Intelligent Automation & Soft Computing
DOI: 10.32604/iasc.2023.030278
Article

Tech Science Press

Secure and Energy Concise Route Revamp Technique in Wireless Sensor Networks

S. M. Udhaya Sankar[1,*], Mary Subaja Christo[2] and P. S. Uma Priyadarsini[3]

[1]Department of Information Technology, Velammal Institute of Technology, Chennai, 601204, India
[2]Department of Networking and Communication, SRM Institute of Science and Technology, Kattankulathur, 603203, India
[3]Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, 600124, India
*Corresponding Author: S. M. Udhaya Sankar. Email: udhaya3@gmail.com
Received: 22 March 2022; Accepted: 22 April 2022

Abstract: Energy conservation has become a significant consideration in wireless sensor networks (WSN). In the sensor network, the sensor nodes have internal batteries, and as a result, they expire after a certain period. As a result, expanding the life duration of sensing devices by improving data depletion in an effective and sustainable energy-efficient way remains a challenge. Also, the clustering strategy employs to enhance or extend the life cycle of WSNs. We identify the supervisory head node (SH) or cluster head (CH) in every grouping considered the feasible strategy for power-saving route discovery in the clustering model, which diminishes the communication overhead in the WSN. However, the critical issue was determining the best SH for ensuring timely communication services. Our secure and energy concise route revamp technology (SECRET) protocol involves selecting an energy-concise cluster head (ECH) and route revamping to optimize navigation. The sensors transmit information over the ECH, which delivers the information to the base station *via* the determined optimal path using our strategy for effective data transmission. We modeled our methods to accomplish power-efficient multi-hop routing. Furthermore, protected navigation helps to preserve energy when routing. The suggested solution improves energy savings, packet delivery ratio (PDR), route latency (RL), network lifetime (NL), and scalability.

Keywords: Wireless sensor network; wireless security; wireless routing; clustering; *ad hoc* network

1 Introduction

WSNs have various applications in several fields [1–3]. Batteries usually give power to the sensor. They are small and affordable devices that capture valuable data and send it across wireless networks from the source region to sink nodes. The cells in these sensing nodes, on the other hand, are not interchangeable. The link terminates due to charge degradation. These sensors can communicate with one another or with the sink directly. As a result, optimize resource allocation and node interaction to lengthen the lifespan of the channel.

Furthermore, due to the limited computational capabilities and buffer features of WSNs, various challenges exist. A selection of appropriate limitations, routing techniques to reduce the power consumption, and grouping to ensure correct network functioning are some of the multiple methods to lengthen network life [4–7]. WSN routing techniques divide into two categories: multilevel routing and flat routing. The balanced routing algorithm considers all terminals simple because they are all placed at the same tier. Furthermore, restrictions over scalability because of the overhead packet management, and as the channel capacity grows, it increases energy usage. Therefore, the system divides into clusters according to hierarchical routing. Every group has a CH node, which collects data from different nodes in the group and transmits it to the access point. As a result, extending the network duration and the energy demand in WSN is optimally balanced. When evaluating the efficiency and versatility of flat *vs.* multilevel routing protocols, hierarchical (multilevel) routing protocols stand ahead—many researchers and scientists concentrating on cluster-based routing strategies [8–10].

WSNs, on either hand, focuses primarily on how to advance energy conservation while minimizing transmission overhead expenses. Scalability, low costs, accuracy, stability, and ease of delivery are significant benefits of WSN applications over traditional network technology. However, power utilization is a unique resource in WSN circumstances considering the limited restrictions, and it must be dealt with smartly to improve network life and route navigation accuracy. Furthermore, due to the prominent dynamic properties of sensors, conventional and unicast routing techniques are not viable for sensor-based technologies [10–12]. As a result, various academics have recently focused on creating adaptive and robust routing methods to increase power consumption and locate optimal routes to destinations.

Routing strategies play an essential role in WSN since they facilitate low power dissipation, reduced latency, and high bandwidth Quality of Service (QoS). Numerous methods have been designed for application-specific WSN to address the restrictions encountered while delivering datagrams that demand node geolocation data for additional processing. It can use the data or information to calculate the gap between two nodes and even the amount of energy expended. Multi-hop routing enables the system to route outside the energy-constrained network area [13]. The latency has now decreased at the expense of increased power consumption; thus, we must devise routing strategies to concise energy.

This study aims to reduce power consumption by adopting efficient ECH selection, resulting in more extended alive nodes. We organize the remaining portions of this work as follows: The literature review summary is in Section 2, and the discussion of driving factors and research problems is in Section 3. Section 4 describes the collaborative suggested method, Section 5 shows the outcomes and inferences, and Section 5 concludes with future direction.

2 Literature Review

Shende et al. [14] overcame the difficulties by introducing an energy-aware multichannel routing mechanism relying on whale optimization algorithm (WOA) and crow search algorithm (CSA) were combined in the crow whale energy trust routing optimizer [14] depending on power and trust parameters. To determine the paths picked effectively with crow whale optimizer algorithm (CWOA), trustworthiness, and power were calculated. Chose this channel as the best for data transfer; each node's reliability and capacity are updated at the end of each transaction, ensuring that selected trustworthy nodes boost the channel's security. The investigation with 100 and 200 nodes, with and without threats, yielded the shortest latency and highest power bandwidth.

The glowworm swarming optimization model (LBR-GSO) was invented by Sampathkumar et al. [15] and proved beneficial in load balancing and navigation. This strategy combined a pseudo-random pathfinding mechanism with an improved pheromone trail-based update strategy to deal with nodes' power consumption. Furthermore, for route optimization, use feasible heuristics update strategy, including

cost-effective power measures. Finally, the LBR-GSO rendered energy-based broadcasts method decreased control overhead power usage. They examined LBR-GSO for various situations using metrics such as power consumption, power efficiency, and network throughput improvement, and it outperformed the competition.

First, utilizing the WOA by Mohan et al. [16] to select MANET's maximally protected route. Next, the trust feature and the range among nodes assess the routing's efficiency. Next, The k-disjoint path is identified, followed by optimal route analysis and interpretation of the assessed trustworthiness and range measurements. The performance indicators used to test WOA were increased power, bandwidth, and PDR. Finally, Ram et al. [17] suggested a hybrid M-Lion Whale optimizer that incorporated the lion approach and the WOA to find the optimal MANET routing plan for safe routing. Also, various QoS metrics such as range, power, lifespan, reputation, and latency examine these multiple objective approaches. In addition, designed fitness values are to find an optimal pathway with the parameters given. As a result, we attain the highest residual energy, performance, and PDR using this method.

Kumar et al. [18] developed a new exponentially ant colony optimizer (EACO) method to expose connectivity in WSNs after selecting CHs using the fractional artificial bee colony (FABC) strategy. First, CHs employed the fitness value, which takes a range, latency, and power into account. Second, to find multi-path routes, improve the ant colony optimizer (ACO) technique using an exponential smoothing prototype. Finally, EACO weighed several criteria such as power, range, and a revised fitness value to anticipate inter-cluster and intra-cluster delay to find the optimum data transmission paths from every node to BS. They also integrated the artificial bee colony (ABC) and ACO techniques to develop a new hybrid ABC-ACO system [19] that solved WSNs' non-deterministic polynomial constraints. The main functions of this approach are to select the optimal number of sub-regions, choose CH using the ABC algorithm, and effectively transfer data using the ACO strategy. Next, hierarchical clustering aids data transfer based on the cutoff. Finally, CH found the best path for transmitting data to BS using the ACO technique. This technology established a framework for wildfire detection and management. In addition, the ABCACO method increased robustness and performance.

Linear/Nonlinear Programming developed by Kuila et al. [20] created navigation methods that combined the techniques of multi-objective fitness value and particle swarm optimization (PSO). The clustering plan concentrates on load balance to conserve transmission power. By taking into account power consumption, network lifespan, dead sensor network, and packet delivery, the testing results demonstrated the superiority of this strategy.

Pachlor et al. [21] created a central routing scheme called Basestation controlled active clustering technique, which dispersed power dissipation uniformly between all nodes, conserving power and thus increasing network lifespan. Srbinovska et al. [22] proposed a stochastic optimization technique that used a genetic strategy to compute power consumption depending on transmitting duration and intensity—solely tested this optimization method in various settings, which increased in communication range. Del-Valle-Soto et al. [23] developed a power model to assess the amount of energy required by the multi-Parent hierarchical routing mechanism and other widely used communication sensors routing algorithms. Conduct experimentation with a random architecture design and two collector nodes. Different wireless systems, including Bluetooth, Zigbee, and LoRa over WiFi, are used by each node. This project met its goal of examining the efficiency of a power model constructed using multiple routing algorithms of various kinds, Behera et al. [24] focused on developing a strategy for selecting CH and rotating its positioning among nodes with the highest power. Primary and residual power and the optimum value of CH were taken into account while selecting suitable CHs for IoT systems.

3 Motivation and Problem Definition

The above study clearly shows that effective power utilization combined with secure routing is an important area of research. Many previous approaches, it has been discovered, are unable to alter routing efficiency concerning the prevailing situation and limited capabilities of WSN. Furthermore, contemporary work misses next-hop choice based on the best conclusion, and such techniques reduce network-wide performance with accuracy over routing. In addition, while data relay, routing pathways are reconstructed regularly, which adds to the effort and expense of communication. This inefficiency happens by the connection field's periodical transit of forwarding and control signals.

Furthermore, most previous work causes congestion issues and raises packet loss ratio in higher network-dense scenarios. As a result, we must explore the domain of power consumption centered on information gathering and transmission using a lightweight approach to improve network life while maintaining a consistent transmission rate. As a result, this research study proposes an energy-aware and dependable routing algorithm for heterogeneous networks that establish geographically scaled cluster centers by exploiting node positions to solve the challenges mentioned above. Furthermore, depending on a fitness value, the suggested protocol employs up-to-date neighborhood knowledge to uncover more efficient power shorter and far fewer congestion pathways over routing. Several aspects are associated with transmission power, the weighting value of Round Trip Time (RTT), and hop-count encompassed in the fitness weights. The RTT factor is vital in packet forwarding since it helps to avoid unreachable and distant companions and reduces the likelihood of repeated path re-discoveries [25]. Because the quantity of RTT changes from time to time, the suggested approach calculates a weighting factor.

Moreover, rather than flood the overall network field with route request RREQ packets to facilitate data delivery, the suggested technique sends unicast messages to a single next-hop, reducing navigation overhead expenses and power consumption. As a result, the recommended protocol enables dependable next-hop determination, which substantially affects data passing and network connectivity. In addition, overweight wireless routes, identify the nodes and restructure the routed patterns according to network connection and node capabilities to improve route lifespan and packet transmission performance [26].

4 Proposed SECRET Protocol

With WSN optimization, We designed a novel energy-concise, multi-objective safe routing strategy. The suggested SECRET method, which included the route revamping methodologies, was used to perform multi-hop navigation. We created the suggested SECRET with many aims to enable safe energy-concise multi-hop path discovery in WSN. We depict the framework of the SECRET technique in Fig. 1.

4.1 Assumptions

Specific networking characteristics are assumed in a typical network, as highlighted below.

- The network is initially homogeneity, with static nodes.
- Each node has a unique number that is arbitrary in the sensing region.
- Sensor networks are location-aware according to GPS or a positioning computation.
- Compared to regular nodes, heterogeneity nodes could have more considerable energy resources.
- The capacities and limits of all normal nodes are identical.
- Can use the receiving distance to alter the network throughput of the sensor network.
- Each CH is in charge of data aggregation.
- Sensor nodes must always communicate in a single-hop transmission.
- CHs can communicate in either a single-hop or a multi-hop fashion.

4.2 Framework of SECRET Model

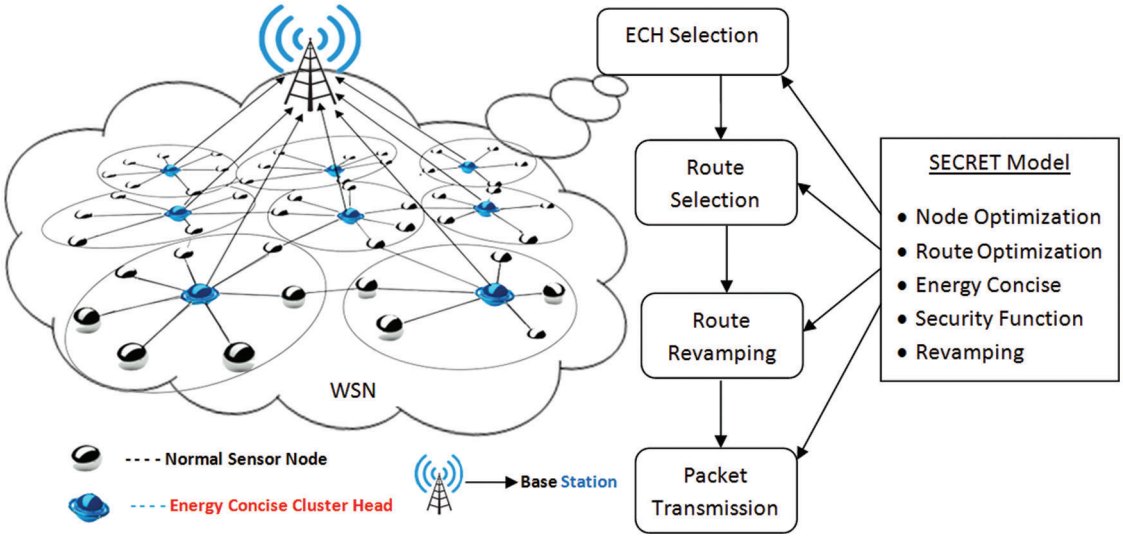

Figure 1: Framework of SECRET model

The node in the network is identified first, proceeded by cluster construction and ECH determination. Next, the suggested SECRET protocol performs multi-hop route discovery and route revamping techniques. Finally, it forwards the packets based on the SECRET protocol.

4.3 Energy Concise Cluster Head Selection

Clusters of sensor nodes form in the wireless channel, and the CH node is the node with the maximum energy efficiency (residual energy) within this cluster. The CH's task is to maintain the rest of the nodes and interact with other CHs till the data reaches the base station. The network's CHs gather, combine, and communicate data to the BS using the most efficient path. Furthermore, every active node has the potential to be a CH, rebalancing the network's total energy usage. As a result, a CH is a node with more energy (En) and the highest rating among several nodes. Thus, E_n is given by Eq. (1),

$$E_n = \frac{E_{res}}{E_{tot}} \times N_f \tag{1}$$

where E_{res} and E_{tot} denote the leftover and total power of a node, respectively, when ultimately charged. N f is the data transfer frequency of the node. Each round identifies the node violation and blocks such nodes from becoming a CH in the subsequent CH selection round since they cannot actively connect to a network. As a result, stop these compromised nodes from serving as a CH, extending the network's lifespan and improving performance.

4.4 Energy Model of SECRET Protocol

This segment describes the energy representation for the suggested SECRET technique for heterogeneous nodes. In the sensing area, arrange the nodes randomly, and n represents the proportion of heterogeneous nodes with increased power compared to regular nodes. Only chosen CHs with more energy (En) are accountable for sending sensing data to BS through a multi-hop route throughout packet transmission. The needed power for the data packet's 'S' volumes at range d_n between sender and receiver calculate using Eqs. (2) and (3) using the wireless power consumption paradigm.

$$T_{En} = \begin{cases} (P_c + (2 * d_n) \times N_f) \times S, & d_n < d_{th} \\ (P_c + 2(2 * d_n) \times N_f) \times S, & d_n > d_{th} \end{cases} \quad (2)$$

$$R_{En} = (E_n) \times S \quad (3)$$

$$\text{where, } P_c = P_n \times (T/1000) \times S \quad (4)$$

T_{En} and R_{En} represent the energy or power utilized in sending and receiving a single data bit. N_f denotes node frequency, and P_c indicates power consumption, and illustrated by Node power P_n at time T is in Eq. (3), based on distance threshold d_{th} from sender and receiver.

4.5 Fitness Function for Energy

We presented the fitness value (FCH)-based CH selection method, which also relies on the D_{nbs}, D_{nch}, starting energy of nodes (E_n), and remaining power (Eres) of the nodes (N). Because the CH must be near its neighbor nodes and BS for optimal energy usage. D_{nbs} and D_{nch} are the node's Euclidean distance (ED) from the BS and its Cluster head CH, correspondingly, and can be written as follows:

$$D_{nbs} = ED(N, BS) \quad (5)$$

$$D_{nch} = ED(N, CH) \quad (6)$$

Every ECH is chosen simultaneously among its cluster members. First, as shown in Eq. (1), the node with the best energy value in each cluster is picked as the network's ECH. Then, the F_{ECH} is used to calculate each cluster member's fitness value calculated as follows:

$$F_{ECH} = \begin{cases} \omega RE_n + (1-\omega)RD_n, & (D_{nbs} > D_{nch}) \\ RE_n, & (D_{nbs} = D_{nch}) \\ \omega RE_n + (1-\omega)RD_n, & (D_{nbs} < D_{nch}) \end{cases} \quad (7)$$

where RE_n is the ratio of the node's remaining power to its initial power, RD_n and RD'_n are the node's relative ED to the cluster head and BS, respectively.

Algorithm 1. Energy concise cluster head selection

if ($E_n = E_{th}$) **then**,
    Cluster the nodes with high energy
else
    Do not perform clustering process
end if
for opti(T_{En}, R_{En}) do
    for every E_n do
        Find the value of D_{nbs} and D_{nch}
        Find F_{ECH}
    end for
    Cluster node with peak FCH, called as $\mathbf{F_{ECH}}$
end for

4.6 Routing Revamping Fitness Function

Fitness Calculation for each link uses the fitness function to assess the route efficiency. The new fitness mechanism effectively creates a path from each gateway to the sink.

The mathematical model shows the overall distance (D) traversed by the gateways as follows:

$$T_D = \sum_{k=0}^{n} D(E_n,\ Ni(E_n)) \tag{8}$$

Total gateway hops are evaluated by

where Ni is the neighboring node, and Ni(En) is the energy of the adjacent nodes.

$$G_H = \sum_{k=0}^{n} Count(Ni(E_n)) \tag{9}$$

Consider the minimum hop count and the minimal distance covered when calculating the path. As a result, a better fitness value yields the optimized value, indicating that the variables mentioned above are inversely proportionate to fitness. Therefore, it describes the newly incorporated route revamping fitness feature as follows:

$$F_R = \frac{c1}{\alpha 1\ \times T_D \times \alpha 2 \times G_H} \tag{10}$$

where $(\alpha 1, \alpha 2) \epsilon \{0, 1\}$ such that, $\alpha 1 + \alpha 2\ = 1$ as well as c1 is the constant of proportionality. The network's maximum displacements and entire hops are well balanced.

Algorithm 2: Route revamp fitness with route selection

---

if F_{ECH} **then**,

Calculate Total Distance of Energy Node from all Other Node (T_D)

Calculate Total Gateway Hop Count (G_H)

else

Recalculate the F_{ECH}

end if

for Opti(T_D, G_H) do

for every F_{ECH} do

Find the value of F_R

end for

Node with High F_R Chosen for routing

end for

---

5 Simulation Outcomes and Analysis

The section compares previous works Taylor Based Grey Wolf Optimization Algorithm (TGWOA) [27], Reliable Cluster-based Energy-aware Routing protocol (RCER) [28] with our SECRET protocol. Using the NS2 simulator to analyze the routing performance of the SECRET protocol and various experiments relies on a node with high-density and variable network load are carried out during the evaluation. The NL, RL,

network throughput, Power saving, and PDR are all used to measure the SECRET protocol's performance. Sensor nodes are stationary and distributed at random in a square-shaped network environment. In the beginning, it assigns power levels in the range of 2j to 6j to nodes to start transmission. In addition, the nodes' broadcast range is set to 25 m to compare the proposed protocol to existing work, and the simulation time is 1500 s as mentioned in Tab. 1.

Table 1: Simulation setup

Parameter	Value
Sensor field	500 × 500 m^2
Simulation Time	1500 s
Initial energy level	2–6 Jules
Pc	50 nJ/bit
Nf	15 nJ/bit/m^2
Packet size, k	128 bits
MAC protocol	IEEE 802.15.4
Transport protocol	UDP
Channel bandwidth	10 mbps
Simulation time	1500 s
Node's transmission range	25 m
Evaluated protocols	RCER, TGWOA, and SECRET

5.1 Network Lifetime Analysis

Fig. 2 compares the network life of the SECRET protocol to that of previous techniques in a scenario with a variable node density. The SECRET approach outperforms the others, with system lifespan improvements of 12.5%, 13.2%, 15.7%, and 25%.

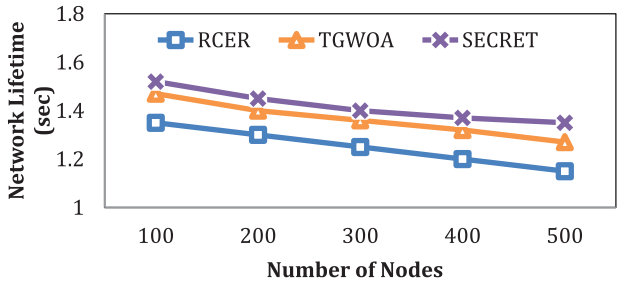

Figure 2: NL with varying number of nodes

In contrast to TGWOA and RCER, the SECRET protocol creates geographically sized groups and begins the CHs selection procedure among a small number of nodes. Furthermore, the most power effective, quickest, and select least congestion next-hops to follow data transmission. In addition, congested and remote next-hops are prevented during packet transmission, resulting in a significant increase in network lifetime for the SECRET protocol.

Fig. 3 compares the network life of SECRET with that of other existing technologies under various network load scenarios. As a result of the increased network congestion, data traffic rises, and a more significant network load on either side reduces network longevity. The SECRET technique increased network longevity by 10.26%, 10.7%, 20.54%, and 45%, respectively, over existing options. Because the position factor is taken into account when generating groups, and the location of CHs is altered based on usage than regularly, SECRET significantly saves energy usage while also prolonging network life.

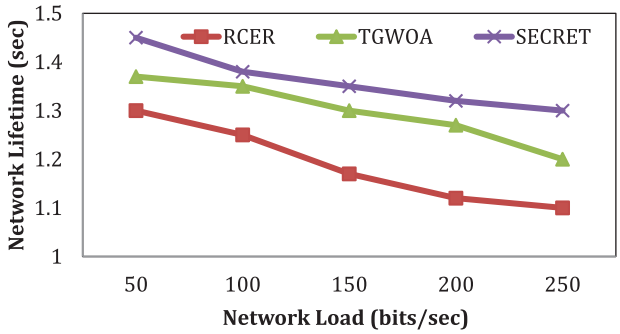

Figure 3: Network lifetime with varying network load

5.2 Energy Saving Analysis

We depict the behavior of the SECRET protocol in Fig. 4, along with a comparison of previous methods for an average power consumption model with various numbers of nodes. According to the findings, the SECRET protocol reduces network power consumption by 15.5%, 17%, 35.5%, and 50%, respectively, compared to existing systems.

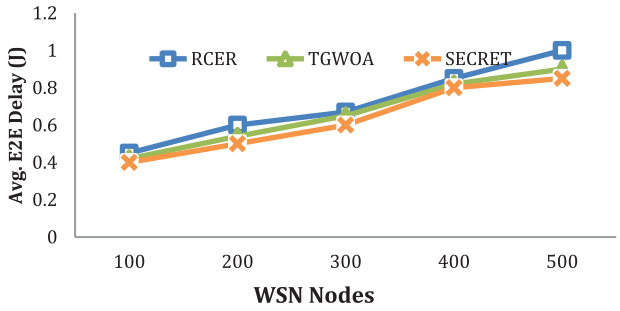

Figure 4: Energy-saving with different number of nodes

SECRET method, unlike RCER and TGWOA, eliminates communication and computation overheads by allowing CHs electing procedure to take place within limited zones. Furthermore, just a tiny network size is responsible for routing decisions, resulting in regulated power consumption.

Fig. 5 exhibits better power consumption efficiency by 25%, 35%, 45%, and 55% with varied network loads. Reduced energy usage aims to optimize network load between the next hops. Furthermore, a small number of sensor nodes participated in the voting and shifted their locations due to network measurements [29–31]. Integrating the connection latency factor into route selection also minimizes re-transmissions, resulting in much lower energy use.

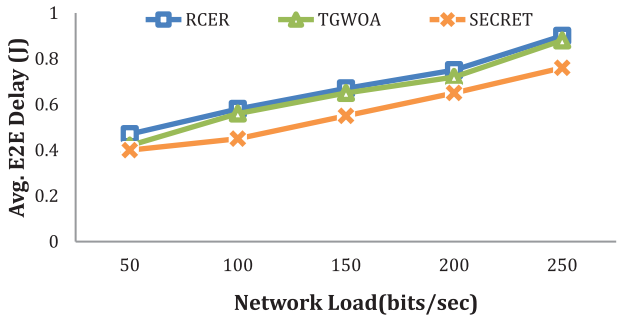

Figure 5: Energy saving with varying network load

5.3 Network Throughput Analysis

In Fig. 6, The SECRET method's performance is contrasted to prior work in terms of system throughput by taking a varied number of nodes into account. In comparison to previous systems, SECRET obtained higher network throughput by 18.5%, 24.5%, 30.5%, and 38.5%, according to simulated data. RCER and TGWOA choose next-hops based on non-optimal routing decisions, but the SECRET method chooses next-hops based on multiple criteria.

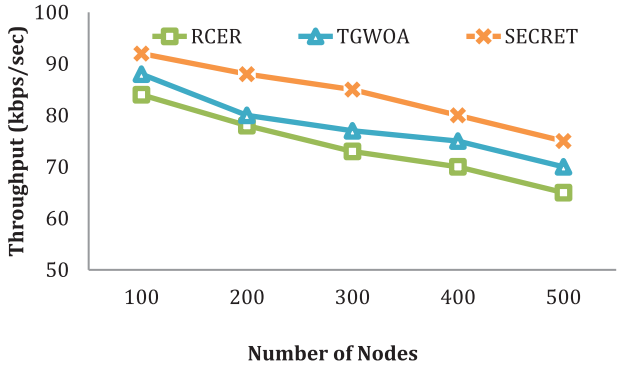

Figure 6: Throughput with different number of nodes

As a result, SECRET identifies the least trafficked, dependable, and power-efficient nodes for datagram transmission. As a result, neighbors with the fewest hop counts, the highest residual power, and the shortest RTT gives greater weight [32,33]. The SECRET protocol's route decision reduces the length of the transmission link and conserves power, but it also creates a reliable way, increasing system throughput.

In a changing network load situation, Fig. 7 compares the performance of SECRET with other alternatives in terms of network performance. In reality, a more extensive network load affects bandwidth utilization and routing reliability in high-traffic environments. Based on the findings, the SECRET method has the best data delivery performance, with improvements of 18%, 20%, 35%, and 40% over previous work. Due to multi-criterion data navigators, the next-hop location is re-formulated using network measurements. Furthermore, including connection delay in routing decisions reduces traffic load by reducing the number of re-forwardings, which substantially impacts data delivery performance.

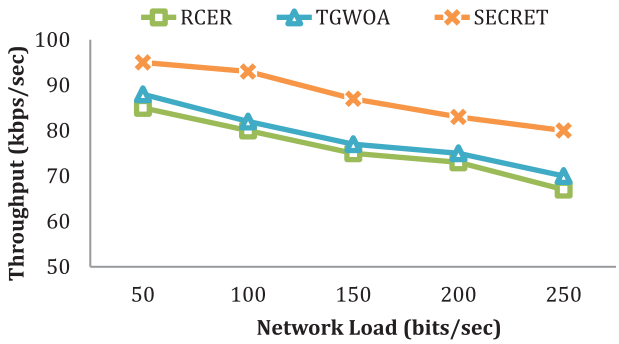

Figure 7: Throughput with varying network load

5.4 Route Lifetime Analysis

Fig. 8 shows the route lifespan compared to existing systems in a situation with a variable node density. According to the modeling results, SECRET obtains a 17% higher route lifespan than previous methods. 18%, 25%, and 37% are the percentages. SECRET's improved performance is that it incorporates node capabilities and a link latency component for routing revamp.

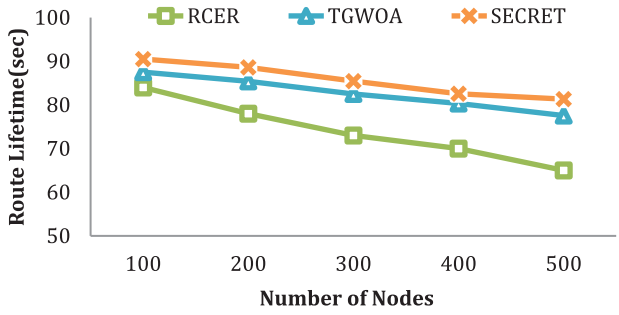

Figure 8: RL with different number of nodes

In contrast, RCER and TGWOA schemes regularly restructured routing pathways without viewing network restrictions. Furthermore, nodes with insufficient power levels have a lesser chance of being involved in routing decisions. Moreover, the multi-criteria for selecting next-hops increase the integrity of the transmission process [34–36].

From the perspective of route lifespan under fluctuating network load, Fig. 9 shows how SECRET performs better than previous systems. The computational results reveal that SECRET outperforms the opposition, with gains of 19%, 22%, 43%, and 47%. Existing techniques shortened the path lifespan due to substantial network traffic and many re-transmissions in increased network load circumstances. However, SECRET also leads to resilient navigation with a reasonably steady performance by detecting fatigued and increased latency nodes on multipath routing.

5.5 PDR Analysis

The simulation studies of SECRET with other alternatives under a variable amount of nodes situation are depicted in Fig. 10 to assess system stability. According to the results of the experiments, the SECRET method achieved a higher packet delivery than the previous method by 23.5, 25, 28, and 40 percent.

Unlike RCER and TGWOA, the SECRET method's established data transmission pathways are more trustworthy because the channel quality component considers the routing decision. Furthermore, SECRET stops energy-inefficient intermediary nodes from data forwarding, and the SECRET protocol honestly chooses the next-hop based on the multi-criteria SECRET approach [37–39].

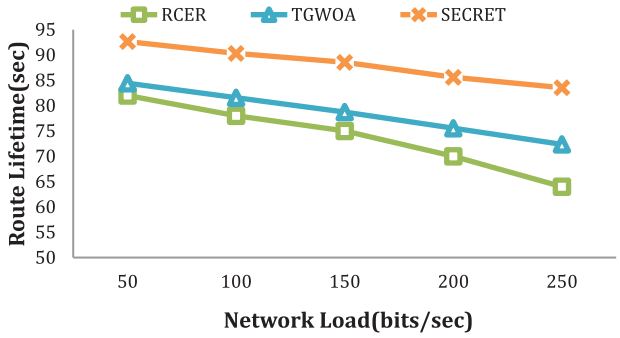

Figure 9: Route lifetime with varying network load

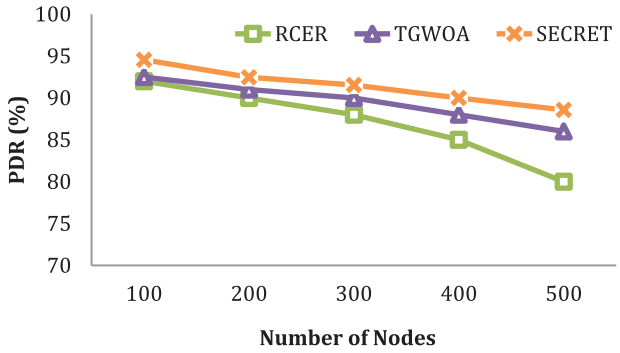

Figure 10: PDR with different number of nodes

SECRET's functionality concerning previous methods depicts in Fig. 11. The modeling tests determine the system reliability in PDR under changing network loads. Because it prioritizes those next-hops appropriate for message transmission, SECRET achieved superior reliability than current methods like 22, 25, 29, and 34 percent. In addition, due to the non-optimal selection procedure, present systems produce severe congestion issues under large network load, resulting in a low PDR. Furthermore, because SECRET regularly detects link traffic delays and faulty nodes based on response periods, overburdened nodes and connections are given the weakest weights for message transmission. As a result, the SECRET procedure has been successful in minimizing packet transmission disruptions and improving the network's performance [40,41].

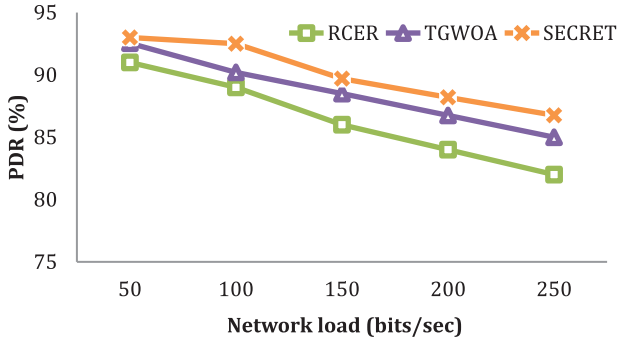

Figure 11: PDR with varying network load

6 Conclusion and Future Scope

We suggest a SECRET method for increasing the network's lifespan in this research. This technique presents a new fitness value for ECH classification. The route optimization technique relies on the nodes' residual energy, their ED from BS and the cluster head, and their relative ED. The routing protocol approach conserves energy by eliminating long distances between the transmitter and the receiver. We have proved that the SECRET outperforms other algorithms based on PDR, network lifespan, Route Lifespan, energy savings, and performance. Because more scientific studies are published annually, there would be plenty of future opportunities to suggest sophisticated meta-heuristic algorithms to improve WSN coverage and connection. The goal functions addressed here are range and latency and might include other essential restrictions to boost performance. Despite their suitability for handling the location-based sensor deployment challenge, existing algorithms affect the initiation and number of iterations. As a result, choosing the proper initialization process and convergence rate can attain the goals at low computational complexity. It is something that can research thoroughly in the future.

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

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

References

[1] M. A. Mughal, P. Shi, A. Ullah, K. Mahmood, M. Abid *et al.,* "Logical tree based secure rekeying management for smart devices groups in IoT enabled WSN," *IEEE Access*, vol. 7, pp. 76699–76711, 2019.

[2] Y. Zhang, M. Chen, D. Huang, D. Wu, Y. Li *et al.,* "Personalized and professionalized medical recommendations based on hybrid matrix factorization," *Future Generation Computer Systems*, vol. 66, no. 1, pp. 30–35, 2017.

[3] H. Zhang, J. Li, B. Wen, Y. Xun and J. Liu, "Connecting intelligent things in smart hospitals using NB-IoT," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1550–1560, 2018.

[4] H. Lee and K. Ke, "Monitoring of large-area IoT sensors using a LoRa wireless mesh network system: Design and evaluation," *IEEE Transactions on Instrumentation and Measurement*, vol. 67, no. 9, pp. 2177–2187, 2018.

[5] Y. Xiuwu, L. Qin, L. Yong, H. Mufang, Z. Ke *et al.,* "Uneven clustering routing algorithm based on glowworm swarm optimization," *Ad Hoc Networks*, vol. 93, no. 3, pp. 1–8, 2019.

[6] R. Priyadarshi, B. Gupta and A. Anurag, "Deployment techniques in wireless sensor networks: A survey, classification, challenges, and future research issues," *The Journal of Supercomputing*, vol. 76, no. 9, pp. 7333–7373, 2020.

[7] H. Ghafoor and I. Koo, "CR-SDVN: A cognitive routing protocol for software-defined vehicular networks," *IEEE Sensors Journal*, vol. 18, no. 4, pp. 1761–1772, 2018.

[8] J. Li, B. N. Silva, M. Diyan, Z. Cao and K. Han, "A clustering based routing algorithm in IoT aware wireless mesh networks," *Sustainable Cities and Society*, vol. 40, no. 1, pp. 657–666, 2018.

[9] K. Guravaiah and R. L. Velusamy, "Energy efficient clustering algorithm using RFD based multi-hop communication in wireless sensor networks," *Wireless Personal Communication*, vol. 95, no. 4, pp. 3557–3584, 2017.

[10] X. Liu and P. Zhang, "Data drainage: A novel load balancing strategy for wireless sensor networks," *IEEE Communication Letter*, vol. 22, no. 1, pp. 125–128, 2018.

[11] M. Sajwan, D. Gosain and A. K. Sharma, "Hybrid energy-efficient multi-path routing for wireless sensor networks," *Computers & Electrical Engineering*, vol. 67, no. 1, pp. 96–113, 2018.

[12] A. Panchal and R. K. Singh, "REHR: Residual energy based hybrid routing protocol for wireless sensor networks," in *IEEE Conference on Information and Communication Technology*, Allahabad, India, pp. 1–5, 2019.

[13] K. Vinoth Kumar, T. Jayasankar, V. Eswaramoorthy and V. Nivedhitha, "SDARP: Security based data aware routing protocol for ad hoc sensor networks," *International Journal of Intelligent Networks*, vol. 1, no. 1, pp. 36–42, 2020.

[14] D. K. Shende and S. S. Sonavane, "CrowWhale-ETR: CrowWhale optimization algorithm for energy and trust aware multicast routing in WSN for IoT applications," *Wireless Networks*, vol. 26, no. 6, pp. 4011–4029, 2020.

[15] A. Sampathkumar, J. Mulerikkal and M. Sivaram, "Glowworm swarm optimization for effectual load balancing and routing strategies in wireless sensor networks," *Wireless Networks*, vol. 26, no. 6, pp. 4227–4238, 2020.

[16] R. Mohan and A. V. Reddy, "T-Whale: Trust and whale optimization model for secure routing in mobile Ad-Hoc network," *International Journal of Artificial Life Research*, vol. 8, no. 2, pp. 67–79, 2018.

[17] C. Ram and A. Venugopal, "M-LionWhale: Multi-objective optimization model for secure routing in mobile Ad-hoc network," *IET Communications*, vol. 12, pp. 1–7, 2018.

[18] R. Kumar, K. Dilip and K. Dinesh, "EACO and FABC to multi-path data transmission in wireless sensor networks," *IET Communications*, vol. 11, no. 4, pp. 522–530, 2017.

[19] R. Kumar and K. Dilip, "Hybrid swarm intelligence energy efficient clustered routing algorithm for wireless sensor networks," *Journal of Sensors*, vol. 2016, pp. 1–19, 2016.

[20] P. Kuila and P. K. Jana, "Energy efficient clustering and routing algorithms for wireless sensor networks: Particle swarm optimization approach," *Engineering Applications Artificial Intelligence*, vol. 33, pp. 127–140, 2014.

[21] R. Pachlor and D. Shrimankar, "VCH-ECCR: A centralized routing protocol for wireless sensor networks," *Journal of Sensor*, vol. 2017, pp. 1–10, 2017.

[22] M. Srbinovska and M. Cundeva-Blajer, "Optimization methods for energy consumption estimation in wireless sensor networks," *Journal of Sustainable Development of Energy, Water and Environment Systems*, vol. 7, no. 2, pp. 261–274, 2019.

[23] C. Del-Valle-Soto, C. Mex-Perera, J. A. Nolazco-Flores, R. Velázquez and A. Rossa-Sierra, "Wireless sensor network energy model and its use in the optimization of routing protocols," *Energies*, vol. 13, no. 3, pp. 728, 2020.

[24] T. M. Behera, S. K. Mohapatra, U. C. Samal, M. S. Khan, M. Daneshmand *et al.,* "Residual energy-based cluster-head selection in WSNs for IoT application," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5132–5139, 2019.

[25] A. Panchal and R. K. Singh, "EADCR: Energy aware distance based cluster head selection and routing protocol for wireless sensor networks," *Journal of Circuits, Systems, and Computers*, vol. 30, no. 4, p. 2150063, 2021.

[26] S. M. M. H. Daneshvar, P. Alikhah Ahari Mohajer and S. M. Mazinani, "Energy-efficient routing in WSN: A centralized cluster-based approach via grey wolf optimizer," *IEEE Access*, vol. 7, pp. 170019–170031, 2019.

[27] R. Rahim, S. Murugan, S. Priya, S. Magesh and R. Manikandan, "Taylor based grey wolf optimization algorithm (TGWOA) for energy aware secure routing protocol," *International Journal of Computer Networks and Applications*, vol. 7, no. 4, p. 93, 2020.

[28] K. Haseeb, N. Abbas, M. Q. Saleem, O. E. Sheta, K. Awan *et al.,* "RCER: Reliable cluster-based energy-aware routing protocol for heterogeneous wireless sensor networks," *PLoS One*, vol. 14, no. 10, pp. 1–24, 2019.

[29] N. Partheeban, K. Sudharson and P. J. Sathish Kumar, "SPEC- serial property based encryption for cloud," *International Journal of Pharmacy & Technology*, vol. 8, no. 4, pp. 23702–23710, 2016.

[30] K. Sudharson, A. Mudassar Ali and N. Partheeban, "NUITECH – natural user interface technique formulating computer hardware," *International Journal of Pharmacy & Technology*, vol. 8, no. 4, pp. 23598–23606, 2016.

[31] D. Dhinakaran and P. M. Joe Prathap, "Ensuring privacy of data and mined results of data possessor in collaborative ARM," in *Pervasive Computing and Social Networking: Lecture Notes in Networks and Systems*. Vol. 317. Singapore: Springer, 2022.

[32] S. Arun and K. Sudharson, "DEFECT: Discover and eradicate fool around node in emergency network using combinatorial techniques," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 10, pp. 1–12, 2020.

[33] K. Sudharson and V. Parthipan, " A survey on ATTACK – anti terrorism technique for adhoc using clustering and knowledge extraction," in *Advances in Computer Science and Information Technology. Computer Science and Engineering. CCSIT 2012. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*. Vol. 85. Berlin, Heidelberg: Springer, pp. 508–514, 2012.

[34] A. A. Abins, J. Katiravan and S. M. Udhaya Sankar, "Performance optimization using heuristic approach in opportunistic WSR," *Dynamic Systems and Applications*, vol. 30, no. 8, pp. 1304–1317, 2021.

[35] K. Kowshika, M. Ramakrishnan, J. Raja and S. M. Udhaya Sankar, "Energy aware detection and prevention of packet drop attack in wireless and mobile adhoc networks by packet drop battling mechanism," *International Journal of Advanced Research in Engineering and Technology*, vol. 11, no. 10, pp. 1882–1892, 2020.

[36] T. Sujithra, M. Sumathi, M. Ramakrishnan and S. M. Udhaya Sankar, "ID based adaptive-key signcryption for data security in cloud environment," *International Journal of Advanced Research in Engineering and Technology*, vol. 11, no. 4, pp. 205–220, 2020.

[37] S. M. Udhaya Sankar, V. Vijaya Chamundeeswari and K. Jeevaa, "An enhanced method to detect and prevent wormhole attach in m commerce," *Asian Journal of Information Technology*, vol. 16, no. 1, pp. 77–81, 2017.

[38] S. M. Udhaya Sankar and V. Vijaya Chamundeeswar, "JIGSPASSZLE: A novel jigsaw based password system using mouse drag dynamics," *Middle-East Journal of Scientific Research*, vol. 21, no. 11, pp. 2039–2051, 2014.

[39] S. M. Udhaya Sankar, V. Vijaya Chamundeeswari and K. Jeevaa, "Identity based attack detection and manifold adversaries localization in wireless networks," *Journal of Theoretical and Applied Information technology*, vol. 67, no. 2, pp. 513–518, 2014.

[40] W. Sun, X. Chen, X. R. Zhang, G. Z. Dai, P. S. Change *et al.,* "A multi-feature learning model with enhanced local attention for vehicle re-identification," *Computers, Materials and Continua*, vol. 69, no. 3, pp. 3549–3561, 2021.

[41] J. Zhang, Z. Wang, Y. Zheng and G. Zhang, "Design of network cascade structure for image super-resolution," *Journal of New Media*, vol. 3, no. 1, pp. 29–39, 2021.