven objectives: distance, inter-cluster distance, energy, delay, intra-cluster distance, link lifetime, and trust. The proposed routing technique derives a fitness function including trust factor from ensuring security. The design of the QFO-MOSR technique with a multi-objective fitness function shows the novelty of the work. To validate the performance of the QFO-MOSR technique, a series of experiments were carried out, and the results are investigated in terms of different measures. The experimental analysis ensured that the QFO-MOSR technique is superior to other methods in terms of different measures.

Keywords: Fog computing; internet of things; wireless sensor networks; energy efficiency; cluster heads; firefly algorithm; fitness function

1 Introduction

Next-generation Wireless Sensor Networks are expected to be placed in Internet of Things (IoT). The IoT has transformed the present world of technology. The electronic devices such as home appliances, medical equipment, cameras etc., can interact via the internet connecting several Sensor Nodes (SN). Therefore, these devices have few restrictions and involve processing power, bandwidth, storage, and a restricted power source. WSN is widely utilized in the monitoring activities of the present society like heat energy in greenhouses, emission from hydraulic power plants, forest fire, and production of vehicles in the automobile industry.

In traditional WSN, the SN can transfer their raw data to BS for storage and analysis. Current developments in IoT technology have allowed WSN for transferring raw data to the cloud for storage and processing [1,2]. But rather than transferring the large quantity of sensed data produced in the SN on the network and later process them by utilizing a Cloud Computing (CC) framework, a few processes are executed nearer to the WSN using fog computing. Fog computing consists of network devices like proxy servers, routers, gateways, and set-top boxes [3]. These devices have high processing ability and memory compared to other SN. This method does not preserve SN's energy dissipation in communication; however, it offers location awareness, higher bandwidth, and lower latency for WSN. Cisco's 'Fog Computing' was established to conquer restrictions in CC [4,5]. They contain a power source, higher processing power, and more storage for fog servers from the network. This novel technique is designed at the end of the network. It provides various advantages for end-users and involves fewer bottlenecks, data security, effective network bandwidth utilization, high speed of analysis resolving higher latency over the network, and increased trustworthiness of transmitted sensed data.

The combination of fog computing with WSN and IoT makes a novel kind of service named Fog as a Service (FaaS). But for the absolute utilization of fog computing, every fog node should satisfy the following conditions: (i) simultaneous data collection from lower end nodes, (ii) high processing power and efficiency for supporting real-world data analysis and processing, (iii) higher service trustworthiness, and (iv) low power utilization, to attain long time exploitation. In the WSN framework, they offer to the elemental SN. The combination of fog computing with WSN could conquer several challenges. In hierarchical WSN, a sink node, i.e., a CH, is generally utilized for aggregating the sensed data in cluster members, and cluster routing protocols are placed to decrease the energy consumption and network traffic [6]. Thus, the balanced load of hierarchical WSN is a significant problem that defines an entire network's efficiency. Simultaneously, at a higher level, CH is compromised and captured, which would influence the data security of the whole network [7,8]. Generally, these security attacks are classified as internal and external attacks for WSN.

This paper presents a Quantum Firefly Optimization based Multi-Objective Secure Routing (QFO-MOSR) protocol for Fog-based WSN. The QFO-MOSR technique is derived from the concepts of quantum computing and the FF optimization algorithm. Besides, a multi-objective fitness function is derived by the QFO-MOSR technique using seven objectives: distance, inter and intra-cluster distance, energy, delay, link lifetime, and trust. The design of the QFO-MOSR technique with a multi-objective fitness function shows the novelty of the work. To validate the performance, the QFO-MOSR, including the trust factor in the fitness function, ensures security. To investigate the effectual outcome of the QFO-MOSR technique, simulations occur, and the results are examined under distinct dimensions. In short, the contributions of the paper are listed as follows.

- Design a new QFO-MOSR technique for Fog-based WSN.
- Design a fitness function using seven inter-related parameters to select CH.
- Include trust factor in the fitness function to ensure security in Fog-based WSN.
- Validate the performance of the QFO-MOSR technique using the Network Simulator (NS)-3.

2 Literature Review

Fang et al. [9] presented a Gaussian Distribution based Comprehensive Trust Management System (GDTMS) for FIWSN. Additionally, their trust decision, namely, the grey problem solving, is presented to attain the tradeoff between security energy consumption and transmission efficiency. The presented tradeoff could efficiently choose the secure and robust transmit node, specifically the trust management-based secure routing system. Additionally, the proposed method is also appropriate to defend against bad-mouthing attacks. Arapoglu et al. [10] proposed a GDTMS for FIWSN. Moreover, in this trust management, the analytical hierarchy procedure is presented to attain the tradeoff between energy consumption security and transmission efficiency. The presented trade-off could efficiently choose the robust and secure transmit node. In Fang et al. [11], a Lightweight Trust Management Scheme (LTMS) is presented depending upon binomial distribution for protecting from internal attacks. Concurrently, environment, energy, distance, and security domains are assumed and presented to a Multi-dimensional Secure Clustered Routing (MSCR) system by utilizing dynamic dimensional weight in hierarchical WSN. Revanesh et al. [12] proposed a distributed protocol named Secure Coronas Based Zone Clustering and Routing (SC-ZCR). Abidoye et al. [13] proposed an effective routing protocol for data transmission in WSN known as energy effective hierarchical routing protocol for WSN based on fog computing. Fog computing is combined with the presented system because of its ability to enhance the restricted power source of WSN and the need for IoT applications. Furthermore, they proposed an enhanced ACO method to construct an optimum path for effective data transmission to SN. Cara et al. [14] developed and designed a wireless SN for fog computing architecture to address two significant problems: deployment and development of strong transmission facilities, such as network resilience provisioning and energy consumption. The implementation is directed by investigating the related macro architectural feature and functioning limitations of the network architecture. Wang et al. [15] presented a Fog-based hierarchical trust method for this cybersecurity deficiency. This hierarchical method comprises two divisions, trust among Cloud Service Providers (CSP) and trust in the basic framework and Sensor Service Provider (SSP). Rafi et al. [16] presented an enhanced LEACH protocol called LEACH with Dijkstra's Algorithm (LEACH-DA) in a cloud platform that enhances the power utilization/energy use depending upon shorter path selection. Similarly, the presented architecture includes load balance by selecting a suitable CH node between its alternative by estimating its traffic condition with the base station or cloud. Moreover, they utilize a fog computing module for this condition (i.e., LEACH-DA-Fog) to raise the network lifetime related to the actual execution of the basic protocol. Borujeni et al. [17] presented a novel technique depending upon Fog-based energy-efficient routing protocol for WSNs (P-SEP) that utilizes ACO-based routing of FN (FEAR) and PEGASIS-based routing of FN (FECR) methods in execution. This method develops the efficiency of fog enabled WSN and extends the network lifespan. The efficiency of the presented technique is calculated towards P-SEP. Though several techniques are available in the literature, there is still a need to design a new protocol to achieve energy efficiency and security in Fog-based WSN. Besides, most of the works have not considered the interrelated metrics and trust factors to select CHs.

3 The Proposed QFO-MOSR Model

Fig. 1 showcases the overall working process of the QFO-MOSR model. The proposed QFO-MOSR model aims to select the routes to the destination optimally. Once the presented model derives a fitness function, the possible paths towards the destination are identified. Followed by that, the QFO-MOSR model chooses an optimal route to the destination from the available paths. A significant component in introducing the technique is solution encoding. The proposed technique for detecting an optimum path from source (S) to destination (D) is assumed as a binary search problem. Here, D = {p_1, p_2, … , p_k} denotes destination containing *'k'* paths created using an intermediate node among S and D nodes [18]. The number in the network is based on node count N, thus the interval 0 ≤ p_k ≤ N. Henceforth, the solution count present in the network among S and D is denoted by S ^ E = {1, 2, …, k}, in which *'k'* indicates the overall number of paths. The *k* solution count is present among S and D pairs. This technique detects an optimal path with maximal trust, and another chosen objective utilizes multi-objective FF, which is determined by the following sections.

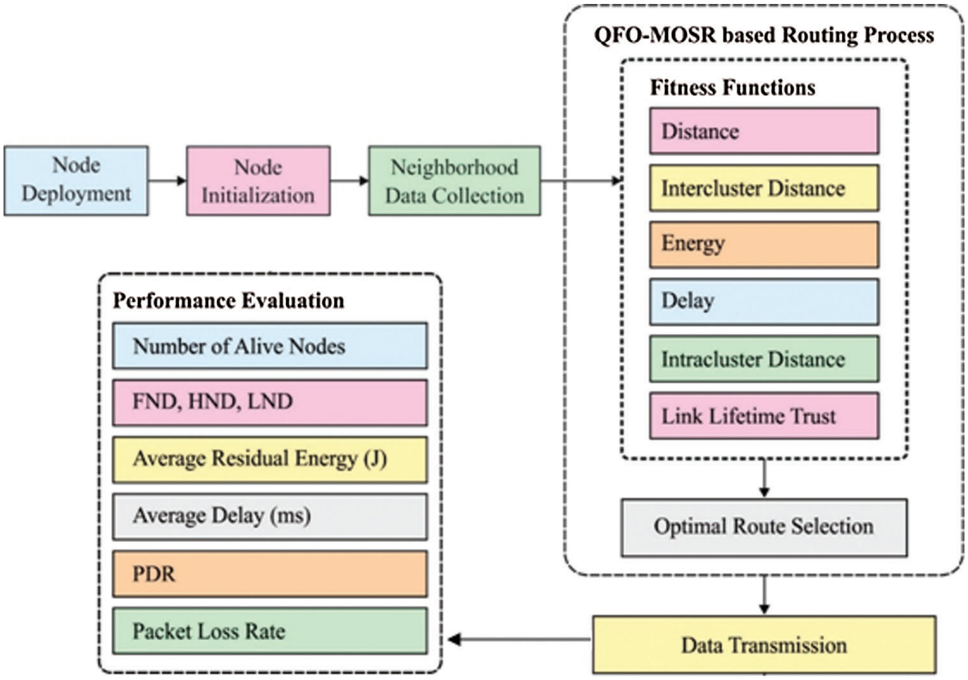

Figure 1: Working process of QFO-MOSR model

3.1 Design of QFO Algorithm

FF is a moderately novel technique that is established in [19]. This method is based on specific behavioural patterns, mainly flashing features of fireflies in the tropical summer sky. Fireflies belong to the insect family known as Lampyridae. Firefly is a type of beetle, which uses the concept of bioluminescence for attracting prey/mates. The luminance made by FF allows other fireflies to trail their path after prey.

Few flashing features of fireflies have been idealized to improve the FF method. Every FF is considered unisex to an individual FF that would attract another FF.

1. The attraction of an individual FF to other is relative to its intensity, by increasing the distance among them; subsequently, the one with lesser intensity would often move towards high brightness. When there is no brighter FF than a provided FF, it will move arbitrarily.
2. The brightness/light intensity of FF is defined using the landscape of objective function to be improved.

The light intensity of one FF is caused by the nature of the encoded cost function, and the intensity is about the value of FF. The main problem in FF growth is the creation of objective function (i.e., attractiveness) and difference in the light intensity. Hence, reduction of light intensity is because of distance among fireflies that results in differences of intensity and thus, reduce the attraction between them. Eq. (1) is utilized for representing light intensity with changing distance:

$$I(r) = I_0 \exp\left(-\gamma \cdot r^2\right), \tag{1}$$

where I represents brightness of S at D r from firefly, I_0 denotes early light intensity if $r = 0$; and C indicates light absorption coefficient that describes the difference of attraction and impacts the cFF algorithm's convergences speed and entire performance [20]. C usually differs from 0.1 to 10. Since FF attraction is related to brightness witnessed by nearby FFs, they could denote attraction β at Cartesian distance r from FF, which is given by Eq. (2):

$$\beta = \beta_0 \exp\left(-\gamma \cdot r^2\right), \tag{2}$$

where β_0 represents attraction at a distance $r = 0$. The light intensity I and attraction β are similar manners. The distance among two FFs i and j at x_i and x_j is given by Eq. (3):

$$r_{ij} = ||x_i - x_j||. \tag{3}$$

The motion of FF i attracted by another brighter FF 'j' is given as:

$$\Delta x_i = \beta_0 e^{-\gamma \cdot r_{ij}^2}\left(x_j^t - x_i^t\right) + \alpha(N_{rand} - 0.5), \tag{4}$$

where t represents iteration. The initial term is performed in Eq. (4) due to attractiveness. Another term $\alpha(N_{rand} - 0.5)$ denotes randomization and increases the search space. α indicates the randomization coefficient and arbitrary amount vector acquired from Gaussian Distribution $\alpha \in [0,\ 1]$. The value N_{rand} denotes in '0' and '1'. The succeeding motion of FF i is upgraded by Eq. (5):

$$x_i^{t+1} = x_i^t + \Delta x_i. \tag{5}$$

The motion of FFs includes; the present location of i^{th} FF, attracted to other fireflies, and arbitrary walk containing randomization variable α and arbitrarily created number from the range '0' and '1'. Where $\beta_0 = 0$, the motion is based on the arbitrary walk. In contrast, variable C contains a critical effect on convergence speed. Besides the initial step, each performance is continually executed till the optimization procedure is terminated.

For improving the effectiveness of the FF algorithm, the QC concept is integrated into it. QC is current research on quantum computers by occurrences of quantum methods like the quantum gate, state superposition, and entanglement [21]. The primary data unit in QC is the Q bit. It might be in state |0>, |1> or superposition of states |0> and |1> concurrently. With Dirac notation, the Q bit denoted by the integration of states |0> and |1> is given as Eq. (6):

$$|Q> \ = \alpha|0 + \beta|1 > such\ that\ |\alpha|^2 + |\beta|^2 \ = 1 \tag{6}$$

where α and β represent complex numbers. $|\alpha|^2$ (resp. $|\beta|^2$) denotes likelihood for finding Q-bit in state zero (denoted in state one). A quantum register of size n is later established from a group of nQ bits. It denotes as the superposition of nQ bits, and mainly it comprises till 2^{n} probable values concurrently. A quantum register is as follows Eq. (7):

$$\Psi = \sum_{x=0}^{2^n-1} C_X|X> \tag{7}$$

The amplitude C_x fulfils the succeeding Eq. (8):

$$\sum_{x=0}^{2^n-1} |C_X|^2 = 1 \tag{8}$$

The Q bit state is altered using a Quantum gate (Q gate) [22]. A Q gate is a reversible gate denoted by unitary operator U act on Q bit basis state fulfilling $U^+U = UU^+$, in which U^+ indicates Hermitian adjoint of U. There are several Q gates, like the controlled-*NOT*, Hadamard, Rotation, *NOT* gate, and so on. Fig. 2

demonstrates the QFO technique's flowchart. They utilize rotation angle in Q bit depiction, whereas every quantum FF solution Qf_i (i^{th} quantum FF in a quantum population) relates to vector $\Theta_i = (\theta_{i1}, \ldots, \theta_{im})$ of parameters θ_{ij} with $\theta_{ij} \in \left[0, \frac{\pi}{2}\right]$ for $(1 \leq j \leq m)$.

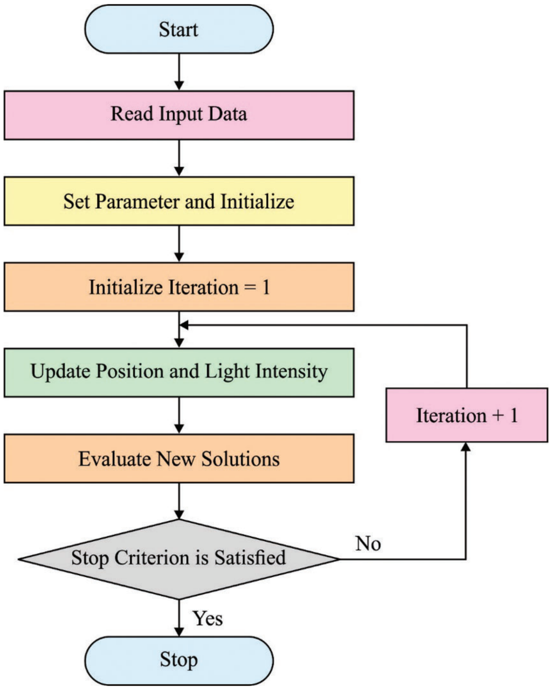
Start
Read Input Data
Set Parameter and Initialize
Initialize Iteration = 1
Update Position and Light Intensity
Evaluate New Solutions
Stop Criterion is Satisfied
No
Iteration + 1
Yes
Stop

Figure 2: Flowchart of QFO

Every quantum FF solution Qf_i represents a string of quantum bits, evaluated by: Eq. (9)

$$Qf_i = \begin{bmatrix} \cos(\theta_{i1})|\cos(\theta_{i2})| & \cdots & |\cos(\theta_{im}) \\ \sin(\theta_{i1})|\sin(\theta_{i2})| & \cdots & |\sin(\theta_{im}) \end{bmatrix} \tag{9}$$

The likelihood amplitude of a single quantum bit is determined by a pair of amounts $(cos(\theta_{ij}), \ sin(\theta_{ij}))$ in which $|cos(\theta_{ij})|^2$ denotes the likelihood of eliminating item x_j and $|sin(\theta_{ij})|^2$ that embodies the likelihood of choosing the item x_j (i^{th} binary firefly). $cos(\theta_{ij})$ and $sin(\theta_{ij})$ fulfil Eq. (10):

$$|cos(\theta_{ij})|^2 + |sin(\theta_{ij})|^2 = 1. \tag{10}$$

```
Firefly Algorithm
Need: $\beta_0$, $\gamma$
Generate an early population of $n$ fireflies with d dimension search:
$x_{ik}$, $i = 1, \ldots, n$ and $k = 1, \ldots, d$;
Calculate the population fitness ($f(x_i)$, which is equivalent to the brightness $I_i$);
while (not end criteria) Do
```

```
For (i = 1: n: every firefly) Do
    For (j = 1: n: each firefly) Do
        If ($I_i < I_j$) Then
            Move FF ‘i’ towards ‘j’ in d dimensional;
        End If
        Attraction differs with distance ‘r’ by $\exp[-r^2]$;
        Calculate novel solutions and upgrade brightness;
    End For
End For
End While
Ranking the FFs and detect an optimum solution
End If
End
```

3.2 Application of QFO Algorithm for Secured Routing Process

The FF is calculated to find an optimum solution from the collection of variables. The fitness calculated for the presented QFO-MSR model utilizes 7 variables, such as link lifetime, delay, distance, energy, intra-cluster distances, trust model, and inter-cluster distances are utilized for routing. Now, the fitness is assumed by maximization operation. Henceforth, the solution offering maximal value of fitness is assumed to multi-hop routing. It is Eq. (11) as,

$$O = W_1 \times P + W_2 \times (1 - T) + W_3 \times (1 - X^*) + W_4 \times X + W_5 \times (1 - D) + W_6 \times M + W_7 \times N \tag{11}$$

where W_1, W_2, W_3, W_4, W_5, W_6, and W_7 denotes weight calculated by fuzzy membership operation. P denotes node energy, T indicates transmission delay, X^* represents inter-cluster distance, D indicates distance among two hops, X denotes intra-cluster distance and M indicates link time, and the trust module is represented by N. Eq. (12) calculates the weight,

$$W = \begin{cases} 0; \ if \ r < f \\ \dfrac{r-f}{p-f}; \ if \ f \le r \le p \\ \dfrac{q-r}{q-p}; \ if \ p \le r \le q \\ 0; \ if \ r \ge q \end{cases} \tag{12}$$

where p, q, and r denotes vertices of triangular membership function $T(f)$. Now, p indicates low boundary, q represents medium boundary with membership value one, and r denotes upper boundary with membership value ‘0’ [23].

i) Energy: The network energy is determined by the energy summation of each hop that denotes energy continued in nodes. The energy contains higher value, and it is Eq. (13) as:

$$P = \frac{1}{b}\sum_{n=1}^{b} E(J_n) \tag{13}$$

where b denotes hop count, which cooperates in multi-hop routing and $E(J_n)$ denotes energy of n^{th} hop.

ii) Delay: The delay is calculated by hop, which plays in routing and the delay have to be lesser to perform effectual routing. The delay calculated by the ratio of hop essential for routing overall nodes limited in WSN is Eq. (14) as:

$$T = \frac{b}{l} \tag{14}$$

where l denotes overall nodes existing in WSN, and b represents the overall hop count required for routing.

iii) Intra-cluster Distance: It can be estimated using the summation of distance among hops, and the separate node existing in the hop is minimum. When it is minimal, the node is nearer to the hop; thus, the energy and data loss decrease. It is Eq. (15) as:

$$X = \frac{1}{b}\left(\frac{\sum_{n=1}^{b}\sum_{t\in k}^{s} X(J_n, L_t)}{\beta}\right) \tag{15}$$

where, β denotes regularization factor, $X(J_n, L_t)$ denotes distance among n^{th} hop and t^{th} node and the overall nodes are denoted by s.

iv) Inter-cluster Distance: The ratio of distance calculated among 2 clusters is the so-called inter-cluster distance, and it has to be maximum to provide an efficient routing. It is Eq. (16) as follows,

$$X^* = \left(\frac{\sum_{x=1}^{no}\sum_{t=x+1}^{no} X(G_x, G_t)}{\beta}\right) \tag{16}$$

where $X(G_x, G_t)$ denotes distance among two clusters, and no denotes overall CHs.

v) Distance: The summation of distance calculated amongst two hops is given by Eq. (17). The distance has to be maximum to multi-hop routing as follows,

$$D = \frac{1}{b} \times \left(\frac{\sum_{n=1}^{b-1} X(J_n, J_{n+1})}{\beta}\right) \tag{17}$$

vi) Link Lifetime: The network lifetime is acquired from the link lifetime and must be maximum for attaining an efficient routing. It is given in Eq. (18).

$$M = \frac{1}{b} \times \sum_{\mathrm{n}=1}^{b-1} \frac{M(J_n, J_{n+1})}{\beta} \tag{18}$$

where, $M(J_n, J_{n+1})$ denotes link lifetime of n^{th} and $(n+1)^{th}$ hops.

vii) Trust model: It gives security to the proposed method in the routing procedure. It is utilized for calculating the trust of agents with suspicious behaviour. Numerous variables are assumed for calculating the trust that includes integrity and forwarding rate factors, direct and indirect trusts. Now, every hop in WSN gives a high trust degree to evaluate the trust level among hops and adjacent hops. It is Eq. (19) as:

$$N = \left\{N^d + N^i + N^F + N^I\right\} \tag{19}$$

where, N^d denotes direct trust, N^i indicates indirect trust, N^F denotes forwarding rate factor, and N^I represents integrity factor.

viii) Direct Trust: It is called local trust, and it presents the trust value of agent computed from familiarity while communicating with targeted agents Eq. (20).

$$\left(N^d\right)_y^z(n, n+1) = fun_y^z(n, n+1) \tag{20}$$

where, $\left(N^d\right)_y^z$ denotes direct trust for y^{th} transaction and z^{th} the time interval, fun denotes satisfaction measure, y represents transaction, z indicates time interval, n denotes calculation hop, and $n+1$ indicates hop to be calculated. The fulfilment measures are utilized for computing fulfilment degrees of an agent, which contain stated service. Therefore, the fulfilment measures keep the record of fulfilment level using exponential average upgrade functions as follows Eq. (21),

$$fun_y^z(n, n+1) = \eta \times fun_v + (1-\eta) \times fun_{y-1}^z(n, n+1) \tag{21}$$

where, fun_{v} denotes fulfilment value of the current transaction, and $fun_{y-1}^z(n, n+1)$ denotes fulfilment value of $y-1$ transaction at z^{th} time interval, η represents weight Eq. (22).

$$fun_{\mathrm{v}} = \begin{cases} 0; & \textit{if} \text{ transaction is thoroughly unsatisfactory} \\ 1; & \text{if the transaction is fully satisfactory} \\ \in (0,1); & \text{otherwise} \end{cases} \tag{22}$$

The weight g differs according to accumulated deviations $Z_y^z(n, n+1)$ as follows

$$\eta = Y + j \times \frac{\gamma_y^z(n, n+1)}{1 + Z_y^z(n, n+1)} \tag{23}$$

$$\gamma_y^z(n, n+1) = \left| fun_{y-1}^z(n, n+1) - fun_v \right| \tag{24}$$

$$Z_y^z(n, n+1) = j \times \gamma_y^z(n, n+1) + (1-j) \times Z_{y-1}^z(n, n+1) \tag{25}$$

where Y denotes threshold and pose set value fixed to 0.25, j represents user-defined constant factor, $\gamma_y^z(n, n+1)$ indicates a current error, and $Z_y^z(n, n+1)$ denotes accumulated deviations. Initially, the weight g is fixed to one, and it alters based on Eqs. (23)–(25)

ix) Indirect Trust: It is evaluated from knowledge attained using other hops. All hops use the knowledge of other hops for providing effective decisions to all transactions. For attaining this approach, each hop requests other hops for offering suggestions regarding other hops. The resulting hop gathers the recommendations from another hop together with feedback credibility of the suggested hop. Therefore, the indirect trust of n^{th} hop regarding $(n+1)^{th}$ hop is as follows Eq. (26),

$$\left(K^i\right)_y^z(n, n+1) = \begin{cases} \dfrac{\sum_{a \in V - \{n\}} H_y^z(n, a) \times \left(N^d\right)_y^z(a, n+1)}{\sum_{a \in V - \{n\}} H_y^z(n, a)}; & \textit{if } |V - \{n\}| = 0 \\ 0; & \textit{If } |v - \{n\}| > 0 \end{cases} \tag{26}$$

where, V denotes the collection of agents communicated with $n+1$, a denotes hop that communicates with other hops to make forecast regarding marinating trust, feedback creditability is represented by H_y^z The feedback credibility is used to compute the accurateness of feedback data which suggests hop given to the evaluator. Therefore, it is Eq. (27) by,

$$H_y^z(n, n+1) = \begin{cases} 1 - \dfrac{\ln\left(S_y^z(n, n+1)\right)}{ln\varphi} & \textit{if } S_y^z(n, n+1) > \varphi \\ 0; & \textit{otherwise} \end{cases} \tag{27}$$

where, S_y^z denotes similarity. The similarity measures are defined by determining that the two hops are equivalent. The comparison is calculated via detecting the customized variance depending upon fulfilment rating regarding the communicated agent and later uses the variance rating to describe comparison. Consequently, the comparison of two hops n and $(n+1)$ is as follows Eq. (28),

$$S_y^z(n,n+1) = \begin{cases} S_{y-1}^z(n,n+1) + \dfrac{1 - S_{y-1}^z(n,n+1)}{\omega}; & if\ R_y^z(n,n+1) < l \\ S_{y-1}^z(n,n+1) + \dfrac{S_{y-1}^z(n,n+1)}{\delta}; & otherwise \end{cases} \tag{28}$$

where l denotes comparison deviation constant, E denotes collection of agents, x and d denote reward and punishment factors, and $R_y^z(n,n+1)$ denotes customized variance as follows Eq. (29),

$$R_y^z(n,n+1) = \sqrt{\frac{\sum_{a\in E(n,n+1)}\left(fun_y^z(n,a) - fun_y^z(n+1,a)\right)}{|E(n,n+1)|}^{2}} \tag{29}$$

x) Forwarding Rate Factor: The nodes in WSN have lesser energy distribution while transferring and sensing the information. Therefore, the collection of information finds out the possibility for examining and judging whether the node is assailed or not. Therefore, it is equated as follows Eq. (30),

$$\left(N^F\right)^z(n,n+1) = \frac{A^z(n,n+1)}{B^z(n,n+1)} \tag{30}$$

where, $A^z(n,n+1)$ denotes the number of feedback packets, $B^z(n,n+1)$ denotes the number of packets to forward, n indicates calculation hop, and $n+1$ represents hop to be estimated.

xi) Integrity Factor: If the data packet is relocated to an adjacent node, the S node studies whether the data packet interferes or not and finds whether the data packet is relocated in a particular time and guarantees reliability and accuracy of the data packet information. It is given by Eq. (31),

$$K^I(n,n+1) = \frac{U^z(n,n+1)}{E^z(n,n+1)} \tag{31}$$

where, $U^z(n,n+1)$ denotes the amount of wholly forwarded packets and $E^z(n,n+1)$ denotes the number of packets to forward.

4 Performance Validation

This section examines the routing performance of the QFO-MOSR technique concerning different measures. The proposed model is simulated using a PC i5-8600k processor, GeForce 1050Ti, 4 GB RAM, 16 GB OS Storage, and 250 GB SSD File Storage. The simulation tool is used in NS3. Besides, the results are simulated in different measures under a varying number of rounds and nodes. A detailed comparative study of the QFO-MOSR technique with existing techniques also takes place. Tab. 1 and Fig. 3 investigate the QFO-MOSR technique's lifetime analysis in terms of the Number of Alive Nodes (NAN). From the results, it can be clear that the QFO-MOSR technique has achieved improved outcomes with the higher NAN, whereas the FEAR technique has obtained the minor outcome with the lower NAN. For instance, under 500 rounds, the QFO-MOSR technique has attained an increased NAN of 492 rounds, whereas the FEAR, P-SEP, A Quantum Ant Colony Multi-Objective Routing (QACMOR), and Artificial Fish-Swarm (AFA) models have accomplished decreased NAN of 229, 488, 392, and 342 rounds, respectively. Then, under 1000 rounds, the QFO-MOSR approach has obtained an increased NAN of 395 rounds, whereas the FEAR, P-SEP, QACMOR, and AFA models have accomplished decreased NAN of 0, 225, 100, and 90 rounds correspondingly.

Likewise, under 1500 rounds, the QFO-MOSR technique has attained an increased NAN of 224 rounds, whereas the FEAR, P-SEP, QACMOR, and AFA techniques have accomplished decreased NAN of 0, 82, 12, and 0 rounds, respectively. Finally, under 1900 rounds, the QFO-MOSR technique has attained an increased NAN of 96 rounds, whereas the FEAR, P-SEP, QACMOR, and AFA models have accomplished decreased NAN of 0, 0, 0, and 0 rounds correspondingly. Comprehensive lifetime analysis of the QFO-MOSR technique takes place in Tab. 2 and Fig. 4. From the resultant values, it is apparent that the QFO-MOSR technique has depicted improved network lifetime. For instance, the QFO-MOSR technique has offered an FND of 397 rounds, whereas the FEAR, P-SEP, QACMOR, and AFA models have depicted a reduced FND of 75, 198, 88, and 111 rounds respectively.

Table 1: Analysis of QFO-MOSR for NAN

Rounds	FEAR	P-SEP	QACMOR	AFA	QFO-MOSR
0	500	500	500	500	500
100	475	500	492	500	500
200	442	495	490	485	500
300	349	492	485	475	500
400	294	490	450	460	494
500	229	488	392	342	492
600	199	485	325	260	490
700	178	425	275	225	483
800	80	350	210	155	476
900	52	340	175	112	427
1000	0	225	100	90	395
1100	0	190	82	55	364
1200	0	160	65	25	328
1300	0	138	50	12	297
1400	0	110	35	0	275
1500	0	82	12	0	224
1600	0	55	0	0	198
1700	0	0	0	0	156
1800	0	0	0	0	127
1900	0	0	0	0	96
2000	0	0	0	0	0

Moreover, the QFO-MOSR model has offered an HND of 1442 rounds, whereas the FEAR, P-SEP, QACMOR, and AFA techniques have depicted a reduced HND of 445, 984, 625, and 711 rounds correspondingly. Furthermore, the QFO-MOSR technique has offered an LND of 1994 rounds, whereas the FEAR, P-SEP, QACMOR, and AFA methods have showcased a reduced LND of 995, 1612, 1544, and 1329 rounds correspondingly. A brief Average Residual Energy (ARE) analysis of the QFO-MOSR technique with existing methods is provided in Tab. 3 and Fig. 5. For instance, under 500 rounds, the

QFO-MOSR approach has obtained a superior ARE of 0.494 J, whereas the FEAR, P-SEP, QACMOR, and AFA models have exhibited lower ARE 0.277, 0.4875, 0.3925, and 0.3425 J correspondingly. In addition, under 1000 rounds, the QFO-MOSR methodology has attained a maximum ARE of 0.406 *J*, whereas the FEAR, P-SEP, QACMOR, and AFA models have exhibited lower ARE of 0, 0.225, 0.1, and 0.09 J correspondingly. Also, under 1500 rounds, the QFO-MOSR technique has obtained a superior ARE of 0.218 *J*, whereas the FEAR, P-SEP, QACMOR, and AFA models have exhibited lower ARE of 0, 0.0825, 0.0125 and 0 *J* correspondingly. Additionally, under 1900 rounds, the QFO-MOSR algorithm has obtained a superior ARE of 0.054 *J*, whereas the FEAR, P-SEP, QACMOR, and AFA models have demonstrated minimum ARE of 0, 0, 0 and 0 *J* correspondingly.

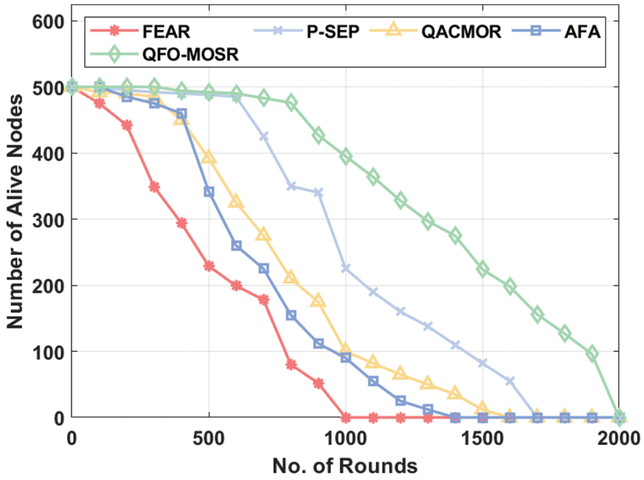

Figure 3: NAV analysis of QFO-MOSR

Table 2: Analysis of QFO-MOSR for FND, HND, LND

	Rounds				
Methods	FEAR	P-SEP	QACMOR	AFA	QFO-MOSR
FND	75	198	88	111	397
HND	455	984	625	711	1442
LND	995	1612	1544	1329	1994

Brief average delay analysis of the QFO-MOSR method with existing techniques is provided in Tab. 4 and Fig. 6. For instance, under 50 nodes, the QFO-MOSR approach has attained a lesser average delay of 92 *ms*, whereas the FEAR, P-SEP, QACMOR, and AFA models have exhibited higher average delay 282, 121, 113 and 99 *ms* correspondingly. Besides, under 150 nodes, the QFO-MOSR approach has achieved a lesser average delay of 94 *ms*, whereas the FEAR, P-SEP, QACMOR, and AFA models have portrayed higher average delay of 302, 140, 131 and 129 *ms*, respectively. Moreover, under 300 nodes, the QFO-MOSR algorithm has attained a minimum average delay of 120 *ms*, whereas the FEAR, P-SEP, QACMOR, and AFA models have exhibited higher average delay of 372, 171, 161 and 152 *ms*, respectively. Furthermore, under 500 nodes, the QFO-MOSR model has achieved a minimum average delay of 141 *ms*, whereas the FEAR, P-SEP, QACMOR, and AFA models have exhibited maximal average delay 643, 229, 201 and 188 *ms* correspondingly.

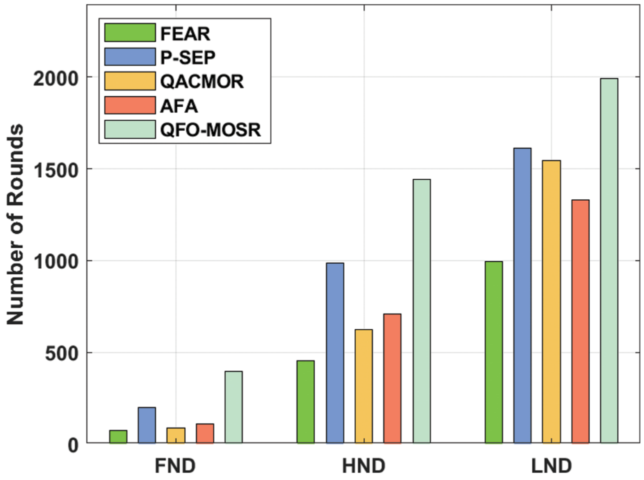

Figure 4: Analysis of QFO-MOSR

Table 3: Analysis of QFO-MOSR for average residual energy

Rounds	FEAR	P-SEP	QACMOR	AFA	QFO-MOSR
0	0.5	0.5	0.5	0.5	0.5
100	0.475	0.5	0.4925	0.49	0.5
200	0.406	0.495	0.49	0.485	0.5
300	0.3605	0.4925	0.485	0.475	0.5
400	0.339	0.49	0.45	0.46	0.5
500	0.277	0.4875	0.3925	0.3425	0.494
600	0.2165	0.485	0.325	0.26	0.487
700	0.1925	0.425	0.275	0.225	0.465
800	0.1105	0.35	0.21	0.155	0.432
900	0.0455	0.34	0.175	0.1125	0.410
1000	0	0.225	0.1	0.09	0.406
1100	0	0.19	0.0825	0.055	0.396
1200	0	0.16	0.065	0.025	0.342
1300	0	0.1375	0.05	0.0125	0.304
1400	0	0.11	0.035	0	0.286
1500	0	0.0825	0.0125	0	0.218
1600	0	0.055	0	0	0.176
1700	0	0	0	0	0.135
1800	0	0	0	0	0.096
1900	0	0	0	0	0.054
2000	0	0	0	0	0

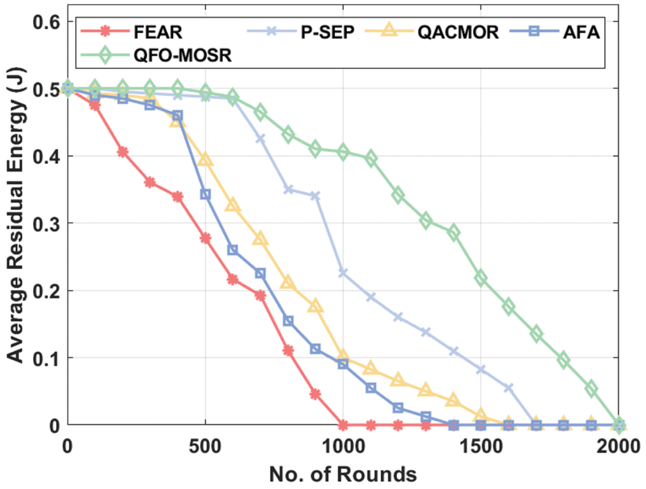

Figure 5: Average residual energy analysis of QFO-MOSR

Table 4: Result analysis of QFO-MOSR for average delay

Nodes	FEAR	P-SEP	QACMOR	AFA	QFO-MOSR
50	282	121	113	99	92
100	288	128	123	114	87
150	302	140	131	129	94
200	329	146	141	136	102
250	351	161	146	144	117
300	372	171	161	152	120
350	391	176	166	164	125
400	444	191	183	174	132
450	565	211	191	183	137
500	643	229	201	188	141

A brief PDR analysis of the QFO-MOSR approach with existing techniques is provided in Tab. 5 and Fig. 7. For instance, under 50 nodes, the QFO-MOSR algorithm has achieved a superior PDR of 0.865%, whereas the FEAR, P-SEP, QACMOR, and AFA models have exhibited reduced PDR of 0.777%, 0.677%, 0.731%, and 0.747% correspondingly. In the meantime, under 200 nodes, the QFO-MOSR technique has reached a higher PDR of 0.841%, whereas the FEAR, P-SEP, QACMOR, and AFA models have exhibited minimal PDR of 0.727%, 0.607%, 0.677%, and 0.677% correspondingly. At the same time, under 350 nodes, the QFO-MOSR methodology has reached a higher PDR of 0.809%, whereas the FEAR, P-SEP, QACMOR, and AFA models have demonstrated lesser PDR of 0.697%, 0.537%, 0.607%, and 0.627% correspondingly. Meanwhile, under 500 nodes, the QFO-MOSR technique has reached a maximum PDR of 0.747%, whereas the FEAR, P-SEP, QACMOR, and AFA models have showcased minimal PDR 0.657%, 0.512%, 0.527%, and 0.567% correspondingly. A brief packet loss analysis of the QFO-MOSR approach with existing techniques is provided in Tab. 5 and Fig. 8. The figure has shown that the QFO-MOSR technique has showcased better results with minimal packet loss under the specific number of nodes. For instance, under 50 nodes, the QFO-MOSR approach has obtained a minimum packet loss of 0.0198, whereas the FEAR, P-SEP, QACMOR, and AFA methods have showcased higher packet loss of 0.2, 0.11, 0.07, and 0.04 correspondingly.

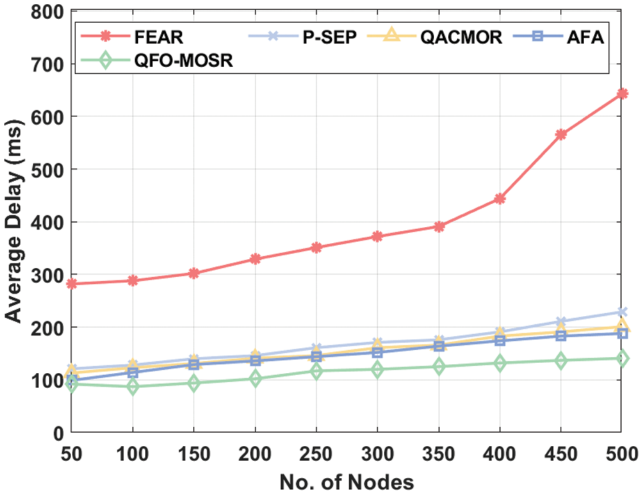

Figure 6: Average delay analysis of QFO-MOSR

Table 5: Result analysis of QFO-MOSR for packet delivery ratio and packet loss

Nodes	Packet delivery ratio					Packet loss				
	FEAR	P-SEP	QACMOR	AFA	QFO-MOSR	FEAR	P-SEP	QACMOR	AFA	QFO-MOSR
50	0.777	0.677	0.731	0.747	0.865	0.2	0.11	0.07	0.04	0.019
100	0.747	0.657	0.717	0.737	0.852	0.21	0.13	0.07	0.05	0.023
150	0.737	0.627	0.707	0.727	0.869	0.215	0.16	0.08	0.06	0.030
200	0.727	0.607	0.677	0.677	0.841	0.228	0.18	0.11	0.11	0.042
250	0.717	0.587	0.657	0.667	0.826	0.262	0.20	0.13	0.12	0.051
300	0.707	0.557	0.617	0.647	0.838	0.279	0.23	0.17	0.14	0.062
350	0.697	0.537	0.607	0.627	0.809	0.316	0.25	0.18	0.16	0.074
400	0.687	0.527	0.577	0.607	0.795	0.365	0.26	0.21	0.18	0.093
450	0.677	0.517	0.557	0.587	0.764	0.399	0.27	0.23	0.20	0.106
500	0.657	0.512	0.527	0.567	0.747	0.489	0.28	0.26	0.22	0.126

Simultaneously, under 150 nodes, the QFO-MOSR technique has reached a lower packet loss of 0.0308, whereas the FEAR, P-SEP, QACMOR, and AFA models have exhibited higher packet loss 0.215, 0.16, 0.08, and 0.06, respectively. Along with that, under 300 nodes, the QFO-MOSR technique has reached a lower packet loss of 0.0628, whereas the FEAR, P-SEP, QACMOR, and AFA models have exhibited higher packet loss of 0.279, 0.23, 0.17, and 0.14, respectively. Eventually, under 500 nodes, the QFO-MOSR methodology has reached a lower packet loss of 0.1267, whereas the FEAR, P-SEP, QACMOR, and AFA techniques have exhibited higher packet loss 0.489, 0.28, 0.26, and 0.22 correspondingly.

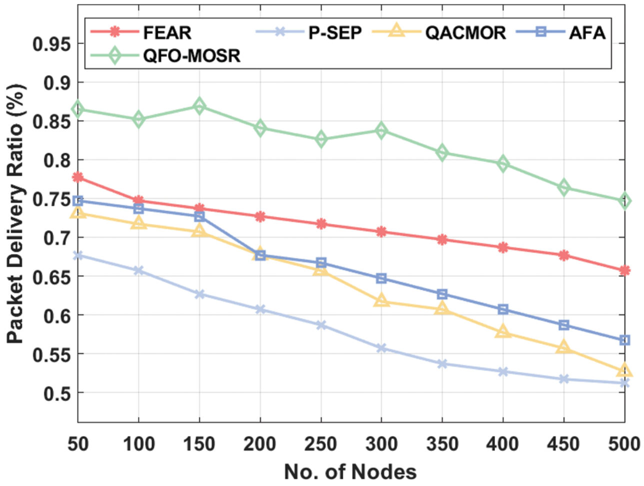

Figure 7: PDR analysis of QFO-MOSR

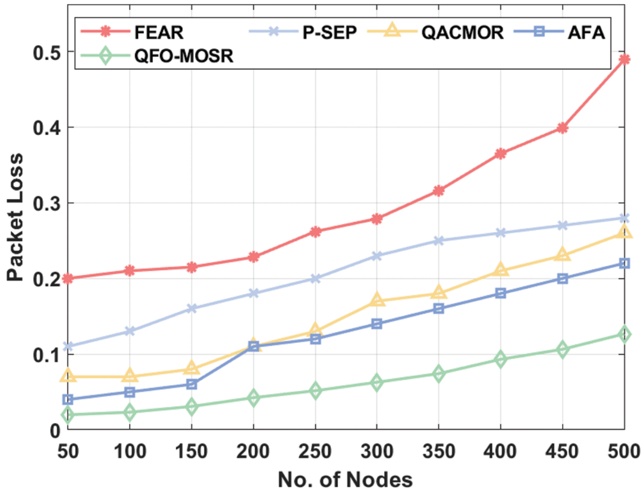

Figure 8: Packet loss analysis of QFO-MOSR

5 Conclusion

This paper has developed an effective QFO-MOSR protocol for Fog-based WSN. The proposed QFO-MOSR protocol derives an optimal set of routes to the destination using a fitness function involving seven parameters. The QFO-MOSR technique is derived from the concepts of quantum computing and the FF optimization algorithm. The proposed routing technique derives a fitness function including trust factor from ensuring security. To investigate the effectual outcome of the QFO-MOSR technique, simulations occur, and results are examined under diverse dimensions. The experimental analysis ensured that the QFO-MOSR technique is superior to other methods in terms of different measures. Therefore, it can be employed as an effective tool in several real-world applications. As a part of future work, the secrecy of the Fog-bases WSN can be guaranteed using the design of deep learning-based intrusion detection methodologies.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] A. Ali, Y. Ming, S. Chakraborty and S. Iram, "A comprehensive survey on real-time applications of WSN," *Future Internet*, vol. 9, no. 4, pp. 1–22, 2017.

[2] M. Buvanesvari, J. Uthayakumar and J. Amudhavel, "Fuzzy based clustering to maximize network lifetime in wireless mobile sensor networks," *Journal of Advanced Research in Dynamical and Control Systems*, vol. 12, pp. 2156–2167, 2017.

[3] A. Yassine, S. Singh, M. S. Hossain and G. Muhammad, "IoT big data analytics for smart homes with fog and cloud computing," *Future Generation Computer Systems*, vol. 91, no. 4, pp. 563–573, 2019.

[4] S. P. Singh, A. Nayyar, R. Kumar and A. Sharma, "Fog computing: From architecture to edge computing and big data processing," *The Journal of Super Computing*, vol. 75, no. 4, pp. 2070–2105, 2019.

[5] S. Arjunanand and P. Sujatha, "Lifetime maximization of wireless sensor network using fuzzy-based unequal clustering and ACO based routing hybrid protocol," *Applied Intelligence*, vol. 48, no. 8, pp. 2229–2246, 2018.

[6] X. Zheng, W. Zheng, Y. Yang, W. Guo and V. Chang, "Clustering-based interest prediction in social networks," *Multimedia Tools and Applications*, vol. 78, no. 23, pp. 32755–32774, 2019.

[7] G. Kadiravan, A. Sarigaand and P. Sujatha, "A novel energy-efficient clustering technique for mobile wireless sensor networks," in *Proc. of IEEE Int. Conf. on System, Computation, Automation and Networking*, Pondicherry, India, pp. 1–6, 2019.

[8] J. Uthayakumar, T. Vengattaramanand and P. Dhavachelvan, "A new lossless neighborhood indexing sequence (NIS) algorithm for data compression in wireless sensor networks," *Ad Hoc Networks*, vol. 83, no. 2009, pp. 149–157, 2019.

[9] W. Fang, W. Zhang, W. Chen, Y. Liu and C. Tang, "TMSRS: Trust management-based secure routing scheme in industrial wireless sensor network with fog computing," *Wireless Networks*, vol. 26, no. 5, pp. 3169–3182, 2020.

[10] O. Arapoglu, V. K. Akram and O. Dagdeviren, "An energy-efficient, self-stabilizing and distributed algorithm for maximal independent set construction in wireless sensor networks," *Computer Standards and Interfaces*, vol. 62, no. 2, pp. 32–42, 2019.

[11] W. Fang, W. Zhang, W. Chen, J. Liu, Y. Ni *et al.,* "MSCR: Multidimensional secure clustered routing scheme in hierarchical wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2021, no. 1, pp. 1–20, 2021.

[12] M. Revanesh, V. Sridhar and J. M. Acken, "Secure coronas-based zone clustering and routing model for distributed wireless sensor networks," *Wireless Personal Communications*, vol. 112, no. 3, pp. 1829–1857, 2020.

[13] A. P. Abidoye and B. Kabaso, "Energy-efficient hierarchical routing in wireless sensor networks based on fog computing," *EURASIP Journal on Wireless Communications and Networking*, vol. 2021, no. 8, pp. 1–26, 2021.

[14] M. C. Cara, E. H. Junco, M. Q. Montesinos, L. O. Barbosa and E. A. Antunez, "FROG: A robust and green wireless sensor node for fog computing platforms," *Journal of Sensors*, vol. 2018, pp. 1–13, 2018.

[15] T. Wang, G. Zhang, M. Z. A. Bhuiyan, A. Liu, W. Jia *et al.,* "A novel trust mechanism based on fog computing in sensor-cloud system," *Future Generation Computer Systems*, vol. 109, no. 6, pp. 573–582, 2020.

[16] A. Rafi, A. U. Rehman, G. Ali and J. Akram, "Efficient energy utilization in fog computing-based wireless sensor networks," in *Proc. 2nd Int. Conf. on Computing, Mathematics and Engineering Technologies*, Sukkur, Pakistan, pp. 1–5, 2019.

[17] E. M. Borujeni, D. Rahbari and M. Nickray, "Fog-based energy-efficient routing protocol for wireless sensor networks," *The Journal of Supercomputing*, vol. 74, no. 12, pp. 6831–6858, 2018.

[18] R. M. Chintalapalli and V. R. Ananthula, "M-LionWhale: Multi-objective optimization model for secure routing in mobile ad-hoc network," *IET Communications*, vol. 12, no. 12, pp. 1406–1415, 2018.

[19] M. B. Imamoglu, M. Ulutas and G. Ulutas, “A new reversible database watermarking approach with firefly optimization algorithm,” *Mathematical Problems in Engineering*, vol. 2017, no. 2, pp. 1–14, 2017.

[20] S. B. Tao, D. Z. Liu and A. P. Tang, “Bridge critical state search by using quantum genetic firefly algorithm,” *Shock and Vibration*, vol. 2019, pp. 1–11, 2019.

[21] S. Akama, *Elements of Quantum Computing: History, Theories and Engineering Applications*. New York: Springer, 2015.

[22] D. Zouache, F. Nouioua and A. Moussaoui, “Quantum-inspired firefly algorithm with particle swarm optimization for discrete optimization problems,” *Soft Computing*, vol. 20, no. 7, pp. 2781–2799, 2016.

[23] A. Vinitha, M. S. S. Rukmini and D. Sunehra, “Secure and energy-aware multi-hop routing protocol in WSN using taylor-based hybrid optimization algorithm,” *Journal of King Saud University-Computer and Information Sciences*, vol. 1, pp. 1–12, 2019.