https://doi.org/10.1051/itmconf/20268701021

Secure Hybrid Routing Strategy for Efficient Path Identification in Underwater Wireless Sensor Networks

Sunith Kumar T
Manipal Institute of Technology
Manipal Academy of Higher Education
Manipal, India
sunith.mitmpl2023@learner.manipal.edu

Yashwanth N
Manipal Institute of Technology
Manipal Academy of Higher Education
Manipal, India
yashwanth.n@manipal.edu

Bhaskar Awadhiya
Manipal Institute of Technology
Manipal Academy of Higher Education
Manipal, India
awadhiya.bhaskar@manipal.edu

Anush Bekal
Department of Electronics and Communication Engineering
Sahyadri College of Engineering & Management
Mangaluru, India
anush.ec@sahyadri.edu.in

Vidya Rao
Manipal Institute of Technology
Manipal Academy of Higher Education
Manipal, India
vidyarao.mit@manipal.edu

***Abstract* -- Underwater Wireless Sensor Networks (UWSNs) are important devices that are used in ocean monitoring, environmental studies, and measurements of underwater structures. Nevertheless, data routing in UWSNs has a number of challenges, which are the lack of bandwidth, excessive propagation delay, energy, erratic communication conditions due to the nature of acoustic channels. These issues necessitate such routing protocols that are specially tailored to the underwater environments. The paper involves a performance analysis of the current routing protocols and the suggestion of a better routing scheme named MRAR-UWSN (Mobility and Reliability Aware Routing to UWSNs) which will ensure a higher efficiency and reliability of communication. The protocol under consideration is based on adaptive routing decisions to minimize packet loss and enhance the effectiveness of transmitting data to the destination with the network density varying. The simulation experiments were done in a 500 x 500 x 500 m 3 network with node densities of 100 to 300 nodes. The findings reveal that MRAR-UWSN is better than the current protocols, including DBR, EEDBR and EZMR. MRAR-UWSN has an average throughput of 32 at 300 nodes as opposed to the 21 of DBR, 25 of EEDBR, and 17 of EZMR. Moreover, the suggested solution will decrease the packet drop ratio to 25, when DBR, EEDBR, and EZMR demonstrate 63, 54, and 47, respectively. The above findings suggest that the proposed protocol is reliable, scalable and efficient in routing data and hence it is applicable in ocean monitoring, environmental surveillance, disaster management, and underwater exploration.**

***Keywords**: Underwater Wireless Sensor Network, Data Encryption, Hybrid Routing Algorithm, Data Processing, Visualization & Analysis*

I. INTRODUCTION

The UWSNs is an excellent device that allows exploring and maintaining the watch over the huge and incomprehensible ocean. These networks consist of sensor nodes which generate power themselves and are well located underwater to provide data about things such as salinity, temperature, the speed of current and even the pressure. This knowledge is extremely helpful as it can be used to promote science, protect marine lives, and assist in various corporate operations, including fisheries management and offshore exploration. UWSNs are potentially very promising [1], yet they contain a good number of peculiar and challenging issues that make them unlike other networks. The marine environment under the sea is inherently harsh and turbulent. In this environment, communication is based on acoustic waves which are characterized by a low bandwidth, multipath propagation and high attenuation. It is due to these that data requires more time to reach its destination, is less reliable, and more energy consuming [2]. Unlike on land, where it is easy to replace or replace batteries, underwater sensor nodes are frequently located in remote and inaccessible locations and therefore energy efficiency is the number one consideration. The environment under the water is in a state of constant change such as water currents, changes with time, and marine life hence making UWSNs more difficult to use. Security is another issue. Attackers can intrude UWSNs in numerous ways, among them as Eavesdropping, data modification, and denial of service attacks [3]. Such weaknesses may undermine the integrity and the security of obtained information, thus threatening scientific and commercial activities. Regrettably, the routing protocols that have been developed to support terrestrial network are incompatible with these problems. They are frequently in conflict with objectives of data security, energy efficiency, and dependability which contributes to the fact that UWSNs can be attacked and inefficient [4].

II. RELATED WORKS

The UWSNs are transforming the way we are seeing the oceans- environmental studies and pipeline inspections among others are made possible. However, be it honest, the world under the sea is not a place to communicate in. Such challenges as low bandwidth, annoying delays, extremely limited energy budgets, and security threats make designing effective routing protocol a nightmare. These are the issues that scientists have been snacking at with certain work-arounds. As an illustration, they came up with a depth-based routing scheme in [5] that exploits an extremely intelligent mechanism that utilizes the positioning of nodes to conserve energy without compromising on the delivery of data. Article [6] allows specific nodes to combine the information in form of clusters, reducing the number of unnecessary sends. These are not bad initiatives, however, [7] argues that energy efficiency is a matter of concern especially with regard to the dynamic and unpredictable underwater networks.

Another poor weak point is security. Eavesdropping, tempering and attacks are simple through open under water channels. Encryption and authentication were [8] preferred to lock things down though it came at a cost of energy that was too high, not an optical attribute of battery limited sensors. The reason why [9] did not do a better job by encrypting the entire data but most significant amounts, which were intended to maintain a balance between security and efficiency, is smart. Meanwhile, [10] presented a trust-driven mechanism which monitors the behaviour of a node in order to remove the rotten actors. However, [11] adds that it is not a silver bullet since in many cases, good security is in conflict with the UWSN energy limitations.

In recent years, there is the arrival of machine learning, and it is associated with fresh hopes. On-the-fly adaptive routing protocol, which is designed using reinforcement learning, is implemented by [12] to improve both energy saving and data delivery. And [13] trained a deep learning model, which detected and prevented real-time attacks. But, as [14] reminds us, AI-based solutions, in these cases, are expensive to maintain, as they demand a lot of computational power, which one can hardly possess when he or she is in the ocean. The real progress notwithstanding, energy drain and unreliable connections are still the bottlenecks of UWSNs. The security gaps also do not facilitate its progress. The next giant step can be hybrid routing with a lite encryption - as one of the examples of what was presented in this survey. With the capability to reduce the energy price of security and adjust machine learning to underwater demands, the networks can finally have the ability to achieve their potential [15]. The future is obvious: the more energy-aware, smart, and meaner protocols are the ticket into the future of the UWSNs.

A. Limitations of Existing Systems

Many of the available systems can be said to be restricted in one or more of the following: high energy consumption, low ratio of packet delivery, vulnerability to numerous attacks and inability to dynamically adapt to underwater environments; as it is witnessed Table 1.

Table 1: Limitations of different studies and technologies used.

Study	Main Objectives	Merits	Demerits	Year	Technologies Used
1. Secure Data Transmission in UASNs [16]	To develop a lightweight encryption protocol for secure data transmission in UASNs.	Reduces energy consumption and computational overhead.	Limited scalability for large networks.	2021	Lightweight Cryptography, Acoustic Modems
2. DoS Attack Mitigation [17]	To propose a mechanism for detecting and mitigating Denial-of-Service (DoS) attacks in UASNs.	Effective in identifying malicious nodes and ensuring network availability.	High false-positive rate in dynamic underwater environments.	2022	Machine Learning, Intrusion Detection Systems
3. Energy-Efficient Authentication [18]	To design an energy-efficient authentication scheme for UASNs.	Minimizes energy consumption while maintaining high security.	Vulnerable to replay attacks in high-latency scenarios.	2021	Hash Functions, Symmetric Key Cryptography
4. Secure Localization [19]	To enhance node localization security against spoofing attacks.	Improves accuracy and reliability of node positioning.	Requires additional hardware for implementation.	2023	Time-of-Arrival (ToA), Digital Signatures
5. Privacy-Preserving Data Aggregation [20]	To ensure privacy and integrity in data aggregation processes.	Protects sensitive data from eavesdropping and tampering.	Increases latency due to additional encryption layers.	2022	Homomorphic Encryption, Data Aggregation Protocols

6. Resilient Routing Protocols [21]	To develop secure and resilient routing protocols for UASNs.	Enhances network robustness against routing attacks.	Complex to implement in highly dynamic underwater environments.	2023	Multi-Path Routing, Trust-Based Mechanisms
7. Jamming Attack Detection [22]	To detect and mitigate jamming attacks in UASNs.	Provides real-time detection and response to jamming.	High computational cost for continuous monitoring.	2022	Signal Processing, Anomaly Detection Algorithms
8. Secure Key Management [23]	To propose a distributed key management system for UASNs.	Ensures secure key distribution and reduces single points of failure.	Requires significant initial setup and coordination.	2022	Elliptic Curve Cryptography, Distributed Systems

B. Different Types of Routing Threats and Attacks

There are other threats to UWSNs that have to be addressed with the help of specific solutions. The properties of the aquatic environment contribute to the vulnerability of networks to selective forwarding attacks (discarding node critical packets), wormhole attacks (namesake pseudo routing), Sybil attacks (node false identities), blackhole attacks (total assimilation of information), and jamming (impedance of signals). The current countermeasures involve multipath routing, systems of trust, cryptographic authentication and frequency-hopping. The possible solutions must however take into account the limited nature of the network resources towards the security control. The two methods utilized in our proposed hybrid routing usage are distance-vector, and location-based routing which is done by dynamically selecting the best paths to come up with a routing that puts into consideration the node energy, the distance and quality of the links. In this system, symmetric-key encryption is used with effective key management and authentication steps to come up with an overall solution against all threats.

Terrestrial and underwater networks (as illustrated in Table 2) have different requirements in form of routing protocols.

But in underwater it is another story altogether. Sound waves fight slower speeds, more energy desires and relentless interference of moving currents, changing temperatures and even marine activity [24]. This chaotic environment brings the dependability of underwater communication to a fraction of the same kind when done on land. When on the ground, things are predictable, stable, whereas in the ocean, the networks struggle with the hostile nature of water and must adopt specialty and sometimes costly ways of simply getting the data flowing. The variations between the two cannot be any bigger.

1. **Vector-Based Forwarding (VBF)**:

Whereas the ground networks use effective RF waves, UWSNs use fast and energy-inefficient acoustic messages, which are prone to noise, current, and temperature change. A future study should examine the adaptive security models that may safeguard networks without affecting the performances amidst such perilous environments.

Naturally the inherent differences between both terrestrial and underwater networks (as shown in Table 2) require specific routing schemes. UWSNs are required to employ slow energy consuming acoustic signals that are limited by currents, noise, and variations in temperature whereas the earth networks can employ efficient RF waves that can be administered at long distances. The problems are in redesigning processes that focus on energy usage, acceptance of delays and ensuring delivery of data, despite changing conditions underwater. The subsequent study must be directed to the adaptive security models capable of maintaining the performance of the networks, as well as dealing with the dynamically evolving threats in the dynamic environment. There is a high disparity in both the underwater and terrestrial environments in terms of how they support communication and the exchange of data

The nodes that are in this pipeline relay the data as the data goes out of the pipeline and the out-of-pipeline nodes go to sleep, consuming less energy. In dense networks where positions of nodes are fixed, VBF is simple to apply and works better. Nevertheless, it is ineffective when used in sparse/ mobile networks because the fixed vector path might be inflexible to vary situations. The VBF can be used in the non-dynamic or predictable underwater conditions where the primary concerns are energy efficiency and simplicity [25]. The shortest (perpendicular) distance d can be computed by taking the formula as below (1):

$$d = \frac{|(P-S)\times(D-S)|}{|D-S|} \quad (1)$$

P= Position of the node where P is the Position of the node, S is the Source Position and D is the Destination position.

2. Hop-by-Hop Vector-Based Forwarding (HH-VBF):

The method follows a fixed pattern of vectors to pass the data packets between the source and destination location and simultaneously enables the individual nodes to optimally decide on forwarding at the local conditions by considering the actual conditions at the time e.g. the reliability of the links and the density of the node neighbours. Nonetheless, HH-VBF has an improved location accuracy and requires a higher level of computation. HH-VBF increases VBF by increasing the number of forwarding paths. The likelihood of a node to forward a packet is P_f as in (2):

$$P_f = e^{-\frac{d^2}{2\sigma^2}} \quad (2)$$

Where, d is the normal distance between the node and the pipeline and σ represents the standard deviation that determines the width of the pipeline.

III. Proposed Method

A. Architecture Diagram:

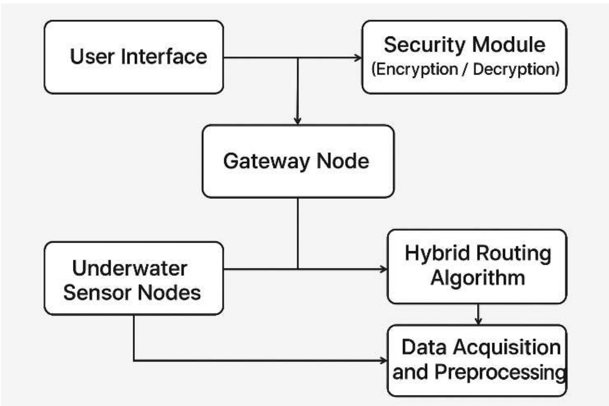

Figure 1: Proposed Architecture for Hybrid Algorithm for UWSNs

On the top end in Figure 1, the User Interface is the primary user interface that is used to allow users to send and receive data. The sensor nodes gather data on the environment, such as temperature, pressure, and salinity; they relay it back into the system. In order to guarantee secure communication, Security Module (Encryption/Decryption) has the ability to encrypt data before sending them and then decrypt them after receipt. The Hybrid Routing Algorithm influences data transfer between the sensors, security module, and gateway to be energy efficient and reliable for communication. This system is applied in marine research, environmental monitoring, defence systems among others.

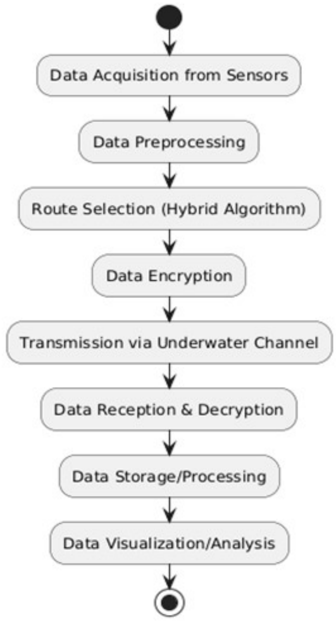

Figure 2: Flow chart for proposed model

It is worth considering the background noise elimination before any serious conversation. The true magic that occurs in the information relaying process is what comes up all through. Our routing system is a routing cop, which is always looking to find the shortest paths among sensors, security checks and surface stations, which are underwater. Security is built up by incorporating it gradually. Information is encrypted to military level before it can start moving up. The data is sent to monitoring stations and it is decrypted and stored in an organized database. Marine biologists analyse such processed data through simple interfaces so that numbers have the ability to visually indicate the ocean health. Moreover, this system is no mere theory, in fact, it is already utilizing resources to assist research teams to track the changes on the reefs systems, enable navies to track sensitive areas (some of which are more sensitive than human eyes have been able to see) and enable environmentalists to have full-frontal views of underwater ecosystems, which were previously impossible. The greater the use, the more it gets to know how to give the precise enthusiastic insight that researchers demand due to the endless feedback mechanism.

VI. Results

The average throughput performance of DBR, EEDBR, ZPR, and the proposed MRAR-UWSN protocol, with respect to node densities, is indicated in the graph. The more nodes one has, the better the throughput of all protocols is because there is more connectivity.

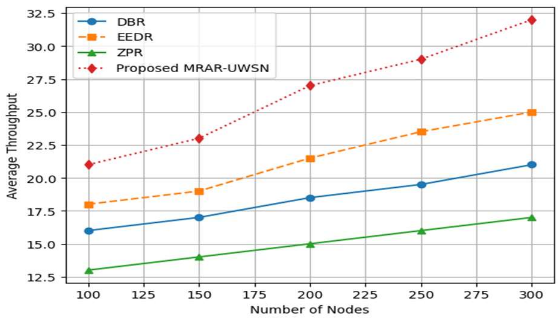

Figure 3: Average throughput vs Number of nodes

Nevertheless, MRAR-UWSN is always the highest throughput as shown in Figure 3 one that can show better delivery of packets and higher routing efficiency.

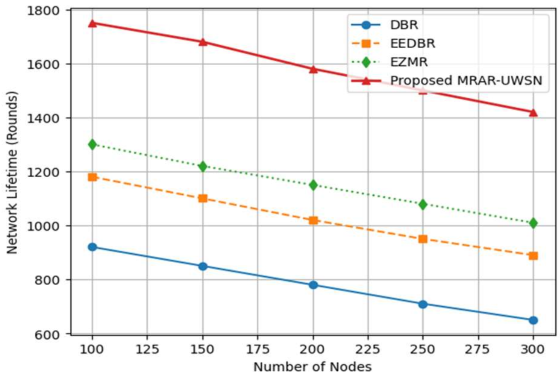

Figure 4: Network lifetime vs Number of nodes

Figure 5 shows the ratio of packets dropped by DBR, EEDBR and EZMR in addition to the proposed MRAR-UWSN protocol with the node density. The congestion and collisions in a network lead to packet drops. Nevertheless, MRAR-UWSN experiences much less loss of packets than other protocols, meaning that it is more reliable and effective in selecting of a route in dense sensor networks of underwater network.

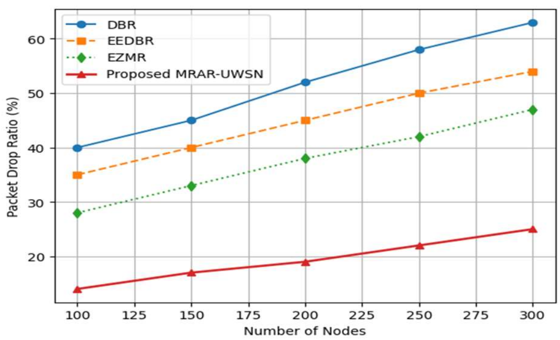

Figure 5: Packet drop rate vs Number of nodes

The findings indicate that MRAR-UWSN is always better than the current protocols regarding throughput and reliability. The higher the density of nodes, the higher the throughput can be due to the improvement of connection, and the higher the ratio of packet drops is due to congestion. Nevertheless, MRAR-UWSN is able to sustain a higher throughput and reduce substantially on the loss of packets than DBR, EEDBR and EZMR.

V. Conclusion

Underwater conditions are very different to terrestrial networks and hence conventional Wireless Sensor Network (WSN) routing protocol cannot be applied in Underwater Acoustic Sensor Networks (UASNs). Whereas terrestrial WSN is based on radio frequency communication offering it high speed and energy efficiency, underwater communication is based on acoustic signals that travel much slower and are influenced by environmental factors such as noise, changes in temperature and ocean currents. These issues bring about high latency, unreliable communication networks and high energy usage hence necessitating routing protocols that are unique to underwater environments.

In order to solve these problems, this research paper compares the performance of proposed MRAR-UWSN routing protocol with the performance of the existing routing protocols like DBR, EEDBR and EZMR. The results of simulation have shown that MRAR-UWSN can enhance the overall network performance, in terms of its increasing node density. The proposed protocol has an average throughput of 32 at 300 nodes, which is better than that of DBR (21), EEDBR (25), and EZMR (17). Moreover, the ratio of packets drop is decreased to 25, which is lower compared to 63% in DBR, 54% in EEDBR, and 47% in EZMR.

These gains show that the MRAR-UWSN has increased reliability, packet forwarding efficiency, and scalability in dense underwater deployments. Thus, the suggested protocol can be used to serve in the solution of important tasks like oceanographic surveillance, environmental surveillance, disaster reduction, and exploration of deep waters.

References

[1] V. Krishnaswamy and S. S. Manvi, “Analysis of acoustic channel in underwater acoustic sensor network,” in Proc. IEEE Int. Advance Computing Conf. (IACC), Bangalore, India, Jun. 12–13, 2015, pp. 233–236.

[2] A. Khan, I. Ali, A. Ghani, N. Khan, M. Alsaqer, A. U. Rahman, and H. Mahmood, “Routing protocols for underwater wireless sensor networks: Taxonomy, research challenges, routing strategies and future directions,” Sensors, vol. 18, no. 5, p. 1619, 2018.

[3] M. S. Khan, A. Petroni, and M. Biagi, “Cooperative communication-based protocols for underwater wireless sensors networks: A review,” Sensors, vol. 24, no. 8, p. 4248, 2024.

[4] J. Luo, Y. Chen, M. Wu, and Y. Yang, “A survey of routing protocols for underwater wireless sensor networks,” IEEE Communications Surveys & Tutorials, vol. 23, no. 1, pp. 137–160, 2021.
[5] I. U. Khan, M. Islam, M. Ismail, A. B. Qazi, S. Jan, I. Ullah, Z. Farid, and Z. Wadud, “Adaptive hop-by-hop cone vector-based forwarding protocol for underwater wireless sensor networks,” International Journal of Distributed Sensor Networks, vol. 16, p. 1550147720958305, 2020.
[6] P. Nazareth and B. R. Chandavarkar, “Cluster-based multi-attribute routing protocol for underwater acoustic sensor networks,” Wireless Personal Communications, vol. 134, pp. 781–808, 2024.
[7] D. Jiaxin, H. Guangjie, L. Chuan, and M. Miguel, “Itrust: An anomaly-resilient trust model based on isolation forest for underwater acoustic sensor networks,” IEEE Transactions on Mobile Computing, vol. 21, no. 5, pp. 1684–1696, 2020.
[8] R. Zhu, A. Boukerche, L. Long, and Q. Yang, “Design guidelines on trust management for underwater wireless sensor networks,” IEEE Communications Surveys & Tutorials, vol. 26, no. 4, pp. 2547–2576, 2024.
[9] H. Panchal and S. Gajjar, “Fuzzy-based unequal clustering protocol for underwater wireless sensor networks,” International Journal of Communication Systems, vol. 36, no. 16, Nov. 2023, doi: 10.1002/dac.5581.
[10] M. Kumar, N. Goyal, A. K. Singh, R. Kumar, and A. K. Rana, “Analysis and performance evaluation of computation models for node localization in deep sea using UWSN,” International Journal of Communication Systems, vol. 37, p. e5798, 2024.
[11] C. S. Nandyala, H.-W. Kim, and H.-S. Cho, “QTAR: A Q-learning-based topology-aware routing protocol for underwater wireless sensor networks,” Computer Networks, vol. 222, p. 109562, 2023.
[12] V. Krishnaswamy and S. S. Manvi, “Trusted node selection in clusters for underwater wireless acoustic sensor networks using fuzzy logic,” Physical Communication, vol. 47, p. 101388, 2021.
[13] B. Diao, C. Li, Q. Wang, Z. An, and Y. Xu, “A channel-aware routing protocol with nearest neighbor regression for underwater sensor networks,” arXiv preprint arXiv:2108.05057, 2021.
[14] A. Celik, N. Saeed, B. Shihada, T. Y. Al-Naffouri, and M.-S. Alouini, “Opportunistic routing for opto-acoustic Internet of underwater things,” arXiv preprint arXiv:2002.08420, 2020.
[15] M. Salman, J. Bolboli, and W. Y. Chung, “A robust UWOC-assisted multi-hop topology for underwater sensor network nodes,” arXiv preprint arXiv:2403.19180, 2024.
[16] A. B. Sarawar, A. S. M. Badrudduza, M. Ibrahim, I. S. Ansari, and H. Yu, “Secrecy performance analysis of integrated RF-UWOC IoT networks enabled by UAV and underwater-RIS,” arXiv preprint arXiv:2407.18766, 2024.
[17] H. K. M.Tanaka, “Muometric positioning system (μPS) with cosmic muons as a new underwater and underground positioning technique,” Scientific Reports, vol. 10, p. 18896, 2020, https://doi.org/10.1038/s41598-020-75843-7.
[18] R. Kumar, P. Singh, and T. K. Sharma, “SEECR: Secure energy efficient and cooperative routing protocol for underwater wireless sensor networks,” in Proc. IEEE Int. Conf. Advanced Networks and Telecommunications Systems (ANTS), 2020, pp. 1–6.
[19] V. P. Natarajan and S. Jayapal, “An improving secure communication using multipath malicious avoidance routing protocol for underwater sensor network,” Scientific Reports, vol. 14, p. 30210, 2024. https://doi.org/10.1038/s41598-024-80976-0.
[20] Y. Zhang, N. Wang, and X. Li, “Routing protocol for underwater wireless sensor networks based on a trust model and void-avoided algorithm,” Sensors, vol. 22, no. 24, p. 9525, 2022.
[21] N. Goyal, M. Dave, and A. K. Verma, “A novel fault detection and recovery technique for cluster-based underwater wireless sensor networks,” International Journal of Communication Systems, vol. 31, no. 4, p. e3485, 2018.
[22] S. Kumar, B. Kumari, and H. Chawla, “Security challenges and application for underwater wireless sensor network,” in Proc. Int. Conf. Emerg., vol. 2, 2018, pp. 15–21.
[23] S. Jiang, “Security in UWANs,” in Wireless Networking Principles: From Terrestrial to Underwater Acoustic. Singapore: Springer, 2018, pp. 337–367, doi.org/10.1007/978-981-10-7775-3_13.
[24] J. Luo, Y. Chen, M. Wu and Y. Yang, "A Survey of Routing Protocols for Underwater Wireless Sensor Networks," in IEEE Communications Surveys & Tutorials, vol. 23, no. 1, pp. 137-160, First quarter 2021, doi: 10.1109/COMST.2020.3048190.
[25] K. G. Omeke et al., “DEKCS: A Dynamic Clustering Protocol to Prolong Underwater Sensor Networks,” IEEE Sens J, vol. 21, no. 7, pp. 9457–9464, Apr. 2021, doi: 10.1109/JSEN.2021.3054943.