Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 1444024, 15 pages
https://doi.org/10.1155/2021/1444024

Review Article

Analysis of Security Attacks and Taxonomy in Underwater Wireless Sensor Networks

Irfan Ahmad,[1] **Taj Rahman**,[1] **Asim Zeb**,[2] **Inayat Khan**,[3] **Inam Ullah**,[4] **Habib Hamam**,[5,6,7] **and Omar Cheikhrouhou**[8]

[1]*Qurtuba University of Science & Technology Peshawar, Peshawar 25000, Pakistan*
[2]*Department of Computer Science, Abbottabad University of Science and Technology, Abbottabad 22500, Pakistan*
[3]*Department of Computer Science, University of Buner, Buner 19290, Pakistan*
[4]*College of Internet of Things (IoT) Engineering, Hohai University (HHU), Changzhou Campus, China*
[5]*Faculty of Engineering, Uni de Moncton, Moncton, NB, Canada E1A3E9*
[6]*Spectrum of Knowledge Production & Skills Development, Sfax 3027, Tunisia*
[7]*School of Electrical Engineering, Dept. of Electrical and Electronic Eng. Science, University of Johannesburg, Johannesburg 2006, South Africa*
[8]*CES Laboratory, National School of Engineers of Sfax, University of Sfax, Sfax 3038, Tunisia*

Correspondence should be addressed to Omar Cheikhrouhou; omar.cheikhrouhou@isetsf.rnu.tn

Received 23 September 2021; Revised 30 October 2021; Accepted 3 November 2021; Published 24 December 2021

Academic Editor: Hamada Esmaiel

Underwater Wireless Sensor Networks (UWSN) have gained more attention from researchers in recent years due to their advancement in marine monitoring, deployment of various applications, and ocean surveillance. The UWSN is an attractive field for both researchers and the industrial side. Due to the harsh underwater environment, own capabilities, and open acoustic channel, it is also vulnerable to malicious attacks and threats. Attackers can easily take advantage of these characteristics to steal the data between the source and destination. Many review articles are addressed some of the security attacks and taxonomy of the Underwater Wireless Sensor Networks. In this study, we have briefly addressed the taxonomy of the UWSNs from the most recent research articles related to the well-known research databases. This paper also discussed the security threats on each layer of the Underwater Wireless sensor networks. This study will help the researchers design the routing protocols to cover the known security threats and help industries manufacture the devices to observe these threats and security issues.

1. Introduction

Underwater Wireless Sensor Networks (UWSNs) are commonly used nowadays to detect and monitor the underwater environment. It contains several sensors and vehicles placed in a selected area to perform specific tasks. These networks are further connected with base stations and satellites to process the detected data for further processing. UWSNs support several applications such as river and sea pollution discovery, a compilation of oceanographic data, resource exploration, disaster prevention, monitoring, and marine surveillance [1]. Due to the attenuation of radio signals in an underwater environment, the global positioning system (GPS) cannot be used to locate sensor nodes. Therefore, UWSNs use an acoustic method of communication to send and receive the data between the source and destination. Terrestrial wireless sensor networks (TWSN) and UWSNs have distinct characteristics and functionalities. These variations can be observed in a variety of ways. To begin, UWSNs communicate by acoustic signals rather than radio transmissions like TWSNs do. TWSNs have more static networks, whereas UWSNs have more dynamic networks.

Third, compared to TWSNs, the underwater placement is unmanaged and limited. Node localization is more difficult in UWSNs than TWSNs. In addition, underwater sensor devices have more expensive hardware and are constrained by resources (i.e., memory and energy). It is also difficult to repair or recharge the batteries once they have been deployed [2]. In underwater sensor networks, the speed of sound is assumed to be constant. However, acoustic signals have distinct characteristics from radio waves. Underwater, acoustic signals travel at around 1500 m/s, which is five times a magnitude slower than radio waves. The speed is changeable and is determined by the water's temperature, pressure, and salinity. These variables cause changes in the speed of sound in underwater situations. Different applications rely on wireless sensor networks (WSNs), which serve as a key link between the physical environment and the Internet of Things [3]. WSNs are widely used in the industry for continuous object boundary detection, which is essential for WSNs [4]. Improper packet size determination degrades network performance in terms of latency, resource utilization, throughput efficiency, and energy consumption in multihop underwater networks. Still, using the optimum packet size will increase [5].

Underwater wireless sensor networks are made up of nodes deployed both on the underwater and surface of the water. All nodes must communicate and share data with other devices in the same network and the ground station. Sensor network communication methods feature data transmission via acoustic, electromagnetic, or optical wave mediums. Because of the attenuation properties of water, acoustic communication is the most common and widely utilized approach among various types of media. The poor transmission factor is generated from the conversion of energy and absorption into temperature in the water. On the other hand, acoustic signals operate at low frequencies, allowing them to be broadcast and received over great distances. Figure 1 shows the Underwater Wireless Sensor Network environment.

2. UWSNS Taxonomy

This article suggests a taxonomy based on trend analysis and surveys of reliable published articles over the last few years. Before developing the thematic taxonomy, the utmost frequently discussed issues in the related work are also considered. Figure 2 depicts a UWSN thematic taxonomy to help realize its features. It divides the vital elements into Communication, Architectural Elements, Security, Applications, Routing Protocols, and Standards. These characteristics are discussed in the sections that follow:

2.1. Architectural Elements. The underwater wireless sensor network architecture types are categorized based on the network's three-dimensional area of the applications and sensor nodes.

2.1.1. Sensors. Smart things in IoT networks, also known as sensor nodes in Wireless Sensor Networks (WSN), are required to sense configuration parameters on a regular basis, collect and route received data packets to the middle, similar to the mobile sink in WSN, for anomalous investigation and source persistence [6]. For maximizing the network abilities for data collection, the mobile node requires two transceivers. Remotely operated underwater vehicles (ROVs), autonomous underwater vehicles (AUVs), and sea gliders are examples of such vehicles. The third type of hybrid architecture consolidates mobile and static sensor nodes to carry out particular tasks. Mobile nodes can act as routers or controllers in a hybrid system to interact with static or basic data sensors. The sensor nodes in the dynamic architecture can move freely, allowing the network topology to change dynamically. Finally, ocean depth anchors are used in two-dimensional UWSN architecture to collect data from sensor devices.

Underwater sink-node can gather data from deep-sea sensors and transfer it to offshore base stations via surface channels. Underwater sinks are provided for this purpose, along with vertically and horizontally acoustic transmitters. Sensor nodes communicate with horizontal transceivers to collect data or provide instructions received by the offshore base station, whereas vertical transceivers send data to the base station. Through the use of various planned underwater sink nodes, a surface sink equipped with acoustic transceivers is capable of managing parallel communication [7]. The ocean floor is used to anchor sensor nodes in the architecture of underwater three-dimensional sensor networks. The depth of these sensor nodes is adjusted via wires attached to these anchors. However, the marine ecosystems' existing properties impact a significant obstacle to such a network.

2.1.2. Network Operations. The underwater sensor network operation goals are to maintain and enhance various functions, attributes, and specific requirements for improved functionality. As per recent publications, we conclude that the critical application development trends favour a greater emphasis on implementation and localization responsibilities that have made the foundation for UWSN architecture to improve full network functionality. As a result, this section contextualizes each job's strategies and features that enhance the network's performance.

(i) Localization

Localization methods have been extensively investigated in underwater sensor networks and are crucial for providing information about the location of sensor nodes in typical applications. We classified localization methods into three broad branches: mobile, hybrid, and stationary algorithms based on research articles. Classification is contingent upon sensor node movement in UWSNs. According to these categories, the majority of researchers concentrated on techniques for the localization of stationary nodes. For the static localization process, all sensor nodes are permanent and constant in the particular selected area, either tethered to sea floats or secured on the seafloor. The position of stationary nodes can be determined using a variety of methods. A recent approach [8] advocated using conventional ray equations to handle uncertainty in the anchor node position based on the rigidity theory. Some new research, such as [9], has supported that energy usage is reduced by minimizing the communication burden in the transmission process. To support near real-time decision making, an accurate border identification of continuous objects is an essential

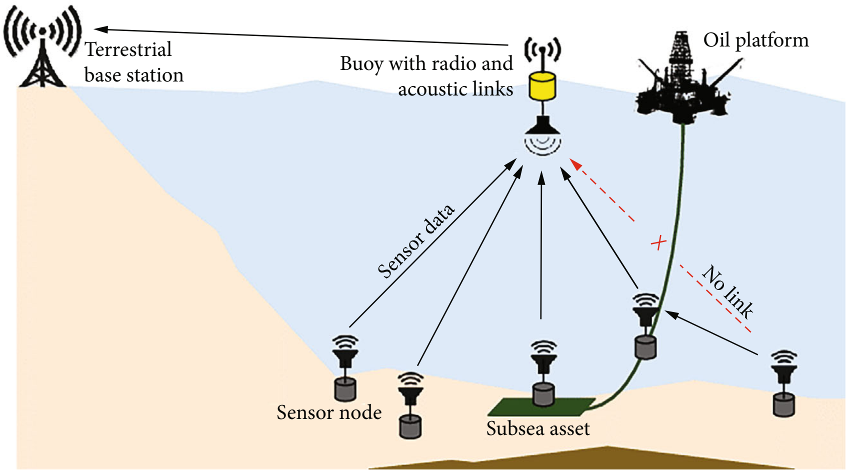

Figure 1: Environment of UWSNs.

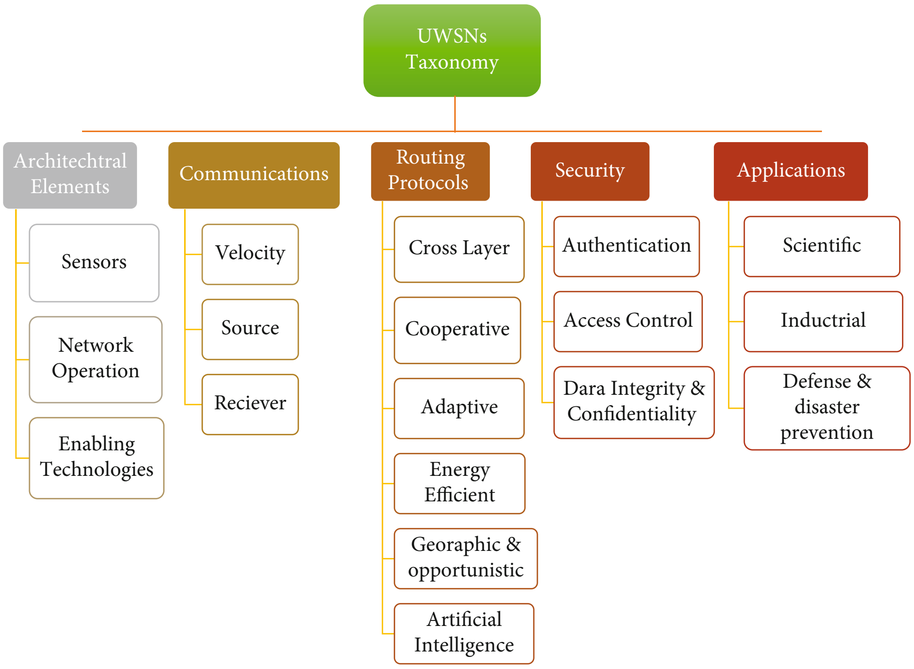

Figure 2: Underwater wireless sensor networks taxonomy.

research topic that relies on wireless sensor networks (WSNs) installed inside the geographical region to be monitored [10]. The researchers discovered that the unpredictability of sound speed made distance estimate for node identification less reliable.

(ii) Deployment

UWSNs are made up of hops placed underwater and nodes deployed on the water's surface, and they perform their jobs in specific locations. Underwater sensors that occupy a sparse area must be deployed optimally to make the best use of the low power consumption. Based on the ability to support different critical activities, such as localization, network topology, and routing protocol, which substantially affect net performance, node placement is a crucial step in underwater sensor networks. According to [11], there are three types of node deployment in UWSNs: limited mobility or self-adjusted, movement-assisted or accessible mobility, and static or fixed placement. All nodes are moored on the seafloor or affixed to surface buoys in a specific region of interest in the static node deployment. A disturbance in the sensor node area, according to [12], is an approach for achieving a final predicted configuration. To report their detection status, the nodes exchange control messages with each other and with the sink node. Nodes at the phenomenon boundary must be carefully selected for accurate tracking and detection [13]. After some network modifications have happened, such as node failure or target/event detection, reorganization or redeployment is required. The authors predicted that mobile sensor nodes would adjust their existing location actively to facilitate ultimate connectivity and stabilize the network coverage. Moreover, refs. [14] enhanced detection rates in mobile sensor nodes compared to the static and hybrid sensor nodes.

2.1.3. Enabling Technologies. In industry 4.0, this novelty has developed the driving force for deploying the Internet of Things industry (IIoT). Data from various sensor devices can be securely forwarded to the cloud network and updated regularly, thanks to IIoT. According to [15], IIoT combines IoT technologies and industrial wireless connections into a unified system comprising terminals, cloud networks, equipment, and machines. As a result, recent advancements in IoT and UWSNs have rekindled interest in the Internet of Underwater Things (IoUT). Aside from the greenhouse effect, underwater nodes and vehicles consume a lot of power, which can cause critical missions or applications to fail rashly. This problem prompted the authors in [16] to develop a new design based on energy efficiency for UWSNs, precisely discovering offshore oil and gas environments. In the coming years, communication in underwater systems will face some threats, including complex architectural design, integrating underwater vehicles or heterogeneous nodes, and various other underwater applications. SDN IIoT architecture incorporates 3 layers model [15]. Node data is transferred to the control layer from the physical layer via a southbound edge, and then through the northbound interface, data are transferred to the application layer. Relationships of SDN, IIoT, IoUT, and industry 4.0 among enabling technologies are shown in Figure 3.

2.2. Communication. Over the last half-century, there has been a substantial increase in acoustic study and development, mainly marine acoustics. Commercially, an auditory method is used to disclose ocean mammals and even submarines. The army sector is also similar to public acoustic communication, especially in ocean surveillance applications. As a result, this section covers the fundamentals of underwater acoustic communication, such as sources, receivers, and sound velocity properties. Furthermore, all aspects influence the sound speed and affect the network functioning or devices installed in the network.

2.2.1. Sound Velocity. The acoustic waveform in the sea is affected by sound velocity and the surrounding environment. Through actual investigation, [17] discovered that many main elements influence the excellent speed in water: salinity, temperature, and hydrostatic pressure. The following sections discuss the key points of these aspects.

(i) Temperature

The sound intensity and climate of the water are strongly associated when the water temperature rises. The velocity increases as well. When near the water's surface, the temperature increases, the sound velocity is also increasing.

(ii) Salinity

The salinity ratio is the second component that affects the sound velocity in water. However, as compared to temperature, salinity has a more negligible effect on sound speed. Sound speed is affected by the concentration of solidified salts in pure water. The ocean average level salinity is 35 Pascal. However, this figure fluctuates based on soil and qualities of water, atmosphere, and rock. Another aspect is affecting the level of salinity that they change with the depth of water.

(iii) Hydrostatic pressure

The sound speed of the water is also being affected by hydrostatic factors. Hydrostatic pressure enhances sound speed and depth [18]. This is because the increase in the center of the hydrostatic pressure is directly proportional.

(iv) Sound velocity profile

Based on ocean depth, the ocean is divided into two major zones. Each degree of profound results in distinctive sound velocity changes referred to as sound velocity profiles.

(v) Ocean depth below 200 m

The ocean consists of two main ocean-depth areas. Each depth causes various variations in sound speeds, known as sound velocity profiles. The top surface (0–100 m) is liable to wind, temperature, and environmental change. This layer can be mixed, and wind power converted into isothermic energy. The sound speed is significantly reduced when the wind is more than seven m/s because of the dominance of balloons at a distance of 10 m lower than the water's surface. The temperature varies seasonally in the seasonal thermocline region (100–200 m); the temperature decreases depending on the water depth. As a result, the thermocline is weak in winter, as the water surface is always excellent.

(vi) Ocean depth of more than 200 meters

The primary thermocline is located at depths of 200–100 m and has the lowest sound speed. The temperature of the water begins to rise at this depth. Temperature features in the deep isothermal layer are determined by water density and salinity. However, the temperature and salinity are considerably less significant than the hydrostatic pressure on sound velocity.

(vii) Ray bending

The amount of ray bending is determined by the difference in sound velocity, defined by salinity changes, pressure, and water temperature. The sound speed increases with depth in qualitative ray bending, paralleling the growing number of bubble populations. With improved routes at the sea surface, the number of bubbles reduces. A reflection occurs near the surface when acoustic energy concentrates within a layer. It does not transmit on all sides because it reduces the sound speed when the wave fronts propel toward the ocean depth. The SOFAR (Sound Fixing and Ranging) channel is named after this velocity profile.

(viii) Extended distance propagation

In the SOFAR channel geometry, attenuation and thermometry all impact sound reduction in signal-to-noise

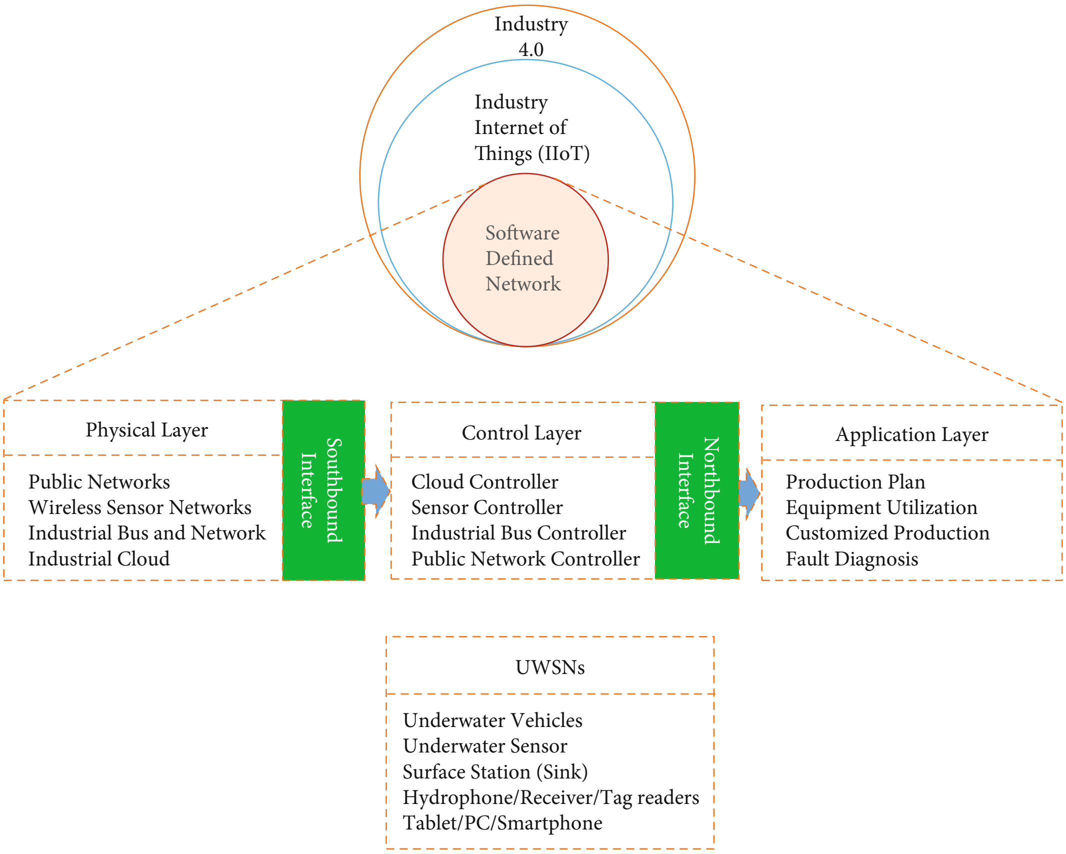

Figure 3: Relationship of IIoT, SDN, IoUT, and industry 4.0.

amplitude caused by long-distance transmission. However, the action on the SOFAR channel is slightly various. The rays do not bend spherically but instead spread in the form of a cylinder symmetry from a line source. The geometric spreading can decrease the power of acoustic waves as distance decreases based on inverse-square law.

Finally, noise, low variable speed, frequency-dependent absorption, and the architecture of communications in underwater networks are significantly affected. As a result of the considerable delays in spreading submarine transmission, spatial uncertainty and spatial unfairness also affect the networks [19]. As the reception time of the packet relies on the distance from the transmitter, the emitter first and then the receiver will be free.

(ix) Sea surface

There are varied proportions to the sound velocity parameters in various regions, such as at the frontier, bottom, and sea interface. Factors affecting the increase or decrease of sonority are the density and composition of rocks and trash in the sea bottom. Moreover, another factor influencing the sound speed is the bubble population near the surface of the sea. Average water density rises due to the presence of bubbles. As demonstrated in formulations and experiments, the speed of sound reduces the incidence of bubbles.

2.3. Routing Protocols. The routing protocol made a critical scheme challenge inside a network layer to identify and support network routes by providing different needs for acoustic communication. Several protocols to boost the network performance for underwater sensor networks have been developed and examined in the past and the present. The authors examined the previous study on UWSN routing protocols and identified that energy efficiency is the primary goal of most routing protocols (see Table 1—routing table). The main issue is to keep the limited amount of energy when using the UWSNs.

Underwater Acoustic communications use more energy than terrestrial radiofrequency. Static sink would suffer from battery power if the sensors located one hope away, potentially resulting in energy holes. In addition, it may result in preventing messages from reaching the sink node and network disconnectivity. In designing a routing protocol, the unique component of the underwater situation should be taken into account by using a time-varying channel. Most current studies on the network layer focused on minimizing latency while producing energy-efficient communication. But neglected to account for essential propagation factors such as bottom surface reflections, the Doppler effect and frequency-dependent attenuation, all of which, significantly impact energy consumption via rate and power.

Furthermore, modern routing protocols stress the usage of opportunistic routing, adaptive routing, cooperative,

Table 1: Shows the current routing protocols based on its features.

Protocols	Concentration points	Sink (multiple/ single)	Mobility	Multihop	Location known	Void avoidance
BLOAD [20]	Balanced energy consumption, energy holes avoidance	Single	Yes	No	Yes	No
EMGGR [21]	Void avoidance, reliability	Single	Yes	Yes	Yes	Yes
ECBCCP [22]	Reliability, energy conservation	Multiple	Yes	Yes	Yes	No
EULC [23]	Balanced energy dissipation, improved network lifetime, hot spot mitigation	Single	Yes	Yes	Yes	Yes
iAMCTD [24]	Packet delivery ratio, energy efficiency	Multiple	Yes	No	No	No
SACRP [25]	Packet delivery ratio, energy efficiency, clustering	Single	No	Yes	Yes	No
QL-EEBDG [26]	Packet delivery ratio, energy efficiency, clustering	Multiple	Yes	No	Yes	No
EnOR [27]	Packet delivery ratio, energy efficiency, improved network lifetime	Single	No	Yes	Yes	No
EECAR-AC [28]	Network lifetime, void avoidance	Multiple	Yes	Yes	Yes	Yes
QERP [29]	End-to-end delay, improve network energy consumption, and packet delivery ratio (PDR)	Single	Yes	No	Yes	Yes
EEDC-AA [30]	Prolong underwater network lifetime, and balance energy consumption	Multiple	Yes	No	Yes	No
JREM [31]	Energy holes and balancing energy consumption, and increase network lifetime by avoiding	Single	No	Yes	Yes	Yes
PCR [32]	Energy efficient data, opportunistic routing, and reliability	Multiple	No	Yes	Yes	Yes
EBOR [33]	Network lifetime, reliability, PDR, energy consumption	Multiple	No	Yes	Yes	No
RBCRP [34]	Reduce outage probability, load balancing	Multiple	Yes	Yes	Yes	No
CSQSR [35]	Network lifetime, application-specific QoS	N/A	No	No	Yes	No
AREP [36]	Link asymmetry, void handling	Single	Yes	No	Yes	Yes
VA-GMPR [37]	Void avoidance, load balancing, reliability	Single	Yes	Yes	Yes	Yes
P-AUV [38]	Low latency, energy efficiency	Multiple	Yes	Yes	Yes	No
RPO [39]	Reliability, energy efficiency	Multiple	No	N/A	Yes	N/A

artificial intelligence-related, and cross-layer routing protocols to meet the various requirements of UWSNs. The underwater environment is, by definition, unreliable and scant and hostile. As a result, these inconsistent states uncover UWSNs to the natural division caused by sensor mobility, decreasing the accuracy of data transmission from sender to receiver. As a result, routing protocol designs and approaches are necessary to address these difficulties.

2.4. Security. UWSN sensor nodes are often infrequently installed in harsh and dangerous conditions. As a result, they are susceptible to network attacks. One of the most important factors of UWSNs is security to ensure that an application smoothly functions and generates secure data. Internal and external attacks have been made against UWSNs due to their characteristics (e.g., limited bandwidth, high propagation latency, computational capability limitations, and high bit error rates).

2.4.1. Authentication. As previously stated, the acoustic channel is open; further, without encryption, a malicious attacker can readily grab manipulate their content. As a result, to filter malicious attacks, the receiving node must identify the data source, services, and channels, to access and share the applications and data on that network, nodes must be authorized. A trust management system and intrusion detection can be used to recognize aberrant behaviour and remove rogue nodes from the web. These procedures confirm that only verify nodes have access to the system's resources [40]. During transmission, all of the nodes connected with the network must have the authorization or permission of the network services. After the competition of the authentication process, the devices will be ready to carry out any duties that have been allocated to them using the encoded procedures. As a result, in UWSN, the implementation of a robust authentication technique is critical.

2.4.2. Access Control. The data access limitation is used in the access control process to protect the data (front–end and back end), resources, and services of underwater sensor networks. Intelligent devices or adaptive methods can help avoid or reduce the risk of malicious nodes and unauthorized data vulnerability. The two kinds of access methods are present: distributed and centralized. To permit a connection, all control access inquiries must process through the server in a centralized approach. However, with the distributed control access technique, an entity is designated by the access control server to authorize access to UWSN resources. Services that are used by the system should always be present in the system to reduce any communication problems in UWSNs.

2.4.3. Confidentiality and Data Integrity. In addition, integrity is a critical security requirement. During data transmission, each node must maintain the confidentiality of the data. The packet's header must also be encrypted in some security techniques to protect each node's identity. The node can ensure that the messages must be newly generated, and information that is already stored from previous broadcasts is not received or transferred by utilizing the difference time approach. If a node has older communicated data, then the mentioned node cannot refuse the completed transmission. Nonrepudiation is the legal term for this process.

More work is undertaken to discover the existing techniques of attacks. According to the researchers, the invasion in UWSNs happened through data transfer in physical node attacks, denial of service (DoS), and impersonation and replication. According to [41], DoS attacks are common in UWSNs due to their challenges, low operational costs, and high effectiveness. [42, 43] have conducted a more profound study of DoS attacks on the physical layer. They put the results to the test in a real-world environment. A data assault is another common security concern with UWSNs. One way for protecting data from DoS assaults is data management utilizing information-centric architecture. Attacks from innovative DoS types are still capable of damaging the data. As a result, ref. [44] detected different types of mobile attackers by the use of machine learning in information-centric architecture.

According to prior investigations, security challenges in underwater sensor networks are focused primarily on routing, data aggregation, localization, and intrusion detection models. Five methods, including the secure localization and trust model, are proposed in the evaluation process [45]. The authors in [46] refined the implementation of the mentioned trust model by establishing a single point of trust management in underwater sensor networks by utilizing a cloud paradigm. The mentioned management methodology aims to govern each sensor node's trustworthiness using a mathematical technique to gather trust proof.

Multiple experiments are conducted in [47] and discovered that the effective encryption technique could maintain the integrity and secrecy of the data. Furthermore, the method has the potential to decrease communication overhead on the upper layer. The authors in [48] developed a crucial model to generate more helpful hash bits for underwater sensor networks secure acoustic communications.

2.5. Applications. The technology used in underwater wireless sensor networks can replace conventional methods by remote control of underwater appliances and onshore systems, advanced data recording devices, and real-time monitoring. Underwater wireless sensor network applications are typically classified into three branches: commercial, military and security, and scientific (see Figure 4). Sensor devices are utilized in the military to sense the enemy's activity and position. It can be used to monitor ports and harbors, detect enemy submarines, identify underwater mine locations, and conduct border surveillance. In addition, sensor nodes can see marine environments in advance of natural disasters by performing seismic monitoring.

2.5.1. Scientific. UWSNs have diverse applications in science, including ocean sampling, environmental monitoring, and most importantly, Great Barrier Reef activities. For example, the ecological monitoring application is used to track the amount of trash, both biological and chemical, accumulated on the sea-bed [8]. Furthermore, in [49], a robotic model

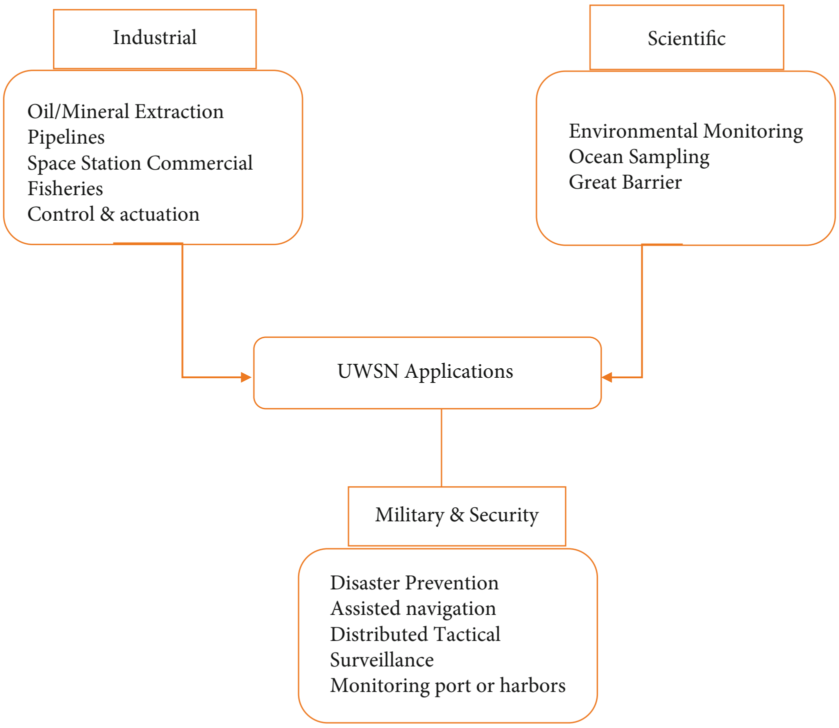

Figure 4: Application of UWSNs.

was used to evaluate the level of oxygen in the water and track temperature and pressure [50]. The authors in [51] present a coral reefs application that integrates big data, IoT, and sensor networks to assess the impact of humidity, pressure, ocean temperature, marine ecosystems, and salinity on coral bleaching. Deep maritime conditional surveillance can also be accomplished by using a variety of agents and communication methods.

2.5.2. Commercial. UWSN industrial applications have an important effect on commercial activity facilitation. Underwater sensor network monitors applications such as underwater gas and oil pipeline monitoring. The researchers in [52] have been developed a model for underwater tracking of gas and oil pipelines. The network was created to provide facts on the health of channels that are linked across large environments. Additionally, [53] developed a monitoring system for underwater gas and oil pipelines, including the desired components requiring control.

One of the most labour-intensive industries that help in a healthy economy is referred to as fish farming. Moreover, it necessitates a rigorous monitoring system to assess the fish's environmental conditions. In [54] proposed a Zigbee-based underwater sensor network observation system for big fish farms that can be accessed through remote control for interested users. Additionally, the system can monitor fish farms based on pH values, water level, humidity temperature, and dissolved oxygen. Further, wireless cameras are interconnected with the design and the Internet to enable remote monitoring from any location in the world. Additionally, the researchers of [55] built a comparable commercial fishery monitoring system that communicates via acoustic waves.

2.5.3. Disaster Prevention and Defense Application. Underwater sensor networks are used for military and defense applications to detect possible enemies before ports and port surveillance and control in [56]. Sea mines discovery in [57], border protection against illegal fighting ships in [58]. In addition, underwater sensors network advanced technologies such as the mobile UWSNs provide warning alerts prior to the natural disasters, such as seismic and seafloor activities [59].

The network settings are classified by the characteristics of the application, the region, the network's size and frequency of communication, the distance among hops, the sensor types, and the total number of sensor devices. In general, the overall communication among the hops is accomplished through acoustic waves or a combination of radiofrequency and acoustic signals. Therefore, it is difficult to detect and prevent a malicious node disguised as a valid user from disturbing the network. Even worse, internal threats may be initiated by hacked nodes that were previously correct.

The network settings are classified by the characteristics of the application, the region, the network's size and frequency of communication, the distance among hops, the sensor types, and the total number of sensor devices. In general, the overall communication among the hops is accomplished through acoustic waves or a combination of radiofrequency and acoustic signals. Therefore, it is difficult to detect and prevent a malicious node disguised as a valid user from disturbing the network. Even worse, internal threats may be initiated by hacked nodes that were previously correct.

3. Security Threats and Attacks

Many limitations exist in underwater acoustic channels and UWSNs, causing potential security risks. As a result, UWSNs are subject to a variety of risks, including malicious attacks. These challenges and attacks were thoroughly examined and evaluated in this work. These attacks can be passive or active, depending on the behaviour of the malicious attacker. As illustrated in Figure 5, these challenges and attacks are classified broadly into active and passive attacks.

3.1. Passive Attacks. Passive attacks are attempts performed by effected devices to detect the activities and gather data transferred in the network without interfering with its functioning, such as interference, eavesdropping, impersonation, message distortion, message replay, and secret information leakage. The acoustic channels are open channels and easily come under attack.

Using a hydrophone or underwater microphone, malicious attackers can capture packets transmitted in the data channel. Furthermore, the attacker can determine the nature of communication by evaluating packet flow, detecting packet exchange, identifying the data transferring hosts, and determining the position of nodes. Unfortunately, it is challenging to determine the mentioned attacks because the network functionality is unaffected. So, the efficient solution is to use encryption technologies that make it difficult for eavesdroppers to obtain any information. Unfortunately, the current encryption algorithms used in wireless networks cannot be immediately translated into UWSNs due to the high energy consumption and massive overhead. The encryption techniques utilized by UWSNs will be discussed in further detail in the following sections.

3.1.1. Eavesdropping. Additionally, eavesdropping is referred to as "passive information collecting." Eavesdropping on confidential data is possible through the tapping of communication cables. As a result, wireless networks are much more vulnerable to passive attacks than wireless connections. Because UWSNs use short-range transmissions, an attacker must be nearby to eavesdrop on important information, making UWSNs less vulnerable to tapping than lengthy wireless communication technologies. Interception of messages transmitted by UWSNs may expose valuable information such as gateways, the physical location of specific nodes, key distribution centers, timestamps, message identifiers (IDs), and other fields, even nearly everything that was not secured. Using a mathematical model that takes underwater acoustic channel characteristics, including ambient noise and signal attenuation in [60], the authors looked into the possibility of eavesdropping attempts. Underwater acoustic signal channels are shown to be related to an intercept's success condition. According to the authors, both isotropic and array eavesdroppers are considered when calculating the eavesdropping probability. To make matters even more complicated, node density and wind speed all impact the probability of a collision.

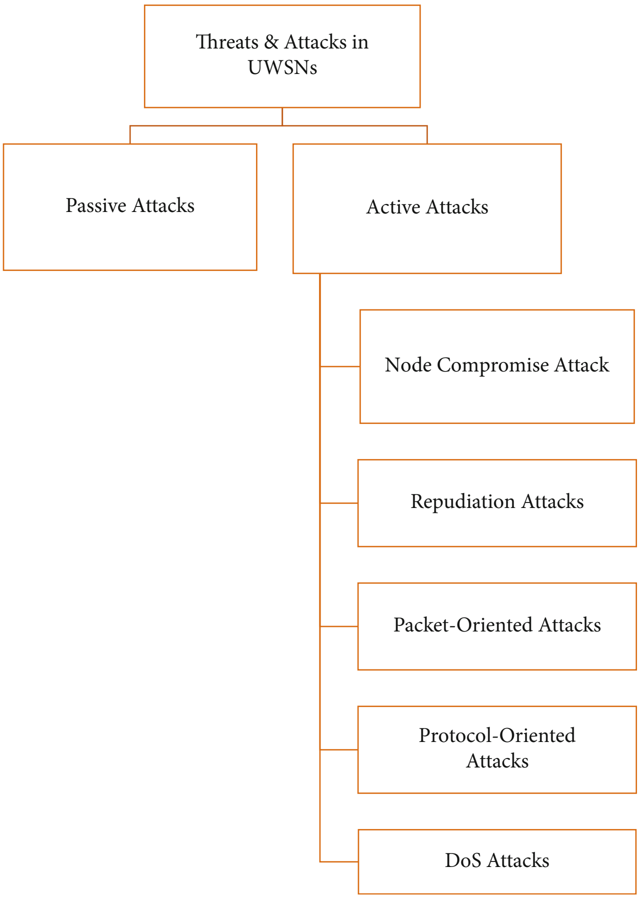

Figure 5: Security threats and attacks.

3.1.2. Node Malfunctioning. It can occur for many reasons, including defective sensors or energy depletion due to sensor overloading or other denial-of-service attacks.

3.1.3. Node Destruction. Physically destroying a node (by using an electrical surge, physical force, or gunfire) in any way possible so that the node is rendered inoperable.

3.1.4. Traffic Analysis. For attackers, the traffic pattern of a network may be as helpful as the substance of data packets. By examining traffic patterns, sensitive data about the networking infrastructure can be gleaned. In UWSNs, the nodes closest to the access point, i.e., the sink, transmit more packets than the other nodes because they relay more packets. Similarly, clustering is a critical component of UWSN stability.

3.1.5. Node Outage. Such a threat happens if a node's standard functionality is compromised. For instance, if a central node in a heterogeneous network fails to operate normally, the WSN protocols must be robust enough to offset the negative consequences of such node outages by choosing new cluster heads and offering alternate network channels.

3.2. Active Attacks. Active attacks aim to inject, change, destroy, or delete data carried over a network. Active cyberattacks may capture network data and attempt to alter or destroy packets to disturb network communication and operation. Both internal and external attackers can carry out active attacks if the attacks are conducted out by hops that are not part of the network, and they are classified as external attacks, which are capable of finding and protecting. If an attempt is launched from an insider node, it is classified as an inside threat, which can cause significant harm to the network. According to the results of the prior research, interior attacks are harder to trace and may cause more danger than outside ones. The possible answer to this problem is to use security techniques such as encryption, trust management, and authentication.

3.3. Attacks Occur on Physical Layer

3.3.1. Node Capture. An attacker seizes control of the sensor node using a physical attack, such as connecting wires to its circuit board and accessing both stored data and continuous communication in the UWSN [61]. Capturing a node may disclose vital data, most notably cryptographic keys, compromising the entire UWSN. Additionally, attackers can tamper with the actual wiring of the electronic board or the content of the nodes' memory, allowing them to utilize the seized slave node in any way they like. Two issues occur in this instance:

(i) The hijacked node can make unlimited requests on behalf of the attacker

(ii) Hijacked nodes may offer erroneous information to genuine users

3.3.2. Jamming DoS. According to [62], a hostile machine may lead to jam its transmission in case of sending information with same frequency. The jamming signal adds to the carrier's noise. Its intensity is sufficient to drop the SNR below the threshold required for the nodes utilizing that channel to receive data effectively. Constant jamming can be carried out in a region, effectively preventing all nodes in that zone from communicating. However, temporary jamming using random time intervals can be used to disrupt signals successfully. There are a limited number of antijamming devices available for UWSNs that can be used to defend against WSN jamming attacks. Acoustic communication underwater frequently makes use of spread-spectrum techniques. Frequency-hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS) are two of these approaches gaining popularity because of their superior performance in noisy environments and dealing with multipath interference. FHSS and DSSS approaches can withstand interference from jammers to a certain extent. If FHSS is employed, the jamming attacker will still jam a large portion of the spectrum. Even worse, a powerful jamming signal can compromise the DSSS system.

3.4. Attacks Occur on Data Link Layer. Algorithms at the data link layer, particularly MAC address techniques, provide numerous options for exploitation. For example, continuous channel jamming via DoS assaults or more complicated cases depending on MAC layer addressing techniques. Collision, Dos, weariness, spoofing, desynchronization, link-layer jamming, flooding, and unfairness are all examples of data link layer attacks.

3.4.1. Denial of Sleep (Sleep Deprivation Torture). A denial of sleep attack will result in energy depletion for battery-powered devices [63]. This attack can be carried out by collision threats or repetitive handshaking, which involves repeatedly manipulating the clear to send (CTS) and request to send (RTS) flow control signals, thereby preventing the node from entering the sleep state.

3.4.2. Collision. During this type of attack, an attacker communicates on the same frequency as a legitimate network node. As a result, the two broadcasts collide, rendering the data received unintelligible to the recipient. At some point, the receiver will request retransmission of the same packet [64]. A single byte of a message colliding would result in a CRC (cyclic redundancy check) error, rendering the entire message unusable. This assault is more advantageous for an attacker than jamming, as it consumes less transmission energy and has a lower risk of detection [65]. A colluding collision attack can be mitigated via a mitigating colluding collision strategy. The error-correcting code, in a sense, is a practical method of preventing collisions.

3.4.3. Jamming Attack. A datalink layer jamming attack is similar to a physical layer jamming attack, but it is more intelligent and effective. The potential hacker can accomplish this purpose by sending a request to send (RTS) packets continuously. The valid nodes are denied access to the channel. The potential hacker can assign the highest priority to himself and constantly utilize the medium regarding MAC protocols. As a result, scheduled MAC protocols can protect against the exploit. These attacks can be mitigated with antireplay prevention and link-layer verification. Consequently, receiving a significant number of RTS packets costs energy and utilizes channels on a node [66].

3.4.4. Exhaustion Attack. This type of attack can be used to keep the communication line busy and drain the device's energy by hosting a malicious node into the network. It can be triggered by the attacker or by a hijacked node with the attacker's internal program code. Another type of exhaustion attack is when the hijacked node sends RTS/CTS messages or requests to join to push the receiver node to transmit and receive. A strategy proposed by [58] is based on fuzzy logic for defending against dispersed node exhaustion attacks. Rate limiting on each node of the network is a reasonable solution. [58] proposes a fuzzy logic-based antidistributed-node-exhaustion solution.

3.4.5. Unfairness. It is a weak type of DoS attempt in which the attacker decreases the network's performance rather than entirely blocking authorized sensor nodes from using the communication channel. A minor frames method is utilized to cut down on time. It is vulnerable to further disparity. An attacker, for example, may resend at a faster rate instead of just randomly stopping [67]. Most of the DoS attacks on the data link layer listed above can be mitigated by utilizing error detection code, limiting transmission speed, and splitting packets into short frames. To lower the amount of time required, consider using a small frames approach. Utilizing this strategy results in a smaller impact at the sacrifice of effectiveness. In addition, it is open to future exploitation. Instead of randomly delaying, an attacker might retransmit at a higher speed.

Most datalink layer denial-of-service attacks described above can be mitigated using rate limiter, error detection code, and packet slicing.

3.5. Network Layer Attacks. Routing the packets from source to destination is the main task of the network layer. Due to the particular features, the network layer is subject to various threats and attacks that disrupt the network's routing, including selective forwarding, replay, misdirection, neglect and greed, sinkhole, Sybil, wormhole, blackhole/gray hole, homing, and hello flooding attacks.

3.5.1. Selective Forwarding Attack. There is a possibility that the adjacent node will locate different routes to the destination node. As a result, to avoid detection, it intentionally transmits and drops specific packets. The attacker who is focused on overwhelming and changing a packet created from a few source nodes can effectively transfer the rest packets while minimizing suspicion of misbehaviour [68].

Evidential assessment is used in [69] to discover node capture attacks that employ the Dempster–Shafer theory of integrated numerous facts. These attacks can be detected and isolated from the network using trust management and reputation methods based on behaviour evaluation [46].

3.5.2. Misdirection Attack. In this type of attack, the attacker redirects packets to invalid paths, modifies the routes, or redirects the packets to a hijacked node. This attack can be mitigated by changing the route path, including the source route in each packet.

3.5.3. Greed and Neglect. This type of attack is a variation of the selective forwarding threat. The attacker may drop incoming packets at random while still acknowledging the source node or giving high precedence to its packets [70, 71]. Declaring alternate routing paths is a feasible solution to this type of attack by sending repeated messages. But in conversation, more power would be required, and UWSNs would face the most serious energy shortage.

3.5.4. Gray Hole/Black Hole Attack. In this type of attack, the attacker broadcasts fake routing information with the shortest path or lowest cost toward the receiver. The hijacked nodes would choose this path as the best option, even though it passes over the adversary computer. Furthermore, the adversary can evaluate, change, or even destroy packets at will. A black hole attack occurs when the attacker drops all data packets. If the attacker removes some crucial packets, then it is called a gray hole attack.

This form of attack damages those sensor nodes located a long distance away from the sink node. In a more sophisticated manner, the adversary may drop necessary packets at a specific period or a specified percentage, proving it more challenging to detect.

3.5.5. Sybil Attack. An attacker can use the Sybil attack to create many identities and appear in multiple locations simultaneously. The primary purpose of these fake identities is to prevent the information transmission operation from taking place. These numerous identities can be taken by inventing defects or hijacking legitimate node IDs. As a result, the Sybil attack can severely harm distance-based or location-based routing schemes. Furthermore, the attacker can act as a base station or recipient, sending acknowledgment packets to sensor nodes to prevent retransmission. In [72, 73], the researchers provided a lightweight and robust scheme based on the received signal strength indicator for detecting the Sybil attacks. Also, the authors in [74] designed the random key predistribution method for protecting the Sybil attacks.

3.5.6. Homing Attack. A potential hacker may monitor the traffic in a homing attack to identify and target nodes with individual responsibility, such as sinkhole nodes or cluster heads. Furthermore, the attacker may execute additional DoS operations to block or disable these specific nodes. The use of "dummy packets" in an antitraffic analysis method helps hide the location of the base station from observers [75]. It is unfortunate that these dummy packets use up a lot of nodes' energy, particularly for UWSNs. As a result, it should only be utilized when preventing traffic analysis is absolutely necessary.

3.6. Attacks on Transport Layer. The UWSN transport layer has the responsibility for source to destination reliable communication of data. This layer of common attacks contains the synchronization flooding attack and desynchronization attack.

3.6.1. Synchronization Flooding Attack. An intruder may create new user request indefinitely until the resources required by each connection are consumed or reach the highest limit. A popular type of DoS attack includes delivering a large number of common packets, such as internet control message protocol (ICMP), transmission control protocol (TCP), and user datagram protocol (UDP), all intended at the exact location. Because of the large data flood created by these packets, the network can no longer differentiate between authentic and fraudulent traffic in [76].

3.6.2. Desynchronization Attack. A desynchronization attack occurs when a malicious user disrupts existing connections between nodes by sending faked packets with faked sequence numbers or control signals that desynchronize destinations. Synchronization is critical and challenging for UWSNs; additionally, the global positioning system (GPS) is ineffective [77].

4. Open Issues and Challenges

UWSNs have a wide range of uses, including civic, military, and a variety of others. UWSN research and implementation have been increasingly popular in both academia and industry. Following a study of existing developments and investigations, various problems remain to be explored to progress further.

4.1. Reliability. In order to ensure reliability in all aspects, such as hop-by-hop, data, and end-to-end reliability, reliability is essential. The ability to successfully convey and transfer data between participating sensor nodes in the UWSNs is critical to its stability. Reliability ensures that packets are delivered successfully between sensor nodes involved in joint operations [78]. Therefore, proposing a cooperation method that takes this reliability into account and solves it.

4.2. Propagation Delay. The MAC or retransmission timeout (RTO) waiting time directly impacts throughput. The authors of [79] discovered that the current fixed RTO is not efficient. Furthermore, because of the lengthy propagation delay in UWSNs, a handshaking method that enables all nodes to share a channel costs a lot more than in a terrestrial sensor network. It will gradually result in high handshaking overheads, resulting in a limited bandwidth.

4.3. Variance Delay. Variance delay is a factor that leads to erroneous round-trip time (RTT) estimates and makes measuring the waiting time in the MAC protocol challenges. However, according to [80], most MAC protocol studies did not account for the variable delay in their findings.

4.4. Mobility of Nodes. While nodes in terrestrial networks are likely to remain static, underwater vertices will certainly wander due to underwater shipping activity, currents, winds, and other factors. Because the oceanic current is spatially dependent, nodes may drift in different directions. While GPS updates can pinpoint reference nodes tied to surface buoys, maintaining submerged underwater nodes at precise positions is problematic. It may have an impact on the accuracy of the localization.

4.5. Efficiency. Efficiency is essential for providing a cooperative mechanism and making communication easier between nodes in a communication network. Underwater localization collaborative control tasks necessitate a reliable means for transferring and receiving data. In order to use resources that enable efficient delivery of information, cooperative gaming strategies must include efficiency; otherwise, the cost of such information distribution will rise, i.e., delays and throughput will grow.

4.6. Privacy and Security. The authors of [81] explained how security assaults might affect underwater localization and countermeasures and how privacy is affected. For the sensor node to be localized, it must show specific information, leading to privacy gaps. When gathering location-related information, location privacy is a topic that is discussed. DoS attacks, range-based assaults, no range estimation attacks, noncooperation, and deceptive advertising information are some examples of these types of attacks.

4.7. Communication Range. In the underwater environment, a signal's absorption depends on the water's depth, one of the distinctive characteristics. Signal absorption can be minimized by lowering the frequency. Even nevertheless, when the transmission range expands, new issues arise regarding interruption probability and high data collision rates.

4.8. Hardware Dependent. Sensor nodes in the water, such as autonomous underwater vehicles (AUVs), wheels, or unscrewed aircraft, use battery power and are difficult to change once in place. As a result, customizing another system is difficult because different applications have distinct data formats, protocols, and service constraints.

4.9. Reliability of Link. High delivery rates in real-time scenarios require good link reliability as well. The sensor nodes in the network's link dependability factor might affect the delivery rates and, as a result, the transmission loss, which lowers the aggregated strength of the waveform's propagation from sender to the receiver. Data transmission reliability can be harmed by noise in the underwater environment, resulting in dropped transmissions. If the link is unreliable, continuous transmission of data will increase node energy consumption and bandwidth utilization. Data transmission efficiency must be taken into account to prevent using unreliable connections.

5. Conclusion and Future Directions

Wireless sensor networks are a great area nowadays for researchers. As advancements are made in technology, this field is also growing faster than other fields. As the nature of the network, it broadcast the signals in an open environment. Underwater Wireless Sensor Networks is one of the branches of this network that operates underwater to monitor the marine environment and collect data for different purposes. This study first investigated the Underwater Wireless Sensor Network taxonomy from the latest research articles and well-known databases. This paper also indicates and analyses the current security threats for Underwater Wireless Sensor Networks on each layer. UWSNs have come a long way in recent years, but there is still more to be done, especially when it comes to building large-scale systems. There is room for improvement in a future study on node mobility with high monitoring area to explore the impact on the network connection, energy consumption, network longevity, and coverage resulting from these findings. Studies should focus on creating cooperative control among a few underwater vehicles to raise the efficiencies of UWSNs and improve their performance. Future research should improve the cars' ability to communicate cooperatively by increasing the channel capacity and autonomy level. Future studies could look at environmental factors and underwater vehicle designs simultaneously, extending the algorithm's usefulness. A high-level planning layer follows this that the researchers construct to specify the ideal vehicle configurations or strategic regions of interest for the vehicle to investigate. Complex network scenarios such as mobility, multipath fading, and shadowing could potentially be addressed in the research.

Data Availability

Data will be available upon request from the corresponding author.

Conflicts of Interest

The authors declare no conflict of interest.

References

[1] X. Xiao, H. Huang, and W. Wang, "Underwater wireless sensor networks: an energy-efficient clustering routing protocol based on data fusion and genetic algorithms," *Applied Sciences*, vol. 11, no. 1, p. 312, 2021.

[2] R. Mhemed, F. Comeau, W. Phillips, and N. Aslam, "Void avoidance opportunistic routing protocol for underwater wireless sensor networks," *Sensors*, vol. 21, no. 6, p. 1942, 2021.

[3] S. Khisa and S. Moh, "Survey on recent advancements in energy-efficient routing protocols for underwater wireless sensor networks," *IEEE Access*, vol. 9, pp. 55045–55062, 2021.

[4] J. Xiang, Z. Zhou, L. Shu, T. Rahman, and Q. Wang, "A mechanism filling sensing holes for detecting the boundary of continuous objects in hybrid sparse wireless sensor networks," *IEEE Access*, vol. 5, pp. 7922–7935, 2017.

[5] D. Zhao, G. Lun, R. Xue, and Y. Sun, "Cross-layer-aided opportunistic routing for sparse underwater wireless sensor networks," *Sensors*, vol. 21, no. 9, p. 3205, 2021.

[6] X. Du, Z. Zhou, Y. Zhang, and T. Rahman, "Energy-efficient sensory data gathering based on compressed sensing in IoT networks," *Journal of Cloud Computing*, vol. 9, pp. 1–16, 2020.

[7] D. B. Kilfoyle and A. B. Baggeroer, "The state of the art in underwater acoustic telemetry," *IEEE Journal of Oceanic Engineering*, vol. 25, no. 1, pp. 4–27, 2000.

[8] M. Stojanovic, "Acoustic (underwater) communications," in *Encyclopedia of Telecommunications*, Wiley, Hoboken, NJ, USA, 2019.

[9] K. M. Awan, P. A. Shah, K. Iqbal, S. Gillani, W. Ahmad, and Y. Nam, "Underwater wireless sensor networks: a review of recent issues and challenges," *Wireless Communications and Mobile Computing*, vol. 2019, Article ID 6470359, 20 pages, 2019.

[10] H. Ping, Z. Zhou, T. Rahman, and Y. Duan, "Localization and tracking of continuous objects boundary area leveraging planarization algorithms in duty-cycled wireless sensor networks," in *43rd Annual Conference of the IEEE Industrial Electronics Society*, Beijing, China, 2017.

[11] G. Han, C. Zhang, L. Shu, N. Sun, and Q. Li, "A survey on deployment algorithms in underwater acoustic sensor networks," *International Journal of Distributed Sensor Networks*, vol. 9, no. 12, Article ID 314049, 2013.

[12] J. Vilela, Z. Kashino, R. Ly, G. Nejat, and B. A. Benhabib, "A dynamic approach to sensor network deployment for mobile-target detection in unstructured, expanding search areas," *IEEE Sensors Journal*, vol. 16, no. 11, pp. 4405–4417, 2016.

[13] T. Rahman, Z. Zhou, and H. Ning, "Energy efficient and accurate tracking and detection of continuous objects in wireless sensor networks," in *IEEE International Conference on Smart Internet of Things (SmartIoT)*, Xi'an, China, 2018.

[14] B. Wang, *Coverage Control in Sensor Networks*, Springer Science & Business Media, Berlin, Germany, 2010.

[15] J. Wan, S. Tang, Z. Shu, S. W. Di Li, M. Imran, and A. V. Vasilakos, "Software-defined industrial internet of things in the context of industry 4.0," *IEEE Sensors Journal*, vol. 16, pp. 7373–7380, 2016.

[16] R. W. Coutinho, A. Boukerche, L. F. Vieira, and A. A. Loureiro, "On the design of green protocols for underwater sensor networks," *IEEE Communications Magazine*, vol. 54, no. 10, pp. 67–73, 2016.

[17] T. G. Leighton, *The Acoustic Bubble*, vol. 96, no. 4, 1994, Academic Press, London, UK, 1994.

[18] Y. Yang, W. Zhao, and X. Xiao, "The upper temperature limit of life under high hydrostatic pressure in the deep biosphere," in *Deep Sea Research Part I*, vol. 176, Oceanographic Research Papers, 2021.

[19] A. A. Syed, W. Ye, J. Heidemann, and B. Krishnamachari, "Understanding spatio-temporal uncertainty in medium access with ALOHA protocols," in *Proceedings of the Second Workshop on Underwater Networks*, pp. 41–48, Montréal, QC, Canada, September 2007.

[20] I. Azam, N. Javaid, A. Ahmad, W. Abdul, A. Almogren, and A. Alamri, "Balanced load distribution with energy hole avoidance in underwater WSNs," *IEEE Access*, vol. 5, pp. 15206–15221, 2017.

[21] F. Al Salti, N. Alzeidi, and B. R. Arafeh, "EMGGR: an energy-efficient multipath grid-based geographic routing protocol for underwater wireless sensor networks," *Wireless Networks*, vol. 23, no. 4, pp. 1301–1314, 2017.

[22] S. Rani, S. H. Ahmed, J. Malhotra, and R. Talwar, "Energy efficient chain based routing protocol for underwater wireless sensor networks," *Journal of Network and Computer Applications*, vol. 92, pp. 42–50, 2017.

[23] R. Hou, L. He, S. Hu, and J. Luo, "Energy-balanced unequal layering clustering in underwater acoustic sensor networks," *IEEE Access*, vol. 6, pp. 39685–39691, 2018.

[24] N. Javaid, M. R. Jafri, Z. A. Khan, U. Qasim, T. A. Alghamdi, and M. Ali, "IAMCTD: improved adaptive mobility of courier nodes in threshold-optimized dbr protocol for underwater wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 10, no. 11, 2014.

[25] Y. D. Chen, D. R. Wu, W. Chen, and K. P. Shih, "A self-adaptive cooperative routing protocol for underwater acoustic sensor networks," in *Proceedings of the OCEANS'15 MTS/IEEE Washington*, pp. 1–5, Washington, DC, USA, October 2015.

[26] Z. Jin, Y. Ma, Y. Su, S. Li, and X. Fu, "A Q-learning-based delay-aware routing algorithm to extend the lifetime of underwater sensor networks," *Sensors*, vol. 17, no. 7, p. 1660, 2017.

[27] R. W. Coutinho, A. Boukerche, L. F. Vieira, and A. A. Loureiro, "EnOR: energy balancing routing protocol for underwater sensor networks," in *Proceedings of the IEEE International Conference on Communications (ICC)*, pp. 1–6, Paris, France, May 2017.

[28] M. R. Bharamagoudra, S. S. Manvi, and B. Gonen, "Event driven energy depth and channel aware routing for underwater acoustic sensor networks: agent oriented clustering based approach," *Computers and Electrical Engineering*, vol. 58, pp. 1–19, 2017.

[29] F. Muhammad, G. Tuna, and V. C. Gungor, "QERP: quality-of-service (QoS) aware evolutionary routing protocol for underwater wireless sensor networks," *IEEE Systems Journal*, vol. 12, pp. 2066–2073, 2018.

[30] Y. Jing, X. Yang, X. Luo, and C. Chen, "Energy-efficient data collection over AUV-assisted underwater acoustic sensor network," *IEEE Systems Journal*, vol. 99, pp. 1–12, 2018.

[31] B. Fatma, C. Zidi, and R. Boutaba, "Joint routing and energy management in underwater acoustic sensor networks," *IEEE Transactions on Network and Service Management*, vol. 14, no. 2, pp. 456–471, 2017.

[32] R. W. L. Coutinho, A. Boukerche, and A. A. F. Loureiro, "PCR: a power control-based opportunistic routing for underwater sensor networks," in *Proceedings of the 21st ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, pp. 173–180, Montreal, QC, Canada, November 2018.

[33] Z. Jin, Z. Ji, and Y. Su, "An evidence theory based opportunistic routing protocol for underwater acoustic sensor networks," *IEEE Access*, vol. 6, pp. 71038–71047, 2018.

[34] N. Javaid, S. Hussain, A. Ahmad, M. Imran, A. Khan, and M. Guizani, "Region based cooperative routing in underwater wireless sensor networks," *Journal of Network and Computer Applications*, vol. 92, pp. 31–41, 2017.

[35] L. E. Emokpae, Z. Liu, G. F. Edelmann, and M. A. Younis, "Cross-stack QoS routing approach for underwater acoustic sensor networks," in *Proceedings of the 2018 Fourth Underwater Communications and Networking Conference (UComms)*, pp. 1–5, Lerici, Italy, August 2018.

[36] G. Han, L. Liu, N. Bao, J. Jiang, W. Zhang, and J. J. P. C. Rodrigues, "Arep: an asymmetric link-based reverse routing protocol for underwater acoustic sensor networks," *Journal of Network and Computer Applications*, vol. 92, pp. 51–58, 2017.

[37] T. Al-Subhi, B. Arafeh, N. Alzeidi, K. Day, and A. Touzene, "A void avoidance scheme for grid-based multipath routing in underwater wireless sensor networks," *Wireless Sensor Network*, vol. 10, no. 7, pp. 131–156, 2018.

[38] A. Bereketli, M. Tümçakır, and B. Yeni, "P-AUV: position aware routing and medium access for ad hoc AUV networks," *Journal of Network and Computer Applications*, vol. 125, pp. 146–154, 2019.

[39] M. Ali, A. Khan, K. Aurangzeb et al., "CoSiM-RPO: cooperative routing with sink mobility for reliable and persistent operation in underwater acoustic wireless sensor networks," *Sensors*, vol. 19, no. 5, p. 1101, 2019.

[40] E. Felemban, F. K. Shaikh, U. M. Qureshi, A. A. Sheikh, and S. B. Qaisar, "Underwater sensor network applications: a comprehensive survey," *International Journal of Distributed Sensor Networks*, vol. 11, no. 11, Article ID 896832, 2015.

[41] Y. W. Law, M. Palaniswami, L. V. Hoesel, J. Doumen, P. Hartel, and P. Havinga, "Energy-efficient link-layer jamming attacks against wireless sensor network MAC protocols," *ACM Transactions on Sensor Networks (TOSN)*, vol. 5, no. 1, pp. 1–38, 2009.

[42] S. Misra, M. Dash, A. V. Khatua, and M. S. O. Vasilakos, "Jamming in underwater sensor networks: detection and mitigation," *IET Communications*, vol. 6, no. 14, pp. 2178–2188, 2012.

[43] M. Zuba, Z. Shi, Z. Peng, J. H. Cui, and S. Zhou, "Vulnerabilities of underwater acoustic networks to denial-of-service jamming attacks," *Security and Communication Networks*, vol. 8, no. 16, 2645 pages, 2015.

[44] R. Martin and S. Rajasekaran, "Data centric approach to analyzing security threats in underwater sensor networks," in *Proceedings of the OCEANS 2016 MTS/IEEE Monterey*, pp. 1–6, Monterey, CA, USA, September 2016.

[45] G. Han, L. Liu, J. Jiang, L. Shu, and J. J. Rodrigues, "A collaborative secure localization algorithm based on trust model in underwater wireless sensor networks," *Sensors*, vol. 16, p. 229, 2016.

[46] J. Jiang, G. Han, C. Zhu, S. Chan, and J. J. Rodrigues, "A trust cloud model for underwater wireless sensor networks," *IEEE Communications Magazine*, vol. 55, no. 3, pp. 110–116, 2017.

[47] C. Peng, X. Du, K. Li, and M. Li, "An ultra-lightweight encryption scheme in underwater acoustic networks," *Journal of Sensors*, vol. 2016, Article ID 8763528, 10 pages, 2016.

[48] Y. Luo, L. Pu, Z. Peng, and Z. Shi, "RSS-based secret key generation in underwater acoustic networks: advantages, challenges, and performance improvements," *IEEE Communications Magazine*, vol. 54, no. 2, pp. 32–38, 2016.

[49] A. G. Lazaropoulos, "Designing the undersea internet of things (IoT) and machine-to-machine (M2M) communications using underwater acoustic MIMO networks," *Trends Renew. Energy*, vol. 2, pp. 13–50, 2016.

[50] A. Majid, I. Azam, A. Waheed et al., "An energy efficient and balanced energy consumption cluster based routing protocol for underwater wireless sensor networks," in *Proceedings of the IEEE 30th International Conference on Advanced Information Networking and Applications (AINA)*, pp. 324–333, Crans-Montana, Switzerland, March 2016.

[51] W. Lin, D. Li, Y. Tan, J. Chen, and T. Sun, "Architecture of underwater acoustic sensor networks: a survey," in *Proceedings of the First International Conference on Intelligent Networks and Intelligent Systems*, pp. 155–159, Wuhan, China, November 2008.

[52] H. Saeed, S. Ali, S. Rashid, S. Qaisar, and E. Felemban, "Reliable monitoring of oil and gas pipelines using wireless sensor network (WSN)—REMONG," in *Proceedings of the 2014 9th International Conference on System of Systems Engineering (SOSE)*, pp. 230–235, Adelade, Australia, June 2014.

[53] M. Z. Abbas, K. A. Bakar, M. A. Arshad, M. Tayyab, and M. H. Mohamed, "Scalable nodes deployment algorithm for the monitoring of underwater pipeline," *Telkomnika*, vol. 14, no. 3, pp. 1183–1191, 2016.

[54] L. A. Abdul-Rahaim and A. M. A. Ali, "Remote wireless automation and monitoring of large farm using wireless sensors networks and internet," *International Journal of Computer Science & Engineering Technology (IJCSET)*, vol. 6, pp. 118–137, 2015.

[55] Y. Taniguchi, "Experimental evaluation of effect of turbidity on the performance of visible light communication in an underwater environment," *International Journal of Simulation: Systems, Science and Technology*, vol. 17, pp. 1–4, 2016.

[56] G. Antonelli, A. Caffaz, G. Casalino et al., "The widely scalable mobile underwater sonar technology (WiMUST) H2020 project: first year status," in *Proceedings of the OCEANS 2016-Shanghai*, pp. 1–8, Shanghai, China, April 2016.

[57] S. Kumar, A. Perry, C. Moeller et al., "Real-time tracking magnetic gradiometer for underwater mine detection," in *In*

Proceedings of the Oceans'04 MTS/IEEE Techno-Ocean'04, vol. 2, pp. 874–878, Kobe, Japan, November 2004.

[58] S. Kamalesh and P. G. Kumar, "Fuzzy based secure intrusion detection system for authentication in wireless sensor networks," *Journal of Computational and Theoretical Nanoscience*, vol. 14, no. 5, pp. 2465–2472, 2017.

[59] S. Kemna, M. J. Hamilton, D. T. Hughes, and K. D. LePage, "Adaptive autonomous underwater vehicles for littoral surveillance," *Intelligent Service Robotics*, vol. 4, no. 4, pp. 245–258, 2011.

[60] Q. Wang, H. N. Dai, X. Li, and H. Wang, "On modeling eavesdropping attacks in underwater acoustic sensor networks," *Sensors*, vol. 16, no. 5, p. 721, 2016.

[61] I. Butun, *Prevention and Detection of Intrusions in Wireless Sensor Networks, [Ph.D. thesis]*, University of South Florida, 2013.

[62] F. Hu and N. K. Sharma, "Security considerations in ad hoc sensor networks," *Ad Hoc Networks*, vol. 3, no. 1, pp. 69–89, 2005.

[63] F. Stajano and R. Anderson, "The resurrecting duckling: security issues for ubiquitous computing," *Computer*, vol. 35, no. 4, pp. supl22–supl26, 2002.

[64] T. Borgohain, U. Kumar, and S. Sanyal, "Survey of security and privacy issues of internet of things," 2015, https://arxiv.org/abs/1501.02211.

[65] W. Znaidi, M. Minier, and J.-P. Babau, *An Ontology for Attacks in Wireless Sensor Networks, [Ph.D. Thesis]*, INRIA, 2008.

[66] C. Pu, S. Lim, B. Jung, and M. Min, "Mitigating stealthy collision attack in energy harvesting motivated networks," in *Proceedings of the 2017 IEEE Military Communications Conference (MILCOM 2017)*, pp. 539–544, Baltimore, MD, USA, October 2017.

[67] F. Stajano and R. J. Anderson, "The resurrecting duckling," in *Proceedings of the 7th International Workshop on Security Protocols*, Cambridge, UK, April 1999.

[68] P. Pandarinath, "Secure localization with defense against selective forwarding attacks in wireless sensor networks," in *Proceedings of the 2011 IEEE 3rd International Conference on Electronics Computer Technology (ICECT)*, vol. 5, pp. 112–117, Kanyakumari, India, April 2011.

[69] M. R. Ahmed, M. Aseeri, M. S. Kaiser, N. Z. Zenia, and Z. I. Chowdhury, "A novel algorithm for malicious attack detection in uwsn," in *Proceedings of the 2015 IEEE International Conference on Electrical Engineering and Information Communication Technology (ICEEICT)*, pp. 1–6, Dhaka, Bangladesh, May 2015.

[70] C. Ioannou and V. Vassiliou, "The impact of network layer attacks in wireless sensor networks," in *Proceedings of the 2016 IEEE International Workshop on Secure Internet of Things (SIoT)*, pp. 20–28, Heraklion, Greece, September 2016.

[71] I. Khan, M. A. Khan, S. Khusro, and M. Naeem, "Vehicular lifelogging: issues, challenges, and research opportunities," *Journal of Information Communication Technologies and Robotics Applications*, vol. 8, no. 2, pp. 30–37, 2017.

[72] M. Demirbas and Y. Song, "An RSSI-based scheme for Sybil attack detection in wireless sensor networks," in *Proceedings of the 2006 International Symposium on World of Wireless, Mobile and Multimedia Networks*, pp. 564–570, Washington, DC, USA, January 2006.

[73] I. Khan and S. Khusro, "Towards the design of context-aware adaptive user interfaces to minimize drivers' distractions," *Mobile Information Systems*, vol. 2020, 23 pages, 2020.

[74] F. Yavuz, J. Zhao, O. Yagan, and V. Gligor, "On secure and reliable communications in wireless sensor networks: towards k-connectivity under a random pairwise key pre-distribution scheme," in *Proceedings of the 2014 IEEE International Symposium on Information Theory (ISIT)*, pp. 2381–2385, Honolulu, HI, USA, July 2014.

[75] H. Chen and W. Lou, "On protecting end-to-end location privacy against local eavesdropper in wireless sensor networks," *Pervasive and Mobile Computing*, vol. 16, pp. 36–50, 2015.

[76] I. Ahmad, M. S. Niazy, R. A. Ziar, and S. Khan, "Survey on IoT: security threats and applications," *Journal of Robotics and Control (JRC)*, vol. 2, no. 1, pp. 42–46, 2021.

[77] I. F. Akyildiz, D. Pompili, and T. Melodia, "Underwater acoustic sensor networks: research challenges," *Ad Hoc Networks*, vol. 3, no. 3, pp. 257–279, 2005.

[78] D. Muhammed, M. Anisi, M. Zareei, C. Vargas-Rosales, and A. Khan, "Game theory-based cooperation for underwater acoustic sensor networks: taxonomy, review, research challenges and directions," *Sensors*, vol. 18, no. 2, p. 425, 2018.

[79] Y. Chen, F. Ji, Q. Guan, Y. Wang, F. Chen, and H. Yu, "Adaptive RTO for handshaking-based MAC protocols in underwater acoustic networks," *Future Generation Computer Systems*, vol. 86, pp. 1185–1192, 2017.

[80] H. Li, Y. He, X. Cheng, H. Zhu, and L. Sun, "Security and privacy in localization for underwater sensor networks," *IEEE Communications Magazine*, vol. 53, no. 11, pp. 56–62, 2015.

[81] I. Khan, S. Khusro, N. Ullah, and S. Ali, "AutoLog: toward the design of a vehicular lifelogging framework for capturing, storing, and visualizing LifeBits," *IEEE Access*, vol. 8, pp. 136546–136559, 2020.