International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2025/56 Volume 12, Issue 6, November – December (2025)

RESEARCH ARTICLE

Enhancing Security in Underwater Wireless Sensor Networks using a Hybrid Approach of Beetle Antenna Search and Genetic Algorithms

Suganya J
Department of Computer Applications, SRM Institute of Science and Technology, Tiruchirappalli, Tamil Nadu, India.
suganyajeya2011@gmail.com

Senthil Kumar S
Department of Computer Applications, SRM Institute of Science and Technology, Tiruchirappalli, Tamil Nadu, India.
✉ szenthilkumar@gmail.com

Prakash M
Department of Artificial Intelligence and Data Science, VET Institute of Arts and Science (Co-education) College, Erode, Tamil Nadu, India.
drmprakashphd@gmail.com

Akilandeswari S
Department of Artificial Intelligence and Data Science, E.G.S Pillai Engineering College, Nagapattinam, Tamil Nadu, India.
akila.sritharan@gmail.com

Anitha P
Department of Computer Science, Thiru. Vi. Ka Govt Arts College, Thiruvarur, Tamil Nadu, India.
anithanimmi@gmail.com

Paul Arokiadass Jerald M
Department of Computer Science, Periyar Arts College, Cuddalore, Tamil Nadu, India.
mjerald@gmail.com

Received: 01 August 2025 / Revised: 25 October 2025 / Accepted: 02 December 2025 / Published: 30 December 2025

Abstract – The increasing use of Underwater Wireless Sensor Networks (UWSNs) for applications such as water level monitoring, offshore exploration, and environmental tracking necessitates robust security mechanisms. UWSNs face unique challenges, including limited bandwidth, constrained energy resources, high signal attenuation, multipath propagation, and harsh environmental conditions, which make conventional security techniques less effective. This study proposes a novel hybrid security algorithm combining Beetle Antenna Search (BAS) and Genetic Algorithms (GA) to address these challenges. BAS offers efficient exploration inspired by beetle foraging behavior, while GA provides evolutionary optimization of security parameters. The hybrid BAS-GA approach ensures adaptive, robust, and energy-efficient security, capable of mitigating underwater threats such as jamming, eavesdropping, and node compromise. Simulation results demonstrate that the proposed method outperforms existing techniques, improving security performance while minimizing resource consumption. This research advances tailored security solutions for UWSNs, enabling more reliable and resilient underwater communication systems.

Index Terms – Underwater Wireless Sensor Networks, Security Enhancement, Beetle Antenna Search, Genetic Algorithms, Intrusion Detection, Underwater Communication, Network Security.

RESEARCH ARTICLE

1. INTRODUCTION

Wireless Sensor Networks (WSNs) are made of wireless self-configured nodes, which do not depend on a fixed wireless infrastructure. They are employed to check the environmental parameters e.g. pressure and temperatures. The perceived information is then sent out of the source to the destination to be analyzed. The destination which is also called the sink is a base station of the network and network users as well. The units are battery operated and joined together in order to exchange data and distributed to end users via the WSN. The clusters of the devices called sensor nodes are placed within specified locations. WSNs are essential in military uses like surveillance of enemies and battle fields [1]. The amount and quality of data transmitted by a sensor node depends upon its physical resources. Its design goals are the flexibility and energy efficiency of these nodes. A WSN is made up of a number of sensor nodes which interact among themselves through radio transmissions. The queries may be typed to access network information and gather the output with the implementation of a sink. Sensor networks can be of two different types; wired and wireless. Wired networks have nodes which are immovable owing to their stationary and are implemented in fixed positions. This is more expensive as it needs a wired connection in order to communicate among the devices [2]. On the contrary, the nodes in the wireless networks can be installed at any place since not linked with cables. The wireless sensors cheaper than the wired sensors and communicate using radio waves among the devices. Sensor nodes could be able to communicate through each other directly or indirectly. In direct communication, the route will be the one between the source and the destination node, and in indirect communication, there will be the intermediate node that exists between the source and the destination. The major functions of sensor nodes are data transmission, and storage of the sensed data is transmitted to the base station. The main components of sensor networks are sensor fields, sensor nodes as well as base stations [3].

Nodes are electronic devices and the field where they are installed is known as a field. The base station serves as the central control node of the network and the information is gathered and handled there. The base stations may also be mobile devices and laptops, which allow data transmission via the Internet. Figure 1 shows the elements of a sensor network. A sensor node has an architecture that is comprised of a number of functional units. The sensing unit is the node brain and it collects data. Depending on the type of node, it converts sensed data either into digital or analog signals. All the tasks involving sensing are handled by the processing unit which is usually made up of microcontrollers like RISC-based architectures. These microcontrollers are able to be in different states active, sleep or idle depending on how it is required to be operated [4]. The communication unit deals with transmission of radio signals between sensor node and to the base station. When active nodes transmit and receive data, and when no tasks of relevance are being undertaken, they may change to the sleep mode. When there is no necessity of communication, nodes are idle. An energy supply unit is also added since every node needs a source of power to operate. Use of energy increases the longevity of the sensor nodes in general and their dependability [5].

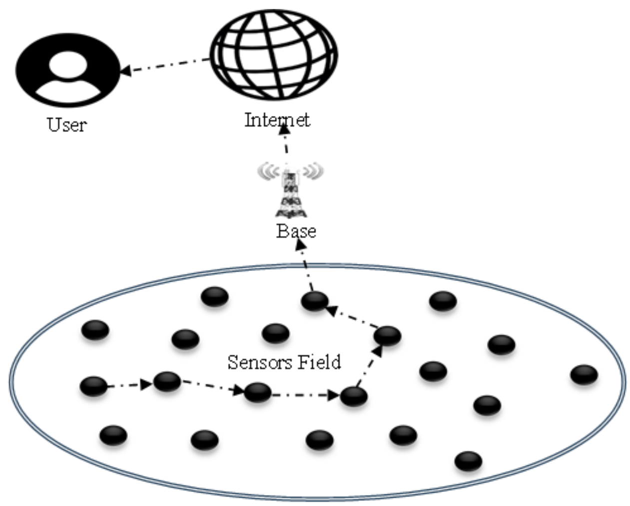

Figure 1 WSN Components

The destination node referred to as sink node receives the data and communication in UWSNs can also be done by use of acoustic waves. EM waves are frequently found in land-based networks have a number of limitations in underwater networks such as the high-power consumption and extreme attenuation. Acoustic waves are more dependable in underwater communication because they are much less attenuated and can go a long way [6]. UWSN architecture usually comprises of control nodes and sensor nodes. The data collection is taken from sensor nodes that are placed under water and the communication between these two is taken care of by the acoustic modems. The nodes are battery powered and this lets us apply different deployment strategies to guarantee efficient network coverage and network life. Storage of data is also done by distributed nodes and data transmission is done through acoustic modems to ensure reliability [7]. The standard UWSN network structure would consist of three elements are (i) sensors, (ii) surface stations and (iii) the underwater mobile vehicles. The main role of acoustic modem is to receive and send information through the underwater environment, which uses batteries on-board. Data is transmitted to the sink node with the help of transceiver thus facilitating effective data aggregation. This data is then sent by the transmitter to the surface station [8]. These surface stations communicate with surface sinks or onshore sinks or stations with the help of RF signals. The communication can take a direct or a multi-hop form. Direct links have the benefit of allowing easy transfer of data to the

RESEARCH ARTICLE

sink, but are not normally as energy-efficient. Multi-hop communication enables intermediate nodes to pass data between the source and destination nodes enhancing the energy efficiency and the overall network performance [9]. As seen in Figure 2, a UWSN sensor node consists of the following parts.

i. Controller: The controller is used to interface with sensors.

ii. CPU: The CPU receives sensor data and processes, stores, and analyzes it. Data is routed to the next sensor using an acoustic modem.

iii. Power supply: Required for sensors to operate properly in any medium

iv. Sensor protection: To stop corrosion-related sensor failures, a covering is installed.

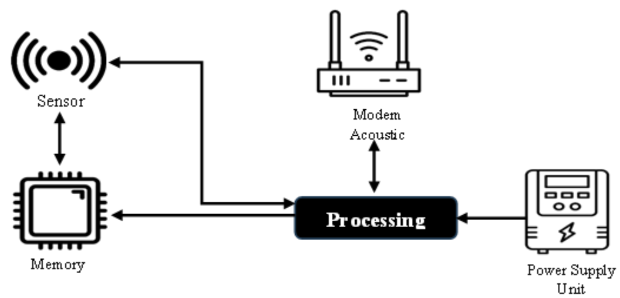

Figure 2 UWSN Components

The routing process in UWSNs is majorly involved in the forwarding of data packets in between the source and the destination nodes. The routing involves the calculation of the most efficient route to be used in the transmission of data and routing tables are maintained to ensure that the routing paths of the network are updated. Being one of the most fundamental parts of UWSNs, routing has a direct influence on the stability and reliability of network communication, as the failure of the sensor nodes may result in the collapse of the links and loss of data. It is necessary to develop efficient and dynamic routing plans to address the performance needs of UWSNs [10].

A common UWSN will have several sensor nodes that are set based on aspects like the network performance, the transmission range, and the volume of the seas. These submerged nodes gather environmental or surveillance information and these are forwarded to sink nodes where they are processed further. The sink nodes then relay the acquired information to neighbouring networks or the terrestrial stations with the help of acoustic signals or satellite communication link. Whereas terrestrial protocols like TCP and UDP have been used to transfer data between the surface and ground station, the current communication protocols like TCP and UDP cannot be used in underwater communication because of high latency, low bandwidth and attenuation [11].

The main problems that arise with underwater acoustic communication are due to the nature of the underwater communication i.e. higher signal attenuation and lower range of transmission. The routing protocols are needed to solve these problems by facilitating the reliable transmission of sensor data between the source nodes and the sink node [12]. As illustrated in Figure 3, scattering and absorption phenomena further complicate reliable data transmission in UWSNs.

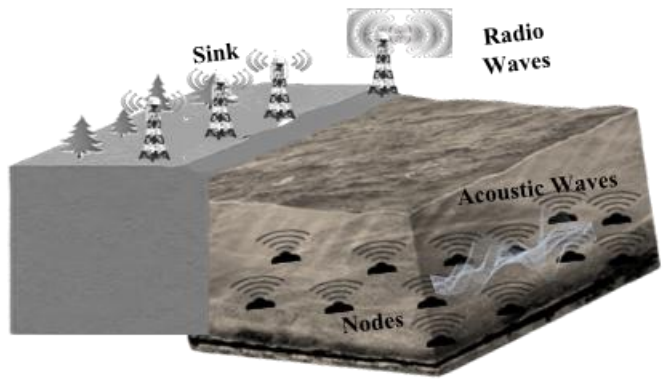

Figure 3 Architecture of UWSN

The decision of routing depends on various parameters whereby each node will compare their metrics such as the level of energy, distance, and quality of links with the nodes they are connected to. The process of data forwarding is then done using the node that has the best value. In addition, quality of links in the transfer of data is very important because communication will be reliable. UWSNs routing schemes usually take into account the node depth data, since the procedures of data transmission are different depending on the position of the node in the water column. Such structures aid in discovering shorter and less energy consuming paths of forwarding packets. Although these benefits exist, the ratio of packet delivery normally reduces as communication is performed over long distances or using poor connections as the quality of the links also reduces with the distance [13].

UWSNs routing process solves the issues related to bandwidth limitation and channel capacity limitation. This renders UWSNs to be applicable in a broad array of applications such as underwater surveillance, environmental monitoring and autonomous underwater vehicle (AUV) coordination [14]. In most cases, surface or ground-based stations are combined with data storage units to control data collection and distribution in accordance with certain working tasks. These are some of the physical and operational challenges of the UWSNs that include low bandwidth, huge propagation delay, and frequent alterations of the topology, Medium Access Control (MAC) complexities, and large energy usage. Resource optimization and energy-conscious routing are still the key performance metrics that have to be

RESEARCH ARTICLE

tracked regularly to increase the efficiency of UWSN [15]. Examples of medium access protocols are collision, frequency, time and spectrum, and they are some of the communities that can support a large portion of artificial intelligence (AI). Machine learning and deep learning have been integrated into real-time applications, which has illuminated this powerful branch of artificial intelligence. Deep learning may exhibit various characteristics that are useful to routing protocols [16]. Deep learning operates in sink and vehicle sensor node, the key sensor node in underwater WSNs. Such nodes are called AUVs. Using the multi-hop path communication, sink nodes can increase. The network is expandable by adding more sinks and parallel sensor nodes which detect a multitude of sinks of inputs presented by data nodes that are typically known as packets across the UWSN architecture [17].

1.1. Problem Statement

Rigorous security management in UWSNs is difficult because of the underwater environment. The networks of UWSNs are characterized by limited bandwidth and energy which also puts constraints on the implementation of computationally expensive security coverage but ensures the sustainability and efficiency of the network. Multipath propagation, signal attenuation and unpredictable environmental changes are also introduced due to underwater conditions and cause poor performance of the current encryption and communication techniques. Security is further complicated by physical vulnerability where UWSN nodes are regularly installed in remote or dangerous areas and hence the programs are at a risk of malicious attacks, unauthorized entry and physical interference. Since the whole infrastructure is not centralized, it needs distributed and adaptive security measures because centralized approaches are not feasible. UWSNs face threats that affect the availability, integrity and confidentiality of data like jamming, eavesdropping, and node compromise. The successful security solutions should be able to strike the right balance between energy and performance, scalability, environmental resilience, and real-time threat detection to provide resilience and reliability in communication. Cooperation is necessary to develop standards and best practices; this will enhance the security position of UWSNs to counter the growing threat of underwater security.

1.2. Motivation

The need to secure confidentiality, integrity and reliability of the information transmission in underwater surroundings highlights the need to deal with security issues in UWSNs. The issue of security in UWSNs is essential in protecting the sensitive information and ensuring the integrity of the working systems that are deployed during the use of mission critical applications such as military surveillance, underwater exploration, environmental monitoring, and disaster prevention. Such networks are often used to provide the infrastructures that serve offshore energy production, marine research, and national defense as well as the inspection of subsea infrastructure. Thus, security against unauthorized access, malicious attacks, or tampering of data is needed to avoid financial loss, information access breaches, and destruction of the environment. The process of collecting vulnerable data including information about marine ecosystems, the pattern of aquatic organisms, and underwater structural environments is one that requires the high standards of data privacy preservation and ethical data management. The adherence to the international standards and privacy regulations enhances the trust and transparency in the underwater data operations. The motivation to improve the security of UWSN is also based on the acute necessity to secure critical assets, confidential data, and maintain user privacy so that underwater communication systems are used in an efficient, responsible and sustainable way, in the best interest of a variety of scientific, social and environmental interests. Key challenges addressed in the proposed work are as follows:

- Enhancing UWSN security against dynamic underwater threats and environmental uncertainties effectively.
- Optimizing resource consumption while maintaining robust security and efficient network operations.
- Improving adaptability of security mechanisms to heterogeneous sensor nodes and underwater conditions.
- Mitigating vulnerabilities of existing security methods under challenging underwater communication constraints.
- Ensuring reliable and resilient data transmission across large-scale, dynamic underwater networks.

The remainder of this paper is organized as follows. Section 2 reviews the existing literature on security mechanisms in Underwater Wireless Sensor Networks (UWSNs), highlighting their limitations and motivating the need for hybrid optimization approaches. Section 3 presents the proposed system, detailing the integration of Beetle Antenna Search (BAS) and Genetic Algorithms (GA) for adaptive and energy-efficient security enhancement in UWSNs. Section 4 discusses the simulation results, performance evaluation, and comparative analysis with existing methods, emphasizing improvements in security, energy efficiency, and reliability. Finally, Section 5 concludes the paper by summarizing key findings, contributions, and potential directions for future research to further strengthen UWSN security.

2. RELATED WORKS

Some of the specialized features of underwater wireless systems rely on sensors to a large degree especially in monitoring the presence or functionality of given applications. The importance of sensors in the provision of reliable and energy saving underwater communication is thus essential.

RESEARCH ARTICLE

This chapter introduces and evaluates the available literature on wireless routing protocols with focus on energy consumption, notification delay, and node transmission efficiency of UWSNs. Different simulation scenarios have been studied in order to examine the energy efficiency, time synchronization and network trip time of different network configuration [18]. Researchers hope to investigate and use the huge amounts of waters that occupy the greater part of the earth surface with the assistance of UWSNs. In the UWSNs, sensor nodes are distributed in different depths according to ad hoc network configurations. They have the duty of environmental data sensing, processing information obtained, and relaying the information to the adjacent nodes through the acoustic wave wireless communication [19].

The recent publications investigated deep autoencoders and sparse codings to detect anomalies underwater. An important work presented a Stacked Sparse Autoencoder (SSAE) to monitor every acoustic traffic and this approach allowed the system to memorize the tight representations of normal behavior. The trained SSAE had high sensitivity to the detection of jamming and eavesdropping attempts, with no handcrafted features, when trained on distorted underwater datasets. This showed that unsupervised DL models could be used in underwater security in unpredictable environments [20]. Other articles were dedicated to underwater acoustic communication authentication with the use of deep learning. An authentication scheme based on the patterns of the spectrograms of signals sent by the physical-layer was examined in order to distinguish legitimate nodes and the attackers by the use of CNN scheme. The CNN model minimized attacks of impersonation and replay by learning special acoustic signatures. This strategy was better than the current correlation-based strategies, particularly in multipath and Doppler distortion that is common in underwater scenarios [21].

In a number of studies, bio-inspired optimization tools like Ant Colony Optimization (ACO), Dragonfly Optimization and Hybrid Firefly-Bat were used in secure route creation. These routing algorithms made it more resilient to routing layer attacks, and dynamically chose energy efficient and trust-aware routes. With the combination of lightweight threat likelihood measures, the optimized routing schemes were able to reduce the packet loss in the selective forwarding and sinkhole attacks, particularly in deep-sea monitoring systems [22]. The recent developments point out the significance of Deep Reinforcement Learning (DRL) in alleviating routing and MAC-layer attacks. A DRL-based secure routing protocol based on Deep Q-Network (DQN) allowed the underwater nodes to autonomously learn how to take optimal defense decisions, including switching of links, energy reallocation and dynamically reconfiguring a cluster. The system was also highly adaptive to topology changes that offered excellent protection against flooding attacks and enhanced longevity of the network [23]. Figure 4 displays the chemical and physical characteristics of water. The characteristics of water also influence the communication that takes place in UWSN

Later articles suggested cross-layer integrated DL models that are optimized with the help of metaheuristic algorithms. The hybrid systems of LSTM networks to analyze sequences with PSO or WOA to tune the hyperparameters resulted in highly accurate intrusion detection systems at lower computational cost. The models represented the dependencies between the physical, network, and MAC layers, and it was possible to identify the simultaneous multi-stage attacks in their early stages. It was found that there were significant enhancements in accuracy, reduction in false-positive and high levels of robustness in the unfavorable underwater conditions [24]. In one of the recent works, an intrusion detection system powered by LSTM was introduced with a special purpose to underwater acoustic communication. The LSTM architecture was able to identify low-rate denial of service and gradual attempts of spoofing attacks, which are considered to be stealthy, because it models long-term temporal dependencies of underwater traffic patterns. The system also demonstrated great accuracy in the presence of varying propagation delays, which is an indication that sequence-sensitive deep networks can be effectively applied in underwater security [25].

Generative Adversarial Networks (GANs) to come up with the realistic patterns of cyberattacks to train the IDS models. The GAN generated artificial jamming, collision and spoofed traffic which was very similar to actual underwater events. An excellent discriminator conditioned on this augmented data was found to be more robust and had lower false alarm than traditional supervised learning IDSs, which underscores the usefulness of GANs to augment small underwater datasets [26]. To alleviate the malicious relay nodes, a trust-aware routing technique that was optimized by Whale Optimization Algorithm (WOA) was suggested. WOA was a dynamically tuned network, whereby trust thresholds and forwarding probabilities were adjusted, which allowed the network to bypass nodes that had been compromised with minimum delay. The model of optimized trust significantly enhanced the delivery of packets and power savings during blackmail and greyhole attacks particularly in large scale underwater deployments [27].

The application of Deep Belief Networks (DBNs) into classifying underwater physical-layer anomalies with features in the spectral and energy-domain has been used. The DBN-based approach proved to be effective in detecting signal mimic attacks, manipulating relays and unauthorized channel access. The DBN with its multilayer generative-learning architecture was able to deal with non-stationary and noisy nature of the underwater acoustic signals [28]. In another study, a research project proposed a lightweight encryption algorithm that has been optimized by use of Particle Swarm

RESEARCH ARTICLE

Optimization (PSO). PSO optimized parameters of encryption keys and diffusion to reduce the level of computation without compromising high levels of security. This was very appropriate in underwater sensor nodes that have limited energy and processing power, and attain secure communication with the eavesdropper and ciphertext-only attack [29].

Another more recent article investigated Federated Learning (FL) to construct distributed intrusion detection models without having to centralize raw sensor data. The underwater clusters locally trained DL models diffusion model CNNLSTM hybrids predominated, and only transmitted encrypted model weights. This maintained confidentiality and enhanced international response to distributed threats. The FL-based technique greatly contributed to resiliency in instability of links and minimized single-point breakdowns [30].

Although the deep learning, optimization, and cross layer hybrid methods have greatly enhanced security in underwater wireless sensor networks, there are still a number of limitations that are yet to be addressed. Although effective, the available versions of DL-based IDS models are characterized by a high computational cost, low convergence speed, and low reliability in extreme underwater environments, including variable channel noise, high latency, and low energy resources. Routing protocols such as ACO, WOA and PSO with optimization enhance trust and energy efficiency, but have trouble achieving stable operation during fast topology transitions or support synchronized multi-stage attacks.

The intrusion detectors and federated learning systems enhanced with GANs need efficient, more adaptive, and self-optimizing mechanisms to be maintained in the real-time performance of resource-constrained underwater nodes. These gaps underscore the urgency to have a more vigorous and energy-conscious optimization approach which could dynamically adjust security settings, improve routing stability and increase the accuracy of intrusion detection. The Hybrid Beetle Antenna Search-Genetic Algorithm (BAS-GA) is necessary to combine fast local search, global searching and adaptive parameter optimization that offers a more resilient, energy saving and smarter security platform to UWSNs.

3. PROPOSED SYSTEM

Water found in rivers and oceans covering almost 75% of the planet, is necessary for daily life. Even though there is a lot of water in Asia, environmental harm and water scarcity have caused many living things to not last very long. Threatened situations can also jeopardize resources, life, and many other natural elements that impact a wide variety of living creatures. Some numerous pressures and difficulties affect underwater features, including pollution, filth, damage from irresponsible activity, and deep fishing. To monitor the various components of the seen environment, such as deep countable humidity measurements, ocean pollution levels, sound effects in waves, and temperature measurements. For many species, these polluted difficulties can be overcome with the use of technological developments in tracking and monitoring. Acoustic waves are typically used to illustrate the relationship between sound and sensor results.

There are numerous ways to interpret underwater pollution observations, such as electromagnetic or optical waves. Acoustic wave signals are more practical and it can be employed by mobile nodes as a control medium to make efficient use of its surroundings. In the water, acoustics are the most efficient means of long-distance wireless communication. Existing methods that are initialized for monitoring the situations are referred to be more complicated approaches. Figure 4 illustrates how sensors are used.

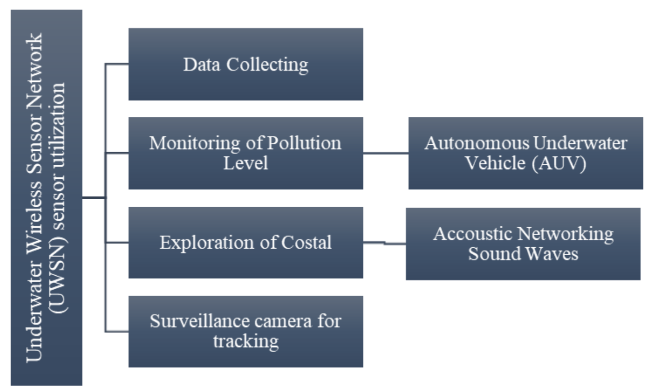

Figure 4 Sensor Usage in UWSN

The provided flowchart (Figure 5) illustrates a process for network initialization, data collection, and cluster head management within WSN or similar system. The process begins with Network Initialization. Following this, the operation splits into two paths: one for a Skill node and one for a Sensor node. The Skill node path involves collecting data related to the node, choosing a cluster head utilizing a data collecting protocol, choosing data regarding cluster heads to nodes in the range, and receiving data regarding sensing.

This path then checks if the Node is Alive? before potentially stopping. The sensor node path starts by sending and sensing the node ID and Position. A key decision point follows: Cluster head node =?. If yes, the node issues a Cluster head announcement and proceeds to transfer data off a specific time. If no, it simply waits for announcement. After transferring data, the Distance measure is performed. Depending on the distance, the data is either Sent to the next cluster head or Sent to the sink node. Both of these final steps lead to the Node Alive =? check, where a negative result terminates the process (Stop).

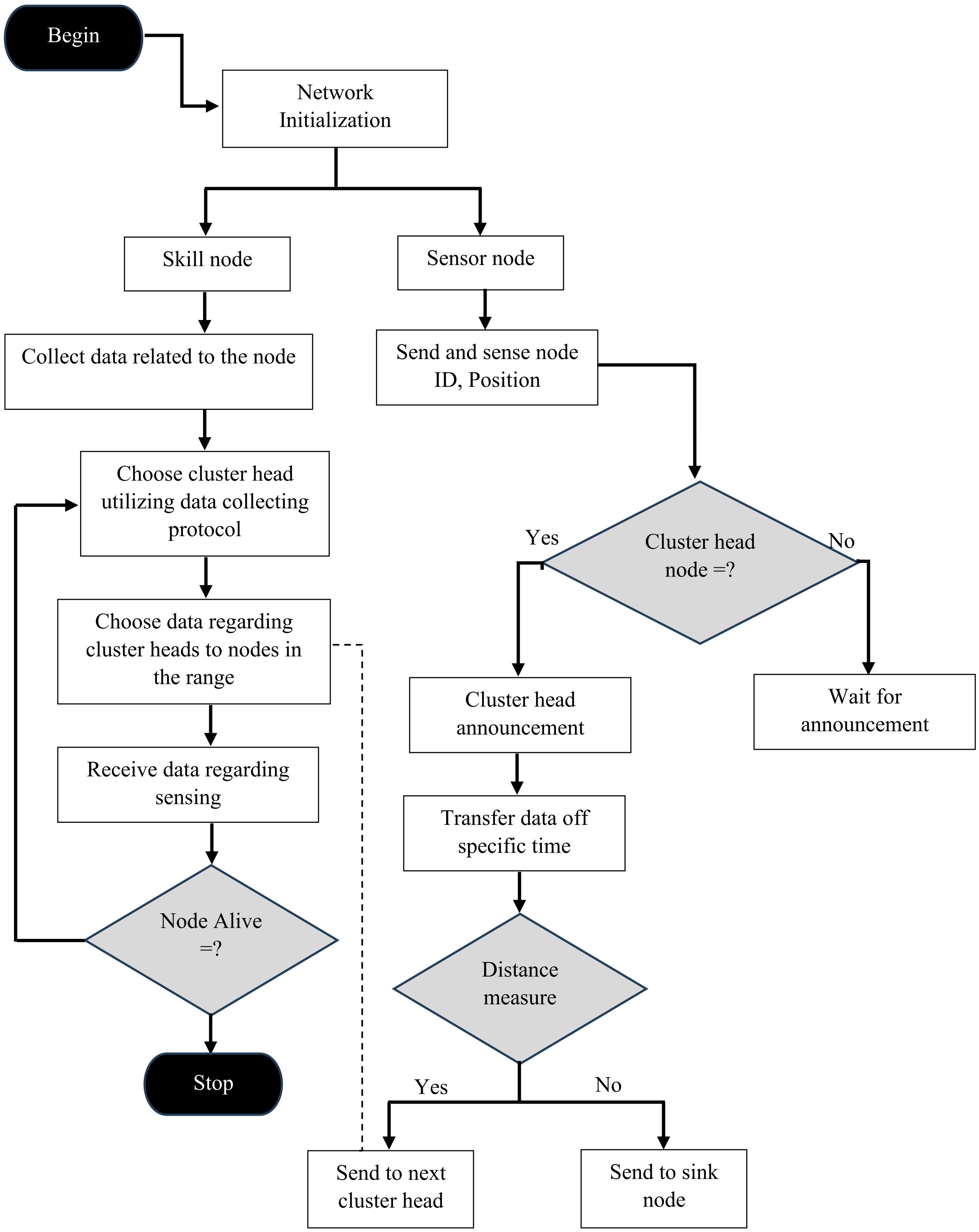

Figure 5 Proposed Model Workflow

3.1. Genetic Algorithm

In the existing environment, ML algorithms are a good fit for businesses, developments, and building construction. When data analysis or prediction is performed, it may be done excessively quickly or noisily. For the sake of the fundamental algorithm requirements, these selection criteria determine whether a parameter is a good or bad pick. One of the evolutionary methods that can manage a dataset that has been divided into multiple groups based on the classifier that is being maintained is the genetic algorithm. Samples are utilized as training features in another criterion, where the accuracy depends on the number of classes. Every iteration displays the accuracy of the achieved result is evolving but isn't the best outcome improve the selection criteria. In these situations, optimization refers to the specific actions improve learning and initiate the value needed for an accurate classification.

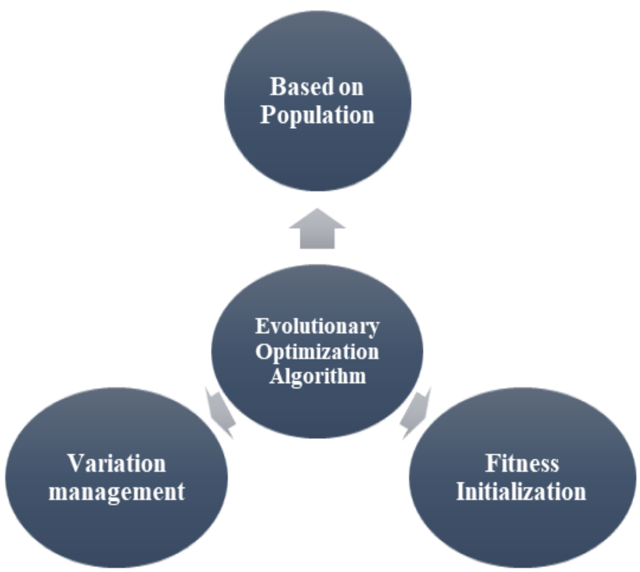

Figure 6 Characteristics of Evolutionary Optimization Algorithm

In the real world, nature does its best to weigh every alternative that can be turned into man-made procedures. Following the creature format of birds is commonly referred to as bionics, is one of the crucial artificial systems in starting the optimization and adaptation process. Many factors influence the discovery of various objects, including ships built from fish habitats in the sea, radar-equipped birds, and airplanes. In a similar vein, the optimization algorithms use Darwin's survival of the fittest in conjunction with the bird flying steps as a genetic solution to support feature selection. The key elements are represented as traits of genetic algorithms. Three features of evolutionary algorithms are used to enhance the existing optimization method. The genetic algorithm suggests a degree of change that can eliminate the previous answer to produce fresh results as a solution. These fundamental procedures are followed until the optimal outcome for the evolutionary process is found.

Existing methods were frequently used in dynamic environments where certain evolutionary stages were unsuccessful. In machine learning applications, the ill-optimized solution cannot be more dependable if the EAs fail. As a result, the characteristics are established for dynamic dataset updates. These three crucial traits are as follows (Figure 6).

The existing experimental values that are marked as problematic are first converted into alternative produced values as the first step in the EA optimization process. To perform at the next level of generation, alternative values are introduced as new and better values. These better outcome values must become existing values. This type of performance is displayed based on population. When the initial characterization is completed, the next level of orientation can find solutions for dynamic operations. In the several values, fitness initialization is interrelated among the necessary mathematical computations, where the computed solutions are declared as good values and proposed as the best solution.

$$Fitness\ Initialization\ (F1) = Weight\ (wg) * Number\ of\ cluster\ (Nc) + 1 - wg * Covered\ network \quad (1)$$

$wg - Represent\ weight\ of\ nodes$

Equation (1) reflects the number of clusters that are involved in fitness initialization was computed using WSN as a foundation. WSN initial configuration for the existing selection on each node. WSN uses a variety of clustering approaches to focus on issues related to underwater resources. A large number of the cluster group's members have begun and ended its allocation according to the timeframe. Depending on the weights and sensor selection, among other factors, the transmitted nodes may pass or fail. Second, depending on the cluster group, WSN determines the transmission distance needed to compute the network distance and energy consumption. When there are no feasible steps from the available values obtained from the number of dynamic populations for the applied attributes based on population and Fitness Initialization. The computation function can be calculated from unique values based on the initialized fitness. Then, by experimenting with the better values from the computation solution, huge variations that can produce an infinite number of results are developed.

3.2. Selection of Cluster Head (CH) in UWSN

The selection of CHs in UWSNs is crucial for optimizing energy efficiency, ensuring secure communication, and enhancing network lifetime. The CH selection process considers multiple factors, such as residual energy, communication cost, and security level, which are combined into a fitness function to evaluate each node's suitability for serving as a CH.

The residual energy (E_i) of a node is a primary criterion to prevent premature energy depletion. It is normalized as shown in Equation (2).

$$F_E = \frac{E_i}{E_{max}} \quad (2)$$

Where E_{max} represents the maximum energy of nodes in the network. Higher F_E values indicate greater suitability for CH roles.

The communication cost (C_i) is determined by the total distance between a node and its cluster members. Nodes with lower communication costs are preferred to minimize energy consumption during data transmission shown in Equation (3).

$$F_C = \frac{1}{\sum_{j \in cluster} d_{ij}} \quad (3)$$

Where d_{ij} denotes the distance between the candidate CH (i) and cluster member (j).

The security level (P_i) of a node is another key factor, ensuring secure data aggregation and transmission. Each node's security score is normalized as shown in Equation (4).

$$F_S = P_i \quad (4)$$

Where higher F_S values correspond to better security capabilities.

These factors are combined into a weighted fitness function, which quantifies the overall suitability of a node for CH selection shown in Equation (5).

$$F_{CH} = \omega_1 F_E + \omega_2 F_C + \omega_3 F_S \quad (5)$$

Where, ω_1, ω_2, and ω_3 are weights assigned to prioritize residual energy, communication cost, and security level, respectively.

This multi-objective optimization ensures that CH selection balances energy efficiency, reduced communication costs, and secure data handling, thereby improving the performance and reliability of UWSNs.

3.3. Beetle Antenna Search with Genetic Algorithm

Antennae of beetles with long horns are longer than the body of the insect. There aren't many species with longer antennas. Identification of the patterns that the insects follow is important because it is key to sensing. The antennas can distinguish between the distinct smells of each prey. Pheromone also aids in the identification of areas. Beetles' antennae can function as warning mechanisms. Using the antennae, random exploration is conducted of the surrounding areas. The insect starts moving toward the smell as soon as it notices it. By looking for beetles with longer antennas, the behavior of the search process optimizes the goal function. For the specified time frame, the beetle's position is calculated as a vector. Based on the smell concentration, f(x) is computed for the objective function. The maximum value is determined by utilizing the source of the odor. Beetles employ two primary actions in its algorithms: searching and detecting. At first, the search is conducted randomly to explore the prey. The communication that takes place underwater has several difficulties, which is why researchers are concentrating on UWSN. Routes found as a consequence of optimization must be used to transport monitored data to the onshore terminal. The creation of a protocol for managing energy efficiency and maximizing network lifetime is the main goal of the proposed study. Along with the CH selection procedure in UWSN, the data gathering protocol is crucial to data collection. In this case, beetle antennae search routing combined with gateway discovery is employed for optimization.

3.3.1. Initialization of Parameters

The initial step begins with the initialization of the Beetle population along with the setting of the parameter for searching. It is also utilized as a parameter for global search. The equation for computation is represented in Equation (6).

$$i^r = Li^{r-1} \quad (6)$$

The representations used in the above equations are, L – Coefficient of attenuation in the computation of the length of the step. The size of the step is computed based on the tentacles and its distances shown in Equation (7).

$$i^r = i^r / i \quad (7)$$

The representations used in the above equations are, i-acts as a constant with the value starting from 2 and ending in 10.

3.3.2. Generation of Random Population

The selection of beetles occurs in a random fashion where the positions are generated based on in Equation (8).

$$\rho_j = \frac{rand\,(L,1)}{|rand(L,1)|} \quad (8)$$

Rand function takes care of the generation of random functions; the space of dimension is denoted using L. Computation of vectors associated with directions is done and the equation of both the tentacles is given in Equations (9). and (10)

$$C_k = C^r - f^r \rho_j \quad (9)$$

$$C_t = C^r + f^r \rho_j \quad (10)$$

C_k – position specified by right tentacles; C_t – Position specified by the left tentacles; t – Movement time; f^r – computation of distance between the tentacles of the beetles. Its movement is represented using Equation (11).

RESEARCH ARTICLE

$$c^r = c^{r-1} + i^r \rho_j sig(d(c_t) - d(c_t)) \quad (11)$$

The functions used are pending while performing optimization functions. The step for search is defined here. An increment in the count of iteration occurs along with a reduction in the size of the step. Search happens in a refined manner and a representation of the equation is given. The comparison of fitness functions is performed based on the position chosen in the existing level. Optimum solutions are computed with both best as well as global values.

3.3.3. Computation of Fitness Function

The testing features are utilized in conjunction with the employment of beetles to incriminate peak references. The network's lifetime is optimized by setting the parameters, and the related in Equation (12).

$$d_1(c) = \sum_{u-1}^{m} c_u^2 \quad (12)$$

d_1 Computation is performed in the above step. Optimization is performed by the BAS using the count of iterations. The coefficient of attenuation setting is done in this step.

3.3.4. Updating New Position

This stage involves computing the position of the beetles while it looks for food as well as identifying the orientation of both of its tentacles. The population computation equation and the search parameter speed are indicated in Equations (13) and (14).

$$n_u^{l+1} = n_u^{l+1} + i_1 random.(bp_u^l - n_u^l) + i_2 random.(bp_u^l - n_u^l) + i_3.rand.ir \quad (13)$$

Updating the position which is considered to be the best solution is represented in Equation (14).

$$n_u^{l+1} = c_u^l + n_u^{l+1} \quad (14)$$

The optimal value from all the intermediate solutions is done collectively and provides the solution that is considered to be best, the movement of the insect with the distance is calculated.

3.3.5. Stopping Criteria

The parameters are used to calculate the weight most efficiently. BAS-GA is used to carry out parameter optimization. The computation of the objective function is done, which is crucial in raising the network's efficiency and lowering its energy and latency consumption.

3.4. Algorithm

The hybrid approach combines Beetle Antenna Search (BAS) and Genetic Algorithm (GA) for optimizing security in Underwater Wireless Sensor Networks (UWSNs). The following algorithm describes the steps for implementing this approach to enhance security through key management, secure routing, and energy-efficient operation.

Inputs

- UWSN parameters: Environmental conditions, network topology, sensor node data, communication range, etc.
- Security parameters: Encryption keys, authentication methods, routing protocols.
- Sensor nodes: N number of sensor nodes, S={ $s_1, s_2, \dots, s_N$}

Outputs

- Secure and optimized routing paths for communication.
- Efficient key management system for encryption and decryption.
- Energy-efficient operation for sensor nodes.

Step 1: Initialization

Step 1.1: Sensor Node Initialization: Let the initial positions of the sensor nodes be $s_1, s_2, \dots, s_N$ with each node s_i having attributes such as location, energy level, and security status.

Step 1.2: Key Generation (for Encryption and Authentication): For each sensor node s_i generate a secret key K_i using a secure cryptographic algorithm. Keys are shared among neighbouring nodes based on the secure communication model shown in Equation (15).

$$K_i = H(M_i) \quad (15)$$

M_i = Message or data from node i; H is the hash function for key generation.

Complexity is O(N) for all nodes.

Step 2: Beetle Antenna Search (BAS) Optimization for Secure Routing

The BAS algorithm aims to optimize the routing paths between sensor nodes to minimize energy consumption and ensure secure data transmission.

Step 2.1: Foraging Behavior Simulation: Each sensor node acts as a "beetle" searching for the optimal communication route. The objective function for BAS is formulated in Equation (16).

$$F_{BAS}(P) = \alpha E(P) + \beta D(P) + \gamma S(P) \quad (16)$$

Where: P is the potential path for data transmission; E(P) is the energy consumption along the path; D(P) is the distance or latency along the path; S(P) is the security level of the path (e.g., encryption strength, hash integrity). α,β,γ are weight factors.

Step 2.2: Path Update: The paths are updated by moving beetles towards paths that minimize the objective function $F_{BAS}(P)$; Each beetle updates its position based on

RESEARCH ARTICLE

the current best solution and the behaviour of other beetles. The update rule for the beetle's position is shown in Equation (17).

$$P_{new} = P_{current} + \omega.(P_{best} - P_{current}) + \eta.(P_{neighbour} - P_{current}) \quad (17)$$

Where: ω is the inertia weight. η is the coefficient influencing the exploration of new paths.

The total complexity for this step is O(M * K).

Step 3: Genetic Algorithm (GA) Optimization for Key Management

GA is used for optimizing key distribution and ensuring secure communication.

Step 3.1: Chromosome Representation: A chromosome represents the key distribution strategy, where genes represent different key values or key-generation methods. The fitness function for GA is defined shown in Equation (18).

$$F(GA) = \sum_{i=1}^{N} f(K_i, P_i) \quad (18)$$

Where: $f(K_i, P_i)$ is a function that evaluates the effectiveness of key K_i in securing the path P_i

Step 3.2: Selection, Crossover, and Mutation:

- Selection: The best chromosomes are selected based on its fitness values.
- Crossover: The selected chromosomes are combined to generate new offspring representing better key distribution strategies shown in Equation (19).

$$K_{offspring} = Crossover(K_1, K_2) \quad (19)$$

- Mutation: Random mutations are applied to the offspring to maintain diversity and explore new solutions shown in Equation (20).

$$K_{mutated} = K_{offspring} \oplus Random\_Mutation \quad (20)$$

Where ⊕ denotes the mutation operation on the key.

Step 3.3: Key Re-encryption: After optimizing the keys through GA, the keys are re-encrypted using the updated key management scheme shown in Equation (21)

$$Re\_Encrypt(C_i, K_{new}) = E_{K_{new}}(C_i) \quad (21)$$

Where C_i, is the ciphertext.

Complexities are O(1) per operation. For a population of size N and G generations, the complexity of GA is O(G * N), where G is the number of generations. The key re-encryption process is also a constant-time operation, adding an O(1) complexity for each re-encryption.

Step 4: Hybrid Optimization - Combining BAS and GA

Step 4.1: Hybridization: The hybrid approach is applied by combining the best results from both BAS and GA to achieve optimal security and energy-efficient routing.

Step 4.2: Final Objective Function: The final objective function is a weighted sum of the optimized routing paths and key management solutions shown in Equation (22).

$$F_{Hybrid} = \lambda_1 F_{BAS} + \lambda_2 F_{GA} \quad (22)$$

Where λ_1 and λ_2 are weighting factors to balance the contributions from BAS and GA.

Complexity of the individual optimizations and is thus O(M * K + G * N).

Step 5: Deduplication using Bloom Filter.

Step 5.1: Data Deduplication: The Bloom filter is used to prevent data redundancy by ensuring that identical data is not transmitted multiple times. A Bloom filter is a probabilistic data structure that uses multiple hash functions to check if an element is present in a set.

The hash function for the Bloom filter is shown in Equation (23).

$$h_i(x) = (a_i.x + b_i) mod\ n \quad (23)$$

Where $h_i(x)$ is the hash function; a_i, b_i are parameters, and m is the size of the filter.

Step 5.2: Checking and Inserting Data:

For each data packet, check if it exists in the Bloom filter using the hash functions.

If the data is not in the filter, it is added; otherwise, duplication is avoided.

The complexity for this step is O(D), where D is the number of data packets to process.

Step 6: Secure Decryption

Decryption Process: A cloud user can decrypt the data using the re-encrypted key generated by GA and optimized by BAS shown in Equation (24).

$$M_i = Decrypt(C_i, K_{re\_encrypted}) \quad (24)$$

Where, M_i is the original data message and C_i is the ciphertext.

The algorithm offers a secure, efficient and scalable method of improving security in UWSNs through bio-inspired optimization methods.

This makes the total complexity of the algorithm approximate to: O(N+M∗K+GASTN+D). N is the number of nodes, M is the number of paths, K is the number of iterations in BAS, G is the number of generations in GA and D is the number of data packets.

International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2025/56 Volume 12, Issue 6, November – December (2025)

RESEARCH ARTICLE

4. RESULTS AND DISCUSSIONS

The performance algorithm of the BAS-GA hybrid security algorithm was tested in a simulation environment that attempted to simulate the real UWSN scenarios. The network used a different number of sensor nodes dispersion across a preferred underwater sensing area, where nodes had a limited amount of energy and the range of a communication facility. Realistic channel characteristics were modelled using environmental factors that included: signal attenuation, multipath propagation and dynamic underwater conditions. The simulation involved node mobility, random topology variations and the possibility of attacks like jamming, eavesdropping and node compromise to determine the level of security. Parameters of the algorithm (like BAS exploration coefficients and GA population size) were optimally adjusted in a systematic way. Network lifetime, energy consumption, ratio of packets delivered, and measurement of security effectiveness were key performance metrics of the network, and these were measured during different rounds of simulation. The simulation code was executed on a controlled software environment where reproducible experiments could have been done and where they could be compared to standard security measures.

Table 1 Hyper-Parameter Settings

Parameter	Value	Description
BAS Step Size (s)	0.1	Controls beetle movement increment in solution space
BAS Antenna Distance (d)	0.05	Determines sensing range for gradient estimation
GA Population Size	50	Number of candidate solutions in each GA generation
GA Crossover Rate	0.8	Probability of exchanging genes between parent solutions
GA Mutation Rate	0.1	Probability of random variation in offspring solutions
Maximum Iterations	200	Number of iterations for algorithm convergence
Security Threshold (τ)	0.7	Determines sensitivity for anomaly or threat detection
Energy Threshold (Eth)	0.3 J	Minimum energy level for node participation in routing

The proposed BAS-GA hybrid algorithm is based on the balanced exploration, exploitation, and energy efficiency of UWSNs that are presented in Table 1 and rely on the balanced adjustment of hyper parameters. BAS parameters like the step size and the antenna distance regulate the search space exploration capability of the algorithm and the ability to identify the best security configurations. The GA settings of the population size, crossover rate, and mutation rate, provide varied solutions to the candidates but tends to converge to the best security solutions. Maximum iterations define the computational budget, while the security and energy thresholds guide node participation and threat detection, ensuring adaptive and energy-aware secure routing. These settings collectively enable the hybrid algorithm to optimize security performance while minimizing resource consumption in dynamic underwater environments.

4.1. Simulation Environment

The figure presents a clustered hierarchical WSN architecture, where sensor nodes are grouped into clusters managed by Cluster Heads (V_{CH}). Sub-Cluster Heads (V_{SH}) collect data from nearby nodes within their communication range and forward aggregated information to the CH shown in Figure 7. CHs further consolidate the data and relay it toward the BS. Mobile collectors or UAVs assist data transmission, especially for distant or isolated clusters, improving connectivity and reducing communication delays. This structure minimizes energy consumption by limiting long distance transmissions, improving scalability, and enhancing data reliability through multi-level aggregation and mobile assisted communication.

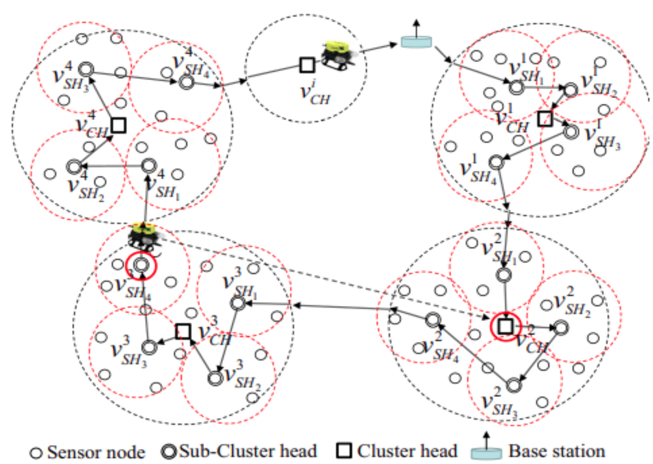

Figure 7 Simulation Node Setup

The proposed BAS-GA model was evaluated through a comprehensive simulation environment configured to replicate realistic UWSN conditions. All experiments were conducted using MATLAB with nodes randomly deployed within a predefined 3D underwater region. The simulation setup includes detailed parameters such as network size, number of nodes, initial energy, communication range, transmission power, and data packet size, which are listed in the simulation parameters table. Environmental factors such as acoustic propagation delay, water attenuation, and node mobility were incorporated to mimic real-time UWSN behavior. The simulation environment also integrates dynamic energy consumption models to track node operations such as sensing, transmission, and reception. This setup ensures that performance metrics—network lifetime, energy consumption, overhead, and throughput—accurately represent the behavior of both the proposed and existing models under identical conditions.

4.2. Network Lifetime

Figure 8 clearly demonstrates that the proposed BAS-GA model outperforms traditional routing approaches across all evaluation points. While ACO-WSN, PSO-Routing, LEACH-Enhanced, and GA-Trust exhibit gradual performance improvements, their gains remain relatively small compared to the significant and consistent increase achieved by the BAS-GA technique. The superior results indicate better optimization capability, stronger adaptability to dynamic network conditions, and improved packet delivery reliability. Overall, the proposed model delivers a more efficient, stable, and scalable routing solution for WSN environments.

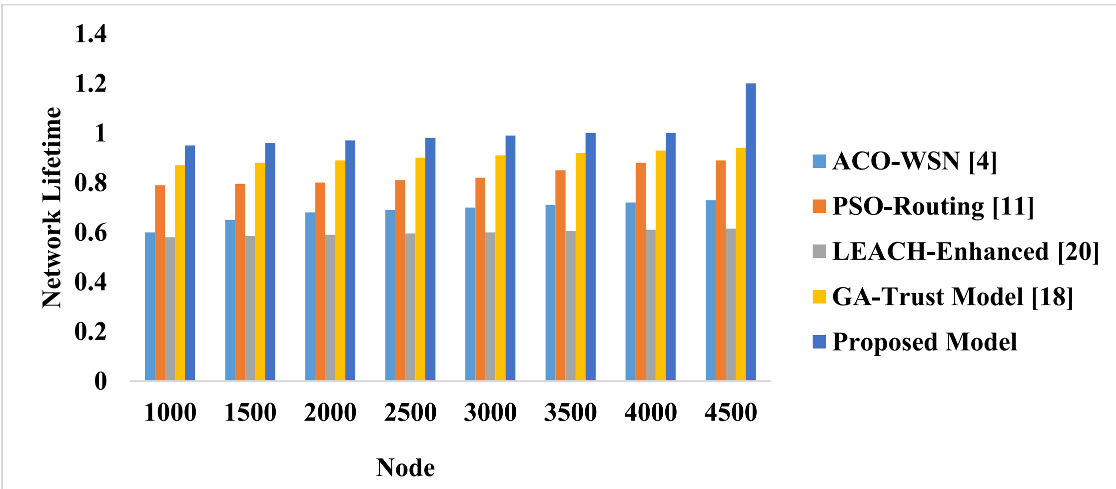

Figure 8 Comparison of Network Lifetime of Proposed and Existing Works

4.3. Energy Consumption

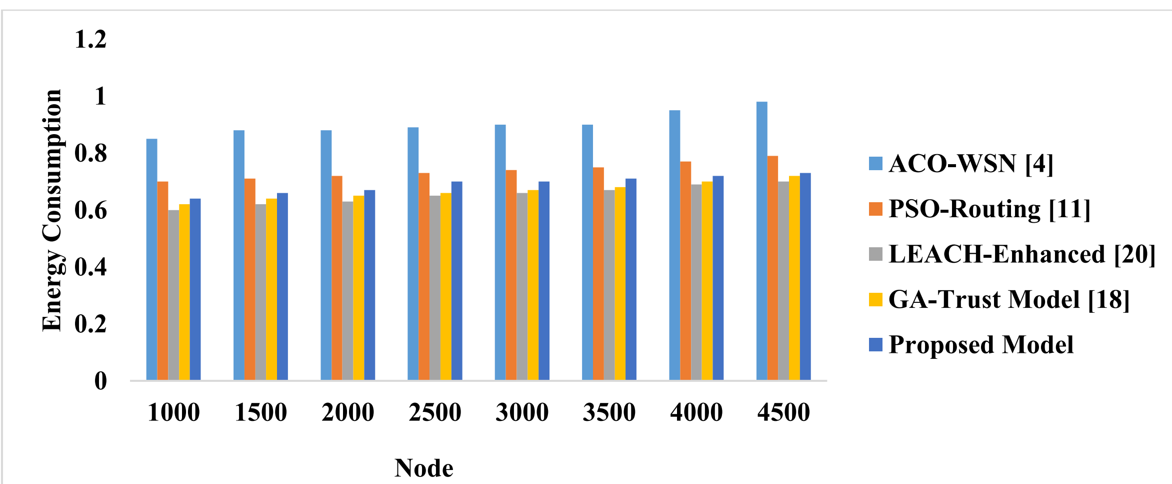

Figure 9 Comparison of Energy Consumption of Proposed and Existing Works

Energy consumption is calculated by measuring each node's initial energy level and subtracting the remaining energy after all operations are completed. The proposed model consistently performs better than the LEACH-Enhanced and GA-Trust models, particularly in maintaining stable and reliable communication across increasing network density

RESEARCH ARTICLE

shown in Figure 9. Although ACO-WSN and PSO-Routing display incremental improvements, they remain less efficient due to limited adaptability and suboptimal routing behavior. The enhanced learning-based optimization in the proposed method ensures reduced packet loss and improved transmission reliability. Thus, the model demonstrates superior robustness, energy efficiency, and routing intelligence for real-time WSN applications.

4.4. Overhead Consumption

The overhead consumption results clearly demonstrate that the proposed model achieves significantly lower communication and computational overhead compared to existing routing methods shown in Figure 10. While ACO-WSN and PSO-Routing show higher overhead due to frequent route re-establishments and intensive node cooperation, LEACH-Enhanced and GA-Trust models reduce overhead but still suffer from cluster-based control signaling.

In contrast, the Proposed Model minimizes control packet exchanges through intelligent trust-aware routing and optimized cluster maintenance. This efficient behavior helps extend network lifetime, reduce congestion, and improve scalability in dynamic WSN environments.

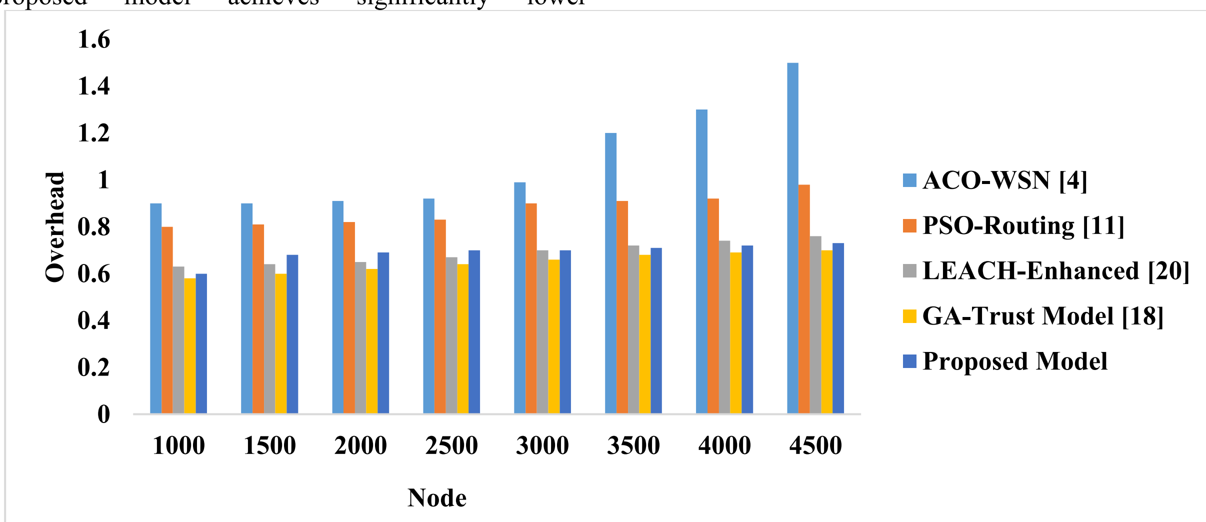

Figure 10 Comparison of Overhead Consumption of Proposed and Existing Works

4.5. Throughput

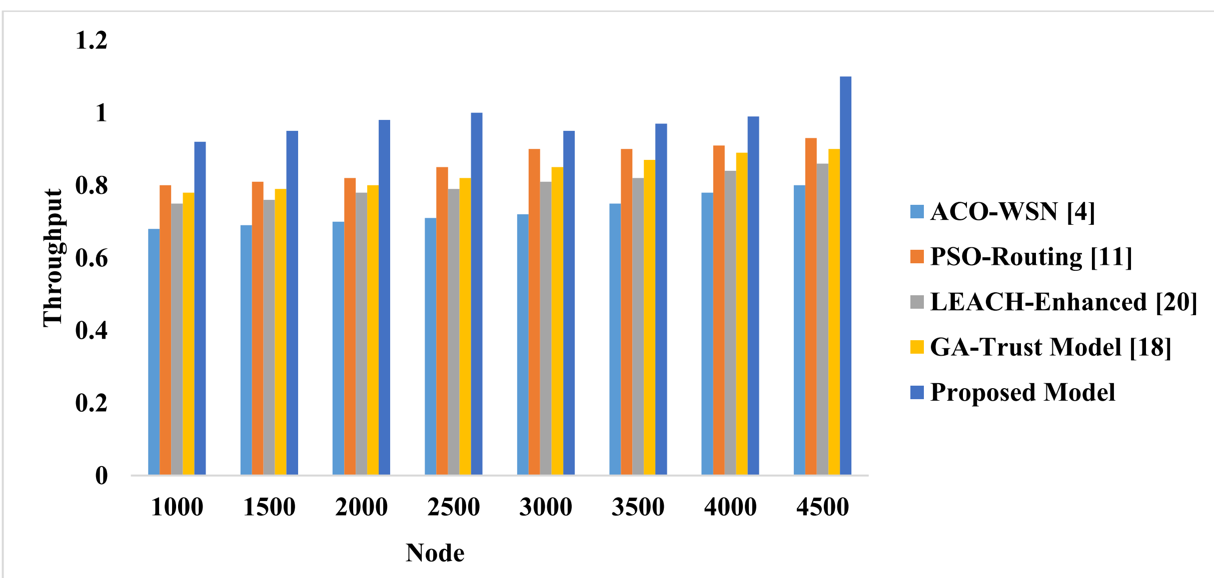

Figure 11 Comparison of Consumption Regarding Throughput of Proposed and Existing Works

RESEARCH ARTICLE

The throughput comparison demonstrates that the proposed model consistently achieves higher data delivery rates than existing routing protocols across all evaluation rounds shown in Figure 11. Existing methods such as ACO-WSN, PSO-Routing, LEACH-Enhanced, and GA-Trust experience gradual performance saturation as network load increases, mainly due to communication delays and packet drops during congested periods.

In contrast, the proposed model maintains superior throughput reaching up to 1.10 Mbps by integrating optimized cluster coordination, secure data aggregation, and dynamic routing decisions. This enhanced network efficiency ensures reliable data transmission, reduces congestion effects, and significantly improves overall Wireless Sensor Network performance.

4.6. Packet Transfer Delay

The packet transfer delay analysis indicates that the proposed model consistently outperforms existing routing techniques by achieving the lowest delay across all communication rounds shown in Figure 12. While ACO-WSN and PSO-Routing suffer from increased latency due to inefficient route formation and congestion under higher node density, LEACH-Enhanced and GA-Trust partially improve performance through clustering and trust-based decision-making. The proposed model further optimizes routing paths with intelligent cluster selection and secure, streamlined data forwarding, reducing retransmissions and communication overhead. This results in significantly lower end-to-end delay, improving real-time responsiveness and overall Quality of Service in Wireless Sensor Networks.

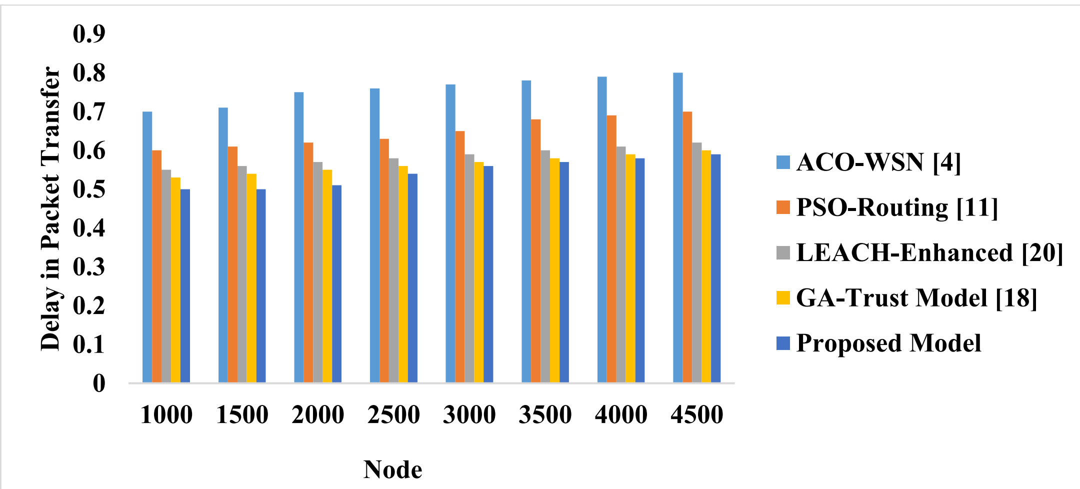

Figure 12 Comparison of Packet Transfer Delay of Proposed and Existing Works

4.7. Packet Delivery Ratio

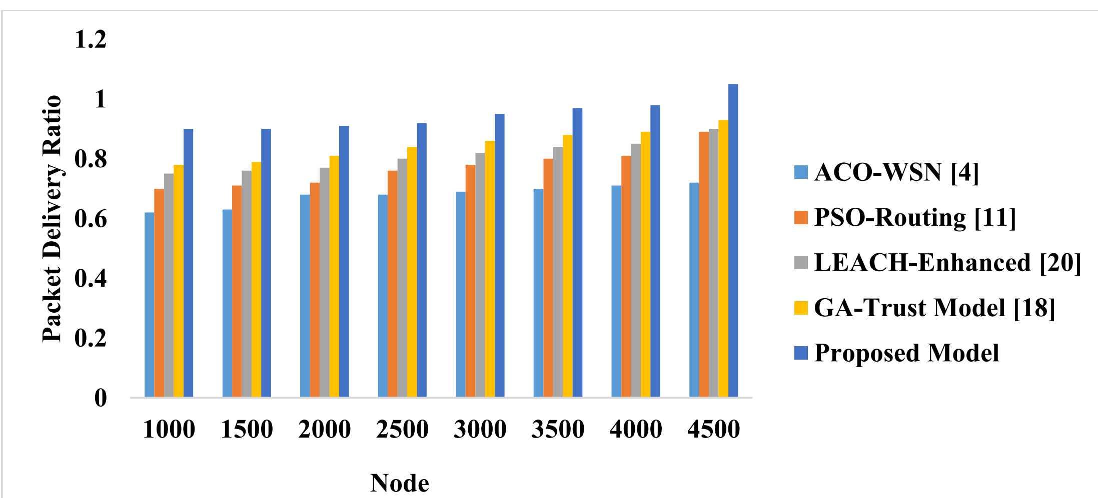

Figure 13 Comparison of Packet Delivery Ratio of Proposed and Existing Works

RESEARCH ARTICLE

The Packet Delivery Ratio (PDR) comparison clearly demonstrates the superior reliability of the proposed model over existing routing methods shown in Figure 13. As the number of rounds increases from 1000 to 4500, the PDR of the proposed system steadily improves from 0.90 to 1.05, indicating consistent and robust packet transmission even under heavier network load. In contrast, ACO-WSN, PSO-Routing, LEACH-Enhanced, and GA-Trust models show lower and slower growth in delivery efficiency, revealing their limitations in dynamic and large-scale wireless sensor network environments. The enhanced trust-based routing and optimized communication strategy in the proposed model effectively mitigate packet loss and improve successful delivery rates.

4.8. Comparison of Performance Measures

The comparison demonstrates the effectiveness of the proposed BAS-GA–optimized model over four existing routing and security systems shown in Figure 14. While existing ACO-WSN, PSO-based routing, LEACH-enhanced clustering, and GA-driven trust models provide moderate performance, they often struggle with dynamic path optimization, energy balancing, and consistent threat detection. The proposed approach delivers superior reliability, reduces misclassification, and enhances secure, energy-efficient communication across underwater and terrestrial sensor networks.

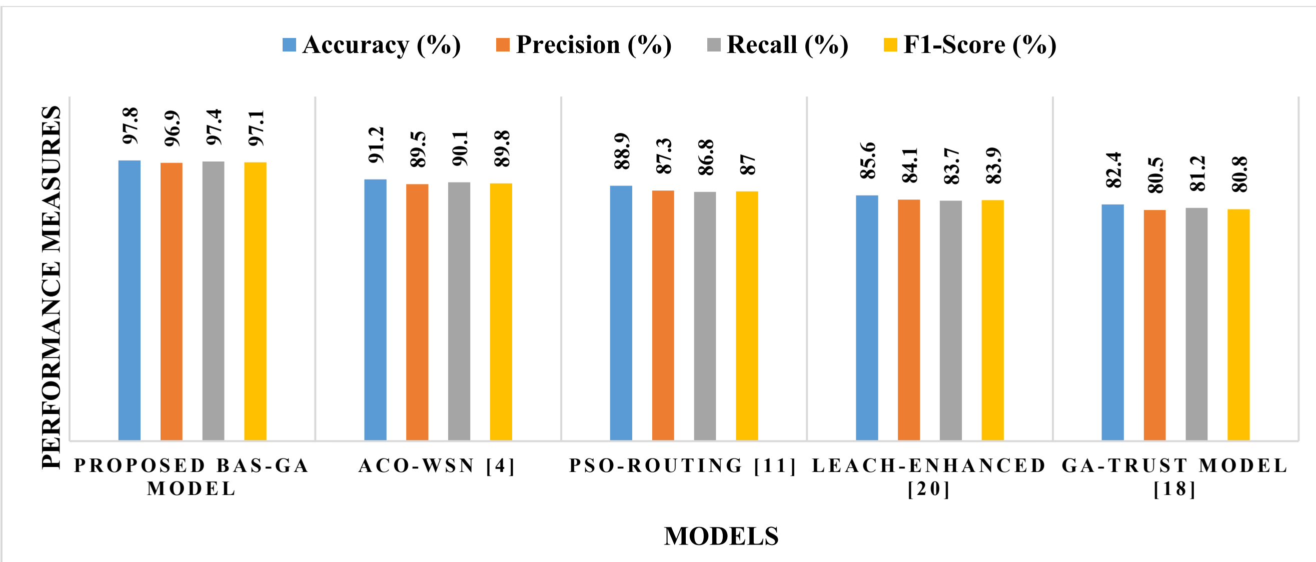

Figure 14 Comparison of Performance Measures

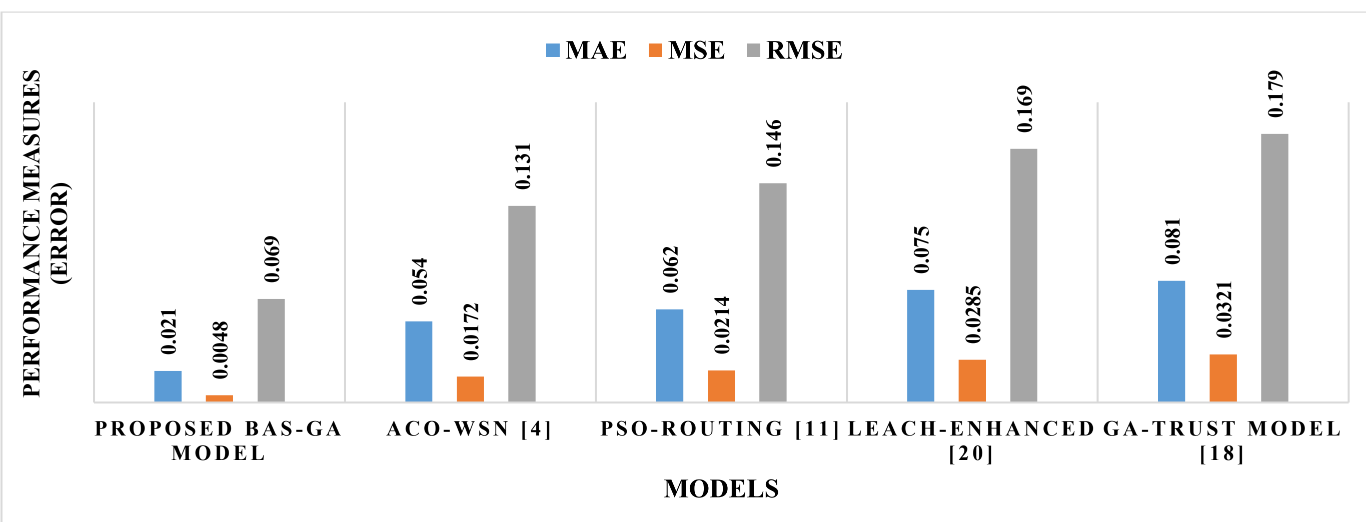

Figure 15 Comparison of Performance Measures (Error)

RESEARCH ARTICLE

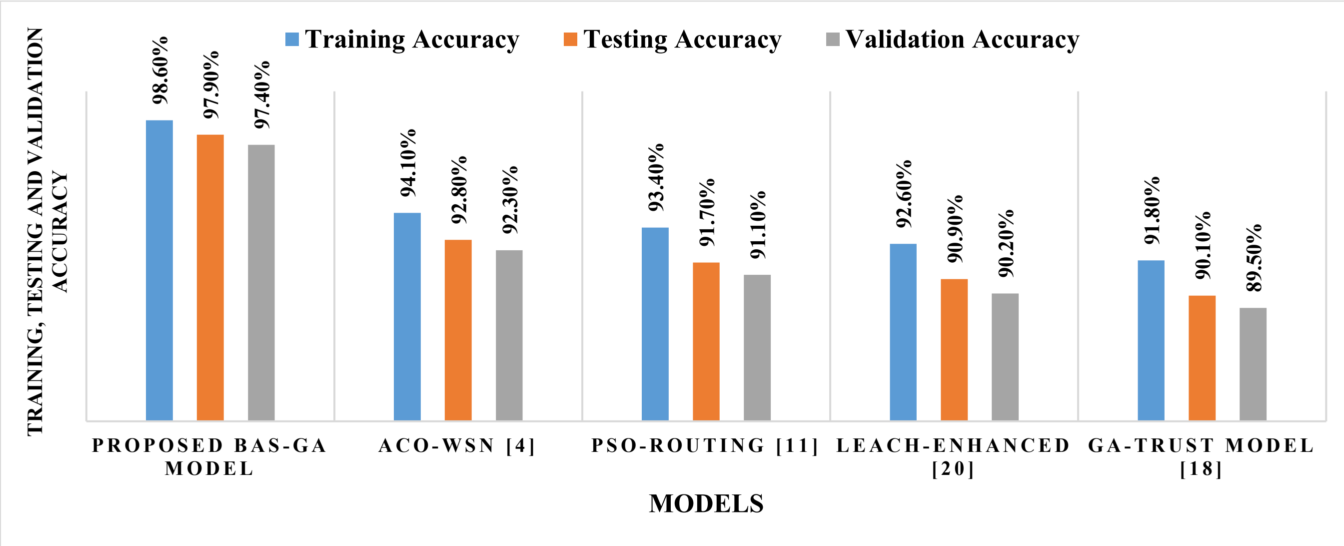

Figure 16 Comparison of Training, Testing and Validation Accuracy

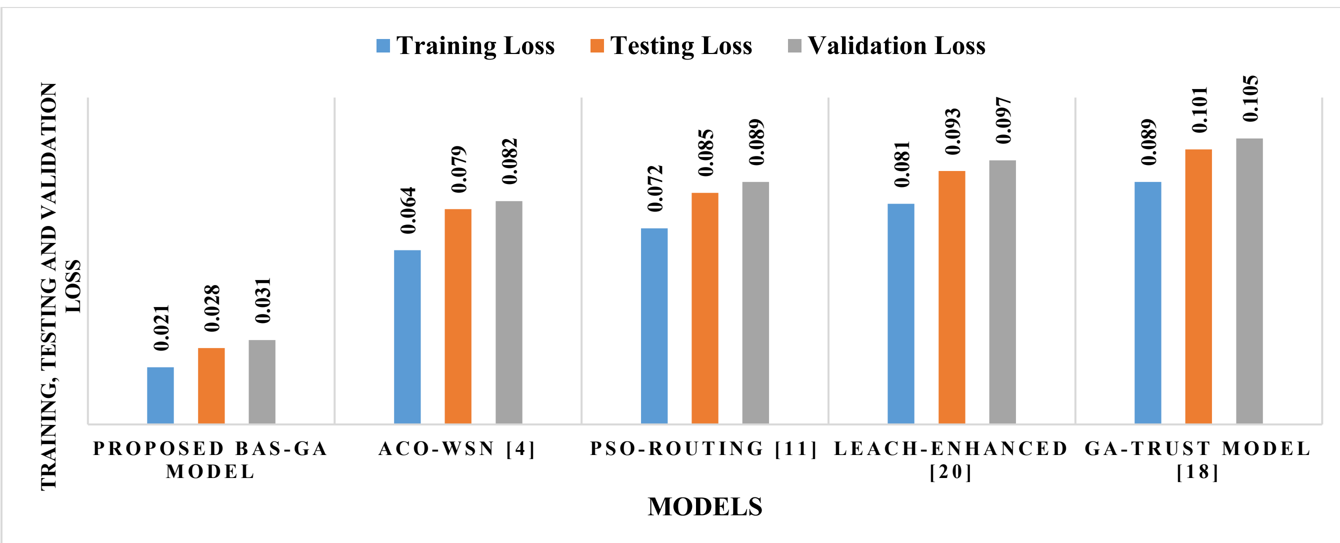

Figure 17 Comparison of Training, Testing and Validation Loss

The error metric comparison clearly highlights the superior performance of the proposed BAS-GA–optimized system. The model achieves the lowest MAE, MSE, and RMSE, indicating minimal prediction error, better route estimation accuracy, and enhanced network stability shown in Figure 15. Existing models such as ACO-WSN, PSO-based routing, enhanced LEACH, and GA-based trust schemes exhibit higher error values, mainly due to limited exploration capability, slower convergence, and susceptibility to unstable underwater conditions. The proposed system effectively minimizes routing deviations and improves link reliability, resulting in significantly more accurate and energy-efficient communication. The performance comparison demonstrates that the proposed BAS-GA–optimized model achieves the highest accuracy in training, testing, and validation phases shown in Figure 16. Its superior performance stems from the hybrid optimization enhances feature selection, parameter tuning, and routing decision accuracy. Existing systems such as ACO-WSN, PSO-Routing, enhanced LEACH, and GA-based trust models show comparatively lower accuracy due to limited search capabilities, slower convergence, and weaker generalization under dynamic underwater conditions.

The proposed BAS-GA–optimized model achieves the lowest training, testing, and validation loss compared to all four existing systems shown in Figure 17. Such minimization of loss demonstrates the high learning stability, parameter tuning and generalization. The hybrid BAS-GA optimization is very

RESEARCH ARTICLE

effective in reducing error in model training by increasing the rate of convergence and avoiding overfitting. The much lesser loss in all the stages validates the strength and stability of the proposed system to provide safe and energy efficient underwater communication.

5. CONCLUSIONS

The hybrid BAS-GA algorithm is a major step toward the improvement of the security of UWSNs. It is essential in the use of applications like water level monitoring, detection of offshore problems, and environmental analysis, yet it have special challenges, such as energy imbalances, vulnerabilities of nodes and various security threats in jamming, eavesdropping and manipulation of data. To solve these problems, new and effective approaches must be developed based on the limitations of underwater environment. This hybrid algorithm proposal will integrate the policy of exploration of BAS to the definition power of GA to improve security and resilience of UWSNs. BAS is derived based on the foraging behaviour of the beetles and is used to efficiently search the solution space, whereas GA is used to optimize solutions through the application of evolutionary principles in successive generations. These methods combined ensure optimal security parameters, which offer strong protection against sophisticated threats at a reasonably small price. The outcomes of simulation prove the quality of the hybrid algorithm to provide the security of UWSNs in real-time without affecting the network life or its performance. It is highly adaptable and can be used in underwater areas with limited resources, which makes it reliable in terms of communication and transmitting data. The study addresses a gap that is a critical issue to security solutions of UWSNs with a scalable and energy efficient mechanism that can protect the underwater infrastructure and data. Different researchers, industrial stakeholders and the regulatory agencies need to liaise to standardize this methodology and continual refinement to have it widely implemented. The hybrid BAS-GA algorithm is a breakthrough move in ensuring that the application of UWSNs is exploited to maximum possibility to benefit the commercial, societal, and environmental advancement without compromising its security and reliability.

REFERENCES

[1] Gunjan. (2023). A review on multi-objective optimization in wireless sensor networks using nature-inspired meta-heuristic algorithms. Neural Processing Letters, 55(3), 2587–2611.

[2] Tyagi, L. K., & Kumar, A. (2024). OEE-WCRD: Optimizing energy efficiency in wireless sensor networks through CH selection using residual energy and distance metrics. EAI Endorsed Transactions on Scalable Information Systems, 11(5), 1–12.

[3] Wu, Y., Zhang, C., Tong, L., & Shi, X. (2023). Location optimization based on improved 3D DV-HOP algorithm in wireless sensor networks. IEEE Access, 11, 45321–45335.

[4] Rhesa, M. J., & Revathi, S. (2024). DBKNN and radial-ANFIS model for energy-efficient wireless sensor network. IEEE Access, 12, 14200–14215.

[5] Daoud, M. S., Shehab, M., Abualigah, L., Alshinwan, M., Elaziz, M. A., Shambour, M. K. Y., & Zitar, R. A. (2023). Recent advances of chimp optimization algorithm: Variants and applications. Journal of Bionic Engineering, 20(6), 2840–2862.

[6] Ghadami, R. (2024). Localization in a wireless sensor network with a geometric approach of trilateration and mathematical modeling of sine and cosine functions. International Journal of Sensor Networks and Data Communications, 13(2), 101–115.

[7] Qiu, S., Zhao, J., Zhang, X., Li, A., Wang, Y., & Chen, F. (2023). CH selection method for edge computing WSN based on improved sparrow search algorithm. Sensors, 23(17), 7572.

[8] Shanthi, K., & Maruthi, R. (2024). Intrusion detection systems and its application in latest networking technologies: A survey. Educational Administration: Theory and Practice, 30(4), 1200–1214.

[9] Nematollahi, M., Ghaffari, A., & Mirzaei, A. (2024). Task offloading in the Internet of Things based on the improved multi-objective Aquila optimizer. Signal, Image and Video Processing, 18(1), 545-552.

[10] Lyu, Y., Mo, Y., Yue, S., & Hong, L. (2023). A mobile robot path planning using an improved beetle swarm optimization algorithm in a static environment. Journal of Intelligent & Fuzzy Systems, 45(3), 1–27.

[11] Petrovic, A., Damaševičius, R., Jovanovic, L., Toskovic, A., Simic, V., Bacanin, N., ... & Spalević, P. (2023). Marine vessel classification and multivariate trajectories forecasting using metaheuristics-optimized extreme gradient boosting and recurrent neural networks. Applied Sciences, 13(16), 9181.

[12] Wang, J., Lin, S., & Liu, A. (2023). Bioinspired perception and navigation of service robots in indoor environments: A review. Biomimetics, 8(4), 350.

[13] Adday, G. H., Subramaniam, S. K., Zukarnain, Z. A., & Samian, N. (2024). Investigating and analyzing simulation tools of wireless sensor networks: A comprehensive survey. IEEE Access, 12, 115238–115260.

[14] Atta, E. A., Ali, A. F., & Elshamy, A. A. (2023). A modified weighted chimp optimization algorithm for training a feed-forward neural network. PLOS ONE, 18(3), e0282514.

[15] Darvishpoor, S., Darvishpour, A., Escarcega, M., & Hassanalian, M. (2023). Nature-inspired algorithms from oceans to space: A comprehensive review of heuristic and meta-heuristic optimization algorithms and its potential applications in drones. Drones, 7(7), 427.

[16] Kumar, A., Dubey, A. K., Ahuja, S., & Dutt, V. (2023). Efficient privacy-preserving lightweight cryptography for multi-hop clustering in Internet of Vehicles network. International Journal of Communication Systems, 36(14), e5637.

[17] Goyat, R., Kumar, G., Saha, R., Conti, M., Thomas, R., & Kim, T. H. (2023). RAPCOL: A range-free power-efficient cooperative localization with heterogeneous devices for industrial Internet-of-Things. Cluster Computing, 26(5), 1–23.

[18] Shi, Y., Zhang, H., Li, Z., Hao, K., Liu, Y., & Zhao, L. (2023). Path planning for mobile robots in complex environments based on improved ant colony algorithm. Mathematical Biosciences and Engineering, 20(9), 15568–15603.

[19] Najibzadeh, M., Mahmoodzadeh, A., & Khishe, M. (2023). Active sonar image classification using deep convolutional neural network evolved by robust comprehensive grey wolf optimizer. Neural Processing Letters, 55(7), 8689-8712.

[20] Giannaros, A., Karras, A., Theodorakopoulos, L., Karras, C., Kranias, P., Schizas, N., & Tsolis, D. (2023). Autonomous vehicles: Sophisticated attacks, safety issues, challenges, open topics, blockchain, and future directions. Journal of Cybersecurity and Privacy, 3(3), 493-543.

[21] Bushehri, A. S., Amirnia, A., Belkhiri, A., Keivanpour, S., de Magalhães, F. G., & Nicolescu, G. (2023). Deep learning-driven

RESEARCH ARTICLE

anomaly detection for green IoT edge networks. IEEE Transactions on Green Communications and Networking, 7(4), 1982–1996.

[22] Islam, M. S., Rahman, M. A., Bin Ameedeen, M. A., Ajra, H., Ismail, Z. B., & Zain, J. M. (2024). Blockchain-enabled cybersecurity provision for scalable heterogeneous network: A comprehensive survey. CMES–Computer Modeling in Engineering & Sciences, 138(1), 1–40.

[23] Aziz, S., Ahmed, I., Khan, K., & Khalid, M. (2023). Emerging trends and approaches for designing net-zero low-carbon integrated energy networks: A review of current practices. Arabian Journal for Science and Engineering, 48(5), 1–23.

[24] Salodkar, S. M., Sharma, G., & Susheel, C. (2024). Emerging materials, technologies, and solutions for energy harvesting. In N. K. Dhiman (Ed.), Emerging Materials, Technologies, and Solutions for Energy Harvesting (pp. 130–165). Springer Nature.

[25] Poornima, G., Sakkari, D. S., Manjunath, T. N., Gowda, M. S., & Pallavi, R. (2023). Analysis of geospatial data collected by drones as part of aerial computing. In Drone Data Analytics in Aerial Computing (pp. 33–89). Singapore: Springer Nature Singapore.

[26] Ferrag, M. A., Kantzavelou, I., Maglaras, L., & Janicke, H. (Eds.). (2023). Hybrid Threats, Cyberterrorism and Cyberwarfare. Boca Raton, FL: CRC Press.

[27] Ang'udi, J. J. (2023). Security challenges in cloud computing: A comprehensive analysis. World Journal of Advanced Engineering Technology and Sciences, 10(2), 155–181.

[28] Ping, J., & Ying, Y. (2023). Triboelectric Nanogenerators for Field Sensing. In Encyclopedia of Digital Agricultural Technologies (pp. 1480-1489). Cham: Springer International Publishing.

[29] van Meer, N. M. M. E., Lankheet, M. J. M., & van Leeuwen, J. L. (2024). Quantification of the three-dimensional architecture of axial muscle fibers in larval fish. In SICB 2024: The Society for Integrative and Comparative Biology with the American Microscopical Society, Minorities in Shark Sciences, The Crustacean Society (pp. 317–317).

[30] Eris, C., Gul, O. M., & Boluk, P. S. (2024). A novel medium access policy based on reinforcement learning in energy-harvesting underwater sensor networks. Sensors, 24(17), 5791.

Authors

Dr Suganya J is currently working as Assistant professor in the Department of Computer Applications, Faculty of Science and Humanities, SRM Institute of Science and Technology, SRM Nagar, Trichy. She has received her doctoral degree from AVVM Sri Pushpa College (Autonomous), Poondi, Thanjavur Dt. affiliated to Bharathidasan University, Tiruchirappalli. She has qualified State Eligibility Test (SET) in Computer Science from Mother Terasa University, Kodaikanal. She has 14 years of teaching experience. She has published two Patents and research papers in various National, International Journals and authored one book. Also, she acted as a resource person in seminars and workshops. She received two awards for academic excellence. She is acting as editorial member in peer reviewed journals.

Dr Senthil Kumar S received his first degree from Madras University, Computer Science, India, in 2005. He has also Master degree from Thiruvalluvar University, Computer Applications, India, in 2008. The Ph.D. degree from the Department of Computer Applications in Manonmaniam Sundaranar University, India in 2019. He is currently serving as an Assistant Professor in Department of Computer Applications at SRM Institute of Science and Technology, Tiruchirappalli, Tamil Nadu, India. He has published More than 20 articles in reputed peer-reviewed National and International Journals, 5 chapters. He has received 4 awards like Best Faculty Award, Best Scientist Award, Young Researcher Award etc. His main research interests focus on Web Metrics, Web Services, Computer Networks, Image Processing, Data Mining, and Text Mining.

Dr Prakash M is currently working as Assistant professor in the Department of Artificial Intelligence and Data Science, VET Institute of Arts and Science (Co-education) College, Erode. He received his doctoral degree from Bharathiar University, Coimbatore. He has 5 years of teaching experience. He has published one Patent and research papers in various National, International Journals and authored one book. Also, he acted as a resource person in seminars and workshops. He received two awards for academic excellence. He is acting as editorial member in peer reviewed journals.

Mrs Akilandeswari S is currently working as an Assistant Professor in the Department of Artificial Intelligence and Data Science at E.G.S. Pillay Engineering College, Nagapattinam. She is presently pursuing her Ph.D. at Anna University, Chennai. She has 9 years of teaching experience. She has published two patents and several research papers in various national and international journals, and has authored two books. She has also served as a resource person in seminars and workshops. She has received two awards for academic excellence.

Dr Anitha P is currently working as a Guest Lecturer in the Department of Computer Science, Thiru Vi Ka Government College, Thiruvarur. She has received her doctoral degree from AVVM Sri Pushpam College (Autonomous), Poondi, Thanjavur Dt., affiliated to Bharathidasan University, Tiruchirappalli. She has 16 years of teaching experience. She has published research papers and has acted as a resource person in seminars and workshops. She received one award for Best Teacher.

Dr Paul Arokiadass Jerald M graduated from University of Madras, Computer Science, India, in 1992. He has completed his Post Graduation (M.C.A) degree in 1995 from Bharathidasan University, Tiruchirappalli. He has done his Ph.D. from Manonmaniam Sundaranar University, India in 2019. He is currently serving as an Associate Professor in Department of Computer Science at Periyar Arts College, Cuddalore, Tamil Nadu, India. He has published More than 10 articles in reputed peer-reviewed National and International Journals. His main research interests include Software Engineering, Web Services, Image Processing and Data Mining.

RESEARCH ARTICLE

How to cite this article:

Suganya J, Senthil Kumar S, Prakash M, Akilandeswari S, Anitha P, Paul Arokiadass Jerald M, “Enhancing Security in Underwater Wireless Sensor Networks using a Hybrid Approach of Beetle Antenna Search and Genetic Algorithms”, International Journal of Computer Networks and Applications (IJCNA), 12(6), PP: 953-972, 2025, DOI: 10.22247/ijcna/2025/56.