*Nat. Volatiles & Essent. Oils, 2021; 8(5): 5062 – 5070*

# Eapd – Exploration of Availability Possibilities and Desires in Underwater Sensor Network

**Mrs. Deepthi B P [1], Dr. Lekha J[2]**

*[1]PhD Research Scholar , [2] Assistant Professor*

*[1,2] Department of computer science, Sri krishna arts and science college*

*[1]deeptham08@gmail.com, [2]lekhaj@skasc.ac.in*

**Abstract**

Sensors are located at different depths of the ocean and on the surface of the water, making them more difficult to monitor, and their environment is highly variable. And its resources are much smaller than other network components. So, making connections in these and pursuing them with confidence is one of the most challenging. It operates underwater under different conditions which increases the failure rate of its contacts. Also, there may be a predominance of certain malicious nodes, this can lead to errors and losses in data transmissions. Security calculations may cause delays in communication. This will increase data loss, delay, lifetime reduction, etc. All these will affect the performance of the network. As well as make various changes to the channels, only then can communication losses be reduced and delivery ratio increased. Network performance can be enhanced by linking sensors to accurate calculations with optimization on channel, security, energy saving, trusted neighbor selection, required path selection, etc. in this network.

**Keywords**: Underwater Sensor; Resources; Failure Rate; Malicious Node; Errors; Losses; Optimization;

## Introduction

The sensors can be placed on the network statically or mobile. Sensors can be placed only with random mobility, especially in the underwater network. In addition, underwater sensors require protocols that can adapt to changes in the environment. Therefore, the depth and density of the water, the ability to detect nearby sensors, or the ability to interact with mobile data collectors, robots, and unmanned vehicles, detect the void region, and overtake them are essential. Also, have the knowledge to update the underwater network changes immediately.

Because sensors operate underwater, the transmission range varies due to the movements of many objects, and it is difficult to maintain constant contact with neighbors, as well as to maintain a data path for long periods of time. This can lead to loss of function of the sensors. Thus, network connections may be completely conceded. All of these are features that can greatly affect the network.

Network channels are a major factor in making connections. Channel losses and its overload are another factor affecting network connectivity. Private channels and network propagation are used in the underwater network. This is different from ground level channels. This network operates in three dimensions. Similarly, its physical layers are different. Consider all of these in the protocols and report the methods of establishing a network connection. Similarly, data may incur losses due to sensor failure or circuit fault, and sometimes the data it provides may be incorrect. Therefore, it is important to test the reliability and then send the data to a destination as shown in Figure.1. It is important to place the sensors as needed according to the context in which the data is to be sensed. This is because the transmission area of the sensors is very small. It is important to have a few sensors within its range.

Sometimes more energy can be expended when it comes to transferring more data to a particular area. This will shorten the life of the sensor. This can cause holes in the network. This will also reduce the performance of the network. New protocols require steps for energy monitoring and maintenance. Placing sensors with the minicam where needed can take photos and video of difficult situations and some important objects. So that clear details about that environment can be obtained.

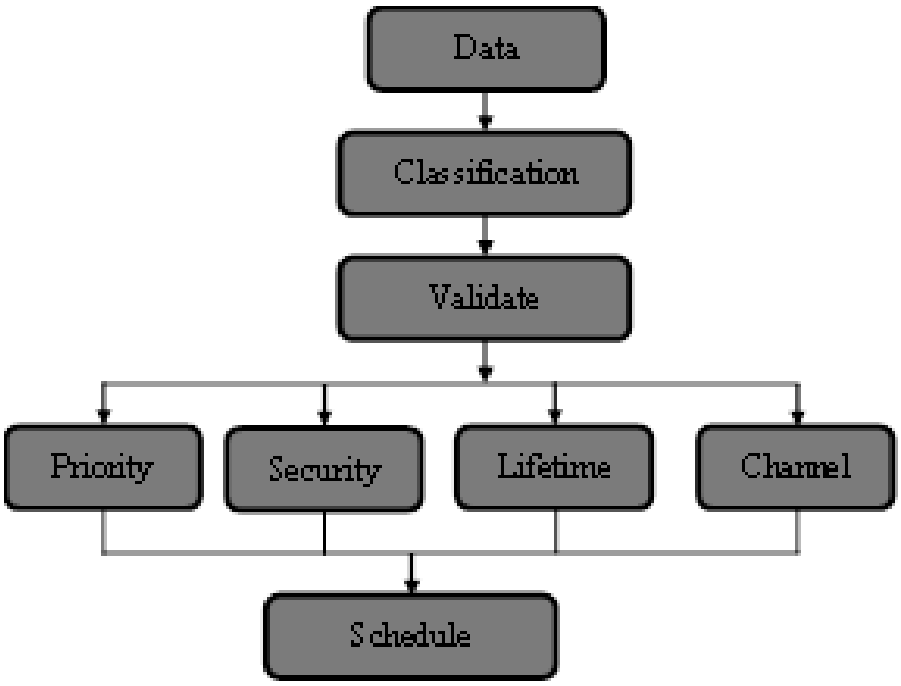


Figure.1 Underwater Communication

The sensors are small in size and its inbuilt components are small. Because its storage and buffer sizes are small, its parameters selections must be the same. Also, the protocol computations must be compatible with the sensor's hardware configuration. Like this you can set the path selection with new optimization techniques and a lot of calculations considering the needs of many networks. You can make several changes in each layer and create a cross layer protocol. We can select each neighbor and make neighbor selection accordingly. An underwater network with many features like this can be set up and protocols developed to create the best network communication.

Sensors are used underwater for different tasks. They are:

- Monitoring underwater tubes and pipelines
- Water pollution level observations
- Water quality check
- Disaster Warning
- Object detection
- Sea border surveillance

The second part of this paper gives a collection of previous research on the underwater sensor network as related works. The third section describes the various features required for an underwater sensor network. The fourth part gives the conclusions of the factors described in this paper.

**Related Works**

The utmost purpose of this study is to improve investigation achievements to lay down the fundamental principle for the development of different leading communication techniques for active underwater communication and networking for enhanced ocean monitoring and examination applications [4]. We designed sensors provided with sovereign and unmanned vehicles for an underwater survey. They used

autonomous unmanned vehicles for inspection of underneath underwater natural resources [1]. Traditionally, the broadcast channels were taken via cryptography-based solutions at higher layers, where collective protection is set up a priori by pre-handed out a set of distributed secret keys among the network bodies [8]. The sensors can be set up promptly to screen an extensive body of water, and it can assemble effectively the instruction through a self-organized network. These features of underwater sensor networks gratify the specifications of building an extensible and disseminated data recovery environment for the applications specified [17]. The marine environment is especially sensitive to malignant attacks because of the large bit failure rates, great and variable propagation holds, and poor information measures of acoustic channels. Achieving reliable entomb vehicle and sensor-AUV communication is surprisingly tight because of the quality of AUVs and accordingly the operation of sensors with water currents [12]. The exhaustion of low-frequency bands to cope with the exponential production for rich-speed wireless connection is another reason for analysing unique technologies. The clear light range is improper and hardware readily feasible, which can be accepted for data broadcast [19]. We deployed underwater sensor nodes in shallow or deep water, where it is difficult to charge or restore the nodes' batteries. To prolong the network's life, the computational efficiency and storage capacity are constricted. Hence, virtually all present probes for UWSNs concentrate on preserving energy utilization at the expenditure of capability and security [2]. The sensor nodes which are placed under the water sense different physical sizes like climate, pressure, turbidity, etc., and pause it onto the cluster head. The cluster head aggregates the taken instruction from its sensor nodes and moves it on to the surface buoy via an undersea sink node [10]. If a competitor gained information about the current topography, it can easily expand a malicious node at a good position where it can pick up packets from various nodes in the network. Here, the attacker will promote that packet with a bogus depth, forecasting a stronger position [7]. It regularly varied the network topography in an offshore situation. Under such educates, the communication pathway between source to destination pair can no longer. There are many investigators are currently occupied in improving routing protocols for delay-tolerant wireless sensor networks [14]. The spatial density of sensors within WSN is essential. As sensors become sparser in a field, each hop must deal with a higher distance. This involves power utilization, the number of hops needed to arrive at the sink, and how reports might route through a network [16]. It used UWSNs for an expanded range of applications, such as monitoring the marine situation for scientific exploration to commercial exploitation and coastline protection to underwater pollution supervise, from water-based disaster preventions to water-based sports compensation [3]. The positions of unknown nodes hit a significant character in many WSNs applications, such as monitoring applications include environmental monitoring, health survey, and tracking applications include tracking objects, beasts, humans, and vehicles [13]. Data aggregation is one of the key handling of aggregators to soften the network expenditure by wiping out the redundant data, since cutting down the packet size being imparted to the sink. It, however, impedes the already existing security demands for underwater sensor networks and involves new security modified [18]. Achieve in strong inter-vehicle and sensor-AUV communication is especially problematic because of the flexibility of AUVs and the evolution of sensors with water currents The special aspects of the underwater acoustic channel and the variations between underwater sensor networks and their ground-based counterparts take the advancement of competent and dependable security systems [5]. These nodes package communication, sensing, and calculation in a short cylindrical water-tight container. Each unit incorporates an acoustic modem and an optical modem implemented using green light and created in our lab [9]. Recent researches corresponding to UAN mainly directed on its structure and management. Though these studies have covered nearly all the considerations within the UAN infrastructure, it has made few struggles for its security, which is surely a remarkable concern when put into practice [15]. To single out the position of the node, the localization schemes are developed the anchor nodes are called reference nodes to known the location information. The node's positions could be

calculated by the position of the evidence nodes and the distance between the reference and normal nodes is still measured [11]. It is an internal architecture of an underwater sensor node that attaches between the other sensors, which receive the data and preserve it in the memory, deal with it, and transfer it to the base station. In underwater sensor nodes are used an acoustic link to get through with each new cause of huge strength [6].

**Eapd Deliberation**

**Network Design Necessities**

First, we need to build a network structure from the deep sea to the sea level. The data collected from sea deep and it should be sent to the sea level or to the nearest communication mobile tower. These data range from natural changes under the sea to emergency data such as complexity changes and life safety. The configuration runs on a variety of equipment ranging from sensors, sonobuoy, base stations and operational servers. Key features such as power, channel, bandwidth, storage, buffer etc. will act as its resource. A protocol will work to run all of these properly. The combination of all these will determine its quality. In an underwater sensor network, this type of communication requires attention because there is a channel under the sea and a channel above the sea. The signals sent from the bottom of the ocean must be added to the base station very quickly by the sonobuoy above the ocean. Otherwise, those signals will fade at high speed.

**Security Needs in Underwater Communication**

The cryptography technique encrypts and sends data, and when it is added to the receiver or destination, it decrypts the encrypted data and opens the original data without changing the originality of the data, which is challenging in the underwater sensor. It plays an important role in data security. But how we use it in the network is also very important. During this key sharing, we can generate both symmetric key and asymmetric key. Symmetric key generation uses both the source and the destination to encrypt and decrypt the same key. Similarly, an asymmetric key is a source and destination that uses different keys to perform encryption and decryption. Determining what type of keys are needed for the network we are designing is one of the most important. When we share this key, we can attach the hash value as well. This will add an identification code to each key. This will give each encrypted data a unique identity. Similarly, each data may be of different size. In this secure transmission line digital signature is also a method of secure delivery. It is a source node, a shared key generated using the private key and some required parameters. When it receives the destination and decrypts it, it opens the source enclosed parameters and checks its signature.

In this, the public key that is created between the source and the destination is used to extract the enclosed parameters in the source and thereby find the signature of the source and the destination. The methods to be used in underwater sensor communication should be clearly stated in the protocol, and Integrate practices that are less computational cost.

We can also generate a secure certificate and send it with the data. It combines information about the node that sends the data with some information about the features of the data being transmitted generates a certificate and encrypts it, thus avoiding information exchange between the network. It is also important to monitor energy.

**Attacker Roles Among Network Sensors**

The malicious nodes that operate between the sensors collect the data and perform various actions such as causing losses, altering the authenticity of the data, and increasing the transmission distance, which affects

the operation of the network as shown in Figure. 2. Many malicious nodes can operate on the network, such as vampire, sybil attack, blackhole, worm connections, denial of service attack and so on. Accuracy and speed are essential in this connection. Similarly, these can be turned off and act differently on the layers. There is a need to find all of these and release them from contact and continue communication. It is important to identify outdated data, distinguish malicious activities, classify the data and determine its originality and the nature of the data.

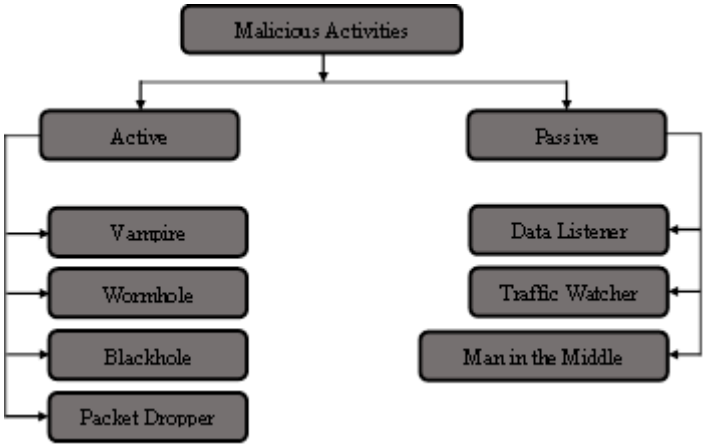


Figure. 2 Malicious Activities

**Energy Preservation Methods**

Each sensor consumes a lot of energy during transmission and notifications shared on the MAC layer during channel selections. Also, many control packets are used to maintain network connections. Energy will still be expended. Too much energy is consumed when the network is disconnected and the load on the network is shared. There will be high power usage even when network failures occur. Energy usage is when data is received and forwarded by one sensor to another sensor.

Also, if there are malicious nodes in the network, of course, the energy usage will be used too much and efforts will be made to reduce the lifespan of the network. The neighbor near each sensor should be a trusted node. Otherwise there will be a problem with the network connection and the resources will be misused. Connections must be without loops during network connections. This will confuse the nature of the network.

Choosing a loop-free neighbor is important here, as well as monitoring long-lasting neighbor relationships. In addition, multipath, multi-channel and cluster routing for load balancing reduce energy consumption. As well as a secure communication system and trust calculations tailored to the nature of the network will further reduce its energy salinity.

**Channel Availability and Requirements**

Generally, radio signals travel deeper into the water than the ground. More signals will be affected depending on the water heat, salinity, and penetration of the water. The optical channels used here are also affected by some moving objects, which can cause changes and effects on the channel frequency. This will greatly reduce the channel quality. The bandwidth of the channels operating at the depth of the water is very low. The amount of data that goes through it will also be less. As well as the effects of the selected channel's behavior on the transmission. This will cause data loss in the channel as well as increase its energy consumption. Similarly the signals traveling underwater travel in different directions and reach the

base station. Then its channels will keep changing. The signals of this network travel from the ground to the depths of the ocean through different nodes and interact with moving nodes, causing greater losses.

Modulation methods and forward error correction methods operating in channels also play an important role in transmission. When too many signals are shared, there will be interference between them and data breaks and delays in delivery. As well as a variety of noises in the water can affect signal communication. Noise caused by energy consumption, noise caused by turbulence in water, noise caused by heat generated in water My various types of noise can cause damage and loss of contact. The choices in this type of network and the methods of using them should be clearly stated in the protocol. Only then can its losses be minimized and transmissions increased.

**Underwater Sensor Routing Methodologies**

**Data Aggregation**

Aggregating data on the network avoids the need to repeatedly send the same data multiple times. It is widely used in tree routing. This saves network resources by summarizing data of the same value and type collected from the same network area and then averaging that data according to the number of nodes that sent it. This can be applied to the cluster network as well as shown in Figure.3. If the network density under the sea is high, the data collected in that area will be the same and the lifespan of the network will be extended by aggregating them with the same values.

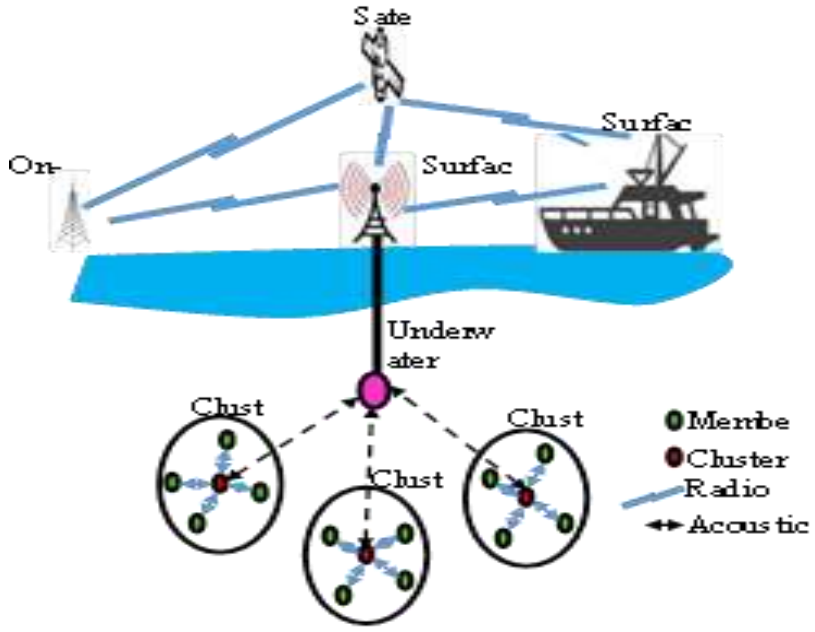


Figure.3 Cluster Routing in Underwater Network

**Mobile Data Collectors**

Mobile data collectors travel many kilometers across the network. Thus, even if some sensors are in the depths of the water these collectors will receive data from those sensors as they travel through its area. It also collects data from nodes that cannot send data to other forwarders. Similarly, due to mobility and distance in the sparse network, it may be difficult to get a forwarder. void regions may develop more. This issue will also be resolved by the data collectors. This routing system will also solve various complications such as interference, channel shortage, congestion, collision that occur in dense networks. These data collectors can be a marine, robotics, or an unmanned vehicle. This routing system requires routing with many parameters. The routing protocol should specify the routes required for the data collectors to travel,

the time to wait, the directors to move, and the messages to notify the sensors of its arrival. This can align the overload problem of the network.

**Result Discussion**

The number of sensors must be changed according to the region of the network. Also, sensors that sense various data should be placed. The specific network size required for the simulation must be specified. Also, the transmission range should be assigned according to the nature of the sensors. Protocols that can monitor various situations must be embedded in them. The functions of all these can be predicted and their performance can be calculated as follows. These include packet delivery ratio, delay, packet loss, energy consumption, overheads. All of these are calculations that measure the performance of the network. Various network parameters discussed in Table.1.

| **Considerations** | **Underwater Communication** | **Wireless Communication** | |
|---|---|---|---|
| | | **Sensor** | **Adhoc** |
| Bandwidth | Tiny | Slight | Reasonable |
| Energy Utilization | Huge | Minor | Little |
| Sensor Compactness | Minimum | Huge | Reasonable |
| Strength | Moderate | Weak | Upright |
| Storage | Very Less | Minimum | Inadequate |
| Action Ability | Minimum | Weak | Normal |
| Atmosphere | Water | Air | Air |
| Deployment Cost | Classy | High | High |

Table.1 Network Parameter Classification

**Conclusion**

In this extension, several features of the underwater sensor network are described. It describes the communication methods, requirements, changes, current system, and future network improvements that will be required. It also describes the parameters, features, and innovations in the protocol that should be included in the sensors. Existing MAC, channel. And the features required in the physical layers are also discussed. Above all are the methods required for security and trust communication. Thus, many things and future needs for underwater communication have come to the fore in this discussion.

**References**

1. Muhammad Khalid, Farah Ahmad, Muhammad Arshad, Waqar Khalid, Naveed Ahmad & Yue Cao, “E2MR: Energy Efficient Multipath Routing Protocol for Underwater Wireless Sensor Networks”, IET Research Journals, The Institution of Engineering and Technology 2015.
2. Guang Yanga, Lie Daia, Guannan Sia, Shuxin Wanga, Shouqiang Wanga, “Challenges and Security Issues in Underwater Wireless Sensor Networks”, International Conference on Identification, Information and Knowledge in the Internet of Things, 2019.

3. Emad Felemban, Faisal Karim Shaikh, Umair Mujtaba Qureshi, Adil A. Sheikh, and Saad Bin Qaisar, “Underwater Sensor Network Applications: A Comprehensive Survey”, Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume, 2015.
4. Ian F. Akyildiz, Dario Pompili, Tommaso Melodia, “Challenges for Efficient Communication in Underwater Acoustic Sensor Networks”.
5. Ekta Deshmukh, Rajendra Singh Yadav, Nandini Upadhyay, “Securing Underwater Wireless Communication Networks”, International Journal of Advanced Research in Computer and Communication Engineering(IJARCCE), Vol. 5, Special Issue 3, November 2016.
6. Syed Mohtashim Mian, Dr. Rajeev Kumar, “Review on Intend Adaptive Algorithms for Time Critical Applications in Underwater Wireless Sensor Auditory and Multipath Network”.
7. Ayman Alharbi, “DBSR: A Depth-Based Secure Routing Protocol for Underwater Sensor Networks
8. ”, International Journal of Advanced Computer Science and Applications(IJACSA), Vol. 11, No. 9, 2020.
9. Waqas Aman, Muhammad Mahboob Ur Rahman, Junaid Qadir, Haris Pervaiz, Qiang Ni, “Impersonation Detection in Line-of-Sight Underwater Acoustic Sensor Networks”, 7 Aug 2018.
10. Carrick Detweiller, Iuliu Vasilescu, Daniela Rus, “An Underwater Sensor Network with Dual Communications, Sensing, and Mobility”.
11. M.Karpagam, D.Prabha, “Underwater Wireless Sensor Network Based Marine Environment Monitoring System”, International Journal of Oceans and Oceanography, Volume 13, Number 2, 2019.
12. Baranidharan. V and Kiruthiga Varadharajan, “Secure Localization Using Coordinated Gradient Descent Technique for Underwater Wireless Sensor Networks”, ICTACT Journal on Communication Technology, March 2018.
13. L.Vetrivendan, Dr.R.Viswanathan, K.Punitharaja, “Security in Underwater Wireless Communication”, International Journal of Engineering Research in Computer Science and Engineering(IJERCSE), Vol 5, Issue 4, April 2018.
14. Jinfang Jiang, Guangjie Han, Chuan Zhu, Yuhui Dong, Na Zhang, “Secure Localization in Wireless Sensor Networks: A Survey”, Journal of Communications, Vol. 6, no. 6, September 2011.
15. R.M. Gomathi, J. Martin Leo Manickam, A. Sivasangari, “A Comparative Study on Routing Strategies for Underwater Acoustic Wireless Sensor Network”, Contemporary Engineering Sciences, Vol. 9, 2016.
16. Yangze Dong, Pingxiang Liu, “Security Considerations of Underwater Acoustic Networks”, August 2010.
17. Brian Yarbrough, Neal Wagner, “Assessing Security Risk for Wireless Sensor Networks Under Cyber Attack”, April 15, 2018.
18. Weichao Wang, Jiejun Kong, Bharat Bhargava, Mario Gerla, “Visualisation of wormholes in underwater sensor networks: a distributed approach”, Int. J. Security and Networks, Vol. 3, No. 1, 2008.
19. Rakesh Kumar and NavdeepSingh, “A Survey on Data Aggregation And Clustering Schemes in Underwater Sensor Networks”, International Journal of Grid Distribution Computing Vol.7, No.6, 2014.
20. Giuseppe Schirripa Spagnolo, Lorenzo Cozzella, Fabio Leccese, “A Brief Survey on Underwater Optical Wireless Communications”, October 5-7, 2020..

**Author Profile**

FIRST AUTHOR: DEEPTHI B P MCA, MPhil Computer science, PhD Research scholar at Sri Krishna arts and Science College.

SECOND AUTHOR: Dr. LEKHA. J MSc Computer Science, MPhil Computer Science, PhD. Associate Professor of Sri Krishna Arts and Science College