Wireless Personal Communications
https://doi.org/10.1007/s11277-024-11604-3

# An Effective Congestion and Interference Secure Routing Protocol for Internet of Things Applications in Wireless Sensor Network

Ramdas Vankdothu[1] · Mohd Abdul Hameed[2]

Accepted: 21 September 2024

## Abstract

This paper provides an effective Wireless Sensor Network (WSN) routing solution for Internet of Things (IoT) applications cognizant of congestion, security, and interference. Because several sources try to deliver their packets to a destination simultaneously, which is a common case in IoT applications. The proposed congestion and interference aware safe routing protocol is claimed to work in networks with high traffic. The signal to interference ratio (SINR), congestion level, and survival factor is used in our suggested procedure to estimate the cluster head selection factor first. The adaptive fuzzy c-means clustering method clusters the network nodes based on the cluster head selection factor. After that, data packets are encrypted using Adaptive Quantum Logic-based packet coding. Finally, the Adaptive Krill Herd (AKH) optimization method identifies the least congested corridor, resulting in optimal data transmission routing. The exploratory findings show that the provided strategy outperforms previous methodologies in network performance, end-to-end delay, packet delivery ratio, and node remaining energy level.

**Keywords** Cluster head choosing factor · Clustering · Data security · Optimization · Routing

## 1 Introduction

The Internet of Things (IoT) results from a wide range of empowering innovations, such as embedded systems, wireless sensor networks, cloud computing, big data, which are utilizing to accumulate, process, surmise, and transmit information [1, 2]. There are three layers in IoT design: perception layer, network layer, and application layer, including RFID, WSN, sensors, readers, IP Cam, MEMS, etc. [3]. As the quantity of sensors in an IoT framework develops, in any case, the issue of how to move information amongst those

✉ Ramdas Vankdothu
vankdr@unisa.ac.za

[1] Department of Mathematical Sciences, University of South Africa, UNISA 0003, Johannesburg, South Africa

[2] Department of Computer Science and Engineering, Osmania University, Hyderabad, India

Published online: 17 December 2024

devices turns out to be progressively complex, and data transfer needs should be offset with working contemplations and foundation costs [4]. Consequently, the Wireless Sensor Networks (WSNs) have a significant job in improving IoT, and various advances have just been institutionalized to help their joining. The incorporation of WSN with the Internet may assume a significant job in advancing the engineering of the Internet since WSN distributions might be utilized to help the sensorial capacities required by future applications [5].

Therefore the WSNs are part of the IoT and have been read for a long time. In any case, joining the sensors and actuators that structure a WSN in the IoT requires innovations and conventions [6, 7]. WSN gives an inventive and powerful answer for issues in numerous circles of life. With WSN's assuming such a vital job in improving everyday life, improvement of minimal effort, low-power remote sensor systems involves great research intrigue [8]. The Future Internet plans to coordinate heterogeneous correspondence innovations, both wired and remote, to contribute considerably to attest to the idea of IoT [9]. Despite what might be expected, WSNs are self-sorting out systems of little, ease devices that communicate in a multi-hop way to give screen and control functionalities. WSN bits ordinarily coordinate an IEEE 802.15.4 [10].

IoT systems rely on remote connections to ensure last-mile connectivity in sensor systems and then on WSNs. IoT gateways (IGWs) are used to connect several types of sensors (IoT gadgets) that communicate with the IoT cloud via various innovations, for example, 802.11a/b, Bluetooth, Bluetooth low vitality, and Zigbee [11–13]. A fundamental driving force of IoT that facilitates the interconnection of devices is organizing and explicitly directing in the system. It includes producing traffic courses and transmitting the steered parcels from source to definite goal in a system [14]. In any event, the current trend toward IP-based sensor organization (for instance, 6LoWPAN and IPv6) enables the WSN to be connected to the web [15–18]. The ongoing progressions of WSNs in IoT have been broadly advanced in natural, modern, and biomedical detecting and observing applications, which essentially rely upon continuous information [19]. To adapt to new difficulties for structuring IoT gadget the executives, some key qualities ought to be considered, for example, restricted assets of remote sensor gadgets, disseminated organized condition and gigantic information gathered from an assortment of utilizations, and so on [20–22].

This article posted in Research Square https://www.researchsquare.com/article/rs-790102/v1. https://doi.org/10.21203/rs.3.rs-790102/v1, This work is licensed under a CC BY 4.0 License.

The manuscript's structure is as follows: Sect. 2 reviews the literature about the proposed strategy. Section 3 contains a brief explanation of the proposed system, Sect. 4 contains an examination of the exploratory findings, and Sect. 5 ends the study.

## 2 Related Works

Al-Turjman et al. [23] developed an agile framework for service-based applications in smart cities with a high volume of multimedia data. We explore and suggest an optimized data delivery technique that works with constrained assets in highly dynamic topologies. Additionally, we provide a sound mathematical model for determining the routing of data packets. The suggested approach enables data routing to be performed on available vehicle assets while ensuring service quality in various multimedia security and safety applications. They performed an analytical study to validate the simulation results in terms of packet received ratio, energy consumption, and average end-to-end delay in determining the usefulness of the proposed model.

Memos et al. [24] presented a future Internet of Things network design and its associated security concerns. They summarised the most recent research on media security and protection in wireless sensor networks (WSNs). As a result, they proposed an Efficient Algorithm for Media-based Surveillance System (EAMSuS) in IoT networks for the Smart City Framework, which combines two calculations for WSN packet routing and security presented by different researchers, while also recovering the new media compression standard, High-Efficiency Video Coding (HEVC).

Esfahani et al. [25] offered a lightweight authentication solution based purely on hash and XOR operations for M2M communications in an Industrial IoT environment. While achieving mutual authentication, session key agreement, device identity confidentiality, and resistance to accompanying attacks such as replay attack, man-in-the-middle attack, impersonation attack, and modification attack, the proposed mechanism has a low computational cost, communication overhead, and storage overhead.

Tomovic et al. [26] proposed a novel type of Internet of Things architecture has been presented that combines the benefits of two emerging technologies: software-defined networking and fog computing. Software-defined networking implies a coherently concentrated system control plane that enables the utilization of sophisticated traffic control and resource management components. In contrast, fog computing enables examining and supervising a small amount of data at the network edge, supporting applications that demand extremely low and predictable latency. Additionally, they evaluate the suggested design's advantages and possible services.

Elappilaa et al. [27] Survivable Path Routing was created as a low-energy routing approach for WSNs. This protocol should work in high-traffic systems where numerous sources attempt to transmit packets to the same destination concurrently, as is the case with IoT applications for remote healthcare monitoring. The next-hop node is chosen based on three factors: the link's signal to interference and noise ratio, the path's survival factor from the next-hop node to the destination, and the congestion level at the next-hop node.

An automated sensor setup has been used by Wu et al. [28] to evaluate subsurface water pipes by including an SN self-localization computation. The goal of this research is to use estimations of the radio's RSS from over-the-ground RNs, along with the position and speed of an SN inside a funnel. Given the distinct engineering framework models—which comprised SN components and estimate models—used by the automated sensor organization.

Protecting the aquifers and soils that give humanity and the natural world essential resources, as well as overseeing the functionality and safety of regionally dispersed infrastructure susceptible to low probability/high consequence underground disasters, are challenging and costly undertakings, as Pamukcu [29] pointed out. This activity requires sustainable sensing systems that enable a sustained response to perceived dangers. This chapter discusses the need for sustainable subsurface sensing systems and gives particular focus to time and space-continuous systems, in addition to giving an overview of current developments in environmental and geotechnical subterranean sensing [30].

Altuwairiqi [31] introduced the industrial revolution may benefit from the major technology known as a wireless sensor network (WSN). In wireless sensor networks (WSNs), battery power is provided to Sensor Nodes (SNs). Since the battery in a WSN cannot be replenished, energy is the most important resource. Over time, a number of strategies have been developed and put into practice to protect WSNs, a limited resource. This paper proposes an optimized multi-hop routing in WSNs based on improved Honey Badger

Algorithm (I-HBA) and suggests a model to handle the energy and security issues. There are two phases in this multi-hop routing method: choosing a Cluster Head (CH) and routing the packets. For effective data transport, energy-efficient CHs are selected using the I-HBA. Next, the selected CH receives the data from the SNs and uses the fewest possible hops to relay it to the base station (BS). The best hops are chosen using the recommended I-HBA. For efficient routing in WSNs, the suggested model makes use of a multi-objective fitness function with eight parameters. Moreover, a trust model incorporating data, integrity, forwarding rate factor, and direct and indirect trust is used to provide security-conscious multihop routing [31, 32]

## 3 Proposed Methodology

In the proposed work, cluster head choosing factor from the start evaluated by signal to interference ratio of nodes, Congestion level, and survivability factor of nodes. Subsequently, network nodes are clustering utilizing adaptive fuzzy c-means clustering dependent on the cluster head choosing factor. After that, data packets are encoding using adaptive quantum logic coding, and finally, an optimized route is obtained by adaptive krill herd optimization. Figure 1 depicts the proposed methodology's flow diagram.

The wireless sensor network comprises a group of nodes $N = \{N_1, N_2, N_3 \ldots N_i\}$ and assumes the source $N_1$ and the destination as $N_i$. The suggested study clusters nodes in

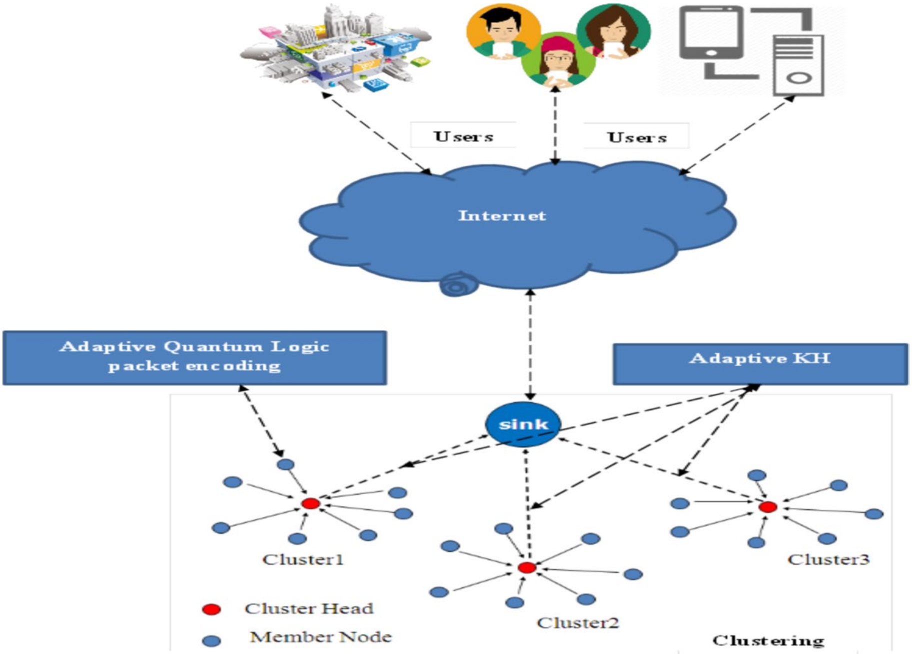


Fig. 1 The proposed methodology is depicted as a block diagram

the network based on three effective parameters. The following sections cover the suggested design process in depth.

A. Node Selection Using Three Factors

The following paper addresses three characteristics for clustering nodes: the link's signal to interference and noise ratio, the path's survivability factor from the next-hop node to the destination, and the level of congestion at the next-hop node.

(1). Survivability Factor

The survival factor is defined as the ratio of the smallest amount of energy remaining between each node along that path to the total energy required for communication along that path. The path survivability factor equals the ratio of the path's total energy consumption to the minimal power accessible value between nodes. This proportion is meant by the condition (1),

$$P_s = {}^{M_p}\!/_{E_p} \tag{1}$$

here $E_p$ is the total energy utilization of path L, $M_p$ is the minimum power available value among the nodes in path L.

(2). Signal to Interference and Noise Ratio (SINR)

SINR is defined as the ratio of the transmitted signal's quality to the sum of interference and ambient noise. On account of a transmission edge $e_i$, the amount of interference and noise at the receiver $\mathrm{Re}_i$ is denoted as,

$$I_f(e_i) = \sum_{m:m\neq i} G(Te_m, \mathrm{Re}_i)p(Te_m) + \eta_i \tag{2}$$

here $G(Te_m, \mathrm{Re}_i)$ is the path gain between the transmitter $Te_m$ on the link $e_m$ and the receiver $\mathrm{Re}_i$ on the edge $e_i$, $p(Te_m)$ is the transmission power of the transmitters $Te_m$ on edge $e_m$, $\eta_i$ is ambient noise around the receiver node $\mathrm{Re}_i$. At that point, the SINR estimation of an edge $e_i$ can be characterized as,

$$\tilde{\theta}(e_i) = \frac{G(Te_i, \mathrm{Re}_i)p(Te_i)}{I_f(e_i)} \tag{3}$$

From the above condition (3), it tends to be seen that when $I_f(e_i)$ increments, for keeping up the equivalent SINR esteem on the connection, the transmission power $p(Te_i)$ needs to rise in like manner. Nonetheless, whenever $p(Te_i)$ expanded, different connections in the topology may encounter more interference. As a result, such connections must also increase their transmission capacity to maintain consistent signal strength and communication quality. It may increase the nodes' energy consumption and result in a shorter system lifetime.

(3). Congestion Level Factor

The multiple nodes connecting the source to the sink are constructed first, and then cross-layer data is shared as a state frame. This frame is transmitted upstream to keep the node's congestion information current and to share it with other nodes. A node's congestion level is denoted by,

$$C_l = {}^{T_r}\!/_{S_r} \tag{4}$$

where $T_r$ is the input traffic rate, and $S_r$ is the service rate. The input traffic rate of a node is defined as the number of packets that flow into the physical layer of the protocol stack in a unit of time. Additionally, service rate refers to the number of packets that are streamed downward to the channel in a unit of time.

B. Cluster Head Choosing Factor

The next-hop node is chosen from its routing table dependent on the Cluster head Choosing Factor (CCF) at each node. CCF is a function that involves three factors; the survivability factor $P_s$ of the path to the destination through that next-hop, the SINR value $\tilde{\theta}(e_i)$ of the link $e$ between the current node and the next-hop node, and the congestion level $C_l$ at the next hop. That is,

$$CCF = \left(\alpha * \tilde{\theta}(e_i)\right) + \left(\beta * P_s\right) + \left(\gamma * \left(1 - C_l\right)\right) \tag{5}$$

here $\alpha$, $\beta$, and $\gamma$ values are utilized for setting various weights on the three components, $\tilde{\theta}(e_i)$, $P_s$, and $C_l$ of the PCF. The requirement can pick their values for forcing the strength for these three components in the cluster head selection. In our simulation, each of the three weighting coefficients is similarly considered as, $\alpha = \beta = \gamma = {}^{1}\!/_{3}$, to demonstrate equivalent impact by all the components in PCF. The values are standardized with the end goal that,

$$\alpha + \beta + \gamma = 1 \tag{6}$$

This CCF factor is given in condition (6) is taken as an input to the adaptive fuzzy c-means clustering. This is adequately performed by using the three factors: SINR, congestion level, and survivability factor in the clustering of sensor nodes network.

C. CCF based Adaptive Fuzzy c-means clustering algorithm

The node with the best value in SINR, congestion level, and survivability will transform into the cluster head among the system nodes. The sensor nodes are clustered by utilizing the adaptive fuzzy c-means (AFCM) clustering algorithm. Here, support kernel matrices are confined by utilizing the deliberate CCF factor in clustering. This algorithm starts with a lot of initial cluster centers. The AFCM algorithm dispenses the info data of each class by using fuzzy memberships.

$$\tilde{J}_{\sigma n} = \sum_{l=1}^{L} \sum_{m=1}^{M} (v_{ij})^n \frac{\hat{S}_l - q_m^2}{CCF_l} \tag{7}$$

In condition (4), $\tilde{S}_l$ signifies the support value, $q_m$ signifies the $m$th cluster center and $n$ signifies the constant esteem. Where $CCF$ demonstrates the Cluster head is choosing a factor in the cluster $l$, and it is referenced in condition (5). The membership function describes the probability that a pixel has a place with a particular cluster. The membership functions and cluster centers are updated by the conditions (8) and (9).

$$\bar{v}_{lm} = \frac{1}{\sum_{k=1}^{q}\left(\frac{\tilde{S}_l - q_m/\bar{\sigma}_l}{\tilde{S}_l - q_k/\bar{\sigma}_l}\right)^{\frac{2}{n-1}}} \tag{8}$$

The clusters centroid is processed by utilizing the condition (9),

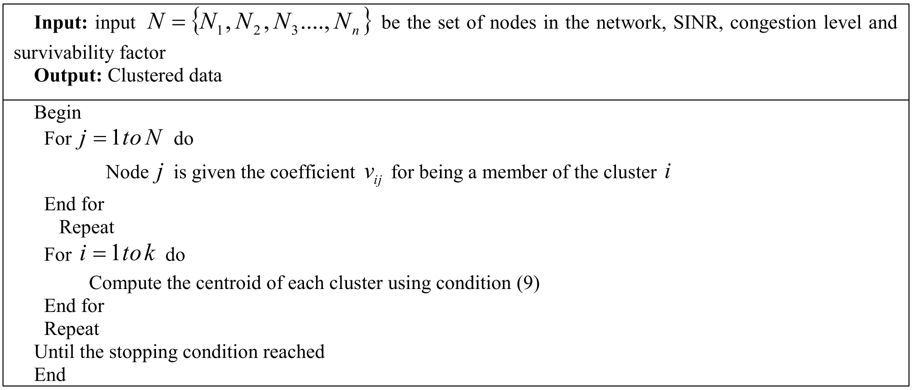
$$z'_m = \frac{\sum_{l=1}^{L} \bar{v}_{lm}^{n} \cdot \tilde{S}_l}{\sum_{l=1}^{L} \bar{v}_{lm}^{n}} \tag{9}$$

Repeat the calculation until the coefficients change among two cycles is close to $\psi$, the given limit.

$$\max_{\mathrm{lm}} \overline{V}_{lm}^{(k)} - \overline{V}_{lm}^{(k+1)} < \psi \tag{10}$$

In condition (8), $\psi$ is a range of 0 and 1. Repeat the steps until effective clustering got. This AFCM clustering is denoted in algorithm 1.

**Algorithm 1** CCF based Adaptive fuzzy c-means clustering



**Input:** input $N = \{N_1, N_2, N_3 ...., N_n\}$ be the set of nodes in the network, SINR, congestion level and survivability factor
**Output:** Clustered data

```
Begin
 For $j = 1 to N$ do
        Node $j$ is given the coefficient $v_{ij}$ for being a member of the cluster $i$
 End for
   Repeat
 For $i = 1 to k$ do
       Compute the centroid of each cluster using condition (9)
 End for
 Repeat
Until the stopping condition reached
End
```

Once the clustering of nodes is finished, the nodes in clusters are assumed to forward the packets and perform an AQLG operation on the received packets before rebroadcasting them.

D. Securing data packets using Adaptive Quantum Logic Coding

The purpose of our suggested study is to achieve a higher level of security and to reduce system congestion in a scenario of multimedia information distribution. To accomplish this, the network coding approach is used to minimize the number of retransmissions. Adaptive quantum coding is not equal to the direct delivery of subsystems; this is also scientifically explained. For instance, Consider two nodes $R_A$, $R_B$ and the relating composited system $R_{AB}$. The quantum information of subsystems just as composited framework are $|\psi_A\rangle$, $|\psi_B\rangle$ and $|\psi_A\rangle \otimes |\psi_B\rangle$ respectively. If two subsystems ensnared one another, the relationship can be depicted as seeks after,

$$R_{AB} = R_A \otimes R_B \tag{11}$$

But,

$$|\psi_{AB}\rangle \neq |\psi_A\rangle \otimes |\psi_B\rangle \tag{12}$$

There is a composited quantum bit $\left|\psi_{AB}^{+}\right\rangle$, which is an entangled quantum state, besides, $|\psi_A\rangle$ and $|\psi_B\rangle$ is an entangled pair. It must satisfy the underneath condition,

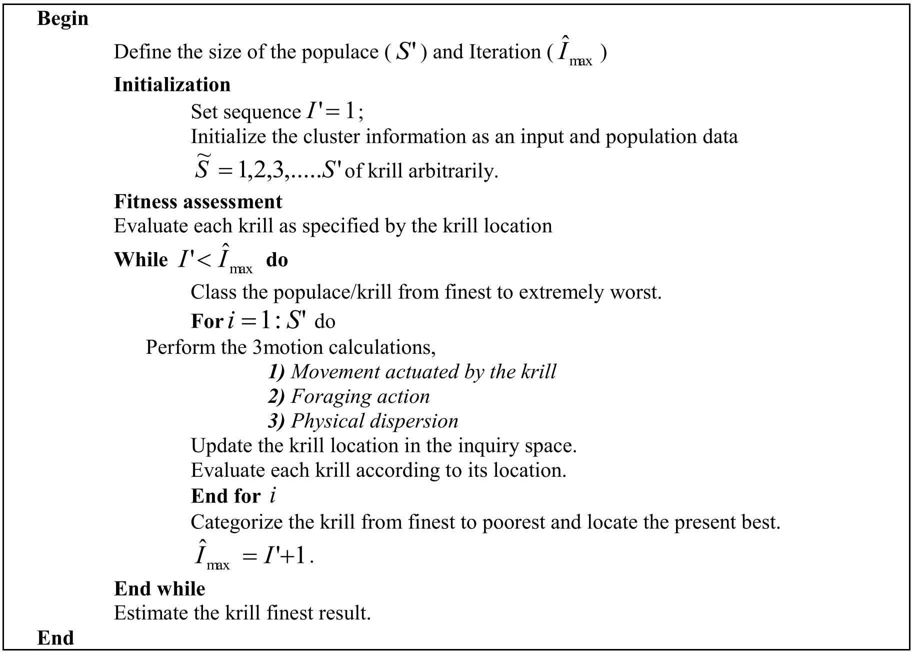
$$\left|\psi_{AB}^{+}\right\rangle = \frac{1}{\sqrt{2}}\{|0_A\rangle \otimes |1_B\rangle + |1_A\rangle \otimes |0_B\rangle\} \tag{13}$$

The feature of this condition can be described that when the, $|\psi_A\rangle$ is $|0\rangle$. the state of $|\psi_B\rangle$. certainly is opposite $|1\rangle$. vice versa. Be that as it may, when $|\psi_A\rangle$. is collapsed to Eigen state $|1\rangle$. by measurement, $|\psi_B\rangle$. unavoidably collapses to opposite Eigen state $|0\rangle$. vice versa. In this way, the data packet is coded before the transmission to secure the transmission data. Finally, the coded data packet is transmitted through the clustered nodes to the destination node securely.

### E. Secure routing using adaptive krill herd optimization

Effective Routing to transmit the data packets is acquired by utilizing the Adaptive Krill herd (AKH) algorithm. This optimization algorithm chooses a congestion-free path for data transfer. This is an iterative heuristic strategy necessitated by the inherent krill herd phenomenon. This is primarily used to resolve optimization concerns. Algorithm 2 contains the pseudocode for krill herd optimization.

**Algorithm 2** Pseudo-code for the algorithm for optimizing krill herds



```
Begin
        Define the size of the populace ( $S'$ ) and Iteration ( $\hat{I}_{\max}$ )
        Initialization
                Set sequence $I' = 1$;
                Initialize the cluster information as an input and population data
                $\widetilde{S} = 1,2,3,.....S'$ of krill arbitrarily.
        Fitness assessment
        Evaluate each krill as specified by the krill location
        While $I' < \hat{I}_{\max}$ do
                Class the populace/krill from finest to extremely worst.
                For $i = 1 : S'$ do
            Perform the 3motion calculations,
                        1) Movement actuated by the krill
                        2) Foraging action
                        3) Physical dispersion
                Update the krill location in the inquiry space.
                Evaluate each krill according to its location.
                End for $i$
                Categorize the krill from finest to poorest and locate the present best.
                $\hat{I}_{\max} = I' + 1$.
        End while
        Estimate the krill finest result.
End
```

The described krill herd optimization resulted in a successful selection of a congestion-free path through the preceding steps.

*Step 1*

The optimization starts with the initialization of standardized data.

*Step 2*

Fitness esteem is assessed reliant on the adaptive krill individual positions. This adaptive technique can lessen the computational time to reach an ideal solution, maintain a strategic distance from neighborhood minima, and have faster convergence. The adaptive methodology for KH is detailed as:

$$X_i^{t+1} = X_i^t + R_n * \left(\frac{1}{t}\right)^{|((bestf(t) - fit(t))/(bestf(t) - worstf(t))|} \tag{14}$$

where $R_n$ is the arbitrary number,$X_i^{t+1}$ a new solution of $i$th dimension in the $t$th iteration $f(t)$ is the fitness value.

*Step 3*

Consequently, the fundamental iteration starts by positioning the krill from the finest to the exceedingly poor.

*Step 4*

From that point onwards, movement updates are handled for each krill utilizing the going with conditions,

(a) The searching update is done by,

$$\overline{F}_z\left(\hat{t}+1\right) = S_f\beta_x + \omega_i\overline{F}_z\left(k'\right) \tag{15}$$

$$\beta_z = \beta_z^{food} + \beta_z^{best} \tag{16}$$

where $S_f$ denotes the foraging speed, $\omega_i$ denotes the inertia weight, $\beta_z^{best}$ denotes the finest result of the $z$th krill individual.

(b) The induced movement relates to the thickness preservation of information is represented as,

$$\overline{M}_z\left(\hat{t}+1\right) = \widehat{\overline{M}\overline{z}_{iz\,\max}} \tag{17}$$

$$\alpha_z = \alpha_z^{total} + \alpha_z^{t\arg et} \tag{18}$$

where $\overline{M}_{max}$ denotes the most extreme activated speed, $\omega_i$ denotes the inertia weight, $\alpha_z^{total}$ denotes the nearby effect of the $z$th krill individual has on its neighbours, $\alpha_z^{t\arg et}$ is the finest result of the $z$th krill.

(c) The final movement update is coordinating the physical distribution through irregular action and is represented as,

$$\overline{D}_y\left(\hat{t}+1\right) = \overline{D}\frac{1-i}{i_{max}}{}_{max} \tag{19}$$

where $\overline{D}_{max}$ denotes the greatest diffusion speed, $\delta$ denotes the random directional vector between $-1$ and 1.

*Step 5*

In perspective on the recently demonstrated advancements, utilizing special parameters of development during the time, the location of the $y$th krill amidst an opportunity to $\hat{t}+\Delta\hat{t}$ is passed on by the related condition and it is used to calculate a node individual location.

$$\overline{K}_z\left(\hat{t}+\Delta\hat{t}\right) = \overline{K}_z\left(\hat{t}\right) + \Delta\hat{t}\frac{d\overline{K}_z}{d\hat{t}} \tag{20}$$

where $\Delta\hat{t}$ signifies a fundamental constant. Hereby utilizing the reference condition, the krill individual's position is refreshed and the best outcome is obtained (Fig. 2).

*Step 6*

At the conclusion, the halting condition is utilised to ensure that function assessment are completed. Regardless of whether the pausing condition has not been reached yet, classify the krill population from best to worst and estimate the best node individual site. Figure 3 depicts the flow chart for optimizing krill herds.

This proposed advancement results in effective routing for the data transmission in wireless sensor networks for IoT applications. Additionally, the suggested secure routing results in a high packet receipt rate, reduced end-to-end latency, and reduced energy consumption.

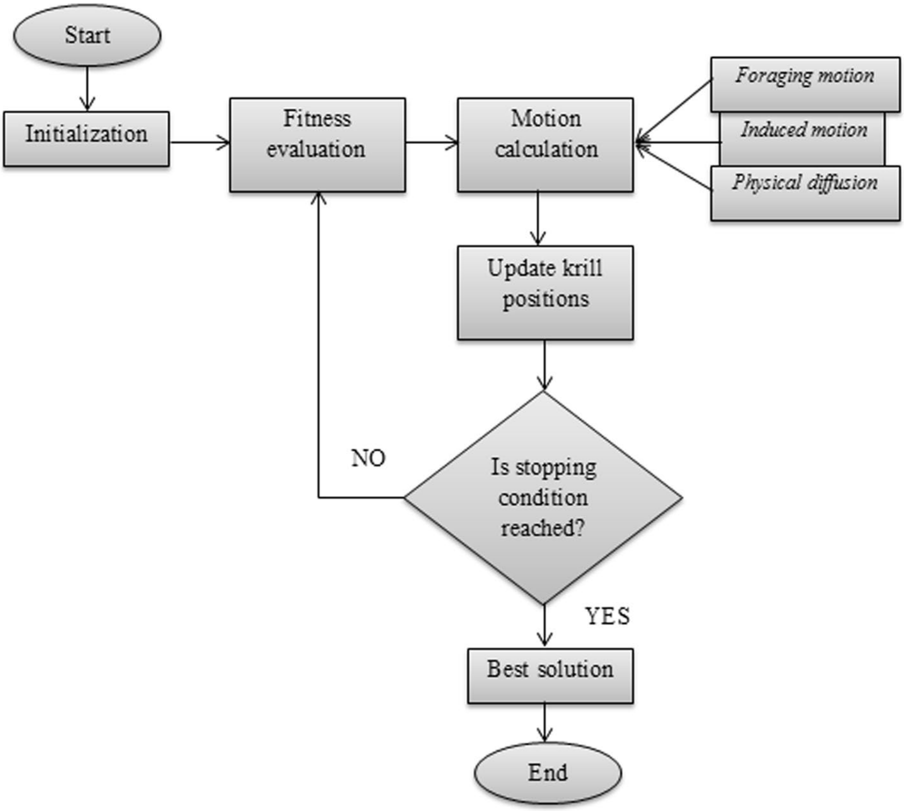
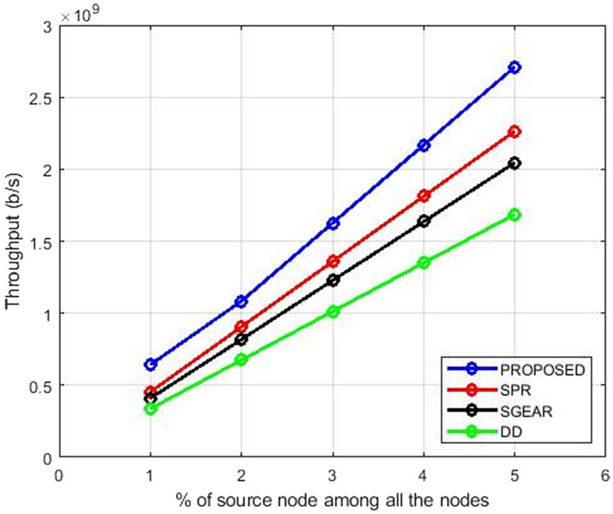


**Fig. 2** Flow diagram of adaptive krill herd optimization

**Fig. 3** Comparison analysis of proposed throughput



## 4 Results and Discussion

Our suggested efficient routing protocol in a WSN for IoT applications is implemented using MATLAB 2018a's working stage. To evaluate the proposed work's performance, various execution estimates such as packet delivery ratio, energy consumption, packet drop, and remaining energy are compared to the existing Directed Diffusion Routing Protocol, Sub-Game Energy-Aware Routing Protocol (SGEAR), and Survivable Path Routing (SPR) protocols. The simulation parameters utilized in the proposed routing protocol is given in Table 1.

The exhibition of the proposed work analysis with different execution estimates such as packet delivery ratio, energy consumption, packet drop, the remaining energy is portrayed in subsections.

B. Throughput

Throughput is the quantity of information where a network or entity transmits or gets data with the one determined time–space. It holds the fundamental parts of measures the bit/second.

$$T_h = \frac{D_p * S_p}{t_s} \tag{21}$$

where $T_h$ signifies the throughput,$D_p$ signifies several delivered packet, $S_p$ signifies the size of the packet, $t_s$ signifies total simulation time. The throughput of our proposed technique is essentially higher than the existing Directed Diffusion Routing Protocol, Sub-Game Energy-Aware Routing Protocol (SGEAR), and Survivable Path Routing (SPR) [27]. Subsequently, our proposed routing gives a better outcome over the current strategies. The examination graph for the throughput is appeared beneath in Fig. 3.

As illustrated in Fig. 3, our proposed routing protocol has a significantly greater throughput than the existing Directed Diffusion Routing Protocol, Sub-Game Energy-Aware Routing Protocol (SGEAR), and Survivable Path Routing (SPR).

**Table 1** simulation parameters

| Parameter name | Parameter value |
|---|---|
| Propagation mode | Shadowing model |
| Transmitting range | 40 m |
| MAC Protocol | IEEE 802.15.4 |
| Traffic flow | Constant Bit Rate |
| Data transfer rate | 10 pkt/sec |
| Packet size | 50 bytes |
| Initial energy | 100 J |
| Cycle time | 10 s |

C. Packet Delivery Ratio

It is portrayed as the proportion of total packets received to the target by the total number of packets transmitted from the source. A high packet delivery ratio will adjust the enhanced performance of the protocol.

$$PDR = \left( {}^{R_p}\!/_{S_p} \right) * 100 \tag{22}$$

where $PDR$ signifies the Packet delivery ratio, $R_p$& $S_p$ be the total number of packets received and transmitted. The comparison graph regarding packet delivery ratio is given in Fig. 4,

As illustrated in Fig. 4, our suggested routing has a significantly greater packet delivery ratio than the existing Directed Diffusion Routing Protocol, Sub-Game Energy Aware Routing Protocol (SGEAR), and Survivable Path Routing (SPR).

D. End To End Delay

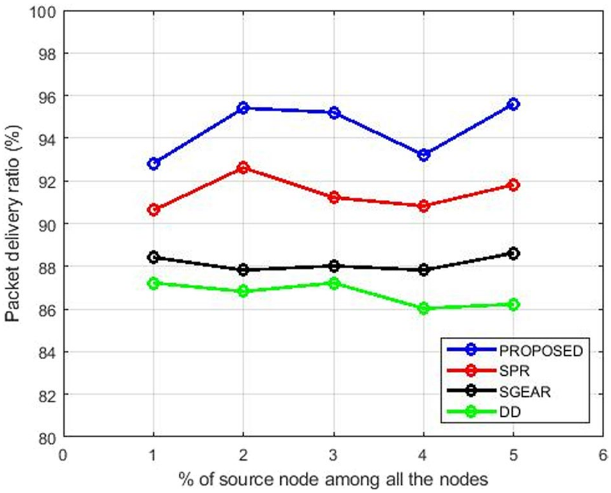
It is described as the average time consumed by the packet to accomplish destination, this embraces the route discovery time and the queue handling time at the time of transmission. The end to end delay is gotten by taking the difference between the packets sending time to the receiving time.

$$D_{end-end} = t_r - t_s \tag{23}$$

where $D_{end-end}$ signifies the end to end delay, $t_r$ be the receiving time, $t_s$ signifies the sending time. The comparison graph in terms of end to end delay is given in Fig. 5,

As illustrated in Fig. 5, our proposed routing protocol has a much longer end-to-end delay than the existing Directed Diffusion Routing Protocol, Sub-Game Energy-Aware Routing Protocol (SGEAR), and Survivable Path Routing Protocol (SPR).

**Fig. 4** Comparison analysis of proposed packet delivery ratio



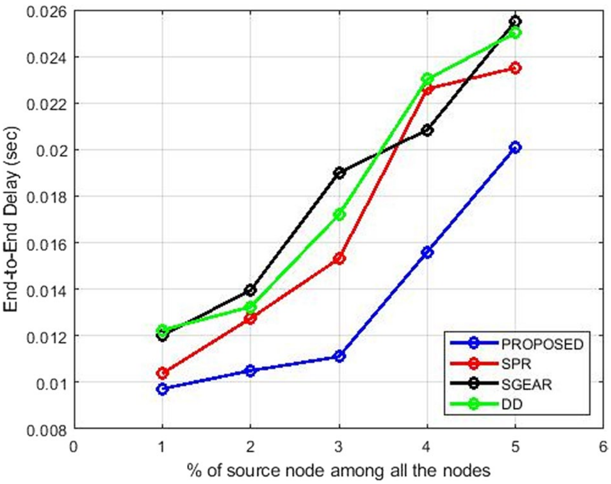


**Fig. 5** Comparison analysis of proposed End to End delay

E. Packet Drop

The number of packets dropped by a malicious node and not received by the destination is referred to as packet drop.

$$P_d = \overline{T}_n - \overline{p}_d \tag{24}$$

here $T_n$ is the total number of packets, $M_d$ is the message drop, $p_d$ is the packets delivered to the destination. The comparison graph of proposed secure routing with existing Directed Diffusion Routing Protocol, Sub-Game Energy-Aware Routing Protocol (SGEAR), and Survivable Path Routing (SPR) in terms of packet drop for a varying number of nodes is delineated in Fig. 6.

Figure 6 delineates that the proposed secure routing provides better outcomes regarding packet drop than the existing Directed Diffusion Routing Protocol, Sub-Game Energy-Aware Routing Protocol (SGEAR), and Survivable Path Routing (SPR).

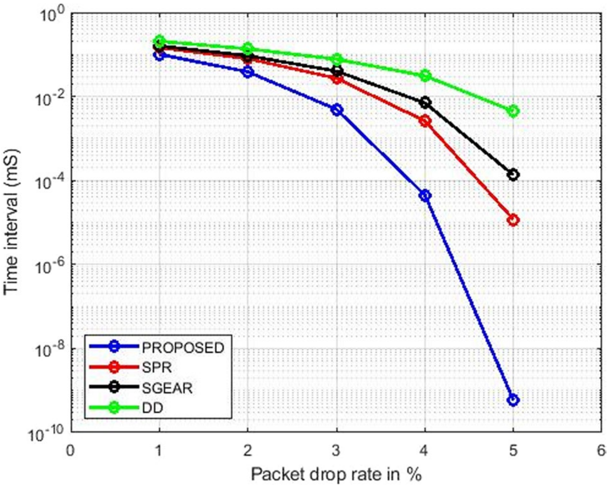


**Fig. 6** Comparison graph in terms of packet drop

**Fig. 7** Comparison graph in terms of remaining energy for proposed routing with existing Directed Diffusion (DD) Routing Protocol

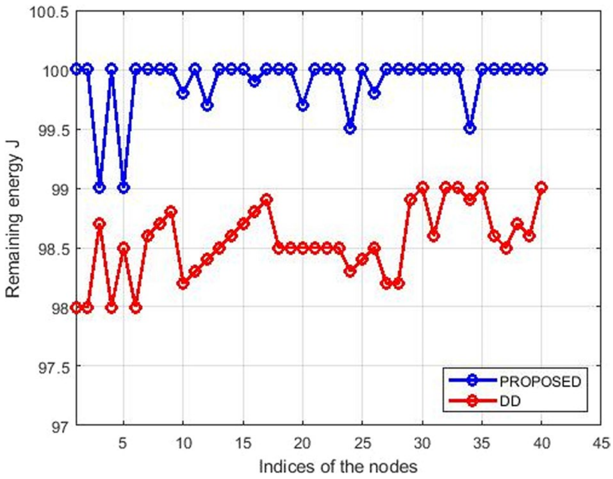
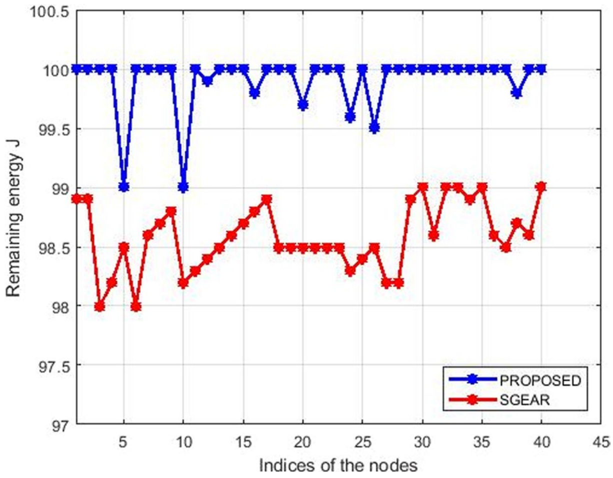


**Fig. 8** Comparison graph in terms of remaining energy for proposed routing with existing Sub-Game Energy-Aware Routing Protocol (SGEAR)



F. Remaining Energy

Nodes spread across the topological area must maintain a constant energy level to ensure the network's survival. The system's source nodes initiate information packets at a rate of ten per second, and they travel over multi-hop paths to the destination node. Figures 7, 8 and 9 show a comparison of the nodes' residual energy levels following ten rounds of information exchange between source and destination.

Routing proposed in conjunction with the existing Survivable Path Routing (SPR) As illustrated in Figs. 7, 8 and 9, the network nodes with the directed diffusion protocol have a larger degree of uniqueness in their energy strength. However, for the proposed protocol, the energy capabilities of the network nodes are nearly the same. Thus, it may be beneficial to maintain network connectivity for an extended length of time and gradually improve the system's survivability. The proposed protocol's maintenance phase assists in doing this, as the relay nodes send each data packet after being checked for compliance with a specified

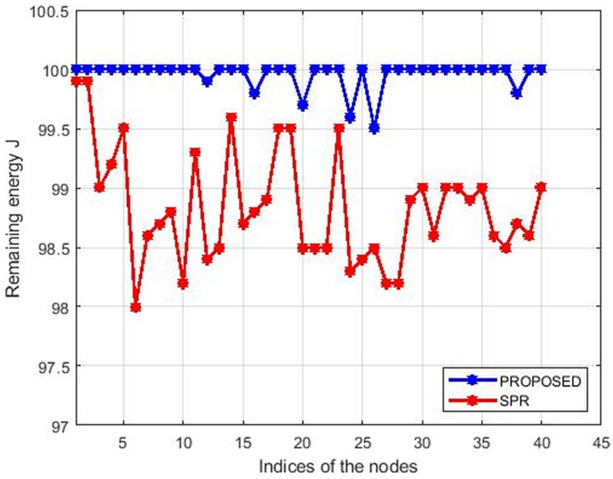


**Fig. 9** Comparison graph in terms of remaining energy

energy threshold. If the residual energy limit of any node falls below that threshold, the routes are rearranged, and the path selection metrics are updated. As a result, all nodes in the system will keep the same battery capacity, extending the network's connectivity.

## 5 Conclusion

In high-traffic IoT application situations, the wireless communication connection used by the sensor network nodes to send data might be subject to interference. The suggested routing method takes into account the noise level, possible interference, and connection quality before choosing a next-hop node for communication. Thus, the SINR, congestion level, and survival characteristics are included in the node selection process during clustering. Other critical factors for the best route selection are the survival factor of the path and the congestion levels at nodes. Adaptive quantum logic technology also enhances the security of data transmission. Adaptive krill herd optimization then offers more secure data transmission route after that. The results of the simulation show that in high-traffic networks, the suggested protocol performs better than the current methods. It has a low energy consumption, a short end-to-end latency, and a high packet reception rate [33–35].

**Author Contributions** The author's declare no contribution**.**

**Funding** Open access funding provided by University of South Africa. There are no funding details available.

**Data Availability** There is no data available in this manuscript.

**Code Availability** There is no code available in this manuscript.

## Declarations

**Conflict of interest** The authors declare s no conflict of Interest.

**Informed Consent** There is no Informed Consent.

## References

1. Hakiri, A., Berthou, P., Gokhale, A., & Abdellatif, S. (2015). Publish/subscribe-enabled software defined networking for efficient and scalable IoT communications. *IEEE Communications Magazine, 53*(9), 48–54.
2. Alanazi, S., Al-Muhtadi, J., Derhab, A., Saleem, K., AlRomi, A. N., Alholaibah, H. S., & Rodrigues, J. J (2015). On the resilience of wireless mesh routing protocol against dos attacks in iot-based ambient assisted living applications. In *2015 17th international conference on e-health networking, application & services (HealthCom)* (pp. 205–210). IEEE.
3. Sung, W.-T., Chen, J.-H., & Tsai, M.-H. (2016). Applications of wireless sensor network for monitoring system based on IoT. In *2016 IEEE international conference on systems, man, and cybernetics (SMC)* (pp. 000613–000617). IEEE.
4. Lee, H.-C., & Ke, K.-H. (2018). Monitoring of large-area IoT sensors using a LoRa wireless mesh network system: Design and evaluation. *IEEE Transactions on Instrumentation and Measurement, 67*(9), 2177–2187.
5. Granjal, J., Monteiro, E., & Silva, J. S. (2015). Security in the integration of low-power wireless sensor networks with the internet: A survey. *Ad Hoc Networks, 24*, 264–287.
6. Kharrufa, H., Al-Kashoash, H., Al-Nidawi, Y., Mosquera, M. Q., & Kemp, A. H. (2017). Dynamic RPL for multi-hop routing in IoT applications. In *2017 13th annual conference on wireless on-demand network systems and services (WONS)* (pp. 100–103). IEEE.
7. Da Costa, G. A., & Kleinschmidt, J. H. (2016). Implementation of a wireless sensor network using standardized IoT protocols. In *2016 IEEE international symposium on consumer electronics (ISCE)* (pp. 17–18). IEEE.
8. Nair, K., Kulkarni, J., Warde, M., Dave, Z., Rawalgaonkar, V., Gore, G., & Joshi, J. (2015). ptimizing power consumption in IoT based wireless sensor networks using bluetooth low energy. In *2015 international conference on green computing and Internet of Things (ICGCIoT)* (pp. 589–593). IEEE.
9. Mainetti, L., Patrono, L., & Vile, A. (2011). Evolution of wireless sensor networks towards the internet of things: A survey. In *SoftCOM 2011, 19th international conference on software, telecommunications and computer networks* (pp. 1–6). IEEE.
10. Mainetti, L., Patrono, L., Stefanizzi, M. L., & Vergallo, R. (2015). A smart parking system based on IoT protocols and emerging enabling technologies. In *2015 IEEE 2nd world forum on Internet of Things (WF-IoT)* (pp. 764–769). IEEE.
11. Kotagi, V. J., Singh, F., & Murthy, C. S. R. (2017). Adaptive load-balanced routing in heterogeneous IoT networks. In *2017 IEEE international conference on communications workshops (ICC workshops)* (pp. 589–594). IEEE.
12. Vankdothu, R., Hameed, M. A., & Fatima, H. (2022). A brain tumor identification and classification using deep learning based on CNN-LSTM method. *Computers and Electrical Engineering, 101*, 107960.
13. Vankdothu, R., & Hameed, M. A. (2022). Adaptive features selection and EDNN based brain image recognition on the internet of medical things. *Computers and Electrical Engineering, 103*, 108338.
14. Airehrour, D., Gutierrez, J., & Ray, S. K. (2016). Secure routing for the internet of things: A survey. *Journal of Network and Computer Applications, 66*, 198–213.
15. Bera, S., Misra, S., Roy, S. K., & Obaidat, M. S. (2016). Soft-WSN: Software-defined WSN management system for IoT applications. *IEEE Systems Journal, 12*(3), 2074–2081.

16. Vankdothu, R., Hameed, M. A., Ameen, A., & Unnisa, R. (2022). Brain image identification and classification on Internet of Medical Things in healthcare system using support value based deep neural network. *Computers and Electrical Engineering, 102*, 108196.
17. Vankdothu, R., & Hameed, M. A. (2022). Brain tumor segmentation of MR images using SVM and fuzzy classifier in machine learning. *Measurement: Sensors Journal, 24*, 100440.
18. Vankdothu, R., & Hameed, M. A. (2022). Brain tumor MRI images identification and classification based on the recurrent convolutional neural network. *Measurement: Sensors Journal, 24*, 100412.
19. Al-Turjman, F., & Radwan, A. (2017). Data delivery in wireless multimedia sensor networks: Challenging and defying in the IoT era. *IEEE Wireless Communications, 24*(5), 126–131.
20. Sheng, Z., Mahapatra, C., Zhu, C., & Leung, V. C. M. (2015). Recent advances in industrial wireless sensor networks toward efficient management in IoT. *IEEE Access, 3*, 622–637.
21. Madhu, B., Chari, M. V. G., Vankdothu, R., Silivery, A. K., & Aerranagula, V. (2022). Intrusion detection models for IOT networks via deep learning approaches. *Measurement: Sensors Journal, 25*, 100641.
22. Ahemad, M. T., Hameed, M. A., & Vankdothu, R. (2022). COVID-19 detection and classification for machine learning methods using human genomic data. *Measurement: Sensors Journal, 24*, 100537.
23. Al-Tudjman, F. (2018). QoS: Aware data delivery framework for safety-inspired multimedia in integrated vehicular-IoT. *Computer Communications, 121*, 33–43.
24. Memos, V. A., Psannis, K. E., Ishibashi, Y., Kim, B.-G., & Gupta, B. B. (2018). An efficient algorithm for media-based surveillance system (EAMSuS) in IoT smart city framework. *Future Generation Computer Systems, 83*, 619–628.
25. Esfahani, A., Mantas, G., Matischek, R., Saghezchi, F. B., Rodriguez, J., Bicaku, A., Maksuti, S., Tauber, M. G., Schmittner, C., & Bastos, J. (2017). A lightweight authentication mechanism for M2M communications in industrial IoT environment. *IEEE Internet of Things Journal, 6*(1), 288–296.
26. Tomovic, S., Yoshigoe, K., Maljevic, I., & Radusinovic, I. (2017). Software-defined fog network architecture for IoT. *Wireless Personal Communications, 92*(1), 181–196.
27. Elappila, M., Chinara, S., & Parhi, D. R. (2018). Survivable path routing in WSN for IoT applications. *Pervasive and Mobile Computing, 43*, 49–63.
28. Wu, D., & Chatzigeorgiou, D. (2015). Node localization in robotic sensor networks for pipeline inspection. *IEEE Transaction on Industrial Informatics, 12*(2), 809–819.
29. Pamukcu, S., Cheng, L., & Pervizpour, M. (2018). Introduction and overview of underground sensing for sustainable response. In *Underground sensing monitoring and hazard detection for environment and infrastructure* (pp. 1–42).
30. Yuan, X., & Chen, Y. (2022). Secure routing protocol based on dynamic reputation and load balancing in wireless mesh networks. *Journal of Cloud Computing, 11*(1), 77. https://doi.org/10.1186/s13677-022-00346-x
31. Altuwairioi, M. (2024). An optimizedmulti-hop routing protocol for wireless sensor network using improved honey badger optimization algorithm for efficient and security QOS. *Computer Communications, 214*, 244–259.
32. Sharma, S. K., & Chawla, M. (2023). Compatibility analysis of cluster-based WSN framework for IoT applications. *Wireless Personal Communications, 131*(2), 1365–1380. https://doi.org/10.1007/s11277-023-10486-1
33. Vankdothu, R., & Cheng, X. (2024). Energy efficient TDMA and secure based MAC protocol for WSN using AQL coding and ASGWI Clustering. *Wireless personal Communications, 136*(4), 2125–2143.
34. Nayini D., Kalyani, M., Vankdothu, R. (2024). A hybrid approach: SVM-ensemble transfer learning for comprehensive rice plant disease detection. *African Journal of Biological Science*, *6*(Si2).
35. Ladda, A., Devunuri, S., & Vankdothu, R. (2024). Resource management system database maintenance in cloud computing. *MATEC Web of Conferences, 392*, 01134.

**Publisher's Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

**Ramdas Vankdothu** received his Master's in Computer Science and Engineering from Kakatiya University Warangal, India. He is pursuing his Doctoral degree in Computer Science and Engineering at Osmania University Hyderabad, India. His research interest is Machine Learning, Deep Learning, Big Data analytics, Image Processing. He published above 10 papers in peer-reviewed International journals and conferences.

**Mohd Abdul Hameed** did his B.Tech CSE in 2004 and M.TechCSE in 2007 in Jawaharlal Nehru University Hyderabad. He did Ph.D. in 2017 at Osmania University Hyderabad. Working as Assistant Professor in Department of Computer Science and Engineering University College of Engineering (A), Osmania University Hyderabad from 2013 to Till Date. Also holding additional responsibility of Training and Placement officer, University College of Engineering (A), Osmania University Hyderabad. His research area is Data Mining, Big Data, Machine Learning, Deep Learning, Soft computing, etc. Contributed to more than 30 research papers in reputed International Journal and Conference.