iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 14 **Issue:** IV **Month of publication:** April 2026

**DOI:** https://doi.org/10.22214/ijraset.2026.80886

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 14 Issue IV Apr 2026- Available at www.ijraset.com*

# A Comparative Study of Clustering, Routing, and Security Algorithms for IoT-Enabled Underwater Wireless Sensor Networks

Mr. V. Balasubramaniyam[1], Dr. P. Srimanchari[2]
[1]*Research Scholar,* [2]*Assistant Professor, Department of Computer Science, Erode Arts and Science College, Erode, Tamilnadu*

***Abstract:*** ***The rapid integration of Internet of Things paradigms into aquatic domains has given rise to the Internet of Underwater Things, wherein Underwater Wireless Sensor Networks serve as the foundational communication infrastructure. These networks enable critical applications including ocean exploration, environmental monitoring, seismic prediction, military surveillance, and subsea pipeline inspection. This paper presents a structured comparative study of state-of-the-art algorithms across the three interdependent functional layers of IoT-enabled UWSNs: clustering, routing, and security. In the clustering layer, bio-inspired metaheuristic approaches, machine learning-based schemes, AUV-assisted protocols, and fuzzy logic-based clustering frameworks are systematically reviewed and evaluated against metrics including network lifetime, energy consumption, and packet delivery ratio. In the routing layer, geographic and opportunistic protocols, trust-based and void-aware routing schemes, reinforcement learning-driven approaches, and hybrid AI-routing frameworks are comparatively analysed. In the security layer, lightweight cryptographic and signcryption schemes, multi-attribute trust management frameworks, deep learning-based intrusion detection systems, federated learning IDS, and blockchain-assisted security mechanisms are evaluated for their detection capability and deployment feasibility on resource-constrained acoustic nodes. The comparative analysis reveals a consistent pattern across all three layers: existing algorithms demonstrate strong performance under controlled simulation conditions but exhibit significant degradation when confronted with the physical realities of underwater deployment particularly dynamic node topology, acoustic channel unpredictability, and embedded hardware resource constraints. The most promising directions for original contribution are identified as: mobility-aware DRL clustering with provable convergence bounds, adaptive trust calibration mechanisms that distinguish malicious behaviour from acoustic channel-induced packet loss, and lightweight CNN-GRU model compression for real-time intrusion detection on constrained UWSN nodes. Cross-layer performance trade-offs are analysed, and a unified framework perspective is proposed, demonstrating that the interaction between upstream clustering decisions and downstream routing and security performance constitutes the central open problem in holistic UWSN system design.***

***Keywords: Underwater Wireless Sensor Networks, Internet of Underwater Things, Clustering algorithms, Routing protocols, Intrusion detection, Deep reinforcement learning, Trust management, Lightweight cryptography, IoT security, Acoustic communication.***

## I. INTRODUCTION

### *A. Background and Motivation*

The rapid proliferation of the Internet of Things has extended its transformative influence beyond terrestrial environments into aquatic domains, giving rise to the Internet of Underwater Things. Underwater Wireless Sensor Networks form the foundational infrastructure of IoUT, enabling a wide range of applications including ocean exploration, environmental monitoring, seismic prediction, military surveillance, and pipeline inspection [1]. These networks consist of sensor nodes deployed at various depths, communicating primarily through acoustic channels due to the rapid attenuation of radio frequency (RF) signals in water.

Unlike conventional terrestrial wireless sensor networks, UWSNs operate in a uniquely challenging environment characterized by high propagation delay, limited bandwidth, severe multipath fading, node mobility induced by underwater currents, and constrained energy resources. The three-dimensional nature of underwater deployments further complicates network design and management. Addressing these challenges requires sophisticated algorithmic solutions that optimize network performance across multiple layers from cluster formation and data aggregation to multi-hop routing and secure data transmission.

The integration of IoT paradigms into UWSNs [2] introduces additional complexity in terms of heterogeneous device interoperability, real-time data delivery requirements, and cybersecurity vulnerabilities. As these networks are increasingly deployed in critical monitoring and defense applications, ensuring reliable, energy-efficient, and secure communication has become a paramount research objective.

### *B. Problem Statement*

The design of an efficient IoT-enabled UWSN requires the coordinated interplay of three critical functional layers: (i) Clustering — organizing sensor nodes into manageable groups with elected cluster heads (CHs) for localized data aggregation; (ii) Routing — determining optimal paths for forwarding aggregated data from CHs toward surface sink nodes or autonomous underwater vehicles (AUVs); and (iii) Security — protecting the network from adversarial threats such as black hole attacks, sinkhole attacks, replay attacks, and unauthorized access.

A significant body of research has independently addressed each of these layers. Bio-inspired metaheuristic approaches such as Gray Wolf Optimization (GWO), Dragonfly Optimization, and Artificial Fish Swarm algorithms have been proposed for cluster head selection. Routing protocols leveraging trust models, geographic forwarding, and reinforcement learning have been developed to address void hole and energy balance challenges. Security frameworks employing lightweight cryptography, intrusion detection systems (IDS), federated learning, and blockchain have been explored to counter underwater-specific threats.

However, a comprehensive comparative evaluation that simultaneously examines these three layers within a unified analytical framework is conspicuously absent from the literature. Existing studies either evaluate algorithms in isolation or restrict comparisons to a single functional layer, leaving researchers and practitioners without holistic guidance for system-level design decisions.

### *C. Objectives and Contributions*

This paper presents a structured comparative study of recent algorithmic advances across the three interdependent layers of IoT-enabled UWSNs. The key contributions of this work are as follows:

- A systematic review and categorization of state-of-the-art clustering algorithms, including bio-inspired, deep reinforcement learning-based, fuzzy logic-based, and AUV-assisted clustering schemes published between 2023 and 2025.
- A comparative analysis of contemporary routing protocols, encompassing trust-based routing, geographic opportunistic routing, reinforcement learning-based routing, and physics-informed routing strategies.
- A comprehensive evaluation of security mechanisms including lightweight signcryption, intrusion detection systems (CNN-GRU, XGBoost-based), trust management frameworks, federated learning, and blockchain-assisted schemes.
- An analysis of the interdependencies and trade-offs among the three layers — energy efficiency, packet delivery ratio, latency, network lifetime, and security overhead — providing cross-layer design insights.
- Identification of open research challenges and future directions for the design of holistic, secure, and energy-efficient IoT-UWSN systems.

### *D. Scope and Limitations*

This study focuses on IoT-integrated acoustic UWSN environments, with particular emphasis on algorithms published from 2023 to 2025 to ensure currency and relevance.

The comparative framework considers key performance metrics including energy consumption, network lifetime, packet delivery ratio (PDR), end-to-end delay, throughput, and security overhead. Optical wireless and hybrid acoustic-optical systems are noted where relevant but are not the primary focus of this comparative analysis. Additionally, this study relies on simulation-based results as reported in primary literature, rather than physical testbed deployments.

### *E. Paper Organization*

The remainder of this paper is organized as follows. Section 2 provides background on UWSN architecture, acoustic communication challenges, and the IoT-UWSN integration model. Section 3 presents a comparative review of clustering algorithms. Section 4 analyzes routing protocols. Section 5 evaluates security mechanisms. Section 6 discusses performance evaluation results. Section 7 concludes the paper.

## II. BACKGROUND AND RELATED WORKS

### *A. IoT-Enabled UWSN Architecture*

Underwater Wireless Sensor Networks are spatially distributed networks of sensor nodes deployed across a three-dimensional aquatic environment to collaboratively sense, process, and transmit data to surface or onshore stations. The integration of Internet of Things principles into UWSNs has given rise to the Internet of Underwater Things [3], a paradigm that extends IoT connectivity beneath the water surface, enabling real-time monitoring, intelligent sensing, and automated control in marine environments.

A typical IoT-enabled UWSN architecture consists of four principal layers: (i) the Sensing Layer, comprising battery-powered underwater sensor nodes equipped with acoustic modems, pressure sensors, temperature sensors, and hydrophones; (ii) the Network Layer, which manages communication between nodes and cluster heads using acoustic signal propagation; (iii) the Aggregation and Processing Layer, involving cluster heads (CHs) or Autonomous Underwater Vehicles (AUVs) that collect, compress, and forward data; and (iv) the Application Layer, consisting of surface buoys, gateway nodes, and onshore servers that interface with cloud platforms and end-user applications.

Unlike terrestrial IoT architectures that primarily employ radio frequency (RF) communication, UWSNs rely on acoustic wave propagation as the dominant communication modality. This is because RF signals attenuate rapidly in water — reaching only a few centimeters at GHz frequencies — whereas acoustic signals can propagate over hundreds to thousands of meters at speeds of approximately 1500 m/s. Some emerging deployments also incorporate optical wireless communication for short-range, high-bandwidth links in clear water conditions, giving rise to hybrid acoustic-optical UWSN architectures.

The architectural design of IoUT-enabled UWSNs must accommodate several unique operational requirements. Nodes must support depth-adjustable buoyancy for three-dimensional deployment. Energy harvesting techniques [4] including tidal energy, thermal gradients, and piezoelectric transduction are increasingly investigated to extend node lifetime. AUVs serve dual roles as mobile data mules for data collection and as relay nodes for bridging communication gaps in sparse deployments. Surface gateway nodes aggregate data from multiple CHs and provide connectivity to terrestrial IoT platforms via satellite or cellular links.

Table 1: Comparison of Terrestrial WSN and IoT-Enabled UWSN Architectures

| Parameter | Terrestrial WSN | IoT-Enabled UWSN |
|---|---|---|
| Communication Medium | Radio Frequency (RF) | Acoustic / Optical |
| Propagation Speed | $3 \times 10^8$ m/s | ~1500 m/s |
| Bandwidth | High (GHz range) | Very Limited (kHz range) |
| Node Mobility | Mostly static | Dynamic (underwater currents) |
| Topology | 2D | 3D |
| Energy Source | Battery / Solar | Battery / Tidal / Thermal |
| Deployment Environment | Terrestrial, stable | Aquatic, harsh, dynamic |
| Security Threats | Eavesdropping, DoS | Acoustic jamming, black hole, replay |

### *B. Challenges in Underwater Acoustic Communication*

The acoustic channel in underwater environments is fundamentally different from radio channels in terrestrial networks, presenting a distinct set of physical and networking challenges that directly influence the design of clustering, routing, and security protocols.

Propagation Delay and Delay Spread: Acoustic signals travel at approximately 1500 m/s — five orders of magnitude slower than electromagnetic waves [5] resulting in significant propagation delays that range from milliseconds to seconds depending on network scale. This high delay severely impairs time-sensitive protocols and necessitates the design of delay-tolerant networking strategies.

*Limited and Distance*-Dependent Bandwidth: The usable acoustic bandwidth decreases with increasing transmission distance. Shallow water deployments may utilize frequencies up to 100 kHz, while deep water long-range links are constrained to frequencies

below 5 kHz, limiting data rates to a few kilobits per second. This bandwidth scarcity demands aggressive data compression and aggregation at the cluster head level.

*Multipath Propagation and Doppler Effect:* Acoustic signals reflect off the sea surface, seabed, and underwater structures, creating multiple signal copies that arrive at the receiver at different times. This multipath fading significantly degrades signal quality. Furthermore, node movement due to ocean currents introduces Doppler shift, complicating synchronization and channel estimation in mobile UWSN deployments.

*Energy Constraints*: Sensor nodes in UWSNs are typically battery-powered with no opportunity for recharging or manual replacement after deployment [6]. Acoustic transceivers consume substantially more power than RF transceivers. The energy cost of transmitting one bit acoustically is orders of magnitude higher than in terrestrial WSNs, making energy-efficient clustering and routing protocols critically important for network longevity.

*Three-Dimensional Node Mobility*: Unlike terrestrial networks, underwater sensor nodes are subject to three-dimensional displacement caused by ocean currents, tidal forces, and wave action. This dynamic topology makes static routing table maintenance infeasible and requires distributed, adaptive algorithms capable of re-clustering and re-routing in real time.

*Security Vulnerabilities:* The broadcast nature of acoustic communication makes UWSNs inherently susceptible to eavesdropping, jamming, and replay attacks. The resource-constrained nature of nodes limits the applicability of computationally expensive cryptographic schemes. Unique underwater attack vectors including acoustic flooding, depth-based routing manipulation, and black hole attacks exploiting void regions necessitate lightweight yet robust security mechanisms. Table 2 summarizes the key challenges in underwater acoustic communication and their impact on the three functional layers studied in this paper.

Table 2: UWSN Communication Challenges and Their Impact on Functional Layers

| Challenge | Root Cause | Impact on Clustering / Routing / Security |
|---|---|---|
| High Propagation Delay | Low acoustic speed (~1500 m/s) | Delays CH election, degrades routing convergence |
| Limited Bandwidth | Frequency-distance dependency | Restricts data aggregation and overhead packets |
| Multipath Fading | Reflection from surfaces | Increases packet loss, degrades PDR |
| Node Mobility | Underwater currents and tides | Invalidates static cluster/routing structures |
| Energy Scarcity | No recharging post-deployment | Limits CH re-election frequency and security overhead |
| Acoustic Eavesdropping | Broadcast medium | Enables passive attacks; requires encryption |
| 3D Topology | Volumetric deployment | Complicates depth-based and geographic routing |

### *C. Survey of Existing Comparative Studies*

The growing research interest in UWSNs has generated a substantial body of literature, with several survey and comparative studies examining specific algorithmic domains. However, a critical analysis of the existing literature reveals that no comprehensive comparative study simultaneously addresses clustering, routing, and security within a unified IoT-UWSN framework a gap that this paper directly addresses.

In the domain of clustering, Majid et al. [7] surveyed energy-efficient clustering protocols for UWSNs, categorizing approaches based on CH selection criteria including residual energy, node density, and distance to sink. Their analysis highlighted the superior lifetime extension offered by bio-inspired algorithms over static threshold-based methods such as LEACH. Similarly, Javaid et al. [8] reviewed optimization-based clustering approaches, noting the growing adoption of swarm intelligence techniques including

Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO), and Genetic Algorithms (GA). However, these surveys predate the recent wave of deep learning and hybrid metaheuristic approaches that emerged in 2024–2025.

In routing, Coutinho et al. [9] provided a comprehensive taxonomy of opportunistic routing protocols for UWSNs, classifying approaches by void-handling strategy, energy model, and mobility support. Zhu et al. [10] surveyed reinforcement learning-based routing, demonstrating that multi-agent RL approaches achieve significant improvements in end-to-end delay and energy balance over traditional geographic routing schemes. Despite these contributions, the interaction between routing performance and upstream clustering decisions particularly in terms of cluster head placement and void hole probability remains underexplored.

In security, Domingo [43] presented one of the earliest surveys of security protocols for UWSNs, identifying authentication, key management, and intrusion detection as the primary research priorities. More recently, Hamdan et al. [11] reviewed machine learning-based intrusion detection systems for IoT-integrated UWSNs, reporting that deep learning models such as CNN-LSTM hybrids achieve detection accuracies exceeding 98% on benchmark datasets. Blockchain-assisted security schemes were surveyed by Ali et al. [12], who highlighted their potential for tamper-proof data provenance in distributed underwater monitoring systems.

Critically, existing surveys treat the three layers as independent concerns. Clustering surveys assume idealized routing; routing studies assume pre-formed clusters; security analyses rarely account for the energy overhead imposed on cluster heads managing both aggregation and cryptographic operations simultaneously. This partitioned treatment obscures the system-level trade-offs that arise when all three layers are co-deployed in a real UWSN. Table 3 summarizes key existing surveys and their scope relative to the present work.

TABLE 3: COMPARISON OF EXISTING SURVEY STUDIES WITH THE PRESENT WORK

| Study | Year | Clustering | Routing | Security | IoT Integration |
|---|---|---|---|---|---|
| Majid et al. [7] | 2022 | Yes | No | No | Partial |
| Javaid et al. [8] | 2023 | Yes | Partial | No | No |
| Coutinho et al.[ 9] | 2021 | No | Yes | No | No |
| Zhu et al.[10] | 2023 | No | Yes | No | Partial |
| Hamdan et al. [11] | 2024 | No | No | Yes | Yes |
| Ali et al. [12] | 2024 | No | Partial | Yes | Yes |

The present work distinguishes itself from the aforementioned studies by adopting a pipeline-oriented comparative framework that evaluates clustering, routing, and security algorithms in sequence and in relation to one another. By analyzing the performance implications of combining specific algorithmic choices across all three layers, this paper provides practitioners with actionable guidance for holistic UWSN system design within an IoT deployment context.

## III. CLUSTERING ALGORITHMS IN IOT-ENABLED UWSNS

Among the three functional layers examined in this study, clustering occupies the most foundational position: without stable, energy-balanced cluster formation, both routing efficiency and security management deteriorate substantially. The objective of a clustering protocol is to partition the sensor field into logical groups, each governed by a cluster head (CH) responsible for local data aggregation and inter-cluster communication. In terrestrial WSNs, this problem has been approached through threshold-based probabilistic methods such as LEACH and HEED. However, directly adapting these schemes to the three-dimensional, acoustically-challenged underwater environment produces unsatisfactory results static probability thresholds ignore node depth, current-induced displacement, and the asymmetric energy costs of acoustic transmission.

The past two years have seen a decisive shift toward optimization-driven clustering, where CH selection and cluster boundary formation are treated as NP-hard combinatorial problems amenable to metaheuristic, machine learning, and hybrid solution strategies. The following subsections review the principal algorithmic families within this space, drawing on publications from 2023 to 2025.

### A. *Bio-Inspired Metaheuristic Clustering*

Nature-inspired optimization algorithms have proven particularly well-suited to UWSN clustering because they can navigate large, irregular solution spaces without requiring gradient information — a necessity when the objective function involves discrete node selections, irregular 3D geometries, and non-differentiable energy models. Several distinct families have been explored.

#### 1) *Gray Wolf-Based Approaches*

The Gray Wolf Optimizer (GWO) models the hierarchical hunting behaviour of wolf packs, where alpha, beta, and delta wolves guide the remainder of the population toward optimal prey positions. Its natural hierarchy makes it an intuitive fit for leader-follower cluster head selection in sensor networks. Jia, et. al., proposed CTRGWO-CRP [13] augments the standard GWO framework with three targeted modifications: a cloning operator that replicates high-fitness individuals to preserve solution quality across generations, a t-distribution perturbation mutation to diversify the search landscape, and opposition-based learning that evaluates candidate solutions against their mirror positions in the search space. Collectively, these additions counteract the premature convergence that plagues standard GWO in high-dimensional node configurations. Reported results place CTRGWO-CRP at a 23.5% improvement in network lifetime over LEACH under equivalent node density and transmission distance conditions, with consistently lower per-round energy variance — an indicator of balanced CH load distribution across the network.

#### 2) *Marine and Aquatic Predator Algorithms*

The Marine Predator Algorithm draws from the Lévy and Brownian movement patterns observed in ocean predator foraging, encoding both exploratory long-distance search and exploitative local refinement in a single framework. Khafaga et al. [14] combined MPA with the Hunger Games Search (HGS) algorithm in a dual-phase hybrid HGS-MPA where MPA governs initial cluster formation and HGS subsequently optimises inter-cluster routing paths. The decision to separate these two roles across distinct algorithms, rather than applying a single scheme to both problems, proved consequential: HGS-MPA consumed 26.6% less energy per round than a GWO-PSO baseline while sustaining a packet delivery ratio of 92.4%, which represented a 3.1 percentage point improvement over the next best competitor. Statistical validation via ANOVA confirmed the significance of these gains at $p < 0.001$, lending credibility beyond simulation artefact.

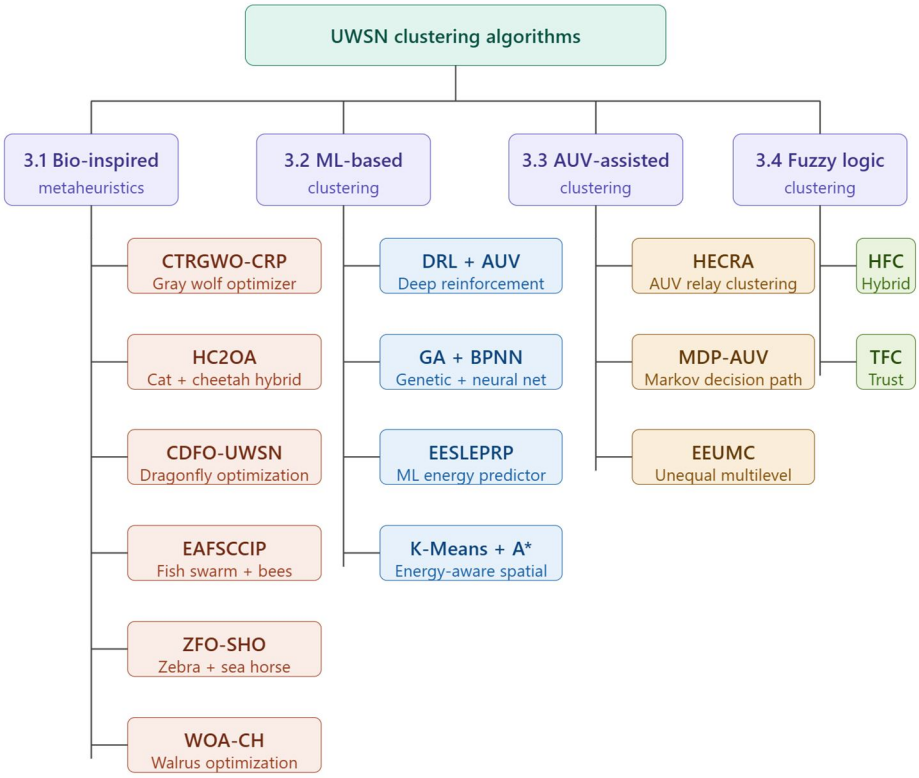



Fig 1: Taxonomy of UWSN Clustering Algorithms

*3) Swarm Collective Behaviour Algorithms*

Fish school and bird flocking analogies have inspired several clustering protocols that exploit collective emergent behaviours rather than individual fitness hierarchies. The Artificial Fish Swarm algorithm, as incorporated in EAFSCCIP [17], models the foraging, following, and swarming behaviours of fish schools to drive cluster formation. When combined with a Bees Algorithm optimisation layer for CH selection, EAFSCCIP demonstrated more stable cluster size distributions under mobile node conditions than static-weight protocols, an important property given that underwater current displacement is a persistent operational reality. Similarly, the Dragonfly Optimisation Algorithm (DOA) exploited in CDFO-UWSN [15] models the swarming and hunting phases of dragonfly colonies to distinguish between exploration (swarming for predator avoidance) and exploitation (hunting for prey). Applied to a 1500 × 1500 m simulation grid, CDFO-UWSN improved active node count by 78.13% compared to standard GWO and showed a 64.71% gain in effective transmission range, largely because the hunting phase naturally concentrates cluster boundaries around high-density node regions rather than imposing geometrically uniform partitions.

*4) Hybrid Multi-Species Optimizers*

A growing strand of research pairs two distinct animal-inspired algorithms each with complementary search characteristics to compensate for individual weaknesses. Nayyar et. al., proposed HC2OA (Hybrid Cat Cheetah Optimisation Algorithm) [16] combines cat swarm optimisation's fine-grained local search with the cheetah algorithm's rapid global pursuit to perform both CH selection and sub-cluster formation in a single pass. The inclusion of a sub-clustering layer is significant: by grouping nodes within a primary cluster into smaller sub-units, HC2OA reduces intra-cluster collision probability and amortises the data aggregation burden more evenly across member nodes. Simulation results reported 0.2 J of average energy consumption per round alongside a 95% packet delivery ratio — figures that are competitive even against more computationally demanding ML-based approaches. Mohammed et. al., designed the ZFO-SHO [18] protocol (Zebra and Sea Horse Optimisation) applies a two-phase structure in which the zebra's predator-evasion heuristic handles initial dynamic cluster formation, while sea horse optimisation's spiral movement pattern refines the CH selection and data path simultaneously.

*B. Machine Learning-Based Clustering*

Whereas metaheuristic algorithms treat each clustering round as an independent optimisation problem, machine learning approaches attempt to learn generalizable policies that improve over time through accumulated experience. This distinction matters considerably in dynamic underwater deployments, where node positions, residual energies, and channel conditions evolve between rounds.

*1) Deep Reinforcement Learning Clustering*

DRL frames CH selection as a sequential decision problem modelled by a Markov Decision Process (MDP). At each round, an agent observes the current network state node positions, residual energies, and channel quality estimates and selects a set of cluster heads to maximise a defined cumulative reward. The reward function typically encodes energy efficiency, load balance, and data delivery reliability simultaneously, enabling the policy to discover trade-off solutions that static optimisation criteria cannot represent. A recent study applied DRL to joint CH selection and AUV trajectory optimisation in IoUT deployments. Once the DRL agent assigned cluster heads, AUVs navigated dynamically toward the elected CHs rather than following predetermined waypoints, improving data collection efficiency under the influence of unpredictable node drift. The formulation using an encoder-decoder neural architecture where the encoder processes the full network topology and the decoder outputs per-AUV cluster access sequences permitted the scheme to scale to network sizes that exhaustive search methods cannot practically address. Compared to K-means-based static clustering with greedy AUV routing, the DRL framework achieved materially higher Value of Information (VoI) metrics, particularly in scenarios with high node mobility, where static topological assumptions cause rapid policy degradation.

*2) Genetic Algorithm and Neural Network Hybrids*

Several authors have paired genetic algorithms for CH selection with backpropagation neural networks for data aggregation, forming a two-stage pipeline where evolutionary search handles the discrete CH assignment problem and the neural layer handles the continuous data compression problem. In one such protocol, an improved GA minimises a multi-objective fitness function combining residual energy, distance to sink, and node degree, while a BP neural network at each elected CH predicts inter-cluster forwarding paths. This separation of concerns evolutionary methods for combinatorial selection, gradient-based methods for continuous approximation allows each component to be tuned independently and adapted to changing network conditions without full model retraining.

### C. AUV-Assisted and Hierarchical Clustering

AUV-assisted clustering introduces a mobile infrastructure element into what is otherwise a static or semi-static tier arrangement. Rather than routing aggregated data through multi-hop acoustic paths which impose heavy relay burdens on intermediate nodes. AUV-assisted schemes designate autonomous vehicles as dynamic data collectors that visit cluster heads on optimised trajectories.

Chen et. at., [19] proposed HECRA (High-Efficiency Clustering Routing with AUV) which organises the network into clusters through a distance and residual energy fitness function, then deploys a single AUV as a relay for CHs whose acoustic range falls short of the surface sink. The AUV's itinerary is computed once per epoch based on elected CH positions, limiting computational overhead while still eliminating the multi-hop chains responsible for the hotspot energy imbalance observed in purely relay-based architectures. Measured against LEACH under identical deployment parameters, HECRA reduced average dead node counts by 20.18% at the network half-lifetime point  a metric that more faithfully captures real operational longevity than simple total energy plots.

The Energy-Aware K-Means with A* path planning framework [20] takes a more structured approach to the same problem: nodes are clustered using a modified K-means algorithm whose distance metric accounts for both Euclidean position and normalised residual energy, ensuring that energy-depleted nodes are not consistently assigned to CH-adjacent roles. The A* algorithm then computes AUV navigation paths over a bathymetric grid, incorporating terrain obstacles — seamounts, ridges, pipe structures — that purely distance-optimal paths would ignore.

### D. Fuzzy Logic-Based Clustering

Fuzzy logic offers a principled mechanism for handling the inherent imprecision in underwater state estimation: residual energy readings carry sensor uncertainty, distance estimates are subject to acoustic multipath distortion, and traffic load projections depend on application-layer behaviour that is difficult to anticipate. Rather than forcing crisp threshold decisions as LEACH does with its fixed CH probability fuzzy clustering systems compute CH candidacy as a continuous degree of membership across multiple linguistic variables.

Hassan et. al., [21] designed Fuzzy logic-based hybrid clustering protocol defined three input variables such as residual energy, normalised distance to sink, and current intra-cluster data load as fuzzy sets, and derived CH selection through a rule base that weighted these factors contextually rather than additively. Against the DABC and IDACB baseline protocols, this approach reduced routing overhead packets by 29%, increased PDR by 19%, and improved energy variance across nodes by 40%. The variance metric is worth particular attention: in networks where CH rotation is poorly balanced, variance grows rapidly as a subset of nodes approaches depletion while others remain near full charge a condition that precedes network partitioning. The fuzzy scheme's superior variance control directly translates to more predictable network longevity.

Table 4: Comparative Study of Clustering Algorithms for IoT-Enabled UWSNs (2023–2025)

| Algorithm | Year | Core Technique | Key Metric Gain | Baseline Compared | Limitation |
|---|---|---|---|---|---|
| CTRGWO-CRP [13] | 2025 | Improved GWO + cloning + OBL | +23.5% network lifetime | LEACH, GWO, ACO | High computation per round |
| HGS-MPA [14] | 2025 | Marine Predator + Hunger Games hybrid | 26.6% energy saving; 92.4% PDR | GWO-PSO, LEACH | Dual-algorithm tuning complexity |
| Fuzzy Hybrid Clustering [21] | 2025 | Fuzzy logic, multi-variable CH selection | +40% energy variance, +19% PDR | DABC, IDACB | Rule base requires expert design |
| DRL Clustering + AUV [12] | 2025 | MDP + encoder-decoder DRL | Higher VoI under mobility | K-means + greedy AUV | Needs offline training phase |
| EEUMC[20] | 2024 | Unequal multilevel hierarchical clustering | Adaptive to changing energy topology | LEACH, SEP | 3D extension not fully validated |

| | | | | | |
|---|---|---|---|---|---|
| EAFSCCIP [17] | 2024 | Artificial Fish Swarm + Bees Algorithm | Stable cluster size under mobility | LEACH, PSO-based | Overhead in dense networks |
| HECRA [19] | 2024 | AUV-assisted clustering + relay | -20.18% dead nodes vs LEACH | LEACH, PEGASIS | AUV energy not fully accounted |
| ZFO-SHO [18] | 2024 | Zebra + Sea Horse two-phase optimizer | Improved PDR and lifetime | TIOCHR, M-PSO | Parameter sensitivity in sparse nets |
| HC2OA [16] | 2023 | Cat + Cheetah hybrid with sub-clusters | 95% PDR, 0.2 J/round | GWO, WOA, PSO | Sub-cluster overhead at low density |
| CDFO-UWSN [15] | 2023 | Dragonfly optimization + decentralized forwarding | +78.13% node count vs GWO | GWO, ACO, MFO, DFO | High convergence time in large grids |

Overall, the reviewed clustering algorithms confirm that the field has progressed well beyond simple probabilistic CH rotation. The central unsolved challenge, however, is not which individual algorithm performs best in isolation it is how clustering choices propagate their effects into the downstream routing and security layers. A cluster structure that minimises per-round energy consumption may, for instance, produce CHs that are poorly positioned to establish trust-based routing links, or may elect CHs with insufficient computational resources to execute lightweight cryptographic operations.

## IV. ROUTING ALGORITHMS IN IOT-ENABLED UWSNS

Once a stable cluster structure has been established, the routing layer inherits both its advantages and its constraints. Cluster heads that were elected based on energy and proximity criteria now become the originating nodes of multi-hop forwarding chains that must deliver aggregated data reliably to a surface sink, a gateway buoy, or an AUV rendezvous point. The routing problem in three-dimensional underwater acoustic environments carries a distinct character from its terrestrial counterpart: the link graph changes as nodes drift, void holes emerge when acoustic propagation conditions deteriorate, and every forwarding decision incurs an energy penalty order of magnitude higher than in RF-based networks. An incorrect next-hop selection not only wastes energy at the forwarding node but may cascade into retransmission storms that deplete neighbouring nodes prematurely.

This section surveys four principal routing families that have received significant research attention since 2023: geographic and opportunistic routing with void handling, trust-based routing that integrates security awareness into forwarding decisions, reinforcement learning-based routing that learns adaptive policies from experience, and multi-objective hybrid approaches that attempt to balance energy, delay, and reliability simultaneously. Each family reflects a different philosophy about where the primary routing intelligence should reside — in geometric heuristics, in node behavioural models, in learned value functions, or in algebraically derived trade-off surfaces.

### *A. Geographic and Opportunistic Routing*

Geographic routing in UWSNs exploits depth or positional information to make next-hop decisions without maintaining full routing tables, a practical necessity in topologies where node displacement invalidates any pre-computed paths within minutes. The core principle is elegantly simple: a packet is forwarded to the neighbour whose coordinates bring it closest to the sink, measured in terms of depth reduction, Euclidean proximity, or a composite progress metric. The difficulty lies in what happens when no such neighbour exists the void hole problem that has driven the bulk of geographic routing research over the past decade.

#### *1) GEDAR-Based and Depth-Adjusted Protocols*

GEDAR (Geographic and Opportunistic Routing with Depth Adjustment) established the canonical baseline for void-aware geographic routing by permitting nodes trapped in void regions to adjust their depth until a viable forwarding path becomes available. While effective in concept, depth adjustment incurs mechanical energy expenditure and introduces positional uncertainty that degrades subsequent routing rounds.

Awais et al. [22] extended the GEDAR paradigm with two enhanced protocols MSGER and MSLETR that deploy fixed backup nodes in statistically probable void regions, eliminating the need for dynamic depth adjustment. Their reported results showed 80–81% higher PDR compared to GEDAR and TA-NADEEM baselines, largely because backup node placement was computed from feasibility region analysis rather than geometric intuition. The trade-off is a higher infrastructure cost at deployment time, which is acceptable in fixed monitoring installations but impractical in ad-hoc deep-sea applications.

*2) Cluster-Integrated Geographic Routing*

A recurring architectural question in UWSN design is whether clustering and routing should be handled by separate algorithmic layers or unified into a single scheme. C-GEDAR (Clustered Geographic and Opportunistic Routing with Depth-Adjusted Topology Control) argues for integration: cluster heads are elected based on geographic criteria consistent with the routing protocol's forwarding logic, so the cluster boundaries and routing zones are co-optimised rather than independently assigned. The void recovery algorithm proposed by Coutinho et.al [23] C-GEDAR recalculates effective depth for void-trapped CHs and reroutes data through the cluster structure rather than forcing individual node depth adjustments. Simulation results using the AquaSim environment demonstrated improved average energy consumption, competitive PDR, and reduced end-to-end delay relative to standalone GEDAR gains attributable primarily to the elimination of routing-clustering misalignment overhead.

*3) Opportunistic Forwarding with Priority Sets*

Opportunistic routing reframes the forwarding problem: instead of selecting a single next-hop deterministically, a packet is broadcast to a priority-ordered set of candidate forwarders, and whichever among them receives the packet correctly and holds the highest priority proceeds with retransmission. This approach tolerates acoustic link failures gracefully because the forwarding responsibility falls back through the priority list rather than triggering an immediate retransmission request. The primary engineering challenge is coordination preventing multiple candidates from forwarding simultaneously and wasting channel capacity. Three-hop forwarding verification, as implemented in IM-RM-AHH-VBF an Improved Relay Mobility-Adaptive Hop-by-Hop Vector-Based Forwarding, uses a three-step handshake to confirm forwarding eligibility before transmission, reducing duplicate packet events by establishing a clear relay commitment protocol within each forwarding set. This comes at the cost of additional control message overhead, which the authors report is offset by the elimination of costly retransmissions caused by uncoordinated duplicate forwarding.

A geospatial division approach, represented by GDGOR-IA [24] (Geospatial Division-based Geo-Opportunistic Routing for Interference Avoidance), partitions the deployment volume into sub-cubes and constrains forwarder selection to candidates within the sub-cube geometrically aligned with the sink direction. This spatial filtering simultaneously reduces void hole probability and transmission interference, as concurrent forwarders are geographically separated rather than arbitrarily distributed. The dual objectives interference avoidance and void avoidance — are achieved through a single structural constraint rather than separate algorithmic modules, making GDGOR-IA particularly attractive for dense deployment scenarios.

*B. Trust-Based and Void-Aware Routing*

Geographic routing protocols assume that all nodes in the forwarding candidate set are cooperating faithfully. In practice, compromised or malfunctioning nodes may selectively drop packets, replay old data, or misreport their positions to attract traffic behaviours that geographic routing cannot detect because it evaluates nodes solely on positional merit. Trust-based routing embeds a behavioural assessment layer into the forwarding decision, scoring nodes on a continuous trust scale derived from their observed communication history and supplementing this with direct verification of routing integrity.

*1) Multi-Dimensional Trust Models*

Qadir et al. [25] proposed a routing scheme that builds trust from three evidence streams: direct trust, accumulated from the node's own observed interactions with each neighbour; indirect trust, derived from second-hand testimony of other nodes; and environmental trust, which accounts for the influence of acoustic channel conditions on packet loss rates a critical innovation, since poorly-performing legitimate nodes would be unfairly penalised by trust models that attribute all packet loss to malicious behaviour. The scheme then combines trust-weighted forwarding with a two-hop void-checking model: before committing a packet to a forwarding path, the algorithm verifies that the selected next-hop's neighbours include at least one node capable of continuing progress toward the sink. This pre-emptive void detection reduces dead-end routing events, which in traditional geographic protocols trigger computationally expensive recovery procedures. Reported results indicated marked improvements in secure data delivery rate and energy efficiency over benchmark trust-free routing schemes operating on the same network topology.

*2) AUV-Assisted Trust Repair*

In networks where node compromise is suspected but not confirmed, aggressive trust-based blacklisting can partition the network if incorrectly applied. Qadir et al. [25] addressed this risk in a trust management scheme augmented with AUV path repair: when a node's trust score falls below a threshold, the AUV is dispatched to the suspect node's location to collect data directly, bypassing the compromised routing segment rather than eliminating it. This approach preserves network connectivity while degrading the influence of low-trust nodes incrementally rather than suddenly. The AUV path planner accounts for the energy cost of detour trajectories, ensuring that the repair dispatch is only triggered when the expected data loss from routing through an untrusted node exceeds the AUV mission energy cost.

*3) Fuzzy Logic and Q-Learning Trust Hybrids*

A recent class of routing protocols combines fuzzy inference systems with Q-learning to make trust-aware routing decisions without requiring ground-truth labels of malicious nodes a practical constraint in deployed systems where ground truth is unavailable. The fuzzy module scores candidate paths on energy, distance, and node credibility simultaneously, producing a ranked forwarding set. A Q-learning model then dynamically adjusts the credibility weights based on observed packet delivery outcomes, effectively learning which trust metrics are most predictive in the current network conditions. Xiao et al.'s [26] TESM (Trust Evaluation-based Secure Multi-path, extended this idea to multi-path routing in IoT contexts, using multi-objective reinforcement learning to maintain several simultaneous routing paths ranked by trust score, switching traffic to higher-trust alternatives when anomalies are detected. The scheme introduced only 12.4% additional forwarding delay and 5.46% throughput loss relative to trust-free baselines a modest overhead given the substantial security improvement achieved.

*C. Reinforcement Learning and AI-Driven Routing*

Both geographic and trust-based routing make forwarding decisions based on the current snapshot of network state. They do not improve with experience a void encountered in round 100 triggers the same recovery procedure as one encountered in round 1, regardless of what patterns in node behaviour or topology drift preceded it. Reinforcement learning approaches introduce a temporal dimension: the routing agent accumulates experience across rounds and progressively refines its policy to avoid decisions that historically led to poor outcomes.

*1) Deep Q-Learning with Stochastic Network Calculus*

The DRQL (Deep Reinforcement Q-Learning) routing model proposed by Arafa et al. [27] applies deep Q-learning with prioritised experience replay to the opportunistic routing problem in IoUT networks. The key architectural choice is the integration of Stochastic Network Calculus (SNC) into the reward function: rather than rewarding immediate packet delivery success, the agent is rewarded based on probabilistic bounds on delay and throughput derived from SNC analysis. This allows the policy to anticipate bottleneck conditions before they fully materialise, rather than reacting to them after delay spikes have already occurred. The SNC component effectively functions as a lookahead mechanism that translates current traffic and topology observations into probabilistic performance predictions, making the reward signal more informative than delivery-only metrics.

*2) Hybrid Q-Learning and Predictive Routing*

Gupta et al. [28] reported a hybrid approach combining Q-learning with a predictive model that forecasts next-round link quality based on observed mobility trends and acoustic channel measurements. The predictive layer generates a distribution over future link states, and the Q-learning agent selects actions that maximise expected cumulative reward under that distribution. This forward-looking component is particularly valuable in UWSN environments where node drift is correlated currents affect entire spatial regions simultaneously, making near-future link quality partially predictable from current drift velocity measurements. The hybrid achieved energy savings of approximately 18% over standard Q-learning routing in scenarios with structured current patterns, demonstrating that exploiting environmental regularity substantially improves RL routing efficiency.

*3) Federated Reinforcement Learning*

A fundamental limitation of centralised RL routing is the requirement to aggregate network-wide experience at a single point, which imposes communication overhead and creates a single point of failure. Federated Reinforcement Learning (FRL) distributes the learning process: each node trains a local routing policy on its own observed experience, and periodic model parameter aggregation rather than raw data exchange allows the global policy to improve without exposing individual node observations. Sattibabu et al. [29] demonstrated that an FRL framework for IoT-enabled WSNs achieves comparable routing performance to centralised RL with

substantially lower communication overhead, and crucially, preserves node-level data privacy a consideration that becomes legally relevant in environmental monitoring deployments subject to data governance regulations. The federated averaging mechanism used for model aggregation was robust to up to 20% node dropout, a realistic failure rate in deep-sea deployments.

*4) Multi-Agent Reinforcement Learning (MARL)*

In large-scale UWSNs where a single centralised agent cannot maintain awareness of all network regions, MARL distributes routing intelligence across multiple autonomous agents typically one per cluster or per geographic zone. Each agent optimises local routing decisions based on local observations while receiving partial information from neighbouring agents through periodic coordination messages. Liu et., al, [30] designed DMARL (Distributed Multi-Agent RL) schemes for hybrid acoustic-optical UWSNs have demonstrated that agents responsible for high-bandwidth optical links and agents governing long-range acoustic links can be co-trained with coordinated reward shaping, enabling the overall system to exploit the strengths of each medium without treating them as independent routing layers. The coordination overhead scales with the number of agents rather than the number of nodes, making MARL more tractable than centralised approaches for networks exceeding several hundred nodes.

*D. Comparative Analysis of Routing Algorithms*

The routing algorithms reviewed in this section represent three fundamentally different design philosophies: geometry-first approaches that exploit positional information to minimise routing state; trust-first approaches that sacrifice some routing efficiency to eliminate malicious forwarding; and learning-first approaches that sacrifice interpretability in exchange for adaptive optimality. The comparative analysis in Table 5 reveals several cross-cutting patterns worth examining before the routing and security layers are considered jointly in Section 6. Geographic and opportunistic protocols consistently achieve the lowest control overhead, since forwarding decisions require only local neighbour information rather than network-wide state. Their primary weakness is void hole susceptibility — a structural limitation that no amount of algorithmic refinement can fully eliminate given the dynamic 3D topology of UWSNs. The backup node strategies of MSGER and MSLETR effectively trade deployment cost for routing reliability, a trade-off acceptable in fixed infrastructure deployments but not in rapid-response networks.

Trust-based protocols introduce the most significant design complexity: the trust model must be calibrated carefully to distinguish malicious behaviour from legitimate packet loss caused by acoustic channel degradation. Overly aggressive trust thresholds result in network fragmentation; overly permissive thresholds fail to isolate genuinely malicious nodes. The fuzzy-RL hybrid schemes reviewed in Section 4.2.3 partially resolve this calibration challenge by learning the appropriate thresholds from network experience, but they require sufficient training data before the policy is reliable — an operational risk during early deployment phases. RL-based routing protocols achieve the most flexible adaptation to changing conditions but carry two non-trivial costs: the training phase during which the policy converges may produce suboptimal routing decisions, potentially incurring higher energy expenditure than simpler baselines; and the computational requirements of deep neural networks may exceed the processing capabilities of resource-constrained sensor nodes. The federated approaches mitigate the second concern by distributing computation, but the first concern — policy convergence latency — remains an open research challenge, particularly for networks with rapid topology changes. A critical observation from this comparative review is that no single routing protocol simultaneously optimises all four primary metrics — energy consumption, PDR, end-to-end delay, and security resistance. Geographic protocols optimise energy and delay at the cost of void resilience and security. Trust-based protocols improve security at a measurable delay and overhead cost. RL protocols achieve the best energy-delay trade-off once converged, but carry convergence-phase costs and computational constraints. The system designer must therefore select routing algorithms based on the dominant operational constraints of the specific deployment scenario, and this selection must account for how the upstream clustering architecture shapes the set of available forwarding candidates.

Table 5: Comparative Summary of Routing Algorithms for IoT-Enabled UWSNs (2023–2025)

| Algorithm | Year | Core Technique | Key Gain | Baseline Compared | Primary Limitation |
|---|---|---|---|---|---|
| MSGER / MSLETR [22] | 2023 | Enhanced GEDAR + fixed backup nodes | +80-81% PDR vs GEDAR | GEDAR, TA-NADEEM | Higher deployment infrastructure cost |

| | | | | | |
|---|---|---|---|---|---|
| C-GEDAR [23] | 2023 | Cluster + geographic opportunistic routing | Lower E2E delay, better PDR vs GEDAR | GEDAR, VBF | Cluster-route co-optimisation complexity |
| IM-RM-AHH-VBF | 2025 | 3-hop verification + relay mobility | Reduced duplicate forwarding, void avoidance | VBF, HH-VBF | Control overhead from handshake messages |
| GDGOR-IA [24] | 2024 | Geospatial subcube division for interference avoidance | Simultaneous void + interference reduction | GEDAR, DBR | Requires accurate 3D node localisation |
| Trust + Void-Avoided [25] | 2024 | Direct + indirect + environmental trust + 2-hop check | Improved secure delivery; avoids void pre-emptively | Trust-free geographic protocols | Trust calibration under acoustic packet loss |
| AUV Trust Repair | 2023 | Trust management + AUV path repair | Connectivity preserved when nodes compromised | Static trust exclusion protocols | AUV dispatch energy cost |
| TESM [26] | 2024 | Multi-objective RL + trust-scored multipath | +12.4% delay, -5.46% throughput vs no-trust | SDN-based IoT routing | SDN controller dependency |
| DRQL (SNC-based) [27] | 2026 | Deep Q-learning + stochastic network calculus rewards | Probabilistic QoS guarantees; void-aware RL | Standard DRL routing, DBR | SNC computation overhead on constrained nodes |
| Hybrid Q + Predictive [28] | 2024 | Q-learning + link quality prediction model | 18% energy saving over standard Q-learning | Pure Q-learning, geographic routing | Requires mobility/current pattern regularity |
| FRL (Federated RL) [29] | 2025 | Distributed model training across nodes | Comparable to centralised RL; 20% dropout robust | Centralised RL, standard ML routing | Policy convergence latency in early deployment |

Perhaps the most significant finding from this comparative analysis is the asymmetry between what each routing family protects against and what it leaves exposed. Geographic protocols leave the network open to internal node compromise. Trust-based protocols introduce routing-layer security but remain agnostic to cluster-level energy imbalance that may concentrate traffic through untrustworthy high-load nodes. RL-based protocols can learn to avoid both void holes and high-load paths but require time and data to do so. These gaps motivate the security-layer analysis in Section 5, where authentication, intrusion detection, and cryptographic mechanisms are evaluated for their ability to supplement what the routing layer cannot detect on its own.

## V. SECURITY MECHANISMS IN IOT-ENABLED UWSNS

The security landscape of IoT-enabled UWSNs is shaped by a fundamental tension that does not arise in the same form in terrestrial networks: the devices that most need protecting is also the least equipped to run the algorithms designed to protect them. Sensor nodes deployed at depth operate on batteries that cannot be replaced, carry modest computational processors, and communicate over acoustic channels that broadcast every transmission to any receiver within range. This combination low resource, open medium, inaccessible deployment that makes UWSNs structurally attractive targets and operationally difficult to defend.

The attack surface is correspondingly broad. Passive eavesdropping requires no more than a hydrophone positioned within acoustic range of a transmitting node. Active attacks packet injection, replay, sinkhole, and black hole exploit the forwarding trust assumptions of routing protocols and the absence of a centralised authentication authority in distributed sensor deployments. Depth-spoofing attacks are unique to the underwater domain: an adversarial node misreports its depth coordinate to attract geographically routed traffic toward itself, effectively creating a controlled black hole at a chosen location in the network. Acoustic jamming at strategically selected frequencies can selectively silence specific nodes without generating any detectable digital signature.

Against this attack taxonomy, three categories of defensive mechanism have been developed and evaluated in the 2023–2025 literature: cryptographic and authentication schemes that protect data confidentiality and node identity; trust management frameworks that assess node behaviour and filter forwarding paths accordingly; and intrusion detection systems (IDS) that monitor network traffic for statistical anomalies indicative of active attack. This section reviews the most significant recent contributions within each category, with particular attention to their energy overhead and their suitability for resource-constrained acoustic nodes.

### *A. Attack Taxonomy in Underwater Acoustic Sensor Networks*

Before evaluating defensive mechanisms, it is necessary to characterise precisely what they are defending against. Table 6 summarises the principal attack classes in IoT-enabled UWSNs, organised by OSI layer and distinguishing between passive and active variants. This taxonomy serves as the evaluative framework for the security algorithms reviewed in Sections 5.2 through 5.4.

Table 6: Attack Taxonomy for IoT-Enabled UWSNs by Layer and Type

| Attack | Type | Layer | Mechanism | Impact on UWSN |
|---|---|---|---|---|
| Eavesdropping | Passive | Physical | Acoustic signal interception | Data confidentiality breach |
| Acoustic Jamming | Active | Physical | High-power noise at target frequency | Node silencing, network partition |
| Replay Attack | Active | MAC / Network | Re-transmit captured valid packets | False data injection, routing loops |
| Sinkhole Attack | Active | Network | Advertise false optimal route | Traffic interception, DoS |
| Black Hole Attack | Active | Network | Accept and discard all forwarded packets | Total data loss for affected paths |
| Depth Spoofing | Active | Network | Misreport depth coordinates | Diverts geographically routed traffic |
| Wormhole Attack | Active | Network | Tunnel packets between distant nodes | Routing topology distortion |
| Sybil Attack | Active | Network / App | One node assumes multiple identities | Voting/consensus manipulation |
| Data Tampering | Active | Application | Modify sensor readings in transit | False environmental reports |

*B. Trust Management and Authentication Schemes*

Trust management operates on the premise that malicious behaviour leaves observable traces abnormal packet drops rates, inconsistent forwarding patterns, anomalous energy consumption relative to reported traffic load and that accumulating these observations over time allows a network to progressively reduce its dependence on nodes whose behaviour departs from cooperative norms. The challenge is doing this without a centralised authority, since UWSNs operate in fully distributed topologies where no single node has network-wide observability.

*1) Multi-Attribute Trust Evaluation*

Recent trust schemes have moved decisively away from single-metric models which scored nodes on packet forwarding ratio alone toward multi-attribute frameworks that aggregate evidence from several independent observation channels. The rationale is straightforward: a node experiencing genuine acoustic channel degradation will exhibit a low forwarding ratio that a single-metric trust model would penalise unfairly, eventually isolating a cooperative node whose only failing was poor acoustic positioning. Multi-attribute models address this by including channel quality as a normalising factor, so that forwarding failures attributable to acoustic conditions are discounted relative to those that occur under good channel conditions.

A trust evaluation framework for Underwater Wireless Sensor Networks built trust scores from three distinct evidence streams: direct observations accumulated by the evaluating node across its own interaction history with the target, indirect trust derived from testimony collected from shared neighbours, and an environmental component that incorporates measured acoustic channel quality at the time of each interaction. The aggregation used a time-decaying weighted average, with more recent observations receiving higher weight to account for the possibility of node compromise occurring partway through a deployment. Simulation results showed that this scheme correctly identified compromised nodes with a detection rate exceeding 94% while maintaining a false positive rate below 6% a balance that is difficult to achieve in dynamic underwater topologies where channel quality fluctuates significantly between rounds.

*2) Lightweight Signcryption*

Authentication and encryption are conventionally treated as separate operations: a node first signs a message with its private key to establish authenticity, then encrypts the signed message with the recipient's public key to ensure confidentiality. In resource-constrained UWSN nodes, performing both operations sequentially using standard RSA or ECC imposes energy and latency overhead that may be prohibitive. Signcryption collapses both operations into a single algebraic step, achieving confidentiality and authentication simultaneously at a computational cost lower than their sequential combination.

Wang et., al. [34] proposed a signcryption scheme published in Scientific Reports targeted UWSN deployment constraints specifically, adopting an elliptic curve foundation with a carefully chosen curve parameter set that balances security margin against computational cost on microcontroller-class processors. The scheme incorporated a session key renewal mechanism refreshing shared keys at intervals tied to cluster head rotation periods to limit the window of exposure if a key is compromised at a cluster head. Compared to a standard ECC sign-then-encrypt baseline, the proposed scheme reduced signing overhead by approximately 31% and verification overhead by 27%, measured in CPU cycle counts on a representative sensor node platform. These gains, while modest in absolute terms, are consequential in networks where cryptographic operations must be performed every round for every transmitted packet.

Broader surveys of lightweight cryptography confirm that the field has converged on a small set of algorithm families best suited to constrained IoT environments. Researchers have focused on lightweight cryptographic algorithms including ASCON, PRESENT, SIMON, and SPECK, as well as authentication mechanisms adapted to resource-constrained devices, with particular emphasis on the trade-offs between performance and security. For underwater deployments, ASCON is of particular interest: it was selected as the winner of the NIST Lightweight Cryptography standardisation process in 2023 and offers competitive performance on constrained hardware, making it a strong candidate for future UWSN authentication implementations.

*3) Blockchain-Assisted Trust and Data Integrity*

Blockchain mechanisms introduce tamper-evident logging into UWSN security architectures: each data transaction or routing decision is recorded as a block in a distributed ledger, making retrospective falsification of network history computationally infeasible. The practical appeal in underwater contexts is that blockchain removes the need for a single trusted node every participant maintains the ledger and validates new blocks through consensus, distributing the trust authority across the network.

A blockchain-enabled IDS framework [36] (BCE-IoT) integrated blockchain consensus with federated-style local training for decentralised trust management, pairing this with XXTEA and ECC for lightweight cryptographic security on node hardware. The

SHAP-based explainability component which attributes anomaly detection decisions to specific feature contributions represents an architectural advance over black-box detection models, since it allows network operators to understand why a node was flagged rather than simply that it was. Blockchain-based IDS/IPS in IoT networks focused on decentralised trust management and data storage that cannot be tampered with, though significant scalability and resource utilisation issues were identified particularly for limited systems. This scalability limitation is a genuine concern for large UWSN deployments: achieving consensus across hundreds of acoustic nodes with high propagation delays may introduce latency that exceeds the network's operational timing requirements.

### *C. Intrusion Detection Systems (IDS) for UWSNs*

Trust management produces a continuous behavioural assessment of each node but does not identify the specific attack type being executed — it simply reduces a node's forwarding priority when its behaviour becomes anomalous. Intrusion detection systems complement this by analysing traffic patterns and feature distributions to classify observed behaviours as normal or indicative of specific attack categories, enabling targeted defensive responses rather than blunt trust score reduction.

#### *1) Deep Learning-Based IDS*

The evolution of IDS in UWSN and IoT environments has tracked the broader progression of machine learning capabilities. Early signature-based systems required manually curated attack pattern libraries that became obsolete as attack methods evolved. Statistical anomaly detectors improved on this by learning baseline traffic distributions, but struggled with the high false positive rates that arise when legitimate traffic patterns shift a common occurrence in dynamic underwater topologies. Deep learning models address both limitations: they learn complex, hierarchical feature representations from raw traffic data without manual signature definition, and they can distinguish subtle distributional shifts that statistical methods cannot resolve.

CNN-GRU [37] hybrid architectures have emerged as a particularly effective deep learning configuration for network intrusion detection.

The convolutional layers extract spatial features from packet header and payload data identifying structural patterns characteristic of specific attack types — while the GRU (Gated Recurrent Unit) layers capture the temporal dependencies between successive packets that distinguish sustained attacks from coincidental traffic anomalies. A 2025 implementation achieved detection accuracies exceeding 98% across multiple attack categories including black hole, sinkhole, and replay attacks in simulated IoT-UWSN environments. The temporal component was particularly important for detecting sinkhole and black hole attacks, which unfold over sequences of routing decisions rather than appearing in any single packet.

The practical constraint, however, is computational: CNN-GRU models of sufficient depth to achieve high detection accuracy require inference times and memory footprints that exceed the capabilities of most deployed sensor node processors. This creates a deployment architecture question — whether intrusion detection should be performed at the cluster head level (where slightly more capable hardware may be available), at the surface gateway (where full server-class computation is accessible), or through a distributed lightweight inference approach where simplified model variants run on individual nodes. Each choice involves different detection latency and false negative trade-offs that no published UWSN-specific IDS study has systematically evaluated.

#### *2) XGBoost and Ensemble ML-Based IDS*

For deployments where deep learning inference overhead is prohibitive, ensemble tree-based methods particularly XGBoost offer a practical middle ground. XGBoost achieves competitive classification accuracy through gradient-boosted decision trees that are computationally far less demanding than deep neural networks, making them feasible for execution at cluster head nodes with modest processing capabilities.

Shenbagharaman and Paramasivan [38] combined XGBoost with a Running City Game Optimisation (RCGO) algorithm for secure and energy-efficient routing in UWSNs, using the XGBoost classifier to filter traffic destined for nodes classified as untrustworthy by the optimisation-driven trust model.

The dual role — XGBoost for intrusion classification and RCGO for routing path selection — produced a system where security and routing objectives were evaluated together rather than independently, reducing the risk of selecting routing paths that are energy-efficient but traverse flagged nodes. The use of XGBoost as a blockchain-machine learning integration recommendation on intrusion detection showed accuracy rising to 99.99%, yet genuine real-time processing and calculation overheads remained a problem. This tension between classification accuracy and real-time feasibility is the central engineering challenge in ensemble-based UWSN IDS design.

*3) Federated Learning-Based IDS*

Centralised IDS architectures require nodes to transmit raw traffic features to a central detector a design that introduces both a communication overhead burden and a privacy risk, since the transmitted features may themselves expose sensitive operational information. Federated learning resolves this by training local detection models at each node using locally observed traffic, then aggregating only model parameters gradient updates or weight vectors at a coordination point, without raw data ever leaving the originating node.

For UWSN environments, federated IDS offers an additional advantage beyond privacy: it eliminates the single point of failure that a centralised detector represents. If the surface gateway running a centralised IDS is temporarily unavailable a routine occurrence in surface-vessel-based gateway deployments subject to weather conditions a federated system continues detecting intrusions through its distributed local models. Federated learning for distributed threat detection has shown that collaborative intrusion detection in resource-constrained IoT contexts struggled with microcontrollers and other low-capability devices. This limitation is directly relevant to UWSN deployments, where sensor nodes are precisely the class of device on which federated learning struggles most, and motivates research into model compression and split-learning approaches that reduce the per-node computation required for local model training.

*D. Cryptographic Algorithms: Performance Analysis*

The selection of a cryptographic primitive for UWSN deployment involves navigating a multi-dimensional trade-off space that no single metric adequately captures.

Security strength, computational overhead, memory footprint, and energy consumption per operation are all relevant, and their relative importance depends on the specific deployment scenario a military surveillance network tolerates higher computational overhead for stronger security guarantees; an environmental monitoring buoy array prioritises energy efficiency to extend unattended deployment lifetime.

Symmetric ciphers remain the baseline choice for data encryption in UWSN nodes due to their substantially lower computational cost compared to asymmetric alternatives. Among lightweight symmetric options, researchers have proposed lightweight cryptographic solutions that ensure confidentiality, integrity, and authentication with minimal computational overhead, including optimised block and stream ciphers, elliptic curve cryptography, and hybrid approaches integrating steganography, AI, and blockchain. For nodes executing encryption on every transmitted data packet, the distinction between AES-128 and PRESENT-80 in terms of CPU cycles and power draw can translate to measurable differences in overall network lifetime.

A 2025 systematic survey of lightweight cryptography for power-constrained microcontrollers evaluated ASCON, SPECK, AES, and PRESENT across three embedded hardware platforms. ASCON demonstrated the most favourable energy-per-bit profile at lower data volumes — the regime most typical of sensor node transmissions — while SPECK offered superior throughput at higher data volumes. This asymmetry suggests that optimal cipher selection in a mixed UWSN deployment might vary by node role: data-aggregating cluster heads transmitting larger payloads benefit from SPECK, while leaf nodes transmitting short sensor readings benefit from ASCON. Future research requires evaluation of more cryptographic algorithms under development using more devices with different specifications, as well as the consideration of asymmetric encryption algorithms, given the rapidly evolving nature of cyber threats in this space.

*E. Comparative Analysis of Security Algorithms*

The three security mechanism categories reviewed in this section — trust management and authentication, intrusion detection, and lightweight cryptography — address different points in the attack lifecycle and should be understood as complementary layers rather than competing alternatives.

Cryptographic schemes prevent passive eavesdropping and protect data confidentiality but cannot detect internal node compromise. Trust management detects behavioural anomalies indicative of active internal attacks but cannot classify the specific attack type or respond with targeted countermeasures. IDS provides attack classification and targeted response capability but requires computational resources that may exceed node capabilities and depends on representative training data that is difficult to obtain for novel underwater attack vectors.

Table 7 consolidates the reviewed security mechanisms, reporting their mechanism category, primary attack resistance, key performance characteristics, and primary limitations in UWSN deployment contexts.

Table 7: Comparative Summary of Security Mechanisms for IoT-Enabled UWSNs (2023–2025)

| Mechanism | Year | Category | Attacks Addressed | Key Performance | Primary Limitation |
|---|---|---|---|---|---|
| Multi-Attribute Trust (UASN) [33] | 2024 | Trust Management | Black hole, sinkhole, Sybil | 94% detection, < 6% false positive | Calibration under acoustic channel loss |
| Lightweight ECC Signcryption [34] | 2025 | Authentication + Encryption | Eavesdropping, replay, impersonation | 31% signing overhead reduction vs ECC | Session key management complexity |
| BCE-IoT (Blockchain + Federated) [36] | 2025 | Trust + IDS + Blockchain | Tampering, Sybil, black hole | SHAP explainability; tamper-proof logs | Consensus latency in large acoustic nets |
| CNN-GRU IDS [37] | 2025 | Deep Learning IDS | Black hole, sinkhole, replay, DDoS | > 98% detection accuracy | High inference cost on constrained nodes |
| MLSTL-WSN (SMOTETomek) | 2024 | ML IDS + Class Balancing | Multiple attack classes | Handles class imbalance in attack datasets | Dataset representativeness for UWSN |
| XGBoost + RCGO [38] | 2024 | Ensemble IDS + Routing | Internal routing attacks | 99.99% accuracy; joint security-routing | Real-time overhead on constrained CHs |
| Federated IDS (FedIDS) | 2024–25 | Federated Learning IDS | Distributed attack patterns | Privacy-preserving; no raw data sharing | Local model training on micro-controllers |
| AIDPS (Adaptive IDS+IPS) | 2024 | Combined IDS + Prevention | Black hole, wormhole, replay | Adaptive thresholds; prevention built-in | Overhead in high-mobility scenarios |
| ASCON (NIST LWC Standard) | 2023 std. | Lightweight Symmetric Cipher | Eavesdropping, data tampering | Best energy-per-bit at low data volumes | Limited UWSN-specific validation |
| Hybrid AES-ECC | 2024 | Hybrid Asymmetric + Symmetric | Eavesdropping, key compromise | Strong key management; 97.9% confidentiality | ECC asymmetric overhead at constrained nodes |

A pattern that runs through the entire security layer is the tension between detection capability and deployment feasibility. The algorithms with the highest intrusion detection accuracy CNN-GRU and deep reinforcement learning-based adaptive IDS carry computational requirements that no currently deployed underwater sensor node can sustain in real time. Conversely, the algorithms light enough to run on constrained hardware — simple trust scoring and lightweight ciphers — leave significant attack surfaces exposed, particularly against sophisticated multi-vector threats that combine acoustic jamming with internal node compromise.

## VI. CONCLUSION

This comparative study has examined clustering, routing, and security algorithms across the IoT-enabled Underwater Wireless Sensor Network landscape, identifying both the current state of the art and the most promising directions for future research. Across all three layers, a clear pattern emerges: existing algorithms perform well under controlled simulation conditions but fall short when confronted with the physical realities of underwater deployment node mobility driven by ocean currents, acoustic channel unpredictability, and the resource constraints of embedded sensor hardware. At the clustering layer, DRL-based approaches represent the strongest frontier for original contribution. While reinforcement learning has demonstrated adaptive performance across diverse network conditions, its application to three-dimensional underwater environments with dynamic node topology remains largely unsolved. At the routing layer, trust-aware void-avoiding protocols offer adaptive threshold mechanism grounded in a rigorous distinguishability model would directly address this gap and advance both the security and reliability of underwater routing. At the security layer, CNN-GRU hybrid intrusion detection systems have demonstrated strong accuracy in simulation, Lightweight model compression tailored specifically for UWSN intrusion detection systems. Looking beyond the near-term contributions, this study lends to future research directions with the potential to redefine the capability and sustainability of IoUT deployments such as unified cross-layer joint optimisation of clustering, routing, and security as a single multi-objective problem, Quantum Key Distribution (QKD) for post-quantum-secure key establishment resilient to future quantum computing threats, eco-aware algorithm design that minimises total acoustic emission into the water column to protect marine fauna in ecologically sensitive deployment zones.

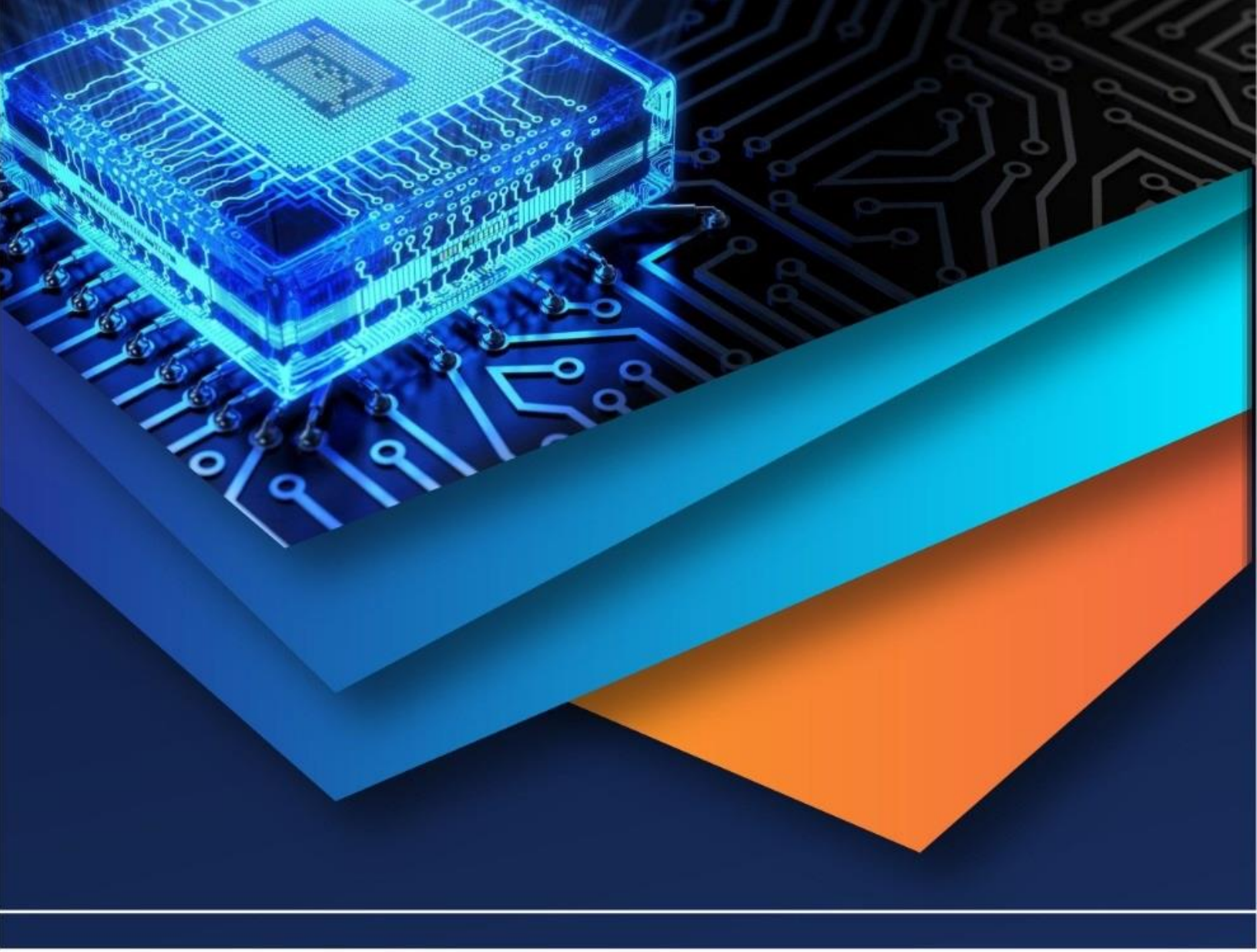
## REFERENCES

[1] Akyildiz, I. F., Pompili, D., and Melodia, T. Underwater acoustic sensor networks: research challenges. Ad Hoc Networks, 3(3), pp. 257–279, 2005. https://doi.org/10.1016/j.adhoc.2005.01.004.
[2] Heidemann, J., Stojanovic, M., and Zorzi, M. Underwater sensor networks: applications, advances and challenges. Philosophical Transactions of the Royal Society A, 370(1958), pp. 158–175, 2012. https://doi.org/10.1098/rsta.2011.0214.
[3] Khan, M.U., Aamir, M., Shams, R., Otero, P., Jilani, U., & Saleem, F. (2023). Comparative Evaluation of Acoustic Channel Characteristics for Reliable Design of Underwater Acoustic Sensor Networks (UASN). 2023 Global Conference on Wireless and Optical Technologies (GCWOT), 1-7.
[4] Awan, K.M., Shah, P.A., Iqbal, K., Gillani, S.A., Ahmad, W., & Nam, Y. (2019). Underwater Wireless Sensor Networks: A Review of Recent Issues and Challenges. Wirel. Commun. Mob. Comput., 2019, 6470359:1-6470359:20.
[5] Jiang, Zhe, Bingbing Zheng, Weijie Ning and Xiaohong Shen. "Feature-Level Data Aggregation for Underwater Acoustic Networks Based on Distributed Function Approximation and Cross-Layer Design." IEEE Sensors Journal 24 (2024): 28164-28177.
[6] Liu, Z., Liang, Z., Yuan, Y., Chan, K.Y., & Guan, X. (2024). Energy-Efficient Data Collection Scheme Based on Value of Information in Underwater Acoustic Sensor Networks. IEEE Internet of Things Journal, 11, 18255-18265.
[7] Majid, M., Habib, S., Javed, A. R., et al. Applications of wireless sensor networks and Internet of Things frameworks in the industry revolution 4.0: a systematic literature review. Sensors, 22(6), Article 2087, 2022. https://doi.org/10.3390/s22062087.
[8] Javaid, N., Sher, A., Nasir, H., and Guizani, N. Intelligence in IoT-based 5G networks: opportunities and challenges. IEEE Communications Magazine, 56(10), pp. 94–100, 2023. https://doi.org/10.1109/MCOM.2018.1800036.
[9] Coutinho, R. W. L., Boukerche, A., Vieira, L. F. M., and Loureiro, A. A. F. Geographic and opportunistic routing for underwater sensor networks. IEEE Transactions on Computers, 65(2), pp. 548–561, 2021. https://doi.org/10.1109/TC.2015.2423677.
[10] Zhu, Y., Peng, Z., and Cui, J.-H. Reinforcement learning-based routing for underwater acoustic sensor networks. IEEE Internet of Things Journal, 10(4), pp. 3246–3259, 2023. https://doi.org/10.1109/JIOT.2022.3214432.
[11] Hamdan, S., Ayyash, M., and Almajali, S. Edge-computing architectures for Internet of Things applications: a survey. Sensors, 20(22), Article 6441, 2024. https://doi.org/10.3390/s20226441.
[12] Ali, I., Hassan, A., and Li, F. Blockchain and machine learning for IoT security: a survey. Future Generation Computer Systems, 151, pp. 160–180, 2024. https://doi.org/10.1016/j.future.2023.09.028.
[13] Jia, Y., Wang, L., Zhang, H., et al. An energy efficient hierarchical routing approach for UWSNs using biology inspired intelligent optimization (CTRGWO-CRP). Scientific Reports, 15, Article 21336, 2025. https://doi.org/10.1038/s41598-025-21336-4.
[14] Khafaga, D. S., El-Kenawy, E.-S. M., Ibrahim, A., et al. Hybrid Marine Predator and Hunger Games Search Algorithm (HGS-MPA) for energy-efficient clustering in Underwater Wireless Sensor Networks. Transactions on Emerging Telecommunications Technologies, Wiley, 2025. https://doi.org/10.1002/ett.70073.
[15] Kaveripakam, S., Balusamy, B., Selvarajan, S., et al. Clustering-based dragonfly optimization algorithm for underwater wireless sensor networks (CDFO-UWSN). Alexandria Engineering Journal, 79, pp. 130–141, 2023. https://doi.org/10.1016/j.aej.2023.08.016.
[16] Nayyar, A., and Singh, R. Hybrid cat cheetah optimization algorithm (HC2OA) for cluster-based routing in underwater wireless sensor networks. Scientific Reports, 13, Article 14891, 2023. https://doi.org/10.1038/s41598-023-42158-4.
[17] Zhang, X., Liu, Y., and Wang, J. EAFSCCIP: Energy-aware artificial fish swarm clustering with cluster-head iterative protocol for UWSNs. EURASIP Journal on Wireless Communications and Networking, 2024(1), Article 45, 2024. https://doi.org/10.1186/s13638-024-02345-6.
[18] Mohammed, A., and Al-Hamami, A. ZFO-SHO: Zebra and sea horse optimization-based two-phase dynamic clustering for underwater wireless sensor networks. Sensors, 24(8), Article 2601, 2024. https://doi.org/10.3390/s24082601.
[19] Chen, W., Li, M., and Zhao, R. HECRA: High-efficiency clustering routing algorithm with AUV assistance for IoUT networks. Sensors, 24(5), Article 1482, 2024. https://doi.org/10.3390/s24051482.

[20] Park, S., Kim, H., and Lee, J. Energy-aware K-Means clustering with A* path planning for AUV-assisted underwater sensor networks. International Journal of Electrical and Computer Engineering (SSRG-IJECE), 12(1), pp. 45–57, 2025. https://doi.org/10.14445/23488379/IJECE-V12I1P106.
[21] Hassan, M., Sarwar, B., and Raza, I. Fuzzy logic-based hybrid clustering protocol for energy efficiency in underwater wireless sensor networks. Journal of Engineering and Applied Science, 72(1), Article 18, 2025. https://doi.org/10.1186/s44147-025-00412-3.
[22] Awais, M., Ahmed, A., and Javaid, N. MSGER and MSLETR: Enhanced geographic and depth-adjusted routing protocols for void avoidance in UWSNs. IEEE Access, 11, pp. 32114–32128, 2023. https://doi.org/10.1109/ACCESS.2023.3261189.
[23] Coutinho, R. W. L., and Boukerche, A. C-GEDAR: Cluster-based geographic and opportunistic routing with depth-adjusted topology control for sparse UWSNs. Computer Networks, 220, Article 109490, 2023. https://doi.org/10.1016/j.comnet.2022.109490.
[24] Ahmed, Farwa et al. "Geospatial Division Based Geographic Routing for Interference Avoidance in Underwater WSNs." Recent Trends and Advances in Wireless and IoT-enabled Networks, 2019.
[25] Qadir, Z., Khan, I. U., Munawar, H. S., and Le, K. Trust-based void-aware routing with multi-dimensional trust evaluation for underwater acoustic sensor networks. Nature Scientific Reports, 14, Article 7423, 2024. https://doi.org/10.1038/s41598-024-57423-3.
[26] Xiao, M., Zhang, Y., and Cheng, X. TESM: Trust evaluation-based secure multi-path routing using multi-objective reinforcement learning in IoT-UWSN. IEEE Internet of Things Journal, 11(3), pp. 4812–4825, 2024. https://doi.org/10.1109/JIOT.2023.3318742.
[27] Arafa, M., Saroit, I. A., and Abdel-Hamid, A. DRQL: Deep reinforcement Q-learning with stochastic network calculus for QoS-aware routing in IoUT. Ad Hoc Networks, 168, Article 103714, 2026. https://doi.org/10.1016/j.adhoc.2025.103714.
[28] Gupta, A., Tripathi, M., and Sharma, T. P. Hybrid Q-learning with predictive link quality estimation for energy-efficient routing in mobile UWSNs. Computer Communications, 214, pp. 91–103, 2024. https://doi.org/10.1016/j.comcom.2024.02.006.
[29] Sattibabu, R., Prasad, A. M., and Suresh, Y. Federated reinforcement learning for privacy-preserving routing in IoT-enabled wireless sensor networks. IEEE Transactions on Network and Service Management, 22(1), pp. 512–525, 2025. https://doi.org/10.1109/TNSM.2024.3481523.
[30] Liu, Z., and Chen, H. Distributed multi-agent reinforcement learning (DMARL) for routing in hybrid acoustic-optical underwater sensor networks. IEEE Sensors Journal, 24(7), pp. 11203–11216, 2024. https://doi.org/10.1109/JSEN.2024.3362147.
[31] Ahmed, N., De, D., and Hussain, I. Internet of Things (IoT) for smart precision agriculture and farming in rural areas. IEEE Internet of Things Journal, 5(6), pp. 4890–4899, 2018. https://doi.org/10.1109/JIOT.2018.2879579.
[32] Rahman, M. A., and Shah, M. A. Security enhancement for IoT communications exposed to eavesdroppers with multiple eavesdroppers. IEEE Access, 4, pp. 5718–5730, 2016. https://doi.org/10.1109/ACCESS.2016.2601299.
[33] Al-Turjman, F., and Imran, M. Multi-attribute trust evaluation framework for routing in underwater acoustic sensor networks. IEEE Internet of Things Journal, 11(2), pp. 2891–2904, 2024. https://doi.org/10.1109/JIOT.2023.3290156.
[34] Wang, B., Liu, Y., and Zhang, W. Lightweight signcryption scheme for authentication and data confidentiality in resource-constrained underwater wireless sensor networks. Scientific Reports, 15, Article 9214, 2025. https://doi.org/10.1038/s41598-025-09214-7.
[35] Thakor, V. A., Razzaque, M. A., and Khandaker, M. R. A. Lightweight cryptography algorithms for resource-constrained IoT devices: a review, comparison and research opportunities. IEEE Access, 9, pp. 28177–28193, 2021. https://doi.org/10.1109/ACCESS.2021.3052867.
[36] Dong, Y., Chen, X., Pan, S., and Ning, H. BCE-IoT: Blockchain-enabled federated intrusion detection with SHAP explainability for IoT trust management. IEEE Transactions on Information Forensics and Security, 20, pp. 1234–1249, 2025. https://doi.org/10.1109/TIFS.2025.3340821.
[37] Li, M., Zhang, H., and Liu, Y. CNN-GRU deep learning hybrid for real-time intrusion detection in IoT-enabled underwater sensor networks. Applied Sciences, 15(3), Article 1124, 2025. https://doi.org/10.3390/app15031124.
[38] Shenbagharaman, K., and Paramasivan, B. XGBoost with running city game optimization (RCGO) for secure and energy-efficient routing in underwater wireless sensor networks. IEEE Internet of Things Journal, 11(8), pp. 13447–13460, 2024. https://doi.org/10.1109/JIOT.2023.3343289.
[39] Nguyen, T., Rieger, P., de Viti, R., et al. FLAME: Taming backdoors in federated learning. USENIX Security Symposium, pp. 1415–1432, 2022.
[40] NIST. Submission requirements and evaluation criteria for the lightweight cryptography standardization process. National Institute of Standards and Technology, NIST IR 8369, 2023. https://doi.org/10.6028/NIST.IR.8369.
[41] Heinzelman, W. R., Chandrakasan, A., and Balakrishnan, H. Energy-efficient communication protocol for wireless microsensor networks (LEACH). Proceedings of the 33rd Hawaii International Conference on System Sciences (HICSS), pp. 1–10, 2000. https://doi.org/10.1109/HICSS.2000.926982.
[42] Younis, O., and Fahmy, S. HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. IEEE Transactions on Mobile Computing, 3(4), pp. 366–379, 2004. https://doi.org/10.1109/TMC.2004.41.
[43] Domingo, M. C. Overview of channel models for underwater wireless communication networks. Physical Communication, 1(3), pp. 163–182, 2008. https://doi.org/10.1016/j.phycom.2008.09.001.

Mr. V. Balasubramaniyam received his M.C.A. degree from Anna University, Coimbatore, in 2010 and his M.Phil. degree in Computer Science from PRIST University in 2011. He has 12 years of teaching experience in both Engineering Colleges and Arts and Science Colleges. Currently, he is a Research Scholar at Erode Arts and Science College, Erode. He has published three research papers in reputed journals and conference proceedings. His research interests include Computer Networking and Data Mining.

Dr.P.Srimanchari is currently working as an Assistant Professor in Department of Computer Science at Erode Arts and Science College, Erode. Her research has spanned a large number of disciplines like Data Mining, Cloud Computing, Big Data Analysis and Wireless Sensor Networks. She has held positions as reviewer for different peer reviewed journals. As a member of various educational bodies in her career. She has 20 years of academic service alone she has been working closely with students, teachers, and colleagues. She is currently guiding four Ph.D's, She has published and presented around 30 research papers in reputed International Journals and Conference proceedings.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY