Multi-objective CH selection with Scheduling based energy efficient secure transmission in WSN using Siamese graph convolutional Mantis Search attention network

Author : Ananth Kumar M.S., Assistant Professor, Dept. of ECE, C.M.R.Institute of Technology, Bengaluru.

Abstract

In Wireless Sensor Networks (WSNs), energy efficiency, secure data transmission, and reduced latency are critical for enhancing network lifetime and reliability. Previously several optimization algorithms were used for optimal cluster head selection, but they do not provide sufficient results and still there are challenges in secure data transmission. To overcome these challenges this work is motivated. In this manuscript, a Multi-objective CH selection with Scheduling based energy efficient secure transmission in WSN using Siamese graph convolutional Mantis Search attention network (EST-SGCMSAN) is proposed. Initially, the cluster head is selected using the novel multi-objective CH selection strategy using the Red Piranha Alpine Skiing Optimization algorithm (RPASOA), designed to minimize energy usage and reduce transmission delay. Furthermore, an advanced sleep scheduling mechanism with duty cycling is introduced, leveraging a Siamese Graph Convolutional Mantis Search Attention Network (SGCMSAN) for reliable and energy-efficient scheduling. To address the security challenges inherent in sensor nodes, which often face constraints in processing power, storage, and energy, an AES-based signature generation approach utilizing White Box Cryptography (WBC) is implemented. This method ensures secure data transmission while maintaining low computational overhead. The proposed system aims to significantly extend the network lifetime of WSNs through optimized CH selection, efficient scheduling, and robust security measures. The experimental simulations are done with the help of python platform. The results show that the introduced approach performs better than previous approaches in a number of performance measures, Higher throughput 98%, higher packet delivery ratio 0.993%, less energy consumption 0.40mJ.

Key words: Siamese graph convolutional Attention Network, AES-based signature generation, White Box Cryptography (WBC), Wireless Sensor Networks (WSNs), Mantis Search, Red Piranha Alpine Skiing Optimization algorithm.

ananthkumarms@hotmail.com

International Conference on Medical Imaging, Electronic Imaging, Information Technologies, and Sensors (MIEITS 2025), edited by Lazim Abdullah, Kamal Jadidy Aval, Samad Rashid, Proc. of SPIE Vol. 13631, 1363106
 · 0277-786X · doi: 10.1117/12.3058672

1 Introduction

The growing ubiquity of IT services offers quick accessibility to a wide range of offerings across various networks. Routing is a process of determining a path between source and destination upon request of data transmission[27]. The quality of human life has improved with the technological advancement and miniaturization of sensors[28]. The sensing field may contain obstacles of any shape and size[29]. Wireless Sensor Network (WSN) is widely used for a range of applications and is installed in various environments. WSN is made up of many sensor nodes that are constrained by their inherent energy needs[1-2]. The total amount of broadcasts a sensor is able to carry out is constrained by this restricted energy. Furthermore, communication between distant nodes is limited by radio architecture. These restrictions motivate every sensor node to carry out a collaborative communication[3-4].

The majority of the sensor nodes use power for packet sending and receiving. The sensors respond to impulses during the period of time during which they are supposed to awaken up, although they do not contribute anything to the conveyance of data[5]. The method of assigning nodes of sensors to certain circumstances is called programming[6]. The duration is divided into several activity periods. Schedule is implemented to assign the conditions for sensor nodes while conserving their electrical power[7]. Only those nodes designated for the awakening stage hear the full duty cycle[8].

But the loss of energy also happens while you listen to the information. A variety of scheduling techniques have been put out in the past to assist in WSN lifetime optimisation[9]. On the other hand, it uses the nodes' power or the amount of programmed broadcasts from the detector. When it came to organizing the sensor nodes, models used largely performed poorly[10]. Cluster-based methods are applied in many scenarios where only a handful of cluster leaders are chosen. There is no need to worry about it once it's relayed to the cluster head. Despite all of the improvements made, sensor nodes still don't perform well enough to provide the desired Quality of Service (QoS).

WSN QoS depends entirely on a number of factors, including throughput, energy consumption with delay, and so on. Although transit speed could be greater with effective route choosing, it increases when energy usage is greater. Additionally, how well throughput and energy are used affects how long sensor nodes last. Enhancing the energy consumption capabilities of sensor nodes can prolong their lifespan, hence contributing to the attainment of high throughput efficiency. Using an optimum strategy for routing and regulating sensor networks that are wireless can help increase energy efficiency and network longevity because of the energy limits of the sensor nodes in these networks.

Clustering is one of the most common methods for energy conservation in sensor networks that are wireless. For optimal clustering, nevertheless, selecting an energy-efficient group head is essential. Inadequate cluster head selection (CHs) consumes more energy than additional sensor nodes since information packets need to be sent between cluster members and the sink node. It thus reduces the network's longevity and effectiveness, because private communication must be ensured by this network implementing the necessary security procedures.

Wireless Sensor Networks (WSNs) play a crucial role in various applications, including environmental monitoring, healthcare, and industrial automation, where numerous sensor nodes collaborate to collect and transmit data wirelessly. While transmitting the data several challenges are noted such as less efficiency, reliability, security, network life time with high energy consumption, delay. To overcome these issues this work is motivated.

Novelty and contribution

The novelty and contribution of this work is given below:

- In this manuscript, a Multi-objective CH selection with Scheduling based energy efficient secure transmission in WSN using Siamese graph convolutional Mantis Search attention network (EST-SGCMSAN) is proposed.
- The Red Piranha[11] Alpine Skiing[12] Optimization algorithm (RPASOA) is used to select the optimal cluster head in a Wireless Sensor Network by optimizing key network parameters such as energy consumption, node degree, residual energy, distance, delay, and RSSI, thereby enhancing the network's efficiency, longevity, and reliability.
- The Siamese Graph Convolutional Mantis Search Attention Network[13] (Siam-GCAN) and Mantis Search Optimization[14] are used in wireless sensor network scheduling to optimize wake-up schedules, reduce energy consumption, and ensure timely data transmission, improving network efficiency.
- Integrating AES-based signature generation with White Box Cryptography (WBC)[15] in Wireless Sensor Networks can improve data transfer efficiency while reducing processing power, storage, and energy consumption.

The outline of this novel paper is prepared as section 2 Literature reviews, section 3 proposed methodologies, section 4 results and discussion, section 5 conclusion and future work.

2. Literature Survey

Numerous investigations on lifetime maximizing with trustworthy scheduling and routing in WSN have been proposed in the literature in the past; a small number of these new studies are discussed in this part.

In 2022, Abadi, A.F.E., et al.[16] have presented a reinforcement-learning-based routing and energy-efficient control protocol for wireless sensor networks. Reinforcement Learning Based Energy Efficient Protocol (RLBEEP) was utilized in WSN to extend its useful life. RLBEEP was utilized to determine the best routing and control processes, limiting the transfer of information and streamlining the structure of nap planning.

In 2022, Wilson, A.J., et al.[17] have presented an Energy-efficient flood disaster monitoring for real-time in WSN using a group clustering approach. Screening for optimal transmission of data is done using Black Widow

optimization (BWO) with an Energy optimal Ensemble Clustering Method (EECM). To determine the best route among nodes, the BWO algorithm was applied.

In 2020, Sinde, R., et al.[18] have presented a WSN network lifespan refinement employing energy-efficient clustering and sleep scheduling based on DRL. E2S-DRL was utilized to reduce network latency and increase the lifespan of the Energy Efficient Scheduling (E2S) system. Zone-based clustering was employed for grouping. DRL algorithm was used to perform duty rotation. ACO and the FireFly Algorithm were utilized for routing.

In 2021, Jaiswal, K., et al.[19] have presented a Grey Wolf-based optimized clustering strategy to enhance Quality of Services (QoS) in WSN for Internet of Things workloads. Grey Wolf Optimizer (GWO), which enhances QoS, is used to choose the CH. Load balancing was implemented using the priority factor, giving each node an equal opportunity to become the central hub.

In 2021, Rezaeipanah, A., et al.[20] have proposed a hybrid approach with energy awareness for WSNs that uses multihop routing based on re-clustering. The Energy Aware Hybrid Approach (EAHA), a multihop routing method built around energy-aware re-cluster, was employed to extend the lifetime of the network. K-means and the Open Source Development Model Algorithm were integrated and applied to the task of clustering.

In 2021, Balasubramani, M., et al.[21] have presented an extension system that uses WSN clustering algorithms and Energy Aware Efficient Data Aggregation (EAEDA). The EAEDA with Data Rescheduling (EAEDA-DR) was used to build the clusters. The aggregation SN selection was used to combine the detected data from different sensors.

In 2022, Mehra, P.S.[22] have presented an enhancement in fuzzy unequal clustering and routing method for maintainable WSNs called E-FUCA. Using E-FUCA, adjustable dimension uneven clusters were created to address the areas of high activity and resource loop problems. The following bounce was chosen using the Fuzzy Interference System (FIS).

In 2021, Al-Otaibi, S., et al.[23] have presented a metaheuristic hybridization algorithm for dynamic cluster-based routing protocols in wireless sensor networks. Brain Storm Optimization (BSO) with Levy Distribution (LD), which chooses the CH by calculating the fitness function, was used to cluster the data in the Hybridization of the Metaheuristic Cluster Based Routing (HMBCR).

In 2023, Anitha, S, et, al.[24] have introduced an innovative method of securing networks that also extends network lifetime and uses fewer resources in the NTM-LEACH-RSA algorithm. It uses distance, confidence, and threshold value functions for cluster formation and head election. Additionally, the technique uses the RSA encryption algorithm to guarantee integrity and safeguard the transmission of information. Simulation packages outperform current algorithms in terms of effectiveness.

In 2024, Puttaswamy, C.,et, al.[25] have presented a process for strengthening wireless sensor networks' (WSNs) defences versus active assaults and performance. It suggests a two-pronged approach that consists of a lightweight encryption protocol and sophisticated cluster head choosing. The method makes use of trust index, local and global network qualifiers, and fuzzy logic to maximize the CH selection process. The solution improves energy effectiveness and dependability, while also greatly enhancing the performance of networks.

In 2024, Yuvaraja, M., et, al.[26] have introduced an innovative method for choosing cluster heads that maximizes network endurance and energy consumption by utilizing the Spider Monkey Optimised Fuzzy C-Means Algorithm (SMOFCM). By addressing sensor challenges such as processing power and storage capacity, the hybrid cryptography technique—which uses RSA, AES, and the proposed algorithm—reduces energy consumption and increases the network's lifespan and data communication speed.

In 2023, Urooj, S.,et, al.[27] have presented a cutting-edge algorithm that blends AES with ECC cryptography, generating keys using asymmetric Elliptic Curve Cryptography and encrypting and decrypting data utilizing a hybrid technique. The method can manage multiple security risks, including side-channel attacks, and resolves key transfer problems. It is also more straightforward and dependable. Table 1 shows the summary of reviewed approaches.

Table 1: Summary of reviewed approaches

References	Methods	Objectives	Limitations
[16]	RLBEEP	To determine the best routing and control processes	Organization is needed amongst the nodes
[17]	BWO-EECM	Real-time in WSN using a group clustering approach	Limited on power supply
[18]	DRL	To reduce network latency and increase the lifespan of the Energy Efficient Scheduling (E2S) system.	Opportunity of information robbery
[19]	GWO	To enhance Quality of Services (QoS) in WSN for Internet of Things	For data receiving the time is limited
[20]	EAHA	WSNs that uses multihop routing based on re-clustering	Relatively Short speed
[21]	EAEDA-DR	Allow well-organized observing	High cost

		and data gathering across numerous submissions.	
[22]	E-FUCA	To use smallest amount of sensors to exploit the network period	Low secure
[23]	BSO-LD	Dynamic cluster-based routing protocols in wireless sensor networks	Since it is intended for low-speed applications, it can't be utilized for communication at a high rate.
[24]	NTM-LEACH-RSA	Securing networks that extends network lifetime and uses fewer resources	WSN's computational and communication abilities are constrained. It is vulnerable to security risks.
[25]	c-RSA-AES	Strengthening wireless sensor networks' (WSNs) defenses versus active assaults and performance	Communication uncertainty
[26]	SMOFCM	Maximizes network endurance and energy consumption	Resulting in faulty data transfer and reception
[27]	AES- ECC	Cryptographic data security for reliable WSN	More susceptible to outside influence

Problem statement

Wireless Sensor Networks (WSNs) play a crucial role in various applications, including environmental monitoring, healthcare, and industrial automation, where numerous sensor nodes collaborate to collect and transmit data wirelessly. While transmitting the data several challenges are noted from the existing papers reviewed in[16-22], such as less efficiency, reliability, security, network life time with high energy consumption, delay. During the routing process the routing overhead occurs which may lead to loss of data packets. Since the sensor nodes hold limited battery storage there is a need to preserve the energy to increase the network lifetime. Delay in data transmission occurs due to improper routing process in WSN which leads to reduction in network lifetime. Selecting the proper CH is a major issue in WSN, improper selection of CH causes increase in energy usage and network overhead thereby affects the network lifetime. Key issues include optimizing energy consumption to extend network lifetime, developing effective cluster head selection algorithms for balanced data aggregation, ensuring reliable data transmission amidst dynamic environments, implementing robust security measures against threats, addressing scalability concerns, and integrating seamlessly with IoT and cloud platforms. By tackling these challenges through

innovative network design, advanced protocols, and efficient system architectures, this research aims to significantly improve the performance and deployment feasibility of WSNs across various application domains.

3 Proposed Methodology

In this section, a Multi-objective CH selection with Scheduling based energy efficient secure transmission in WSN using Siamese graph convolutional Mantis Search attention network (EST-SGCMSAN) is explained. Figure 1 shows the Multi-objective CH selection with Scheduling based energy efficient secure transmission in WSN using EST-SGCMSAN. Initially, the cluster head is selected using the novel multi-objective CH selection strategy using the RPASOA, designed to minimize energy usage and reduce transmission delay. Furthermore, an advanced sleep scheduling mechanism with duty cycling is introduced, leveraging a SGCMSAN for reliable and energy-efficient scheduling. To address the security challenges inherent in sensor nodes, which often face constraints in processing power, storage, and energy, an AES-based signature generation approach utilizing White Box Cryptography (WBC) is implemented. This method ensures secure data transmission while maintaining low computational overhead. The proposed system aims to significantly extend the network lifetime of WSNs through optimized CH selection, efficient scheduling, and robust security measures.

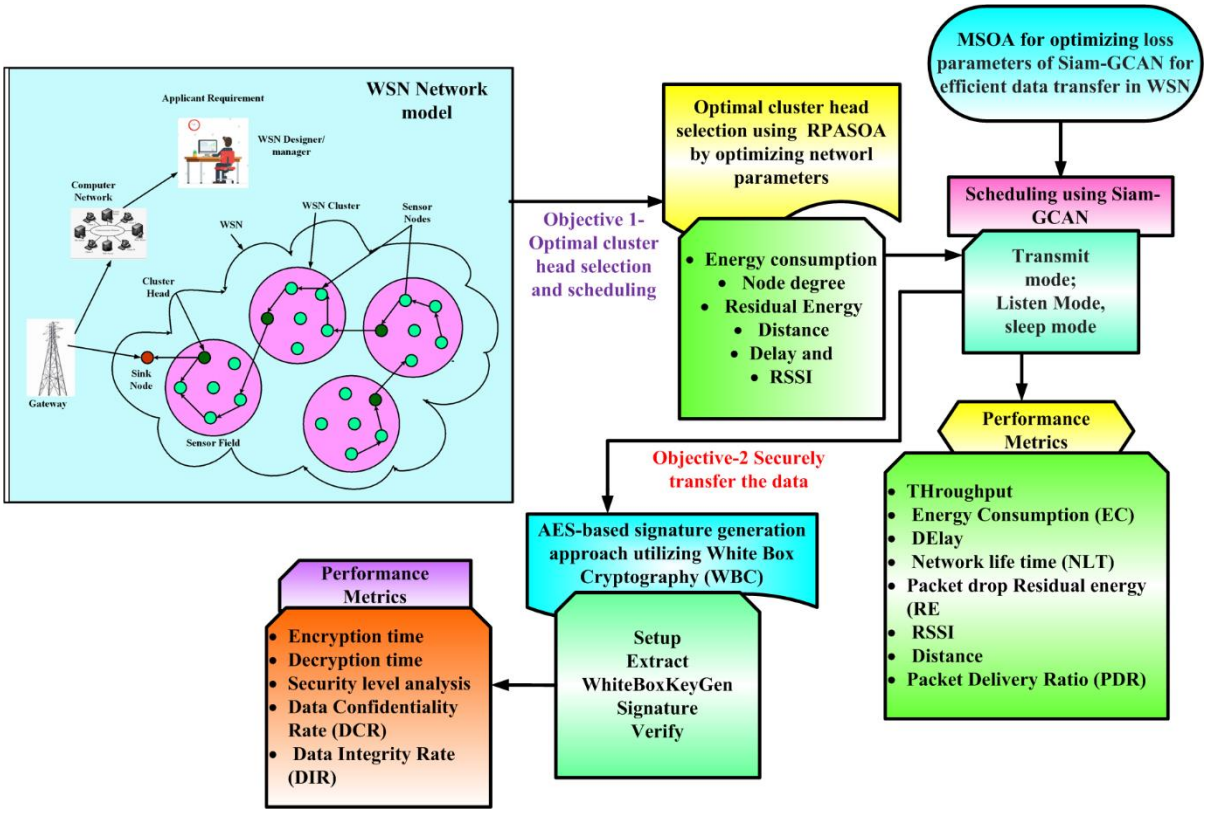

Figure 1: Work flow diagram of Multi-objective CH selection with Scheduling based energy efficient secure transmission in WSN using EST-SGCMSAN

3.1 Network model of WSN for efficient data transmission

In a Wireless Sensor Network (WSN), spatially dispersed nodes convey information gathered from monitored or controlled fields via wireless channels. Figure 2 shows the Network model. WSNs are pivotal in various applications such as pressure and light monitoring.

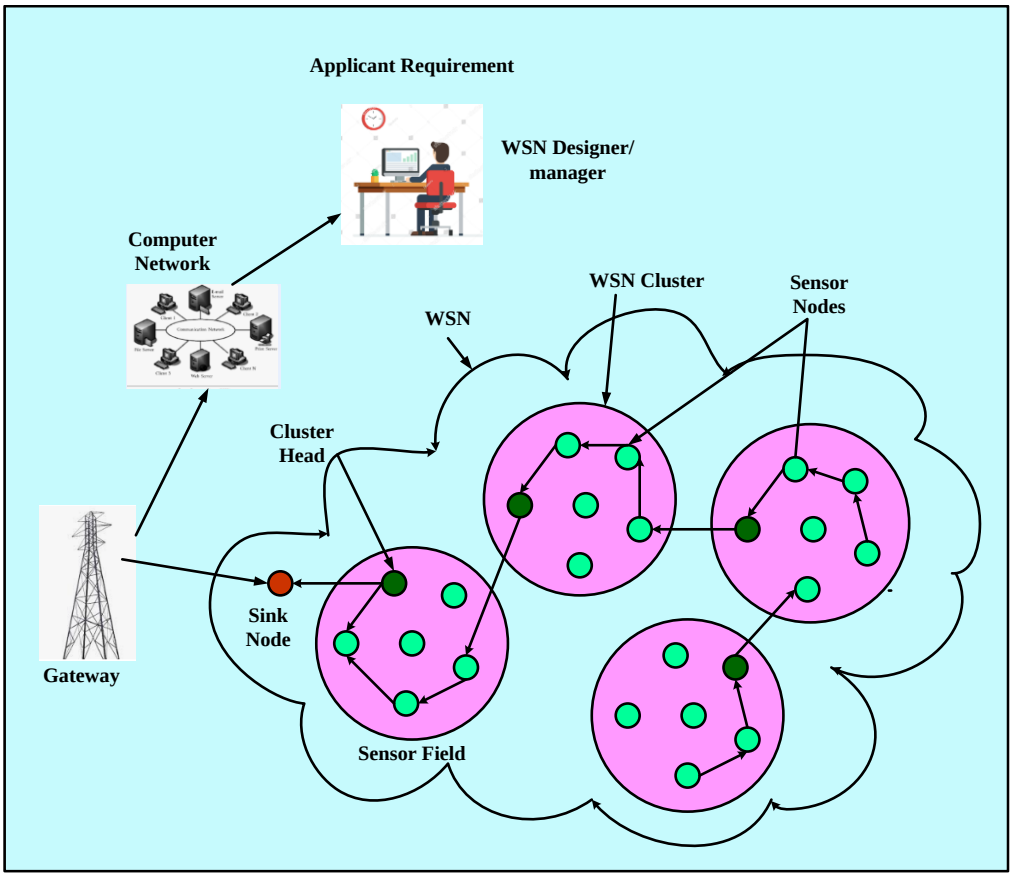

Figure 2: Network model

The network consists of diverse Sensor Nodes (SNs), denoted by X_s, which actively sense and transmit data between Base Stations (BS) and Cluster Heads (CH). Typically, SNs are distributed arbitrarily across the application area and organize into clusters, each led by a CH. The number of CHs, denoted by X_c, is predetermined, and SNs within a cluster maintain a minimal distance from their CH. SNs gather and relay data to their respective CHs, which then transmit consolidated information to the BS.

Each SN uniformly distributes data within its radio range, optimizing coverage across the network. This clustering approach facilitates efficient data aggregation and transmission, reducing energy consumption and ensuring load balancing among SNs. The selection of CHs is based on metrics such as energy efficiency, delay, and distance to

BS, security, trust, and Received Signal Strength Indication (RSSI). This Cluster Head-Based Routing (CHBR) method enhances overall network performance and longevity by minimizing data transmission overhead and operational costs.

The optimal method for selecting Cluster Heads (CHs) in a Wireless Sensor Network (WSN) prioritizes nodes with minimal energy consumption to enable efficient handling and transmission of data packets, crucial for extending network node lifespan. Alongside energy efficiency, factors like proximity to the Base Station (BS) for reduced transmission delays, robust security measures to safeguard data integrity, trustworthy node behaviour ensuring reliability, strong Received Signal Strength Indication (RSSI) for improved connectivity, and minimal transmission delay for timely data delivery are pivotal in CH selection. The BEA-SSA model, illustrated in Figure 1, organizes nodes into clusters (e.g., Cluster 1, Cluster 2, Cluster 3), each led by a CH connected directly to the BS. CHs are chosen based on comprehensive evaluation of these criteria to optimize data throughput, minimize energy consumption, and enhance overall WSN performance, ensuring reliability across diverse monitoring and control applications. The network model equations such as Energy consumption, Node degree, Residual Energy, Distance, Delay are given below:

- **Energy consumption**

In Wireless Sensor Networks (WSNs), energy efficiency is a critical concern due to the limited battery capacity of sensor nodes. The energy model proposed addresses this issue by detailing the energy consumption aspects crucial for data transmission. In this, the transmitter energy is represented as the $Tx_{Ey}(X:Dis)$, X is represented as the number of packets, Dis is represented as the distance, then the receivers energy is represented as $Rx_{Ey}(X:Dis)$, energy amplification needed for data transmission is given as Amp_{Ey}. Then the energy consumptions equations are given (1-6):

$$Tx_{Ey}(X:Dis)=Ey\begin{cases}Ey_{elEy}\times X+E_{xy}\times X\times Dis^{2}, if\ Dis<Dis_{0}\\ E_{elEy}\times X+E_{xy}\times X\times Dis^{2}, if\ Dis<Dis_{0}\end{cases} \quad (1)$$

$$E_{elEy}=Tx_{Ey}+Ey_{agr} \quad (2)$$

$$Rx_{Ey}(X:Dis)=Ey_{elEy}X \quad (3)$$

$$Amp_{Ey}=Ey_{fs}Dis^{2} \quad (4)$$

$$Dis_0 = \sqrt{\frac{Ey_{fs}}{PWAMP_{Ey}}} \quad (5)$$

$$Ey_{total}(\beta) = Tx_{Ey}(X : Dis) + Rx_{Ey}(X : Dis) + Ey_1 + Ey_{Cost} \quad (6)$$

where, $elEy$ is represented as the electric energy, agr is represented as the aggregated data, Dis_0 is represented as the threshold distance, Ey is represented as the energy, fs is represented as the requisite energy as employing free space, $PWAMP_{Ey}$ is represented as the energy in power amplifier, Ey_1 is represented as the energy for entire idle state, Ey_{Cost} is represented as the energy cost for whole sense phase.

- **Node degree**

Node degree D_{NX} is a statistic that establishes a node's maximum degree and indicates how many neighbour nodes it may connect with, which enhances network performance and its equation is given in (7):

$$D_{NX} = C_{NX}(NX_j) \quad (7)$$

Where, $C_{NX}(NX_j)$ is represented as the neighbour count of the node NX_j,

- **Residual Energy**

Residual energy (R_{Ey}), the difference between total primary and consumed energy, is used to select the highest energy node to prevent frequent sensor node death in the network and its equation is given in (8):

$$R_{Ey} = \Pr_{Ey} - C_{Ey} \quad (8)$$

Where, $\Pr_{Ey}$ is represented as the primary energy, C_{Ey} is represented as the consumed energy.

- **Distance**

The distance (Dis) parameter, known as the distance between the sensor and the sink, is directly proportional to network delay and its equation is given in (9):

$$Dis = \sqrt{((NX_{k,a} - NX_{j,a})^2 + (NX_{k,b} - NX_{j,b})^2)} \quad (9)$$

Where, $NX_{k,a}$ and $NX_{k,b}$ are represented as the position of the sink node, $NX_{j,a}$, $NX_{j,b}$ are represented as the position of the sensor node.

- **Delay**

In this, delay (D_e) refers to the time interval between the initiation of data transmission by a sensor node and a cluster of nodes and the successful reception of that data at its intended destination, such as a Base Station or another node and its equation is given in (10):

$$(D_e) = \frac{Max\left(P_{C_{NX}}^{t}\right)_{t=1}^{P_{C_{NX}}^{Ey}}}{CC} \quad (10)$$

Where, CC is represented as the cluster counts, $P_{C_{NX}}^{t}$ is represented as the delay or time taken by each cluster, $P_{C_{NX}}^{Ey}$ is represented as the total number of Cluster Heads (CHs) involved in the network, t is represented as the time.

- **Received Signal Strength Indication (RSSI)**

Received Signal Strength Indication (RSSI) $(RSSI_{WSN})$ does indeed follow an inverse-square law relationship with distance in wireless communication systems. This means that as the distance between the transmitter (sender) and receiver increases, the strength of the received signal decreases proportionally to the square of the distance and its equation is given in (11):

$$RSSI_{WSN} = -36 \times \log(Dis) - 55$$
$$Dis = 10^{(RSSI_{WSN}+55)/-36} \quad (11)$$

Where, Dis is represented as the distance.

For efficient data transmission the network parameters such as Energy consumption, Node degree, Residual Energy, Distance, Delay and RSSI are optimized using RPASOA and using this algorithm the optimal cluster head is selected.

3.2 RPASOA for selecting optimal cluster head by optimizing network parameters

The Red Piranha Alpine Skiing Optimization Algorithm (RPASOA) is employed to select optimal cluster heads in a Wireless Sensor Network (WSN) by optimizing critical network parameters. This metaheuristic algorithm models the dynamic and adaptive behaviours of red piranhas in alpine skiing environments, enabling efficient exploration and exploitation of the solution space. RPOA is a novel metaheuristic approach inspired by the dynamic and adaptive behaviours of red piranhas. ASOA is an innovative metaheuristic algorithm inspired by the movements and strategies of alpine skiers navigating slopes. It is designed to optimize complex problems by mimicking the

balance between exploration and exploitation found in skiing, where skiers dynamically adjust their paths to achieve the fastest descent.

Energy Consumption is optimized for minimizing the energy usage of nodes to prolong network lifespan. Node Degree is optimized for balancing the number of connections each node maintains to ensure network robustness without excessive energy drain. Residual Energy is optimized by selecting nodes with higher remaining energy to act as cluster heads, ensuring longer periods of effective operation. Distance is calculated by reducing the average distance between nodes and their cluster heads to minimize energy consumption and latency. Delay is optimized for decreasing communication delay to enhance real-time data processing capabilities. RSSI (Received Signal Strength Indicator) is optimized Ensuring strong and reliable signal strength for effective data transmission.

In this, Red Piranha Optimization Algorithm (RPOA) is used to optimize Energy consumption, Node degree, Residual Energy and Alpine Skiing Optimization Algorithm (ASOA) is used for optimizing Distance, Delay and RSSI. The pseudocode for RPASOA for optimal cluster head selection is given in table 1. In this, first initialize the initial population of RPASOA for optimizing network parameters for optimal cluster head selection. Next randomly generate the dynamic and adaptive behaviours of red piranhas and exploration behaviour of ASOA for attaining the best solution. Then the fitness function is used to attain the objective function that is optimally select cluster head by optimizing network parameters in WSN for efficient data transmission. The fitness function equation is given in (12):

$$FF = Min\left(\left(Ey_{total}(\beta), R_{Ey}, D_{NX}, Dis, D_e,\right), Max\left(RSSI_{WSN}\right)\right) \rightarrow \left(Optimal\ cluster\ head\ selection\right) \quad (12)$$

The Attacking of the prey of RPOA is used to optimize $Ey_{total}(\beta), R_{Ey}, D_{NX} = \chi$ and its equation is given in (13):

$$F_{P(n)} = \left|F.(\chi)Y_{prey} - Y_{P(n)}(t)\right| \quad (13)$$

Where, $P(n)$ is represented as the position of the n^{th} search agent, Y_{prey} is represented as the predicted location of the prey at the iteration t, $F.(\chi)$ are represented as the coefficient vectors for optimizing the network parameters such as $Ey_{total}(\beta), R_{Ey}, D_{NX}$ for optimal cluster head selection.

Then the exploration and exploitation β phase of ASOA is used to optimize $Dis, D_e, RSSI_{WSN} = \alpha$ for selecting optimal cluster head and its equation is given in (14):

$$\beta = \left(\frac{\Gamma(1+\alpha) \times \sin\left(\frac{\pi\alpha}{2}\right)}{\Gamma(1+\alpha) \times \sin\left(\frac{\alpha-1}{2}\right)} \right)^{\frac{1}{\alpha}} \quad (14)$$

Where, α is represented as the optimizing parameter for optimal cluster head selection. In this, the selected parameters are χ, α, by using these equations optimal cluster head is selected. Until the stopping requirement is met, this process is carried out repeatedly.

Table 2: Pseudocode for RPASOA for Optimal Cluster Head Selection

Algorithm: RPASOA for Optimal Cluster Head Selection
Input: - Sensor nodes - Network parameters: Energy consumption, Node degree, Residual Energy, Distance, Delay, RSSI - Maximum iterations MaxIter **Output:** - Optimal Cluster Head CH
1. Initialize population of solutions (cluster heads) randomly 2. Evaluate fitness of each solution based on network parameters
3. Attacking the prey of RPOA is used to optimize $Ey_{total}(\beta), R_{Ey}, D_{NX} = \chi$ and its equation is given in (13):
4. The exploration and exploitation β phase of ASOA is used to optimize $Dis, D_e, RSSI_{WSN} = \alpha$ for selecting optimal cluster head and its equation is given in (14):
5. Select best solutions to form new population/ Return best solution as Optimal Cluster Head CH
6. **The** loop continues until a termination condition (e.g., a maximum number of iterations) is met.

Hence, RPASOA effectively balances the exploration and exploitation phases to ensure robust and energy-efficient cluster head selection, enhancing network performance, reliability, and lifespan by ensuring optimal resource utilization and strong communication links. After selecting the cluster head, the cluster is formed based on intra-cluster and inter-cluster.

3.3 Duty Cycling Phase

One important method for lowering WSN energy use is duty cycling. In our work, we presented the Siam-GCAN algorithm, which adaptively determines the scheduling mode of each node during duty cycle.

3.3.1 Scheduling using Siam-GCAN

In this, the Siam-GCAN is used for scheduling each sensor node's scheduling modes adaptively. To avoid data collisions, it partitions time intervals into slots for sensor nodes. Using the Siam-GCAN algorithm, nodes adaptively switch between the transmit; listen, and sleep modes and its explanations are given below:

- **Transmit mode**

When the sensor node is in transmit mode, it sends data from the nearby sensor node as well as data it has sensed to the sink node.

- **Listen mode**

Sensor nodes sense their environment and gather information from nearby nodes when they are in listen mode. But they cut off their transmitter circuitry, which restricts the amount of data that can be sent.

- **Sleep mode**

Sensor nodes that are in sleep mode use less energy and have a longer-lasting network because they are not transmitting or receiving data from any node and have their radios turned off.

Figure 3 shows the Siam-GCAN for scheduling process.

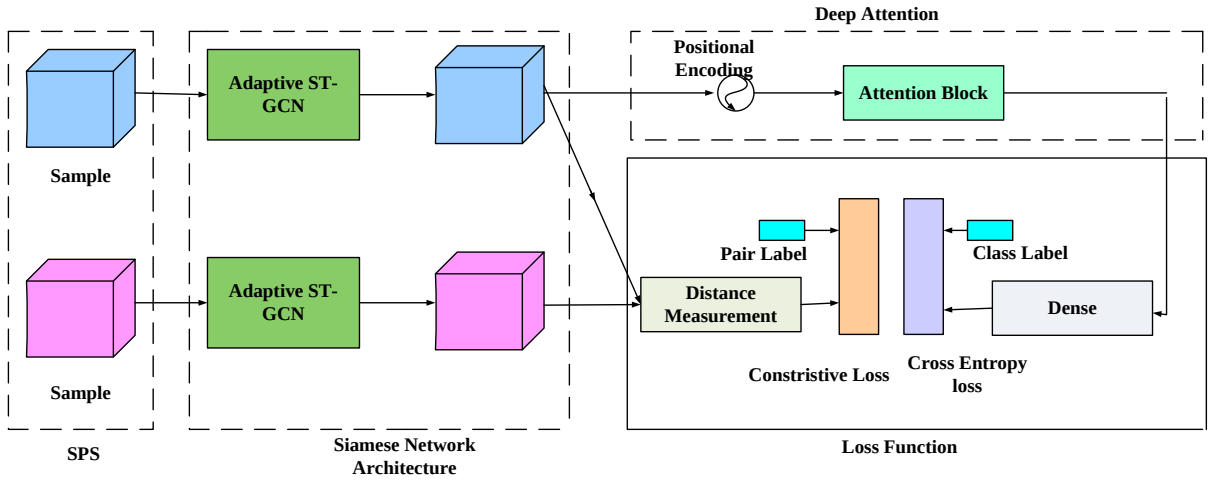

Figure 3: Siam-GCAN for scheduling process

It consists of four steps, they are: sample pairs selection (SPS), Siamese Network Architecture (SNA), deep attention, and loss function. And its explanations are given below:

- **Sample Pairs Selection (SPS)**

In WSN scheduling, first construct the sample pairs to exploit intra-cluster and inter-cluster information. This helps the network learn optimal scheduling modes (Sleep, Listen, and Transmit) by understanding similarities and differences between node states. In this, the data is collected based on the sensor data over a period and divide the samples (network data) into $X_j \in \Re^{t \times m \times g}$, t is represented as the time, m is represented as the number of sensor nodes, g is represented as the number of sensor nodes (energy level, buffer size). Then the data constructed as every samples as X_j, randomly select a sample X_j, from the same zone (positive pair) and a sample X_l, from a different zone (negative pair). Input pairs are denoted as (X_1, X_2).

- **Siamese Network Architecture (SNA)**

The SNA consists of two identical adaptive Spatial-Temporal Graph Convolutional Networks (ST-GCNs) that share weights. These networks learn spatial-temporal representations of sensor node states. In this, the Input pairs are denoted as (X_1, X_2) and its feature extracted data are represented as the $H(X_1)$ and $H(X_2)$ from the input samples. From this the distance (Dis) are measured in equation (15):

$$dis = Dis(X_1, X_2) = \| H(X_1) - H(X_2) \|_2 \quad (15)$$

- **Deep Attention**

The deep attention layer refines the learned features by focusing on significant aspects of the sensor data. In this, deep attention is done by the process of 3 stages, they are Positional Encoding, Multihead Attention, Output Aggregation and its explanations are given below:

In Positional Encoding, add 1-D to the input embeddings. Then these outputs are given to the multihead attentions and its equations are given in (16):

$$g_i = attention(Q_j, K_{j,} V_j) = soft\max\left(\frac{Q_j K_{j,}^{\ T}}{\sqrt{dis_l}}\right)V_j \qquad (16)$$

Where, $Q_j, K_{j,} V_j$ are represented as the queries, keys, values, $Q_j, K_{j,} \in \Re^{I\times n\times dis_l}$ and $V_i \in \Re^{I\times n\times dv}$, where dis_l is the dimension of queries and keys and dis_V is the dimension of values. Then combine the outputs of multiple attention heads for combining different sensor nodes, this will decrease the energy and the concatenation equation is given in (17):

$$Multi-Head(Q,K,V) = Concat(g_1,.....,g_n)\omega_0 \qquad (17)$$

where $\omega_0 \in \Re^{dis_{fusion}\times disv}$ is a weighting matrix, where $d_{fusion} = m \times d_v$, ω_0 are represented as the weight function. By using these equations the scheduling is done, hence the energy consumption is reduced, while transferring the data, by finding shortest path.

After performing residual connection and layer normalization, the output $D(G(s_1))$ of the deep attention layer is obtained.

D. Loss Function

The Siam-GCAN loss function is made up of three parts: the loss function for the graph learning layer $(Loss_{GL})$, the contrastive loss function $(Loss_{CLoss})$, and the cross-entropy loss, which measures the error between predicted and true labels, and its equations are given below:

$$Loss_{CE} = \frac{1}{m}\sum_{j=1}^{m}\sum_{y=1}^{C} x_{j,y}\log\hat{x}_{j,y} \qquad (18)$$

where m is represented as the number of samples, C is represented as the number of classes, $x_{j,y}$ is represented as the probability that sample j belongs to the category y, and $\hat{x}_{j,y}$ denotes the prediction probability that the sample j belongs to the category y.

The final loss function of the model is as follows:

$$Loss_{Siam-GCAN} = Loss_{GL} + \lambda Loss_{CLoss} + Loss_{CE} \quad (19)$$

where λ is represented as the adjustment parameter. Using these equations, the energy consumption is reduced based on scheduling process. Then to improve the network efficiency and to reduce the node distance, the loss parameters λ is optimized using Mantis search optimization algorithm (MSOA). The detailed explanations of MSOA are given below:

3.3.2 MSOA for optimizing loss parameters of Siam-GCAN for efficient data transfer in WSN

To optimize the loss parameters of Siam-GCAN for efficient data transfer in Wireless Sensor Networks (WSNs) using the MSOA, by minimizing energy consumption, maximizing data accuracy, and minimizing latency. MSA initializes a population of potential solutions, iteratively evaluates their performance, and selects the best solutions based on Pareto dominance. Through controlled perturbations and adaptive adjustments, the algorithm balances exploration and exploitation, refining the solutions over successive iterations. This process continues until convergence, ultimately yielding a set of optimized parameters that enhance the overall efficiency and performance of Siam-GCAN in WSNs. Figure 4 shows the flow chart of EST-SGCMSAN for efficient data transfer in WSN. The step-by step procedures of EST-SGCMSAN for efficient data transfer in WSN are given below:

Step 1: Initialization

Initialize the initial population of MSOA for optimizing the loss parameter of Siam-GCAN for attaining best solution that is to improve the network efficient and to reduce the node distance.

Step 2: Random generation

Randomly generate the exploitation phase of MSOA for attaining best solution.

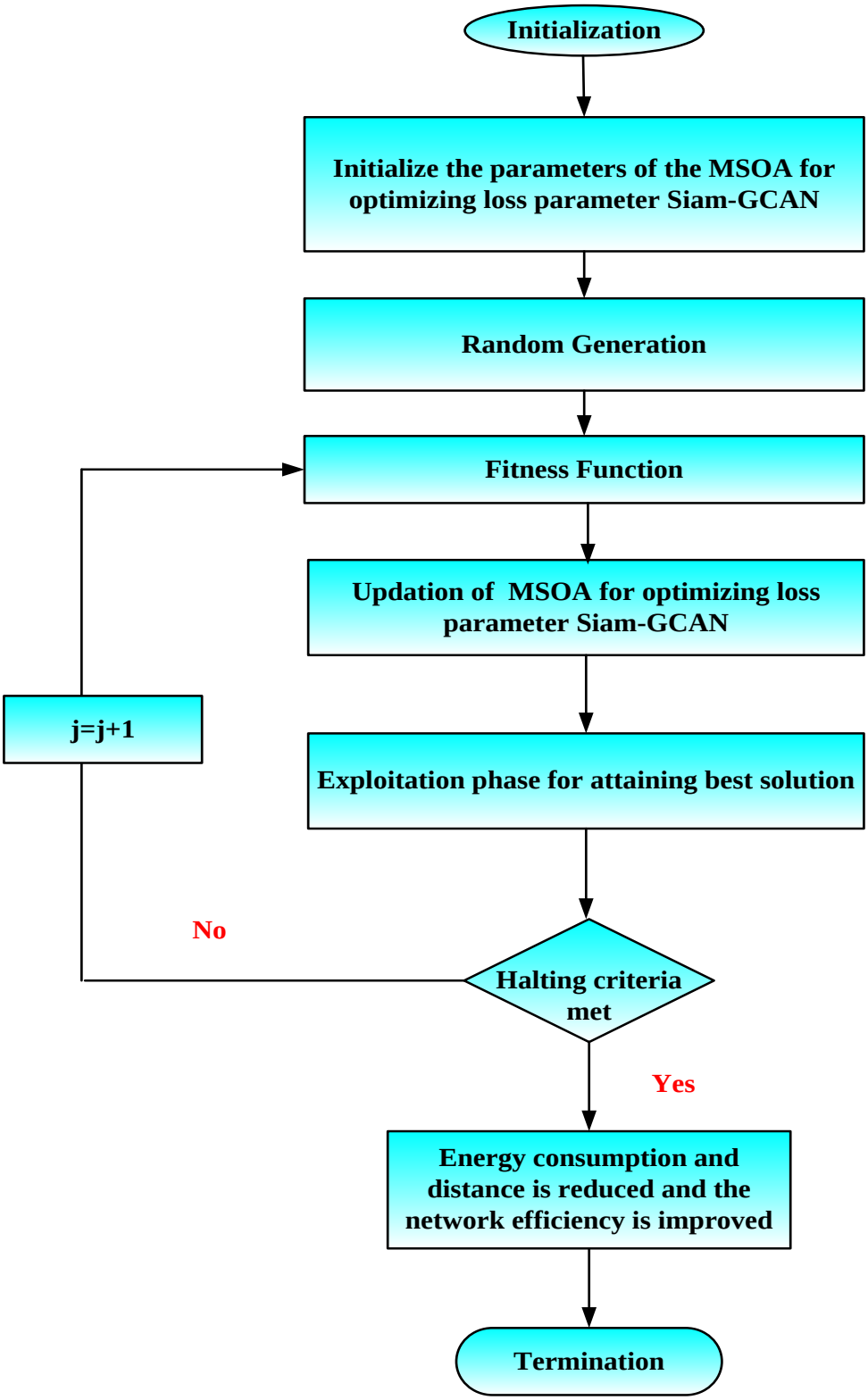

Figure 4: Flow chart of EST-SGCMSAN for efficient data transfer in WSN

Step 3: Fitness Function

In this, fitness function is used to attain the objective solution, that is to improve the network efficiency and to reduce the node distance by optimizing loss parameter λ and its equation is given in (20):

$$Fitness\ function = Optimize(\lambda) \qquad (20)$$

Step 4: Exploitation phase for attaining best solution

In this, exploitation phase is used to attain the best solution (improve the network efficiency and to reduce the node distance) and its equation is given in (21):

$$a_{j,i}^{t+1} = \lambda\left(\frac{a_{j,i}^{t+1} + a_{j,i}^{*}}{2} + r_x * dis_{xj,i}^{t}\right) \qquad (21)$$

Where, $a_{j,i}^{t+1}$ is represented as the position of the prey and it is used to reduce the distance among them and hasten the attacking process, $a_{j,i}^{*}$ is represented as the j^{th} dimension of the prey, $dis_{xj,i}^{t}$ is represented as the praying mantis's size determines the variation in the strike distance, λ is the optimizing parameter. Hence, this approach balances exploration and exploitation, leading to optimized loss parameters for Siam-GCAN, thereby enhancing the efficiency of data transfer in WSNs.

Step 5 Termination

Once the best answers are obtained using equations (17), end the operation. Additionally, equation (17) yields the most accurate answer that is to improve the network efficient and to reduce the node distance. This iteration is continuing until the halting criteria $j = j + 1$ is met. Finally, the proposed EST-SGCMSAN accurately classifies the skin cancer regions as cancer and non-cancer regions.

By this process, the energy consumption and distance is reduced and the network efficiency is improved. Then to securely transfer the data an AES-based signature generation approach utilizing White Box Cryptography (WBC) is implemented and its explanations are given below:

3.4 AES-based signature generation approach utilizing White Box Cryptography (WBC) for securely transfer the data in WSN

To further enhance the efficiency of data transfer in Wireless Sensor Networks (WSNs), an AES-based signature generation approach utilizing White Box Cryptography (WBC) can be integrated. This approach focuses on securely transferring data while reducing processing power, storage, and energy consumption. The AES-based

signature generation approach with White Box Cryptography (WBC) adds a layer of security and efficiency. By incorporating WBC, the encryption and decryption processes become more lightweight, minimizing the computational load on the sensor nodes. This method reduces the processing power required, decreases storage needs by efficiently managing cryptographic keys, and conserves energy, which is critical in resource-constrained WSN environments. Coupled with the Mantis Search Algorithm (MSA) to fine-tune the model parameters, this approach ensures secure, accurate, and efficient data transfer, significantly enhancing the overall performance and longevity of the WSN. The detailed explanations of AES-based signature generation approach utilizing White Box Cryptography (WBC) for securely transferring the data in WSN are given below:

Setup: The Setup algorithm initializes the system parameters for the Identity-Based Signature (IBS) scheme by selecting groups and pairing such as H_1, H_2, H_3: groups with order of K and its pairing function is given as $x: H1 \times H2 \to H3:$. Then these parameters are randomly picked by means of random generator G_2 of H_2 and computes $G_1 = \psi(G_2) \in H_1$, where, ψ is an isomorphism from H_2 to H_1. Then generate the master secret and public keys randomly as $x \in S_K$ and then compute $M = xG_2$ and $h = e(G_1, G_2)$. Then the system parameters are selected as $Parameters = (M, h, G_1, G_2, H_1, H_2, H_3, e)$. Th extract algorithm is used to generates the user's private key based on their identity.

Extract: The Extract algorithm generates the user's private key based on their identity. Using this algorithm identity Hash is computed and its equation is given in (22):

$$f_{ID} = F_1(ID), where, f_{ID} \in S_K \quad (22):$$

Then the private key $(\Pr i_{ID})$ generated output equation is given in (23):

$$output(\Pr i_{ID}) = (f_{ID} + x)^{-1} G_1 \qquad (23)$$

Then these outputs are given to the WhiteBoxKeyGen Algorithm for generating white-box keys for a user.

WhiteBoxKeyGen: The WhiteBoxKeyGen algorithm generates the white-box keys for a user. In this, first select the random scalars such as numbers $s_1, s_2, ..., s_m \geq x_m \in_K, where, m \geq 256$ and then compute $z_j = y^{s_j}$ and $S_j = s_j \Pr i_{ID}$ $for\ j = 1,2,3,...m$, where, S_j is the values used in the WhiteBoxKeyGen phase of the identity-based signature scheme to securely generate and store cryptographic keys, $z_j = y^{s_j}$ are critical in the WhiteBoxKeyGen phase of the identity-based signature scheme, it helps in creating secure cryptographic keys by leveraging the randomness and difficulty of solving discrete logarithms in H_3 and the additional random scalars

$x_1, x_2, ..., x_{256} \in X_K$. Then secondly compute the random scalars such as numbers as $v_j = y^{z_j}$ and $Z_j = 2^{j-1} \Pr i_{ID} + z_j \Pr i_{ID}$ $for\ j = 1,2,3,...m$, where, Z_j is the values used in the WhiteBoxKeyGen phase of the identity-based signature scheme to securely generate and store cryptographic keys, $v_j = y^{z_j}$ are critical in the WhiteBoxKeyGen phase of the identity-based signature scheme. After that delete the random scalars as $Deletes\{s_1, s_2, ..., s_m\} and\ x_1, x_2, ..., x_{256}$.

Sign: The Sign algorithm generates a signature for a given message and identity. In this, first generate $m-bit$ the random binary number br and it is given as $br_m br_{m-1}, ...br_2 br_1$ and then compute z'_j and X_1 and its equation is given in (24-25):

$$z'_j = \prod_{j:br_{j-1}} z_i \qquad (24)$$

$$X_1 = \sum_{j:br_{j-1}} X_i \qquad (25)$$

Then compute the hash in equation (26):

$$p_{hash} = G_2(n, z') \qquad (26)$$

Where, p_{hash} is represented as the binary number denoted in $p_{hash256}, p_{hash255}, ... p_{hash1 p_{hash2}}$ and the signature X_2 is computed using equation (27):

$$X_2 = \sum_{j:p_{hash-1}} X_j \qquad (27)$$

And setting X' value is given in equation (28):

$$X' = X_1 + X_2 \qquad (28)$$

The output of the signature is given in (29):

$$\chi = (p_{hash}, X') \qquad (29)$$

Finally, verify the validity of the given signature using verification process.

Verify: The Verify algorithm checks the validity of the given signature. For the verification process first compute the d_1 and d_2, where, d_1 represents a product involving specific v_j values based on the binary representation of p_{hash}, d_2 involves the evaluation of a bilinear pairing function e over certain group elements, adjusted by components from the signature and the verification process. In this, first compute the d_1 using hash function p_{hash} as $p_{hash256}, p_{hash255},...p_{hash2}, p_{hash1}$ and its equation is given in (30):

$$d_1 = \prod_{j:p_{hash-1}} v_j \quad (30)$$

And the d_2 is calculated in equation (31):

$$d_2 = \frac{e(X', P_{hashID} G_2 + M)}{e(G_1, G_2)^h} \quad (31)$$

Where, M is represented as the computed value derived from the master secret key and a G_1 of a group G_2.

Then the final verification key is represented in equation (32):

$$p'_{hash} = G_2(n, z) \quad (32)$$

Where, G_2 is represented as the binary value extracted from the signature, p'_{hash} is represented as the value computed during the verification process, n is represented as the message (this is the original message that was signed) n, z is a parameter derived during the signature generation process.. In this, security is confirmed by checking the conditions, if $p_{hash} = p'_{hash}$, then the signature is valid, and the output is 1. if $p_{hash} \neq p'_{hash}$, then the signature is not valid, and the output is 0.

By this process the data collected using WSN sensor is efficiently and securely transferred to the destination.

The proposed EST-SGCMSAN system enhances Wireless Sensor Networks (WSNs) by integrating multi-objective cluster head selection via RPASOA for energy efficiency and reduced delay. It employs a novel sleep scheduling mechanism using SGCMSAN to optimize energy use. Security is ensured through AES-based signatures with White Box Cryptography, addressing node constraints.

4 Results and Discussions

The outcomes of the suggested EST-SGCMSAN are discussed. The performance of the proposed EST-SGCMSAN method is compared with existing models, like RLBEEP [16], BWO-EECM [17], DRL [18], GWO [19], EAHA

[20], EAEDA-DR [21, E-FUCA [22], BSO-LD [23] for cluster head selection and scheduling process. For the security process the proposed EST-SGCMSAN method is compared with existing encryption algorithms used in WSN are analysed NTM-LEACH-RSA [24], c-RSA-AES [25], SMOFCM [26], AES- ECC [27] respectively.

4.1 Simulation setup

The EST-SGCMSAN method is implemented in python with 2 GB random access memory, Intel core processor, Windows 10 OS. Table 3 tabulates the parameters utilized in simulation process.

Table 3: Parameters utilized in simulation process.

Parameters	Values
Monitoring area	100×100 m²
Simulation time	4600 sec
Network	Wireless sensor
Nodes energy	$0.1 Joule$
Nodes in sensor	100, 200
Number of iterations	2000

4.2 Performance comparison of various approaches

The EST-SGCMSAN outcome is determined by few performance metrics in this section. The metrics namely, throughput, Energy Consumption (EC), delay, Network life time (NLT), Packet drop, Residual energy (RE), RSSI, Distance and Packet Delivery Ratio (PDR), are evaluated for 100 nodes and 200 nodes and compared with the existing methods namely, RLBEEP [16], BWO-EECM [17], DRL [18], GWO[19], EAHA[20], EAEDA-DR[21, E-FUCA [22], BSO-LD [23] for cluster head selection and scheduling process in WSN. The explanations of the performance metric are given below:

4.2.1 Network Lifetime

The sensor network's lifetime is determined by the network lifetime statistic. The moment at which a network's initial node fails is commonly used to describe the lifetime of the network. It may additionally be characterized as the node's operating period, during which it can carry out the assigned duty. The symbol for network lifetime is $\hbar$ which might mean and its equations are given in (33):

$$\hbar = \frac{\chi - \beta}{\hat{\lambda} + \Re\gamma} \qquad (33)$$

where, χ signifies primary network energy, β signifies energy of misused, $\hat{\lambda}$ signifies incessant network power consumption, $\Re$ signifies normal reporting rate of the sensor and γ signifies projected reporting energy.

4.2.2 Energy Consumption

The quantity of energy used by the system for sensing, data transmission, and data reception is referred to as the energy consumption measure. It is shown as follows in its representation is $\wp$, and its equations are given in (34)

$$\wp = \sum \aleph + \nu + \xi \qquad (34)$$

where $\aleph$ characterizes the energy used in data transmission, ν characterizes the energy used in receiving data and ξ characterizes the energy used in detecting the field.

4.2.3 Throughput

The quantity of packets received effectively by the receiver in a particular period of time is known as the throughput measure. It is portrayed as N being communicated and its equations are given in (35)

$$\mathrm{N} = \frac{\sum_{j=1}^{m} \partial_j * \partial_k}{t(s)} \qquad (35)$$

where ∂_j characterizes the number of packets in node 'j', ∂_k signifies length of the data packet and $t(s)$ characterizes the time of simulation.

4.2.4 Delay

The amount of period needed to transfer sensed data from the original node to the node of destination is known as the delay. It is portrayed as H and its equations are given in (36):

$$\mathrm{H} = \frac{\wp_d}{\wp_s} \qquad (36)$$

where $\wp_d$ characterizes the period needed to send the data and $\wp_s$ characterizes information that the target node has received.

4.2.5 Packet delivery ratio

A significant PDR value is necessary for the data transmission to be accomplished. While the whole amount of data produced by all source nodes is assessed in Equation (37), the proportion of the total information that is successfully transmitted to all the destination nodes is determined. Furthermore, if the PDR level is set to the highest, the data on the receiving side will be received with no loss.

$$PDR = \frac{\text{Overall quantity of received data}}{\text{overall quantity of transfered data}} \qquad (37)$$

4.2.6 Throughput

The amount of data gathered at the point of reception and the duration of the data transmission procedure are referred to as throughput and its equations are given in (38):

$$T_p = \frac{\text{Number of received data to the users}}{\text{Time delay}} \qquad (38)$$

The performance analysis of each metrics is given below:

Figure 5 Network diagram for finding shortest distance for securely transferring the data using 100 nodes and 200 nodes are given. This diagram shows the optimized shortest paths for securely transferring data using 100 and 200 nodes in a Wireless Sensor Network (WSN). It utilizes RPASOA for optimal cluster head selection and Siam-GCAN with Mantis Search optimization for efficient scheduling, ensuring minimal energy consumption and low transmission delay.

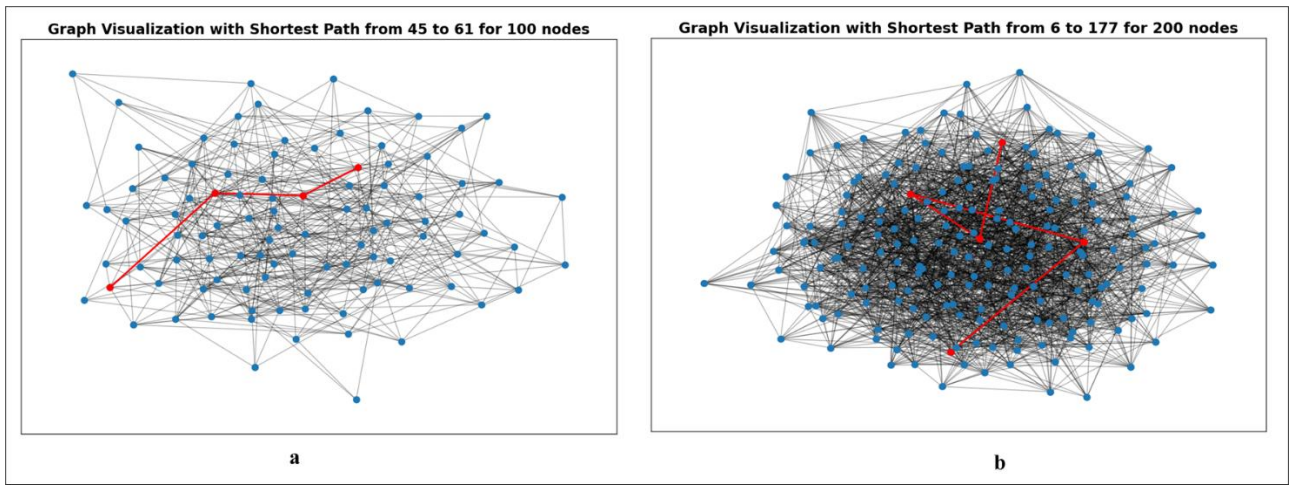

Figure 5 (a): Network diagram for 100 nodes, (b) Network diagram for 200 nodes

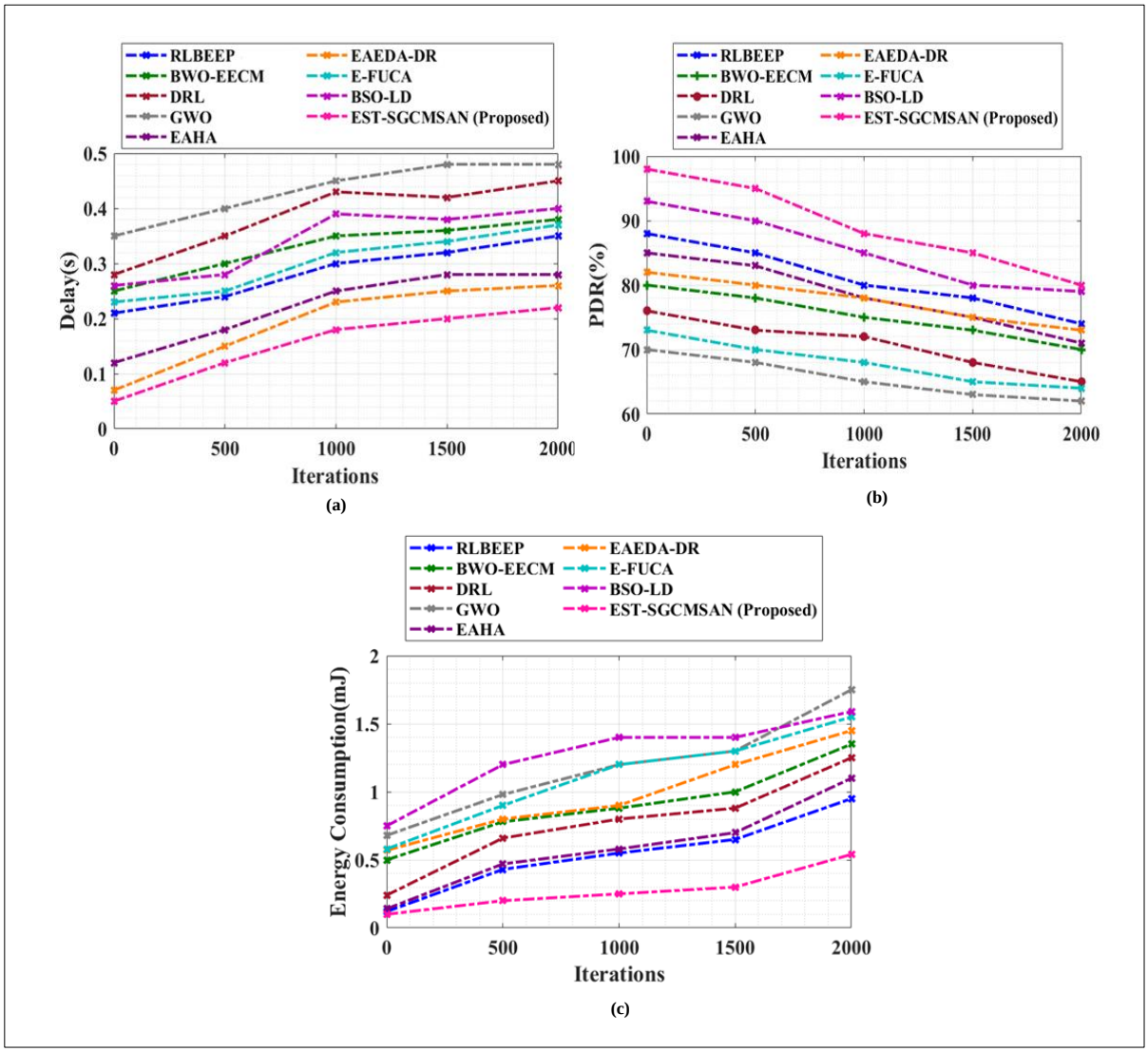

Figure 6: (a) Delay, (b) PDR and (c) Energy Consumption of proposed and existing methods for 100 nodes

Figure 6 shows the (a) Delay, (b) PDR and (c) Energy Consumption of proposed and exiting methods for 100 nodes. The proposed method is EST-SGCMSAN and the existing methods are RLBEEP [16], BWO-EECM [17], DRL [18], GWO [19], EAHA [20], EAEDA-DR [21], E-FUCA [22] and BSO-LD [23]. Figure 6 (a) shows the delay of proposed and existing methods. For the network to function well, packet transmission delays must be as small as possible. The delay is represented in seconds. When 100 nodes, the proposed method uses the first round's delay which is only 0.001s. When employing the proposed approach, the delay value for 100 nodes is 0.15 s as the round progresses, or at the 2000th round. Likewise, when the number of rounds increases. The proposed method gives lower delay as compared to other existing models. Figure 6 (b) shows the PDR of proposed and existing methods. For 100 nodes, the PDR is high at the 500th iteration. The proposed method gives high PDR as compared to other existing models. Figure 6 (c) shows the energy consumption of proposed and existing methods. When the

iterations are increased the energy consumption is reduced. The energy consumption is low at 500th iteration. The proposed method gives lower energy consumption as compared to other existing models.

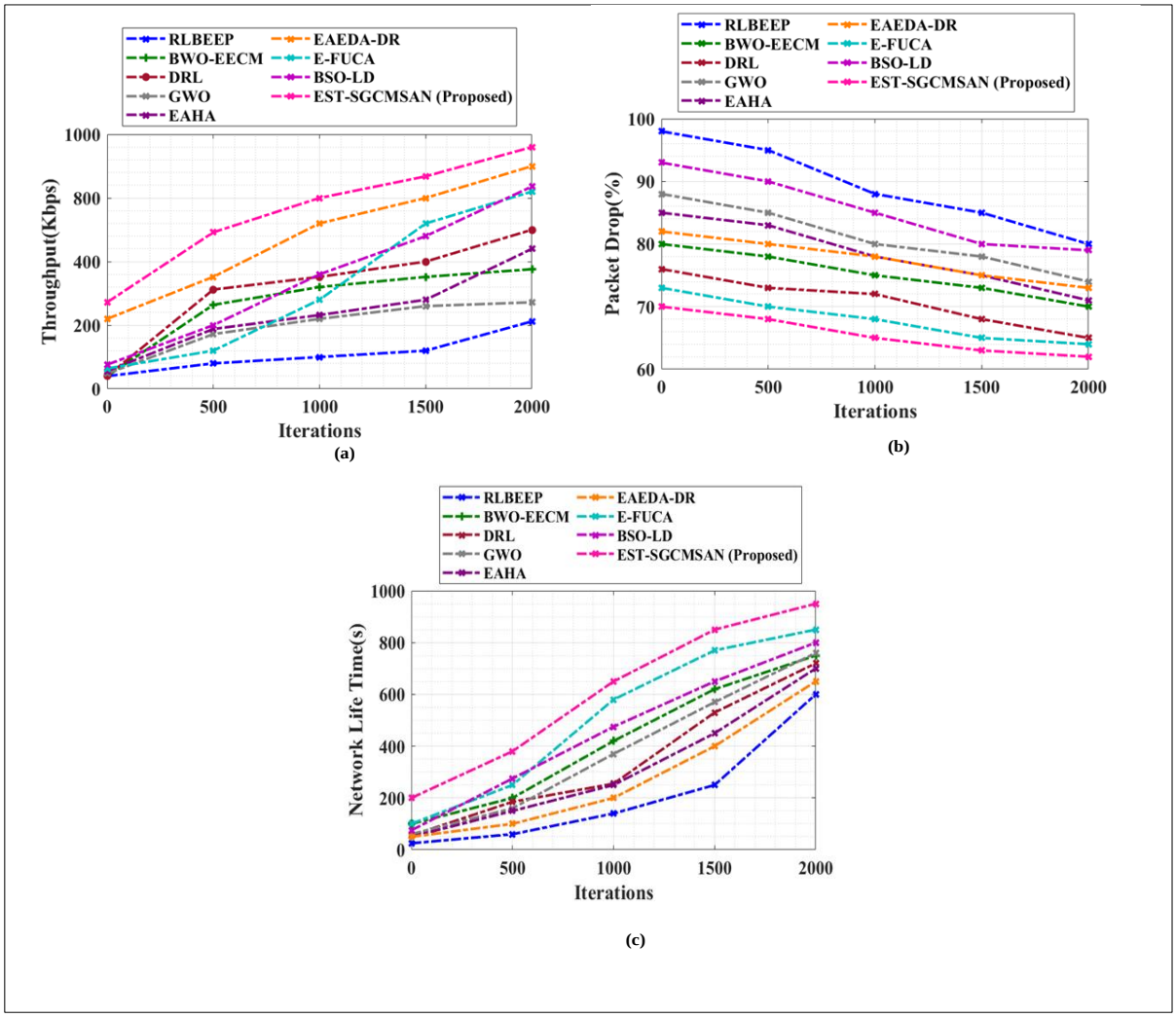

Figure 7: (a) Throughput, (b) Packet Drop and (c) Network Life Time of proposed and existing methods for 100 nodes

Figure 7 shows the (a) Throughput, (b) Packet Drop and (c) Network Life Time of proposed and exiting methods for 100 nodes. The proposed method is EST-SGCMSAN and the existing methods are RLBEEP [16], BWO-EECM [17], DRL [18], GWO [19], EAHA [20], EAEDA-DR [21], E-FUCA [22] and BSO-LD [23]. Figure 7(a) shows the Throughput of proposed and existing methods. The quantity of data that a system can handle in a specific amount of time is measured by its throughput. Typically, throughput is expressed in kbps. Since throughput is essential to data transfer, it must be large. For 100 nodes, throughput of the proposed method is high at 2000 iteration. The proposed method gives high throughput as compared to other existing models. Figure 7 (b) shows the Packet Drop of proposed and existing methods. For 100 nodes, the Packet Drop of the proposed method is lower as compared to other existing methods. Figure 7 (c) shows the Network Life Time of proposed and existing methods. For 100

nodes, the Network Life Time is high at 2000 iterations. The proposed method gives high Network Life Time as compared to other existing models.

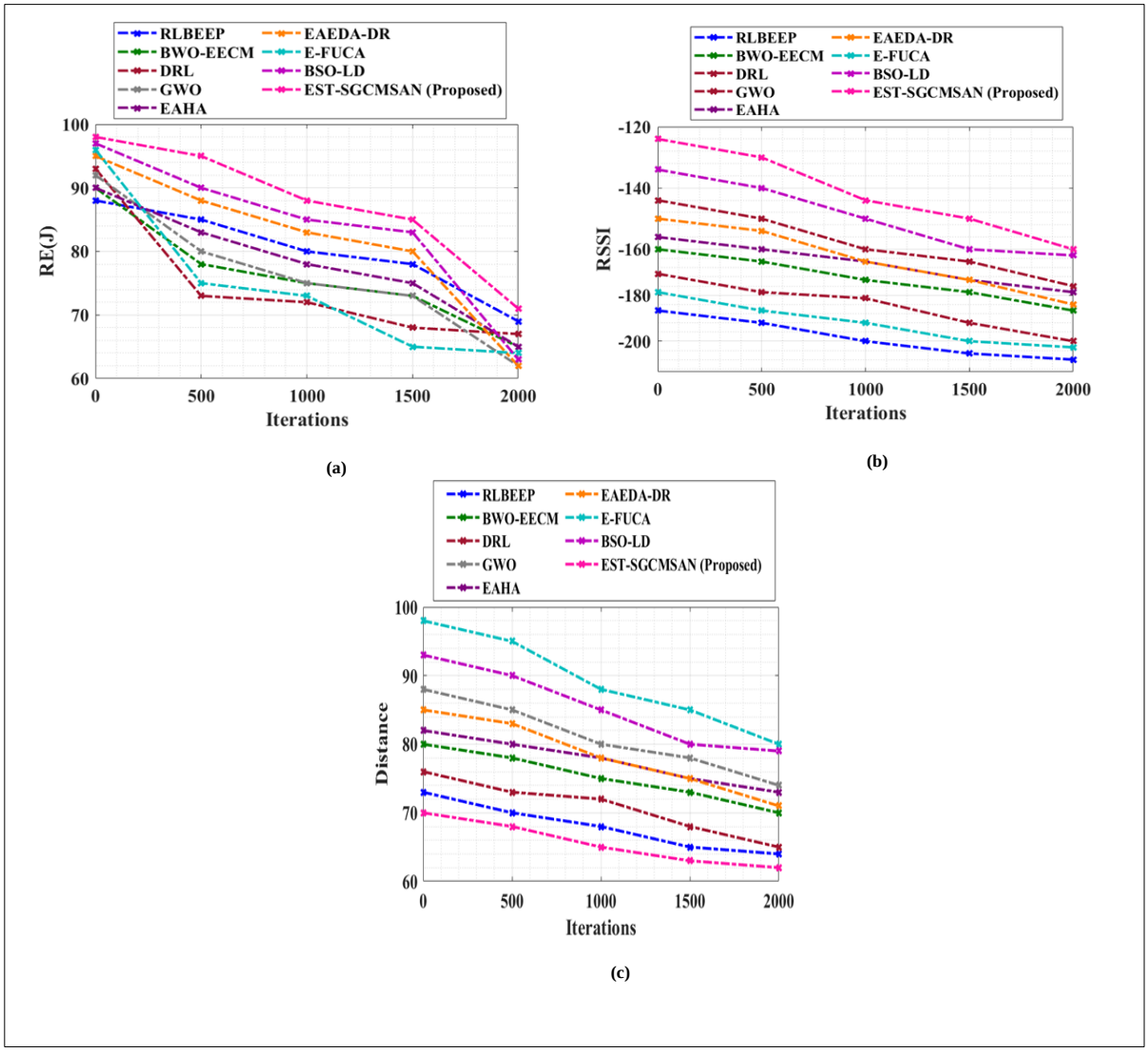

Figure 8: (a) RE (J), (b) RSSI and (c) Distance of proposed and existing methods for 100 nodes

Figure 8 shows the (a) RE (J), (b) RSSI and (c) Distance of proposed and existing methods for 100 nodes. The proposed method is EST-SGCMSAN and the existing methods are RLBEEP [16], BWO-EECM [17], DRL [18], GWO [19], EAHA [20], EAEDA-DR [21], E-FUCA [22] and BSO-LD [23]. Figure (a) shows the RE of proposed and existing methods. For 100 nodes, the Residual Energy of the proposed method is high at 500 iterations. The proposed method gives high Residual Energy as compared to other existing models. Figure 8 (b) shows the RSSI of proposed and existing methods. For 100 nodes, the RSSI of the proposed method is high at 500 iterations. The proposed method gives high RSSI as compared to other existing models. Figure 8 (c) shows the Distance of

proposed and existing methods. For 100 nodes, the Distance of the proposed method is low at 2000 iterations. The proposed method gives lower Distance as compared to other existing models.

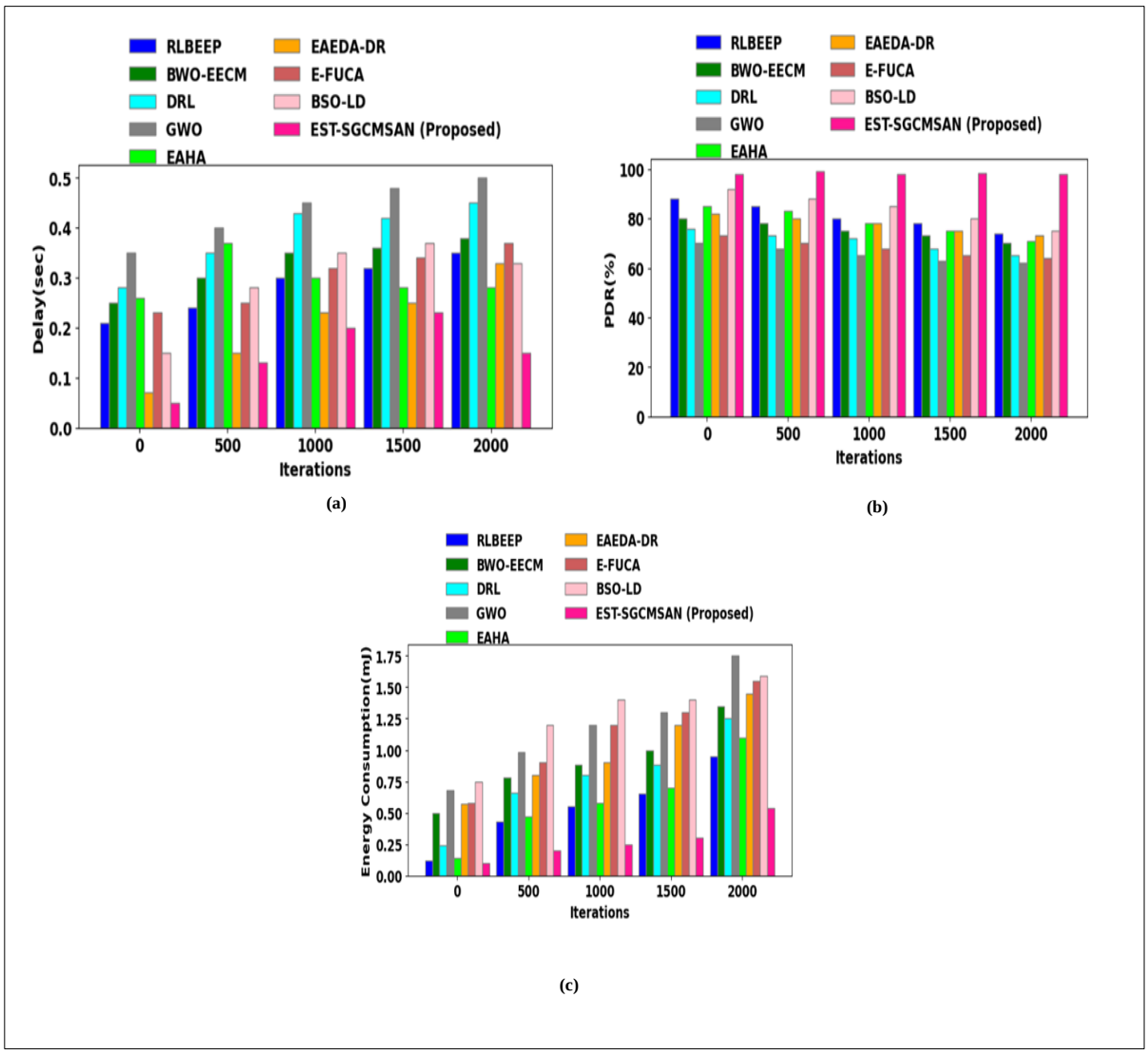

Figure 9: (a) Delay, (b) PDR and (c) Energy Consumption of proposed and existing methods for 200 nodes

Figure 9 shows the (a) Delay, (b) PDR and (c) Energy Consumption of proposed and existing methods for 200 nodes. The proposed method is EST-SGCMSAN and the existing methods are RLBEEP [16], BWO-EECM [17], DRL [18], GWO [19], EAHA [20], EAEDA-DR [21], E-FUCA [22] and BSO-LD [23]. Figure 9 (a) shows the delay of proposed and existing methods. For the network to function well, packet transmission delays must be as small as possible. The delay is represented in seconds. When 200 nodes, the proposed method uses the first round's delay and is only 0.15s. When employing the proposed approach, the delay value for 200 nodes is 0.2 s as the iteration progresses, or at the 2000th round. Likewise, when the number of rounds increases, the proposed method

gives lower delay as compared to other existing models. Figure 9 (b) shows the PDR of proposed and existing methods. For 200 nodes, the PDR is high at the 1000th iteration. The proposed method gives high PDR as compared to other existing models. Figure 9 (c) shows the energy consumption of proposed and existing methods. When the iterations are increased the energy consumption is reduced. For 200 nodes, the energy consumption is low at 500th iteration. The proposed method gives lower energy consumption as compared to other existing models.

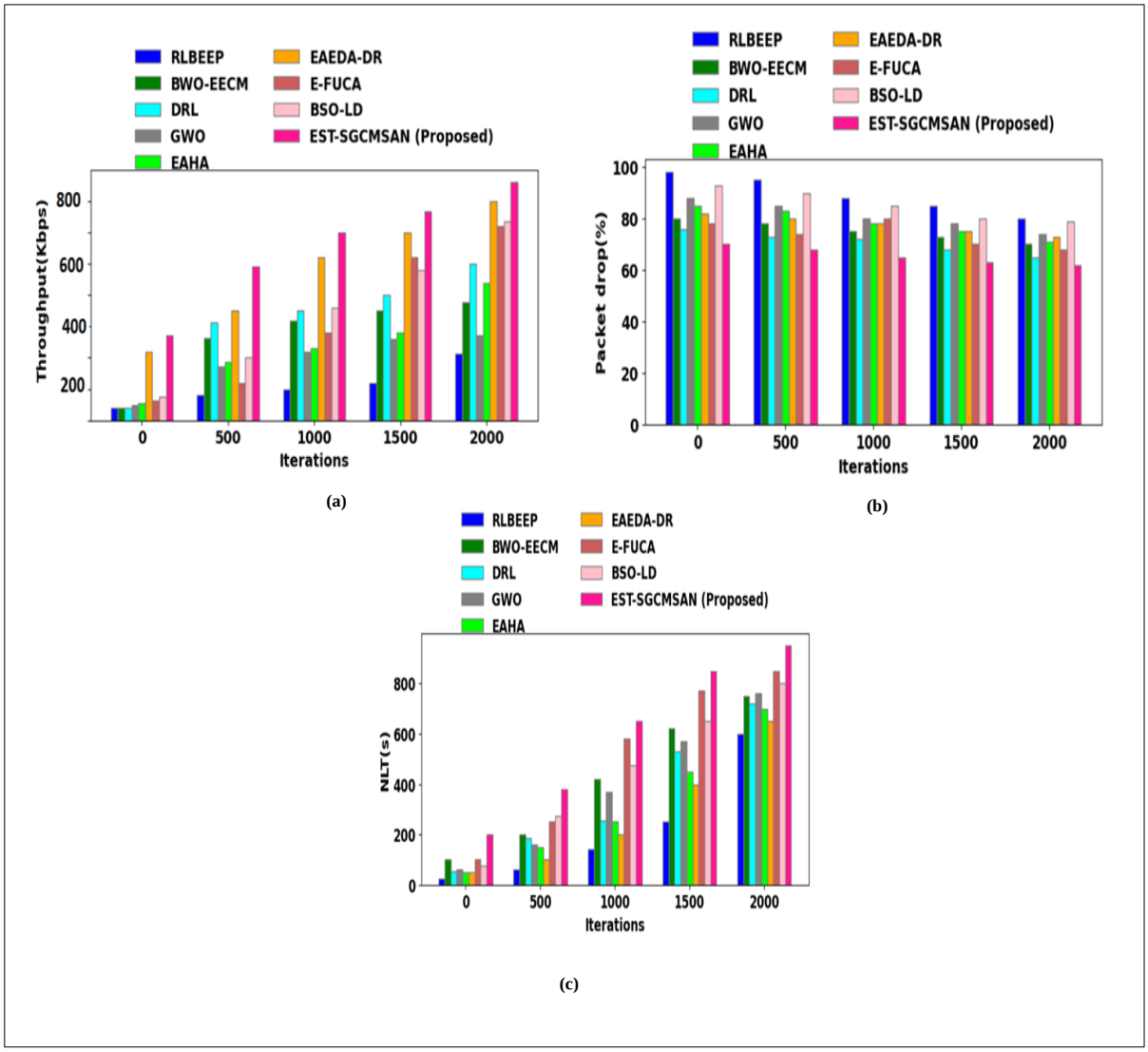

Figure 10: (a) Throughput, (b) Packet Drop and (c) Network Life Time of proposed and existing methods for 200 nodes

Figure 10 shows the (a) Throughput, (b) Packet Drop and (c) Network Life Time of proposed and existing methods for 200 nodes. The proposed method is EST-SGCMSAN and the existing methods are RLBEEP [16], BWO-EECM [17], DRL [18], GWO [19], EAHA [20], EAEDA-DR [21], E-FUCA [22] and BSO-LD [23]. Figure 10 (a) shows the Throughput of proposed and existing methods. The quantity of data that a system can handle in a specific

amount of time is measured by its throughput. Typically, throughput is expressed in kbps. Since throughput is essential to data transfer, it must be large. For 200 nodes, throughput of the proposed method is high at 2000 iteration. The proposed method gives high throughput as compared to other existing models. Figure 10 (b) shows the Packet Drop of proposed and existing methods. For 200 nodes, the Packet Drop of the proposed method is lower as compared to other existing methods. Figure 10 (c) shows the Network Life Time of proposed and existing methods. For 200 nodes, the Network Life Time is high at 2000 iterations. The proposed method gives high Network Life Time as compared to other existing models.

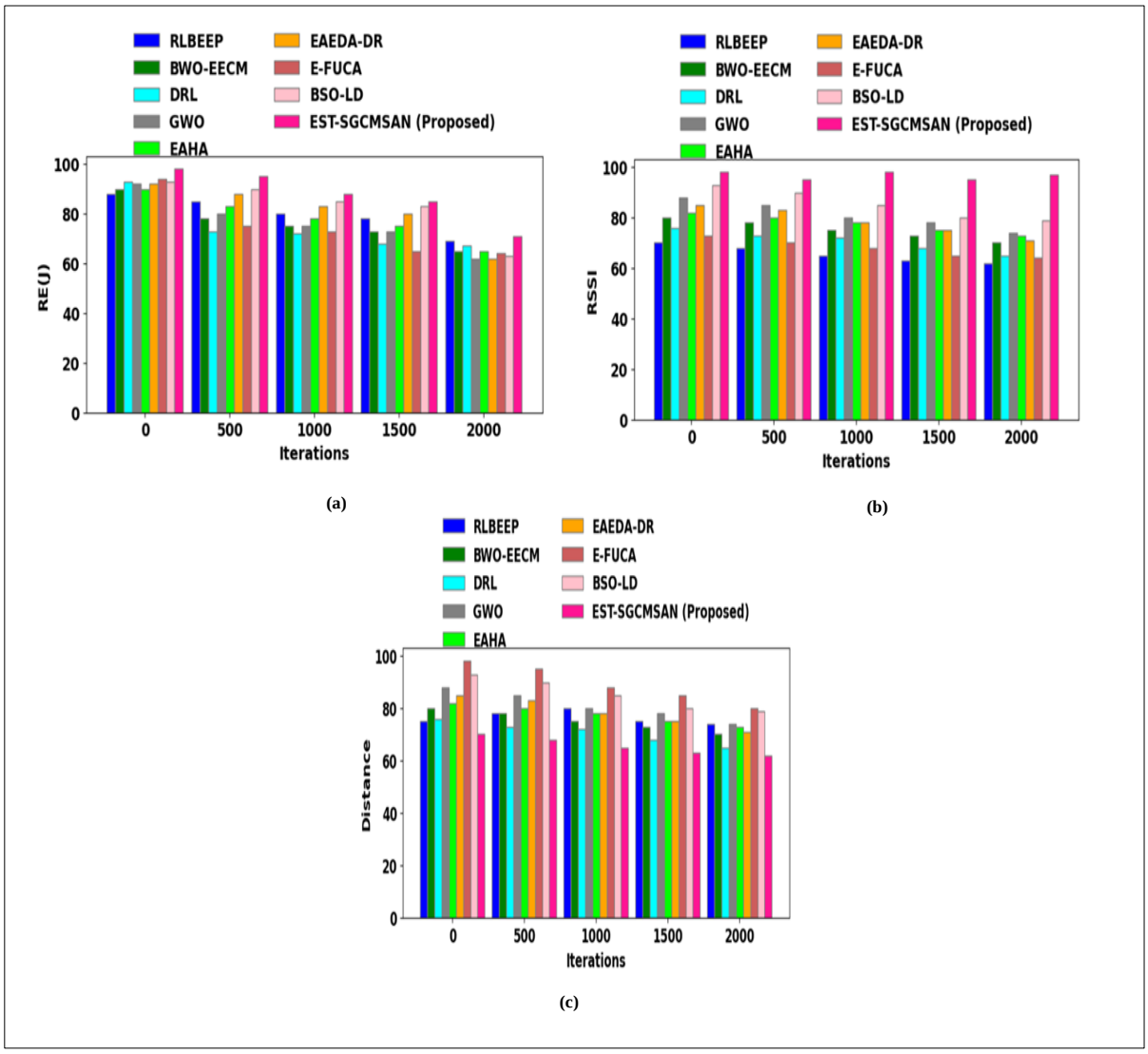

Figure 11: (a) RE (J), (b) RSSI and (c) Distance of proposed and existing methods for 200 nodes

Figure 11 shows the (a) RE (J), (b) RSSI and (c) Distance of proposed and existing methods for 200 nodes. The proposed method is EST-SGCMSAN and the existing methods are RLBEEP [16], BWO-EECM [17], DRL [18],

GWO [19], EAHA [20], EAEDA-DR [21], E-FUCA [22] and BSO-LD [23]. Figure 11 (a) shows the RE of proposed and existing methods. For 200 nodes, the Residual Energy of the proposed method is high at 500 iterations. The proposed method gives high Residual Energy as compared to other existing models. Figure 11 (b) shows the RSSI of proposed and existing methods. For 200 nodes, the RSSI of the proposed method is high at 1000 iterations. The proposed method gives high RSSI as compared to other existing models. Figure 11 (c) shows the Distance of proposed and existing methods. For 200 nodes, the Distance of the proposed method is low at 1500 iterations. The proposed method gives lower Distance as compared to other existing models.

4.3 Security Analysis

For the security process the proposed EST-SGCMSAN method is compared with existing encryption algorithms used in WSN are analysed NTM-LEACH-RSA [24], c-RSA-AES [25], SMOFCM [26], AES- ECC [27] respectively.

4.3.1 Performance Evaluation

The performance of the suggested EST-SGCMSAN model is examined by using numerous statistical measures like Encryption time, decryption time graph, Security level analysis, Data Confidentiality Rate (DCR), Data Integrity Rate (DIR), analysis and is explained as follows:

4.3.1.1 Data Confidentiality Rate (DCR)

This can be formulated in equation (39), in this j represents each individual data and m represents the total number of data

$$DCR = \sum_{j=1}^{m} \frac{Number\,of\ data}{Number\ of\ \ protected\ data} \times 100 \tag{39}$$

4.3.1.2 Data Integrity Rate (DIR)

DIR is defined as the proportion of data unaffected by unsanctioned admission (i.e., attacks) out of the total data volume. This can be formulated in equation (40),

$$DIR = \sum_{j=1}^{m} \frac{Number\,of\ data\ \ not\ altered}{Number\ of\ \ \ data} \times 100 \tag{40}$$

4.3.1.3 Security Analysis

Security Analysis refers to the amount of memory required for storing data within sensor nodes. This can be formulated in equation (41),

$$SC = \sum_{j=1}^{m} Number\ of\ \ data \times Space(data\ storing) \tag{41}$$

4.3.1.4 Encryption time:

It is the difference in the times the encryption algorithm takes to create an encrypted from plain text and the times it takes to start and finish the encryption process.

4.3.1.5 Decryption time:

It is computed as the difference between the encryption start and end times. The evaluations based on these performance metrics are given below:

Table 4: Evaluation analysis of security analysis

Method	Encryption Time (ms)	Decryption Time (ms)	Security Level Analysis	DCR (%)	DIR (%)
NTM-LEACH-RSA [24]	10	15	46	96	98
c-RSA-AES [25]	8	12	57	98	99
SMOFCM [26]	6	10	70	92	95
AES-ECC [27]	5	8	67	99	99.5
EST-SGCMSAN (Proposed)	**7**	**11**	**90**	**97**	**98**

The table 4 presents a comparative analysis of encryption methods used in Wireless Sensor Networks (WSNs), evaluating key metrics over 0-2000 rounds. NTM-LEACH-RSA exhibits moderate encryption and decryption times of 10 ms and 15 ms, respectively, with a security level analysis score of 46. It achieves a data confidentiality rate (DCR) of 96% and data integrity rate (DIR) of 98%. c-RSA-AES shows improved performance with encryption and decryption times of 8 ms and 12 ms, a security level score of 57, DCR of 98%, and DIR of 99%. SMOFCM demonstrates faster processing times (6 ms encryption, 10 ms decryption) and a higher security score of 70, with DCR at 92% and DIR at 95%. AES-ECC achieves the fastest times (5 ms encryption, 8 ms decryption), a security score of 67, and high DCR and DIR rates of 99% and 99.5%, respectively. The proposed EST-SGCMSAN method offers competitive encryption and decryption times (7 ms and 11 ms), a robust security score of 90, and balanced DCR (97%) and DIR (98%) rates, highlighting its efficiency and effectiveness in ensuring secure data transmission in WSNs.

4.4 Statistical Analysis

The statistical analysis of proposed method compared with existing methods with 100 nodes and 200 nodes are analysed here.

Table 5: Statistical analysis of proposed and existing methods for 100 nodes

Metrics	Best	Worst	Mean	Median	STD
RLBEEP [16]	0.001	0.583	0.226	0.174	0.185
BWO-EECM [17]	0.006	0.579	0.228	0.171	0.264
DRL [18]	0.005	0.586	0.231	0.176	0.846
GWO [19]	0.005	0.581	0.225	0.179	0.472
EAHA [20]	0.007	0.578	0.235	0.172	0.322
EAEDA-DR [21]	0.004	0.584	0.223	0.181	0.647
E-FUCA [22]	0.006	0.593	0.229	0.178	0.826
BSO-LD [23]	0.008	0.591	0.224	0.174	
NTM-LEACH-RSA [24]	0.005	0.578	0.236	0.177	0.633
c-RSA-AES [25]	0.007	0.581	0.233	0.178	0.738
SMOFCM [26]	0.007	0.586	0.231	0.175	0.372
AES- ECC [27]	0.008	0.579	0.227	0.179	0.864
EST-SGCMSAN (proposed)	0.009	0.575	0.237	0.182	0.926

Table 5 shows the Statistical analysis of proposed and existing methods for 100 nodes. The proposed method is EST-SGCMSAN and the existing methods are RLBEEP [16], BWO-EECM [17], DRL [18], GWO [19], EAHA [20], EAEDA-DR [21], E-FUCA [22], BSO-LD [23], NTM-LEACH-RSA [24], c-RSA-AES [25], SMOFCM [26] and AES- ECC [27]. The proposed EST-SGCMSAN method attains the Statistical best is 0.009, worst is 0.575, mean is 0.237, Median is 0.182 and STD is 0.926. The above table illustrates that the performance of the proposed method gives better performance as compared to the other existing methods.

Table 6: Statistical analysis of proposed and existing methods for 200 nodes

Metrics	Best	Worst	Mean	Median	STD
RLBEEP [16]	0.002	0.572	0.226	0.182	0.896
BWO-EECM [17]	0.007	0.575	0.228	0.189	0.796
DRL [18]	0.006	0.583	0.231	0.191	0.845
GWO [19]	0.006	0.581	0.225	0.182	0.785
EAHA [20]	0.008	0.584	0.235	0.188	0.746
EAEDA-DR [21]	0.005	0.578	0.223	0.175	0.847
E-FUCA [22]	0.007	0.584	0.229	0.192	0.637
BSO-LD [23]	0.007	0.581	0.224	0.182	0.723
NTM-LEACH-RSA [24]	0.006	0.574	0.236	0.174	0.846
c-RSA-AES [25]	0.006	0.583	0.233	0.184	0.734
SMOFCM [26]	0.007	0.579	0.231	0.183	0.826
AES- ECC [27]	0.003	0.571	0.227	0.174	0.478
EST-SGCMSAN (proposed)	0.009	0.569	0.235	0.194	0.983

Table 6 shows the Statistical analysis of proposed and existing methods for 200 nodes. The proposed method is EST-SGCMSAN and the existing methods are RLBEEP [16], BWO-EECM [17], DRL [18], GWO [19], EAHA [20], EAEDA-DR [21], E-FUCA [22], BSO-LD [23], NTM-LEACH-RSA [24], c-RSA-AES [25], SMOFCM [26] and AES- ECC [27]. The proposed EST-SGCMSAN method attains the Statistical best is 0.009, worst is 0.569, mean is 0.235, Median is 0.194 and STD is 0.983. The above table illustrates that the performance of the proposed method gives better performance as compared to the other existing methods.

5 Conclusion

In this manuscript, a Multi-objective CH selection with Scheduling based energy efficient secure transmission in WSN using Siamese graph convolutional Mantis Search attention network (EST-SGCMSAN) is proposed. Initially, the cluster head is selected using the novel multi-objective CH selection strategy using the RPASOA, designed to minimize energy usage and reduce transmission delay. Furthermore, an advanced sleep scheduling mechanism with duty cycling is introduced, leveraging a SGCMSAN for reliable and energy-efficient scheduling. To address the security challenges inherent in sensor nodes, which often face constraints in processing power, storage, and energy, an AES-based signature generation approach utilizing WBC is implemented. This method ensures secure data transmission while maintaining low computational overhead. The proposed system aims to significantly extend the

network lifetime of WSNs through optimized CH selection, efficient scheduling, and robust security measures. The experimental simulations are done with the help of python platform. The results show that the introduced approach performs better than previous approaches in a number of performance measures, Higher throughput 98%, higher packet delivery ratio 0.993%, less energy consumption 0.40mJ. This indicates the approach's superior efficiency and potential for further development in the field. Future work includes exploring adaptive algorithms for dynamic cluster head adjustment, integrating machine learning for energy optimization, enhancing security with anomaly detection, and validating scalability in diverse conditions. These efforts aim to advance energy-efficient and secure data transmission in Wireless Sensor Networks, ensuring robustness and reliability in practical applications.

References

[1] Vijayalakshmi, S., Kavithaa, G., & Kousik, N. V. (2023). Improving Data Communication of Wireless Sensor Network Using Energy Efficient Adaptive Cluster-Head Selection Algorithm for Secure Routing. *Wireless Personal Communications*, *128*(1), 25-42.

[2] Feng, W., Wang, F., Xu, D., Yao, Y., Xu, X., Jiang, X., & Zhao, M. (2020). Joint energy-saving scheduling and secure routing for critical event reporting in wireless sensor networks. *IEEE Access*, *8*, 53281-53292.

[3] Thomas, D., Shankaran, R., Orgun, M. A., & Mukhopadhyay, S. C. (2021). Sec 2: A secure and energy efficient barrier coverage scheduling for wsn-based iot applications. *IEEE Transactions on Green Communications and Networking*, *5*(2), 622-634.

[4] Bharathi, R., Kannadhasan, S., Padminidevi, B., Maharajan, M. S., Nagarajan, R., & Tonmoy, M. M. (2022). Predictive Model Techniques with Energy Efficiency for IoT-Based Data Transmission in Wireless Sensor Networks. *Journal of Sensors*, *2022*(1), 3434646.

[5] Karthick, G. S. (2023). Energy-aware reliable medium access control protocol for energy-efficient and reliable data communication in wireless sensor networks. *SN Computer Science*, *4*(5), 449.

[6] Gulganwa, P., & Jain, S. (2022). EES-WCA: energy efficient and secure weighted clustering for WSN using machine learning approach. *International Journal of Information Technology*, *14*(1), 135-144.

[7] Mishra, S. D., & Verma, D. (2024). Energy-Efficient and Reliable Clustering with Optimized Scheduling and Routing for Wireless Sensor Networks. *Multimedia Tools and Applications*, 1-27.

[8] Hemanth Kumar, G., Ramesh, G. P., & Ravindra Murthy, C. (2021). Energy efficient multi-hop routing techniques for cluster head selection in wireless sensor networks. *Further Advances in Internet of Things in Biomedical and Cyber Physical Systems*, 3-9.

[9] Dattatraya, K. N., & Rao, K. R. (2022). Hybrid based cluster head selection for maximizing network lifetime and energy efficiency in WSN. *Journal of King Saud University-Computer and Information Sciences*, *34*(3), 716-726.

[10] Chauhan, V., & Soni, S. (2020). Mobile sink-based energy efficient cluster head selection strategy for wireless sensor networks. *Journal of Ambient Intelligence and Humanized Computing*, *11*(11), 4453-4466.

[11] Rabie, A.H., Saleh, A.I. and Mansour, N.A., 2023. Red piranha optimization (RPO): a natural inspired meta-heuristic algorithm for solving complex optimization problems. *Journal of Ambient Intelligence and Humanized Computing*, *14*(6), pp.7621-7648.

[12] Yuan, Y., Ren, J., Wang, S., Wang, Z., Mu, X. and Zhao, W., 2022. Alpine skiing optimization: A new bio-inspired optimization algorithm. *Advances in Engineering Software*, *170*, p.103158.

[13] Nimitha, N., Ezhumalai, P. and Chokkalingam, A., 2024. Optimizing Chromosome Analysis through VGT-MS: Leveraging Visual Geometric Transformer, VGG-16, and Vision Transformer for Enhanced Abnormality Identification.

[14] Moustafa, G., Alnami, H., Hakmi, S.H., Shaheen, A.M., Ginidi, A., Elshahed, M. and Mansour, H.S., 2023. A Novel Mantis Search Algorithm for Economic Dispatch in Combined Heat and Power Systems. *IEEE Access*.

[15] Shukla, P.K., Aljaedi, A., Pareek, P.K., Alharbi, A.R. and Jamal, S.S., 2022. AES based white box cryptography in digital signature verification. *Sensors*, *22*(23), p.9444.

[16] Pandiyaraju, V., Ganapathy, S., Mohith, N., & Kannan, A. (2023). An optimal energy utilization model for precision agriculture in WSNs using multi-objective clustering and deep learning. *Journal of King Saud University-Computer and Information Sciences*, *35*(10), 101803.

[17] Pal, R., Saraswat, M., Kumar, S., Nayyar, A., & Rajput, P. K. (2024). Energy efficient multi-criterion binary grey wolf optimizer based clustering for heterogeneous wireless sensor networks. *Soft Computing*, *28*(4), 3251-3265.

[18] Wilson, A. J., Kiran, W. S., Radhamani, A. S., & Bharathi, M. P. (2024). Optimizing Energy-Efficient Cluster Head Selection in Wireless Sensor Networks using a Binarized Spiking Neural Network and Honey Badger Algorithm. *Knowledge-Based Systems*, 112039.

[19] Xing, P., Zhang, H., Ghoneim, M. E., & Shutaywi, M. (2023). UAV flight path design using multi-objective grasshopper with harmony search for cluster head selection in wireless sensor networks. *Wireless Networks*, *29*(2), 955-967.

[20] Sharma, A., & Kansal, A. (2024). Enhanced CH selection and energy efficient routing algorithm for WSN. *Microsystem Technologies*, 1-13.

[21] Mistarihi, M. Z., Bany Salameh, H. A., Alsaadi, M. A., Beyca, O. F., Heilat, L., & Al-Shobaki, R. (2023). Energy-efficient bi-objective optimization based on the moth–flame algorithm for cluster head selection in a wireless sensor network. *Processes*, *11*(2), 534.

[22] Srivastava, A., & Mishra, P. K. (2022). Multi-attributes based energy efficient clustering for enhancing network lifetime in WSN's. *Peer-to-Peer Networking and Applications*, *15*(6), 2670-2693.

[23] Verma, V., & Jha, V. K. (2024). Secure and energy-aware data transmission for IoT-WSNs with the help of cluster-based secure optimal routing. *Wireless Personal Communications*, *134*(3), 1665-1686.

[24] Dinesh, K., & Santhosh Kumar, S. V. N. (2024). Energy-efficient trust-aware secured neuro-fuzzy clustering with sparrow search optimization in wireless sensor network. *International Journal of Information Security*, *23*(1), 199-223.

[25] Misbha, D. S. (2023). Lightweight key distribution for secured and energy efficient communication in wireless sensor network: An optimization assisted model. *High-Confidence Computing*, *3*(2), 100126.

[26] Lilhore, U. K., Simaiya, S., Dalal, S., Sharma, Y. K., Tomar, S., & Hashmi, A. (2024). Secure WSN Architecture Utilizing Hybrid Encryption with DKM to Ensure Consistent IoV Communication. *Wireless Personal Communications*, 1-29.

[27] Chandrika M. Dixit, Manjima , R.L., & Dr. Jitendranath Mungara, (2012). Modified Long Lifetime Routing in Unreliable Wireless Sensor Networks. Original Research Articles, 23-28.

[28] Geetha, S., Shilpa Pande, Deepalakshmi, P., Sheetal , R., (2019). Patient Monitoring System with Miniaturization of Sensors. International Journal of Engineering and Advanced Technology (IJEAT), 495-501.

[29] Shwetha, G.K., Mrs. Sagarika Behera, Dr. Jithendranath Mungara, (2012). Energy-Balanced Dispatch of Mobile Sensors in Hybrid Wireless Sensor Network with Obstacles. IOSR Journal of Computer Engineering (IOSRJCE), 47-51.