A Comprehensive Survey of Security Challenges and Modern Solutions in Underwater Wireless Sensor Networks

Nour Zahra
Postgraduate Student (PhD)
Systems and Computer Networks Department
University of Aleppo, Syria

Souheil Khawatmi
Assistant Professor
Systems and Computer Networks Department
University of Aleppo, Syria

Bader Aldin Kassab
Assistant Professor
Systems and Computer Networks Department
University of Aleppo, Syria

ABSTRACT

This survey highlights the critical importance of security in Underwater Wireless Sensor Networks (UWSNs), which are being increasingly deployed in sensitive marine applications, such as environmental monitoring and resource exploration. This paper systematically reviews the unique security challenges faced by these networks, including cyberattacks, data breaches, and communication interception. It analyzes fundamental security requirements such as confidentiality, authentication, integrity, and availability, and evaluates key security solutions, including encryption algorithms, secure routing protocols, and intrusion detection systems. By examining recent research (2020–2025), this survey highlights innovative approaches such as machine learning-based security models, lightweight encryption, and dynamic trust management. The findings suggest that integrating advanced technologies (e.g., artificial intelligence and adaptive algorithms) is essential to counter evolving threats in underwater environments. Lastly, the study identifies research gaps and future directions to guide further developments in UWSN security.

Keywords

Underwater Wireless Sensor Networks (UWSNs), Cybersecurity, Lightweight Encryption, Secure Routing, Intrusion Detection, Trust Management, Cyberattacks and Data Protection.

1. INTRODUCTION

Underwater Wireless Sensor Networks (UWSNs) have emerged as pivotal technologies for marine applications, including environmental monitoring, marine life research, seabed exploration, and climate change prediction [1]. Despite their potential, UWSNs face unique challenges such as limited bandwidth, high latency, energy constraints, and vulnerability to cyber threats [2]. These limitations render security a critical concern, as attacks can compromise sensitive data, disrupt operations, and even trigger environmental crises.

The Importance of Security in Underwater Wireless Sensor Networks:

- *Sensitive Data Protection:* The information collected often contains sensitive data related to marine systems or underwater life. Securing this data prevents unauthorized access and enhances privacy.
- *Data Integrity:* Data integrity refers to maintaining the accuracy and reliability of data. Any unauthorized modification can lead to incorrect decisions or unreliable conclusions, impacting studies and research.
- *Operational Continuity:* Security provides strategies for protection against Denial-of-Service (DoS) attacks and mitigating their impact on network operations. Operational continuity is essential to ensure real-time data collection.
- *Identity and Trust Management:* Ensuring data originates only from trusted sources.
- *Avoiding Environmental Crises:* Attacks may result in marine crises affecting ecosystems.
- *Defense and Security Applications:* Given the strategic importance of maritime data, network security is linked to achieving national security and defense objectives.

Evidently, security in underwater wireless sensor networks is not merely a technical issue, but a vital component in ensuring the effectiveness and efficiency of these systems. Addressing these challenges necessitates the development of integrated security strategies that address the multiple and evolving challenges facing these networks, thereby contributing to their optimal utilization in the service of the environment and communities.

The key contributions of this survey are:

- A systematic review of UWSNS security challenges and requirements.
- A comprehensive classification of recent security solutions (2020–2025).

2. RESEARCH METHODOLOGY

Relevant literature was gathered from reputable scientific databases using targeted keywords such as "Underwater Wireless Sensor Networks," "Security," and "Intrusion Detection." After applying quality and publication date filters, the selected studies underwent analysis for their innovative security solutions and their significant impact on the UWSNs field during the specified period. The review incorporates a comparative analysis of various approaches, with an emphasis on their strengths and limitations.

Literature Collection:

- Sources: IEEE Xplore, ScienceDirect, Scopus (2018–2025).
- Keywords: "UWSN security," "underwater encryption," "secure routing."

Inclusion Criteria:

- Peer-reviewed articles focusing on UWSN security.
- Studies proposing innovative solutions (e.g., AI-based, lightweight cryptography).

Analysis Framework:

- Challenges are categorized by OSI layers (Physical, Network, etc.).
- Solutions are evaluated based on efficiency, scalability,

and attack resistance.

3. SECURITY CHALLENGES OF UWSNS

Underwater Wireless Sensor Networks (UWSNs) are vulnerable to various threats and attacks. To fulfill security requirements, a set of security mechanisms and technologies must be implemented to safeguard UWSNs against attacks. Based on the Open Systems Interconnection (OSI) model, UWSN security issues can be logically categorized into distinct components. Figure 1. shows the security architecture of UWSNs, which comprises four layers: the Physical Layer, the Link Layer, the Network & Transport Layer, and the Application Layer [2].

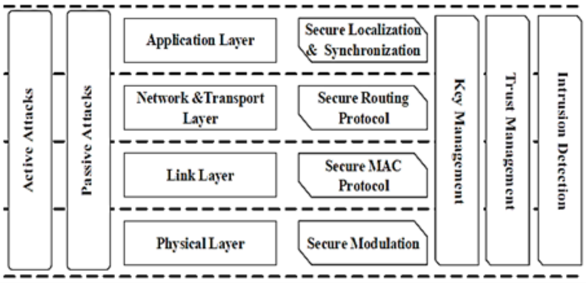


Fig 1: Security Issues of UWSNs [1]

UWSNs face numerous security challenges, including:

- *Key Management:* Effective key management is vital for ensuring secure communication. Robust mechanisms for generating, distributing, and storing encryption keys are indispensable, particularly due to the resource constraints of underwater devices.
- *Intrusion Detection:* Deploying efficient intrusion detection systems (IDS) is necessary to monitor and identify suspicious behaviour or unauthorized access attempts. These systems typically analyze network traffic and employ advanced algorithms to detect anomalies.
- *Trust Management:* Establishing reliable trust management mechanisms is particularly challenging in UWSNs, where the credibility of each node must be continuously validated. A well-designed trust model can significantly mitigate risks and enhance overall network security.
- *Location Security:* These issues relate to determining the geographical locations of devices and ensuring that received data originates from trusted locations. Location security technologies require mechanisms to verify the authenticity of locations and prevent spoofing.
- *Synchronization Security:* Underwater networks require time synchronization between devices to ensure that the data being collected is synchronized. Measures must be in place to protect this synchronization from hacking or manipulation.
- *Routing Security:* Data routing in underwater networks requires ensuring that information is not tampered with during transmission. Secure routing protocols must be developed that prevent attackers from changing or intercepting data routes.
- *Secure MAC protocols:* It aims to provide monitoring and control mechanisms for data transmission and reception with strong protection against various attacks while taking into account harsh environment characteristics such as limited power and variable channel quality.
- *Secure Modulation:* Combining traditional modulation techniques with security mechanisms such as encryption, frequency shifting, and spread spectrum techniques to maintain data confidentiality and integrity in a challenging maritime environment.

UWSNs are susceptible to two primary types of attacks:
Active Attacks in UWSNs: Active attacks are those in which an attacker directly interferes with data or network operation, resulting in a significant impact on network performance or the transmitted information. Some types of active attacks include:

- Data Tampering: Attackers alter transmitted data to compromise its integrity.
- Denial-of-Service (DoS): Attackers overwhelm the network with excessive requests or jamming signals to disrupt operations.
- Routing Attacks: Such as hijacking or manipulating the data path through the network.
- Replay Attacks: The attacker resends old messages to disrupt or deceive the system.

Passive Attacks in UWSNs: Passive attacks are those in which the attacker monitors or eavesdrops on data without interfering with or changing it. The goal is to steal information or collect data from the network without being detected. The most common types of passive attacks include:

- Eavesdropping: Unauthorized interception of data to extract sensitive information.
- Traffic Analysis: Inferring network topology or critical node locations by monitoring communication patterns.

Defense methods against active and passive attacks differ. Active attacks require strong protection mechanisms such as encryption, data integrity verification, and intrusion detection, while passive attacks require strong encryption to ensure data privacy and confidentiality.

Therefore, addressing these security issues is essential to ensure the security and operational efficiency of underwater wireless sensor networks, paving the way for the use of this technology in sensitive applications such as environmental monitoring and marine exploration.

4. SECURITY REQUIREMENTS FOR UWSNS

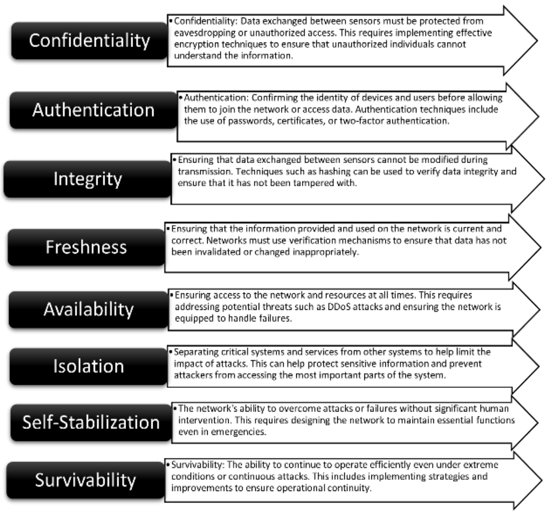
As shown in Figure 2, the security requirements for Underwater Wireless Sensor Networks (UWSNs) constitute fundamental elements for ensuring network safety and operational effectiveness. These requirements can be detailed as follows [2][3]:

- *Confidentiality:* Transmitted data between sensor nodes must be secured against eavesdropping and unauthorized access. This necessitates the implementation of robust encryption mechanisms to prevent data interpretation by unauthorized parties.
- *Authentication:* Verifying the identity of both devices and users prior to granting network access or data privileges. Common authentication methods encompass password-based verification, digital certificates, and multi-factor authentication systems.
- *Data Integrity:* Guaranteeing that transmitted data remains unaltered during propagation across the network. Cryptographic hash functions are typically employed to validate data integrity and detect any unauthorized modifications.
- *Data Freshness:* Maintaining the timeliness and validity of network data. This requires implementing proper verification protocols to prevent the use of stale or inappropriately modified data.
- *Service Availability:* Guaranteeing uninterrupted access to network resources. This involves implementing protection mechanisms against Distributed Denial-of-Service

(DDoS) attacks and establishing robust fault tolerance capabilities.

- *Routing Security:* Data routing in underwater networks requires ensuring that information is not tampered with during transmission. Secure routing protocols must be developed that prevent attackers from changing or intercepting data routes.
- *Isolation:* The segregation of critical systems and services from non-critical components to mitigate attack impacts. This security measure safeguards sensitive data and restricts unauthorized access to core system elements.
- *Self-Stabilization:* The network's capability to autonomously recover from attacks or system failures. This necessitates a design architecture that preserves critical functionality during emergency scenarios.
- *Survivability:* The system's capacity to maintain optimal operation during prolonged attacks or extreme environmental conditions. This is achieved through proactive resilience strategies and continuous system enhancements.

Collectively, these requirements address diverse security dimensions in underwater networks. Their comprehensive integration during the network design and implementation phases is crucial for ensuring robust information and system protection.



• Confidentiality: Data exchanged between sensors must be protected from eavesdropping or unauthorized access. This requires implementing effective encryption techniques to ensure that unauthorized individuals cannot understand the information.

• Authentication: Confirming the identity of devices and users before allowing them to join the network or access data. Authentication techniques include the use of passwords, certificates, or two-factor authentication.

• Ensuring that data exchanged between sensors cannot be modified during transmission. Techniques such as hashing can be used to verify data integrity and ensure that it has not been tampered with.

• Ensuring that the information provided and used on the network is current and correct. Networks must use verification mechanisms to ensure that data has not been invalidated or changed inappropriately.

• Ensuring access to the network and resources at all times. This requires addressing potential threats such as DDoS attacks and ensuring the network is equipped to handle failures.

• Separating critical systems and services from other systems to help limit the impact of attacks. This can help protect sensitive information and prevent attackers from accessing the most important parts of the system.

• The network's ability to overcome attacks or failures without significant human intervention. This requires designing the network to maintain essential functions even in emergencies.

• Survivability: The ability to continue to operate efficiently even under extreme conditions or continuous attacks. This includes implementing strategies and improvements to ensure operational continuity.

Fig 2: Security Requirements for UWSNs

5. SECURITY CLASSIFICATION OF UWSNS

Security mechanisms in Underwater Wireless Sensor Networks (UWSNs) can be systematically classified into four primary categories, as shown in Figure 3:

- ***Encryption Algorithms:*** These cryptographic protocols safeguard data during transmission across the network. They employ diverse techniques, including public-key infrastructure (PKI) and symmetric-key algorithms, to guarantee both data confidentiality and integrity.
- ***Secure Routing Protocols:*** This category focuses on developing robust routing mechanisms that maintain data integrity during transmission. It encompasses trust-based routing architectures and attack-resilient path selection methodologies, which optimize secure route determination to minimize interception risks and data compromise.
- ***Intrusion Detection and Prevention Systems:*** This domain addresses the development and deployment of comprehensive defense strategies, incorporating intrusion detection systems (IDS), advanced encryption technologies, and proactive security mechanisms to thwart unauthorized access and identify anomalous network behaviour.
- ***Secure Authentication Mechanisms:*** This classification encompasses identity verification protocols for both devices and network users. It integrates advanced techniques, including certificate-based authentication and multi-factor authentication (MFA) systems, to guarantee that data exchange occurs exclusively between authenticated nodes.

Each category is an essential part of the security framework for underwater wireless sensor networks, contributing to improved network reliability and security in their unique and complex environments.

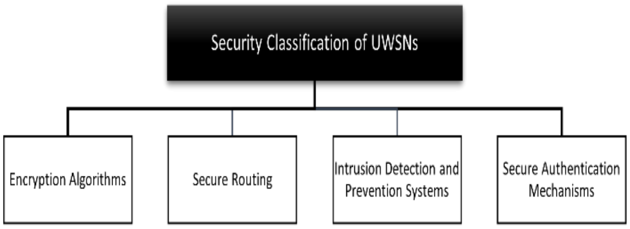

Security Classification of UWSNs
Encryption Algorithms
Secure Routing
Intrusion Detection and Prevention Systems
Secure Authentication Mechanisms

Fig 3: Security Classification of UWSNs

5.1 Related Work on Encryption Algorithms

DBSR: A Depth-Based Secure Routing Protocol for Underwater Sensor Networks (2020) [1]:

- This research aims to enhance the security of the Depth-Based Routing (DBR) protocol by utilizing Elliptic Curve Cryptography (ECC).
- The proposed method employs lightweight cryptographic techniques based on the Elliptic Curve Algorithm, which requires fewer bits to secure transmissions.
- This approach effectively mitigates depth-spoofing attacks by safeguarding depth information.

An Energy-Efficient Crypto Suite for Secure Underwater Sensor Communication Using Genetic Algorithm (2021) [5]:

- This research presents an algorithm designed to generate two halves of a key using a genetic algorithm (GA) to withstand passive attacks.
- The key generation procedure is crucial, playing a significant role in data transmission.
- A novel symmetric encryption method is introduced for transmitting data in underwater wireless sensor networks.

A Lightweight Cryptographic Algorithm for Underwater Acoustic Networks (2022) [6]:

- An encryption algorithm is introduced for the secure transmission of underwater images over underwater wireless sensor networks.
- The logistic map, a fundamental one-dimensional chaotic map, is among the most widely utilized chaotic systems in cryptography.
- The security analysis demonstrates its high level of security and its capability to encrypt various colored images into ciphers that are nearly impossible to decipher.

Table 1 evaluates three prominent encryption solutions for Underwater Wireless Sensor Networks based on five key criteria: energy efficiency, latency, complexity, attack resistance, and specific attack types mitigated.

The comparison reveals that:

DBSR (ECC-Based Routing) demonstrates balanced performance with medium energy consumption and strong resistance against depth-spoofing attacks, making it suitable for applications requiring robust security.

Energy-Efficient Crypto (GA) shows superior energy efficiency but only moderate attack resistance, limiting its use to environments primarily threatened by passive attacks.
Lightweight Image Encryption achieves low latency and complexity, though its moderate attack resistance restricts its effectiveness to specific use cases like image transmission.
Key trade-offs emerge between security strength and resource consumption, with no single solution optimally addressing all criteria. The ECC-based approach offers the most comprehensive security, while genetic algorithm implementations prioritize energy conservation, and lightweight solutions favor computational efficiency. This analysis underscores the need for context-specific algorithm selection in UWSN deployments based on prioritized requirements (e.g., mission-critical security vs. energy preservation).

Table 1. Comparative Analysis of Encryption Algorithms in UWSNs: Energy Efficiency, Latency, and Attack Resistance

Security Solution	Energy Efficiency	Latency	Complexity	Attack Resistance	Attack Types Mitigated	Year
DBSR (ECC-Based Routing) [4]	Medium	Medium	Medium	Strong	depth spoofing attack.	2020
Energy-Efficient Crypto (GA) [5]	High	Medium	High	Moderate	Passive attacks.	2021
Lightweight Image Encryption [6]	Low	Low	Low	Moderate	Data interception.	2022

5.2 Related Work on Secure Routing

Secure Routing in Underwater Acoustic Sensor Networks Based on AFSA-ACOA Fusion Algorithm (2022) [7]:

- This research introduces a routing scheme inspired by the Artificial Fish Swarm (AFS) and Ant Colony Optimization (ACO) algorithms to achieve secure and timely underwater communication.
- The proposed algorithm improves network lifetime, enhances link reliability, balances network load, and ensures system security.
- The effectiveness of the algorithm in optimizing routing paths and strengthening the security of selected routes has been demonstrated.

Secure Fuzzy Simple Shortest Path Routing Protocol (SF-SSP) for Underwater Communication (2023) [8]:

- The primary objective of the proposed protocol is to accurately and efficiently detect malicious nodes that can disrupt communication, drop packets, or launch various attacks on the network.
- This research introduces an intelligent routing technique for the Simple Shortest Path routing protocol, thereby enhancing its performance.
- By employing fuzzy logic, this protocol takes into account multiple node parameters and behaviours to identify potential malicious activities.
- Fuzzy logic rules are employed to evaluate various node parameters and behaviours, forming a fuzzy inference system with linguistic variables and fuzzy rules.

Source Location Privacy Protection Algorithm Based on Polyhedral Phantom Routing in Underwater Acoustic Sensor Networks (2024) [9]:

- This paper introduces a source location privacy protection algorithm known as Polyhedral Phantom Routing (PPR-USLP) for Underwater Acoustic Sensor Networks (UASNs). This method effectively defends against passive attacks.
- The algorithm employs polyhedral phantom routing to introduce phantom nodes, enhance path diversity, and protect the privacy of the source node from passive attacks.
- Simulation results indicate that PPR-USLP exhibits satisfactory performance in terms of improving throughput, balancing load, and ensuring data accuracy, effectively ensuring the privacy of source locations underwater.

Secure and Energy-Efficient Routing Protocol for Underwater Wireless Sensor Networks Using Running City Game Optimization with the XGBoost Algorithm (2025) [10]:

- This study presents a secure and reliable routing protocol for efficient data transmission in UWSNs using ML and meta-heuristic algorithms.
- The Extreme Gradient Boosting Machine, a machine learning classifier, is used to classify different types of attacks in transmitted packets.
- Predominant redundant nodes within the adopted network environment are detected using NSPGCN (Node Similarity Preserving Graph Convolutional Network).
- The Running City Game Optimization focuses on selecting the optimal path between source and destination through an energy function.
- The proposed routing protocol achieves a higher packet delivery ratio (PDR), increased data transmission rate, and extended network lifetime with low energy consumption.

Table 2 systematically compares four secure routing protocols for Underwater Wireless Sensor Networks (UWSNs) using five critical metrics: energy efficiency, latency, complexity, attack resistance, and mitigated attack types.
Key findings reveal:
AFSA-ACO Hybrid Routing (2022) balances medium energy efficiency and latency while demonstrating strong resistance against routing attacks, attributed to its bio-inspired optimization approach.

SF-SSP Fuzzy Routing (2023) excels in energy efficiency and malicious node detection but incurs higher computational complexity due to its fuzzy logic-based decision-making.

PPR-USLP Phantom Routing (2024) prioritizes source location privacy against passive attacks, though its high latency makes it unsuitable for time-sensitive applications.
XGBoost Secure Routing (2025) emerges as the most versatile, resisting multiple attack types via machine learning, albeit with increased complexity.

The analysis highlights a clear trade-off: protocols with advanced features (e.g., AI-driven path selection or phantom nodes) enhance security but often sacrifice latency or energy efficiency. Notably, newer solutions (2024–2025) leverage intelligent algorithms to address multifaceted threats, suggesting a trend toward adaptive, learning-based routing in UWSNs.

Table 2. Performance Evaluation of Secure Routing Protocols in UWSNs: Energy Efficiency, Latency, and Attack Resistance

Security Solution	Energy Efficiency	Latency	Complexity	Attack Resistance	Attack Types Mitigated	Year
AFSA-ACO Hybrid Routing [7]	Medium	Medium	Medium	Strong	Routing attacks.	2022
SF-SSP Fuzzy Routing (GA) [8]	High	Medium	High	Strong	Malicious nodes.	2023
PPR-USLP Phantom Routing [9]	Medium	High	Medium	Strong	Location tracking.	2024
XGBoost Secure Routing [10]	Medium	Medium	High	Strong	Multiple attacks.	2025

5.3 Related work on Intrusion Detection and Prevention Systems

Cluster-based Detection and Reduction Techniques to Identify Wormhole Attacks in Underwater Wireless Sensor Networks (2020) [11]:

- This study presents a novel solution for detecting wormhole attacks in underwater wireless sensor networks.
- The proposed method analyzes round-trip time and other attack characteristics to identify wormhole presence.
- Experimental validation was conducted using the Acoustic Cluster-Based Routing Protocol (EEHRCP).

Optimization using BIHH Technique (2020) [12]:

- Introduces an efficient route estimation method utilizing the Bellman Inora Hex Hamming (BIHH) technique.
- This protocol also ensures security for UWSNs against known attacks, specifically Black Hole Attacks.
- The protocol takes into account various Quality of Service parameters when selecting the route from source to destination
- Routes are rearranged in case of any failure due to unavailability of bandwidth or congestion in any node.

Securing localization-free underwater routing protocols against depth spoofing attacks. (2022) [13]:

- Proposes a security enhancement for Depth-Based Routing (DBR) protocols against depth-spoofing attacks.
- Develops an energy-efficient Depth-based Probabilistic Routing (DPR) protocol.
- Implements packet forwarding through unqualified nodes to mitigate attack impacts.
- Introduces parameter (p) to optimize forwarding probability and maintain network efficiency.

DOIDS: An Intrusion Detection Scheme Based on DBSCAN for Opportunistic Routing in Underwater Wireless Sensor Networks. (2023) [14]:

- This research introduces an intrusion detection system (IDS) named DOIDS, which is based on the Density-Based Spatial Clustering of Applications with Noise (DBSCAN) algorithm.
- DOIDS is specifically designed for UWSNs with sparse node deployment, utilizing a local monitoring mechanism.
- Each node operating DOIDS can identify the next reliable hop. DOIDS considers energy consumption, forwarder nodes, and link quality information of candidate forwarder nodes as feature values for detection.
- The aggregated feature information is then used to detect potential abnormal nodes through the DBSCAN algorithm.
- Finally, a defined decision function reduces the false discovery rate of DOIDS, leading to a final judgment on whether the potential abnormal node is malicious or not.
- It effectively addresses various types of attacks, including selective forwarding attacks, sinkhole attacks, and Sybil attacks.

AIDPS: Adaptive Intrusion Detection and Prevention System for Underwater Acoustic Sensor Networks (2024) [15]:

- This research presents a decentralized, adaptive Intrusion Detection and Prevention System (AIDPS) for Underwater Wireless Sensor Networks (UWSNs).
- AIDPS aims to enhance the security of UWSNs by effectively detecting underwater attacks such as black hole, gray hole, and flooding attacks.
- The research also introduces a cryptography-based IPS for autonomous defense, incorporating incremental machine learning and data distribution-based algorithms.

Table 3. Performance Evaluation of Intrusion Detection and Prevention Systems in UWSNs

Security Solution	Energy Efficiency	Latency	Complexity	Attack Resistance	Attack Types Mitigated	Year
Wormhole Detection (RTT) [11]	Medium	Medium	Medium	Strong	Wormhole attacks.	2020
BIHH Optimization [12]	Medium	High	Medium	Strong	Black hole attacks.	2020
DPR Anti-Spoofing [13]	Medium	Medium	Medium	Strong	Depth-spoofing.	2022
DOIDS (DBSCAN IDS) [14]	Medium	Medium	Medium	Strong	Selective forwarding.	2023
AIDPS Adaptive IDPS [15]	Low	Medium	Medium	Strong	Black, Gray, and Flooding attacks.	2024

Table 3 evaluates five intrusion detection and prevention systems (IDPS) for Underwater Wireless Sensor Networks across key operational parameters including energy efficiency, latency, complexity, attack resistance, and specific threats mitigated.

The comparative analysis demonstrates:
Wormhole Detection (RTT) (2020) provides medium energy efficiency and strong resistance against wormhole attacks through round-trip time analysis, though its effectiveness is limited to this specific attack type.
BIHH Optimization (2020) shows robust performance against black hole attacks but suffers from higher latency due to continuous route recalculation in dynamic underwater environments.
DPR Anti-Spoofing (2022) effectively counters depth-spoofing attacks while maintaining medium energy consumption through probabilistic forwarding, though network density impacts its performance.
DOIDS (DBSCAN-based) (2023) offers comprehensive protection against multiple attacks (selective forwarding, sinkhole) using spatial clustering, with balanced energy-latency tradeoffs ideal for sparse networks.
AIDPS Adaptive System (2024) represents the most advanced solution, employing machine learning to detect black hole, gray hole and flooding attacks, though it remains vulnerable to DoS attacks.
The evolution of IDPS solutions shows clear progression from attack-specific detection (2020-2022) towards adaptive, multi-threat systems (2023-2024). However, the persistent energy efficiency challenges (all solutions rated medium or low) highlight the need for more lightweight detection algorithms. Modern approaches combining machine learning with spatial analysis (e.g., DOIDS, AIDPS) demonstrate particular promise for comprehensive underwater network protection while maintaining reasonable computational overhead.
This analysis underscores that current IDPS solutions must be selected based on: (1) the predominant attack types in the deployment environment, and (2) the available energy budget, as no single solution currently optimizes both security coverage and resource efficiency.

5.4 Related work on Secure Authentication Mechanisms

SAPDA: Secure Authentication with Protected Data Aggregation Scheme for Improving QoS in Scalable and Survivable UWSN (2020) [16]:

- This research proposes a secure authentication and data aggregation mechanism to enhance Quality of Service (QoS) in cluster-based, scalable, and survivable underwater networks.
- The mechanism consists of two modules: authentication and data aggregation.
- In the authentication module, the base station authenticates the cluster head for each cluster.
- In the data aggregation module, sensor nodes within the cluster encrypt their data for security.
- The base station uses timestamp values to analyze and identify compromised data.
- Upon detection, compromised data is discarded, and the associated node (flagged as malicious) is isolated from the network.

SDAA: Secure Data Aggregation and Authentication Using Multiple Sinks in Cluster-Based Underwater Vehicular Wireless Sensor Network. (2023) [17]:

- This research proposes a secure MAC protocol, termed "Improved Methods for Secure Data Aggregation and Authentication," which leverages a cluster-based network and multiple mobile sinks.
- To ensure security, the Base Station authenticates the Cluster Head (CH), thereby establishing trusted clusters with enhanced privacy.
- Additionally, the Base Station authenticates each node before network entry, ensuring privacy protection.

A Dynamic Trust Model for Underwater Sensor Networks Fusing Deep Reinforcement Learning and Random Forest Algorithm. (2024) [18]:

- This study introduces a Dynamic Trust Evaluation Model (DRFTM) for underwater acoustic sensor networks, combining Deep Reinforcement Learning with a Random Forest Algorithm.
- DRFTM evaluates multiple indicators (e.g., communication, data, energy, and environment) to generate evidence-based trust values for subsequent analysis.
- The model employs random forest training to predict trust levels of sensor nodes amid node mobility and dynamic topology changes.
- Meanwhile, Deep Reinforcement Learning optimizes trust-update strategies, boosting detection accuracy.
- Experiments show that DRFTM outperforms existing methods in rapidly detecting malicious nodes while maintaining robustness even in sparse underwater environments.
- Data transmission within the network is secured via mutual authentication between nodes.
- Experimental validation confirms the method's effectiveness in improving network reliability and energy efficiency.

Table 4. Performance Evaluation of Secure Authentication in UWSNs

Security Solution	Energy Efficiency	Latency	Complexity	Attack Resistance	Attack Types Mitigated	Year
SAPDA Secure Auth [16]	Medium	Medium	Medium	Strong	Data tampering.	2020
SDAA Cluster Auth (GA) [17]	Medium	Medium	Medium	Moderate	MAC-layer attacks.	2023
DRFTM Trust Model [18]	Medium	Medium	High	Moderate	Mobile malicious nodes.	2024

Table 4 presents a comparative analysis of three authentication mechanisms for Underwater Wireless Sensor Networks, assessing their performance across five critical parameters: energy efficiency, latency, complexity, attack resistance, and specific threats addressed.

Key observations reveal:

SAPDA Secure Authentication (2020) demonstrates medium efficiency across all metrics, providing reliable protection against data tampering through cluster-based authentication and timestamp verification, though its performance degrades with increasing attacker presence.
SDAA Cluster Authentication (2023) implements mobile sink-based verification to secure MAC-layer communications,

showing improved energy efficiency but only moderate resistance against sophisticated MAC-layer attacks like DDoS. **DRFTM Trust Model** (2024) represents the most advanced approach, combining deep reinforcement learning with random forest algorithms to detect mobile malicious nodes. While achieving high accuracy in dynamic environments, its complex architecture results in higher computational overhead.

The analysis identifies several critical trends:

Modern solutions increasingly incorporate machine learning (DRFTM) to handle dynamic network conditions and mobile threats.

There exists an inherent trade-off between authentication robustness and energy efficiency.

Cluster-based approaches (SAPDA, SDAA) remain practical for resource-constrained environments despite their limited attack coverage.

No current solution provides comprehensive protection against both stationary and mobile attackers while maintaining optimal energy performance.

These findings suggest that future authentication mechanisms should focus on:

- Developing lightweight machine learning models to reduce computational complexity.
- Creating hybrid approaches that combine the efficiency of cluster-based methods with the adaptability of trust models.
- Expanding threat coverage to include emerging attack vectors while preserving energy efficiency.

The evolution of authentication solutions demonstrates clear progress from basic cryptographic verification (2020) to intelligent, behavior-based trust management (2024), reflecting the growing sophistication of threats in underwater environments.

Table 5 provides a critical assessment of seven prominent security solutions for Underwater Wireless Sensor Networks, analyzing their technical approaches, addressed vulnerabilities, advantages, and limitations.

Key findings reveal:

Performance Trade-offs:

- Machine learning-based solutions (e.g., XGBoost Routing 2025, DRFTM 2024) demonstrate superior attack detection capabilities but incur higher computational complexity.
- Lightweight approaches (e.g., Lightweight Image Encryption 2022) offer energy efficiency but provide limited security coverage.

Evolution of Solutions:

- Earlier solutions (2020-2022) focused on specific attacks (wormhole, depth-spoofing).
- Recent advancements (2023-2025) employ AI/ML for multi-threat protection and adaptive security.

Critical Limitations:

- Energy consumption remains a persistent challenge across all solutions.
- Scalability issues in large/dense networks affect most protocols.
- Environmental factors (currents, mobility) are frequently unaddressed.

The analysis highlights that while modern solutions have significantly improved UWSN security, fundamental challenges persist in:

- Balancing security robustness with energy efficiency.
- Maintaining performance in large-scale deployments.
- Addressing the complete spectrum of underwater threats.
- Accounting for environmental dynamics.

These findings underscore the need for future research to focus on:

- Cross-layer security architectures.
- Environment-aware adaptive mechanisms.
- Lightweight AI implementations.
- Comprehensive testing in real-world conditions.

The progression from specialized (2020-2022) to intelligent, multi-threat solutions (2023-2025) reflects the growing sophistication of both UWSN applications and their security requirements.

Table 5. Evaluation of performance metrics for related work on Secure Authentication Mechanisms.

Study Title	Technique	Issue Addressed	Advantages	Disadvantages	Year
Secure and energy efficient routing protocol for underwater wireless sensor network using running city game optimization with XGBoost algorithm. [10]	ML and meta-heuristic algorithms	Energy consumption, security vulnerabilities, and exposure to security attacks	• Increased Packet Delivery Ratio (PDR) and data transfer rate. • Extended network lifetime with low energy consumption.	• Uses complex learning methods.	2025
Source Location Privacy Protection Algorithm Based on Polyhedral Phantom Routing in Underwater Acoustic Sensor Networks. [9]	Source Location Privacy Protection Algorithm Based on Polyhedral Phantom Routing	Passive attacks	• Protect the privacy of underwater resource locations. • Enhance network security. Improve throughput and load balancing.	• Energy consumption increases with increasing network depth and radius.	2024
AIDPS: Adaptive Intrusion Detection and Prevention System for Underwater	Decentralized Adaptive Intrusion Detection and Prevention System	Underwater attacks such as (black hole, gray hole, flooding)	• Detects intrusions even as node count increases. • Lightweight for use in	• Inability to analyze and detect certain attack types (e.g., DoS attacks)	2024

Acoustic Sensor Networks. [15]	(AIDPS)		resource-constrained environments. Covers three types of attacks (black hole, gray hole, and flooding).		
A Dynamic Trust Model for Underwater Sensor Networks Fusing Deep Reinforcement Learning and Random Forest Algorithm. [18]	Dynamic Trust Model combining Deep Reinforcement Learning and Random Forest Algorithm	Malicious nodes disrupting communication, dropping packets, or launching various attacks	• Effective malicious node detection model. • Robust performance in sparse networks. • Accurately assesses trust values for identifying malicious nodes.	• Excludes scenarios with malicious nodes participating in eavesdropping attacks	2024
DOIDS: An Intrusion Detection Scheme Based on DBSCAN for Opportunistic Routing in Underwater Wireless Sensor Networks. [14]	Density-Based Spatial Clustering (DBSCAN) intrusion detection system (DOIDS)	Secure data transmission from sensor to sink nodes against various attacks	• Effective against multiple attack types. • Improves hop count efficiency and packet delivery rate. • Reduces energy consumption in low-threat scenarios	• More effective with small-scale malicious node detection (limited scalability for large networks). • Doesn't account for water current effects on node mobility.	2023
SDAA: Secure Data Aggregation and Authentication Using Multiple Sinks in Cluster-Based Underwater Vehicular Wireless Sensor Network. [17]	Cluster-based authentication using multiple mobile sinks.	Secure communication in UWSNs with network constraints.	• Reduces transmission latency and packet loss. • Energy efficiency. • Enhanced reliability. • Improved packet delivery rates.	• Limited effectiveness against MAC-layer attacks (DDoS, collisions)	2023
Secure Fuzzy Simple Shortest Path Routing Protocol (SF-SSP) for Underwater Communication. [8]	Fuzzy logic protocol evaluating multiple node parameters and behaviours.	Malicious nodes disrupt communication, dropping packets, or launching various attacks.	• Increased throughput. • Secure routing by using only trusted nodes.	• Increased energy consumption. • Packet loss due to attacks.	2023
Securing localization-free underwater routing protocols against depth spoofing attacks. [13]	Energy-efficient Depth-Based Probabilistic Routing (DPR) protocol designed to counter depth spoofing attacks.	Vulnerability of depth-based routing to location spoofing attacks	• Reduces energy consumption. • Increased network life.	• Network density inversely impacts forwarding node performance, reducing the probability of achieving target delivery ratios. • The load increases with the increase in network density. • Increased delay due to routing via a probability parameter. • Not suitable for sparse and large networks.	2022
A Lightweight Cryptographic Algorithm for Underwater Acoustic. [6]	Lightweight image encryption algorithm for underwater transmission.	Encryption challenges in resource-constrained UWSN environments.	• Provides strong cryptographic security. • The algorithm's ability to encrypt different colored images into encrypted images that are impossible to decrypt.	• Only tested on image encryption (no video transmission validation).	2022

Secure Routing in Underwater Acoustic Sensor Networks based on AFSA-ACOA Fusion Algorithm. [7]	Hybrid routing combining: - Artificial Fish Swarm (AFS). - Ant Colony Optimization (ACO) algorithms.	Environmental threats compromising underwater communication security.	• Optimized secure routing paths. • Enhanced path selection security. • Reduces time delay. • Increased network lifetime and reliability. • Load balancing and ensuring network security.	• Limited attack detection capabilities for certain threat types.	2022
An Energy Efficient Crypto Suit for Secure Underwater Sensor Communication using Genetic Algorithm.[5]	Genetic algorithm-based symmetric key generation for energy-efficient cryptography.	Passive attacks	• Reduced computational overhead. • High throughput performance.	• Lacks lightweight encryption for comprehensive attack protection.	2021
DBSR: A Depth-Based Secure Routing Protocol for Underwater Sensor Networks. [4]	Enhanced Depth-Based Routing (DBR) with Elliptic Curve Cryptography (ECC).	Depth information spoofing attacks.	• High packet delivery rate. • Reduced packet loss.	• Specialized only for depth-spoofing attacks. • No key exchange mechanism.	2020
SAPDA: Secure Authentication with Protected Data Aggregation Scheme for Improving QoS in Scalable and Survivable UWSN. [16]	Secure cluster-based authentication with protected data aggregation.	Environmental threats compromising underwater communication security.	• Reduced delay. • Reduced energy consumption.	• Performance degradation under increasing attacker presence	2020
Cluster based Detection and Reduction Techniques to Identify Wormhole Attacks in Underwater Wireless Sensor Networks.[11]	Wormhole detection via round-trip time (RTT) analysis in clustered networks.	Wormhole attack in underwater wireless sensor networks.	• Increased throughput and packet delivery rate. • Reduced energy consumption and latency. • Wormhole attack resistance.	• Cluster head maintenance challenges degrade routing performance.	2020
Underwater Wireless Sensor Network Route Optimization using BIHH Technique. [12]	Bandwidth-optimized routing using Bellman-Inora Hex Hamming (BIHH) metric.	Black hole attack in underwater wireless sensor networks.	• Reduced packet loss rate. • Reduced energy consumption. • Black hole attack resistance.	• Increasing delay due to constantly searching for an alternative path in case of failure.	2020

6. CONCLUSION AND RECOMMENDATIONS

This study provides a comprehensive analysis of the security challenges facing Underwater Wireless Sensor Networks (UWSNs), with a focus on core security requirements and recent innovations in the field. The results of the systematic review reveal that UWSN security still faces significant obstacles, particularly due to energy constraints, complex underwater environments, and diverse cyber threats. However, innovative solutions such as light- weight encryption algorithms, AI-powered intrusion detection systems, and dynamic trust management models show promising potential for enhancing security in these networks.

The study highlights several key points:

Need for Balanced Solutions: Security solutions must strike a balance between stringent security requirements and resource limitations, such as energy and bandwidth.

Importance of Technology Integration: Combining artificial intelligence, blockchain, and advanced cryptography can provide multiple security layers, improving network resilience against attacks.

Current Research Gaps: More work is needed in areas such as testing solutions in real-world environments, improving scalability, and developing cross-layer security protocols.

This study emphasizes that UWSN security is not just a technical challenge but a critical factor in ensuring the success of sensitive applications like environmental monitoring and marine exploration. It also provides clear recommendations for researchers and developers, including:

- Adopting multi-layered approaches to enhance security without overburdening network resources.
- Investing in standardized infrastructure for testing security solutions in realistic underwater environments.
- Exploring emerging technologies such as quantum computing and generative AI to address future threats.

In conclusion, this study serves as a valuable reference for researchers and professionals interested in UWSN security, offering comprehensive insights and clear directions for future research and development in this vital field. These findings are expected to inspire further innovations in underwater network security that contribute to building secure and reliable underwater networks, supporting critical marine applications in the future.

7. REFERENCES

[1] Emad Felemban, Faisal Karim Shaikh, UmairMujtaba Qureshi, Adil A. Sheikh, and Saad Bin Qaisar, " Underwater Sensor Network Applications: A Comprehensive Survey," Hindawi Publishing Corporation International Journal of Distributed Sensor Networks, 14 pages, Volume 2015.

[2] Guang Yang, Lie Dai, Guannan Si, Shuxin Wang, Shouqiang Wang, "Challenges and Security Issues in Underwater Wireless Sensor Networks," Procedia Computer Science, pp. 210–216, 2019, DOI: 10.1016/j.procs.2019.01.225.

[3] Salmah Fattah, Abdullah Gani, Ismail Ahmedy, Mohd Yamani Idna Idris and Ibrahim Abaker Targio Hashem, "A Survey on UnderwaterWireless Sensor Networks: Requirements, Taxonomy, Recent Advances, and Open Research Challenges," *Journal of MDPI,* pp. 1–30, 2020, DOI: 10.3390/s20185393.

[4] Ayman Alharbi, "DBSR: A Depth-Based Secure Routing Protocol for Underwater Sensor Networks," *(IJACSA) International Journal of Advanced Computer Science and Applications*, pp. 628- 634, Vol. 11, No. 9, 2020.

[5] Fozia Hanif, Urooj Waheed, Samia Masood, Rehan Shams and Syed Inayatullah, "An Energy Efficient Crypto Suit for Secure Underwater Sensor Communication using Genetic Algorithm," *Sukkur IBA Journal of Emerging Technologies*, pp. 1 – 17, Vol. 4, No. 2, July – December 2021.

[6] S. B. Goyal, Renjith V. Ravi, Chaman Verma, Maria Simona Raboaca, Florentina Magda Enescu, "A Lightweight Cryptographic Algorithm for Underwater Acoustic Networks," *Procedia Computer Science*, pp. *266–273,* 215 (2022), DOI: 10.1016/j.procs.2022.12.029.

[7] Ziyuan Wang, Jun Du, Zhaoyue Xia, Chunxiao Jiang, Zhengru Fang and Yong Ren, "Secure Routing in Underwater Acoustic Sensor Networks based on AFSA-ACOA Fusion Algorithm," *IEEE International Conference on Communications*, pp. 1409-1414, 16-20 May 2022, DOI: 10.1109/ICC45855.2022.9838802.

[8] Salma S Shahapur, Rajashri Khanai, D A Torse, Chinmay Abhay Nerurkar and H P Rajani, "Secure Fuzzy Simple Shortest Path Routing Protocol (SF_SSP) for Underwater Communication," *Indian Journal of Science and Technology*, pp. 4016-4025, 16(44), 2023, DOI: doi.org/10.17485/IJST/v16i44.2009.

[9] Guangjie Han, *Fellow, IEEE*, Ru Xia, Hao Wang, and Aohan Li, "Source Location Privacy Protection Algorithm Based on Polyhedral Phantom Routing in Underwater Acoustic Sensor Networks," *IEEE INTERNET OF THINGS JOURNAL*, VOL. 11, NO. 5, 1 MARCH 2024, DOI: 10.1109/JIOT.2023.3318567.

[10] A. Shenbagharaman and B. Paramasivan, "Secure and energy efficient routing protocol for underwater wireless sensor network using running city game optimization with XGBoost algorithm," *Elsevier Applied Soft Computing*, Volume 169, January 2025, DOI://doi.org/10.1016/j.asoc.2024.112615.

[11] Tejaswini R Murgod and Dr. S Meenakshi Sundaram, "Cluster based Detection and Reduction Techniques to Identify Wormhole Attacks in Underwater Wireless Sensor Networks," *(IJACSA) International Journal of Advanced Computer Science and Applications*, pp. 58-63, Vol. 11, No. 7, 2020.

[12] Turki Ali Alghamdi, "Underwater Wireless Sensor Network Route Optimization using BIHH Technique," *(IJACSA) International Journal of Advanced Computer Science and Applications*, pp. 343- 349, Vol. 11, No. 6, 2020.

[13] Ayman Alharbi, Alaa M. Abbas and Saleh Ibrahim, "Securing localization-free underwater routing protocols against depth-spoofing attacks," Elsevier *Array,* Volume 13, March 2022, DOI: 10.1016/j.array.2021.100117.

[14] Rui Zhang, Jing Zhang, Qiqi Wang and Hehe Zhang, "DOIDS: An Intrusion Detection Scheme Based on DBSCAN for Opportunistic Routing in Underwater Wireless Sensor Networks," Journal of Sensors*, pp. 1-21, 2023, DOI:* doi.org/10.3390/s23042096.

[15] Soumadeep Das, Aryan Mohammadi Pasikhani, Prosanta Gope, John A. Clark, Chintan Patel, and Biplab Sikdar, "AIDPS: Adaptive Intrusion Detection and Prevention System for Underwater Acoustic Sensor Networks," *IEEE/ACM TRANSACTIONS ON NETWORKING*, VOL. 32, NO. 2, APRIL 2024,

[16] Nitin Goyal · Mayank Dave and Anil Kumar Verma, "SAPDA: Secure Authentication with Protected Data Aggregation Scheme for Improving QoS in Scalable and Survivable UWSNs," *Springer Wireless Personal Communications,* pp. 1-15 2020, DOI: 10.1007/s11277-020-07175-8.

[17] Samuel Kofi Erskine, Hongmei Chi and Abdelrahman Elleithy, "SDAA: Secure Data Aggregation and Authentication Using Multiple Sinks in Cluster-Based Underwater Vehicular Wireless Sensor Network," *Journal of Sensors*, pp. 1-20, 2023, DOI: doi.org/10.3390/s23115270.

[18] BeibeiWang, Xiufang Yue, Yonglei Liu, Kun Hao, Zhisheng Li and Xiaofang Zhao, "A Dynamic Trust Model for Underwater Sensor Networks Fusing Deep Reinforcement Learning and Random Forest Algorithm," *Journal of MDPI*, pp. 1-21,2024, DOI: doi.org/10.3390/app14083374.