Multimedia Tools and Applications
https://doi.org/10.1007/s11042-024-18125-y

A QoS-aware routing approach for Internet of Things-enabled wireless sensor networks in smart cities

D. Karunkuzhali[1] · B. Meenakshi[2] · Keerthi Lingam[3]

Received: 2 June 2023 / Revised: 3 November 2023 / Accepted: 1 January 2024

Abstract
In the Internet of Things (IoT), optimizing machine performance through data analysis and improved connectivity is pivotal. Addressing the growing need for environmentally friendly IoT solutions, we focus on "green IoT." Quality in smart cities heavily relies on efficient data gathering and communication. In this study, we propose a novel software architecture tailored for data collection and communication in IoT-enabled smart applications, emphasizing sustainability from the outset. Specifically, for smart cities utilizing IoT-enabled wireless sensor networks, we introduce a Quality of Service (QoS)-aware routing strategy. In the data collection phase, we employ Chaotic Bird Swarm Optimization (CBSO) for creating IoT sensor clusters, accompanied by Improved Differential Search (IDS) to assess the reliability of individual sensor nodes, ultimately designating the most trusted node as the Cluster Head (CH). In the data transport phase, we implement lightweight signcryption to enhance the security of IoT sensor data. Furthermore, we employ an Optimal Data Routing (ODM) approach to compute the most efficient data transmission paths between source and destination nodes within the IoT network. Finally, the performance of our QoS-aware routing strategy is evaluated through network simulations using NS2 and compared against existing approaches, offering valuable insights into its effectiveness and suitability for smart city IoT applications. The main findings of the study indicate that the proposed QoS-aware routing strategy (QOS-AWARE ROUTING) consistently outperforms existing routing algorithms in terms of energy efficiency, network longevity, and latency, both in scenarios with varying sensor node density and over multiple cycles. Additionally, it demonstrates significant advantages, such as up to 90.8% less energy consumption, 66.8% longer network lifespan, and 80.1% reduced latency when compared to the benchmarked methods.

Keywords Internet of things · QoS-aware routing · Smart cities · Improved differential search · Wireless sensor network

✉ D. Karunkuzhali
karunkuzhali@gmail.com

[1] Department of Information Technology, Panimalar Engineering College, Chennai, India

[2] Department of Electrical and Electronics Engineering, Sri Sairam Engineering College, Chennai, India

[3] Department of Computer Science and Engineering, Gitam University, Visakhapatnam, India

1 Introduction

The internet of things (IoT) encompasses sensors, software, and other data-transfer technologies. Wireless sensor network (WSN) knowledge is a crucial component of IOT, but it has antenna nodes that may supply digital interface in the real world [1]. IOT and WSN's connection with smart devices grows. IoT integrates smart devices, sensors, and embedded technologies to build a smart city. IoT advanced wireless communication and MEMS [2, 3]. In IoT, system nodes may communicate with other nodes, people, or substances. Smart environments, traffic, and monitoring use IOT [4]. This research study presents the Saskatchewan Health Authority four critical health services as an IOTmodel.

IoT Development has major medicinal and multimedia applications [5]. Grid optimization has resulted to energy savings and improved electrical safety [6]. WSN's strong nodes enable IoT communication. IoT describes the Internet from computers, home gadgets, or WSN sensor nodes [7]. Multimedia models may combine to create a shared service beyond remote access This special edition focuses on Smart City and IoT developments [8]. IOT framework Media is omnipresent, effortlessly integrating end-to-end, well-established systems and sensors [9]. So one of the most widely used technologies in the digital era has gone from beautiful stages to integrated healthcare [10]. Due to the cheap of sensors and the breakdown of municipal administration, real-time data-based management of urban systems, including water, electricity, garbage, and transit, is possible [11]. For smart cities with IoT-enabled wireless sensor networks, QoS-aware routing technique is proposed.

This lays the foundation for the research by highlighting the key concepts and motivations behind the study. In this context, the research focuses on the IoT and its interconnection with WSN to build smart cities. The integration of IoT with smart devices, sensors, and embedded technologies plays a pivotal role in advancing various sectors, including healthcare and grid optimization. The research also introduces the Saskatchewan Health Authority's model as a case study, emphasizing the significance of IoT in healthcare. Furthermore, it highlights the potential for real-time data-based management of urban systems made feasible by IoT-enabled wireless sensor networks, with a particular emphasis on the proposed QoS-aware routing technique. The main research question driving this study is, "How can QoS-aware routing enhance the efficiency and performance of IoT-enabled wireless sensor networks in the context of smart cities?" This question sets the stage for the subsequent sections of the research to delve into the proposed methodology and its implications.

1.1 Contributions

The major contributions of proposed QoS-aware routing technique are as follows:

1. The CBSO algorithm develops IoT sensor clusters; the IDS algorithm computes every sensor node's trust degree; the highest trust node acts as CH.
2. Lightweight sign cypher for IoT data encryption. Then, we utilized ODM to determine the optimal source–destination path in IOT.
3. The QoS-aware routing approach deploys and evaluates performance utilizing simulated scenarios. The results compared to existing QoS measurements.

1.2 Organization of paper

The paper's remaining sections are: Section 2 discusses IoT for smart cities, efficient routing strategies, and clustering protocols. Section 3 describes the QoS-aware routing technique's complexity mechanism and system model. Section 4 describes QoS-aware routing using a mathematical model. Section 5 compares proposed and existing routing approaches using simulations. Section 6 concludes the paper.

2 Literature review

Dilek et al. [12] (2022) surveyed QoS support in IoT networks and protocols. Existing research on QSO delivery efficiency had limitations. Majid et al. [13] (2022) focused on industrial automation for Industry 4.0. Over 130 papers from 2014 to 2021 were evaluated. The article discussed Industry 4.0's design, security, deployment, network classification, issues, challenges, and future directions.

Mishra et al. [14] (2022) developed the HGWO-BC algorithm, which improved energy efficiency in data collection for IoT sensor networks using SDN. Simulations demonstrated that it outperformed existing methods in network lifetime, stability, energy conservation, data transmission, and computational needs.

A systematic literature review (SLR) on IoT was conducted Kumar et al. [15] (2022). Comparing IoT apps based on quality of service and environmental evaluation. The review identified application domains, popular designs, and difficulties. Quy et al. [16] (2021) look at a few of the different routing protocols for WSN-MANETs that ensure quality of service.

A hybrid cluster root rotational tree network was developed for QoS-aware LoRa networks (MQ-LoRa) by Muthanna et al. [17] (2022). Multi-weighted sum methodology decreased LoRa IoT wastage of resources and data loss. Fathi et al. [18] (2021) compared competing sensor networks based on service pricing and quality of service. They developed a nonlinear programme that maximized income and social benefit revenue while decreasing wait time for sensors, among other features.

QoS and energy-aware service selection methods were presented by Demir & Kubilay [19] (2021). Using comprehensive simulations on a realistic test-bed, the presented algorithms' message overhead, latency, scalability, reliability, and QoS accuracy were analyzed. Jaiswal et al. [20] (2021) developed a Grey wolf optimization-based cluster head selection approach for WSN. The suggested approach was simulated and evaluated using QoS metrics such as residual energy, stability period, throughput, network lifespan, and delay. Wang et al. [21] (2021) explored a QoS-aware cloud-edge service discovery and selection methodology in IoT. The suggested solution reduced cost 30% better than other algorithms, as per experiments.

Akhtar et al. [22] developed an energy-efficient opportunistic routing system (I-AREOR) based on density, distance, and residual energy. FND, HND, and LND are important hurdles in increasing energy efficiency. This extends FND by including sensor node density, distance, and residual energy. I-AREOR sets power depending on each circuit's dynamic range. I-AREOR clustering increases network life better than existing approaches, as per experiments. It improves performance and communication between software components in diverse configurations. IoT domains include service-based and cloud-based software configuration applications.

Avval et al. [23] (2022) developed a meta-heuristic algorithm based on the elephant herd optimization algorithm is proposed to minimize resource costs, conversion costs, and the cost of continuous development delays. By combining the clan updating factor, separating operator, and the proposed algorithm, we created an effective and efficient method to solve the issue of production scheduling. Many experiments are performed to determine the performance of industrial environments. The outcomes demonstrate that the suggested technique can optimize planning and achieve cost reduction, efficient energy consumption, and latency decrease.

Qin et al. [24] (2023) developed a distributed Cross-interface network Partitioning and Scheduling (CPS) protocol, which leverages the co-existing ZigBee communications to divide the network into partitions and allows only one node in each partition to use its WiFi interface to transmit data at any time, for bandwidth-efficient and delay-constrained data flow delivery in M-IoT. A prototype node is implemented by integrating COTS ZigBee and WiFi interfaces into a BeagleBone Green wireless platform for IoT. Extensive field experiments are conducted in a multi-hop network of 24 prototype nodes that deliver real multimedia data (images and videos). The experiment results show that CPS outperforms the standard WiFi and a state-of-the-art contention control scheme (by 62.6% and 26.4% under high data traffic, respectively) in terms of a QoS metric capturing two basic performance metrics (i.e., bandwidth efficiency and end-to-end delay) of multi-hop communications, while retaining fair QoS performance and high energy efficiency.

2.1 Research gaps

The literature review identifies significant research gaps in the existing literature, such as limited focus on comprehensive QoS support in IoT networks, a primarily industrial automation-oriented perspective in Industry 4.0 studies, a lack of environmental evaluation in IoT applications, limited discussions on practical implementations, and the absence of specific quantitative results in certain energy-efficient routing strategies. To address these limitations, the proposed work endeavors to introduce a holistic QoS-aware routing strategy tailored for IoT-enabled wireless sensor networks in smart cities, offering comprehensive QoS support, expanding its scope beyond industrial contexts, considering environmental sustainability, emphasizing practical implementation, and providing specific quantitative performance metrics, thus contributing to the advancement of the field by addressing these critical research gaps. Table 1 presents a summary of the research gaps identified in the study.

3 Proposed QoS-aware routing problem statement and system model

The problem statement and system model revolve around the implementation of IoT in the context of Smart Cities, where a reliable communication platform is crucial for serving consumers and facilitating distributed resource sharing. An essential challenge in this scenario is to ensure the secure and efficient selection of devices while preventing unauthorized access, data transfer, and transmission. Both internal and external communication constraints must be taken into account.

As a response to these challenges, the research suggests the adoption of a novel data collection and communication software architecture tailored for IoT-based smart applications.

Table 1 Research Gap Summary

Reference	Focus	Advantages	Disadvantages
Dilek et al. [12]	QoS in IoT networks and protocols	Surveyed QoS support in IoT networks	Limited scope in addressing QoS delivery efficiency
Majid et al. [13]	Industrial automation for Industry 4.0	Comprehensive overview of Industry 4.0 aspects	Focuses on industrial applications only
Mishra et al. [14]	HGWO-BC algorithm for IoT sensor networks using SDN	Improved energy efficiency, network lifetime, stability, and computational needs	Validation in real-world scenarios and larger-scale deployments
Kumar et al. [15]	IoT apps, quality of service, environmental evaluation	Identified application domains and popular designs	Environmental evaluation details not provided
Quy et al. [16]	Routing protocols for WSN-MANETs	Examined different routing protocols for QoS	Specific routing protocol advantages not detailed
Muthanna et al. [17]	QoS-aware LoRa networks (MQ-LoRa)	Developed a hybrid cluster root rotational tree network	Specific benefits of LoRa over other networks not discussed
Fathi et al. [18]	Sensor networks, service pricing, quality of service	Developed a nonlinear program for maximizing income	Lack of discussion on the practical implementation of the proposed solution
Demir & Kubilay [19]	QoS and energy-aware service selection	Presented QoS and energy-aware service selection methods	Details on the realistic test-bed and simulation environment are missing
Jaiswal et al. [20]	Grey wolf optimization-based cluster head selection	Developed a cluster head selection approach for WSN	The scope of the evaluation and the network size not specified
Wang et al. [21]	QoS-aware cloud-edge service discovery and selection	Achieved cost reduction in IoT service discovery	The comparison with other algorithms lacks detailed metrics
Akhtar et al. [22]	Energy-efficient opportunistic routing system (I-AREOR)	Extended FND by including sensor node density, distance, and residual energy	Specific quantitative results of energy efficiency improvements are needed
Avval et al. [23]	Meta-heuristic algorithm for optimization	Proposed an algorithm for resource and cost optimization	The practical applicability of the proposed algorithm is not discussed
Qin et al. [24]	Cross-interface network Partitioning and Scheduling (CPS)	Developed a protocol for bandwidth-efficient and delay-constrained data flow delivery	Details on real-world scalability and limitations are not provided

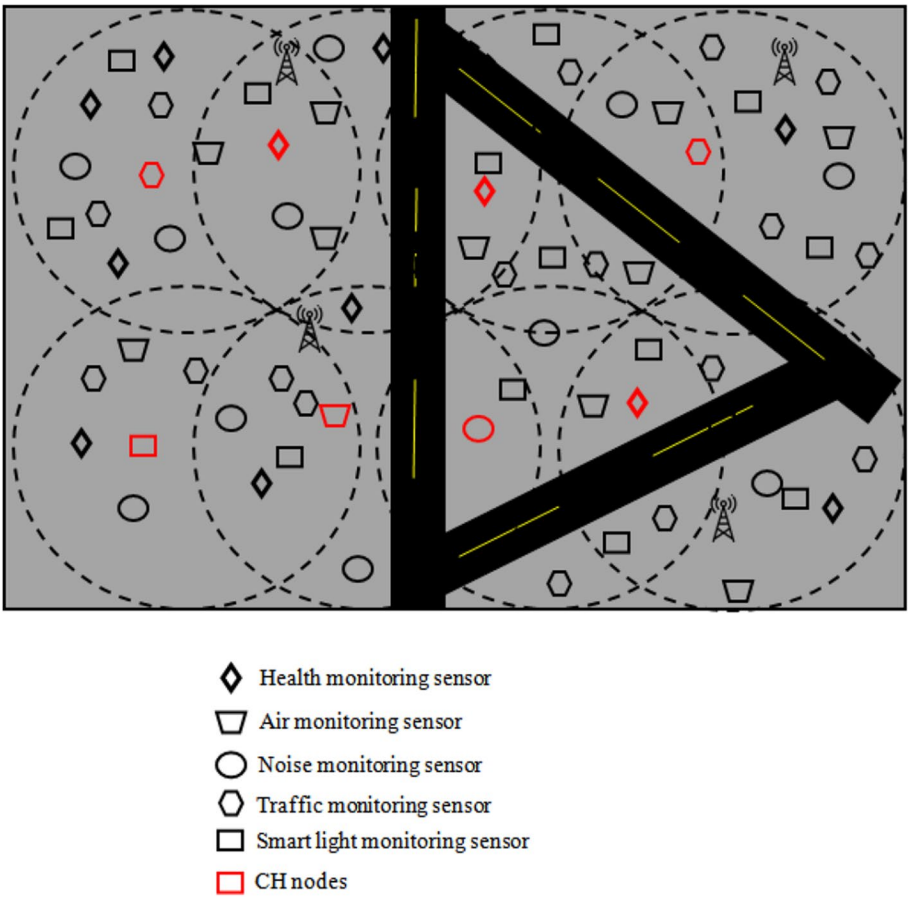

Fig. 1 System model of proposed QOS-AWARE ROUTING technique

Figure 1 illustrates the proposed QoS-aware routing system model, which serves as a solution to address the aforementioned issues. This system model seeks to enhance the overall performance and quality of service for IoT-enabled applications in the context of Smart Cities.

3.1 Objectives

The main objectives of Proposed QoS-aware routing technique are given as follows:

1. To employ proposed approach for smart city application.
2. To evaluate IoT data collecting and transmission issues.
3. To improve IoT resource routing.
4. To recognize how to integrate machine learning with IoT systems.
5. To propose novel optimization techniques to improve energy consumption, network lifespan, delay, throughput, FND, LND, and HND

3.2 System model

The proposed system model for smart cities with IoT-enabled wireless sensor networks comprises a two-phase approach. In the data collection phase, it utilizes Chaotic Bird Swarm Optimization (CBSO) for IoT sensor cluster creation, Improved Differential Search (IDS) for assessing sensor node trustworthiness, and Cluster Head (CH) selection based on the highest trust node. In the data transport phase, lightweight signcryption is employed for data security, and Optimal Data Routing (ODM) calculates the optimal path for data transmission. Finally, Quality of Service (QoS)-aware routing is implemented using Network Simulation (NS2) and compared to existing methods, ensuring efficient and reliable data delivery with a focus on QoS guarantees in smart city IoT networks. Figure 1 shows System model of proposed QOS-AWARE ROUTING technique.

4 QoS aware routing technique for smart cities

4.1 CBSO and IDS data collection

4.1.1 Sensor node clustering using CBSO algorithm

Any IoT-based application must gather and interpret data from relevant devices. After that, you may obtain processed internet information from anywhere. Clustering integrates devices or sensors. Sensors identify the location of corporeal objects to compile IoT data. IoT technology can monitor and compute data in real time. Anytime, data may be sent, stored, and received. Cluster analysis simplifies data management by finding data structures and categorising objects by type. Traffic can automatically link or detach IoT devices. Mobile devices may process and produce real-world data. Analyzing, interpreting, and using situational data to make judgments. CBSO is used to cluster IoT sensor data. For i^{th} particle of swarm population, velocity and position are represented as $f\ Best\ and\ q\ Best$ respectively. The updated equation is expressed as follow:

$$u_{jc}^{New} = l \times u_{jc}^{Old} + d_1 \times s_1 \times (qBest_{jc} - y_{jc}^{Old}) + d_2 \times s_2 \times (fBest_c - y_{jc}^{Old}) \tag{1}$$

$$y_{jc}^{New} = y_{jc}^{Old} + u_{jc}^{New} \tag{2}$$

Here, (0, 1) implies s_1 and s_2. Acceleration constants c_1 and c_2 define a particle's generational velocity.

$$l = 0.5 + \frac{Random}{2.0} \tag{3}$$

Refer to the random number (0, 1) in (3). PSO uses multidimensional spatial data vectors to cluster problems. A group may gather swarm particles. (4) is the logistic map.

$$Y_{(x+1)} = b \times Y_{(x)} \times (1 - Y_{(x)}) \tag{4}$$

where m is the iteration number. Here, b = 4. CPSO's logistics map changes random PSO parameters $s_1 and s_2$. Equation parameters are determined using the logistic map (5).

$$D_{(N+1)} = z \times d_{(N)} \times (1 - d_{(N)}) \tag{5}$$

CPSO's Eq. (6) updates velocity.

$$u_{jc}^{New} = l \times u_{jc}^{Old} + d_1 \times D \times (qBest_{jc} - y_{jc}^{Old}) + d_2 \times (1 - D) \times (fBest_c - y_{jc}^{Old}) \tag{6}$$

Ds implies a function from 0.0 to 1.0 based on a logistic diagram. Solution particles have levels and velocities. CPSO's pseudocode:

$$M = z \times c \tag{7}$$

Fitness function calculates particle fitness. z and m signify cluster and data set sizes. j's cluster centre is represented by and i's data point by:

$$Fitness = \sum ||Y_u - K_f||,\ f = 1, .., z, u = 1, .., m \tag{8}$$

Data vector means y_q. In every centre vector, c represents features. i's data vector subset is D_i.

$$C(z_p.k_u) = \sqrt{\sum_{f=1}^{c} (z_{pf} - k_{fu})^2} \tag{9}$$

$$k_u = \frac{1}{m_u} \sum_{\forall y_p \in d_u} z_p \tag{10}$$

Algorithm 1 provides CBSO data clustering's working function.

Algorithm 1 Clustering using CBSO algorithm

Input	: y, u, d, s
Output	: M and $C(y_q.k_i)$
1	Initialize the values for the input parameters.
2	Update the velocity and position in the equation.
3	Substitute the logistic map in the equation $Y_{(m+1)} = b \times Y_{(m)} \times (1 - Y_{(m)})$
4	Update the velocity in the equation using $Ds_{(T+1)} = z \times ds_{(T)} \times (1 - ds_{(T)})$
5	Compute the pseudo code for CPSO.
6	Evaluate the fitness for each particle.
7	End.

4.1.2 Cluster head selection based on IDS

Instant trust management is based on prior encounters. Many nodes may communicate their ideas on mutual trust because of teamwork. Threatening people may convey misleading remarks to victims to skew results. The improved differential search (IDS) is used to calculate every sensor node's belief degree.

$$Y_{ji} = WA_i + Rand(VA_i - WA_i) \tag{11}$$

This creates a mutant vector U_j:

$$U_j = Y_j + G_j(Y_{qBest} - Y_j) + G_j(Y_{s1} - Y_{s2}) \tag{12}$$

The scaling factor of Y_j is represented by G_j; $Y_{q\,Best}$ it's generally chosen at random 100 of the existing population; the random integer is denoted by s_1 and s_2.

The following generate G_j:

$$G_j = Randd(\mu_G, 0.1) \tag{13}$$

Here, *Randd* implies Cauchy distribution, starting at 0.5 and updated as follows:

$$\mu_G = (1 = d).\mu_G + d.Mean_W(R_G) \tag{14}$$

The Lehmer mean function is defined by:

$$Mean_W(R_G) = \frac{\sum_{j=1}^{|R_G|} G_j^2}{\sum_{j=1}^{|R_G|} G_j} \tag{15}$$

Normal distribution crossover rate:

$$V_{j,i} = \begin{cases} U_{ji}, & if \;\; Rand \le DS_j || i == iRand \\ Y_{ji}, & i \qquad\qquad otherwise \end{cases} \tag{16}$$

Every generation updated μ_{DS}

$$\mu_{DS} = (1 - d).\mu_{DS} + d.Mean_B(R_{DS}) \tag{17}$$

Mean is $Mean_B$. Greed is used to select which individuals will live based on their exercise values.

$$Y_j = \begin{cases} V_j, & if \;\; g(V_j) \le g(Y_j) \\ Y_j, & otherwise \end{cases} \tag{18}$$

Algorithm 2 describes IDS-based cluster head selection.

4.2 Lightweight signcryption and ODM algorithm data transmission

Some contemporary encryption approaches have proved effective. Cryptography is quicker than standard methods for computing. In sequence security relies heavily on cryptography. Cryptography is crucial for Internet devices. To find $r_1 \in \varepsilon(l)$ and satisfy the condition $tcr(r_1) = tcr(r_1^*)$ as follows:

Algorithm 2 CH selection based on IDS

Input	$: Y_{ji}$
Output	$: Y_j$
1	Initialise the parameters
2	The mutant vector is generated by $U_j = Y_j + G_j(Y_{qBest} - Y_j) + G_j(Y_{s1} - Y_{s2})$
3	Select $Y_{q\,Best}$ from the existing population
4	Represent the Cauchy distribution *Rand d*
5	Define the mean using $Mean_W(R_G) = \frac{\sum_{j=1}^{\lvert R_G \rvert} G_j^2}{\sum_{j=1}^{\lvert R_G \rvert} G_j}$
6	Update the each generation $\mu_{DS} = (1-d).\mu_{DS} + d.Mean_B(R_{DS})$
7	The fitness value is expressed as $Y_j = \begin{cases} V_j, & if\ g(V_j) \le g(Y_j) \\ Y_j, & otherwise \end{cases}$
8	End

$$S_R^{tcr}(z) = Qs\left[r_1 \leftarrow R\left(r_1^*\right) : r_1 \neq r_1^* \wedge tcr\left(r_1\right) = tcr\left(r_1^*\right)\right] \tag{19}$$

$$S_c^{kdf}(l) = \left| \underset{L_r \leftarrow L(l)}{Qs} \left[c\left(kdf(L_R)\right) = 1\right] - \underset{\left(l,l' \leftarrow \{0,1\}^{2m(l)}\right)}{Qs} \left[c\left(l,l'\right) = 1\right] \right| \tag{20}$$

Target is:

$$S_R^{mac}(l) = Qs[r_1 \neq r_1^* \wedge t = mac_d(r_1)] \tag{21}$$

Encryption is common in mobile phone data connections. Light cryptography uses little footprints and minimum computing issues. There are efforts to control cryptographic software and worldwide standards and recommendations. PRESENT encrypts data quickly.

$$L_{qa} \rightarrow \left(f_1, f_2, y, x\right) \tag{22}$$

$$L_R \rightarrow (r_1, r_2, r_3, r_4) \tag{23}$$

L_R defines lightweight:

$$L_R \leftarrow D^s c^{s\alpha} \tag{24}$$

while α implies parameter. Improve figure substance

$$Dt = (f_1^s, f_2^s, t) \ and \ L = L_R^1 \tag{25}$$

Algorithm 3 presents light weighted signcryption.

Algorithm 3 Light weighted signcryption technique

Input	:tcr, f, r, S
Output	:Dt, L
1	Initialize the value for the input parameters
2	Satisfy the condition using $tcr(r_1) = tcr(r_1^*)$.
3	Compute the target by $S_R^{mac}(l) = Qs[r_1 \neq r_1^* \wedge t = mac_d(r_1)]$
4	Apply the light-weighted by $L_R \leftarrow D^s c^{s\alpha}$
5	Evaluate the restore of the figure substance by $Dt = (f_1^s, f_2^s, t)$.
6	End.

4.2.1 Optimal decision making (ODM) algorithm path computation

Assume a phishing website discovery tool categorises N-data-point phishing example space $T = \{(X_1, y_1), (X_2, y_2), ..., (X_n, y_n)\}$ with M-attribute data points $Y_j = (y_{j1}, y_{j2}, ...y_{jM})$. Euclidean detachment between y_j and y_i points are:

$$D(Y_j, Y_j) = \sqrt{\sum_Q^M \left| y_{jq} - y_{iq} \right|}^2 \ j, i = 1, ..., N \tag{26}$$

The improved technique chose the first initial cluster centre. Existing centres are used for the remaining clusters. To be a new hub for data point clusters, the following must be true:

$$D(Y_j, center) = MAX\{D(Y_j, center_i) > 0 | center_i \in center\} \tag{27}$$

Residual data points may be assigned to matching clusters by calculating the lowest Euclidean distance to all cluster centres. The cluster data point must meet these conditions:

$$D(Y_j, center) = MIN\{D(Y_j, center_i) > 0 | center_i \in center\} \tag{28}$$

The end centre of each cluster connects the beginning cluster middle and the data point relax, where the starting point is a data point rather than the shortest distance from all other cluster points. The sample g of space T should be a proportion of class g's data points. The guinea coefficient of T is determined as

$$Guinea(T) = 1 - \sum_{j=1}^{j} q_j \tag{29}$$

Therefore, a branch node's burden increases with its data points. Gini coefficient:

$$Guinea(T, A) = \sum_{V=1}^{v} \frac{|T^v|}{T} Guinea(T^v) \tag{30}$$

Compute Gini coefficients. The optimal division feature is:

$$a_* = MIN_{a \in A}\{Guinea(T, A)\} \tag{31}$$

The F value appropriately evaluates phishing detection features.

$$F\_value = * Gini(T, a) - n_r * Gini_i - n_r * Gini)|T| \tag{32}$$

where nl and nr are information points in matching nodes; |T| be total number of information points in example space T. To discover unenthusiastic features, use the attribute variety index ρ.

$$\rho = \frac{\left|Times_{TEM} - Times_{ORI}\right|}{Acc_{TEM} - Acc_{ORI}} \tag{33}$$

When putting another attribute in the original attribute pack, DTOFANN time and accuracy are used where and when the advanced features set is used. Max function f (0, x). The neural network harvest layer is:

$$O_j = \sum_{j=1}^{h} \beta_i (z_i * Y_j + b_i) \; j = 1, 2, ...M \tag{34}$$

where $\beta_i = \beta_{i1}, \beta_{i2}, ...\beta_{ij})$ implies ith weight on linking the ith neuron hidden layer and output layer neuron units? A data point in T, assume neural network output $\widehat{x}_g = (\widehat{x}_1^g, \widehat{x}_2^g, ...\widehat{x}_l^g)$. Consequently,

$$\widehat{x}_g = f(\beta_i - B_i) \tag{35}$$

A neural network's average quadratic error may be deduced:

$$E_g = \frac{1}{2} \sum_{i=1}^{i} \left(\widehat{x}_i^g - x_i^g\right)^2 \tag{36}$$

Then, the data point's weight has become:

$$\begin{aligned} w_i &\leftarrow w_i + \Delta w_i \\ \Delta w_i &= \gamma(X_g, \hat{X}_g) Y_G \end{aligned} \tag{37}$$

Here $\gamma \in (0, 1)$. If the neural network properly predicts the data point $\left(Y_g, X_g\right)$, i.e. $X_g = \widehat{X}_g$,, it won't change. ODM was used to find the best routing between IoT sensor nodes.

5 Results and discussion

5.1 Testing scenario and parameters

In this part, we analyse QOS-AWARE ROUTING using two simulated scenarios: sensor node density and rounds.

In order to thoroughly evaluate the performance of the QoS-aware routing strategy, we conducted simulations using Network Simulation (NS2) under these two key testing scenarios, each with specific parameters.

5.1.1 Sensor node density scenario

Scenario description In the first scenario, we aimed to assess the impact of varying sensor node density on the QoS performance of our routing strategy. Different sensor node densities were simulated to observe how the network behaved under conditions of varying node density.

Parameter settings The parameters for this scenario include:

1. Varying node densities, such as low, medium, and high node density levels.
2. Fixed communication range for nodes.
3. A fixed number of data sources and destinations for consistency.
4. A predefined traffic load for data transmission.

5.1.2 Rounds scenario

Scenario description The second scenario focused on analyzing the performance of our QoS-aware routing strategy over multiple rounds or time intervals. This helps us understand the system's stability and adaptability over time.

Parameter settings The parameters for this scenario include:

1. A fixed sensor node density (chosen based on the results from the first scenario).
2. A varying number of rounds to simulate different time periods.

Table 2 Simulation setup

Parameters	Value
Network size	100×100 m^2
Number of nodes	100–500
Number of rounds	2000–10000
Antenna type	Omni
MAC protocol	IEEE 802.11
Initial energy of sensor node	1.5 J
Data packet size	4000 bits
Average energy of source node	50 nJ/bits
Average energy of destination node	50 nJ/bits
Simulation time	500 s

Table 3 Comparative analysis of proposed and existing routing techniques for set-1 parameters

No. of nodes	Energy consumption (J)						Network lifetime (s)						Delay (s)					
	T1	T2	T3	T4	T5	*P*	T1	T2	T3	T4	T5	*P*	T1	T2	T3	T4	T5	*P*
100	20	30	55	60	65	8	3978	2045	1890	1750	1650	4987	10	15	20	25	30	7
200	30	55	65	70	78	10	3500	1890	1750	1650	1479	3978	15	20	25	30	40	8
300	55	65	105	120	130	23	3218	1750	1650	1479	1238	3500	20	35	30	40	50	10
400	60	105	120	140	145	39	3179	1650	1479	1238	1148	3218	25	30	40	50	87	15
500	100	120	140	145	149	57	3009	1479	1238	1148	1123	3179	30	40	50	87	90	19

3. Dynamic traffic patterns to simulate changing data loads over rounds.
4. Fixed and variable data packet sizes.

By conducting simulations under these two scenarios with well-defined parameter settings, we can gather comprehensive data on the QoS performance of our routing strategy. This analysis provide insights into how the system responds to changes in sensor node density and adapts to dynamic network conditions over multiple rounds, thus offering a more comprehensive evaluation of its effectiveness in smart city IoT applications.

NS2 was used to simulate our experiment. QOS-AWARE ROUTING is compared against I-AREOR, LEACH-CKM, PSO-ECHS, NR-LEACH, and AREOR in terms of energy consumption, network lifespan, latency, throughput, first node dead (FND), half node dead (HND), and full node dead (FND). To test QOS-AWARE ROUTING using the following simulation setup: The network is 100×100 m2. We use 100–500 IoT feeler nodes. This test employed IEEE 802.11 MAC with an Omni antenna. Each sensor node averages 1.5 J with data packet size of 4000 bits. Table 2 outlines QOS-AWARE ROUTING's simulation setup.

5.2 Impact of node density

In 10000 rounds, 100, 200, 300, 400, and 500 sensor nodes are employed. QOS-AWARE ROUTING (P) is compared to I-AREOR (T1) [22], LEACH-CKM (T2) [25], PSO-ECHS (T3) [26], NR-LEACH (T4) [27], and AREOR (T5) [28] in Table 3. (T5). Figure 2 compares QOS-AWARE ROUTING's energy use to earlier methods. Proposed OQR-SC (QOS-AWARE ROUTING) uses 48.3%, 63.4%, 71.5%, 74.3%, and 75.8% less energy than I-AREOR, LEACH-CKM, PSO-ECHS, NR-LEACH, and AREOR.

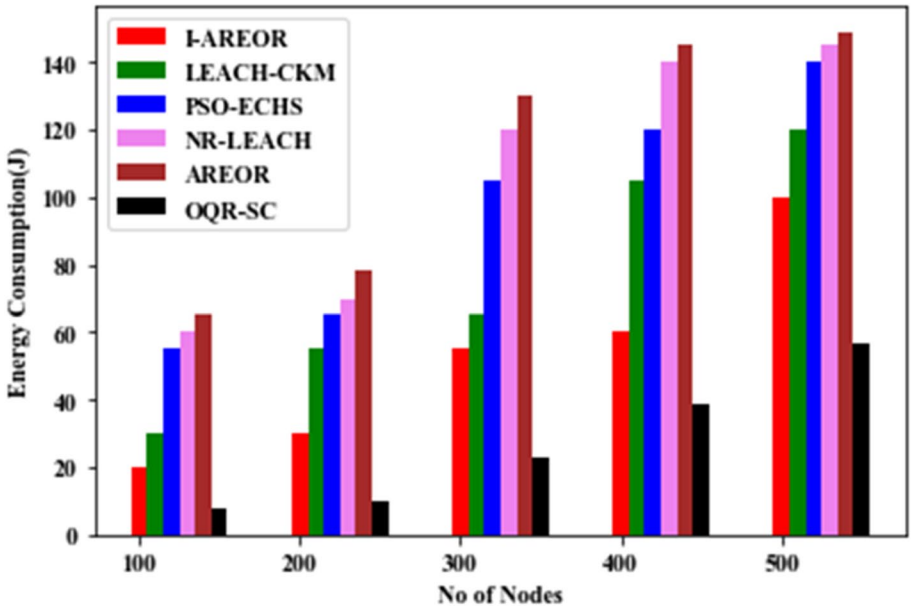

Fig. 2 Energy consumption contrast with the crash of sensor nodes

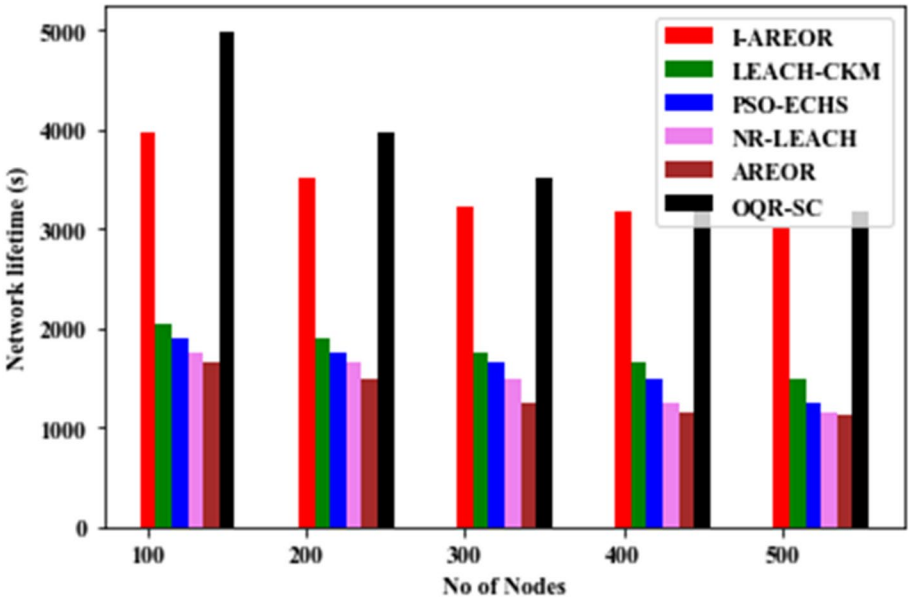

Fig. 3 Network lifetime contrast with the collision of sensor nodes

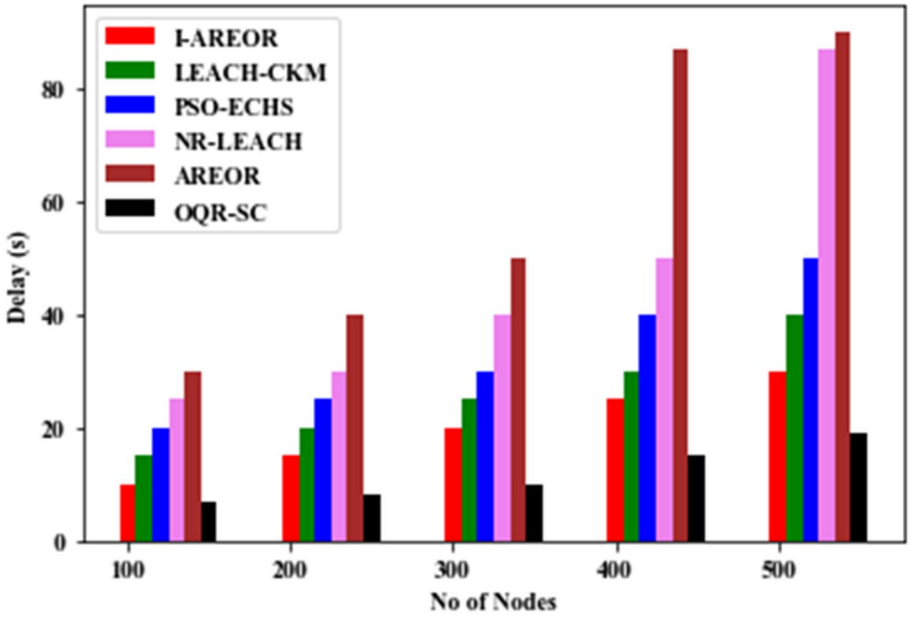

Fig. 4 Delay contrast with the impact of sensor nodes

Table 4 Comparative analysis of proposed and existing routing techniques for set-2 parameters

No. of nodes	Throughput (Mbps)						FND (s)						HND (s)					
	T1	T2	T3	T4	T5	*P*	T1	T2	T3	T4	T5	*P*	T1	T2	T3	T4	T5	*P*
100	475	452	430	410	321	500	3526	650	767	874	2460	4986	6132	767	874	900	879	7500
200	452	430	410	321	300	475	3500	620	650	767	1045	3526	4986	650	767	900	900	7412
300	430	410	321	300	250	452	3218	630	620	650	874	3000	3526	620	650	910	899	7100
400	410	321	300	250	200	430	3179	600	630	620	767	2980	3000	630	620	900	865	7089
500	321	300	250	200	145	410	3009	678	600	630	650	3000	2980	600	610	920	900	6978

Figure 3 compares QOS-AWARE ROUTING to network lifespan techniques. The graph illustrates QOS-AWARE ROUTING has a longer network lifetime than I-AREOR, LEACH-CKM, PSO-ECHS, NR-LEACH, and AREOR. Figure 4 compares QOS-AWARE ROUTING's delay to others. QOS-AWARE ROUTING's latency is 41%, 54.6%, 64.2%, 74.52%, and 80.1% less than I-AREOR, LEACH-CKM, PSO-ECHS, NR-LEACH, and AREOR.

Table 4 compares QOS-AWARE ROUTING (P) to current routing algorithms. Figure 5 compares QOS-AWARE ROUTING's throughput to the previous method. The graph reveals QOS-AWARE ROUTING consumes 7.8%, 20%, 24%, 34%, and 46% more power than I-AREOR, LEACH-CKM, PSO-ECHS, NR-LEACH, and AREOR.

Figure 6 compares QOS-AWARE ROUTING to current approaches. The figure showed QOS-AWARE ROUTING's network lifespan is 11.5%, 81.8%, 81.3%, 79.7%, and 66.8% greater than I-AREOR, LEACH-CKM, PSO-ECHS, NR-LEACH, and AREOR. Figure 7 compares QOS-AWARE ROUTING to current approaches. The graph demonstrates QOS-AWARE ROUTING's delay is 42.8%, 90.9%, 90.2%, 87.4%, and 87.6% greater than I-AREOR, LEACH-CKM, PSO-ECHS, NR-LEACH, and AREOR.

5.3 Impact of rounds

In this case, we use 2000, 4000, 6000, 8000, and 10,000 cycles with a 500 sensor node. Table 4 compares QOS-AWARE ROUTING to current approaches. Table 5 presents a comparative analysis of the proposed and existing routing techniques based on the parameters defined in set-1. Figure 8 compares QOS-AWARE ROUTING's energy use to the previous method. The graph demonstrates QOS-AWARE ROUTING uses 70.2%, 79.7%, 85.1%, 88.7%, and 90.8% less force than I-AREOR, LEACH-CKM,

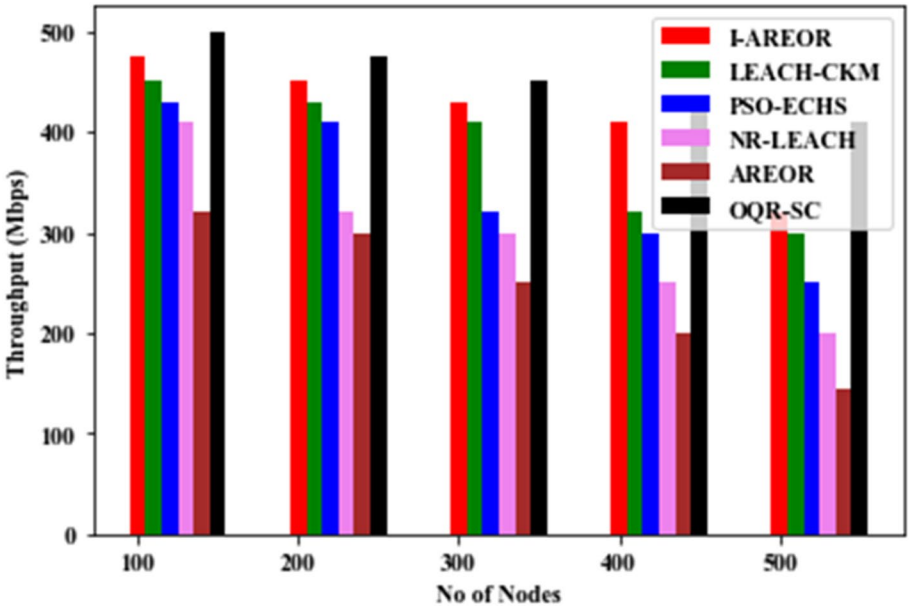

Fig. 5 Throughput contrast with the impact of sensor nodes

Table 5 Comparative analysis of proposed and existing routing techniques for set-1 parameters

No. of rounds	Energy consumption (J)						Network lifetime (s)						Delay (s)					
	T1	T2	T3	T4	T5	*P*	T1	T2	T3	T4	T5	*P*	T1	T2	T3	T4	T5	*P*
2000	25	35	59	68	190	10	3800	3500	3200	3100	3000	3978	15	20	25	30	40	10
4000	35	59	68	190	201	15	3500	3200	3100	3000	2800	3800	20	25	30	40	50	15
6000	59	68	190	201	245	20	3200	3100	3000	2800	2750	3500	25	30	40	50	87	20
8000	68	190	201	245	289	25	3100	3000	2800	2750	2641	3200	30	40	50	87	90	25
10,000	190	201	245	289	297	42	3000	2800	2750	2641	257	3100	40	50	87	90	99	30

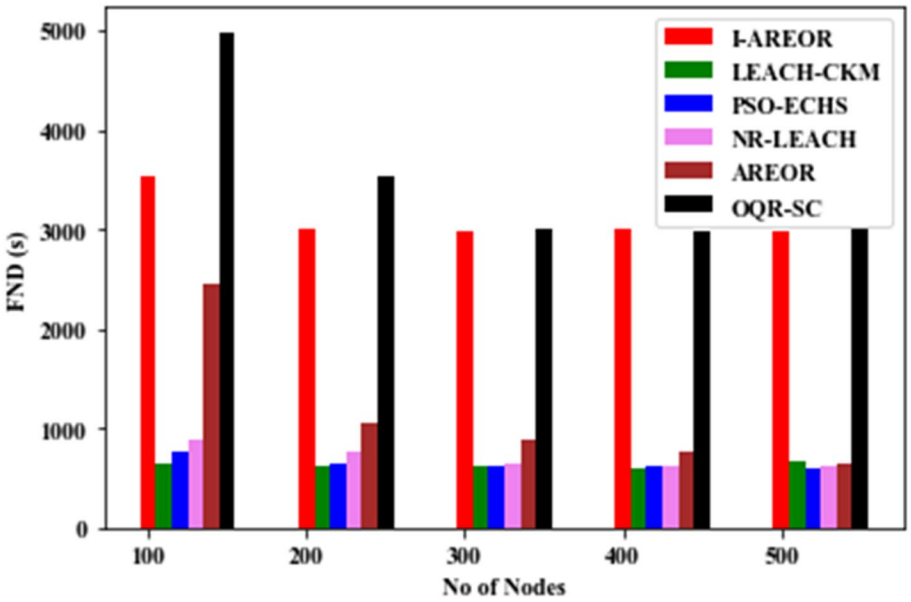

Fig. 6 FND contrast with the impact of sensor nodes

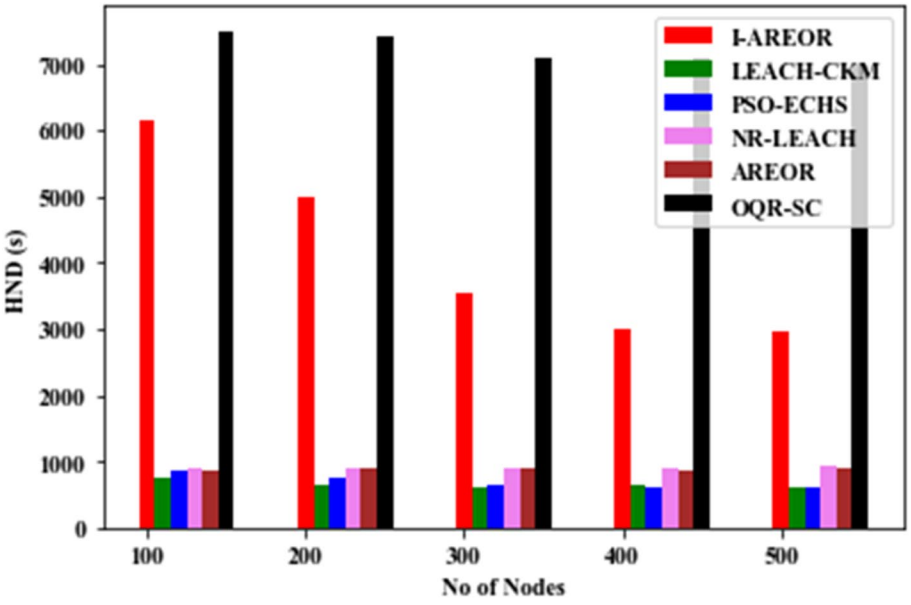

Fig. 7 HND contrast with the impact of sensor nodes

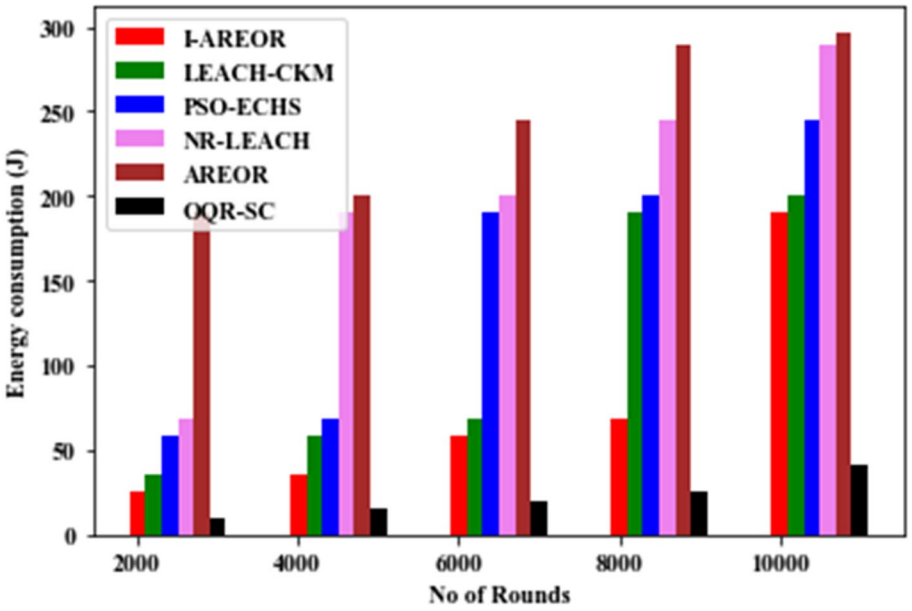

Fig. 8 Energy consumption contrast with the number of rounds

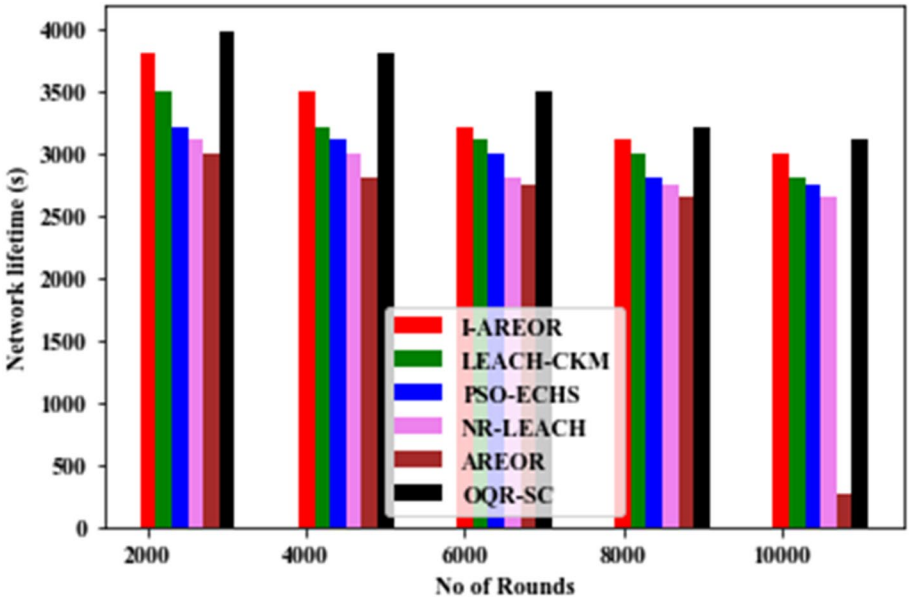

Fig. 9 Network lifetime contrast with the number of rounds

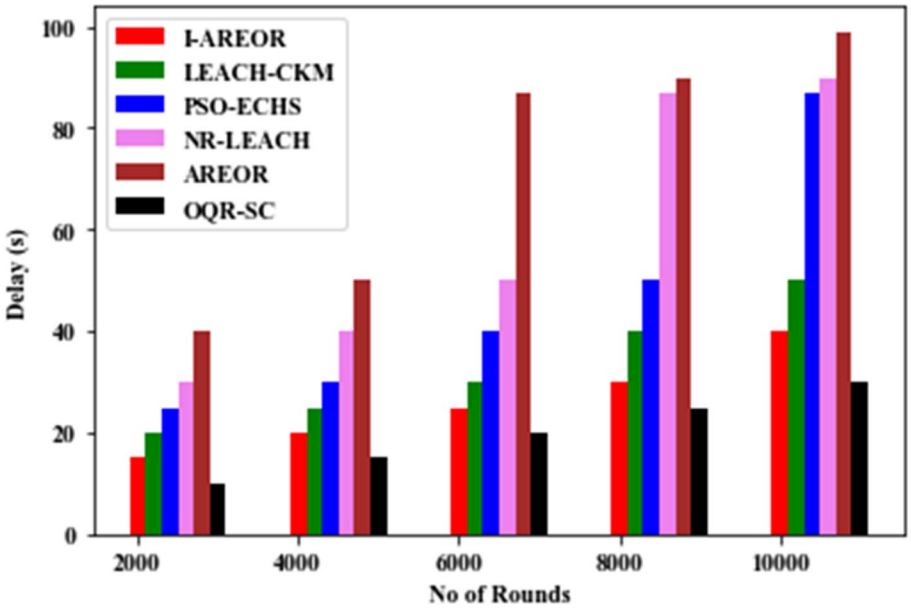

Fig. 10 Delay contrast with the number of rounds

PSO-ECHS, NR-LEACH, and AREOR. Figure 9 compares QOS-AWARE ROUTING to current strategies for network longevity. The graph reveals QOS-AWARE ROUTING increases network lifespan by 5.5%, 11.2%, 15.5%, 18.6%, and 34.8% over LEACH I-AREOR, LEACH-CKM, PSO-ECHS, NR-LEACH, and AREOR. Figure 10 compares QOS-AWARE ROUTING's delay to previous approaches. The graph reveals QOS-AWARE ROUTING has a 23%, 39.3%, 56.8%, 66.3%, and 72.6% smaller delay than I-AREOR, LEACH-CKM, PSO-ECHS, NR-LEACH, and AREOR.

Table 6 compares QoS-aware routing strategy (P) to current routing strategies. Figure 11 compares proposed QoS-aware routing to current routing. The graph reveals proposed QoS-aware routing consumes 7.8%, 15.6%, 24.5%, 28.2%, and 46.3% more power than I-AREOR, LEACH-CKM, PSO-ECHS, NR-LEACH, and AREOR.

Figure 12 compares QoS-aware routing to current approaches. The graph reveals that QoS-aware routing is 11.5%, 81.8%, 81.3%, 79.7%, and 66.8% better than I-AREOR, LEACH-CKM, PSO-ECHS, NR-LEACH, and AREOR. Figure 13 compares QoS-aware routing with current approaches. The graph reveals that QoS-aware routing is 42.8%, 90%, 90.2%, 87.4%, and 87.6% slower than I-AREOR, LEACH-CKM, PSO-ECHS, NR-LEACH, and AREOR.

Table 6 Comparative analysis of proposed and existing routing techniques for set-2 parameters

No. of nodes	FND (s)						HND (s)						FND (s)					
	T1	T2	T3	T4	T5	*P*	T1	T2	T3	T4	T5	*P*	T1	T2	T3	T4	T5	*P*
2000	475	452	430	410	321	500	3526	650	767	874	2460	4986	6132	767	874	900	920	7500
4000	452	430	410	321	300	475	3000	620	650	767	1045	3526	4986	650	767	900	900	7412
6000	430	410	321	300	250	452	2980	630	620	650	874	3000	3526	620	650	910	899	7100
8000	410	321	300	250	200	430	3000	600	630	620	767	2980	3000	630	620	900	865	7089
10,000	321	300	250	200	145	410	2971	678	600	630	650	3000	2980	600	610	920	900	6978

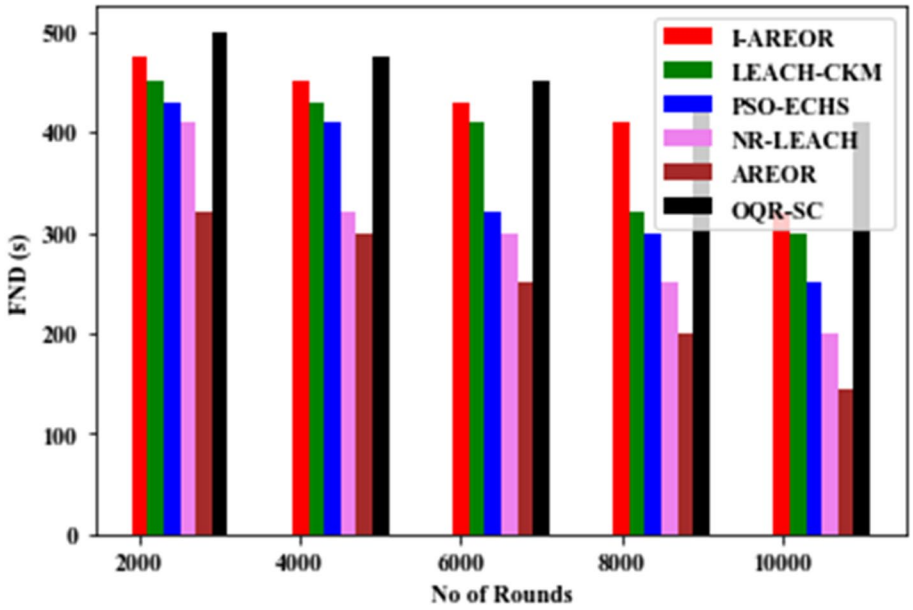

Fig. 11 FND contrast with the number of rounds

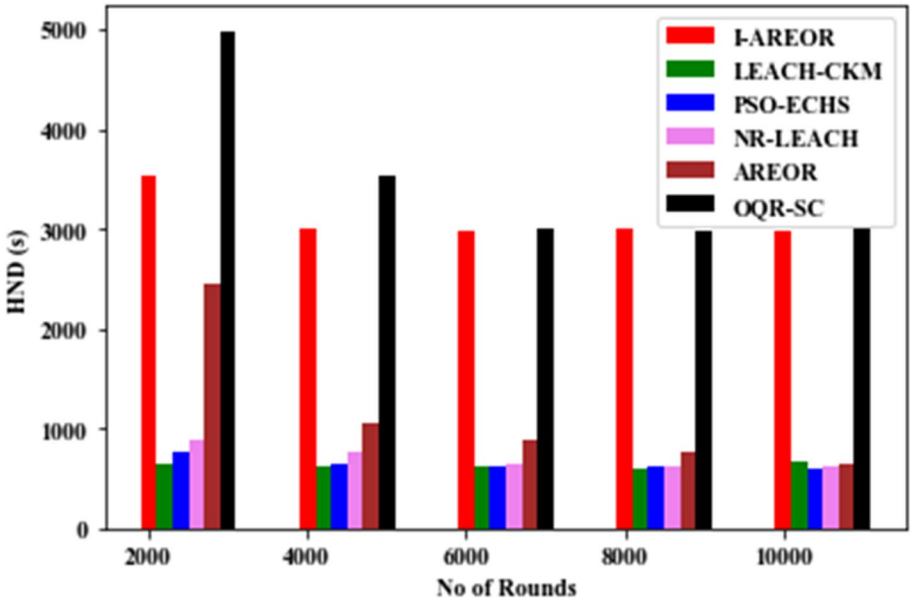

Fig. 12 HND contrast with the number of rounds

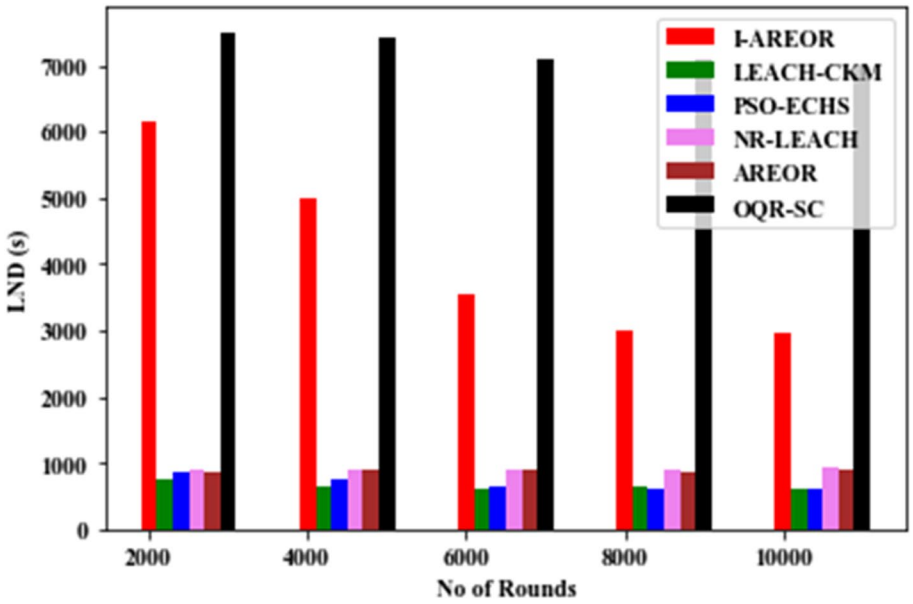

Fig. 13 LND comparison with the number of rounds

6 Conclusion

In this study, we introduced a QoS-aware routing strategy for smart cities, leveraging IoT-enabled wireless sensor networks. Our approach encompasses the use of Chaotic Bird Swarm Optimization (CBSO) for IoT sensor cluster construction, the Improved Differential Search (IDS) technique for estimating the belief degree of individual sensor nodes, and the selection of the highest trust node as the Cluster Head (CH). We further enhanced data security through lightweight signcryption for IoT sensors and optimized data routing using the Optimal Data Routing (ODM) methodology. Simulation results showcased the superior performance of QoS-aware routing across various metrics, including power consumption, grid longevity, latency, performance, FND (Future Node Density), HND (Historical Node Density), and FND.

The main findings of our study unequivocally demonstrate the excellence of the proposed QoS-aware routing strategy (QOS-AWARE ROUTING) when compared to existing routing algorithms. It exhibits remarkable advantages, including up to 90.8% less energy consumption, 66.8% longer network lifespan, and 80.1% reduced latency in both variable sensor node density and multiple-cycle scenarios.

6.1 Limitations

Despite the promising results, our study has certain limitations. We primarily conducted simulations, and real-world implementations may introduce additional complexities and challenges that require further investigation. Moreover, the proposed strategy's adaptability to diverse smart city environments and architectures needs to be explored more

comprehensively. We acknowledge that network dynamics can vary significantly in real-world scenarios, and our model should be further validated in field trials to account for these variations.

6.2 Future work

In future research, we aim to explore adaptive mechanisms to further optimize QoS-aware routing for the ever-evolving and dynamic IoT environments in smart cities. This includes investigating self-adaptive routing algorithms that can adjust to changing network conditions and traffic patterns in real-time. Additionally, we will delve into the integration of edge and fog computing concepts to enhance the overall efficiency and responsiveness of the IoT system. Furthermore, addressing scalability challenges and the potential implications of large-scale IoT deployments will be a critical focus for future work.

Data availability Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

Declarations

Conflict of interest I have no conflict of interest to declare.

References

1. Yadav A, Noori MT, Biswas A, Min B (2022) A concise review on the recent developments in the Internet of Things (IoT)-based smart aquaculture practices. Rev Fish Sci Aquac 1–16
2. Gupta S, Gupta S, Goyal D (2022) Wireless sensor network in IoT and performance optimization. Recent Adv Comput Sci Commun (Formerly: Recent Patents Comput Sci) 15(1):14–22
3. Kumar A, Akhtar MAK, Pandey A, Srivastava RP (2022) Smart city vehicle accident monitoring and detection system using (MEMS, GSM, GPS) Raspberry Pi 4. IETE J Res 1–9
4. Mori H, Kundaliya J, Naik K, Shah M (2022) IoT technologies in smart environment: security issues and future enhancements. Environ Sci Pollut Res 1–19
5. Ajagbe SA, Awotunde JB, Adesina AO, Achimugu P, Kumar TA (2022) Internet of Medical Things (IoMT): applications, challenges, and prospects in a data-driven technology. Intell Healthcare 299–319
6. Ye J, Hu Y (2022) Analysis of smart grid automation technology based on data mining algorithm. In: International conference on multi-modal information analytics. Springer, Cham, pp 1065–1070
7. William P, Badholia A, Verma V, Sharma A, Verma A (2022) Analysis of data aggregation and clustering protocol in wireless sensor networks using machine learning. In: Evolutionary computing and mobile sustainable networks. Springer, Singapore, pp 925–939
8. Sanghavi J, Jadeja D, Mehta V, Vakil A, Lalwani J, Shah M (2022) Online stream processing and multimedia-oriented IoT: tools for sustainable development of smart cities. In: Multimedia technologies in the internet of things environment, vol 3. Springer, Singapore, pp 147–166
9. Dias JP, Restivo A, Ferreira HS (2022) Designing and constructing internet-of-Things systems: An overview of the ecosystem. Internet Things 19:100529
10 Wu B, Pi Y, Chen J (2022) Privacy protection of medical service data based on blockchain and artificial intelligence in the era of smart medical care. Wirel Commun Mob Comput 2022:1
11. Zhao W, Chen J, Hai T, Mohammed MN, Yaseen ZM, Yang X, Zain JM, Zhang R, Qiang X (2022) Design of low-energy buildings in densely populated urban areas based on IoT. Energy Rep 8:4822–4833
12 Dilek S, Irgan K, Guzel Me, Ozdemir S, Baydere S, Charnsripinyo C (2022) QoS-aware IoT networks and protocols: A comprehensive survey. Int J Commun Syst 35:e5156

13 Majid M, Habib S, Javed AR, Rizwan M, Srivastava G, Gadekallu TR, Lin JC-W (2022) Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review. Sensors 22(6):2087
14 Mishra P, Kumar N, Godfrey WW (2022) An evolutionary computing-based energy-efficient solution for IoT-enabled software-defined sensor network architecture. Int J Commun Syst 35(8):e5111
15 Kumar K, Kumar A, Kumar N, Mohammed MA, Al-Waisy AS, Jaber MM, Shah R, Al-Andoli MN (2022) Dimensions of internet of things: technological taxonomy architecture applications and open challenges—a systematic review. Wirel Commun Mob Comput 2022:1
16. Quy VH, Nam VH, Linh DM, Ban NT, Han ND (2021) A survey of QoS-aware routing protocols for the MANET-WSN convergence scenarios in IoT networks. Wirel Pers Commun 120(1):49–62
17 Muthanna MS, Ali AM, Rafiq A, Hammoudeh M, Alkanhel R, Lynch S, Abd El-Latif AA (2022) Deep reinforcement learning based transmission policy enforcement and multi-hop routing in QoS aware LoRa IoT networks. Comput Commun 183:33–50
18. Fathi M, Marufuzzaman M, Buchanan RK, Rinaudo CH, Houte KM, Bian L (2021) An integrated pricing, QoS-aware sensor location model for security protection in society 5.0. IEEE Trans Eng Manag
19. Demir K (2021) A QoS-aware service discovery and selection mechanism for IoT environments. Sādhanā 46(4):1–13
20. Jaiswal K, Anand V (2021) A grey-wolf based optimized clustering approach to improve qos in wireless sensor networks for IoT applications. Peer-to-Peer Netw Appl 14(4):1943–1962
21. Wang R, Lu J (2021) QoS-aware service discovery and selection management for cloud-edge computing using a hybrid meta-heuristic algorithm in IoT. Wirel Pers Commun 1–14
22 Akhtar MDM, Ahamad D, Abdalrahman AEM, Abdalrahman AS, Ali Shatat AS, Ali Shatat AS (2022) A novel hybrid meta-heuristic concept for green communication in IoT networks: An intelligent clustering model. Int J Commun Syst 35(6):e5089
23. Avval DB, Heris PO, Navimipour NJ, Mohammadi B, Yalcin S (2022) A new QoS-aware method for production scheduling in the industrial internet of things using elephant herding optimization algorithm. Cluster Comput 1–16
24. Qin H, Chen W, Li Ni, Wang T, Chen H, Yang G, Peng Y (2023) CPS: Cross-interface network partitioning and scheduling towards QoS-aware data flow delivery in multimedia IoT. J Netw Comput Appl 217:103698
25. Kalaimani D, Zah Z, Vashist S (2021) Energy-efficient density-based fuzzy C-means clustering in WSN for smart grids. Aust J Multi-Discipl Eng 17(1):23–38
26. Badarneh HJA (2021) A coalition model for efficient indexing in wireless sensor network with random mobility. Doctoral dissertation, University of Malaya
27. Radhika M, Sivakumar P (2021) Energy optimized micro genetic algorithm based LEACH protocol for WSN. Wirel Netw 27:27–40
28. Mamatha CR, Ramakrishna M (2023) An energy efficient model for node ranking and routing path computation using optimal type-2 fuzzy logic controller