OQR-SC: An optimal QoS aware routing technique for smart cities using IoT enabled wireless sensor networks

Karunkuzhali D (✉ karunkuzhali.44@gmail.com)

Panimalar Engineering College

Meenakshi B

Sri Sairam Engineering College

Keerthi Lingam

Gitam University

Research Article

Keywords: optimal QoS aware routing technique for smart cities, Internet of things, chaotic bird swarm optimization, improved differential search, optimal decision making

Posted Date: April 23rd, 2021

DOI: <https://doi.org/10.21203/rs.3.rs-442253/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

OQR-SC: An optimal QoS aware routing technique for smart cities using IoT enabled wireless sensor networks

¹Dr.D.Karunkuzhali, ²Dr B Meenakshi, ³Keerthi Lingam

¹Professor, Department of Information Technology, Panimalar Engineering College,
Chennai,

²Department of Electrical and Electronics Engineering, Sri Sairam Engineering
College, Chennai.

³Department of Computer Science and Engineering
Gitam University, Visakhapatnam.

¹*Corresponding Author Email: karunkuzhali.44@gmail.com

Abstract

Internet of things (IoT) makes a machines optimization in everyday which processing the data by very intelligently and make communication more effectively and efficiently. However, in order to decrease the harm of IoT, nearby is angrowinglonging to move en route for green IoT which is environmentally friendly. In smart city environments, the data collection and communication play an important role in defining quality. Since the research period, it has been recommending a new data acquisition and data communication software framework for IoT smart applications. For further improvements, we recommend an optimal QoS aware routing technique for smart cities using IoT enabled wireless sensor networks (OQR-SC). In data gathering phase, we introduce chaotic bird swarm optimization (CBSO) algorithm for IoT sensor cluster formation; the improved differential search (IDS) algorithm used to estimate the faith degree of each sensor node, the highest trust node act as cluster head (CH). In data transferring phase, we illustrates lightweight signcryption technique for data encryption between two IoT sensors. Then, we use optimal decision making (ODM) algorithm to compute the optimal path between source-destination in IoT platform. Finally,

the proposed OQR-SC technique is implemented using network simulation (NS2) tool and analyzes the performance of proposed technique with existing state-of-art techniques.

Keywords: optimal QoS aware routing technique for smart cities, Internet of things, chaotic bird swarm optimization, improved differential search, optimal decision making

1. Introduction

The internet of things (IOT) that includes sensors, software, and other technologies used for transferring data to other Internet devices and systems. Although wireless sensor network (WSN) knowledge is a key constituent of IOT, it does contain antenna nodes associated to wireless channels that can offer digital interface in the real world [1]. As IOT and WSN become more realistic, their connectivity with smart devices is growing. Smart devices are integrated with sensors and embedded systems to provide advanced services, and create a smart city with IOT. IOT enabled rapid advances in wireless communication and micro electro mechanical systems (MEMS) knowledge [2] [3]. In IOT application, system nodes include communiqué capabilities that allow them to converse with extrasubstance, nodes, or individuals. Domain using IOT include smart surroundings, traffic, and monitoring [4]. In numerous IOT applications, communication can be transmitted to specific nodes via multicast transmissions. After that, the multicast source node can send the packet to multiple locations simultaneously [5]. Another example is sending traffic information to certain vehicles registered on the vehicle network. The network can have multiple nodes, making it difficult to manage nodes centrally. Therefore, dispersed multicast routing protocols are more appropriate for IOT network [6].

In general, health care providers offer a wide range of services, including cancer care military, business analysis / cloud services, operative services, emergency services, patient

monitoring services, rehabilitation services, and surgical services. In general, the provision of these services and many other services is likely to be implemented in any medical situation [7] [8]. though, the goal of this investigate paper is to offer the newly established Saskatchewan Health Authority four essential health services as a solution model for IOT [9]. Therefore, the focus services are cancer care services, business analysis/cloud services, operation services and disaster services respectively [10][11]. IOT Development has found significant application mainly in medical and multimedia applications [12]. Grid optimization has led to energy savings and the promotion of electrical safety through route performance. WSN establishes effective ways to communicate in IOT through its powerful nodes [13] [14]. IOT describes the concept of the Internet from computers, home IOT appliances, home electronics, or WSN sensor nodes. The ability to connect with other members of the WSN-IOT is beyond remote access, as multimedia models can collaborate with each other to provide a shared service [15] [16]. Smart City, IOT Special Edition focuses on a range of aspects of developments in Smart City and IOT. The IOT universal Framework Media is ubiquitous, seamlessly integrating end-to-end, well-established systems and sensors to deliver the most challenging tasks [17]. So it has happen to one of the most extensively used technologies in the digital age, making huge change in the industry, from elegant phases to integrated healthcare [18][19]. It is due to the cost of sensors and the breakdown of city management, leading to real-time data-based management of urban system, including the efficient management of water, energy, waste and transport at the city and housing levels [20]. To overcome above problems, an optimal QoS aware routing technique is proposed for smart cities using IoT enabled wireless sensor networks (OQR-SC).

The contributions of proposed OQR-SC technique are summarized as follows:

- CBSO algorithm is used for IoT sensor cluster formation; the IDS algorithm used to compute the trust degree of each sensor node, the highest trust node act as CH.

- A lightweight sign crypt ion technique for data encryption between two IoT sensors. Then, we used ODM algorithm to compute the optimal path between source-destination in IOT platform.
- Finally, the proposed OQR-SC technique implements and analyzes the performance with different simulation scenarios. The results compare with existing state-of-art techniques in conditions of QoS performance metrics.

The rest of the document is prearranged as follows: Sect. 2 describes the recent work connected to IoT for smart cities, efficient routing techniques for smart cities and clustering protocol for smart cities. Sect. 3 gives the difficulty method and system model of planned OQR-SC technique. The complete working function planned OQR-SC technique is discussed in Sect. 4 with proper mathematical model. Sect. 5 provides simulation results and comparative analysis of proposed and existing routing techniques. Lastly, the papers conclude in Sect. 6.

2. Related works

Sobral et al. [21] have planned a novel explanation to improve the presentation of Loading-IOT-Mob IOT networks. The updated version introduce a system that allows nodes to control messages and detect the presence of neighbors using a loading- IOT -mop. As a consequence, these nodes avoid narrow path and out of order paths in data packet due to node movement. Additionally, short control messages were introduced to update the node root list even at low control message frequencies. Load- IOT -Mob performance is calculated according to a number of conditions that vary depending on network size, mobile device, and terminal maximum velocity. The outcome obtain show the effectiveness of the planned explanation based on a slight increase in reminiscence utilization in provisos of pocket delivery speed, latency, power and overhead performance. Zhu et al. [22] have proposed a smart joint routing

protocol with low latency and high dependability suggests embedding a mixed connection screen. A hop delay model explores the possibilities of media access control (MAC) layer settings that support further design. Sharing, maintenance, and execution strategies are designed to develop key features of our routing protocol. Two sub-protocols are developed and the implementation steps related to them are described. Experimental results show that final and final delays can be effectively reduced through comprehensive improvement. Haseeb et al. [23] have proposed raise energy awareness using a secret sharing program to increase energy efficiency by protecting a variety of data from malicious activity, and energy-aware and secure multi-hop routing (ESMR) protocols. The procedure has three main characteristics. The network grassland is divided into internal and external zones according to the location of the node. A multiple clusters are formed in each zone based on the areas adjacent to the node. The data transmission from cluster chapters to each sync node in each zone is protected using a specific effective confidential sharing scheme. A data connection size analysis evaluates the specific solution to reduce routing difficulty. Selem et al. [24] have projected a motivating E-Health monitoring system that efficiently utilizes the concept of the Internet of Things (IoT). The wireless body area network (WBAN) includes target-based sensors that surround the human body and broadcast the composed data to the director and to certain cloud systems. The "body" sensor controls the temperature rise and affects the comfort of the skin. "THE" maintains a high level of network performance in terms of terminal longevity and high pocket performance. Gopika et al. [25] have proposed comprehensive overview of mandatory features for IOT applications using several new technologies related to energy efficient routing algorithms. The key technologies implemented, the dimensions used, and the advantages and disadvantages of existing protocols. From an energy perspective, it shows the challenges facing researchers involved in the IOT route.

Elappila et al. [26] have planned a WSN energy efficient routing equipment or existing root route. This protocol should work on high traffic networks as manifold source try to send their packet to the target at the same time, which is a common situation in IOT application for remote health monitor. To select the next hop node, the algorithm uses the criteria for the operation of three components: the signal-to-noise ratio to be disconnected, the coefficient of performance of the path from the next hop node to the target, and the next hop-level hop node. Simulation results show that the specific protocol performs best on network performance, end-to-end time, packet distribution speed, and remaining node energy levels. The packet drop rate is also low in busy landscape scenes. Conti et al. [27] have proposed a novel scheme SARP is a new and secure routing protocol for certified IOT networks. Large IOT networks with low power and low networks, SARP configured root protocol and built-in RPL features. SARP supports network functionality, device diversity, and network scaling without violating the basic requirements of IOT networks. Darabkh et al. [28] have planned protocols can be improved by considering the following suggestions: Both protocols are based on neighborhood integration and leak vibration electrical ID and practical tools to support this feature may be further explored in the future. Future studies on multicast and single transmission may be considered at the experimental detection stage. In addition, for the first two protocols to be practical, sensitivity strategies need to be more precise and sensitive, perhaps considering the sensitivity of the collaboration. The concept of protocols suggested by the MAC and PHY layers may be further explored in the future, such as SU starvation. KHAN et al. [29] have proposed a novel steering protocol for FANET with customized AntHocNet. Agents Colony optimization techniques or traditional heuristics show better reliability and performance than other traditional best road assortment technique. The energy stabilization parameter given in this study improves energy efficiency and overall phase performance. The protocol exceeds ant colony optimization (ACO) and other

traditional routing protocols used in FANET. Djedjig et al. [30] have planned a cooperation-trust-based routing algorithm for RPL. According to MRDS, in all sections of the RPL route, the child node will select the preferred parent from the more reliable, higher capacity, and better connection quality. MRTS with multi-criteria based trust as routing metric (ERNT) an effective steering idea to reduce network safety risks and preserve its functionality and stability.

3. Problem methodology and System model of proposed OQR-SC technique

Chithaluru et al. [31] have proposed energy-efficient opportunistic routing protocol (I-AREOR) based on advanced adaptive ranking based on local density, relative distance, and residual energy. first node death (FND), the half node death (HND), and last node death (LND) are major challenges in improving energy efficiency. This provides a solution to extend the FND time by considering the local density, relative distance, and residual energy of the sensor nodes. The I-AREOR protocol provides power settings based on the dynamic range of each circuit. Proven results show that I-AREOR clustering technology is more efficient in increasing network life compared to current methods. It provides solutions and enhancements for various software configurations, and provides better performance and easier communication between identified software components. These IoT domains include various IoT software configuration layers, service based, and cloud-based software configuration applications.

- The configuration of the IoT system applies to that part of the application. The Smart City model development of Smart City uses this communication platform to serve users and provide distributed resource sharing. Easy selection of hostile devices on these sites will

prevent inappropriate data transfer, data access, and transmission [21][23]. External and internal barriers must be considered to maintain uninterrupted communication.

The data collection and communication play an important role in defining quality [21]-[31]. Since the research period, it has been recommending a new data acquisition and data communication software framework for IoT smart applications. Fig. 1 shows the scheme model of proposed OQR-SC technique. The main objectives of proposed OQR-SC technique are given as follows:

1. To proposed technique is used for smart city application.
2. To study and analyze the difficulties in data collection and transfer in IoT platform.
3. To optimize routing problems and resources processed through IoT systems.
4. To study and analyze the problem for incorporate machine learning algorithms with IoT platforms.
5. To propose new optimization algorithms to enhance the different performance metrics are energy consumption, network lifetime, delay, throughput, first node dead (FND), last node dead (LND), and half node dead (HND).

Fig. 1 System model of proposed OQR-SC technique

4. Optimal QoS aware routing technique for smart cities (OQR-SC)

4.1 Data gathering phase using CBSO and IDS algorithm

4.1.1 Sensor node clustering using CBSO algorithm

Any IoT-based program must collect data from important devices and process it through various protocols. After that, you can get processed information from any place on the internet at any time. The integration of devices or sensors is called clustering. IoT data compilation is the procedure when sensors are used to determine the position of corporeal objects. plans and technologies associated through Internet of Things (IoT) can monitor and calculate data in real time. Data can be transferred, store and received at any occasion. Accordingly, cluster analysis facilitates data management by locating the data structure and classifying each object according to its nature. IoT devices can automatically connect or disconnect networks due to traffic. In fact, mobile devices are strategic tools that can understand process and create data in the real world. The collected situational information is analyzed, interpreted and used to make decisions in different areas. Here, a chaotic bird swarm optimization (CBSO) algorithm is employed here for the clustering of data in IoT sensors. For i^{th} particle of swarm population, velocity and position are represented as $fBest$ and $qBest$ respectively. The updated equation is expressed as follow:

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

$$y_{jc}^{New} = y_{jc}^{Old} + u_{jc}^{New} \quad (2)$$

Here, the random numbers with (0, 1) are denotes as s_1 and s_2 . Then, the acceleration constants are c_1 and c_2 which controls how much a particle moves in a single generation.

$$l = 0.5 + \frac{Rand}{2.0} \quad (3)$$

In the equation (3), *Rand* refer the randomly generated number with (0, 1). PSO clustering algorithm is problem location designed as multidimensional spatial data vectors. A group is a practical solution for collecting single particles of swarm. In the equation (4), the logistic map is expressed.

$$Y_{(m+1)} = b \times Y_{(m)} \times (1 - Y_{(m)}) \quad (4)$$

where $Y_{(m)}$ refers the m^{th} chaotic number and the m indicates the iteration number. Here, b=4 is used. The lines generated by the logistics map in CPSO change the random PSO parameters s_1 and s_2 . Using the logistic map these parameters are customized in the equation (5).

$$Ds_{(T+1)} = z \times ds_{(T)} \times (1 - ds_{(T)}) \quad (5)$$

For CPSO, the velocity is updated in the equation (6).

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

Ds Denote a function based on the results of a logistic diagram with values ranging from 0.0 to 1.0. All particles in the solution space are generated at individual levels and velocities. For CPSO, the pseudo code is,

$$M = z \times c \quad (7)$$

For each particle the fitness value is calculated by the fitness function. Here, z and m denotes the amount of cluster and data set respectively. For j, the cluster centre is denoted as K_j ; for i the data point is indicated as Y_i .

$$Fitness = \sum \| Y_i - K_j \|, \quad j = 1, \dots, z, i = 1, \dots, m \quad (8)$$

This is a new level of the particle. The q^{th} data vector refers the y_q . In each centre vector the amount of features is represented as c. For cluster i, the data vector subset is D_i .

$$C(y_q, k_i) = \sqrt{\sum_{j=1}^c (y_{qj} - k_{ij})^2} \quad (9)$$

$$k_i = \frac{1}{m_i} \sum_{\forall y_q \in d_i} y_q \quad (10)$$

The algorithm 1 represents the working function of the Clustering of data based on CBSO.

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

Several sensor nodes are usually used in the monitoring zone to obtain accurate information. This reduces the exact requirements for individual sensor nodes. In addition, the system is highly tolerant of many unwanted nodes, which increases the security range of the monitoring area and reduces alertness or blindness. This feature also allows using tracking data to assess trust. The trust management system is instant which is inspired by past interactions; it is the foundation of collaboration that allows many nodes to share their views on mutual trust. Using information from other sources is a challenge in today's IoT communications, where

network companies are not only essentially vulnerable, but also highly diversified and owned by a number of self-employed communities. Therefore, nodes are not required to present credible evidence; instead, threatening individuals may send false statements to specific victims in order to falsify their results. Here the improved differential search (IDS) algorithm is used to compute the belief degree of each sensor node, the highest trust node act as cluster head (CH). The main advantage of selecting the appropriate terminal cluster (CH) in the sensor network cluster is to increase the network life. Choosing a safe CH is a difficult task in terms of safety. While the trust sensor is definite and the remaining parameters are favorable, a specific clustering algorithm allows the foundation to avoid any malignant node to select CH. The selection of CHs was completed using the weight of the member nodes. The population is in certain range in initial stage. It is shown below that each person started the following method:

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

The following generates the mutant vector U_j :

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

The scale factor of Y_j is denoted by G_j ; Y_{qBest} is approximately selected from the top 100 of the existing population; the random integer is denoted by s_1 and s_2 .

The following generate G_j :

$$G_j = Rand d(\mu_G, 0.1) \quad (13)$$

Here, the Cauchy distribution is represented by $Rand d$; the value starts at 0.5 and is updated as follows:

$$\mu_G = (1 = d) \cdot \mu_G + d \cdot Mean_w(R_G) \quad (14)$$

The values between 0 and 1 are constant which is denoted by d ; the Lehmer mean function is given by $Mean_w$ as follows:

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

Using a normal distribution the crossover rate is given as:

$$V_{j,i} = \begin{cases} U_{ji}, & \text{if } Rand \leq DS_j \parallel i == i \text{ } Rand \\ Y_{ji}, & \text{otherwise} \end{cases} \quad (16)$$

μ_{DS} Is updated after each generation:

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

The arithmetic mean is denoted by $Mean_B$. In general, the strategy of choosing greed is to determine which people will survive according to their exercise values, which is expressed as follows:

$$Y_j = \begin{cases} V_j, & \text{if } g(V_j) \leq g(Y_j) \\ Y_j, & \text{otherwise} \end{cases} \quad (18)$$

The working function of cluster head selection based on IDS was described in algorithm 2.

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_{qBest} from the existing population
4	Represent the Cauchy distribution $Rand d$

5	Define the mean using $Mean_w(R_G) = \frac{\sum_{j=1}^{ R_G } G_j^2}{\sum_{j=1}^{ R_G } G_j}$
6	Update the each generation $\mu_{DS} = (1-d).\mu_{DS} + d.Mean_B(R_{DS})$
7	The fitness value is expressed as $Y_j = \begin{cases} V_j, & \text{if } g(V_j) \leq g(Y_j) \\ Y_j, & \text{otherwise} \end{cases}$
8	End

4.2 Data transferring phase using lightweight signcryption and ODM algorithm

Several methods of encryption have been proposed in recent years, some of which have been used successfully. In the case of computational processing, cryptography is considered to be faster and faster than the traditional method. Cryptography is an important communication tool in the field of in sequence security. Cryptography is essential when interacting with various devices on the Internet. To find $r_1 \in \mathcal{E}(l)$ and satisfy the condition $tc_r(r_1) = tc_r(r_1^*)$ as follows:

$$S_R^{tc_r}(z) = Qs[r_1 \leftarrow R(r_1^*) : r_1 \neq r_1^* \wedge tc_r(r_1) = tc_r(r_1^*)] \quad (19)$$

Here, $L(l) \rightarrow \{0,1\}^{2m(l)}$ with random $L \in L(l)$ is a computationally random over by $\{0,1\}^{2m(l)}$ in equation (2),

$$S_c^{kdf}(l) = | Qs_{L_r \leftarrow L(l)} [c(kdf(L_R)) = 1] - Qs_{(l,l' \leftarrow \{0,1\}^{2m(l)})} [c(l,l') = 1] | \quad (20)$$

Compute the target as follows,

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

Light cryptography is a method of encryption that involves small traces minimal computational problems. Attempts are being made to regulate cryptographic software tools and related international standards and guidelines. Encryption and decryption is commonly used on control devices that use a single key. PRESENT is a lightweight module encryption. Encryption is already used as a standard in the data connection layer of communication systems such as cell phones. Even in such cases, encryption in the application layer is useful for the final protection of data from the device to the server and for the communication system, which is different from security.

$$L_{qa} \rightarrow (f_1, f_2, y, x) \quad (22)$$

$$L_R \rightarrow (r_1, r_2, r_3, r_4) \quad (23)$$

The L_R is used to define the lightweight,

$$L_R \leftarrow D^s c^{s\alpha} \quad (24)$$

Where α represent the parameter. Finally, restore the figure substance

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

The algorithm 3 describes the working function of light weighted signcryption technique.

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.

4.2.2 Path computation using optimal decision making (ODM) algorithm

Presume the N-data-point phishing example space $T = \{(Y_1, x_1), (Y_2, x_2), \dots, (Y_n, x_n)\}$ with each M-attribute data point $Y_j = (y_{j1}, y_{j2}, \dots, y_{jM})$ and y_j be the categorization effect of y_j by a phishing website discovery tool. The Euclidean detachment among point y_j and point y_i can be formulate as

$$D(Y_j, Y_i) = \sqrt{\sum_{q=1}^M |y_{jq} - y_{iq}|^2} \quad j, i = 1, \dots, N \quad (26)$$

Using the improved method, the first initial cluster center was approximately selected. The remaining cluster centers are mainly selected from existing centers. In particular, y_j in order to be recognized as a new hub for data point clusters, the subsequent situation should to be content:

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

The residual data points can be set to the matching clusters by scheming the minimum Euclidean distance to the initial cluster center of all clusters C_j . In particular, y_j the following conditions must be met for the data point in the cluster

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

The end center of each cluster joins the starting cluster middle and the relax of the data point, where the starting point is a data point instead of the shortest distance from all other points in that cluster. The sample g of space T should be alien to the classes and q_g be a

percentage of the data points of the class g . Example defined by the guinea coefficient of the example space T is definite as

$$Gini(T) = 1 - \sum_{g=1}^g q_g \quad (29)$$

As a result, the more data points a branch node has, the higher the load. The Gini coefficient characteristic is defined as:

$$Gini(T, A) = \sum_{v=1}^v \frac{|T^v|}{|T|} Gini(T^v) \quad (30)$$

Calculate the Gini coefficients first A . After that, the optimal division characteristic a_* may be with the smallest coefficient being able to be:

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

To better appraise the value of dissimilar attributes when detecting phishing, the new worth of the attribute, the F value, is definite as follows:

$$F_value(A) = (n * Gini(T, a) - n_l * Gini_l - n_r * Gini_r) / |T| \quad (32)$$

Where n_l and n_r are the information of informationpoint in the matching nodes in that order; $|T|$ specify the total numeral of informationpoint in the example space T . The index ρ for the attributevariety is definite as follow to efficiently find unenthusiastic features:

$$\rho = \frac{|Times_{TEM} - Times_{ORI}|}{Acc_{TEM} - Acc_{ORI}} \quad (33)$$

DTOFANN time and accuracy where and when to use the advanced features set are utilized respectively; $Times_{TEM}$ and Acc_{TEM} are the time cost and correctness of the DTOFANN in that orderwhen placing another attribute in the original attribute pack.

Function distinct as $f = \max(0, x)$. The harvest layer of neural network y_j cans be representing as:

$$0_j = \sum_{j=1}^h \beta_i f(z_i * Y_j + b_i) \quad j = 1, 2, \dots, M \quad (34)$$

where $\beta_i = (\beta_{i1}, \beta_{i2}, \dots, \beta_{ij})$ is the i^{th} weight on linking the i^{th} neuron hidden layer units and output layer neuron units. A agreed data point (Y_g, X_g) in the preparation set T, presume the output of the neural network be $\hat{x}_g = (\hat{x}_1^g, \hat{x}_2^g, \dots, \hat{x}_l^g)$. The subsequent association is

$$\hat{x}_g = f(\beta_i - B_i) \quad (35)$$

The average quadratic error of a data point (Y_g, X_g) in a neural network can be calculated:

$$E_g = \frac{1}{2} \sum_{i=1}^l (\hat{x}_i^g - x_i^g)^2 \quad (36)$$

Afterward, the heaviness of the data point (Y_g, X_g) efficient as:

$$\begin{aligned} \omega_i &\leftarrow \omega_i + \Delta\omega_i \\ \Delta\omega_i &= \gamma (X_g, \hat{X}_g) \nabla G \end{aligned} \quad (37)$$

Here the study rate is $\gamma \in (0, 1)$. Therefore, if the neural network at the data point is correctly predicted data point (Y_g, X_g) , i.e. $X_g = \hat{X}_g$, the neural network will not change. Finally, ODM algorithm was used to calculate the optimal path between the sources of the IoT sensor nodes.

5. Results and Discussion

In this segment, we evaluate the presentation of planned OQR-SC method using two different simulation scenarios are impact of sensor node density and rounds. The simulation performed

using Network simulator (NS2) tool. The performance of OQR-SC technique is compared with the state-of-art existing I-AREOR, LEACH-CKM, PSO-ECHS, NR-LEACH and AREOR in terms of energy consumption, network lifetime, delay, throughput, first node dead (FND), half node dead (HND) and full node dead (FND). To verify the performance of proposed OQR-SC technique with the following simulation setup: We fix the network size as $100 \times 100 \text{ m}^2$ area. We vary the number of IoTfeeler node from 100 to 500. The IEEE 802.11 MAC protocol and Omni directional antenna used for this test. The average initial power of each sensor node is 1.5J. The data package size is 4000 bits. Table 1 summarizes the simulation setup of proposed OQR-SC technique.

Table 1 Simulation setup

Parameters	Value
Network size	$100 \times 100 \text{ m}^2$
Number of nodes	100-500
Number of rounds	2000-10000
Antenna type	Omni
MAC protocol	IEEE 802.11
Initial energy of sensor node	1.5J
Data packet size	4000bits
Average energy of source node	50 nJ/bits
Average energy of destination node	50 nJ/bits
Simulation time	500sec

5.1 Impact of node density

In this situation, we differ the number of sensor node as 100, 200, 300, 400 and 500 with the number of round as 10000. Table 2 describes the comparative analysis of proposed OQR-SC technique (P) over the existing routing techniques are I-AREOR (T1), LEACH-CKM (T2), PSO-ECHS (T3), NR-LEACH (T4) and AREOR (T5). Fig. 2 shows the energy consumption

contrast of planned OQR-SC technique over the existing techniques. The plot proved the energy consumption of planned OQR-SC method is 48.3%, 63.4%, 71.5%, 74.3% and 75.8% lower than the existing I-AREOR, LEACH-CKM, PSO-ECHS, NR-LEACH and AREOR respectively.

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

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

Table 2	Delay (s)	P	7	8	10	15	19
		T5	30	40	50	87	90

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

Fig. 3 shows the network lifetime comparison of proposed OQR-SC technique over the existing techniques. The plot proved the network lifetime of proposed OQR-SC technique is 10.4%, 53.2%, 57.5%, 61.4% and 64.8% higher than the existing I-AREOR, LEACH-CKM, PSO-ECHS, NR-LEACH and AREOR respectively. Fig. 4 shows the delay

comparison of proposed OQR-SC technique over the existing techniques. The plot proved the delay of proposed OQR-SC technique is 41%, 54.6%, 64.2%, 74.5% and 80.1% lower than the existing I-AREOR, LEACH-CKM, PSO-ECHS, NR-LEACH and AREOR respectively.

Fig. 4 Delay contrast with the impact of sensor nodes

Fig. 5 Throughput contrast with the impact of sensor nodes

Table 3 Comparative	HND (s)	P	7500	7412	7100	7089	6978
		T5	879	900	899	865	900
		T4	900	900	910	900	920
		T3	874	767	650	620	610

No. of nodes	Throughput (Mbps)						FND (s)							
	T1	T2	T3	T4	T5	P	T1	T2	T3	T4	T5	P	T1	T2
100	475	452	430	410	321	500	3526	650	767	874	2460	4986	6132	767
200	452	430	410	321	300	475	3000	620	650	767	1045	3526	4986	650
300	430	410	321	300	250	452	2980	630	620	650	874	3000	3526	620
400	410	321	300	250	200	430	3000	600	630	620	767	2980	3000	630
500	321	300	250	200	145	410	2971	678	600	630	650	3000	2980	600

Fig. 6 FND contrast with the impact of sensor nodes

Fig. 7 HND contrast with the impact of sensor nodes

Table 3 describes the comparative analysis of proposed OQR-SC technique (P) over the existing routing techniques. Fig. 5 shows the throughput contrast of planned OQR-SC technique over the existing technique. The plot proved the power consumption of planned OQR-SC technique is 7.8%, 20%, 24%, 34% and 46% higher than the existing I-AREOR, LEACH-CKM, PSO-ECHS, NR-LEACH and AREOR respectively.

Table 4	Delay (s)	P	10	15	20	25	30
		T5	40	50	87	90	99

No. of rounds	Energy consumption (J)						Network lifetime (s)									
	T1	T2	T3	T4	T5	P	T1	T2	T3	T4	T5	P	T1	T2	T3	T4
2000	25	35	59	68	190	10	3800	3500	3200	3100	3000	3978	15	20	25	30
4000	35	59	68	190	201	15	3500	3200	3100	3000	2800	3800	20	25	30	40
6000	59	68	190	201	245	20	3200	3100	3000	2800	2750	3500	25	30	40	50
8000	68	190	201	245	289	25	3100	3000	2800	2750	2641	3200	30	40	50	87
10000	190	201	245	289	297	42	3000	2800	2750	2641	257	3100	40	50	87	90

Fig. 8 Energy consumption contrast with the number of rounds

Fig. 9 Network lifetime contrast with the number of rounds

Fig. 6 shows the FND comparison of proposed QQR-SC technique over the existing techniques. The plot proved the network lifetime of proposed QQR-SC technique is 11.5%, 81.8%, 81.3%, 79.7% and 66.8% higher than the existing I-AREOR, LEACH-CKM, PSO-ECHS, NR-LEACH and AREOR respectively. Fig. 7 shows the HND comparison of proposed QQR-SC technique over the existing techniques. The plot proved the delay of proposed QQR-SC technique is 42.8%, 90.9%, 90.2%, 87.4% and 87.6% higher than the existing I-AREOR, LEACH-CKM, PSO-ECHS, NR-LEACH and AREOR respectively.

5.2 Impact of rounds

In this situation, we differ the digit of rounds as 2000, 4000, 6000, 8000 and 10,000 with the fixed sensor node as 500. Table 4 describes the comparative analysis of proposed OQR-SC technique over the existing routing techniques. Fig. 8 show the energy expenditurecontrast of planned OQR-SC technique over the existing technique. The plot proved the force consumption of planned OQR-SC method is 70.2%, 79.7%, 85.1%, 88.7% and 90.8% lower than the existing I-AREOR, LEACH-CKM, PSO-ECHS, NR-LEACH and AREOR respectively. Fig. 9 shows the network lifetime comparison of proposed OQR-SC technique over the existing techniques. The plot proved the network lifetime of proposed OQR-SC technique is 5.5%, 11.2%, 15.5%, 18.6% and 34.8% higher than the existing LEACH I-AREOR, LEACH-CKM, PSO-ECHS, NR-LEACH and AREOR respectively. Fig. 10 shows the delay comparison of proposed OQR-SC technique over the existing techniques. The plot proved the delay of proposed OQR-SC technique is 23%, 39.3%, 56.8%, 66.3% and 72.6% lower than the existing I-AREOR, LEACH-CKM, PSO-ECHS, NR-LEACH and AREOR respectively.

Fig. 10 Delay contrast with the number of rounds

Fig. 11 FND contrast with the number of rounds

Fig. 12 HND contrast with the number of rounds

Table 5 describes the comparative analysis of proposed OQR-SC technique (P) over the existing routing techniques. Fig. 11 show the FND contrast of planned OQR-SC technique over the existing technique. The plot proved the power consumption of planned OQR-SC procedure is 7.8%, 15.6%, 24.5%, 28.2% and 46.3% higher than the existing I-AREOR, LEACH-CKM, PSO-ECHS, NR-LEACH and AREOR respectively.

Table	FND	P	7500	7412	7100	7089	6978
-------	-----	---	------	------	------	------	------

No. of nodes	FND (s)						HND (s)										
	T1	T2	T3	T4	T5	P	T1	T2	T3	T4	T5	P	T1	T2	T3	T4	T5
2000	475	452	430	410	321	500	3526	650	767	874	2460	4986	6132	767	874	900	879
4000	452	430	410	321	300	475	3000	620	650	767	1045	3526	4986	650	767	900	900
6000	430	410	321	300	250	452	2980	630	620	650	874	3000	3526	620	650	910	899
8000	410	321	300	250	200	430	3000	600	630	620	767	2980	3000	630	620	900	865
10000	321	300	250	200	145	410	2971	678	600	630	650	3000	2980	600	610	920	900

Fig. 13 LND comparison with the number of rounds

Fig. 12 shows the HND comparison of proposed OQR-SC technique over the existing techniques. The plot proved the network lifetime of proposed OQR-SC technique is 11.5%, 81.8%, 81.3%, 79.7% and 66.8% higher than the existing I-AREOR, LEACH-CKM, PSO-ECHS, NR-LEACH and AREOR respectively. Fig. 13 shows the LND comparison of proposed OQR-SC technique over the existing techniques. The plot proved the delay of proposed OQR-SC technique is 42.8%, 90%, 90.2%, 87.4% and 87.6% higher than the existing I-AREOR, LEACH-CKM, PSO-ECHS, NR-LEACH and AREOR respectively.

6. Conclusion

We have proposed anbestQoS aware routing technique for smart cities using IoT enabled wireless sensor networks (OQR-SC). A chaotic bird swarm optimization (CBSO) algorithm is used for IoT sensor cluster formation; the improved differential search (IDS) algorithm used to estimate the belief degree of each sensor node, the highest trust node act as CH. A lightweight signcryption technique is used for data encryption between two IoT sensors. The optimal decision making (ODM) algorithm is used to calculate the optimal path between the source-target in the IoT operating system. Consumption Simulation results show the

performance of specific OQR-SC devices compared to current advanced technologies in terms of power consumption, grid longevity, latency, performance, FND, HND and FND.

References

1. Borah, S.J., Dhurandher, S.K., Woungang, I. and Kumar, V., 2017. A game theoretic context-based routing protocol for opportunistic networks in an IoT scenario. *Computer Networks*, 129, pp.572-584.
2. Pan, M.S. and Yang, S.W., 2017. A lightweight and distributed geographic multicast routing protocol for IoT applications. *Computer Networks*, 112, pp.95-107.
3. Fernandes, R.F. and Brandão, D., 2016. Proposal of Receiver Initiated MAC Protocol for WSN in urban environment using IoT. *IFAC-PapersOnLine*, 49(30), pp.102-107.
4. Shende, D.K. and Sonavane, S.S., 2020. CrowWhale-ETR: CrowWhale optimization algorithm for energy and trust aware multicast routing in WSN for IoT applications. *Wireless Networks*, pp.1-19.
5. Kim, T.H., Ramos, C. and Mohammed, S., 2017. Smart city and IoT.
6. Krishna, G.G., Krishna, G. and Bhalaji, N., 2016. Analysis of routing protocol for low-power and lossy networks in IoT real time applications. *Procedia Computer Science*, 87, pp.270-274.
7. Kabilan, K., Bhalaji, N., Selvaraj, C., Kumaar, M. and Karthikeyan, P.T.R., 2018. Performance analysis of IoT protocol under different mobility models. *Computers & Electrical Engineering*, 72, pp.154-168.
8. Elappila, M., Chinara, S. and Parhi, D.R., 2018. Survivable path routing in WSN for IoT applications. *Pervasive and Mobile Computing*, 43, pp.49-63.
9. Han, Z., Li, Y. and Li, J., 2018. A novel routing algorithm for IoT cloud based on hash offset tree. *Future Generation Computer Systems*, 86, pp.456-463.

10. Krishna, G.G., Krishna, G. and Bhalaji, N., 2016. Analysis of routing protocol for low-power and lossy networks in IoT real time applications. *Procedia Computer Science*, 87, pp.270-274.
11. Mujica, G., Portilla, J. and Riesgo, T., 2015. Performance evaluation of an AODV-based routing protocol implementation by using a novel in-field WSN diagnosis tool. *Microprocessors and Microsystems*, 39(8), pp.920-938.
12. Thekkil, T.M. and Prabakaran, N., 2021. Optimization Based Multi-Objective Weighted Clustering For Remote Monitoring System in WSN. *Wireless Personal Communications*, pp.1-18.
13. Jiang, W., Gu, C. and Wu, J., 2017. A quality-of-service evaluation method based on the cloud model for routing protocols in wireless sensor network. *International Journal of Distributed Sensor Networks*, 13(9), p.1550147717731247.
14. Chen, C.H., Lin, M.Y. and Guo, X.C., 2017. High-level modeling and synthesis of smart sensor networks for Industrial Internet of Things. *Computers & Electrical Engineering*, 61, pp.48-66.
15. Vigneshwari, S. and Devi, S., 2017. Fault Diagnosis in WSN Using Optimized Neighborhood Hidden Conditional Random Field. *International Journal of Modern Trends in Engineering and Science*, 4, pp.4-6.
16. Thekkil, T.M. and Prabakaran, N., 2021. Optimization Based Multi-Objective Weighted Clustering For Remote Monitoring System in WSN. *Wireless Personal Communications*, pp.1-18.
17. Sharma, M., Joshi, S., Kannan, D., Govindan, K., Singh, R. and Purohit, H.C., 2020. Internet of Things (IoT) adoption barriers of smart cities' waste management: An Indian context. *Journal of Cleaner Production*, 270, p.122047.

18. Meng, W., Li, W., Tug, S. and Tan, J., 2020. Towards blockchain-enabled single character frequency-based exclusive signature matching in IoT-assisted smart cities. *Journal of Parallel and Distributed Computing*, 144, pp.268-277.
19. Saadeh, M., Sleit, A., Sabri, K.E. and Almobaideen, W., 2018. Hierarchical architecture and protocol for mobile object authentication in the context of IoT smart cities. *Journal of Network and Computer Applications*, 121, pp.1-19.
20. Kothandaraman, D., Harshavardhan, A., Kumar, V.M., Sunitha, D. and Korra, S.N., 2021. BLE in IoT: Improved link stability and energy conservation using fuzzy approach for smart homes automation. *Materials Today: Proceedings*.
21. Sobral, J.V., Rodrigues, J.J.P., Rabêlo, R.A., Saleem, K. and Kozlov, S.A., 2019. Improving the performance of LOADng routing protocol in mobile IoT scenarios. *IEEE Access*, 7, pp.107032-107046.
22. Zhu, M., Chang, L., Wang, N. and You, I., 2020. A smart collaborative routing protocol for delay sensitive applications in industrial IoT. *IEEE Access*, 8, pp.20413-20427.
23. Haseeb, K., Islam, N., Almogren, A., Din, I.U., Almajed, H.N. and Guizani, N., 2019. Secret sharing-based energy-aware and multi-hop routing protocol for IoT based WSNs. *IEEE Access*, 7, pp.79980-79988.
24. Selem, E., Fatehy, M., Abd El-Kader, S.M. and Nassar, H., 2019. THE (temperature heterogeneity energy) aware routing protocol for IoT health application. *IEEE Access*, 7, pp.108957-108968.
25. Gopika, D. and Panjanathan, R., 2020. Energy efficient routing protocols for WSN based IoT applications: A review. *Materials Today: Proceedings*.
26. Elappila, M., Chinara, S. and Parhi, D.R., 2018. Survivable path routing in WSN for IoT applications. *Pervasive and Mobile Computing*, 43, pp.49-63.

27. Conti, M., Kaliyar, P., Rabbani, M.M. and Ranise, S., 2020. Attestation-enabled secure and scalable routing protocol for IoT networks. *Ad Hoc Networks*, 98, p.102054.
28. Darabkh, K.A., Amro, O.M., Al-Zubi, R.T. and Salameh, H.B., 2021. Yet efficient routing protocols for half-and full-duplex cognitive radio Ad-Hoc Networks over IoT environment. *Journal of Network and Computer Applications*, 173, p.102836.
29. Khan, I.U., Qureshi, I.M., Aziz, M.A., Cheema, T.A. and Shah, S.B.H., 2020. Smart IoT control-based nature inspired energy efficient routing protocol for flying ad hoc network (FANET). *IEEE Access*, 8, pp.56371-56378.
30. Djedjig, N., Tandjaoui, D., Medjek, F. and Romdhani, I., 2020. Trust-aware and cooperative routing protocol for IoT security. *Journal of Information Security and Applications*, 52, p.102467.
31. Chithaluru, P., Al-Turjman, F., Kumar, M. and Stephan, T., 2020. I-AREOR: An energy-balanced clustering protocol for implementing green IoT in smart cities. *Sustainable cities and society*, 61, p.102254.

Figures

Figure 1

System model of proposed OQR-SC technique

Figure 2

Energy consumption contrast with the crash of sensor nodes

Figure 3

Network lifetime contrast with the collision of sensor nodes

Figure 4

Delay contrast with the impact of sensor nodes

Figure 5

Throughput contrast with the impact of sensor nodes

Figure 6

FND contrast with the impact of sensor nodes

Figure 7

HND contrast with the impact of sensor nodes

Figure 8

Energy consumption contrast with the number of rounds

Figure 9

Network lifetime contrast with the number of rounds

Figure 10

Delay contrast with the number of rounds

Figure 11

FND contrast with the number of rounds

Figure 13

LND comparison with the number of rounds