



Review

A Systematic Review on Recent Trends, Challenges, Privacy and Security Issues of Underwater Internet of Things

Delphin Raj Kesari Mary ¹, Eunbi Ko ², Seung-Geun Kim ³, Sun-Ho Yum ¹, Soo-Young Shin ⁴
and Soo-Hyun Park ^{1,2,*}

¹ Department of Financial Information Security, Kookmin University, Seoul 02707, Korea; delphinraj@kookmin.ac.kr (D.R.K.M.); junsan86@kookmin.ac.kr (S.-H.Y.)

² College of Computer Science, Kookmin University, Seoul 02707, Korea; sinaa821@kookmin.ac.kr

³ Ocean System Engineering Research Division, Korea Research Institute of Ships & Ocean Engineering, Daejeon 34103, Korea; sgkim@kriso.re.kr

⁴ Special Communication & Convergence Service Research Center, Kookmin University, Seoul 02707, Korea; sy-shin@kookmin.ac.kr

* Correspondence: shpark21@kookmin.ac.kr

Abstract: Owing to the hasty growth of communication technologies in the Underwater Internet of Things (UIoT), many researchers and industries focus on enhancing the existing technologies of UIoT systems for developing numerous applications such as oceanography, diver networks monitoring, deep-sea exploration and early warning systems. In a constrained UIoT environment, communication media such as acoustic, infrared (IR), visible light, radiofrequency (RF) and magnet induction (MI) are generally used to transmit information via digitally linked underwater devices. However, each medium has its technical limitations: for example, the acoustic medium has challenges such as narrow-channel bandwidth, low data rate, high cost, etc., and optical medium has challenges such as high absorption, scattering, long-distance data transmission, etc. Moreover, the malicious node can steal the underwater data by employing blackhole attacks, routing attacks, Sybil attacks, etc. Furthermore, due to heavyweight, the existing privacy and security mechanism of the terrestrial internet of things (IoT) cannot be applied directly to UIoT environment. Hence, this paper aims to provide a systematic review of recent trends, applications, communication technologies, challenges, security threats and privacy issues of UIoT system. Additionally, this paper highlights the methods of preventing the technical challenges and security attacks of the UIoT environment. Finally, this systematic review contributes much to the profit of researchers to analyze and improve the performance of services in UIoT applications.

Keywords: Underwater Internet of Things (UIoT); trends; challenges; security and privacy



Citation: Mary, D.R.K.; Ko, E.; Kim, S.-G.; Yum, S.-H.; Shin, S.-Y.; Park, S.-H. A Systematic Review on Recent Trends, Challenges, Privacy and Security Issues of Underwater Internet of Things. *Sensors* **2021**, *21*, 8262. <https://doi.org/10.3390/s21248262>

Academic Editor: Juan V. Capella

Received: 28 October 2021

Accepted: 6 December 2021

Published: 10 December 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

During the past few decades, researchers and developers have shown much interest in developing UIoT applications such as deep-sea exploration, divers' system monitoring, early warning generation, naval network surveillance, etc. As shown in Figure 1, the UIoT network consists of heterogeneous devices such as underwater sensor nodes (UW-SNodes), underwater cluster heads (UW-CHs), remotely operated underwater vehicles (ROVs), unmanned underwater vehicles (UUVs), autonomous underwater vehicles (AUVs), etc. The UIoT devices can be fixed or mobile, moving from one location to another to gather information and transmit that information via digitally linked devices in water bodies such as the gateway or buoy in surface water. In addition, other devices like moving gateways, satellites, base stations, etc., are utilized to expand the communication range of UIoT applications.

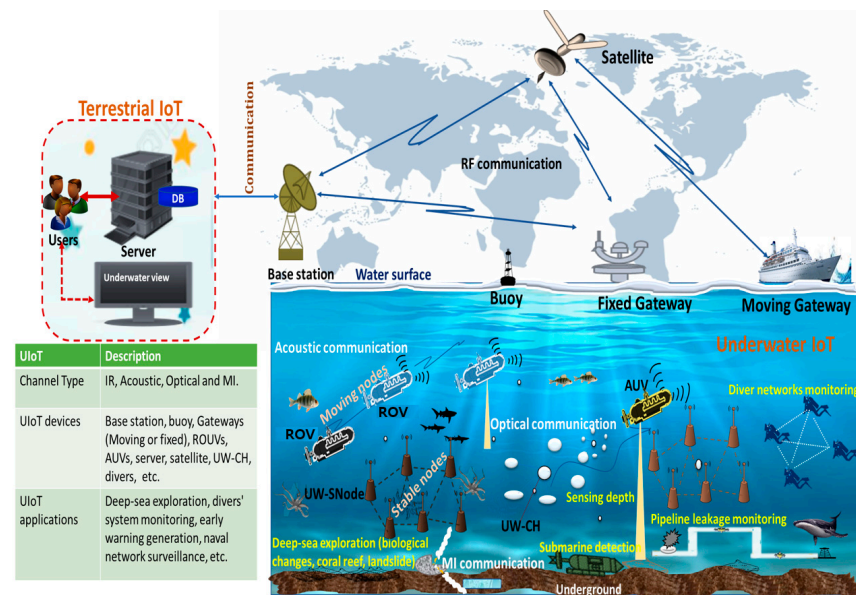


Figure 1. UIoT Architecture.

In the recent survey produced by the United States National Oceanic and Atmospheric Administration (NOAA), 97% of the earth's surface is covered with water [1]. The UIoT environment is coped with smart sensing underwater devices that are installed with heterogeneous functionalities. Many researchers have proposed different methodologies to design and develop various UIoT applications in the last few years. However, the challenges and limitations are still concerns for the UIoT environment based on the application, channel types and channel characteristics. Channel types define the type of medium used in UIoT environments such as RF, acoustic, optical (VLC: visible light communication or IR: infrared) and MI, and channel characteristics represent the technical factors that affect the medium used in UIoT environments, such as propagation speed, turbulence, pressure, node mobility, etc. [2] Security attacks and privacy issues are the other key challenges in the current UIoT system [3].

This research aims at providing a survey of the state-of-the-art research, communication technologies, challenges, security attacks and privacy issues and provides the mitigation methodology to overcome the challenges and security attacks in the current UIoT system. Furthermore, this research will help the researchers and developers to build new UIoT applications by considering the best channel type with security and privacy models. The key contributions of this paper are briefed under research goals in Table 1.

The layout of this paper is delivered as follows: Section 2 represents the prior study insights and recently used communication technologies of the UIoT system. Section 3 describes the technical challenges, security attacks and privacy issues of UIoT system. Section 4 provides the available methods to overcome the challenges, security attacks and privacy issues of the UIoT system. Section 5 highlights the findings, future work and directions of UIoT system, and Section 6 concludes the paper.

Table 1. Research Goals.

Queries (Qs)	Discussion
Q1: What are the current trends of the UIoT system?	UIoT is the growing trend in the current IoT system. Recently, numerous UIoT applications have been developed for the industries. Therefore, Q1 provides the survey based on the latest article and the recently developed UIoT applications. Furthermore, the communication technologies of UIoT are discussed, which includes the pros and cons of UIoT channels such as RF, acoustic, optical and MI.
Q2: What are the challenges of the current UIoT system?	Challenges include technical challenges, security attacks and privacy issues. Therefore, Q2 discusses the technical challenges based on UIoT channel characteristics and the possible security challenges and privacy issues in UIoT.
Q3: What are the possible methods to overcome the challenges, security attacks and privacy issues in the UIoT system?	In the UIoT system, most of the challenges and security issues are still of concern. Likewise, privacy methodologies are not yet considered for the current UIoT system. Therefore, Q3 highlights the countermeasures taken to overcome the challenges, security attacks and privacy issues of the current UIoT system.
Q4 and Q5: What are the findings and future directions?	Q4 discusses the findings based on the systematic review and Q5 highlights the future direction of this paper.

2. Q1: What Are the Recent Trends of UIoT System?

This section discusses the recent trends and applications developed in the UIoT system along with the communication technologies of the current UIoT system.

2.1. Prior Research

Many articles discuss the latest research and applications developed in the UIoT system [4]. For example, in [5], Gussen et al. unveiled a survey on underwater communication technologies, including the pros and cons of using optical, acoustic and RF channels in the UIoT environment. Furthermore, the research shows that the RF channel is unsuitable for the underwater environment due to its high absorption rate. In [5,6], the channel characteristics of electromagnetic (EM) signals in UIoT and the use of EM signals in the military application were discussed. In [7–10], the challenges and merits of using acoustic signals in UIoT were discussed. Furthermore, the research shows that an acoustic signal reveals low absorption rates underwater. Therefore, the acoustic signal is used for long-distance communication in the UIoT environment, but the drawbacks are low bandwidth (1–100 kHz), limited speed (≈ 1500 m/s) and high delay in data transmission.

In [11–14], the latest research on underwater optical communication (UwOC) techniques was discussed, and the strength and weaknesses of optical signals were shortened. Additionally, the research showed that UwOC are used for short-range communication with a high data rate in the UIoT environment, but UwOC cannot be applicable for long-range distances due to high attenuation.

In [15], Kumar et al. developed a single hybrid optical, acoustic modem to achieve a high bandwidth rate, low battery consumption and long-distance data transmission. In [16], a built-in optical, acoustic communication technique was proposed by integrating the optical system into the existing acoustic communication technology to offer a high data rate, long-distance data transfer and low latency in underwater communication. In addition, from [17–20], other acoustic–optical combined technologies were discussed. In [21], Delphin et al. proposed the new technique by considering multiple mediums and bandwidths based on the distance for reliable data transmission in the UIoT environment. In [22], Delphin et al. developed the underwater hybrid software-defined modem to support the fast and reliable communication system in UIoT. Figure 2 shows that the UIoT applications are grouped into five major categories and have numerous subdivisions according to the survey carried out by Chien-Chi Kao et al. [23]. Moreover, in [24,25], the classifications and descriptions of each UIoT application are indicated.

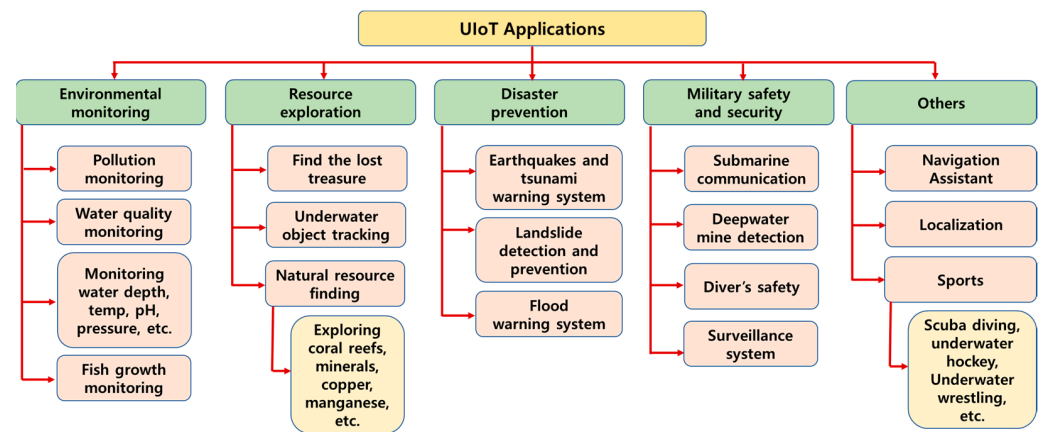


Figure 2. Existing applications of UIoT.

2.2. Communication Technologies of UIoT

Based on the research highlighted in Section 2.1, the recent communication trends in UIoT are described underneath and the essential channel attributes are briefed in Table 2.

Table 2. Communication technologies of UIoT [2–25].

Attributes	Acoustic	RF	Optical	MI
Channel speed	≈1500 m/s	≈ 3.33×10^8 m/s	≈ 3.33×10^8 m/s	≈ 3.33×10^8 m/s
Communication range	≈kilometer (km)	≈10 m	≈10–100 m	≈10–100 m
Data rate	≈kbps	≈Mbps	≈Gbps	≈Mbps
Signal operation	Audible	Non-visible and non-audible	Visible	Non-visible and non-audible
Frequency band	10–15 kHz	30–300 Hz	≈ 5×10^{14} Hz	-
Size of the Antena	≈0.1 s	≈0.5 s	≈0.1 s	≈0.1 s
Channel characteristics dependency	Undersea noise, temperature, pressure, Doppler spread, salinity, etc.	Conductivity	Undersea noise, attenuation, turbidity, scattering, etc.	Conductivity
Bandwidth	≈1–100 Kilohertz (kHz)	≈Megahertz (MHz)	≤150 Megahertz (MHz)	≈Megahertz (MHz)
Purpose of each channel	Long-range communication	Surface water communication	Short-range communication	Underground communication in deep sea
Transmission power	>10 watts (W)	megawatts (MW)–watts(W)	megawatts (MW)–watts(W)	10^{-8} watts (W)
Power loss dependency	≈0.1 dB per meter (m) or per hertz (Hz)	≈28 dB per kilometer (km) or one million hertz (HZ)	Depending on the turbulence of water	Depending on the permeability of undersea soils

From the physics perception, unlike satellite, TV, mobile and radio communication frequency ranges, the conductivity of radiofrequency in seawater is very high. Thus, Radiofrequency (RF) wave propagation is affected strongly. For this reason, it is not easy to establish links using ultra-high frequency (UHF) and very high frequency (VHF) more than 10 m away from the sea surface. As for lower frequencies, RM attenuation can be considered short enough for reliable communication to occur over a few kilometers. However, the frequencies from 3 kHz to 30 kHz and from 3 Hz to 3 kHz are not enough to transmit at high data rates.

The channel performance and behavior are the main difference between optical and RF channels in the UIoT environment. There is an insulating material named dielectric utilized for optical channel propagation in UIoT. This mechanism is explained by the plasma frequency, operating as either a dielectric or conductor, following the frequency range. There are changes from a conductor to a dielectric at around 250 GHz in seawater. Attenuation and scattering are minor in the case of short-distance communication. Furthermore, the speed is up to 3×10^8 m/s. Therefore, the optical signal is more reliable in short-range communication up to 10 m and suitable up to 100 m. Visible light communication (VLC) is the communication technology derived from an optical signal in UIoT. The ranges are from 450 nanometers to 550 nanometers at 500 Mbps and a distance of 100 m. Moreover, the speed is very high, up to 5 m. Therefore, VLC is very effective in short-range and one-to-one communication.

As stated, electromagnetic signals and optical signals have a limited transmission range. In addition, these signals are heavily affected by attenuation, scattering, and turbulence. This leads to a limit on the transmission distance. Therefore, acoustic communication technology is used for long-distance propagation in UIoT. The communication distance is up to 1 km at a speed of approximately 1500 m/second.

Magnetic Induction (MI) based communication technology is most commonly used in the underground of the seabed. It can cover a maximum of 10 m. The MI signal propagation speed is the same as the speed of light inside water, 3×10^8 m/s. Moreover, the data rate is in the order of kilobits per second (kbps).

3. Q2: What Are the Challenges of the Current UIoT System

This section describes the UIoT system's challenges, including channel characteristics, technical challenges, security challenges and privacy issues.

3.1. Channel Characteristics of UIoT

Delphin et al. pointed out that most of the characteristics of IoT systems are suitable for the UIoT environment since UIoT is the subclass of IoT [26]. Most of the available IoT protocols are designed and developed for stable nodes. Additionally, the performance of IoT networks can be reduced with the addition of new nodes and variations in terrestrial environment techniques. This statement highlights why the existing protocols and security models of terrestrial IoT should not be directly applied to UIoT.

3.1.1. Underwater Channel

Unlike terrestrial IoT, UIoT nodes typically communicate via acoustic, optical, RF and MI channels [27]. This results in long propagation delay, high battery consumption, high error rate, etc. Moreover, the behavior of each channel's characteristics is different in the UIoT environment [2–4]. For example, the bandwidth of the acoustic channel is only a small percentage when compared to the RF channel [28]. Furthermore, due to the open characteristics of this UIoT environment, the attackers can easily inject the malicious node and steal the data or hack the communication channel [29].

3.1.2. Energy Consumption and Storage

UIoT nodes are designed with limited battery power, computational capacity and memory space [21]. Furthermore, the nodes consume more power for data gathering, processing and transferring. Compared to terrestrial networks, the nodes are rechargeable using solar energy. However, in UIoT networks, it is not easy to maintain or recharge due to the natural behavior of the environment. This may cause power constraints in UIoT networks.

3.1.3. Environmental Condition

Due to internal waves, mammals activity and other objects' behaviors lead to dynamic topology formation in UIoT networks [30]. The frequent changes of the UIoT network topol-

ogy can cause rerouting, transmission loss and data accuracy issues [31]. Compared with the terrestrial IoT, in UIoT networks, the nodes are sparsely deployed for data gathering and transmission. Furthermore, since the UIoT nodes are mobile, localization, synchronization and secure communication are the other issues in UIoT networks.

3.2. Technical Challenges of UIoT

As a branch of the terrestrial internet of things (T-IoT), some particularities of UIoT are similar to T-IoT [32]. Unfortunately, due to the difference in the working environment, some unique particularities and constraints are outlined below.

3.2.1. Limited Resources

In the UIoT environment, the battery and storage capacity of sensing devices are very limited.

Limited battery: The optical and acoustic communication channel in the UIoT environment consumes more power than RF communication. Furthermore, energy harvesting is impossible due to the unavailability of solar power creation in the UIoT environment. This causes data loss and reduces battery lifetime [33]. In addition, the existing low energy consumption or optimization methods used in the terrestrial environment, for example, the methods used in references [34,35], cannot be applied to UIoT networks.

Limited storage capacity: The memory size of devices in the UIoT environment is limited. Moreover, memory formatting is impossible in the UIoT environment. This causes failure in data gathering and data transmitting [2].

3.2.2. Unreliable Channel Condition

In the UIoT Environment, the Cause of Unreliable Communication Channels Refer to the Factors that can Affect Data Transmission Loss Underwater.

Limited bandwidth and transmission delay: In an acoustic communication channel, the bandwidth is limited, such as from 100 kHz to 500 kHz, from 10 kHz to 100 kHz, and from 500 Hz to 10 kHz for short, medium and long-range communication in the UIoT environment, respectively. Furthermore, the data rate is a maximum of 100 kb/s. This causes a delay in data transmission [21].

Attenuation and scattering: Approximately ≤ 150 MHz and Hz to 10 kHz can be used for long-range data transmission in an optical and acoustic communication channel. Even though light spreads much more compared to the sound signal in the UIoT environment, both signals suffer the problem of attenuation and scattering in long-range communication. This causes a transmission loss for long-range communication [36].

High propagation delay: In the UIoT environment, numerous factors such as turbidity, depth, pH level, density, temperature, etc., are the major causes of high propagation delay in optical and acoustic channel communication. This causes transmission loss or delay in transmission [37].

Channel noise: In the UIoT environment, channel noise refers to the noise factor that affects the underwater communication channel, such as environmental and ambient noise. Environmental noise is the noise generated by human beings such as shipping, fishing, naval activities, etc., and ambient noise is the background sound generated from an unknown source such as wind, underwater objects, sea animals, etc. [38]

Node mobility: The UIoT environment consists of static and mobile nodes. The static nodes are placed in a fixed position and the mobile nodes move from one place to another for data collection. However, the characteristics of deep seawater such as internal wave, sediment formation and deliberate motion of other particles, force the nodes to move from one to another at any time in the UIoT environment. This term is also defined as external force mobility. Due to external force mobility, the connectivity can be easily broken, which causes data transmission errors [22].

3.2.3. Insecure Environment

In the UIoT environment, security methods are particularly necessary to monitor naval applications. However, due to the environmental condition, it is difficult to monitor the UIoT networks and devices. In this case, the attackers find it easy to access the nodes or devices in the UIoT environment. Such types of attacks are denial-of-service (DoS) attacks, jamming attacks, flooding attacks, etc. This causes serious damage to the legitimate node in the UIoT environment [39].

3.2.4. High Cost

As shown in Figure 1 of Section 1, in the UIoT environment, the sensor nodes are devices that are sparsely deployed. Additionally, the products are from different vendors. Therefore, it is too costly to install, monitor and manage the network and devices in the UIoT environment [2–4].

3.2.5. Dynamic Topology

Node mobility was discussed in Section 3.3.2. As shown in Figure 3, the UUVs and mobile nodes are automatically moving from one place to another or by external forces. Node mobility can form a new topology by modifying the existing topology. Therefore, node mobility is the major cause of dynamic topology formation in UIoT networks. This causes routing problems in the UIoT environment [40].

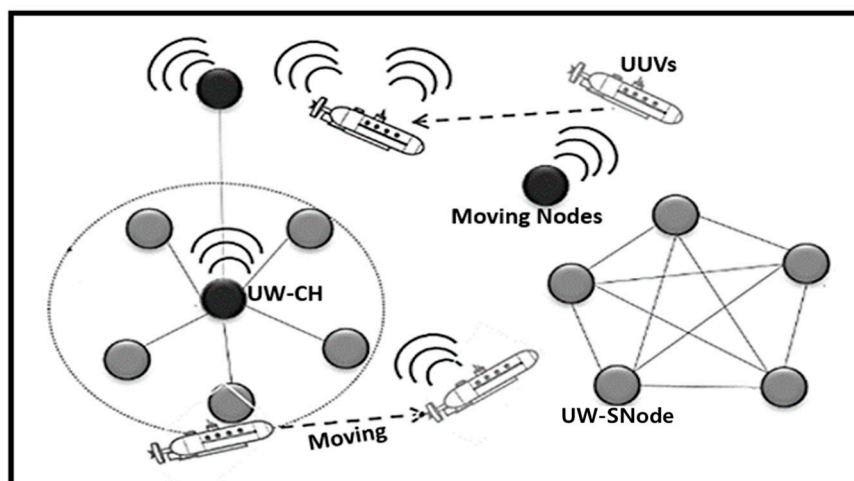


Figure 3. Dynamic topology formation.

3.2.6. Physical Damages

In the UIoT environment, the nodes are too deeply deployed in a harsh environment. Furthermore, nodes can be damaged easily because of marine objects such as deep-sea mammals, waste particles, internal waves, etc., which can cause severe damage to UIoT nodes, such as hardware failure, software error and broken links, making them dead nodes [3].

3.2.7. Network Configuration

In the UIoT environment, since the nodes are mobile or stable, the connectivity can be easily broken or can generate a new topology, which can cause network configuration problems in UIoT networks [21].

3.3. Security Challenges of UIoT

This section describes the security challenges of UIoT that affect confidentiality, privacy, availability, resilience, authentication, safety, etc. The research shows a constant set of challenges for UIoT.

3.3.1. Complex Environment

As discussed in Section 3.2.3, the UIoT is complex and insecure. For most of the applications, the sensor nodes are sparsely deployed and not well managed. This makes way for attackers to inject malicious nodes inside the UIoT networks. Furthermore, as discussed in Section 3.2.7, the underwater nodes can be physically broken due to the natural behavior of deep-sea and other living organisms. Therefore, monitoring and protecting nodes in a complex environment is an important discussion for the developers.

3.3.2. Data Privacy

In the UIoT environment, data privacy is extremely important since it can handle sensitive data in naval applications such as secret operations, identity sharing, enemy submarine tracking, etc. Since the UIoT environment is harsh, it is difficult to apply the privacy methods of terrestrial IoT environments such as k-anonymity, l-diversity, t-closeness and differential privacy to the UIoT environment. Therefore, the attackers can steal private data from UIoT devices.

3.3.3. Network and Device Management

The dynamic behavior of nodes and changes in topology as discussed earlier in Section 3.2.5 and other issues such as the limited battery, limited memory, routing, etc., can impact the management of networks and devices underwater. Therefore, as shown in Figure 4, it is difficult to manage the underwater network management system functionalities such as fault, configuration, accounting, performance, security and constrained (FCAPSC) management in the UIoT environment. Therefore, the attacker can target FCAPSC functionalities [21].

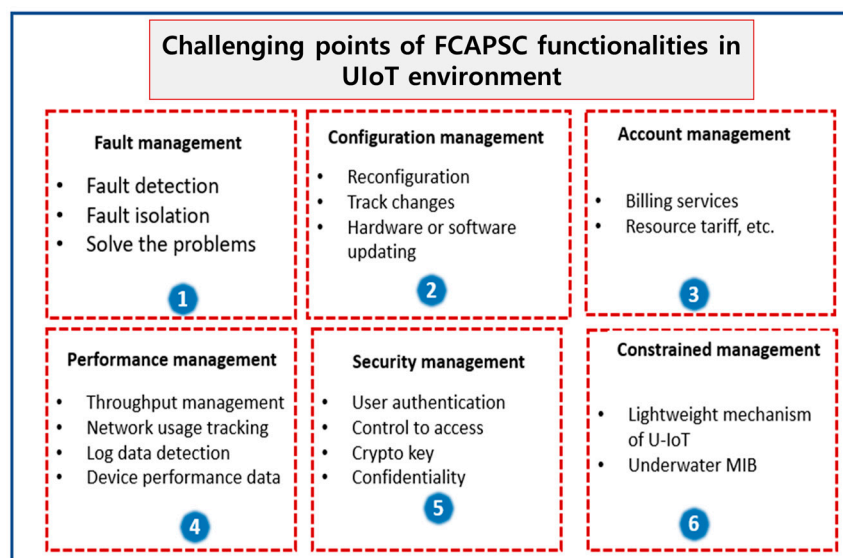


Figure 4. Challenges in adapting FCAPSC functionality.

3.3.4. Localization Techniques

In UIoT networks, node management is necessary to protect the nodes from physical damages and security attacks. In this case, it is necessary to adapt localization techniques to UIoT nodes to identify the location of each node underwater. However, due to heavy-weight and environmental limitations, the localization mechanism in terrestrial networks cannot be applied directly to the UIoT environment [41].

3.4. Security Goals, Attacks and Privacy of UIoT

This Section describes the security goals, attacks and privacy of UIoT networks. Figure 5 illustrates the security goals and classification of attacks in UIoT.

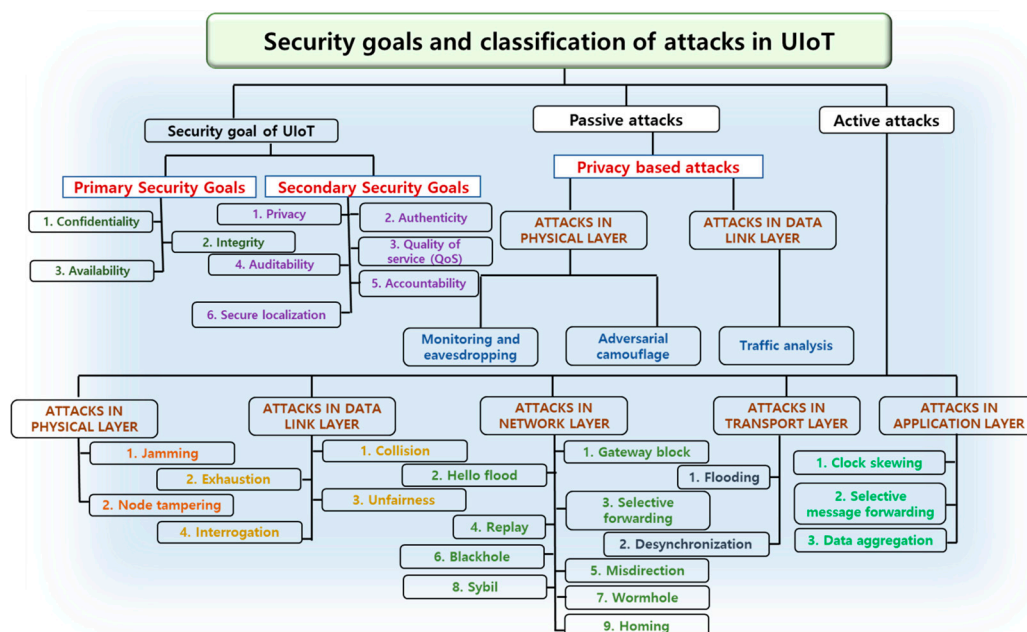


Figure 5. Goals and classification of security attacks in the UIoT environment.

3.4.1. Security Goals of UIoT

It is classified into two parts (1) primary security goals and (2) secondary security goals [42–44]. Integrity, confidentiality and availability are the three primary security goals of UIoT, expected to be available in all UIoT applications. On the other hand, privacy, synchronization, authenticity, quality of service, auditability, accountability and secure localization are the secondary security goals of UIoT. The classification of UIoT security goals are described underneath.

Confidentiality

In UIoT networks, confidentiality is the essential feature for securing underwater data. A key sharing mechanism is a suitable approach that can be utilized to protect the data during transmission. In addition, for confidentiality, an auto-decision-making mechanism must be used for storing and retrieving data in the UIoT environment [42].

Integrity

In UIoT networks, data integrity is essential to maintain the accuracy and reliability of underwater data. Data integrity refers to the approaches to check whether the received data are altered during transmission via an underwater channel. For example, a message integrity check (MIC) can be used to verify the data integrity of received underwater data. In addition, an auto-integrity-checking mechanism such as logs integrity and software integrity can be used to verify the integrity of log reports and device software, respectively, in the UIoT environment [42].

Availability

In UIoT networks, data availability is necessary to provide the quality of services such as preventing UIoT devices from malicious attacks, securing harbor environment, securing diverse life at risk, etc. Self-healing, auto-recovery and centralized data sharing functions are necessary to support availability in UIoT networks [42].

Privacy

In UIoT networks, privacy refers to the information or service that a particular user or device can access. As discussed in Section 3.3.2, it is difficult to adapt the existing privacy

approaches directly to UIoT networks. Hence, it is necessary to port a robust privacy approach for UIoT to protect the data from attackers. The types of privacy approaches that need to be considered in UIoT are categorized underneath:

UIoT data privacy: In UIoT networks, data privacy is necessary in naval applications to protect secret messages from attackers, e.g., enemy submarine attacking and secret message passing.

UIoT device privacy: In UIoT networks, a device identity is generally used to track and transfer information to UIoT devices. This identity is traceable; therefore, it is easy for the attackers to steal the information. In this case, a robust identity protection approach is necessary to hide the device identity from malicious nodes.

UIoT location privacy: In UIoT networks, location information is necessary to track the mobility of UIoT devices. The location information is open and is essential for data transmission between the nodes in the underwater environment. In addition, hiding the location of nodes based on necessity is a challenging task. Hence, it is necessary to port a privacy-based location sharing mechanism for UIoT devices.

Authenticity

In UIoT networks, authentication refers to the verification between sender and receiver node. As discussed in Section 3.3.1, the environmental condition is complex. In addition, it is difficult to adapt the terrestrial authentication scheme to the UIoT environment. Therefore, the attacker finds it easier to block the channel. Hence, it is necessary to design a lightweight authentication scheme for UIoT networks.

Auditability

In UIoT networks, it is necessary to analyze security functions' security activities and performance to provide high-quality services. Hence, an auto-auditing or self-auditing mechanism can be considered to evaluate the security systems in the UIoT environment.

Others

In UIoT networks, other security goals such as audibility, data freshness, self-organization, time synchronization, secure localization, etc., can be considered to provide the quality of services (QoS) in the UIoT environment.

3.4.2. Passive Attacks

The unauthorized attacker attacks the UIoT channel without altering the data. These attacks have silent carriers because they do not carry any signals. The attacker is hidden during a passive attack and can cause node tampering, jamming, message distortion and replaying. Furthermore, the attacker can anticipate the idea of UIoT networks by identifying packet traffic, observing packet exchange nodes and predicting the location of nodes. Passive attacks are also known as privacy-based attacks. The types of passive attacks are mentioned below:

Monitoring and eavesdropping: It is the most commonly used attack against data privacy in UIoT environment. When the network traffic is at its peak, the attacker can steal important information by tapping the network configuration. This type of attack is categorized under privacy-based attacks.

Adversary and camouflage: In this case, the invisible attacker injects an adversary node into the UIoT network. In effect, the adversary node can track and modify the information in UIoT networks, such as stealing packets, rerouting packets and altering nodes.

Traffic analysis: In these attacks, the attacker infuses the UIoT networks by accessing the pattern in the communication channel. Through this, the attacker can listen to the location of each node, the routing path, the behavior, etc.

3.4.3. Active Attacks

The unauthorized attacker can alter, infuse, erase or destroy information in UIoT networks. The active attack can delete or modify the data during transmission and after transmission. Active attacks in UIoT are categorised into five categories: (1) Denial-of-service, (2) Message distortion, (3) Node tampering, (4) Message replay and (5) Masquerade attacks. The types of active attacks are classified under each layer of UIoT networks, such as a physical layer, data link layer, network layer, transport layer and application layer.

Denial of service attacks is one of the deadliest active attacks and can cause a ton of damage. DoS attacks can be used at any layer of UIoT networks. DoS is an active attack that attempts to make assets out of reach to the authentic node. The attacker tries to block the authentic nodes from retrieving the services offered by the network [45]. Figure 6 shows the types of DoS attacks in UIoT.

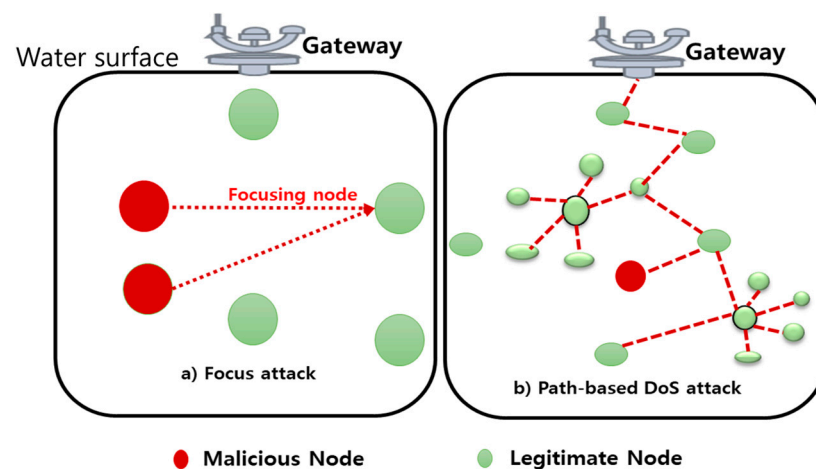


Figure 6. Types of DoS attacks in the UIoT environment.

Node tampering: The UIoT nodes consist of hardware components such as a controller, battery, transmitter and receiver. In node tampering, the attacker can track and modify the software code of underwater nodes. Due to this, the software and hardware parts can be broken, which causes severe damage to the nodes in the UIoT environment. In effect, it causes network lifetime damages and data loss.

Message distortion: In these attacks, the attacker can alter the data sent by one UIoT node to another. It can cause severe damages in case of emergency UIoT applications, e.g., message distortion in the naval application can break the security system. This could cause confusion by passing wrong information to the end-users.

Message Replay: In these attacks, the attacker acts like the source node to send the same information already sent by the source node, or the attacker purposely delays transferring data by hacking. A message replay attack is also known as a play-back attack.

Masquerade: In these attacks, the attacker uses the fake identity to steal the information from a legitimate node. A masquerade attack is a kind of privacy attack.

Jamming attack: In these attacks, the malicious nodes frequently send the noise signal to disturb legitimate nodes in UIoT networks. Additionally, this attack can hack few special nodes inside the UIoT networks, such as root node, gateway, underwater cluster head, etc., which causes jamming in UIoT networks. In effect, it stops data transmission and gathering. Figure 7 shows the jamming attack where a malicious node continuously attacks the root node, disrupting the communication with the member node.

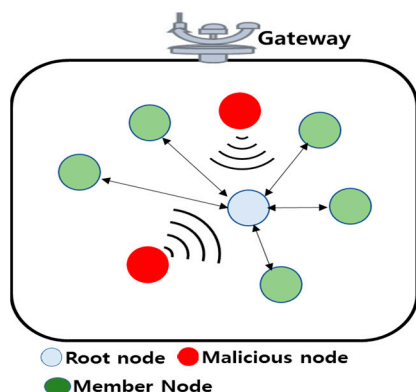


Figure 7. Jamming attack in the UIoT environment.

Collision attack: This attack happens in the data-link layer of UIoT networks. A collision happens when two underwater nodes send packets at the same time. Hence, to avoid the collision in UIoT networks, the underwater nodes follow the data transmission rules, namely, that underwater nodes should not use the same time for data transmission. However, in a collision attack, the attacker will violate the rules and send the packets simultaneously. In effect, the UIoT networks need frequent retransmission and cause power loss.

Exhaustion attack/battery-oriented attack: This attack aims to drain the total energy of underwater nodes in UIoT networks. For example, Figure 8 shows the battery-oriented attack of UIoT networks. Here, the malicious node sent a routing request (RREQ) message to node 0. In response, node 0 sent the routing response (RRES) message to the malicious node. Finally, the malicious node will continuously send the corrupted packets until node 0 becomes dead. In effect, it reduces network lifetime.

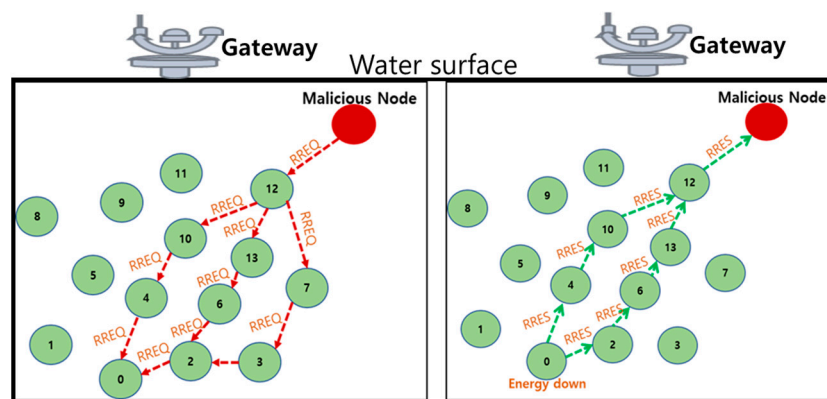


Figure 8. Battery-oriented attack.

Node compromise attack: An attacker can capture, break and compromise UIoT nodes to read or change information from memory. Moreover, what is terrible, is that the compromised nodes can penetrate into the network as authentic nodes to screen or disrupt it, which can prompt considerably more prominent harm. An attacker can find the network by checking the power of the acoustic signal and capturing them. More regrettable, is that without a trace of hack-confirmation equipment or other security systems, the attacker can undoubtedly break and compromise them to inspect private information (e.g., the secret key, the encryption algorithm, the trust esteem) and alter this information in the inward memory. Additionally, the compromised node can be penetrated into the network as an actual node to screen it or perform persistent attacks.

Sybil attack: The Sybil attack is a type of routing attack. In this case, the attacker uses a fake identity to steal the information while routing. Figure 9 shows that the attacker can

locate any place in UIoT networks and use multiple identities to mislead routing. In effect, it causes packet loss or transmission delay [46–48].

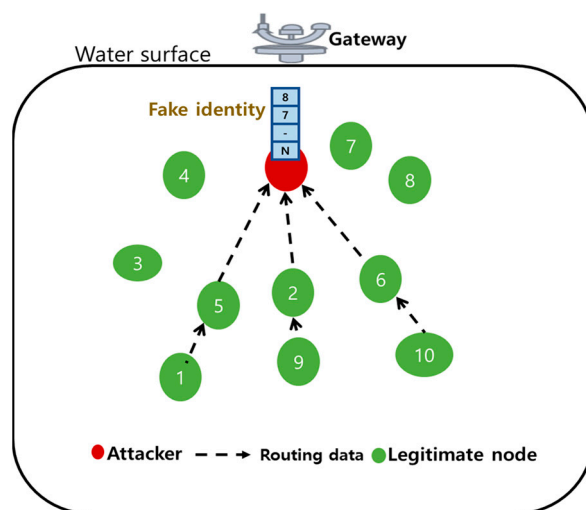


Figure 9. Sybil attack in UIoT environment.

Wormhole attack: An attacker uses two malicious nodes to tunnel traffic through the UIoT networks in a wormhole attack [49–52]. The two plotting nodes capture packets at one end and block them at another end. Wormhole attacks can make fake neighbor associations and give the probability of an alternate path for routing. Figure 10 explains how a wormhole attack occurs, causing a breach in the communication link, only because it looks like the distance of the wormhole node is shorter than legitimate nodes.

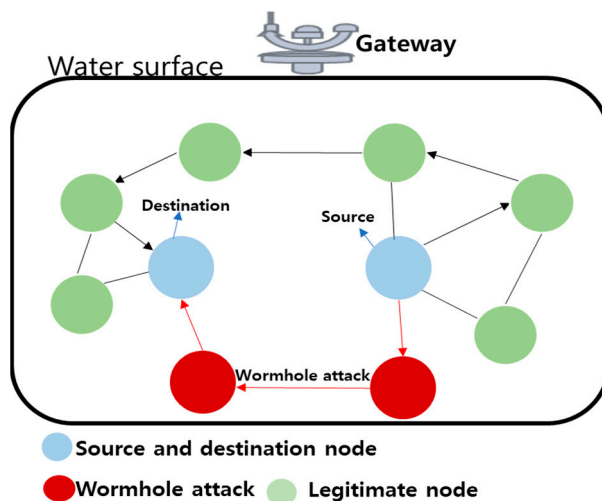


Figure 10. Wormhole attack in the UIoT environment.

Unfairness: This is a type of DoS attack. The attacker aims to reduce the performance of the legitimate nodes instead of completely blocking them from data transmission. In effect, it can create transmission delay in UIoT networks.

Hello flooding attack: In a UIoT environment, every node will send HELLO packets to identify its neighbor node. In a hello flooding attack, the adversary node in a UIoT network will send numerous HELLO packets to legitimate nodes to exhaust their battery power. In this case, the adversary node will convince the legitimate node by transmitting the signal with high intensity. Therefore, the legitimate node will assume the adversary node as the neighbor node and transmit data. In effect, it causes power failure and reduces the network lifetime. Figure 11 shows that the malicious node sends HELLO packets with high signal strength to attract the legitimate nodes in UIoT networks [53].

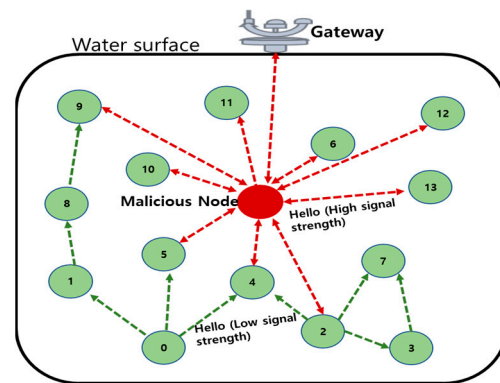


Figure 11. Hello flooding attack in the UIoT environment.

Selective forwarding: In these attacks, the malicious node is located nearby the gateway of UIoT networks. When some packets are detected, the legitimate nodes will find a new route for transmitting the data to the gateway. As shown in Figure 12a, the malicious node can selectively drop some packets before reaching the destination in this attack. In effect, it causes packet loss in UIoT networks.

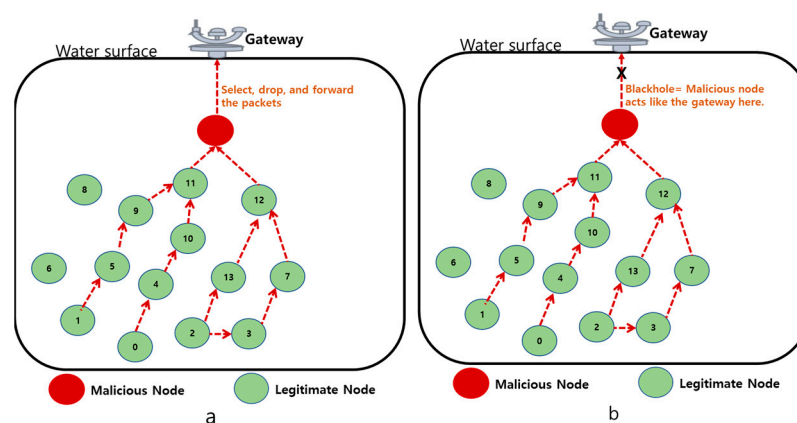


Figure 12. (a) Selective forwarding attack, (b) black hole attack in the UIoT environment.

Blackhole attack: In these attacks, the malicious node acts as the cluster head or gateway to drop the packets while routing. Figure 12b shows that the malicious node can blackhole by modifying or dropping the packets routed from legitimate nodes. The dropped packets are referred to as black hole attacks in UIoT networks.

Gateway block attack: In this attack, the malicious node is located near the gateway and blocks all the data transferred from legitimate nodes to the gateway. In this case, the attacker manages to steal all the routing information sent to the gateway as the destination. In effect, it causes complete packet loss. Therefore, a gateway block attack is referred to as the main threat in UIoT networks.

Misdirection attack: In this attack, the malicious node can be located anywhere in the UIoT network and track the routing path to change the route to the malicious node. In effect, this attack causes packet loss or data transmission delay.

Homing attack: The malicious node observes the traffic in UIoT networks and attacks the most special nodes in UIoT networks, such as cluster head and gateway. Additionally, this attacker can jam or destroy those special nodes using a DoS attack.

Desynchronization attack: This attack disturbs the active connections between the nodes in UIoT networks by sending fake packets. In this case, the fake packets will carry fake sequence numbers to distract the synchronization process between the underwater nodes. In effect, it affects the accuracy in UIoT networks.

Clock skewing attack: In these attacks, the attacker tries to obtain the timestamp information of a legitimate node. Therefore, the time stamp information can be changed in a legitimate node. In effect, it causes a time synchronization problem in UIoT networks.

Data aggregation attack: In these attacks, the attacker tries to aggregate the legitimate node's privacy-based information in UIoT networks. The attacker can steal information such as username, passwords, etc.

4. Q3: What Are the Methodologies Used to Overcome the Challenges in UIoT?

Several methods are proposed to solve the technical and security challenges of UIoT. Some of them provide a general idea, and others give a solution for existing problems. Some of the existing techniques to overcome the UIoT challenges are discussed below.

4.1. Methods to Overcome the Technical Challenges of UIoT

4.1.1. Low Battery Consumption Methods

In [54–64], the existing techniques for solving the battery problem in UIoT are discussed, and some methods are indicated herewith. In [56], Pendergast et al. proposed a powerful and rechargeable module using Panasonic (CGR18650E) to provide sufficient energy, and the experiment result shows that it is reliable and safe in the underwater environment. In [58], Raffaele Guida et al. designed a battery-less underwater node that can recharge via an acoustic signal from a short or long distance. In [59], Guanglin Xing proposed a named data networking (NDN) approach for relay network topology in underwater acoustic sensor networks to identify the node's power consumption in a shallow sea and deep-sea environment. Finally, in [60], Ahmed G, a two-level Redundant Transmission Control (RTC) was proposed to control the communication in underwater acoustic sensor networks, and the performance result shows that energy consumption is lower for the RTC approach.

4.1.2. Memory Management Methods

In [7,65–68], the existing techniques for solving the storage management in UIoT are discussed, and some methods are indicated herewith. In [7], I.F. Akyildiz et al. suggested that underwater sensors need to perform some data caching due to the intermittent underwater channel characteristics. In [65], Zahoor Ali Khan et al. researched Q-learning (QL), comprising of reactive and proactive strategies to reduce the network overhead related to network lifetime. In [66,67] memory management, an essential function to store and retrieve information through smart sensing underwater devices, was studied to solve the challenges of the underwater network management system (U-NMS).

4.1.3. Unreliable Data Transmission Methods

In [68–70], the existing techniques for solving the unreliable data communication in UIoT are discussed, and some methods are indicated herewith. In [68], Li, N et al. show that unreliable channels cause propagation delays. Therefore, three aspects of solving this problem suggested reducing unnecessary routing detection, routing distance between relay nodes and retransmission. In [69], S. Jiang recognized the need for an optimal design to provide reliable end-to-end transmission. Thus, a reliable transmission control was systematically reviewed, focusing on the data link, network and transport layers. Finally, in [70], Fattah S et al. discussed the impact of noise from underwater environments on reliable data transmission, and based on this, link reliability was an essential consideration for data transmission to achieve the rate of high transmission in real-time scenarios.

4.1.4. Noise Modeling Methods

In [71–82], the existing techniques for solving the environmental noise and ambient noise modeling in UIoT are discussed, and some methods are indicated herewith. In [72], Chao Wang et al. designed a PG mixed noise model based on a single-photon avalanche diode (SPAD) in an underwater visible light communication system by considering the

attenuation and turbulence effect. Here, an algorithm for the noise model was also presented. In [76], Bagocius D et al. presented an underwater noise model to identify the noise level of shallow water during different seasons. Finally, in [78], Pennucci et al. provide the conceptual design and describe the effect of using ships in the UIoT environment by providing various shipping noises for noise modeling underwater.

4.1.5. Localization Methods

In [83–86], the existing techniques for solving the localization problem in UIoT are discussed, and some methods are indicated herewith. In [83], T. Islam et al. anticipated that localization is a crucial element in the protocol design given the proposed geographic routing protocols for underwater sensor networks. Suggestively, they resulted in accuracy and coverage of localization as essential factors for performance based on the surveyed centralized and distributed localization algorithms. In addition, P. Liu, B et al. proposed the integrated navigation of the Inertial Navigation System (INS) in AUV with limited doppler velocity log (DVL) to update the depth of the system based on the pressure sensor integrated with AUV [84].

4.1.6. Low-Cost Communication Methods

In [17,87–101], the existing techniques for solving the high-cost issues in UIoT are discussed, and some methods are indicated herewith. In [89], Bridget Benson et al. designed a low-cost acoustic modem to reduce underwater acoustic sensor network cost and power consumption. In [99], Waseem et al. designed a low-cost application to monitor water quality using underwater wireless communication. In [100], Brian R et al. designed and developed a low-cost glider to perform in shallow water, around 3-m depth, 3-m radius and a minimum of 60 h durability. Finally, in [101], Abdillah designed and developed a low-cost coral reef monitoring application for shallow water.

4.1.7. Device Management and Physical Damage Protection Methods

In [102,103], the existing techniques for solving the device management issues in UIoT are discussed, and some methods are indicated herewith. In the case of device management, in ISO/IEC 30140-1, fouling cleaners and housing cases shall be used for cleaning marine wild animals attached to underwater devices, waterproofing and construction of underwater sensor nodes resistant to high water pressures, respectively. In addition, as a functional requirement for underwater device management, identification of available resources and status of the devices are suggested in ISO/IEC 30142. In [26], K. M, D.R. et al. designed and developed the underwater network management system (U-NMS). The proposed system enables automatic software updates and monitoring of underwater devices using fault, configuration, accounting, performance, security and constrained management (FCAPSC) functions of U-NMS for physical damage protection.

4.1.8. Connection and Reconfiguration Methods

In [104–106], the existing techniques for solving the connectivity issues in UIoT are discussed, and some methods are indicated herewith. In [105], L. Furno, a self-reconfiguration algorithm is formulated for underwater robots based on energy heuristics. In [106], a full-duplex, parameter configurable, multiple-user modem is developed and tested to improve the throughput level in the UIoT environment.

4.2. Methods to Overcome the Security Challenges in UIoT

4.2.1. Methods to Prevent DoS Attacks

The existing techniques to prevent DoS attacks in UIoT are discussed herewith. In [107], Martin et al. proposed a cautious calculation that checks the potential DoS attack. This approach breaks down centered and broadcasted DoS attacks to initially distinguish the attack and create pushback alerts or choke the malicious nodes as they enter the UIoT networks. Data entropy is a proportion of the vulnerability related to an

irregular variable. It tends to be deciphered as the normal most limited message length in bits that can send an irregular variable to a recipient [108]. Entropy can be determined by figuring a progression of constant bundles. The entropy esteem gives a depiction of the comparing arbitrary appropriation of these sources IP addresses. The bigger the entropy, the more irregular the source IP. The more modest the entropy, the smaller the dispersion scope of the source IP locations of the parcels, and a few locations have a genuinely high likelihood of an event. The expression for calculating the entropy is shown below:

$$E = - \sum_{k=1}^{Tn} p_k \log_2 p_k$$

Here p_k is the possible outcome probability, Tn is the number of packets analyzed, and E is the entropy.

4.2.2. Methods to Prevent Jamming Attacks

The existing techniques to prevent jamming attacks in UIoT are discussed herewith. In [109], Misra et al. present a shortcoming identification calculation where nodes deliberately trade revelation and affirmative packets. In [110], Bagali et al. present a productive channel task conspire, an original cross-layer plan for helpful correspondence for jamming detection. Finally, in [111], Xiao et al. proposed utilizing the game-hypothetical investigation of sticking to UIoT and proposed a machine learning-based energy management mechanism to adapt to jamming attacks in UIoT networks. The associations between a UIoT and a responsive jamming device are defined as two jamming games.

Exponentially Weighted Moving Average (EWMA) was proposed by Osanaiye et al. [112] as a measurable productive procedure for identifying little changes in time series information. It works by first characterizing an edge that portrays standard conduct before intermittently refreshing the normal of the noticed traffic. The EWMA algorithm can be the countermeasure for jamming attacks. The below expression shows how the EWMA is calculated:

$$x(d) = \lambda.y(d) + (1 - \lambda).x(d - 1) \quad d = 1, 2, 3, \dots N$$

$x(d)$ is the data with moving average time d , λ is the parameter value between 0 and 1, $y(d)$ denotes the signal y at a time ' d ', N is the number of observations in EWMA.

4.2.3. Methods to Prevent Node Compromise Attacks

To defend against node compromise attacks in UIoT networks, a mechanism such as a high-level hardware protection scheme, trustworthiness, data management and configuration management should be adapted for UIoT networks.

4.2.4. Methods to Prevent Sybil Attacks

Message authentication and proper localization mechanisms are necessary to prevent the Sybil attack in the UIoT environment. The existing Sybil attack prevention methods applicable for UIoT networks are explained herewith. In [46], Demirbas et al. proposed the received signal strength indicator (RSSI) based light-weight approach to detect the Sybil attack; this approach can be applicable in UIoT networks. In [47], W. Du et al. proposed a pairwise random key predistribution scheme to secure the communication link that can be used for UIoT networks. Resource-based testing is one of the solutions for Sybil attack prevention in UIoT networks. In [48], Newsome et al. provide an example of resource-based testing. This method can be used in UIoT.

4.2.5. Methods to Prevent Wormhole Attacks

The existing techniques to prevent wormhole attacks in UIoT are discussed herewith. In [49], Gorlatova et al. used the HELLO message based on packet timing analysis to control the wormhole attack, which can be used in UIoT networks. In [50], Kong et al. proposed a two-tire-based localization method to identify the wormhole attack in a short

time in UIoT networks. In [51], Shang-Ming Jen et al. proposed a hop-count-based analysis method to prevent the wormhole attack, which can be applicable in UIoT networks. Finally, in [52], Wang et al. proposed a distributed method to identify the wormhole attack in UIoT networks.

4.2.6. Methods to Prevent Flooding Attacks

The existing techniques to prevent flooding attacks in UIoT are discussed herewith. Bidirectional authentication is necessary to protect the nodes from flooding attacks in UIoT networks. In [53], Prabhjot Kaur et al. proposed a centralized scheme to protect the hello flooding attack that can be used in UIoT networks. In [113], Coutinho et al. proposed a GEDAR, a geographical routing approach that prevents flooding attacks underwater. In the GEDAR approach, the communication is established based on the location information of UIoT nodes.

4.2.7. Methods to Prevent Black-Hole Attacks

The existing techniques to prevent black-hole attacks that can be considered for UIoT are discussed herewith. In [114], a dynamic learning system (DPRAODV) was proposed against black-hole attacks in mobile ad hoc networks. In [115], L. Tamilselvan et al. proposed the cooperative black-hole prevention method using a fidelity table in mobile ad hoc networks. In [116], Hanane Kalkha et al. proposed the tyenHidden Markov Model technique to identify the black-hole attacks in wireless sensor networks.

5. Q4: What Are the Findings Based on the Existing Research Works?

This section highlights the significant findings of this research by reviewing the papers concerning recent trends, technical challenges, privacy and security issues of UIoT. The analysis is provided in Tables 3–5 based on the years from 2010 to 2021, and the results are displayed in Figures 13–15.

Table 3. Systematic analysis on UIoT applications.

Main Clause	Subclause	Paper Count	References Number
Environmental monitoring	Pollution monitoring	3	[117–119]
	Water quality monitoring	11	[120–130]
	Monitoring depth, temperature, pressure, and pH level.	9	[131–139]
	Fish farm and fish growth monitoring	22	[140–161]
Resource exploration	Finding the lost treasure	4	[162–165]
	Underwater object tracking	9	[166–174]
	Natural resource finding (Coral reefs, minerals, manganese, etc.)	13	[175–186]
Disaster prevention	Earthquakes, Tsunami warning system	7	[187–193]
	Landslide detection and prevention	9	[194–202]
Naval applications	Submarine detection	2	[203,204]
	Mine detection	4	[205–208]
	Surveillance	3	[209–211]
Others	Aquathlon (Scuba-diving, underwater hockey, underwater wrestling, etc.)	6	[212–217]
	Navigation assistance	9	[218–226]
	Localization	15	[85,86,227–239]

Table 4. Systematic analysis of the technical challenges in UIoT networks.

Problems	Solutions and Effective Methods	Paper Count	References Number
Transmission issues	Methods to preventing path loss and data loss in UIoT networks.	17	[240–256]
Environmental issues	Methods to solve unreliable channel conditions in UIoT networks.	10	[257–266]
	Methods to solve limited resources in UIoT networks.	15	[26,54–64,267–269]
Insecure environment issues	Methods used to support trust management, security management, hardware protection, etc., in UIoT networks.	19	[42,107,113,270–285]
Cost issues	Lost cost design approaches for UIoT networks	15	[87–101]
Channel noise issues	Methods to prevent ambient noise, mammals noise, other environmental noise in UIoT networks.	12	[71–82]
	Methods to predict noise level in UIoT networks.		
Damages in UIoT devices	Methods to prevent internal or external damages of UIoT devices.	9	[26,286–292]
Device or network configuration issues	Methods supporting self-configuration or auto-configuration mechanism for devices in UIoT networks.	4	[26,104–106]

Table 5. Systematic analysis of security issues and management in UIoT networks.

Main Clause	Subclause	Paper Count	References Number
Key focus on security attacks and management	Papers discussing privacy and security attacks on UIoT networks.	10	[271,293–301]
	Papers discussing attack prevention methods and management in UIoT networks.	19	[42,107,113,270–285]
	Papers discussing message authentication techniques in UIoT networks.	6	[42,302–306]
	Papers discussing localization security in UIoT networks.	10	[42,271,307–314]
	Papers discussing key management in UIoT networks.	6	[315–320]
	Papers discussing information management in UIoT networks.	3	[78,321,322]
	Papers discussing trust management in UIoT networks.	19	[273,275,276,314,323–337]

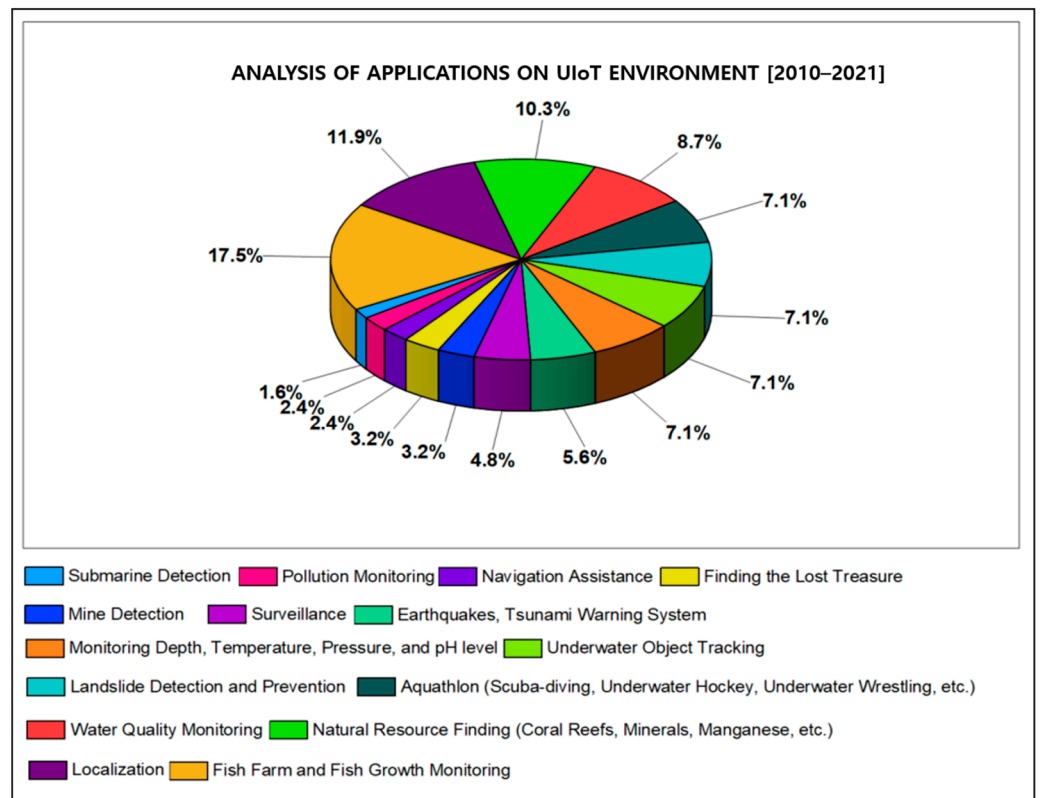


Figure 13. Results based on the systematic analysis of UIoT applications.

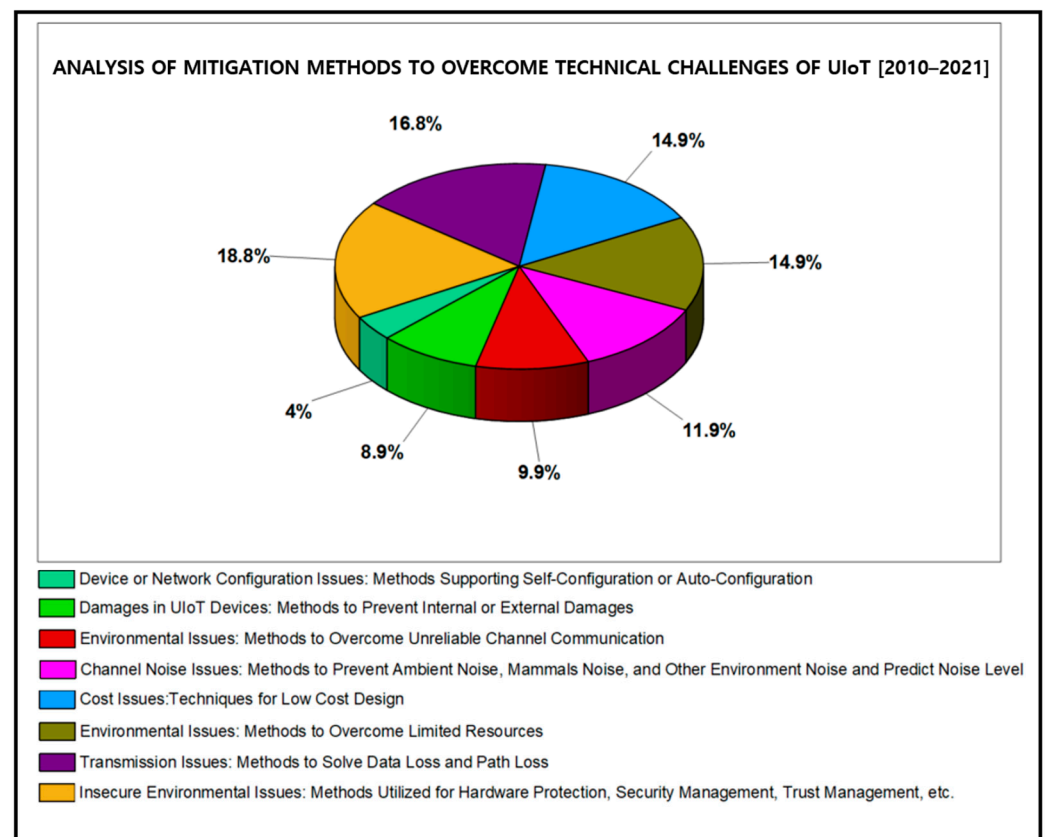


Figure 14. Results based on the systematic analysis of mitigation methods to overcome the technical challenges in UIoT.

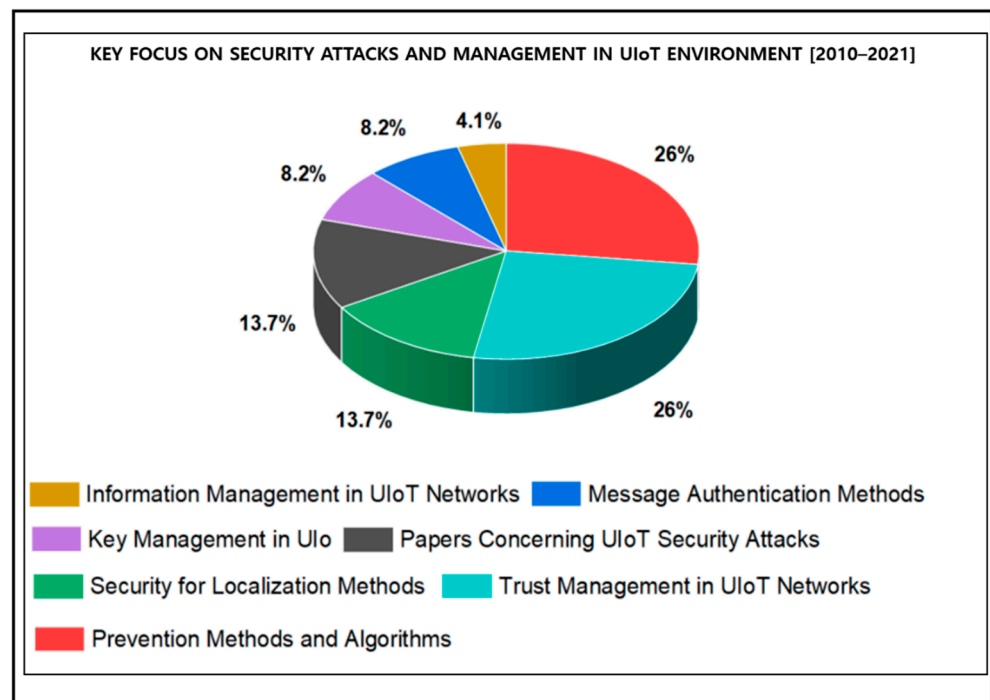


Figure 15. Results based on the systematic analysis of security attacks and management.

6. Q5: Future Direction

According to the results obtained from the current research study conducted based on queries in Table 1, the suggestion for the future direction of UIoT is discussed in the Sections beneath:

6.1. Build Hybrid Communication Models for Future UIoT

Based on the research study in Section 2, acoustic, optical, RF and MI are the communication technologies used in the UIoT environment. As shown in Table 2, each medium has its advantages and disadvantages. To overcome the technical challenges discussed in Section 3.2, it is necessary to port multi-medium (hybrid) communication technology in UIoT [21]. The multi-medium communication technology can improve the transmission speed, increase the battery life, and deliver reliable data transmission in UIoT.

6.2. Build Underwater Automatic Battery Recharging Module for Future UIoT

Based on the research study in Section 3, the devices or nodes in the UIoT environment have limited resources. Additionally, it is difficult to recharge in a constrained underwater environment. In effect, it reduces battery life and network lifetime if any one of the nodes is dead. In [267], Yongil Kim et al. introduced a metal-free sodium-seawater battery (Na-SWB). In [268], J Cho et al. proposed a battery degradation prediction and power optimization mechanism for surface buoys based on sea batteries. In [269], Moon Son et al. proposed a rechargeable seawater battery (SWB) mechanism that produces energy from seawater. Finally, in [338], the Miresearch group developed battery-free sensor nodes for underwater exploration. Therefore, to solve the battery issues in UIoT, it is necessary to build an undersea battery or an automatic recharging mechanism or deploy battery-free nodes.

6.3. Build Standard Security Models for Future UIoT

Sections 3.3 and 3.4 describes the security issues and possible security attacks in UIoT networks. This research study shows that it is necessary to build a robust security model that includes high-level security architecture, confidentiality, integrity, availability, quality

of service (QoS), etc., to protect the UIoT nodes from attacks such as DoS attacks, routing, jamming attacks and so on.

6.4. Build Privacy Models for Future UIoT

Based on the discussion in Section 3.3.2, it is necessary to handle privacy issues in essential applications of UIoT such as diver networks, naval applications, tracking applications, etc. However, since the terrestrial privacy models are heavyweight, it is difficult to apply in UIoT environments. Moreover, as discussed in Section 3.4.1, it is necessary to consider data privacy, device privacy and location privacy in UIoT. Hence, it is necessary to build lightweight privacy models for UIoT systems by adapting privacy models in terrestrial networks such as k-anonymity, l-diversity, t-closeness and differential privacy.

7. Conclusions

This paper reviews existing research papers based on recent trends, applications, challenges, security and privacy issues of UIoT. Additionally, the possible solutions to overcome the technical challenges, privacy and security issues are discussed based on the systematic studies. The research goals are developed in Table 1, including four research queries from Q1 to Q4, and the solutions are provided under Sections 2–5. Section 2 provides the survey based on the latest articles, the recently developed applications and the existing communication technologies of UIoT. Section 3 describes the existing challenges of UIoT systems, including technical challenges, privacy and security attacks in UIoT networks. Section 4 provides the methodology to overcome the challenges described in Section 3. In Section 4, the significant findings are highlighted by reviewing the total number of papers concerning UIoT applications, technical challenges, privacy and security issues of UIoT. Finally, the future direction in Section 5 shows that the hybrid communication technologies in UIoT that include acoustic, optical, IR and MI medium can overcome the technical challenges of the UIoT system. Therefore, further research needs hybrid modem technology to support fast, reliable and low power consumption-based communication in UIoT. Moreover, in the future, the privacy and security issues can be solved by building standard security models and security architecture for UIoT. Furthermore, it is necessary to build battery-free sensors or undersea energy models for energy storage and automatic recharging in the future.

Author Contributions: Funding acquisition, S.-G.K.; Investigation, S.-H.P.; Methodology, D.R.K.M. and E.K.; Project administration, S.-H.P. and S.-G.K.; Resources, D.R.K.M. and S.-H.Y.; Supervision, S.-H.P.; Visualization, S.-Y.S.; Writing—original draft, D.R.K.M. and E.K.; Writing—review and editing, D.R.K.M., S.-G.K., E.K. and S.-H.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research was a part of the project titled “Development of the wide-area underwater mobile communication systems”, funded by the Ministry of Oceans and Fisheries, Korea (NTIS No. 1525010926).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. NOAA, America’s Coastal & Ocean Agency. How Much Water Is in the Ocean? Available online: <https://oceanservice.noaa.gov/facts/oceanwater.html> (accessed on 28 October 2021).
2. Awan, K.M.; Shah, P.A.; Iqbal, K.; Gillani, S.; Ahmad, W.; Nam, Y. Underwater Wireless Sensor Networks: A Review of Recent Issues and Challenges. *Wirel. Commun. Mob. Comput.* **2019**, *2019*, 6470359. [CrossRef]
3. Yang, G.; Dai, L.; Si, G.; Wang, S.; Wang, S. Challenges and Security Issues in Underwater Wireless Sensor Networks. *Procedia Comput. Sci.* **2019**, *147*, 210–216. [CrossRef]

4. Gussen, C.M.G.; Diniz, P.S.R.; Campos, M.L.R.; Martins, W.A.; Costa, F.M.; Gois, J.N. A Survey of Underwater Wireless Communication Technologies. *J. Commun. Inf. Syst.* **2016**, *31*, 242–255. [[CrossRef](#)]
5. Zoksimovski, A.; Sexton, D.; Stojanovic, M.; Rappaport, C. Underwater electromagnetic communications using conduction—Channel characterization. *Ad Hoc Netw.* **2015**, *34*, 42–51. [[CrossRef](#)]
6. Rhodes, M. Electromagnetic propagation in seawater and its value in military systems. In Proceedings of the Conference of System Engineering for Autonomous Systems from the Defense Technology Centre (SEAS DTC'07), Edinburgh, UK, 2007; pp. 1–6.
7. Akyildiz, I.F.; Pompili, D.; Melodia, T. Underwater acoustic sensor networks: Research challenges. *Ad Hoc Netw.* **2005**, *3*, 257–279. [[CrossRef](#)]
8. Akyildiz, I.F.; Pompili, D.; Melodia, T. Challenges for efficient communication in underwater acoustic sensor networks. *ACM Sigbed Rev.* **2004**, *1*, 3–8. [[CrossRef](#)]
9. Chitre, M.; Shahabudeen, S.; Freitag, L.; Stojanovic, M. Recent advances in underwater acoustic communications & networking. In Proceedings of the OCEANS 2008, Quebec City, QC, Canada, 15–18 September 2008; pp. 1–10.
10. Kumar, P.; Trivedi, V.K.; Kumar, P. Recent trends in multicarrier underwater acoustic communications. In Proceedings of the Underwater Technology (UT), Chennai, India, 23–25 February 2015; pp. 1–8.
11. Spagnolo, G.S.; Cozzella, L.; Leccese, F. Underwater Optical Wireless Communications: Overview. *Sensors* **2020**, *20*, 2261. [[CrossRef](#)] [[PubMed](#)]
12. Zeng, Z.; Fu, S.; Zhang, H.; Dong, Y.; Cheng, J. A Survey of Underwater Optical Wireless Communications. *IEEE Commun. Surv. Tutor.* **2016**, *19*, 204–238. [[CrossRef](#)]
13. Kaushal, H.; Kaddoum, G. Underwater Optical Wireless Communication. *IEEE Access* **2016**, *4*, 1518–1547. [[CrossRef](#)]
14. Murgod, T.R.; Sundaram, S.M. Survey on underwater optical wireless communication: Perspectives and challenges. *Indones. J. Electr. Eng. Comput. Sci.* **2019**, *13*, 138–146. [[CrossRef](#)]
15. Kumar, M.; Rani, M. A Design of Novel Hybrid Optoacoustic Modem for Underwater Communication. *Int. J. Innov. Technol. Explor. Eng. (IJITEE)* **2019**, *8*, 3383–3389.
16. Farr, N.; Bowen, A.; Ware, J.; Pontbriand, C.; Tivey, M. An integrated, underwater optical /acoustic communications system. In Proceedings of the OCEANS'10 IEEE SYDNEY, Sydney, NSW, Australia, 24–27 May 2010; pp. 1–6. [[CrossRef](#)]
17. Tennenbaum, A.; Dyakiw, M.; Cui, J.-H.; Peng, Z. Application of Low Cost Optical Communication Systems to Underwater Acoustic Networks. In Proceedings of the OCEANS'10 IEEE SYDNEY, Sydney, NSW, Australia, 24–27 May 2010; pp. 1–6. [[CrossRef](#)]
18. Han, S.; Noh, Y.; Liang, R.; Chen, R.; Cheng, Y.-J.; Gerla, M. Evaluation of underwater optical-acoustic hybrid network. *China Commun.* **2014**, *11*, 49–59. [[CrossRef](#)]
19. Johnson, L.J.; Green, R.J.; Leeson, M.S. Hybrid underwater optical/acoustic link design. In Proceedings of the 2014 16th International Conference on Transparent Optical Networks (ICTON), Graz, Austria, 6–10 July 2014; pp. 1–4. [[CrossRef](#)]
20. Gauni, S.; Manimegalai, C.T.; Krishnan, K.M.; Shreeram, V.; Arvind, V.V.; Srinivas, T.V.N. Design and Analysis of Co-operative Acoustic and Optical Hybrid Communication for Underwater Communication. *Wirel. Pers. Commun.* **2021**, *117*, 561–575. [[CrossRef](#)]
21. Delphin Raj, K.M.; Yum, S.-H.; Ko, E.; Shin, S.-Y.; Namgung, J.-I.; Park, S.-H. Multi-Media and Multi-Band Based Adaptation Layer Techniques for Underwater Sensor Networks. *Appl. Sci.* **2019**, *9*, 3187.
22. Raj, M.K.; Yum, S.-H.; Lee, J.; Ko, E.; Shin, S.-Y.; Park, S.-H. Handover Mechanism Based on Underwater Hybrid Software-Defined Modem in Advanced Diver Networks. *CMC-Comput. Mater. Contin.* **2022**, *70*, 5721–5743.
23. Kao, C.-C.; Lin, Y.-S.; Wu, G.-D.; Huang, C.-J. A Comprehensive Study on the Internet of Underwater Things: Applications, Challenges, and Channel Models. *Sensors* **2017**, *17*, 1477. [[CrossRef](#)] [[PubMed](#)]
24. Felemban, E.; Shaikh, F.K.; Qureshi, U.M.; Sheikh, A.A.; Bin Qaisar, S. Underwater Sensor Network Applications: A Comprehensive Survey. *Int. J. Distrib. Sens. Netw.* **2015**, *11*, 1–14. [[CrossRef](#)]
25. Hollinger, G.A.; Mitra, U.; Sukhatme, G.S. Active Classification: Theory and Application to Underwater Inspection. In *Robotics Research*; Springer Tracts in Advanced Robotics; Springer: Cham, Switzerland, 2016; Volume 100, pp. 95–110. [[CrossRef](#)]
26. Delphin Raj, K.M.; Lee, J.; Yum, S.-H.; Ko, E.; Shin, S.-Y.; Namgung, J.-I.; Park, S.-H. Underwater Network Management System in Internet of Underwater Things: Open Challenges, Benefits, and Feasible Solution. *Electronics* **2020**, *9*, 1142. [[CrossRef](#)]
27. Qiu, T.; Zhao, Z.; Zhang, T.; Chen, C.; Chen, C. Underwater Internet of Things in Smart Ocean: System Architecture and Open Issues. *IEEE Trans. Ind. Inform.* **2019**, *16*, 4297–4307. [[CrossRef](#)]
28. Kong, J.; Ji, Z.; Wang, W.; Gerla, M.; Bagrodia, R.; Bhargava, B. Low-cost attacks against packet delivery, localization and time synchronization services in underwater sensor networks. In Proceedings of the 4th ACM Workshop on Wireless Security, Cologne, Germany, 2 September 2005.
29. Das, A.; Thampi, S. Secure communication in mobile underwater wireless sensor networks. In Proceedings of the 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Shenzhen, China, 10–13 August 2015.
30. Ding, Y.; Li, N.; Song, B.; Yang, Y. The mobile node deployment algorithm for underwater wireless sensor networks. In Proceedings of the 2017 Chinese Automation Congress (CAC), Jinan, China, 20–22 October 2017; pp. 456–460. [[CrossRef](#)]
31. Luo, J.; Yang, Y.; Wang, Z.; Chen, Y.; Wu, M. A Mobility-Assisted Localization Algorithm for Three-Dimensional Large-Scale UWSNs. *Sensors* **2020**, *20*, 4293. [[CrossRef](#)]

32. Patel, K.K.; Patel, S.M. Internet of things (IoT): Definition, characteristics, architecture, enabling technologies, application and future challenges. *Int. J. Eng. Sci. Comput.* **2016**, *6*, 6122–6131.
33. García, D.R.; Montiel-Nelson, J.; Bautista, T.; Sosa, J. A New Method for Gaining the Control of Standalone Underwater Sensor Nodes Based on Power Supply Sensing. *Sensors* **2021**, *21*, 4660. [[CrossRef](#)] [[PubMed](#)]
34. Alazab, M.; Lakshmana, K.; Reddy, G.T.; Pham, Q.-V.; Maddikunta, P.K.R. Multi-objective cluster head selection using fitness averaged rider optimization algorithm for IoT networks in smart cities. *Sustain. Energy Technol. Assess.* **2021**, *43*, 100973. [[CrossRef](#)]
35. Bhattacharya, S.; Kumar, P.; Meenakshisundaram, I.; Gadekallu, T.R.; Sharma, S.; Alkahtani, M.; Abidi, M.H. Deep Neural Networks Based Approach for Battery Life Prediction. *CMC-Comput. Mater. Contin.* **2021**, *69*, 2599–2615. [[CrossRef](#)]
36. Qadar, R.; Bin Qaim, W.; Nurmi, J.; Tan, B. Effects of Multipath Attenuation in the Optical Communication-Based Internet of Underwater Things. *Sensors* **2020**, *20*, 6201. [[CrossRef](#)] [[PubMed](#)]
37. Hwang, H.Y. Analysis of Throughput and Delay for an Underwater Multi-DATA Train Protocol with Multi-RTS Reception and Block ACK. *Sensors* **2020**, *20*, 6473. [[CrossRef](#)]
38. Kim, S.H.; Choi, B.K.; Kim, B.-N. Correlation between Underwater Noise and Sea Level at Jeodo Ocean Research Station. *J. Mar. Sci. Eng.* **2020**, *9*, 1. [[CrossRef](#)]
39. Jiang, S. On Securing Underwater Acoustic Networks: A Survey. *IEEE Commun. Surv. Tutor.* **2018**, *21*, 729–752. [[CrossRef](#)]
40. Misra, S.; Mondal, A.; Mondal, A. DATUM: Dynamic Topology Control for Underwater Wireless Multimedia Sensor Networks. In Proceedings of the 2019 IEEE Wireless Communications and Networking Conference (WCNC), Marrakesh, Morocco, 15–18 April 2019; pp. 1–6. [[CrossRef](#)]
41. Ullah, I.; Chen, J.; Su, X.; Esposito, C.; Choi, C. Localization and Detection of Targets in Underwater Wireless Sensor Using Distance and Angle Based Algorithms. *IEEE Access* **2019**, *7*, 45693–45704. [[CrossRef](#)]
42. Dini, G.; Duca, A.L. A Secure Communication Suite for Underwater Acoustic Sensor Networks. *Sensors* **2012**, *12*, 15133–15158. [[CrossRef](#)]
43. Khanam, S.; Bin Ahmedy, I.; Idris, M.Y.I.; Jaward, M.H.; Sabri, A.Q.B.M. A Survey of Security Challenges, Attacks Taxonomy and Advanced Countermeasures in the Internet of Things. *IEEE Access* **2020**, *8*, 219709–219743. [[CrossRef](#)]
44. Alsamani, B.; Lahza, H. A taxonomy of IoT: Security and privacy threats. In Proceedings of the 2018 International Conference on Information and Computer Technologies (ICICT), DeKalb, IL, USA, 23–25 March 2018; pp. 72–77. [[CrossRef](#)]
45. Raymond, D.R.; Midkiff, S.F. Denial-of-service in wireless sensor networks: Attacks and defenses. *IEEE Pervasive Comput.* **2008**, *7*, 74–81. [[CrossRef](#)]
46. Demirbas, M.; Song, Y. An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks. In Proceedings of the 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks, Buffalo-Niagara Falls, NY, USA, 26–29 June 2006; pp. 564–570. [[CrossRef](#)]
47. Du, W.; Deng, J.; Han, Y.S.; Varshney, P.K. A pairwise key predistribution scheme for wireless sensor networks. *ACM Trans. Inf. Syst. Secur.* **2005**, *8*, 228–258. [[CrossRef](#)]
48. Newsome, J.; Shi, E.; Song, D.; Perrig, A. The Sybil attack in sensor networks: Analysis & defences. In Proceedings of the Third International Symposium on Information Processing in Sensor Networks, Berkeley, CA, USA, 27 April 2004; pp. 259–268.
49. Gorlatova, M.A.; Mason, P.C.; Wang, M.; Lamont, L.; Liscano, R. Detecting Wormhole Attacks in Mobile Ad Hoc Networks through Protocol Breaking and Packet Timing Analysis. In Proceedings of the MILCOM 2006—2006 IEEE Military Communications Conference, Washington, DC, USA, 23–25 October 2006; pp. 1–7. [[CrossRef](#)]
50. Kong, J.; Ji, Z.; Wang, W.; Gerla, M.; Bagrodia, R. *On Wormhole Attacks in Under-Water Sensor Networks: A Two-Tier Localization Approach*; Technical Report; UCLA Computer Science Department: Los Angeles, CA, USA, 2004.
51. Jen, S.-M.; Laih, C.-S.; Kuo, W.-C. A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET. *Sensors* **2009**, *9*, 5022–5039. [[CrossRef](#)] [[PubMed](#)]
52. Wang, W.; Kong, J.; Bhargava, B.; Gerla, M. Visualisation of wormholes in underwater sensor networks: A distributed approach. *Int. J. Secur. Netw.* **2008**, *3*, 10–23. [[CrossRef](#)]
53. Kaur, P.; Gurm, J.S. Detect and prevent HELLO FLOOD Attack using Centralized technique in WSN. *Int. J. Comput. Sci. Eng. Technol.* **2016**, *7*, 379–381.
54. Hyakudome, T.; Yoshida, H.; Ishibashi, S.; Sawa, T.; Nakamura, M. Development of advanced lithium-ion battery for underwater vehicle. In Proceedings of the 2011 IEEE Symposium on Underwater Technology and Workshop on Scientific Use of Submarine Cables and Related Technologies, Tokyo, Japan, 5–8 April 2011.
55. Lin, M.; Li, D.; Yang, C. Design of an ICPT system for battery charging applied to underwater docking systems. *Ocean. Eng.* **2017**, *145*, 373–381. [[CrossRef](#)]
56. Pendergast, D.R.; DeMauro, E.P.; Fletcher, M.; Stimson, E.; Mollendorf, J.C. A rechargeable lithium-ion battery module for underwater use. *J. Power Sources* **2011**, *196*, 793–800. [[CrossRef](#)]
57. Jin, L.; (David) Huang, D. A slotted CSMA based reinforcement learning approach for extending the lifetime of underwater acoustic wireless sensor networks. *Comput. Commun.* **2013**, *36*, 1094–1099. [[CrossRef](#)]
58. Guida, R.; Demirors, E.; Dave, N.; Melodia, T. Underwater Ultrasonic Wireless Power Transfer: A Battery-less Platform for the Internet of Underwater Things. *IEEE Trans. Mob. Comput.* **2020**, 1–12. Available online: <https://ieeexplore.ieee.org/document/9217956> (accessed on 6 December 2021). [[CrossRef](#)]

59. Xing, G.; Chen, Y.; He, L.; Su, W.; Hou, R.; Li, W.; Zhang, C.; Chen, X. Energy Consumption in Relay Underwater Acoustic Sensor Networks for NDN. *IEEE Access* **2019**, *7*, 42694–42702. [[CrossRef](#)]
60. Ahmed, G.; Zhao, X.; Fareed, M.M.S.; Fareed, M.Z. An Energy-Efficient Redundant Transmission Control Clustering Approach for Underwater Acoustic Networks. *Sensors* **2019**, *19*, 4241. [[CrossRef](#)] [[PubMed](#)]
61. Hou, R.; He, L.; Hu, S.; Luo, J. Energy-Balanced Unequal Layering Clustering in Underwater Acoustic Sensor Networks. *IEEE Access* **2018**, *6*, 39685–39691. [[CrossRef](#)]
62. Raza, W.; Ma, X.; Ali, A.; Shah, Z.A.; Mehdi, G. An implementation of partial transmit sequences to design energy efficient underwater acoustic OFDM communication system. *arXiv* **2020**, arXiv:2007.01273.
63. Wang, C.; Zhao, X.; Zhao, Z.; Xu, W.; Cui, L. Software-Defined Multimodal Underwater Wireless Sensor Network Platform Powered by Seawater Battery. In Proceedings of the China Conference on Wireless Sensor Networks, Dunhuang, China, 18–21 September 2020; Springer: Singapore, 2020.
64. Nguyen, C.T.; Nguyen, M.T.; Mai, V.V.; Nguyen, C.T. Reliable Transmission for Underwater Optical Wireless Communication Networks with Energy Harvesting. In Proceedings of the 2020 IEEE Eighth International Conference on Communications and Electronics (ICCE), Phu Quoc Island, Vietnam, 13–15 January 2021.
65. Khan, Z.A.; Karim, O.A.; Abbas, S.; Javaid, N.; Bin Zikria, Y.; Tariq, U. Q-learning based energy-efficient and void avoidance routing protocol for underwater acoustic sensor networks. *Comput. Netw.* **2021**, *197*, 108309. [[CrossRef](#)]
66. Urunov, K.; Shin, S.-Y.; Park, S.-H.; Lim, Y.K. Analysis of the network management system with constrained under-water devices. In Proceedings of the Symposium of the Korean Institute of Communications and Information Sciences, Seoul, Korea, 21–23 June 2017.
67. Urunov, K.; Shin, S.-Y.; Namgung, J.-I.; Park, S.-H. High-Level architectural design of management system for the in-ternet of underwater things. In Proceedings of the 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN), Prague, Czech Republic, 3–6 July 2018; pp. 326–331.
68. Li, N.; Martínez, J.-F.; Chaus, J.M.M.; Eckert, M. A Survey on Underwater Acoustic Sensor Network Routing Protocols. *Sensors* **2016**, *16*, 414. [[CrossRef](#)]
69. Jiang, S. On Reliable Data Transfer in Underwater Acoustic Networks: A Survey From Networking Perspective. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 1036–1055. [[CrossRef](#)]
70. Fattah, S.; Gani, A.; Ahmedy, I.; Idris, M.Y.I.; Hashem, I.A.T. A Survey on Underwater Wireless Sensor Networks: Requirements, Taxonomy, Recent Advances, and Open Research Challenges. *Sensors* **2020**, *20*, 5393. [[CrossRef](#)] [[PubMed](#)]
71. Lloyd, T.P.; Turnock, S.R.; Humphrey, V.F. Modelling techniques for underwater noise generated by tidal turbines in shallow waters. In Proceedings of the International Conference on Offshore Mechanics and Arctic Engineering, Rotterdam, The Netherlands, 19–24 June 2011; pp. 777–785. [[CrossRef](#)]
72. Wang, C.; Yu, H.-Y.; Zhu, Y.-J.; Wang, T. Blind Detection for SPAD-Based Underwater VLC System Under P-G Mixed Noise Model. *IEEE Commun. Lett.* **2017**, *21*, 2602–2605. [[CrossRef](#)]
73. Merchant, N.D.; Brookes, K.L.; Faulkner, R.; Bicknell, A.W.J.; Godley, B.J.; Witt, M. Underwater noise levels in UK waters. *Sci. Rep.* **2016**, *6*, 36942. [[CrossRef](#)]
74. Bagočius, D.; Naršcius, A. Simplistic underwater ambient noise modelling for shallow coastal areas: Lithuanian area of the Baltic Sea. *Ocean. Eng.* **2018**, *164*, 521–528. [[CrossRef](#)]
75. Bagocius, D.; Aleksas, N. Underwater noise level predictions of ammunition explosions in the shallow area of Lithuanian Baltic Sea. *Environ. Pollut.* **2019**, *252*, 1311–1317. [[CrossRef](#)]
76. Kellett, P.; Turan, O.; Incecik, A. A study of numerical ship underwater noise prediction. *Ocean. Eng.* **2013**, *66*, 113–120. [[CrossRef](#)]
77. Magnier, C.; Gervaise, C. Reciprocal modelling between the underwater ambient noise and the coastal maritime traffic density in the Calvi bay. *Proc. Meet. Acoust.* **2019**, *37*, 070006. [[CrossRef](#)]
78. Pennucci, G.; Jiang, Y.-M. Extracting Acoustic Source Information of Shipping Noise for Dynamic Ambient Noise Modelling. *J. Shipp. Ocean. Eng.* **2018**, *8*, 10–20. [[CrossRef](#)]
79. Jalkanen, J.-P.; Johansson, L.; Liefvendahl, M.; Bensow, R.; Sigray, P.; Östberg, M.; Karasalo, I.; Andersson, M.; Peltonen, H.; Pajala, J. Modelling of ships as a source of underwater noise. *Ocean. Sci.* **2018**, *14*, 1373–1383. [[CrossRef](#)]
80. Pan, C.; Jia, L.; Cai, R.; Ding, Y. Modeling and simulation of channel for underwater communication network. *Int. J. Innov. Comput. Inf. Control.* **2012**, *8*, 2149–2156.
81. Gholipour, A.; Zakeri, B.; Mafinezhad, K. Non-stationary additive noise modelling in direction-of-arrival estimation. *IET Commun.* **2016**, *10*, 2054–2059. [[CrossRef](#)]
82. Roul, S.; Kumar, C.; Das, A. Ambient noise estimation in territorial waters using AIS data. *Appl. Acoust.* **2019**, *148*, 375–380. [[CrossRef](#)]
83. Islam, T.; Park, S.-H. A Comprehensive Survey of the Recently Proposed Localization Protocols for Underwater Sensor Networks. *IEEE Access* **2020**, *8*, 179224–179243. [[CrossRef](#)]
84. Liu, P.; Wang, B.; Deng, Z.; Fu, M. INS/DVL/PS Tightly Coupled Underwater Navigation Method With Limited DVL Measurements. *IEEE Sens. J.* **2018**, *18*, 2994–3002. [[CrossRef](#)]
85. Carroll, P.; Mahmood, K.; Zhou, S.; Zhou, H.; Xu, X.; Cui, J.-H. On-Demand Asynchronous Localization for Underwater Sensor Networks. *IEEE Trans. Signal. Process.* **2014**, *62*, 3337–3348. [[CrossRef](#)]
86. Das, A.P.; Thampi, S.M. Fault-resilient localization for underwater sensor networks. *Ad Hoc Netw.* **2017**, *55*, 132–142. [[CrossRef](#)]

87. Benson, B.; Li, Y.; Faunce, B.; Domond, K.; Kimball, D.; Schurgers, C.; Kastner, R. Design of a Low-Cost Underwater Acoustic Modem. *IEEE Embed. Syst. Lett.* **2010**, *2*, 58–61. [CrossRef]
88. Song, Y. Underwater Acoustic Sensor Networks with Cost Efficiency for Internet of Underwater Things. *IEEE Trans. Ind. Electron.* **2020**, *68*, 1707–1716. [CrossRef]
89. Benson, B.; Li, Y.; Kastner, R.; Faunce, B.; Domond, K.; Kimball, D.; Schurgers, C. Design of a low-cost, underwater acoustic modem for short-range sensor networks. In Proceedings of the OCEANS'10 IEEE SYDNEY, Sydney, NSW, Australia, 24–27 May 2010.
90. Cario, G.; Casavola, A.; Lupia, M.; Rosace, C. SeaModem: A low-cost underwater acoustic modem for shallow water communication. In Proceedings of the OCEANS 2015—Genova, Genova, Italy, 18–21 May 2015. [CrossRef]
91. Mitchell, B.; Wilkening, E.; Mahmoudian, N. Low cost underwater gliders for littoral marine research. In Proceedings of the American Control Conference (ACC), Seattle, WA, USA, 17–19 June 2013; pp. 1412–1417.
92. Fischell, E.M.; Kroo, A.R.; O'Neill, B.W. Single-hydrophone low-cost underwater vehicle swarming. *IEEE Robot. Autom. Lett.* **2019**, *5*, 354–361. [CrossRef]
93. Sanchez, A.; Blanc, S.; Yuste, P.; Serrano, J.J. A low cost and high efficient acoustic modem for underwater sensor networks. In Proceedings of the OCEANS 2011 IEEE—Spain, Santander, Spain, 6–9 June 2011. [CrossRef]
94. Zia, M.Y.I.; Otero, P.; Poncela, J. Design of a low-cost modem for short-range under-water acoustic communications. *Wirel. Pers. Commun.* **2018**, *101*, 375–390. [CrossRef]
95. Pinto, D.; Viana, S.S.; Nacif, L.F.M.; Vieira, M.A.M.; Vieira, A.B.; Fernandes, A.O. HydroNode: A low cost, energy efficient, multi purpose node for underwater sensor networks. In Proceedings of the 37th Annual IEEE Conference on Local Computer Networks, Clearwater Beach, FL, USA, 22–25 October 2012.
96. Siregar, S.; Sani, M.I.; Kurnia, M.M.; Hasbiallyh, D. Low-cost communication system for explorer-class underwater remotely operated vehicle. *TELKOMNIKA (Telecommun. Comput. Electron. Control.)* **2019**, *17*, 593–600. [CrossRef]
97. Ji, Z.; Fu, Y.; Li, J.; Zhao, Z.; Mai, W. Photoacoustic Communication from the Air to Underwater Based on Low-Cost Passive Relays. *IEEE Commun. Mag.* **2021**, *59*, 140–143. [CrossRef]
98. Shang, G.-Y.; Feng, Z.-P.; Lian, L. A low-cost testbed of underwater mobile sensing network. *J. Shanghai Jiaotong Univ. (Sci.)* **2011**, *16*, 502–507. [CrossRef]
99. Waseem, M.H.; Alamzeb, M.; Mustafa, B.; Malik, F.; Shakir, M.; Jhan, M.A. Design of a low-cost underwater wireless sensor network for water quality monitoring. *IETE J. Res.* **2013**, *59*, 523–534. [CrossRef]
100. Page, B.R.; Ziaefard, S.; Pinar, A.J.; Mahmoudian, N. Highly Maneuverable Low-Cost Underwater Glider: Design and Development. *IEEE Robot. Autom. Lett.* **2016**, *2*, 344–349. [CrossRef]
101. Abdillah, A.F.; Berlian, M.H.; Panduman, Y.Y.F.; Akbar, M.A.W.; Afifah, M.A.; Tjahjono, A.; Sukaridhoto, S.; Sasaki, S. Design and development of low cost coral monitoring system for shallow water based on internet of underwater things. *J. Telecommun. Electron. Comput. Eng. (JTEC)* **2017**, *9*, 97–101.
102. ISO/IEC 30140-1. Information Technology—Underwater Acoustic Sensor Network (UWASN)—Part 1: Overview and Requirements. Available online: <https://www.iso.org/standard/53260.html> (accessed on 28 October 2021).
103. ISO/IEC 30142. Internet of Things (IoT)—Underwater Acoustic Sensor Network (UWASN)—Network Management System Overview and Requirements. Available online: <https://www.iso.org/standard/53262.html> (accessed on 28 October 2021).
104. Islam, J.; Ho, M.; Sattar, J. Dynamic Reconfiguration of Mission Parameters in Underwater Human-Robot Collaboration. In Proceedings of the 2018 IEEE International Conference on Robotics and Automation (ICRA), Brisbane, QLD, Australia, 21–25 May 2018; pp. 1–8. [CrossRef]
105. Furno, L.; Blanke, M.; Galeazzi, R.; Christensen, D.J. Self-reconfiguration of modular underwater robots using an energy heuristic. In Proceedings of the 2017 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), Vancouver, BC, Canada, 24–28 September 2017; pp. 6277–6284. [CrossRef]
106. Qiao, G.; Liu, S.; Sun, Z.; Zhou, F. Full-duplex, multi-user and parameter reconfigurable under-water acoustic communication modem. In Proceedings of the 2013 OCEANS—San Diego, San Diego, CA, USA, 23–27 September 2013; pp. 1–8. [CrossRef]
107. Martin, R.; Rajasekaran, S. Data centric approach to analyzing security threats in Underwater Sensor Networks. In Proceedings of the OCEANS 2016 MTS/IEEE Monterey, Monterey, CA, USA, 19–23 September 2016; pp. 1–6. [CrossRef]
108. Dong, Q.; Ai, X.; Cao, G.; Zhang, Y.; Wang, X. Study on risk assessment of water security of drought periods based on entropy weight methods. *Kybernetes* **2010**, *39*, 864–870. [CrossRef]
109. Misra, S.; Dash, S.; Khatua, M.; Vasilakos, A.; Obaidat, M. Jamming in underwater sensor networks: Detection and mitigation. *IET Commun.* **2012**, *6*, 2178–2188. [CrossRef]
110. Bagali, S.; Sundaraguru, R. Efficient channel access model for detecting reactive jamming for underwater wireless sensor network. In Proceedings of the 2019 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET), Chennai, India, 21–23 March 2019.
111. Xiao, L.; Li, Q.; Chen, T.; Cheng, E.; Dai, H. Jamming games in underwater sensor networks with reinforcement learning. In Proceedings of the 2015 IEEE Global Communications Conference (GLOBECOM), San Diego, CA, USA, 6–10 December 2015.
112. Osanaiye, O.; Alfa, A.S.; Hancke, G.P. A Statistical Approach to Detect Jamming Attacks in Wireless Sensor Networks. *Sensors* **2018**, *18*, 1691. [CrossRef] [PubMed]

113. Coutinho, R.W.L.; Boukerche, A.; Vieira, L.F.M.; Loureiro, A.A.F. GEDAR: Geographic and opportunistic routing protocol with Depth Adjustment for mobile underwater sensor networks. In Proceedings of the 2014 IEEE International Conference on Communications (ICC), Sydney, NSW, Australia, 10–14 June 2014; pp. 251–256. [CrossRef]
114. Raj, P.N.; Swadas, P.B. DPRAODV: A Dynamic Learning System against Black Hole Attack in AODV based MANET. *IJCSI Int. J. Comput. Sci. Issues* **2009**, *2*, 54–59.
115. Tamilselvan, L.; Sankaranarayanan, V. Prevention of Co-operative Black Hole Attack in MANET. *J. Netw.* **2008**, *3*, 13–20. [CrossRef]
116. Kalkha, H.; Satori, H.; Satori, K. Preventing Black Hole Attack in Wireless Sensor Network Using HMM. *Procedia Comput. Sci.* **2019**, *148*, 552–561. [CrossRef]
117. Premkumardeepak, S.; Krishnan, M.M. Intelligent sensor based monitoring system for underwater pollution. In Proceedings of the 2017 International Conference on IoT and Application (ICIOT), Nagapattinam, India, 19–20 May 2017; pp. 1–4. [CrossRef]
118. Bayrakdar, M.E. Cost Effective Smart System for Water Pollution Control with Underwater Wireless Sensor Networks: A Simulation Study. *Comput. Syst. Sci. Eng.* **2020**, *35*, 283–292. [CrossRef]
119. Hafeez, S.; Wong, M.S.; Abbas, S.; Kwok, C.Y.T.; Nichol, J.; Lee, K.H.; Tang, D.; Pun, L. Detection and Monitoring of Marine Pollution Using Remote Sensing Technologies. In *Monitoring of Marine Pollution*; 2019; Available online: <https://doi.org/10.5772/intechopen.81657> (accessed on 6 December 2021).
120. Cario, G.; Casavola, A.; Gjanci, P.; Lupia, M.; Petrioli, C.; Spaccini, D. Long lasting underwater wireless sensors network for water quality monitoring in fish farms. In Proceedings of the OCEANS 2017, Aberdeen, UK, 19–22 June 2017; pp. 1–6. [CrossRef]
121. Adu-Manu, K.S.; Tapparello, C.; Heinzelman, W.; Katsriku, F.A.; Abdulai, J. Water quality monitoring using wireless sensor networks: Current trends and future research directions. *ACM Trans. Sens. Netw. (TOSN)* **2017**, *13*, 1–41. [CrossRef]
122. de Lima, R.L.P.; Boogaard, F.C.; de Graaf-van Dinther, R.E. Innovative water quality and ecology monitoring using underwater unmanned vehicles: Field applications, challenges and feedback from water managers. *Water* **2020**, *12*, 1196. [CrossRef]
123. Chen, Y.; Han, D. Water quality monitoring in smart city: A pilot project. *Autom. Constr.* **2018**, *89*, 307–316. [CrossRef]
124. Yunbing, H.U. Research on water quality monitoring by means of sensor network. *J. Theor. Appl. Inf. Technol.* **2013**, *49*, 126–130.
125. Jindal, H.; Saxena, S.; Kasana, S.S. A sustainable multi-parametric sensors network topology for river water quality monitoring. *Wirel. Netw.* **2018**, *24*, 3241–3265. [CrossRef]
126. Pappu, S.; Vudatha, P.; Niharika, A.V.; Karthick, T.; Sankaranarayannan, S. Intelligent IoT based water quality monitoring system. *Int. J. Appl. Eng. Res.* **2017**, *12*, 5447–5454.
127. Li, D.; Liu, S. *Water Quality Monitoring and Management: Basis, Technology and Case Studies*; Academic Press: Cambridge, MA, USA, 2018.
128. Jo, W.; Hoashi, Y.; Aguilar, L.L.P.; Postigo-Malaga, M.; Garcia-Bravo, J.M.; Min, B.-C. A low-cost and small USV platform for water quality monitoring. *HardwareX* **2019**, *6*, 1–13. [CrossRef]
129. Xu, L.; Gu, H.; Li, C.; Shi, A.; Shen, J. System Design of Water Quality Monitoring Robot with Automatic Navigation and Self-test Capability. *Int. J. Control. Autom.* **2013**, *6*, 67–82. [CrossRef]
130. Gupta, S.; Kohli, M.; Kumar, R.; Bandral, S. IoT Based Underwater Robot for Water Quality Monitoring. In Proceedings of the IOP Conference Series: Materials Science and Engineering, International Conference on Integrated Interdisciplinary Innovations in Engineering (ICIIE 2020), Panjab University, Chandigarh, India, 28–30 August 2020; Volume 1033.
131. Lu, H.; Zhang, Y.; Li, Y.; Zhou, Q.; Tadoh, R.; Uemura, T.; Kim, H.; Serikawa, S. Depth map reconstruction for underwater Kinect camera using inpainting and local image mode filtering. *IEEE Access* **2017**, *5*, 7115–7122. [CrossRef]
132. Si, J.; Xiong, W.; Zhong, D.; Yan, A.; Wang, P.; Liu, Z. Piezoelectric-based damage-depth monitoring method for underwater energy-relief blasting technique. *J. Civ. Struct. Health Monit.* **2021**, *11*, 251–264. [CrossRef]
133. Tanakitkorn, K.; Wilson, P.A.; Turnock, S.R.; Phillips, A.B. Depth control for an over-actuated, hover-capable autonomous underwater vehicle with experimental verification. *Mechatronics* **2017**, *41*, 67–81. [CrossRef]
134. Yokogawa, Leading Provider of Industrial Automation, Developed Sea Water Surface Temperature Monitoring. 2021. Available online: <https://www.yokogawa.com/library/resources/application-notes/sea-water-surface-temperature-monitoring/> (accessed on 28 October 2021).
135. Schuster, A.; Castagna, O.; Schmid, B.; Cibis, T.; Sieber, A.; GmbH, S. Underwater monitoring system for body temperature and ECG recordings. *Underw. Technol.* **2017**, *34*, 135–139. [CrossRef]
136. Isaak, D.J.; Horan, D.L.; Wollrab, S.P. A simple protocol using underwater epoxy to install annual temperature monitoring sites in rivers and streams. *Gen. Tech. Rep.* **2013**, *314*, 1–28. [CrossRef]
137. Puntsri, K.; Yindeemak, U.; Bubbawan, T. pH and temperature underwater monitoring with application using visible light communications. In Proceedings of the Fourth International Conference on Photonics Solutions (ICPS2019), Chiang Mai, Thailand, 20–22 November 2019. [CrossRef]
138. Johansen, J.E. Underwater Optical Sensorbot for In Situ pH Monitoring. Master Thesis, Arizona State University, Tempe, AZ, USA, 2012.
139. Mathias, R.; Ambalgi, A.P.; Upadhyaya, A.M. Grating based pressure monitoring system for subaquatic application. *Int. J. Inf. Technol.* **2018**, *10*, 551–557. [CrossRef]
140. Costa, C.; Loy, A.; Cataudella, S.; Davis, D.; Scardi, M. Extracting fish size using dual underwater cameras. *Aquac. Eng.* **2006**, *35*, 218–227. [CrossRef]

141. Yoo, S.-H.; Ju, Y.-T.; Kim, J.-S.; Kim, E.-K. Design and Development of Underwater Drone for Fish Farm Growth Environment Management. *J. Korea Inst. Electron. Commun. Sci.* **2020**, *15*, 959–966.
142. Shortis, M.R.; Ravanbakhsh, M.; Shaifat, F.; Harvey, E.S.; Mian, A.; Seager, J.W.; Culverhouse, P.F.; Cline, D.E.; Edgington, D.R. A review of techniques for the identification and measurement of fish in underwater stereo-video image sequences. In Proceedings of the Videometrics, Range Imaging, and Applications XII; and Automated Visual Inspection, Munich, Germany, 13–16 May 2013.
143. Ohrem, S.J.; Kelasidi, E.; Bloecher, N. Analysis of a novel autonomous underwater robot for bio-fouling prevention and inspection in fish farms. In Proceedings of the 2020 28th Mediterranean Conference on Control and Automation (MED), Saint-Raphaël, France, 15–18 September 2020.
144. Garcia, M.; Sendra, S.; Lloret, G.; Lloret, J. Monitoring and control sensor system for fish feeding in marine fish farms. *IET Commun.* **2011**, *5*, 1682–1690. [[CrossRef](#)]
145. Magsumbol, J.-A.V.; Almero, V.J.; Rosales, M.; Bandala, A.A.; Dadios, E.P. A Fuzzy Logic Approach for Fish Growth Assessment. In Proceedings of the 2019 IEEE 11th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment, and Management (HNICEM), Laoag, Philippines, 29 November–1 December 2019.
146. Lloret, J.; Garcia-Pineda, M.; Sendra, S.; Lloret, G. An underwater wireless group-based sensor network for marine fish farms sustainability monitoring. *Telecommun. Syst.* **2015**, *60*, 67–84. [[CrossRef](#)]
147. Delphin Raj, K.M.; Shin, S.-Y.; NAMGUNG, J.I.; Park, S.-H. The RIL based approach for predicting the growth of pearl spot fish using-UWAC. *J. Inst. Electron. Inf. Eng.* **2018**, *55*, 32–40.
148. Marini, S.; Fanelli, E.; Sbragaglia, V.; Azzurro, E.; Fernandez, J.D.R.; Aguzzi, J. Tracking Fish Abundance by Underwater Image Recognition. *Sci. Rep.* **2018**, *8*, 1–12. [[CrossRef](#)]
149. Islam, N.Z.M.; Aziz, N.M.A.N.A.; Abu, N.; Shualdi, W.; Isha, K.M.; Kong, T.C.; Hai, T.C.; Mahat, M.M. Underwater Fish Attraction LED Lamp (UFAL) for Improving Aquaculture Productivity. *J. Adv. Res. Appl. Mech.* **2019**, *53*, 8–14.
150. Ling, Y.J.; Lau, P.Y. Fish monitoring in complex environment. In Proceedings of the International Workshop on Advanced Image Technology (IWAIT), Singapore, 6–9 January 2019; Volume 11049.
151. Dunn, M.; Dalland, K. Observing behaviour and growth using the Simrad FCM 160 fish cage monitoring system. In *Fish Farming Technology*; CRC Press: Boca Raton, FL, USA, 2020; pp. 269–274. [[CrossRef](#)]
152. Almero, V.J.D.; Concepcion, R.S.; Sybingco, E.; Dadios, E.P. An Image Classifier for Underwater Fish Detection using Classification Tree-Artificial Neural Network Hybrid. In Proceedings of the 2020 RIVF International Conference on Computing and Communication Technologies (RIVF), Ho Chi Minh City, Vietnam, 14–15 October 2020; pp. 1–6. [[CrossRef](#)]
153. Boudhane, M.; Nsiri, B. Fish tracking using acoustical and optical data fusion in underwater environment. In Proceedings of the International Conference on Watermarking and Image Processing, Paris, France, 6–8 September 2017.
154. Føre, M.; Frank, K.; Norton, T.; Svendsen, E.; Alfredsen, J.A.; Dempster, T.; Eguiraun, H.; Watson, W.; Stahl, A.; Sunde, L.M.; et al. Precision fish farming: A new framework to improve production in aquaculture. *Biosyst. Eng.* **2018**, *173*, 176–193. [[CrossRef](#)]
155. Terayama, K.; Shin, K.; Mizuno, K.; Tsuda, K. Integration of sonar and optical camera images using deep neural network for fish monitoring. *Aquac. Eng.* **2019**, *86*. [[CrossRef](#)]
156. Zhou, C.; Xu, D.; Lin, K.; Sun, C.; Yang, X. Intelligent feeding control methods in aquaculture with an emphasis on fish: A review. *Rev. Aquac.* **2017**, *10*, 975–993. [[CrossRef](#)]
157. Karimanzira, D.; Jacobi, M.; Pfuetschenreuter, T.; Rauschenbach, T.; Eichhorn, M.; Taubert, R.; Ament, C. First testing of an AUV mission planning and guidance system for water quality monitoring and fish behavior observation in net cage fish farming. *Inf. Process. Agric.* **2014**, *1*, 131–140. [[CrossRef](#)]
158. Torisawa, S.; Kadota, M.; Komeyama, K.; Suzuki, K.; Takagi, T. A digital stereo-video camera system for three-dimensional monitoring of free-swimming Pacific bluefin tuna, *Thunnus orientalis*, cultured in a net cage. *Aquat. Living Resour.* **2011**, *24*, 107–112. [[CrossRef](#)]
159. Shi, C.; Wang, Q.; He, X.; Zhang, X.; Li, D. An automatic method of fish length estimation using underwater stereo system based on LabVIEW. *Comput. Electron. Agric.* **2020**, *173*, 105419. [[CrossRef](#)]
160. da Silva Vale, R.T.; Ueda, E.K.; Takimoto, R.Y.; de Castro Martins, T. Fish Volume Monitoring Using Stereo Vision for Fish Farms. *IFAC-Pap.* **2020**, *53*, 15824–15828. [[CrossRef](#)]
161. Harasti, D.; Lee, K.A.; Laird, R.; Bradford, R.; Bruce, B. Use of stereo baited remote underwater video systems to estimate the presence and size of white sharks (*Carcharodon carcharias*). *Mar. Freshw. Res.* **2017**, *68*, 1391. [[CrossRef](#)]
162. Delgado, J.P.; Staniforth, M. Underwater archaeology. *Archaeology* **2010**, *1*, 227.
163. Castro, F. c Hunters, and the UNESCO Convention on the Protection of the Underwater Cultural Heritage: A Personal Viewpoint. *Odyssey Pap.* **2010**, *13*, 7–9.
164. Bass, G.F. The development of maritime archaeology. In *The Oxford Handbook of Maritime Archaeology*; Oxford University Press: Oxford, UK, 2011; pp. 3–22.
165. Babits, L.E.; Van Tilburg, H. (Eds.) *Maritime Archaeology: A Reader of Substantive and Theoretical Contributions*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2013.
166. Teixeira, F.C.; Pascoal, A. Magnetic navigation and tracking of underwater vehicles. *IFAC Proc. Vol.* **2013**, *46*, 239–244. [[CrossRef](#)]
167. Ghafoor, H.; Noh, Y. An Overview of Next-Generation Underwater Target Detection and Tracking: An Integrated Underwater Architecture. *IEEE Access* **2019**, *7*, 98841–98853. [[CrossRef](#)]

168. Yao, F.; Yang, C.; Zhang, M.; Wang, Y. Optimization of the Energy Consumption of Depth Tracking Control Based on Model Predictive Control for Autonomous Underwater Vehicles. *Sensors* **2019**, *19*, 162. [[CrossRef](#)] [[PubMed](#)]
169. Sheng, M.; Tang, S.; Qin, H.; Wan, L. Clustering Cloud-Like Model-Based Targets Underwater Tracking for AUVs. *Sensors* **2019**, *19*, 370. [[CrossRef](#)] [[PubMed](#)]
170. Bechlioulis, C.P.; Karras, G.C.; Heshmati-Alamdari, S.; Kyriakopoulos, K.J. Trajectory tracking with prescribed performance for underactuated underwater vehicles under model uncertainties and external disturbances. *IEEE Trans. Control. Syst. Technol.* **2016**, *25*, 429–440. [[CrossRef](#)]
171. Wang, Z.; Wang, J.; Fan, R. An Underwater Single Target Tracking Method Using SiamRPN++ Based on Inverted Residual Bottleneck Block. *IEEE Access* **2021**, *9*, 25148–25157. [[CrossRef](#)]
172. Isbitiren, G.; Akan, O.B. Three-Dimensional Underwater Target Tracking With Acoustic Sensor Networks. *IEEE Trans. Veh. Technol.* **2011**, *60*, 3897–3906. [[CrossRef](#)]
173. Kim, J.H.; Yoo, S.J. Adaptive Event-Triggered Control Strategy for Ensuring Predefined Three-Dimensional Tracking Performance of Uncertain Nonlinear Underactuated Underwater Vehicles. *Mathematics* **2021**, *9*, 137. [[CrossRef](#)]
174. Myint, M.; Yonemori, K.; Yanou, A.; Minami, M.; Ishiyama, S. Visual-servo-based autonomous docking system for underwater vehicle using dual-eyes camera 3D-pose tracking. In Proceedings of the 2015 IEEE/SICE International Symposium on System Integration (SII), Nagoya, Japan, 11–13 December 2015. [[CrossRef](#)]
175. Sawa, T.; Kassaya, T.; Hyakudome, T.; Yoshida, H. Natural resource exploration with sonar on underwater vehicle. In *International Conference on Off-Shore Mechanics and Arctic Engineering*; American Society of Mechanical Engineers: New York, NY, USA, 2012; Volume 44946.
176. Moskwa, E.C. Exploring Place Attachment: An Underwater Perspective. *Tour. Mar. Environ.* **2012**, *8*, 33–46. [[CrossRef](#)]
177. Katzschmann, R.K.; DelPreto, J.; MacCurdy, R.; Rus, D. Exploration of underwater life with an acoustically controlled soft robotic fish. *Sci. Robot.* **2018**, *3*. [[CrossRef](#)]
178. Manderson, T.; Higuera, J.C.G.; Cheng, R.; Dudek, G. Vision-Based Autonomous Underwater Swimming in Dense Coral for Combined Collision Avoidance and Target Selection. In Proceedings of the 2018 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), Madrid, Spain, 1–5 October 2018. [[CrossRef](#)]
179. Girdhar, Y.; Dudek, G. Exploring underwater environments with curiosity. In Proceedings of the 2014 Canadian Conference on Computer and Robot Vision, Montreal, QC, Canada, 6–9 May 2014.
180. Carrasco, S.A.; Bravo, M.; Avilés, E.; Ruiz, P.A.R.; Yori, A.; Hinojosa, I.A. Exploring overlooked components of remote South-east Pacific oceanic islands: Larval and macrobenthic assemblages in reef habitats with distinct underwater soundscapes. *Aquat. Conserv. Mar. Freshw. Ecosyst.* **2020**, *31*, 273–289. [[CrossRef](#)]
181. Nocerino, E.; Neyer, F.; Gruen, A.; Troyer, M.; Menna, F.; Brooks, A.; Capra, A.; Castagnetti, C.; Rossi, P. Comparison of diver-operated underwater photogrammetric systems for coral reef monitoring. *ISPRS—Int. Arch. Photogramm. Remote. Sens. Spat. Inf. Sci.* **2019**, *XLII-2/W10*, 143–150. [[CrossRef](#)]
182. Armstrong, R.A.; Pizarro, O.; Roman, C. Underwater Robotic Technology for Imaging Mesophotic Coral Ecosystems. In *Mesophotic Coral Ecosystems*; Springer: Cham, Switzerland, 2019; pp. 973–988. [[CrossRef](#)]
183. Yoshida, H.; Hyakudome, T.; Ishibashi, S.; Sawa, T.; Nakano, Y.; Ochi, H.; Watanabe, Y.; Nakatani, T.; Ota, Y.; Sugawara, M. An autonomous underwater vehicle with a canard rudder for underwater minerals exploration. In Proceedings of the 2013 IEEE International Conference on Mechatronics and Automation, Takamatsu, Japan, 4–7 August 2013.
184. Wakita, N.; Hirokawa, K.; Ichikawa, K.; Yamauchi, Y. Development of autonomous underwater vehicle (AUV) for exploring deep sea marine mineral resources. *Mitsubishi Heavy Ind. Tech. Rev.* **2010**, *47*, 73–80.
185. Di Vito, D.; De Palma, D.; Simetti, E.; Indiveri, G.; Antonelli, G. Experimental validation of the modeling and control of a multibody underwater vehicle manipulator system for sea mining exploration. *J. Field Robot.* **2021**, *38*, 171–191. [[CrossRef](#)]
186. Lopes, L.; Zajzon, N.; Bodo, B.; Henley, S.; Žibret, G.; Dizdarevic, T. UNEXMIN: Developing an autonomous underwater explorer for flooded mines. *Energy Procedia* **2017**, *125*, 41–49. [[CrossRef](#)]
187. Ulvrova, M.; Paris, R.; Kelfoun, K.; Nomikou, P. Numerical simulations of tsunamis generated by underwater volcanic explosions at Karymskoye lake (Kamchatka, Russia) and Kolumbo volcano (Aegean Sea, Greece). *Nat. Hazards Earth Syst. Sci.* **2014**, *14*, 401–412. [[CrossRef](#)]
188. Koba, M.; Yamamoto, A.; Ueno, T.; Yuhi, M. A numerical study on the influence of variation of underwater landslide shape on tsunami generation. In Proceedings of the 28th International Ocean and Polar Engineering Conference, Sapporo, Japan, 10–15 June 2018.
189. Karan, P.P.; Sukanuma, U. (Eds.) *Japan after 3/11: Global Perspectives on the Earthquake, Tsunami, and Fukushima Meltdown*; University Press of Kentucky: Lexington, KY, USA, 2016.
190. Kumar, P.; Kumar, P.; Priyadarshini, P. Srijia Underwater acoustic sensor network for early warning generation. In Proceedings of the 2012 Oceans, Hampton Roads, VA, USA, 14–19 October 2012. [[CrossRef](#)]
191. Kim, D.S.; Hong, S.J.; Park, H.S. Analysis of evacuation system on tsunami disaster prevention in Korea. *J. Coast. Res.* **2013**, *65*, 974–979. [[CrossRef](#)]
192. Karambas, T.V.; Hasiotis, T. A Study of Tsunamis Generated by Underwater Landslides in the Aegean Sea. In Proceedings of the Twenty-second International Offshore and Polar Engineering Conference, Rhodes, Greece, 17–22 June 2012.

193. Hanzawa, M.; Matsumoto, A.; Tanaka, H. Stability of wave-dissipating concrete blocks of detached breakwaters against tsunami. *Coast. Eng. Proc.* **2012**, *1*. [CrossRef]
194. Liao, B.; Zhang, W. Research on landslide stability under water level fluctuation of reservoir: Case of Hushantan landslide of a hydropower station on Yalong River. *Yangtze River* **2013**, *44*, 37–40.
195. Wang, S.-x.; Chen, D.-b.; Shi, L.U.O. Research on engineering effect evaluation of landslide prevention system. *Shanxi Archit.* **2012**, *2012*, 23.
196. Zahari, M.N.B.M.; Nazif, M. Structural Landslide Mitigation Technique. 2010. Available online: <http://www.malrep.uum.edu.my/rep/Record/my-utp-utpedia.1022/Description#tabnav> (accessed on 6 December 2021).
197. Yang, J.; Jian, W.; Yang, H.; Zhang, J. Dynamic variation rule of phreatic line in Huangtupo landslide in Three Gorges reservoir area. *Rock Soil Mech.* **2012**, *33*, 853–858.
198. Kozlova, T.V.; Cherkez, E.A.; Medinets, V.I.; Gazyetov, Y.I.; Snihirov, S.M.; Medinets, S.V. Study of structural-tectonic discreteness of abrasion-landslide bench in a segment of Odesa coastline. In *Geoinformatics: Theoretical and Applied Aspects 2020*; European Association of Geoscientists & Engineers: Houten, The Netherlands, 2020; Volume 2020, pp. 1–5. [CrossRef]
199. Chuanzhi, W.; Lixin, W. Forming Mechanism and Stability Analysis of Diaozhon Dam Landslides in Zhong County of Chongqing. *Urban. Roads Bridges Flood Control.* **2015**, *8*. Available online: https://en.cnki.com.cn/Article_en/CJFDTotal-CSDQ201508111.htm (accessed on 6 December 2021).
200. Zhang, Y.; Shi, S.-W.; Song, J.; Cheng, Y.-J. Evaluation on Effect for the Prevention and Control Against the Landslide Disasters in the Three Gorges Reservoir Area. In *Landslide Science for a Safer Geoenvironment*; Springer: Cham, Switzerland, 2014; pp. 407–414. [CrossRef]
201. Marra, G.; Clivati, C.; Luckett, R.; Tampellini, A.; Kronjäger, J.; Wright, L.; Mura, A.; Levi, F.; Robinson, S.; Xuereb, A.; et al. Ultrastable laser interferometry for earthquake detection with terrestrial and submarine cables. *Science* **2018**, *361*, 486–490. [CrossRef] [PubMed]
202. Lior, I.; Sladen, A.; Rivet, D.; Ampuero, J.; Hello, Y.; Becerril, C.; Martins, H.F.; Lamare, P.; Jestin, C.; Tsagkli, S.; et al. On the Detection Capabilities of Underwater Distributed Acoustic Sensing. *J. Geophys. Res. Solid Earth* **2021**, *126*. [CrossRef]
203. Shakila, R.; Paramasivan, B. Performance Analysis of Submarine Detection in Underwater Wireless Sensor Networks for Naval Application. *Microprocess. Microsyst.* **2020**, 103293. [CrossRef]
204. Chen, B.; Li, R.; Bai, W.; Li, J.; Zhou, Y.; Guo, R. Application analysis of autonomous underwater vehicle in submarine cable detection operation. In Proceedings of the 2018 International Conference on Robotics, Control and Automation Engineering, Beijing, China, 26–28 December 2018.
205. Williams, D.P. On optimal AUV track-spacing for underwater mine detection. In Proceedings of the 2010 IEEE International Conference on Robotics and Automation, Anchorage, AK, USA, 3–7 May 2010.
206. Khaledi, S.; Mann, H.; Perkovich, J.; Zayed, S. Design of an underwater mine detection system. In Proceedings of the 2014 Systems and Information Engineering Design Symposium (SIEDS), Charlottesville, VA, USA, 25 April 2014.
207. Vinutha, K.V.; Vinutha, K.; Yuvaraja, T. Under water mine detection using SONAR. *J. Comput. Theor. Nanosci.* **2018**, *15*, 2150–2152. [CrossRef]
208. Sawas, J.; Petillot, Y.; Pailhas, Y. Cascade of boosted classifiers for rapid detection of underwater objects. In Proceedings of the European Conference on Underwater Acoustics, Istanbul, Turkey, 5–9 July 2010; Volume 164.
209. Artusi, E.; Chaillan, F. Automatic recognition of underwater acoustic signature for naval applications. In Proceedings of the 1st Maritime Situational Awareness Workshop MSAW 2019, Lerici, Italy, October 2019.
210. Ferri, G.; Munafò, A.; Tesei, A.; Braca, P.; Meyer, F.; Pelekanakis, K.; Petrocchia, R.; Alves, J.; Strode, C.; LePage, K. Cooperative robotic networks for underwater surveillance: An overview. *IET Radar Sonar Navig.* **2017**, *11*, 1740–1761. [CrossRef]
211. Macias, E.; Suarez, A.; Chiti, F.; Sacco, A.; Fantacci, R. A Hierarchical Communication Architecture for Oceanic Surveillance Applications. *Sensors* **2011**, *11*, 11343–11356. [CrossRef]
212. Aversa, M.; Lapinsky, S.E. Lung physiology at play: Hemoptysis due to underwater hockey. *Respir. Med. Case Rep.* **2014**, *11*, 16–17. [CrossRef]
213. Vladimirovna, R.E.; Anatolevich, T.I.; Nikolaevna, L.A.; Nikolaevna, B.G. The study of the heart rate in athletes engaged in underwater sports, depending on the specialization. *Eur. J. Mol. Clin. Med.* **2021**, *8*, 1492–1498.
214. Battal, O.; Balcioglu, T.; Duru, A.D. Analysis of gaze characteristics with eye tracking system during repeated breath holding exercises in underwater hockey elite athletes. In Proceedings of the 2016 20th National Biomedical Engineering Meeting (BIYOMUT), Izmir, Turkey, 3–5 November 2016. [CrossRef]
215. Ozen, S. Correlation between Agility and Speed in Elite Underwater Hockey Players. *Int. J. Appl. Exerc. Physiol.* **2020**, *9*, 86–91.
216. Musa, G.; Seng, W.T.; Thirumoorthi, T.; Abessi, M. The influence of scuba divers' personality, experience, and demographic profile on their under-water behavior. *Tour. Mar. Environ.* **2011**, *7*, 1–14. [CrossRef]
217. Ong, T.F.; Musa, G. Examining the influences of experience, personality and attitude on SCUBA divers' underwater behaviour: A structural equation model. *Tour. Manag.* **2012**, *33*, 1521–1534. [CrossRef]
218. Hegrenæs, Ø.; Hallingstad, O. Model-Aided INS with Sea Current Estimation for Robust Underwater Navigation. *IEEE J. Ocean. Eng.* **2011**, *36*, 316–337. [CrossRef]
219. Qin, H.-D.; Yu, X.; Zhu, Z.-B.; Deng, Z.-C. An expectation-maximization based single-beacon underwater navigation method with unknown ESV. *Neurocomputing* **2019**, *378*, 295–303. [CrossRef]

220. Boyer, F.; Lebastard, V.; Chevallereau, C.; Mintchev, S.; Stefanini, C. Underwater navigation based on passive electric sense: New perspectives for underwater docking. *Int. J. Robot. Res.* **2015**, *34*, 1228–1250. [[CrossRef](#)]
221. Hernández, J.D.; Istenič, K.; Gracias, N.; Palomeras, N.; Campos, R.; Vidal, E.; García, R.; Carreras, M. Autonomous underwater navigation and optical mapping in unknown natural environments. *Sensors* **2016**, *16*, 1174. [[CrossRef](#)]
222. Kim, T.; Kim, J.; Byun, S.-W. A Comparison of Nonlinear Filter Algorithms for Terrain-referenced Underwater Navigation. *Int. J. Control. Autom. Syst.* **2018**, *16*, 2977–2989. [[CrossRef](#)]
223. Yuan, X.; Martínez-Ortega, J.-F.; Fernández, J.A.S.; Eckert, M. AEKF-SLAM: A New Algorithm for Robotic Underwater Navigation. *Sensors* **2017**, *17*, 1174. [[CrossRef](#)]
224. Davari, N.; Gholami, A. An asynchronous adaptive direct Kalman filter algorithm to improve underwater navigation system performance. *IEEE Sens. J.* **2016**, *17*, 1061–1068. [[CrossRef](#)]
225. Manderson, T.; Higuera, J.C.G.; Wapnick, S.; Tremblay, J.; Shkurti, F.; Meger, D.; Dudek, G. Vision-based goal-conditioned policies for underwater navigation in the presence of obstacles. *arXiv* **2020**, arXiv:2006.16235.
226. Bahr, A.; Leonard, J.J.; Martinoli, A. Dynamic positioning of beacon vehicles for cooperative underwater navigation. In Proceedings of the 2012 IEEE/RSJ International Conference on Intelligent Robots and Systems, Vilamoura-Algarve, Portugal, 7–12 October 2012.
227. Ullah, I.; Liu, Y.; Su, X.; Kim, P. Efficient and Accurate Target Localization in Underwater Environment. *IEEE Access* **2019**, *7*, 101415–101426. [[CrossRef](#)]
228. Waldmeyer, M.; Tan, H.-P.; Seah, W.K.G. Multi-stage AUV-aided localization for underwater wireless sensor networks. In Proceedings of the 2011 IEEE Workshops of International Conference on Advanced Information Networking and Applications, Biopolis, Singapore, 22–25 March 2011.
229. Callmer, J.; Skoglund, M.; Gustafsson, F. Silent localization of underwater sensors using magnetometers. *Eurasip J. Adv. Signal Process.* **2010**, *2010*, 1–8. [[CrossRef](#)]
230. Li, Z.; Dosso, S.E.; Sun, D. Motion-Compensated Acoustic Localization for Underwater Vehicles. *IEEE J. Ocean. Eng.* **2016**, *41*, 840–851. [[CrossRef](#)]
231. Pinheiro, B.C.; Moreno, U.F.; de Sousa, J.T.B.; Rodriguez, O.C. Kernel-Function-Based Models for Acoustic Localization of Underwater Vehicles. *IEEE J. Ocean. Eng.* **2016**, *42*, 603–618. [[CrossRef](#)]
232. Zheng, C.; Sun, D.; Cai, L.; Li, X. Mobile Node Localization in Underwater Wireless Networks. *IEEE Access* **2018**, *6*, 17232–17244. [[CrossRef](#)]
233. Yan, J.; Xu, Z.; Wan, Y.; Chen, C.; Luo, X. Consensus estimation-based target localization in underwater acoustic sensor networks. *Int. J. Robust Nonlinear Control.* **2016**, *27*, 1607–1627. [[CrossRef](#)]
234. Chang, S.; Li, Y.; He, Y.; Wang, H. Target Localization in Underwater Acoustic Sensor Networks Using RSS Measurements. *Appl. Sci.* **2018**, *8*, 225. [[CrossRef](#)]
235. Gong, Z.; Li, C.; Jiang, F.; Zheng, J. AUV-Aided Localization of Underwater Acoustic Devices Based on Doppler Shift Measurements. *IEEE Trans. Wirel. Commun.* **2020**, *19*, 2226–2239. [[CrossRef](#)]
236. Zhang, B.; Wang, H.; Zheng, L.; Wu, J.; Zhuang, Z. Joint synchronization and localization for underwater sensor networks considering stratification effect. *IEEE Access* **2017**, *5*, 26932–26943. [[CrossRef](#)]
237. Burguera, A.; Bonin-Font, F.; Oliver, G. Trajectory-based visual localization in underwater surveying missions. *Sensors* **2015**, *15*, 1708–1735. [[CrossRef](#)] [[PubMed](#)]
238. Nguyen, T.L.N.; Shin, Y. An efficient RSS localization for underwater wireless sensor networks. *Sensors* **2019**, *19*, 3105. [[CrossRef](#)] [[PubMed](#)]
239. Yan, J.; Xu, Z.; Luo, X.; Chen, C.; Guan, X. Feedback-Based Target Localization in Underwater Sensor Networks: A Multisensor Fusion Approach. *IEEE Trans. Signal. Inf. Process. Over Netw.* **2018**, *5*, 168–180. [[CrossRef](#)]
240. Tang, L.; Liu, M.; Wang, K.-C.; Huang, Y.; Yang, F.; Zhang, D. Study of path loss and data transmission error of IEEE 802.15.4 compliant wireless sensors in small-scale manufacturing environments. *Int. J. Adv. Manuf. Technol.* **2012**, *63*, 659–669. [[CrossRef](#)]
241. Zhang, Y.; Negahdaripour, S.; Li, Q. Error-resilient coding for underwater video transmission. In Proceedings of the OCEANS 2016 MTS/IEEE Monterey, Monterey, CA, USA, 19–23 September 2016; pp. 1–7. [[CrossRef](#)]
242. Esmail, H.; Qasem, Z.A.H.; Sun, H.; Wang, J.; Junejo, N.U.R. Underwater Image Transmission Using Spatial Modulation Unequal Error Protection for Internet of Underwater Things. *Sensors* **2019**, *19*, 5271. [[CrossRef](#)]
243. Esmail, H.; Jiang, D. Optimum Bit Rate for Image Transmission over Underwater Acoustic Channel. *J. Electr. Electron. Eng.* **2014**, *2*, 64. [[CrossRef](#)]
244. El-Banna, A.A.A.; Wu, K.; ElHalawany, B.M. Opportunistic cooperative transmission for underwater communication based on the Water’s key physical variables. *IEEE Sens. J.* **2019**, *20*, 2792–2802. [[CrossRef](#)]
245. Diamant, R.; Lampe, L. Adaptive Error-Correction Coding Scheme for Underwater Acoustic Communication Networks. *IEEE J. Ocean. Eng.* **2014**, *40*, 104–114. [[CrossRef](#)]
246. Ilyas, N.; Alghamdi, T.A.; Farooq, M.N.; Mehboob, B.; Sadiq, A.H.; Qasim, U.; Khan, Z.A.; Javaid, N. AEDG: AUV-aided efficient data gathering routing protocol for underwater wireless sensor networks. *Procedia Comput. Sci.* **2015**, *52*, 568–575. [[CrossRef](#)]
247. Wei, X.; Liu, Y.; Gao, S.; Wang, X.; Yue, H. An RNN-Based Delay-Guaranteed Monitoring Framework in Underwater Wireless Sensor Networks. *IEEE Access* **2019**, *7*, 25959–25971. [[CrossRef](#)]

248. Domingo, M.C. A Distributed Energy-Aware Routing Protocol for Underwater Wireless Sensor Networks. *Wirel. Pers. Commun.* **2009**, *57*, 607–627. [[CrossRef](#)]
249. Sher, A.; Khan, A.; Javaid, N.; Ahmed, S.H.; Aalsalem, M.Y.; Khan, W.Z. Void hole avoidance for reliable data delivery in IoT enabled underwater wireless sensor networks. *Sensors* **2018**, *18*, 3271. [[CrossRef](#)] [[PubMed](#)]
250. Ilyas, N.; Akbar, M.; Ullah, R.; Khalid, M.; Arif, A.; Hafeez, A.; Qasim, U.; Khan, Z.A.; Javaid, N. SEDG: Scalable and Efficient Data Gathering Routing Protocol for Underwater WSNs. *Procedia Comput. Sci.* **2015**, *52*, 584–591. [[CrossRef](#)]
251. Ruby, D.; Jeyachidra, J. Semaphore based data aggregation and similarity findings for underwater wireless sensor networks. *Int. J. Grid High. Perform. Comput. (IJGHPC)* **2019**, *11*, 59–76. [[CrossRef](#)]
252. Akbar, M.; Javaid, N.; Khan, A.H.; Imran, M.; Shoaib, M.; Vasilakos, A. Efficient Data Gathering in 3D Linear Underwater Wireless Sensor Networks Using Sink Mobility. *Sensors* **2016**, *16*, 404. [[CrossRef](#)] [[PubMed](#)]
253. Nasir, H.; Javaid, N.; Ashraf, H.; Manzoor, S.; Khan, Z.; Qasim, U.; Sher, M. CoDBR: Cooperative Depth Based Routing for Underwater Wireless Sensor Networks. In Proceedings of the 2014 Ninth International Conference on Broadband and Wireless Computing, Communication and Applications, Guangdong, China, 8–10 November 2014; pp. 52–57. [[CrossRef](#)]
254. Ali, M.; Khan, A.; Aurangzeb, K.; Ali, I.; Mahmood, H.; Halider, S.I.; Bhatti, N. CoSIM-RPO: Cooperative routing with sink mobility for reliable and persistent operation in underwater acoustic wireless sensor networks. *Sensors* **2019**, *19*, 1101. [[CrossRef](#)] [[PubMed](#)]
255. Javaid, N.; Ahmad, Z.; Sher, A.; Wadud, Z.; Khan, Z.A.; Ahmed, S.H. Fair energy management with void hole avoidance in intelligent heterogeneous underwater WSNs. *J. Ambient. Intell. Humaniz. Comput.* **2018**, *10*, 4225–4241. [[CrossRef](#)]
256. Javaid, N.; Jafri, M.R.; Khan, Z.A.; Qasim, U.; Alghamdi, T.A.; Ali, M. iAMCTD: Improved Adaptive Mobility of Courier Nodes in Threshold-Optimized DBR Protocol for Underwater Wireless Sensor Networks. *Int. J. Distrib. Sens. Netw.* **2014**, *10*. [[CrossRef](#)]
257. Jiang, J.; Han, G.; Shu, L.; Chan, S.; Wang, K. A Trust Model Based on Cloud Theory in Underwater Acoustic Sensor Networks. *IEEE Trans. Ind. Inform.* **2015**, *13*, 342–350. [[CrossRef](#)]
258. Tran-Dang, H.; Kim, D.-S. Channel-aware cooperative routing in underwater acoustic sensor networks. *J. Commun. Netw.* **2019**, *21*, 33–44. [[CrossRef](#)]
259. Hsu, C.-C.; Liu, H.-H.; Gomez, J.L.G.; Chou, C.-F. Delay-Sensitive Opportunistic Routing for Underwater Sensor Networks. *IEEE Sens. J.* **2015**, *15*, 6584–6591. [[CrossRef](#)]
260. Li, C.; Xu, Y.; Xu, C.; An, Z.; Diao, B.; Li, X. DTMAC: A Delay Tolerant MAC Protocol for Underwater Wireless Sensor Networks. *IEEE Sens. J.* **2015**, *16*, 4137–4146. [[CrossRef](#)]
261. Tran-Dang, H.; Kim, D.-S. Channel-aware energy-efficient two-hop cooperative routing protocol for underwater acoustic sensor networks. *IEEE Access* **2019**, *7*, 63181–63194. [[CrossRef](#)]
262. Li, J.; Toulgoat, M.; Zhou, Y.; Lamont, L. Logical Link Control and Channel Scheduling for Multichannel Underwater Sensor Networks. *ICST Trans. Mob. Commun. Appl.* **2012**, *12*. [[CrossRef](#)]
263. Rahman, R.; Frater, M. Delay-tolerant networks (DTNs) for underwater communications. In *Advances in Delay-Tolerant Networks (DTNs)*; Woodhead Publishing: Sawston, UK, 2015; pp. 81–103. [[CrossRef](#)]
264. Behrje, U.; Isokeit, C.; Meyer, B.; Maehle, E. A Robust Acoustic-Based Communication Principle for the Navigation of an Underwater Robot Swarm. In Proceedings of the 2018 OCEANS-MTS/IEEE Kobe Techno-Oceans (OTO), Kobe, Japan, 28–31 May 2018; pp. 1–5. [[CrossRef](#)]
265. Rodríguez-Molina, J.; Bilbao, S.; Martínez, B.; Frasher, M.; Cürüklü, B. An Optimized, Data Distribution Service-Based Solution for Reliable Data Exchange Among Autonomous Underwater Vehicles. *Sensors* **2017**, *17*, 1802. [[CrossRef](#)] [[PubMed](#)]
266. Chen, M.-T.; Shen, Y.-C.; Luis, J.; Chou, C.-F. Energy-efficient OR-based MAC protocol for underwater sensor networks. In Proceedings of the SENSORS, 2014 IEEE, Valencia, Spain, 2–5 November 2014; pp. 118–121. [[CrossRef](#)]
267. Kim, Y.; Varzi, A.; Mariani, A.; Kim, G.; Kim, Y.; Passerini, S. Redox-Mediated Red-Phosphorous Semi-Liquid Anode Enabling Metal-Free Rechargeable Na-Seawater Batteries with High Energy Density. *Adv. Energy Mater.* **2021**, *11*, 2102061. [[CrossRef](#)]
268. Cho, J.; Kim, M.W.; Kim, Y.; Park, J.-S.; Lee, D.-H.; Kim, Y.; Kim, J.J. Seawater Battery-Based Wireless Marine Buoy System With Battery Degradation Prediction and Multiple Power Optimization Capabilities. *IEEE Access* **2021**, *9*, 104104–104114. [[CrossRef](#)]
269. Son, M.; Park, S.; Kim, N.; Angeles, A.T.; Kim, Y.; Cho, K.H. Simultaneous Energy Storage and Seawater Desalination using Rechargeable Seawater Battery: Feasibility and Future Directions. *Adv. Sci.* **2021**, *8*, 2101289. [[CrossRef](#)]
270. Ateniese, G.; Caposelle, A.; Gjanci, P.; Petrioli, C.; Spaccini, D. SecFUN: Security framework for underwater acoustic sensor networks. In Proceedings of the OCEANS 2015—Genova, Genova, Italy, 18–21 May 2015; pp. 1–9. [[CrossRef](#)]
271. Li, H.; He, Y.; Cheng, X.; Zhu, H.; Sun, L. Security and privacy in localization for underwater sensor networks. *IEEE Commun. Mag.* **2015**, *53*, 56–62. [[CrossRef](#)]
272. Han, G.; Jiang, J.; Shu, L.; Guizani, M. An Attack-Resistant Trust Model Based on Multidimensional Trust Metrics in Underwater Acoustic Sensor Network. *IEEE Trans. Mob. Comput.* **2015**, *14*, 2447–2459. [[CrossRef](#)]
273. Su, Y.; Ma, S.; Zhang, H.; Jin, Z.; Fu, X. A Redeemable SVM-DS Fusion-Based Trust Management Mechanism for Underwater Acoustic Sensor Networks. *IEEE Sens. J.* **2021**, *21*, 26161–26174. [[CrossRef](#)]
274. Dargahi, T.; Javadi, H.H.S.; Shafiei, H. Securing underwater sensor networks against routing attacks. *Wirel. Pers. Commun.* **2017**, *96*, 2585–2602. [[CrossRef](#)]
275. Han, G.; He, Y.; Jiang, J.; Wang, N.; Guizani, M.; Ansere, J.A. A Synergetic Trust Model Based on SVM in Underwater Acoustic Sensor Networks. *IEEE Trans. Veh. Technol.* **2019**, *68*, 11239–11247. [[CrossRef](#)]

276. Jiang, J.; Han, G.; Zhu, C.; Chan, S.; Rodrigues, J.J.P.C. A Trust Cloud Model for Underwater Wireless Sensor Networks. *IEEE Commun. Mag.* **2017**, *55*, 110–116. [CrossRef]
277. Nie, D.; Sun, Z.; Qiao, G.; Liu, S.; Yin, Y. Kite-type passive acoustic detection system for underwater small targets. In Proceedings of the 2014 Oceans—St. John's, St. John's, NL, Canada, 14–19 September 2014. [CrossRef]
278. Kozhaeva, K.V.; Mustafin, F.M.; Yakupova, D.E. Methods for calculating the longitudinal stability of the pipeline and security measures in the area of underwater crossing (Russian). *Neftyanoe Khozyaystvo-Oil Ind.* **2016**, *2016*, 102–104.
279. Kim, H.; Lee, J.; Yi, O. Proposal of Piecewise Key Management Design Considering Capability of Underwater Communication Nodes. *Adv. Sci. Lett.* **2017**, *23*, 12729–12733. [CrossRef]
280. Shuvo, M.D.; Firdaus, M.T. *A Model for Underwater Security in Communication Using Secret Key Algorithm and Node Value*; Department of Computer Science and Engineering, Diss. Brac University: Dhaka, Bangladesh, 2021.
281. Lal, C.; Petroccia, R.; Pelekanakis, K.; Conti, M.; Alves, J. Toward the Development of Secure Underwater Acoustic Networks. *IEEE J. Ocean. Eng.* **2017**, *42*, 1075–1087. [CrossRef]
282. Silarski, M.; Hunik, D.; Smolis, M.; Tadeja, S.; Moskal, P. Design of the SABAT System for Underwater Detection of Dangerous Substances. *Acta Phys. Pol. B* **2016**, *47*, 497. [CrossRef]
283. Li, C.; Marzani, F.; Yang, F. Demodulation of Chaos Phase Modulation Spread Spectrum Signals Using Machine Learning Methods and Its Evaluation for Underwater Acoustic Communication. *Sensors* **2018**, *18*, 4217. [CrossRef] [PubMed]
284. Chen, Q. Application of the Vibration Fiber Optic Perimeter Alarm System Based on the GPRS in the Underwater Security. *Electron. Sci. Technol.* **2013**, *7*. Available online: https://en.cnki.com.cn/Article_en/CJFDTotal-DZKK201307011.htm (accessed on 6 December 2021).
285. Arifeen, M.M.; Mamun, A.A.; Ahmed, T.; Kaiser, M.S.; Mahmud, M. A Blockchain-Based Scheme for Sybil Attack Detection in Underwater Wireless Sensor Networks. In *Proceedings of International Conference on Trends in Computational and Cognitive Engineering*; Springer: Singapore, 2021.
286. Huynh, T.; Khatib, M.; Haick, H. Self-Healable Materials for Underwater Applications. *Adv. Mater. Technol.* **2019**, *4*, 1900081. [CrossRef]
287. Elhanafi, A.; Macfarlane, G.; Fleming, A.; Leong, Z. Experimental and numerical investigations on the intact and damage survivability of a floating-moored oscillating water column device. *Appl. Ocean. Res.* **2017**, *68*, 276–292. [CrossRef]
288. Xu, L.; Huang, Z.; Deng, Z.; Du, Z.; Sun, T.L.; Guo, Z.; Yue, K. A Transparent, Highly Stretchable, Solvent-Resistant, Recyclable Multifunctional Ionogel with Underwater Self-Healing and Adhesion for Reliable Strain Sensors. *Adv. Mater.* **2021**, 2105306. [CrossRef]
289. von Bleichert, P. Port Security: The Terrorist Naval Mine/Underwater Improvised Explosive Device Threat. Ph.D. Thesis, Public Policy and Administration, Walden University, Washington, DC, USA, 2015.
290. Khatib, M.; Zohar, O.; Haick, H. Self-healing soft sensors: From material design to implementation. *Adv. Mater.* **2021**, *11*, 2004190. [CrossRef] [PubMed]
291. Khatib, M.; Zohar, O.; Saliba, W.; Haick, H. A Multifunctional Electronic Skin Empowered with Damage Mapping and Autonomic Acceleration of Self-Healing in Designated Locations. *Adv. Mater.* **2020**, *32*, 2000246. [CrossRef]
292. Lopez, A.B.; Vatanparvar, K.; Nath, A.P.D.; Yang, S.; Bhunia, S.; Al Faruque, M.A. A Security Perspective on Battery Systems of the Internet of Things. *J. Hardw. Syst. Secur.* **2017**, *1*, 188–199. [CrossRef]
293. Yang, G.; Dai, L.; Wei, Z. Challenges, Threats, Security Issues and New Trends of Underwater Wireless Sensor Networks. *Sensors* **2018**, *18*, 3907. [CrossRef] [PubMed]
294. Cong, Y.; Yang, G.; Wei, Z.; Zhou, W. Security in underwater sensor network. In Proceedings of the 2010 International Conference on Communications and Mobile Computing, Shenzhen, China, 12–14 April 2010; Volume 1.
295. Lal, C.; Petroccia, R.; Conti, M.; Alves, J. Secure underwater acoustic networks: Current and future research directions. In Proceedings of the 2016 IEEE third underwater communications and networking conference (UComms), Lerici, Italy, 30 August–1 September 2016.
296. Wang, Q.; Dai, H.-N.; Li, X.; Wang, H.; Xiao, H. On Modeling Eavesdropping Attacks in Underwater Acoustic Sensor Networks †. *Sensors* **2016**, *16*, 721. [CrossRef] [PubMed]
297. Zuba, M.; Shi, Z.; Peng, Z.; Cui, J. Launching denial-of-service jamming attacks in underwater sensor networks. In Proceedings of the Sixth ACM International Workshop on Underwater Networks, Seattle, WA, USA, 1–2 December 2011.
298. Domingo, M.C. Securing underwater wireless communication networks. *IEEE Wirel. Commun.* **2011**, *18*, 22–28. [CrossRef]
299. Vasudevan, A.R. Security Challenges in NDN Based Underwater Wireless Sensor Networks: An Overview. In Proceedings of the 2nd International Conference on IoT, Social, Mobile, Analytics & Cloud in Computational Vision & Bio-Engineering (ISMAC-CVB 2020), Tirunelveli, India, 29–30 October 2020.
300. Mohsan, S.A.H.; Naqvi, S.S.A.; Banoori, F.; Siddique, M.I.; Mehdi, M.M.; Bruce, F.N.O.; Mazinani, A. A Systematic Review Study on Research Challenges, Opportunities, Threats and Limitations in Underwater Wireless Sensor Networks (UWSNs). In Proceedings of the International Conference on Intelligent and Interactive Systems and Applications, Shanghai, China, 25–27 September 2020; Springer: Cham, Switzerland, 2020.
301. Jiang, H.F.; Xu, Y. Research Advances on Security Problems of Underwater Sensor Networks. *Adv. Mater. Res.* **2011**, *317–319*, 1002–1006. [CrossRef]

302. Diamant, R.; Casari, P.; Tomasin, S. Cooperative authentication in underwater acoustic sensor networks. *IEEE Trans. Wirel. Commun.* **2018**, *18*, 954–968. [CrossRef]
303. Xiao, L.; Sheng, G.; Wan, X.; Su, W.; Cheng, P. Learning-Based PHY-Layer Authentication for Underwater Sensor Networks. *IEEE Commun. Lett.* **2018**, *23*, 60–63. [CrossRef]
304. Ibragimov, M.; Lee, J.-H.; Kalyani, M.; Namgung, J.-I.; Park, S.-H.; Yi, O.; Kim, C.H.; Lim, Y.-K. CCM-UW Security Modes for Low-band Underwater Acoustic Sensor Networks. *Wirel. Pers. Commun.* **2016**, *89*, 479–499. [CrossRef]
305. Souza, E.; Wong, H.C.; Cunha, I.; Vieira, L.F.M.; Oliveira, L.B. End-to-end authentication in under-water sensor networks. In Proceedings of the 2013 IEEE Symposium on Computers and Communications (ISCC), Split, Croatia, 7–10 July 2013.
306. Yun, C.-W.; Lee, J.-H.; Yi, O.Y.; Park, S.-H.; Shin, S.-Y. Design the Secured Message Authentication Code Protocol for Underwater Wireless Sensor Networks. *Adv. Sci. Lett.* **2016**, *22*, 2491–2495. [CrossRef]
307. Shanthi, M.B.; Anvekar, D.K. Secure localization for underwater wireless sensor networks based on probabilistic approach. In Proceedings of the 2018 Second International Conference on Advances in Electronics, Computers and Communications (ICAIECC), Bangalore, India, 9–10 February 2018.
308. Yan, J.; Meng, Y.; Yang, X.; Luo, X.; Guan, X. Privacy-Preserving Localization for Underwater Sensor Networks via Deep Reinforcement Learning. *IEEE Trans. Inf. Forensics Secur.* **2020**, *16*, 1880–1895. [CrossRef]
309. Zhao, H.; Yan, J.; Luo, X.; Guan, X. Privacy preserving solution for the asynchronous localization of underwater sensor networks. *IEEE/CAA J. Autom. Sin.* **2020**, *7*, 1511–1527. [CrossRef]
310. Ansari, Z.; Ghazizadeh, R.; Shokhmzan, Z. Gradient descent approach to secure localization for underwater wireless sensor networks. In Proceedings of the 2016 24th Iranian Conference on Electrical Engineering (ICEE), Shiraz, Iran, 10–12 May 2016.
311. Cai, W.; Yang, J.; Zhang, M.; Peng, S.; Yang, J. Robust and Cooperative Localization for Underwater Sensor Networks in the Existence of Malicious Anchors. *Sensors* **2019**, *19*, 4519. [CrossRef] [PubMed]
312. Misra, S.; Ojha, T. SecRET: Secure range-based localization with evidence theory for underwater sensor networks. *ACM Trans. Auton. Adapt. Syst. (TAAS)* **2021**, *15*, 1–26. [CrossRef]
313. Chandavarkar, B.R.; Gadagkar, A.V. Mitigating Localization and Neighbour Spoofing Attacks in Under-water Sensor Networks. In Proceedings of the 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India, 1–3 July 2020.
314. Zhang, Y.; Jin, Z.; Luo, Y.; Du, X. Node secure localization algorithm in underwater sensor network based on trust mechanism. *J. Comput. Appl.* **2013**, *33*, 1208–1211. [CrossRef]
315. Verma, S.; Prachi, A. Cluster based Key Management Scheme for Underwater Wireless Sensor Networks. *Int. J. Comput. Netw. Inf. Secur.* **2015**, *7*, 54–63. [CrossRef]
316. Petrioli, C.; Saturni, G.; Spaccini, D. Feasibility Study for Authenticated Key Exchange Protocols on Underwater Acoustic Sensor Networks. In Proceedings of the International Conference on Underwater Networks & Systems, Atlanta, GA, USA, 23–25 October 2019. [CrossRef]
317. Zhao, Y.; Chen, Z.; Ding, J.; Tian, B.; Liu, Y. An Energy-Efficient Key Agreement Mechanism for Underwater Sensor Networks. In *IT Convergence and Security 2017*; Springer: Singapore, 2017; Volume 450, pp. 146–158. [CrossRef]
318. Kim, H.; Lee, J.; Yi, O. Key managements of Underwater Acoustic Communication Environments. In Proceedings of the International Workshop on Information Security Applications, Jeju Island, Korea, 24–26 August 2017; Springer: Cham, Switzerland, 2017.
319. Pelekanakis, K.; Gussen, C.M.G.; Petrocchia, R.; Alves, J. Robust Channel Parameters for Crypto Key Generation in Underwater Acoustic Systems. In Proceedings of the OCEANS 2019 MTS/IEEE SEATTLE, Seattle, WA, USA, 27–31 October 2019.
320. Capossele, A.; Petrioli, C.; Saturni, G.; Spaccini, D.; Venturi, D. Securing underwater communications: Key agreement based on fully hashed MQV. In Proceedings of the International Conference on Underwater Networks & Systems, Halifax, NS, Canada, 6–8 November 2017.
321. Gopinath, M.P.; Tamizharasi, G.S.; Kavisankar, L.; Sathyaraj, R. A secure cloud-based solution for real-time monitoring and management of Internet of under-water things (IOUT). *Neural. Comput. Appl.* **2019**, *31*, 293–308. [CrossRef]
322. Nissen, I.V.O.R. Burst communication—a solution for the underwater information management. *Hydroacoustics* **2015**, *18*, 113–126.
323. Yang, G.; Wei, Z.-Q.; Cong, Y.-P. Hierarchical Trust Management in Underwater Wireless Communication Networks. *Period. Ocean. Univ. China* **2013**, *6*. Available online: https://en.cnki.com.cn/Article_en/CJFDTotat-QDHY201306019.htm (accessed on 6 December 2021).
324. Arifeen, M.; Bhakta, D.; Remu, S.R.H.; Islam, M.; Mahmud, M.; Kaiser, M.S. Hidden Markov Model based Trust Management Model for Underwater Wireless Sensor Networks. In Proceedings of the International Conference on Computing Advancements, Dhaka, Bangladesh, 10–12 January 2020. [CrossRef]
325. Arifeen, M.M.; Islam, A.A.; Rahman, M.M.; Taher, K.A.; Islam, M.M.; Kaiser, M.S. Anfis based trust management model to enhance location privacy in underwater wireless sensor networks. In Proceedings of the 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE), Cox’sBazar, Bangladesh, 7–9 February 2019.
326. Bolster, A.; Marshall, A. Single and Multi-metric Trust Management Frameworks for Use in Underwater Autonomous Networks. In Proceedings of the 2015 IEEE Trustcom/BigDataSE/ISPA, Helsinki, Finland, 20–22 August 2015; Volume 1, pp. 185–693. [CrossRef]
327. Han, G.; Du, J.; Lin, C.; Wu, H.; Guizani, M. An Energy-Balanced Trust Cloud Migration Scheme for Underwater Acoustic Sensor Networks. *IEEE Trans. Wirel. Commun.* **2019**, *19*, 1636–1649. [CrossRef]

328. Jiang, J.; Zhu, X.; Han, G.; Guizani, M.; Shu, L. A dynamic trust evaluation and update mechanism based on C4.5 decision tree in underwater wireless sensor networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 9031–9040. [[CrossRef](#)]
329. Goyal, N.; Dave, M.; Verma, A.K. Trust model for cluster head validation in underwater wireless sensor networks. *Underw. Technol.* **2017**, *34*, 106–113. [[CrossRef](#)]
330. Han, G.; Liu, L.; Jiang, J.; Shu, L.; Rodrigues, J.J. A Collaborative Secure Localization Algorithm Based on Trust Model in Underwater Wireless Sensor Networks. *Sensors* **2016**, *16*, 229. [[CrossRef](#)] [[PubMed](#)]
331. He, Y.; Han, G.; Jiang, J.; Wang, H.; Martinez-Garcia, M. A Trust Update Mechanism Based on Reinforcement Learning in Underwater Acoustic Sensor Networks. *IEEE Trans. Mob. Comput.* **2020**, *1*. [[CrossRef](#)]
332. Cong, Y.P.; Wei, Z.Q.; Yang, G. Trust Management for One-Hop Cluster-Based Underwater Wireless Sensor Networks. *Adv. Mater. Res.* **2012**, *488–489*, 1163–1167. [[CrossRef](#)]
333. Mazdin, P.; Arbanas, B.; Haus, T.; Bogdan, S.; Petrovic, T.; Miskovic, N. Trust Consensus Protocol for Heterogeneous Underwater Robotic Systems. *IFAC-Pap.* **2016**, *49*, 341–346. [[CrossRef](#)]
334. Buddesab, T.; Thriveni, J.; Venugopal, K.R. Trust model genetic node recovery based on cloud theory for underwater acoustic sensor network. *Int. J. Electr. Comput. Eng.* **2019**, *9*, 3759.
335. Han, G.; He, Y.; Jiang, J.; Wang, H.; Peng, Y.; Fan, K. Fault-Tolerant Trust Model for Hybrid Attack Mode in Underwater Acoustic Sensor Networks. *IEEE Netw.* **2020**, *34*, 330–336. [[CrossRef](#)]
336. Du, J.; Han, G.; Lin, C.; Martinez-Garcia, M. ITrust: An Anomaly-resilient Trust Model Based on Isolation Forest for Underwater Acoustic Sensor Networks. *IEEE Trans. Mob. Comput.* **2020**, *1*. [[CrossRef](#)]
337. Liang, K.; Huang, H.; Huang, X.; Yang, Q. CS-Based Homomorphism Encryption and Trust Scheme for Underwater Acoustic Sensor Networks. In Proceedings of the International Conference on Machine Learning and Big Data Analytics for IoT Security and Privacy, Shanghai, China, 6–8 November 2020; Springer: Cham, Switzerland, 2020.
338. MIT, Massachusetts Institute of Technology. A Battery-Free Sensor for Underwater Exploration. 2021. Available online: <https://news.mit.edu/2019/battery-free-sensor-underwater-exploration-0820> (accessed on 28 October 2021).