ISSN 0315-3681 Volume 122 (2), 2025

AUGMENTED Q-LEARNING-BASED ARTIFICIAL BEE COLONY ALGORITHMS IN WIRELESS SENSOR NETWORKS LEVERAGING DEEP LEARNING FOR ENERGY OPTIMIZATION

R. SUDHAKAR[1], P. SRIMANCHARI[2]

[1]Ph.D, Research Scholar, PG and Research Department of Computer Science, Erode arts and science College(Autonomous), Erode, Tamilnadu, India. Email: sudhakartamil699@gmail.com

[2]Assistant Professor of Computer Science, PG and Research Department of Computer Science, Erode arts and science College (Autonomous), Erode, Tamilnadu, India. Email: srimanchari@gmail.com

ABSTRACT

Routing with multiple hops is employed by Wireless Sensor Networks (WSNs) to facilitate efficient data transfer; yet, Use of energy is still a significant issue for maintaining dependable connectivity. Minimizing energy consumption and enhancing network interactions are crucial for the sustained viability of wireless sensor networks (WSNs). Limitations on energy impede the efficacy of data's sensor nodes (SNs) Transmission throughout the network, not withstanding the benefits of multiple-hop routing. The difficulty is in identifying the best strategy to reduce the amount of energy utilize while preserving dependable data transfer. We proposed an ideal approach when choosing a Cluster Head (CH) in Wireless Sensor Networks (WSNs)utilizing an enhanced Algorithm for Artificial Bee Colonies (IQ-ABC) based on Q-learning to enhance multi-hop routing's effectiveness in WSNs. This study introduces an augmented ABC algorithm that incorporates Q-learning to improve the stages of Investigating and exploiting. The exploitative capacity of the IQ-ABC is enhanced by an altered Q-learning process. The IQ-ABC approach recognises the optimal energy-efficient route aimed at each sensor node to communicate data to the collection inside the suggested system. Additionally, a multi-objective fitness function enhances the selection of cluster heads through weighted assignment utilizing fuzzy logic, balancing critical factors like as trust, latency as well as energy efficiency. The simulation findings indicate that, relative to traditional routing algorithms, the IQ- ABC technique greatly lowers energy usage besides helps to enhance the longevity of nodes for sensors. The paper concludes by emphasizing the necessity of optimizing computer resources to sustain how well machine learning works techniques in detecting abnormalities in the network. This paper examines the innovative incorporation of deep learning applications in the deployment of Networks of Wireless Sensors(WSN).

Keywords: Improved Queue Learning, Artificial Bee Colony, Deep learning algorithm, Anomaly Detection, Wireless sensor network, Energy-intensive computations.

I. INTRODUCTION

New developments in wireless technology as well as hardware have made it possible the creation of economical, energy-efficient small gadgets referred to as sensors, capable of brief-range communication via a wireless network. A Wireless Sensor Network (WSN) comprises many sensors that collaborate to accomplish designated tasks [1]. Due to its numerous applicability in Internet of Things (IoT) contexts, Wireless Sensor Networks (WSNs) have recently garnered significant attention from scholars besides of the industry entities WSNs, or wireless sensor networks, are used in forest fire warning prevention systems, wildlife monitoring, in addition environmental surveillance, among other applications. WSNs, or wireless sensor networks, are utilized in applications for smart cities like traffic besides of the air quality systems for monitoring, military in addition to residential surveillance systems, as well as marine environmental surveillance systems. The main purpose is to observe the WSN besides to identify occurrences inside the specified objectives as well as barriers. Monitoring or tracking events by include crucial objectives while preserving dependable network connectivity is Among the core difficulties of Wireless Sensor Networks (WSNs).

The literature addresses many coverage challenges, include barrier coverage, target coverage, and area coverage [3]. Sensors are deployed by either a deterministic or stochastic strategy to establish the wireless network. A stochastic deployment strategy is essential in hostile or inaccessible human environments. A deterministic or grid deployment strategy is necessary for the positioning of sensors in predetermined locations [5]. Due to the irregular distribution of sensors during random deployment, certain areas are sparse while others are notably dense. In congested regions, diverse sensor signals interact with each other during data detection in addition to transmission. Signal interference in wireless media significantly contributes to the quick energy depletion in wireless sensor networks (WSN). Throughout the data transmission phase, signal interfering sources

message dropouts, requiring message resends. WSNs' efficiency in using energy is consequently compromised. To ensure network connectivity as well as coverage of all target points. During deployment, minimizing node interference is crucial. Numerous clustering methodologies have been suggested to achieve energy conservation in networks of wireless sensors (WSNs). Clusters are created within the network during the clustering procedure [8]. The obligation of gathering data since the fellow collisions of every cluster in addition to communicating it to the dishonourable station is allocated to the collection head.

II. RELATED WORKS

The KDD-99 and CICIDS2018 datasets were used by Kim et al.[14] created a model for identifying DoS assaults using a Convolutional Neural Network (CNN). They transformed the experiment's input data into a "image," which was then fed into the suggested CNN model as either a grayscale or RGB image. During the execution of both binary (normal versus attack) in addition to multiclass classification, different quantities of layers were examined. The planned representations surpassed the Recurrent Neural Network (RNN) ideal in in cooperation binary in addition to multiclass classification upon assessment. Their technique achieved over 99% accuracy in both categories. LSTM and DNN models were proposed by Robin Abraham et al. [17] for the binary prediction of unknown DoS and DDoS attacks. The CICIDS2017 dataset was utilized to train these models. To assess the efficacy of their proposed models, the authors subsequently developed a novel dataset for testing, ANTS2019, within a simulated environment. The recommended DNN methodology, once trained on the CICIDS2017 in addition to a section of the ANTS2019 dataset, accomplished an accuracy of 99.68%. To identify four distinct types of security assaults, Lee et al. [15] evaluated the accuracy, precision, recall, in addition to the F1 score of three algorithms: DNN, STL Approach, as well as RNN. The algorithms were trained in addition to an evaluated independently utilizing the KDD as well as NSL-KDD datasets. The LSTM model's accuracy of 79.20% was surpassed by the STL approach's 98.9% accuracy. LuNet is a hierarchical neural network that integrates CNN as well as RNN architectures, as described by Waug et al. [20]. It consists of several CNN as well as RNN layers, wherein the two networks collaborate to extract knowledge from the input data. The NSL-KDD in addition to UNSW-NB15 datasets were employed to evaluate the proposed model [10]. In addition to achieved a max accuracy of 99.05% for multiclass classification and 99.36% for binary classification.Eight different machine learning models were used by Alagha et al. [11] to detect DoS attacks: Bayesian Networks (BN), Support Vector Machine (SVM), J48, K-Nearest Neighbor (KNN), Random Forests (RF), Decision Trees (DT), Naive Bayes (NB), and Artificial Neural Networks (ANN).They utilized their use of the dataset WSN-DS their experiment in addition to choose attributes utilizing a survey of experts. The writers claim that Compared to the Random Forest algorithm, the ANN model, with a precision of 99.7% and a True Positive rate of 98.3%.

Alertnet-Scale-Hybrid-IDS, a method formulated by Jawad et al. [7], effectively monitors network traffic in addition to the at the host level occurrences in real-time to proactively notify of potential intrusions. Consequent to filtering the model utilizing the KDD-99 dataset, the authors engaged it as a standard aimed at assess mentin contradiction of further datasets, include CICIDS2017, Kyoto, WSN-DS, UNSW-NB15, and NSL-KDD. With the WSN-DS dataset, the binary and multiclass classification accuracies were 99.2% and 98.0%, respectively. Using the WSN-DS dataset, Park and associates . [15] created A classifier called Random Forest (RF)to categorize the different kinds of DoS attacks.

The best F1-scores for attacks known as Blackhole, Flooding, Grayhole, Normal, and Scheduling (TDMA)were 96%, 98%, 100%, and 99%, respectively, for the proposed model. They received a 97.8% rating for overall correctness. Several machine learning classifiers were suggested by Barkhoda et al. [2] as a way to identify intrusions in networks of wireless sensors (WSNs). Furthermore, to decision trees, the classifiers include SVM, Random Forest, and Naive Bayes. The classifier was implemented using the WEKA data mining program, and the WSN-DS dataset was used for training. With an accuracy of 96.7%, the SVM classifier outperformed other classifiers.

III. METHODOLOGY

3.1 Automatic Sensor Reading

WSN assaults can be categorized as either intrusive or non-invasive according to their attributes. The timings, power, in addition to the frequency of the designated

channel are often the subjects of non-invasive attacks. Invasive assaults interrupt information transit, routing, service availability, in addition to the various other functions. The module enterprise to generally deliberate an organisation to establishment inaccessible through accomplishment denial-of-service (DoS) attacks. Conversely, assaults that transpire during information transmission are more prevalent. Routing attacks are frequently executed from within a network. Denial of Service incidents can manifest in various forms. These conditions may hinder the performance of WSN nodes besides of the functionality of the network. These could disrupt the network's normal functioning by showing up as software bugs, resource exhaustion, or other issues with the application or infrastructure.

Any disruption to a network's capacity to deliver a service, it the term "denial of service" (DoS), whether it is temporary or persistent. An attacker who deliberately does this is said to be carrying out "denial of service attacks." An intentional attempt by an adversary to render a network's core architecture inoperable A "denial of service" (DoS) assault is what it is called.

A DDoS, or distributed denial-of-service assault may have a greater effect on network functionality than expected. Denial-of-service attacks in wireless sensor networkscan happen at any OSI model layer. Denial-of-service attacks are susceptible due to their capacity to disrupt the protocols linked to targeted networks. Besides inflicting physical damage on network components, denial-of-service assaults can deplete resources, obliterate alterations to the infrastructure configuration as well as more.

A taxonomy of denial-of-service assaults, organized by layers, was originally established for triage systems addressing emergency abnormal services; however, its efficacy may rapidly diminish as the number of incidents escalates. Enhancing the evaluation of first responders' health during mass-casualty incidents is also crucial. Wireless sensing devices, owing to their enhanced portability, scalability, besides swift deployment at disaster sites, may facilitate the immediate tracking in addition to reporting of first responders' health condition as well as the triage levels of many patients.

3.2 Detection of Anomalies with Deep Learning Method

3.2.1 Deep neural network (DNN)

The ABC algorithm, a meta-heuristic optimization tool, is founded on swarm intelligence. In a swarm system, agents communicate with each other than their Environment. This method entails the agent recognizing the optimal food source, with each agent symbolized by a bee in addition to the food provider consisting of a collection of feasible replies inside the domain of search. An enhanced form of the ABC algorithm is the IQ-ABC algorithm, which incorporates Q-learning techniques to enhance problem-solving effectiveness. Like the ABC algorithm's dependence on swarm intelligence to discover optimal solutions, it lacks exploitative characteristics, perhaps leading to local optima. In contrast, IQ-ABC utilize a Q-table to evaluate besides to adjust the quality of food sources, allowing worker bees to refine solutions based on their past performance. This method enhances solution quality by picking suitable bees as well as integrating variable weight values for more precise modifications.

Moreover, the adaptive mechanism employed by scout bees effectively eliminates inferior solutions, promoting a more exploratory search. The curious in addition to predatory behaviors of bee colonies vary. To avoid a local optimum, a search agent will take exploratory actions, such searching the search space for a new food source. Conversely, exploitative behavior entails pursuing a more advantageous food source near the already available one. This study utilizes Q-learning to enhance our methodology in addition to deliver superior problem-solving solutions. Considering that the ABC algorithm exhibits constrained exploitative as well as strong exploratory characteristics, our aim is to augment exploitative behavior. The original phase, the IQ-ABC algorithm organize the position of the foundation as well as to recommends the possible solutions to the particular concern. Initially, as seen, the food supply is generated randomly. Consequently, food resources are linked to foraging bees. The Q-table commences at a value of zero.

$$x_{i,j}^{0}=x_{j}^{min}+rand(0,1)*(x_{jmax}-x_{j}^{min})\text{----------}\ \textbf{(1)}$$

where x_j^{min} Is the lower bound of the j^{th} optimization parameter, as well as $x_j^{max}$is the j^{th} optimization parameter's upper bound.

The IQ-ABC algorithm in the first stage segregates the process into three distinct stages: the worker bee stage, the spectator bee stage, besides of stage of the scout bee. The three stages of the algorithm are repeated until a certain number of values is attained. Analyze the various facets of deep anomaly detection techniques besides of the classifications of datasets examined.

Biomedical engineering specialists increasingly acknowledge deep learning for its capacity to tackle the aforementioned issues.

A notable feature of deep learning is its capacity to articulate non-linearity. Enhancing non-linearity in the model can more effectively differentiate between normal in addition to anomalous samples, as well as more accurately represent data inconsistencies. A further advantage of deep learning is its capacity to independently acquire features. The abundance of extensive data besides of the enhanced computer capabilities has optimized the hierarchical feature learning process in deep learning, eliminating the necessity for manual development in addition to delineation of anomalous characteristics.

The following weights were determined utilizing the fuzzy membership function: W1, W2, W3, W4, W5, W6, W7, as well as W8. The vitality of the nodule is signified by P, the intra-cluster detachment by X, the D stands for disappearance between two hops, T for transmission delay, X* for cluster detachment, M for linking length, and K for trust model. The following formula is used to calculate the weight.

$$O=W1\times P+W2\times(1-T)+W3\times(1-X*)+W4\times X+W5\times(1-D)+W6\times M+W7\times Xbalance+W8\times K \quad \text{--------(2)}$$

where r, p, as well as q are used to symbolize the triangle membership function's vertices. T(f) Here, P is an acronym for the lower boundary, With a membership worth 1, the middle barrier is denoted by q, and the upper limit by r, which has a subscription value of 0.

3.2.2 Multi-objective objective function

A number of factors are used to evaluate the fitness function in order to identify the optimal result. In addition to the intra-cluster distance, the eight parameters that determine the applicability of the proposed IQ-ABC include the trust model, connection time, distance, energy, inter-cluster distance, latency, and cluster head balance factor. These characteristics guarantee that the directing pathways designated are consistent, protected, as well as energy-efficient. Communication is improved via the trust concept. Security, while Energy variables also prolong the network's operating lifespan of the connection longevity.

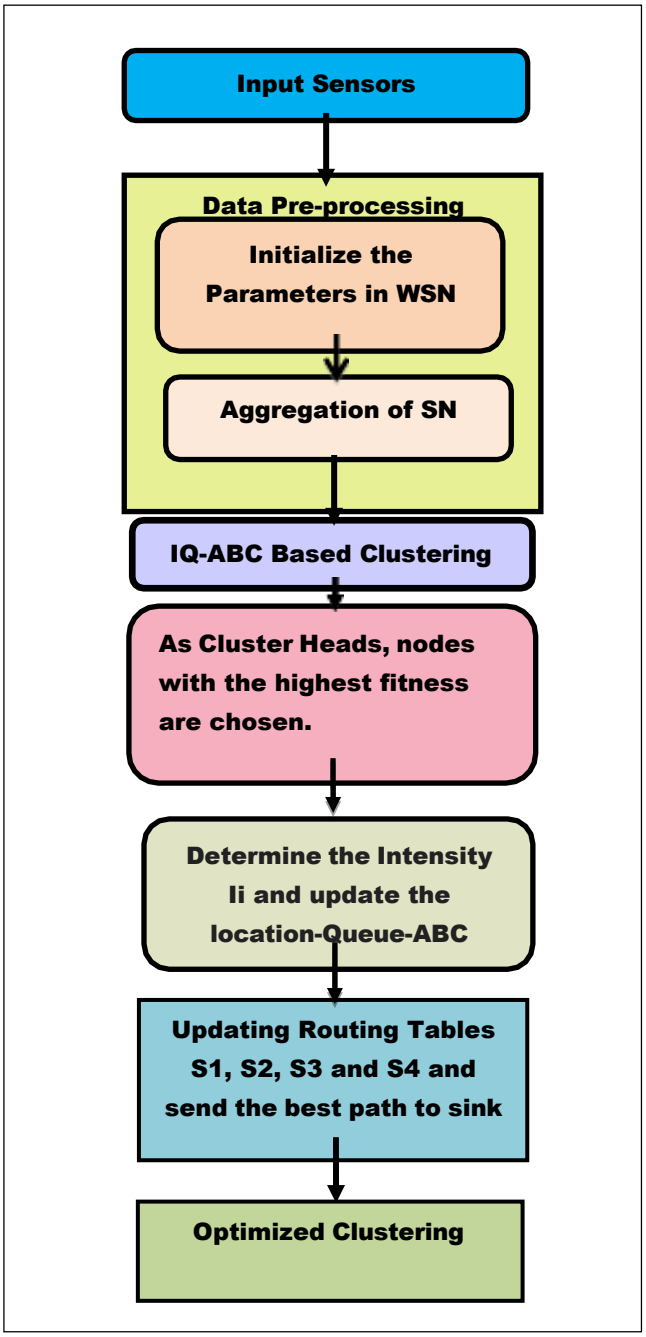

Fig. 3.1 Multi-hop Routing Wireless Sensor Networks IQ-ABC forusing for Optimized Clustering in Deep Learning

Transmission expenditures are minimized by reducing intra- as well as inter-cluster distances, while data delivery is guaranteed to be prompt due to low latency. Additionally, the CH balance factor guarantees that nodes are distributed equally under the burden. The system identifies the most efficient a as well as durable routes by optimizing these parameters. The qualification

purpose is to understood as a expansion function in this occasion.

3.2.3 Proposed IQ-ABC-based multihop routing Encoding of the solutionis essentially a method of expressing the outcome of the IQ-ABC approach as proposed. The optimum data transmission track is the solution. The IQ-ABC approach suggests selecting the most optimal step from the available options when optimizing a WSN. This method is predicated on a fitness function with many objectives that was recently developed. By employing the routing method that minimizes latency, maximizes energy efficiency, assures trust, extends the longevity of connections, also reduces both intra- as well as inter-cluster distances.

BS will transmit a beacon signal to the entire network immediately upon the nodes being situated within the detection zone.To find how far away to the Base Station (BS), each node uses the indicator for received signal strength (RSSI). Because they facilitate efficient network traffic routing with minimal data loss during transmission, the hops that were chosen are CHs. The proposed IQ-ABC approach is modified in this instance to ensure that the optimal path is obtained from the source SN. The routing protocol that has been proposed is based on the IQ-ABC algorithm also is made up of two main parts: I-based clustering and I-based routing. First, there are usually a large number of SNs in a sensing area.

The SNs subsequently transmit a message to a nearby contact to gather information regarding their neighbors. The clustering process commences upon the acquisition of proximate data. Subsequently, the Cluster Heads (CHs) are chosen, in addition to the clusters are accurately arranged via the implementation the IQ-ABC approach. The next stage is to find the best routes within the network by using the routing strategy based on the IQ- ABC algorithm. Network lifespan is increased by the suggested IQ-ABC-based routing strategy besides of energy efficiency by leveraging the benefits of clustering as well as routing.

Cluster Heads (CHs) are then chosen. Subsequently, the optimal channels within the network are determined by employing the routing method based regarding the IQ- ABC algorithm. By utilizing the advantages of clustering in addition to the routing. The suggested routing protocol based on IQ-ABC improves the energy efficiency besides of the longevity of the network. Nodes for sensors are the fundamental components of Wireless Sensor Networks (WSNs).

Algorithm of IQ-ABC Multi-hop Routing for using for Optimized Clustering in Deep Learning

Step 1:	***Sensing Area with N Sensor Nodes (SN) as the input***
Step 2:	***Station Base (BS)***
Step 3:	***Set up the sensing area's SNs and broadcast the base station beacon signal.***
Step 4:	***Do for every SN in SNs***
Step 5:	***Distance_to_BS (SN) CALCULATE_RSSI (SN, BS)***
Step 6:	***Neighbours[SN] -- DISCOVER _NEIGHBORS (SN)***
Step 7:	***def objective_function(x): return sum([xi**2 for xi in x]).***
Step 8:	***bee colony made up of employed bees, onlooker bees, and scout bees***
Step 9:	***Randomly initialize the position of the bee agents in the solution space representing the sensor nodes***
Step 10:	***For { {i in range(pop_size): if random.random()< probabilities[i]:***
Step 11:	***Evaluate the new solution using the defined fitness function. Q-table update***
Step 12:	***if random.random() < probabilities[i]: neighbor= get_neighbors(population[i], bounds) neighbor_fitness= func(neighbor)***
Step 13:	***best_index= fitness.index(min(fitness)) returnpopulation[best_index], fitness[best_index]***
Step 14:	***Optimized Clustering***
Step 15:	***End***

3.2.4 Sensor Nodes

Subsequently, the SNs transmit a message to a contact in the vicinity in order to collect information about their surroundings. The acquisition of proximate data initiates the clustering process. In addition to the clusters being properly arranged using the IQ-ABC approach, the These nodes are energy-limited, compact, as well as cost-effective devices that wirelessly connect to other nodes within the network, process data, besides detect physical attributes. The distributed architecture Sensor nodes that gather, process, and send data to a base station or sink node for additional analysis make up Wireless Sensor Networks (WSNs). Sensor nodes are the building blocks of wireless sensor networks, which enable the accumulation, processing, in addition to transfer of data for a variety of applications. Their design prioritizes energy efficiency, reliable communication, and the optimization of data quality. Despite obstacles such as power besides bandwidth limitations, sensor nodes are essential in a variety of applications, including industrial as well as environmental monitoring, healthcare, in addition to smart cities. In order to satisfy the requirements of contemporary Wireless Sensor Networks (WSNs), sensor nodes are consistently improving by incorporating energy-efficient protocols, low-power technologies, besides miniaturization techniques.

3.2.5 Data set

CICDoS 2019 incorporates both benign besides prevalent DDoS attacks. This record is generated using actual traffic in addition it includes a variety of DDoS attacks that were conducted utilizing TCP/UDP protocols. Exploit-based then reflection-based attacks are included in taxonomy attacks.

The following are examples of reflection-based attacks: Trivial File Transfer Protocol (TFTP), CharGen, Lightweight Directory Access Protocol (LDAP), Simple Network Management Protocol (SNMP), Domain Name System (DNS), Microsoft SQL Server (MSSQL), Network Time Protocol (NTP), Simple Service Discovery Protocol (SSDP), and network Basic Input/Output System (NETBIOS), in addition to PortMap. In addition to SYN Flood, these attacks are exploit-based which involve UDP Flood as well as UDPLag.

During the training day, twelve DDoS assaults were conducted, including Additional to SYN are DNS, LDAP, NTP, MSSQL, UDP, UDP-Lag, NetBIOS, SNMP, SSDP, WebDDoS, and TFTP. PortScan, LDAP, UDP, UDPLag, MSSQL, NetBIOS, and SYN are all included in the Test Day, which was recorded on January 12, 2019 [13]. Deep learning methodologies for the detection of DoS as well as DDoS attacks utilizing the CICDDoS2019 dataset, as well as their respective accuracies.

Fusion Layer

FL for Collaborative Learning introduces a novel approach to model training as well as data utilization. Intellectual property in addition to personal information security are of the utmost importance in the semiconductor manufacturing production process. FL enhances privacy by enabling industrial entities to train models independently of one another, utilizing multiple datasets to facilitate advanced learning, in addition to refraining from exchanging raw data. Promoting the Function of Human Oversight Expert human intervention is indispensable for semiconductor quality assurance. XAI facilitates the connection between intelligent individuals in addition to AI simulations. Professionals may more effectively evaluate the model's logic in addition to determine whether the results align with their expectations in addition to actual knowledge with the assistance of XAI.

IV. RESULTS AND DISCUSSIONS

Over multiple rounds, the IQ-ABC method provides an exhaustive. A comparison of performance indicators among the procedures IQ-ABC, LEACH, HEED, and PSO.

Table.1.1 Comparison table of IQ-ABC Multi-hop Routing for using for Optimized Clustering in Deep Learning

Methods/ Metrics	CS	DS	ACY
PSO	92.31	92.19	92.38
LEACH	92.26	92.11	92.69
HEED	94.14	93.71	93.65
IQ-ABC	94.42	94.82	94.51

The average residual energy for each procedure is shown in Table 4.1. As the number of cycles grows, it falls from 0.41 to 0 for LEACH, 0.39 to 0 for 0.45 to 0 for IQ-ABC, 0.4 to 0 for PSO, and HEED. The highest energy levels are continuously displayed by IQ-ABC. The residual energy standard deviation, which is shown in Figure 4.1, decreases from 0.24 to 0 for LEACH, 0.18

to 0 for HEED, 0.12 to 0 for IQ-ABC and 0.19 to 0 for PSO. This data suggests that PSO in addition to IQ-ABC have more consistent energy consumption as well as reduced deviations.This represents the quantity of iterations or cycles that the algorithm performs before it reaches a solution. To achieve an optimal solution, it is necessary to perform fewer iterations due to a rapid convergence rate. The current solution's proximity to the optimal solution is indicated by the value of the goal function at each iteration. The objective function value's rate of convergence can be evaluated by observing the rate at which it decreases or stabilizes over time.

$$Convergence\ Speed = \frac{F(x0-fq)}{t} \quad \text{--------(3)}$$

- The initial objective function value (f(x0)) is typically at the starting point or the first iteration.
- The optimal objective function value is f∗.
- The number of iterations (or function evaluations) is t.

This formula assumes that the objective function's value decreases steadily as the algorithm approaches the ideal answer. The distribution or diversity of the population of candidate solutions across the search space is represented by diversity in optimization methods, such as the IQ-ABC algorithm. It is crucial to maintain diversity in order to prevent the algorithm from prematurely convergent to suboptimal answers b ensuring the exploration of a variety of regions withi the search space.

The Euclidean distance among solutions within the population is a widely utilized metric for evaluating diversity. The following formula can be utilized to ascertain the diversity of a population of N solutions, denoted as {x1, x2, ..., xN}.

$$D_{min} = min_{ij} \, || x_i - x_j || \text{ ---------- } \textbf{(4)}$$

Accuracy is the degree to which the algorithm's solution is in close proximity to the optimal or true solution in optimization algorithms, such as IQ-ABC as well as other heuristic methods. Accuracy is quantifiable through a variety of methods that are dependent on the specific problem. However, in the majority of optimization scenarios, it is defined as the relative error between the derived in addition to the optimal solutions. The choice of three different scenarios of testing for the evaluation of The routing system based on IQ-ABC technique in wireless sensor networks (WSNs) is motivated by the need to thoroughly Examine the algorithm's effectiveness across different arrangements of the space of the base station (BS).An objective of the investigation is to elucidate the influence of where the BS on efficiency is located in addition to effectiveness of the routing strategy by means of scenario simulations. The experimental design consisted of a comparative analysis of the suggested IQ-ABC approach against established techniques, including HEED, LEACH, the Low-Energy Adaptive Clustering Hierarchy, and the Artificial Bee Colony (ABC) algorithm in addition to Particle Swarm Optimization (PSO).

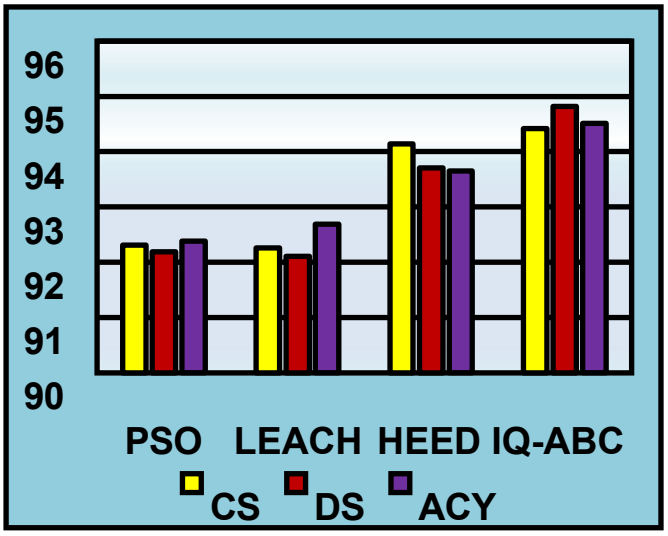

Fig.4.1 Comparison chart for IQ-ABC Multi-hop Routing for using for Optimized Clustering in Deep Learning

The highest residual energy levels are regularly shown by IQ-ABC, which starts at about 0.45J in addition to settling at approximately 0.03 J after 5000 cycles. The variability is reduced from 0.11 J to 0.03 J. It exhibits the best. The number of data packets received increased from 70 at 500 rounds to 5800 at 5000 rounds and the highest node survivability, 15 nodes at 5000 rounds, compared to 97 nodes after 500 rounds. These results emphasize IQ-ABC's reliability in enhancing data transmission performance and extending the lifespan of networks.

V. CONCLUSION

In comparison to existing procedures, the IQ-ABC algorithm demonstrates substantial improvements in data transmission and energy efficiency. Compared to conventional routing algorithms, the IQ-ABC technique significantly lowers energy consumption and increases

the lifespan of sensor nodes, as indicated by the simulation findings. The IQ-ABC optimization technique is implemented in the proposed model to extend the network's lifecycle and improve Several-hop routing. The IQ-ABC method conserves the energy of sensor nodes endowed with non-rechargeable batteries by optimizing data packet routing to achieve the minimal number of hops and selecting efficient cluster heads, thereby reducing energy consumption. The network's dependability, speed, and latency are all suitably assessedby the proposed multi-objective fitness function, which consists of eight factors. Also, the security-conscious routing that incorporates the trust model addresses the concerns and guarantees the security of data transmission. The study's findings suggest that the proposed model substantially enhances the volume of incoming data packets in the WSN, thereby illustrating the efficacy of the approach provided. This work's useful contributions are considerable, as the proposed approach is efficient and flexible across a variety of domains, such as industrial automation, pollution tracking, smart cities, and more purposes. The network is rendered more dependable and sustainable as a result of the enhancements in privacy and energy consumption of Wireless Sensor Networks (WSNs), which in turn reduce operational costs and increase service reliability.

REFERENCES

[1] A. Alagha, R. Mizouni, J. Bentahar, H. Otrok and S. Singh, "Multiagent Deep Reinforcement Learning With Demonstration Cloning for Target Localization," in IEEE Internet of Things Journal, vol. 10, no. 15, pp. 13556-13570, 1 Aug.1, 2023, doi: 10.1109/JIOT.2023.3262663.

[2] F. Afianti and T. Suryani, "Lightweight and DoS resistant multiuser authentication in wireless sensor networks for smart grid environments", IEEE Access, vol. 7, pp. 67107-67122, 2019.

[3] A.H. Bagdadee, M.Z. Hoque and L. Zhang, "IoT based wireless sensor network for power quality control in smart grid", Procedia computer science, vol. 167, pp. 1148-1160, 2020.

[4] Barkhoda, W., & Sheikhi, H. (2020). Immigrant imperialist competitive algorithm to solve the multi-constraint node placement problem in target-based wireless sensor networks. Ad Hoc Networks, 106, 102183.

[5] Chakraborty, S., Goyal, N. K., Mahapatra, S., & Soh, S. (2020). Minimal path-based reliability model for wireless sensor networks with multistate nodes. IEEE Transactions on Reliability, 69, 382–400.

[6] Chandnani N, Khairnar CN (2022 Sep) An analysis of architecture, framework, security and challenging aspects for data aggregation and routing techniques in IoT WSNs. Theor Comput Sci 11(929):95–113.

[7] Haseeb, K., Almustafa, K.M., Jan, Z., Saba, T. and Tariq, U., 2020. Secure and energy - aware heuristic routing protocol for wireless sensor network. IEEE Access, 8, pp.163962- 163974.

[8] Jawad MA, Khurshid F (2021) A review of approaches to energy aware multi-hop routing for lifetime enhancement in wireless sensor networks. In: Proceedings of the international e-conference on intelligent systems and signal processing: e-ISSP 2020. Springer Singapore, Singapore, pp 739–757

[9] Jayalakshmi P, Sridevi S, Janakiraman S (2021) A hybrid artificial bee colony and harmony search algorithm-based metahueristic approach for efficient routing in WSNs. Wirel Pers Commun 121(4):3263– 3279

[10] Jeske M, Rosset V, Nascimento MC (2020) Determining the trade-offs between data delivery and energy consumption in large-scale WSNs by multi-objective evolutionary optimization. ComputNetw 179:107347

[11] Goud, B. & Anitha, R (2023). Emerging Routing Method Using Path Arbitrator in Web Sensor Networks. International Journal on Recent and Innovation Trends in Computing and Communication, 11(4), 232–237. https://doi.org/10.17762/ijritcc.v11i4.6444

[12] Gokalp O (2022) improved artificial bee Colony algorithm with adaptive pursuit based strategy selection. In: Handbook of nature-inspired optimization

algorithms: the state of the art: volume I: solving single objective bound-constrained real-parameter numerical optimization problems. Springer International Publishing, Cham, Pp: 91–115

[13] Guo R, Li H, Yan M, Zhang Y, Guo P. Efficient routing algorithms for maximizing network lifetime in chain-type wireless sensor networks using multiple sinks. In Third International Conference on Green Communication, Network, and Internet of Things (CNIoT 2023) 2023 Oct 20 (Vol. 12814, pp. 120–128). SPIE

[14] J. Lee, S. Yu, M. Kim, Y. Park and A.K. Das, "On the design of secure and efficient three-factor authentication protocol using honey list for wireless sensor networks", IEEE Access, vol. 8, pp. 107046- 107062, 2020.

[15] Majid M, Habib S, Javed AR, Rizwan M, Srivastava G, Gadekallu TR, Lin JC (2022) Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: a systematic literature review. Sensors 22(6):2087

[16] Naik, C., & Shetty, D.P. (2020). Intelligent interference minimization algorithm for optimal placement of sensors using bbo. In Soft computing: theories and applications (pp. 955–969). Springer.

[17] Naik, C., & Shetty, P. D. (2022). Flag: Fuzzy logic augmented game theoretic hybrid hierarchical clustering algorithm for wireless sensor networks. Telecommunication Systems, 79(4), 559–571.

[18] Panchal, A., & Singh, R. K. (2021). Ehcr-fcm: Energy efficient hierarchical clustering and routing using fuzzy c-means for wireless sensor networks. Telecommunication Systems, 76(2), 251–263.

[19] H. Radhappa, L. Pan, J. Xi Zheng and S. Wen, "Practical overview of security issues in wireless sensor network applications", International journal of computers and applications, vol. 40, no. 4, pp. 202-213, 2018.

[20] Robin Abraham and M. Vadivel. 2023. An energy efficient wireless sensor network with Flamingo search algorithm based cluster head selection. Wireless Pers. Commun. 130 (April2023), 1503–1525.