Received <day> <Month>, <year>; | Revised <day> <Month>, <year>; | Accepted <day> <Month>, <year>

DOI: xxx/xxxx

ARTICLE TYPE

Security Challenges of Internet of Underwater Things: A Systematic Literature Review

Aliyu Gana Yisa*[1] | Tooska Dargahi[1] | Sana Belguith[1] | Mohammad Hammoudeh[2]

[1]School of Science, Engineering and Environment, The University of Salford, Manchester, United Kingdom

[2]Faculty of Science and Engineering, Manchester Metropolitan University, Manchester, United Kingdom

Correspondence
Aliyu Gana Yisa, School of Science, Engineering and Environment, The University of Salford. Email: a.g.yisa@edu.salford.ac.uk

Present Address
Present address

Abstract

Water covers approximately 71% of the earth surface, yet much of the underwater world remains unexplored due to technology limitations. Internet of Underwater Things (IoUT) is a network of underwater objects that enables monitoring subsea environment remotely. Underwater Wireless Sensor Network (UWSN) is the main enabling technology for IoUT. UWSNs are characterised by the limitations of the underlying acoustic communication medium, high energy consumption, lack of hardware resources to implement computationally intensive tasks and dynamic network topology due to node mobility. These characteristics render UNWSNs vulnerable to different attacks, such as Wormhole, Sybil, flooding, jamming, spoofing and Denial of Service (DoS) attacks. This article reviews peer-reviewed literature that addresses the security challenges and attacks on UWSNs as well as possible mitigative solutions. Findings show that the biggest contributing factors to security threats in UWSNs are the limited energy supply, the limited communication medium and the harsh underwater communication conditions. Researchers in this field agree that the security measures of terrestrial wireless sensor networks are not directly applicable to UWSNs due to the unique nature of the underwater environment where resource management becomes a significant challenge. This article also outlines future research directions on security and privacy challenges of IoUT and UWSN.

KEYWORDS:
Internet of Underwater Things, Underwater Wireless Sensor Network, Security and Privacy, Resource Management

1 | INTRODUCTION

Advances in acoustic communication and sensor technologies of Underwater Wireless Sensor Networks (UWSNs) lead to the emergence of the Internet of Underwater Things (IoUT) for underwater condition monitoring [1]. UWSNs are composed of mobile or stationery nodes that collect data using onboard sensors and communicate via low frequency acoustic signals. The sensor nodes collect and transmit sensory data to buoyant gateway nodes which in turn relay the data to the nearest coastal remote station [1,2]. There has been an increasing interest in monitoring the underwater environment for scientific, industrial and military purposes, and as such the popularity of UWSN is growing [1 3]. According to a market outlook report for 2017-2026 by Stratistics MRC [4], the Wireless Sensor Network (WSN) market is projected to grow at a Compound Annual Growth Rate (CAGR) of 18.9%

globally, and the underwater segment is expected to see the highest growth during the forecast period. Existing applications include environment monitoring, underwater exploration, disaster alert, military applications, assisted navigation, water-based sports and other commercial purposes [1].

There are several recent research articles on UWSNs that demonstrate advancements in the field. For example, Pessoa et al. (2019) [5] explore the possibility of long-term deployment of a large-scale UWSN of abandoned nodes, powered by visiting Autonomous Underwater Vehicles (AUVs). This study aims to reduce operation costs and increase the lifetime of UWSNs. Another research study by Rahman et al. (2020) [6] presents a new opportunistic routing protocol to improve network performance. Kumar et al. (2020) [7] propose a scheme to prolong the lifespan of UWSNs by increasing energy efficiency. In another study, N. Javaid [8] proposes NADEEM (Neighbour node approaching distinct energy-efficient mates) to enhance energy efficiency and improve data delivery reliability. Also, a recent study by Hussain et al. [9] attempts to improve routing in UWSN by avoiding void hole through two hop verification. The authors propose three schemes and assess their performance using packet delivery ratio, energy consumption and end-to-end delay as performance metrics.

Moreover, there have also been recent real-world applications of UWSNs to solve practical human problems. One of such is their use by archaeologist divers in 2020 to communicate in real-time at the bottom of the sea in Rome [10]. Additionally, they use the technology to monitor water quality, CO2 levels and the volcanic activity of Campi Flegrei. In 2019, MIT researchers invented and tested a battery-free underwater sensor that uses low energy to transmit data [11]. They demonstrated the sensor in a pool and were able to collect water temperature and pressure movements.

1.1 | The Characteristics of UWSNs

This subsection highlights the characteristics of UWSNs that have impact on their security challenges. According to Das and Thampi (2015) [12], "Most current WSN security protocols assume sensor networks as stationary. Moreover, the network performance reduces with the addition of security techniques". This statement underscores the main reason why security mechanisms in terrestrial Wireless Sensor Networks (WSNs) should not be directly applied to UWSN.

1) Communication channel: Unlike WSNs, UWSN nodes typically communicate via acoustic signals [13]. This results in lower propagation speed, lower bandwidth and higher bit error rate than WSNs [14]. The useful acoustic bandwidth is only a small fraction of useful RF bandwidth [15]. Furthermore, due to the open nature of this channel, it is easy for an attacker to intercept or block communications [12].

2) Operating environment: Due to ocean currents, the sensor nodes are mobile, leading to a dynamic network topology [16]. The changes in network topology may influence data routing and accuracy of data transmission [13]. Node mobility also highlights the necessity of secure and accurate localization and time synchronization. Moreover, UWSNs are sparsely populated (low density) compared to their terrestrial counterparts, leading to higher distance between nodes.

3) Energy and hardware: UWSN nodes are limited in energy, computational power and storage space. Furthermore, with higher distances and complex signal processing to account for the attenuation of signals, UWSNs consume more power [13]. While WSNs can be recharged using solar power, UWSNs can not be recharged or maintained easily due to being deployed underwater [13]. This further increases the constraints on energy, which impacts security by reducing the types of security mechanisms that can be implemented.

1.2 | Security Challenges

UWSNs face several security challenges that could potentially compromise the purpose for their existence. The limited energy, computational power and memory of UWSN nodes makes them vulnerable to several attacks, especially those aimed at draining their scarce resources and consequently reducing their lifespan. The high bit error rates during transmission, propagation delays and low bandwidth of the acoustic channel of communication that UWSNs exhibits make them vulnerable to communication manipulation attacks [17]. Furthermore, when UWSNs are applied for military purposes, the nodes become susceptible to tampering or destruction attacks [16]. Attacks on UWSNs can cause serious damage to the reliability, availability and confidentiality of the nodes and the information that they gather. Some of the adverse effects include:

- Node compromise: Where a node is captured by an attacker and has its data read or modified. Such nodes may then be injected into the network to eavesdrop or disrupt communications [13].

- Routing failure: Routing attacks are capable of preventing or diverting the delivery of packets in the network [13].
- Denial of Service: There are different ways of carrying out denial of service attacks to UWSNs, but they all have the same effect of preventing legitimate nodes from accomplishing their mission [13].

  This research focuses on establishing the state-of-the-art on security challenges, risks and specific threats or vulnerabilities in UWSN systems, including issues related to architecture and protocols. Security challenges are discussed further in-depth in 4.

1.3 | Prior Research

A recent study by Qiu et al. (2020) provides an overview of the Underwater Internet of Things (UIoT), highlighting challenges, open research issues, applications, current advances and future system architecture [18]. Although UIoT is a related concept to the IoUT (Internet of Underwater Things); it focuses on the combination of powerful and advanced technology geared towards achieving the smart ocean [18]. Another recent survey on IoT security by Mrabet et al. [19] provides an insight on the protocols, hardware and networking of IoT and their security threats and solutions. However, this article does not cover the unique challenges of IoUT in specific.

Regarding the security challenges facing UWSNs, to the best of our knowledge, there appears to be no systematic literature review (SLR). However, there have been some survey and other research papers that provide insight into various aspects of UWSNs security, which we briefly discuss in this section. The most recent survey on the security challenges of underwater wireless sensor networks is presented by Yang et al. in 2019 [13]. The authors discuss the challenges, constraints and attacks to UWSNs and present a categorization of the attacks. The study presents a recent view of the field and can serve as a good starting point for researchers seeking to understand the security requirements and challenges in UWSN technology. It does provide an overview on the security challenges, but it lacks a detailed explanation on the attacks and countermeasures against them which we provide in this paper. In [20], the authors survey the security challenges of UWSNs, possible attacks and secure localisation and routing techniques. They highlight specific protocols and security mechanisms, as well as open research challenges. They explained that many research studies only present simulation results with localisation and routing algorithms and concluded that performance of the network needs to be evaluated in real world scenarios. Their focus is solely on localisation and routing, and does not cover the wide spectrum of challenges, attacks and security techniques. In 2017, Dargahi et al. present a distributed approach for detection and mitigation of routing attacks to UWSNs [14]. Although it is not a survey paper, it presents a background on the unique challenges of UWSNs and routing attacks, while proposing local monitoring approaches. The focus of [14] is only on routing attacks. Yunus et al. [21] conducted a survey of the existing Medium Access Control (MAC) mechanisms for UWSNs. They highlighted the factors that influence underwater protocol design which includes some of the challenges (i.e., transmission loss, multipath, noise and propagation delay). However, it does not include the attacks to UWSNs and their countermeasures. Since 2010, there have been several research papers in this domain which are included in our literature review in Section 3.

All the above-mentioned studies provide insights into the security challenges, threats and proposed prevention, detection and mitigation techniques. However, some of them are focused on a particular area, such as routing, localisation or access control, and the others are not quite recent. As a growing technology, advances are being made in improving the security features of IoUT and UWSNs with new techniques and protocols. Hence, it is imperative that a current survey of the recent research papers related to the security of UWSNs is provided, in order to aid future research.

1.4 | Research Goals

We aim to provide such an updated review of the state-of-the-art in the field of UWSN security and its challenges. This will help researchers and practitioners who seek to propose new detection, prevention and mitigation methods to overcome UWSN security issues. We have considered three research questions (as presented in Table 1) to formulate our contribution.

The main contributions of this paper are as follows:

- 31 primary studies are identified that are related to the security challenges, attacks and mitigative methods in the UWSNs (which are proposed between 2005 and early 2020). This list of studies could be used as a base for the future work to facilitate research in the field.
- A comprehensive review of the data extracted from the 31 sources is conducted, summarizing the main security challenges, attacks and countermeasures.

TABLE 1 Research Questions

Research Questions (RQ)	Discussion
RQ1: What are the current security challenges in IoUT and UWSN?	As stated in Section 1, there have been recent research studies and real-world applications of UWSN technology. A review of recent findings on the security challenges will help us to understand the trending security risks and threats associated with this technology.
RQ2: What attacks are possible on UWSNs?	A major part of understanding the security challenges of UWSN associates with knowing the attack vectors and their effect on the functionality of the network.
RQ3: What are the methods available to overcome the challenges and defend against possible attacks?	This will provide an insight into the existing methods used to mitigate the challenges and improve the security and privacy of the IoUT to provide an insight into the future research directions.

- A discussion on the main contributing factors to the identified security challenges is provided following a guideline for future research direction.

The layout of this paper is as follows: Section 2 describes the research methodology and the adopted approach for systematic selection of primary studies. Section 3 presents the findings from the primary studies. Section 4 discusses the main challenges and answers the identified research questions. Section 5 highlights future research directions, while Section 6 concludes the paper.

2 | RESEARCH METHODOLOGY

In order to answer the research questions, an SLR was conducted in accordance with the guidance published by Kitchenham and Charters [21]. All papers were passed through inclusion and exclusion criteria and quality assessment to ensure that only relevant and high-quality papers are included.

2.1 | Selection of Primary Studies

Primary studies were obtained by passing keywords to the search facility of online publications and search engines. The keywords were chosen to facilitate the emergence of relevant scholarly articles that would aid providing answers to the research questions. The adopted Boolean operators were AND and OR. The search strings were:

a (“UWSN” OR “underwater wireless sensor network” OR “underwater sensor network”) AND “security”

b ("Underwater sensor network" OR "Underwater Wireless Sensor Network" OR "UWSN") AND ("Cyber Security" OR "Network Security)

The platforms searched were:

- IEEE Xplore Digital Library
- ScienceDirect
- ACM Digital Library

TABLE 2 Inclusion and Exclusion Criteria

Criteria for Inclusion	Criteria for Exclusion
The paper must present empirical data related to the security of underwater wireless sensor networks	Papers focusing on the application of underwater wireless sensor networks
The paper must contain information related to underwater wireless sensor networks	Papers focusing on other kinds of wireless sensor networks (e.g. terrestrial wireless sensor network, unattended wireless sensor network)
The paper must be peer-reviewed and published in a journal or conference proceeding	Non-English papers
	Grey literature such as blogs or government documents

- SpringerLink
- Google Scholar

Depending on the platform, searches were run against the title, keywords or abstract. All papers that appeared in the results were processed and filtered through the inclusion and exclusion criteria as shown in Section 2.2.

2.2 | Inclusion and Exclusion Criteria

Studies to be included in this SLR must present empirical findings. They may be papers on case studies, UWSN security challenges, vulnerabilities in UWSN applications, attacks to UWSN, detection, prevention and mitigation techniques, and proposals for new security mechanisms for UWSN. Studies must be peer-reviewed and written in English. The key inclusion and exclusion criteria are shown in Table 2 .

2.3 | Selection Results

A total of 870 studies were returned in the initial keyword searches on the chosen platforms. After removal of duplicates, this was reduced to 723. The studies were then inspected using the inclusion and exclusion criteria and 41 papers were remaining for studying. The 41 papers were read in full while reapplying the inclusion and exclusion criteria, leaving 31 papers to be finally included as primary studies.

2.4 | Quality Assessment

The quality of primary studies was assessed using a quality assessment checklist according to the guidance set by Kitchenham and Charters [21]. This was to assess the relevance of the papers to the research questions and ascertain the value of the data to answering them. The following quality assessment process was followed.

- **Step 1: UWSN.** The main focus of the paper must be underwater wireless sensor networks.
- **Step 2: Context.** The paper must provide enough context for the objectives and findings of the research.
- **Step 3: Security challenges.** The paper must provide relevant information on the security challenges or attacks to underwater sensor networks. This will be useful in answering the RQ1 and RQ2.
- **Step 4: Security solution.** The paper must provide information on a solution in an attempt to solve at least one security challenge. This will aid in answering the RQ3.

TABLE 3 Excluded Studies

Checklist for the Criteria Steps	Excluded Studies
Step 1: UWSN	[2] [3] [4]
Step 2: Context	
Step 3: Security challenges	[5] [6] [7] [8] [9] [10] [11]
Step 4: Security solution	
Step 5: Data acquisition	

- **Step 5: Data acquisition.** To determine accuracy, the paper must explain how the data was acquired and measured.

2.5 | Data Extraction

All the included primary studies had their data extracted to assess the completeness and accuracy of the information recorded. The data extraction process was performed on all studies that passed the inclusion criteria. The data from each paper was extracted, categorised and recorded. The categories are as follows.

- Context data: data about the objectives and focus of the study.
- Qualitative data: Findings and conclusions presented.
- Quantitative data: When applicable, data observed by experimentation and research.

2.6 | Data Analysis

In order to meet the objectives of answering the research questions, data held within the qualitative and quantitative categories was compiled and analysed thoroughly.

2.7 | Publications Over Time

Research work related to the security of UWSNs have grown over time. The first primary paper was published as far back as 2005. However, few studies were published in that decade. Since 2011, there has been a rise in the publication of primary studies related to UWSN security. This is consistent with the growth in the application of the technology and shows that interest in the research area has grown. Figure 1 shows the number of published primary studies in each year since 2005. Although the number of studies published in each year fluctuates, there is an overall long-term growth.

3 | FINDINGS

Each research paper was read in full, after which relevant qualitative and quantitative data was extracted and summarized. All primary papers had a focus in relation to the security challenges, attacks or security mechanisms and techniques in UWSNs.

3.1 | Key Focus Areas

In order to identify the common focus areas and themes in the primary studies, we performed a count on the number of papers focused on each security area. These include challenges, attacks or security mechanisms as shown in Table 4 and illustrated in Figure 2 . This count only includes papers where the area is a main focus of the research work. It is important to note that there are overlapping focus areas, such as a detection model for a specific attack. The focus areas that received the most attention are attacks, detection algorithms and authentication mechanisms. The findings from the primary studies are discussed in Section 3.2.

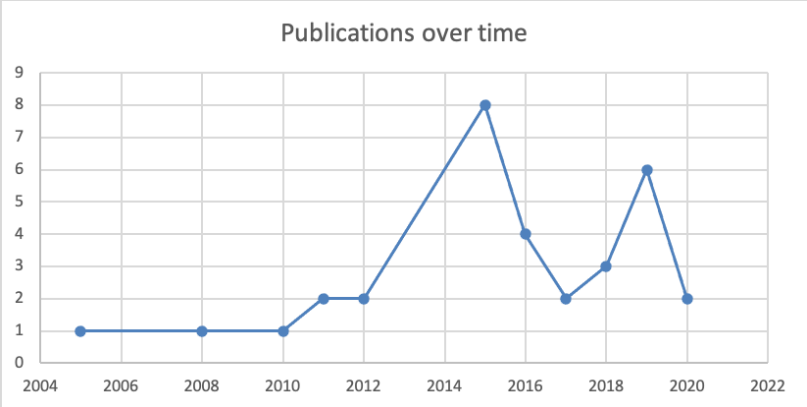

FIGURE 1 Publication Over Time

TABLE 4 Focus Areas

Focus Area	Paper Count
Security Attacks	7
Detection Algorithm	6
Authentication	4
Localization Security	3
Trust Management	3
Key Management	2
Data Management	2

3.2 | Findings

In this section, we discuss the main findings in the selected primary research papers. We introduce for each studied paper, the researched security area as well as the context and the contributions presented. The primary studies are divided into three main categories:

1. Security Challenges: this part includes papers that mainly provide information about the general security challenges, vulnerabilities and constraints of UWSNs,
2. Security Attacks: this part presents papers that provide insights on security attacks and demonstrate the attack methods,
3. Attack Detection and Mitigation: this part includes papers that provide details about methods for detecting and mitigating attacks on UWSNs.

3.2.1 | Security Challenges

Considering that one of our search keywords was "security", all of the primary studies discuss security challenges to some extent. However, this section only includes those papers whose main focus is the security challenges not a specific attack or mitigation.

Cong et al.[16] present the characteristics, attacks, defences and challenges in UWSN. They argue for a multi-layered approach towards securing UWSNs. They state that DoS (Denial of Service) attacks are the most destructive attacks to UWSNs, as they can be executed despite the presence of a strong encryption algorithm. Furthermore, DoS attacks are low-cost and relatively easy to execute, capable of decreasing the availability of the network and wasting scarce energy. Domingo[22] summarises the characteristics and vulnerabilities of UWSNs and explains their security requirements and possible attacks. Also, the differences between the security of terrestrial wireless sensor networks and UWSNs are explained in[22]. The author concludes that security measures for regular WSNs are not directly applicable to UWSNs. Das and Thampi[23] discuss the security requirements of UWSNs, security mechanisms, various DoS attacks and localization methods. Through simulation, they analyse the performance

FIGURE 2 Focus Areas

variation between WSNs and UWSNs. A mobile UWSN was simulated under varying mobility rates to analyse the impact of out-of-coverage problems. They also simulated a flooding attack and measured the performance of the network under varying malicious node densities. They found that there was a high level of degradation in performance during attacks. Mian and Kumar[24] discuss the security requirements, threats and challenges in UWSNs. They also discuss active and passive attacks to UWSNs.

Yang et al.[13] discuss recent security challenges and attacks to the UWSN. They highlight the particularities and constraints that are unique to UWSNs including the communication medium, hardware limitations, dynamic network topology and the operating environment. Shahapur and Kahnai[20] discuss localization and routing protocols, their techniques and security challenges. Approaches to tackling the issues are suggested. We have provided a detailed summary of all the security challenges in Section 4.1.

3.2.2 | Security Attacks

This section includes studies that mainly provide information on specific security attacks. Kong et al.[16] highlight low-cost attacks against localization, packet delivery and time synchronization. They have provided an evaluation of the threats and their impact. The authors conclude that these attacks threaten all UWSNs as they exploit the characteristics of the underwater acoustic channel. They also propose that security should be unified in the design phase of UWSNs. Zuba et al.[25] provide an analysis of various jamming attacks and how they are executed. The metrics used for their analysis are: packet delivery ratio (PDR), packet send ratio (PSR) and network throughput. A view of the network performance during these attacks were shown based on the above mentioned metrics. The results showed that constant and reactive jamming has the most effect, with reactive jamming being the most efficient. They conclude that jamming attacks can be easily launched and degrade the performance of a network to a large extent. Xiao and Zhu[26] discuss the architecture of a wormhole attack and demonstrate the results through simulation using Aqua-Sim[27], which is a simulation software designed for UWSNs. Misra et al.[28] discuss security attacks to UWSNs and present methods for jamming detection while maintaining network operation in the unaffected areas. Similar to the other research studies, they conclude that countermeasures against jamming in terrestrial sensor networks could not be applied directly to UWSN. A list of security attacks that are presented in the primary studies are as follows.

- **Jamming:** a jamming attack is performed by injecting unwanted signals into the channel, thereby occupying the network channel and disrupting legitimate communications[25,29,30,28]. Jamming attacks are especially dangerous to the network because no special hardware is required, the open communication medium can be interfered in order to make the attack smarter; also this attack can be executed with minimal cost[25]. In addition to sabotaging communications, jamming can

degrade the overall lifetime of the network by depleting sensor node batteries[30]. Jamming is classified as a denial of service attack. Jamming can be categorised into four types:

i Constant jamming: the jammer regularly injects noise into the channel to congest the network or corrupt packets[25].

ii Deceptive jamming: the jammer has some information about the network's protocols and utilises legitimate packets instead of noise to disrupt the network[28,25].

iii Random jamming: the jammer randomly switches between sleeping and injecting packets[25]

iv Reactive jamming: the jammer listens to communications and remains idle until activity is sensed, then proceeds to transmit jamming signals[25,28].

- **Wormhole:** in a wormhole attack, an attacker uses two malicious nodes to tunnel traffic through the network[14,26,31]. The two colluding nodes capture packets and transmit them to the destinations using an external communication channel or the existing network infrastructure, leading to the creation of false neighbour connections and an illusion of a shortcut route to increase their probability of being selected in routing[26,31]. The wormhole can be used to perform denial of service by selectively dropping packets, traffic analysis, or to enable further attacks[26,20]. This is categorized under routing and localization attacks.

- **Sybil:** in Sybil attack, an attacker pretends to be in multiple locations simultaneously, with multiple identities[20,24,22], thereby misleading routing protocols[20,22]. This is categorised as a routing attack.

- **Sinkhole:** a malicious node falsely declares itself as the best route to the base station[20,14], deceiving neighbouring nodes into using the route more frequently[14]. A sinkhole attack can be executed by using a compromised insider node or a high-performance external device[14]. This is categorised as a routing attack.

- **Blackhole:** a malicious node attempts to impersonate a destination node or forge route reply messages sent to the source node, and discards packets to ensure that they do not get to the destination[21,32,33]. This is a denial of service attack.

- **Spoofing:** a malicious node pretends to be another node by using a fake MAC address or gaining illegal access to facilitate further attacks[34]. Another type of spoofing in UWSN is acknowledgement spoofing, where a malicious node overhears neighbour nodes and spoofs link-layer acknowledgements with the objective of reinforcing a weak link[22,20]. This directly leads to packet loss and disruption of the network; therefore, it is categorised as a denial of service attack.

- **Flooding:** in flooding attack, an adversary transmits an excessive amount of connection requests to nodes in order to deplete their resources[16,24]. This is a denial of service attack. Hello flooding is a slightly different kind of flooding attack (an insider attack), in which a malicious node sends HELLO packets to other nodes to create a false assumption that the attacker is a neighbour[20]. This is a routing attack.

3.2.3 | Attack Detection and Mitigation

This section reviews the primary studies which propose an attack detection or mitigation solution. Martin and Rajasekaran[32] analyse DoS attacks and propose an adaptive protocol for async channel conditions and a reactive algorithm to detect and defend against DoS attacks. Their approach towards mitigating attacks is based on information-centric networking (ICN) and named data networking (NDN). Ahmad et al.[35] propose a method of intrusion detection through the classification of DoS attacks with attack models. A network simulation was performed using NS2 network simulator to gather network traffic and create a dataset. The dataset was then trained via an Artificial Neural Network for the classification. Ahmed et al.[36] present challenges to security and the differences between UWSN and WSN in environment and application. They apply the use of machine learning - Support Vector Machine in malicious attack detection.

Dargahi et al.,[14] discuss the unique challenges of UWSNs and routing attacks and propose a distributed approach for detecting and mitigating routing attacks. They also provide a detection and isolation model for malicious nodes based on defined thresholds. Wang et al.[31] focus on the detection of wormhole attacks and use a distributed approach for the visualisation and detection of such attacks. Bagali and Sundaraguru[29] discuss different types of jamming attacks to UWSN. They then present an efficient channel allocation scheme and a novel cross-layer design for cooperative communication to detect jammed nodes and utilise the spectrum efficiently. Xiao et al.[30] apply game theory for detecting jamming attacks and propose a learning-based power control

strategy to address jamming attacks with unknown channel parameters of the attacker. They formulate the interactions between a UWSN and a reactive jammer as two jamming games.

Kalkan and Levi[37] propose a key distribution scheme applied to nomadic mobility model and meandering mobility model. According to Yun et al.[38] HIKES (Hierarchical Key Establishment Scheme), using PKET (Partial Key Escrow Table) is used in WSNs, but is not appropriate for UWSNs due to node mobility. Also, replacement of nodes is difficult in UWSN in the case that a node is seized. Instead , a ticket-based authentication scheme is proposed. Xu and Liu[39] propose SenseVault – a three-tier framework for UWSN security. The three tiers are: 1) a cubic cluster formation to adapt to dynamic environments using cryptographic hash functions to derive secret keys for authentication; 2) a lightweight node revocation and authentication key update mechanism based on higher order polynomial (addressing node mobility); 3) VPS (Virtual phase shift), a phase quantisation approach for key generation at the physical layer. According to the authors, it is the first attempt to provide a comprehensive key management framework for secure data collection in mobile UWSNs.

Yuan et al.[40] propose a low computational complexity scheme for authentication using matrix addition and present a simulation of the results. In their scheme, the base station generates a configuration for each node, reducing memory cost. Zero knowledge proof protocol is used to verify authentication and prevent secret key disclosure. Ahmed et al.[17] propose an algorithm based on Dempster-Shafer Theory (DST) to identify attacks. It perceives the parameters of neighbour nodes and makes a decision to identify abnormal nodes based on DST. Khan et al.[33] discuss UWSN security threats and propose an algorithm for data aggregation, encryption and transfer. Li et al.[34] propose an authentication scheme to detect spoofing attacks in UWSN. The spoofing detection is done by evaluating the digital signature or channel characteristics variance with a threshold. The technique based on reinforcement learning.

Jiang et al.[41] highlight UWSN security mechanisms and trust management schemes, and propose a new trust model (Trust Cloud Model). They conclude on three main challenges to trust management: the underwater environment and the acoustic communication channel, node mobility and sparse node deployment. Yang et al.[42] discuss constraints and challenges in UWSN, and study trust management. The authors propose a secure and energy balanced protocol based on an adaptive algorithm to prolong network lifetime and improve security. Arifeen et al.[43] discuss the importance of location privacy and propose a trust management model. Goyal et al.[44] focus on secure authentication of Cluster Heads and protected data aggregation. CHs are authenticated to gateways to ensure that the CHs serving each cluster are not compromised. In the second module, each sensor node protects the data using symmetric key encryption before transmitting to CH. Data is then securely aggregated and transmitted to the base station.

Ansari et al.[45] propose and simulate a gradient descent approach for secure localisation. In the proposed model, which is called cooperative localization method, sensor nodes calculate their positions using received information from anchor nodes and then send a broadcast to neighbours. Each node can then calculate its distance to other nodes and determine its location using the gradient descent approach. Shanthi and Anvekar[46] propose a new framework for secure localisation using probabilistic scheme. They state that compromised or intruding nodes may sabotage the localisation process and lead to disconnection of legitimate nodes. The authors present a model for isolating malicious nodes. Zhao et al.[47] discuss several localization algorithms and propose a new asynchronous localization protocol. The authors developed a privacy preserving mechanism for asynchronous localization.

4 | DISCUSSION

A large percentage of the primary studies are focused on addressing a particular threat or group of attacks, proposing new algorithms[17,36,45] and security models[43,48,29]. The other papers are focused on demonstration and classification of attacks and threats, such as denial of service, localisation and routing attacks[25,26,31], as well as presenting security issues and key research challenges[16,22,13]. These studies are mostly evaluated using simulations. A common theme within majority of the primary studies is the peculiarity of UWSN that makes its operation and security challenges considerably different from its terrestrial counterpart, including energy consumption, localisation, node mobility and maintenance. Researchers are mostly in agreement that the security mechanisms of terrestrial WSNs are not necessarily applicable to UWSNs. UWSNs are limited in hardware resources (computation, energy and storage space) and they consume more power than their terrestrial counterparts due to longer distances and more complex signal processing[13]. Another factor is the unreliable communication channel due to the lower bandwidth of the acoustic channel, coupled with the open and often unsupervised underwater channel, making them more susceptible to eavesdropping and other malicious attacks[13]. A wide range of approaches have been presented towards solving the problems

including machine learning, cryptography, statistics and adaptation of existing networking protocols. In what follows we answer the research questions based on the research findings.

4.1 | RQ1: What are the Current Challenges to Security in Underwater Wireless Sensor Networks?

The security challenges to underwater wireless sensor networks are mostly bordered on the peculiarities of the underwater environment and the limitations caused by the use of acoustic signal as a medium for communication [13]. The studies show a consistent set of challenges to UWSN security:

- Communication medium: due to the use of low-frequency acoustic signals, UWSNs are affected by propagation delay, path loss, noise, Doppler spread, which increases the error rate, packet loss and node failure rate [15,13,14,16]. Furthermore, the open acoustic channel leads to an increased susceptibility to several attacks [13].
- Dynamic network topology: most of the sensor nodes are highly mobile due to the flow of water, moving at speeds of up to 36km/h and resulting in a highly dynamic network topology [13,16]. These variations affect the data routing and influence its accuracy [13].
- Energy, computation and maintenance constraints: nodes deployed run on battery power and due to the underwater environment, renewable energy sources like solar power cannot be adopted, and battery replacement is not possible [16,13,14]. The power consumption is also higher than in terrestrial networks [13], further compounding the problem. This has led to the optimisation of energy efficiency at the expense of security [13].
- Harsh underwater environment and physical security: in military applications, UWSNs may be deployed in hostile environment and are vulnerable to malicious attacks [13 16]. Also, nodes could be physically damaged by underwater organisms, temperature changes and other underwater phenomenon, and protecting the nodes is difficult due to the unattended nature of such environments [13].
- Localisation: localisation is important in UWSNs due to the need to identify the location where data has been recorded [13 20], and while several localisation techniques have been proposed for terrestrial WSNs, they are not directly applicable to UWSNs [20]. Localisation algorithms need to be able to securely determine the location of sensor nodes, even while localisation attacks are present [13].

4.2 | RQ2: What Attacks are Possible to UWSNs

Underwater wireless sensor networks are vulnerable to several attacks, which are either as a result of, or made more severe by the challenges highlighted in Section 4.1. Execution of some of these attacks are low-cost, while at the same time reducing the life and utility of the network. The attacks are generally categorised into active and passive attacks. Active attacks are further categorised as routing, localisation, and denial of service attacks, with some attacks overlapping categories. Due to the unique characteristics of UWSNs, they are more vulnerable to majority of the attacks than terrestrial networks. The possible attacks to UWSNs (as explained in 3.2.2) are Jamming, Wormhole, Sybil, Sinkhole, Blackhole, Spoofing and Flooding attacks.

4.3 | RQ3: What are the Methods Available to Overcome the Challenges and Defend Against Possible Attacks?

Towards improving the security of UWSNs, several approaches have been proposed, some tackling specific challenges or attacks, and others offering general solutions. In [17], the researchers proposed a novel algorithm for attack detection by monitoring the parameters of neighbouring nodes based on Dempster-Shafer Theory. Another algorithm was proposed in [36] to detect malicious attacks using support vector machine (SVM). Some attacks have received more research attention than others. On physical and MAC layer security, multiple primary studies agree that code-division multiple access (CDMA) is a promising technique [16,14]. A recent study by Mrabet et al. Researchers in [49] provide a detailed survey of synchronous and asynchronous optical CDMA systems. CDMA assigns a unique code to each user for transmission of data and provides data confidentiality, efficient bandwidth usage, low interception probability and an effective network control design [49]. Some primary studies were focused on secure localisation. In [45], the researchers proposed a gradient descent approach to secure localization in UWSN, where the nodes

calculate position using previously received information, apply the proposed algorithm and reduce error by cooperative localization. In[46], a new framework for secure localization based on probabilistic scheme is proposed, including a security model for malicious node isolation.

To defend against the attacks highlighted in Section 4.2, some security mechanisms have been proposed by researchers:

a. **Countermeasures to defeat jamming attacks:** Xiao et al. in 2015[30] propose an application of game theoretic study on jamming to UWSN, and propose a learning based power control strategy to address jamming attacks with unknown channel parameters of the attacker. The interactions between a UWSN and a reactive jammer are formulated as two jamming games. A jamming detection algorithm is presented by Misra et al.[28] where nodes strategically exchange discovery and acknowledgement packets. Bagali et al.[29] present an efficient channel allocation scheme, a novel cross-layer design for cooperative communication to detect jamming.

b. **Countermeasures to defeat routing attacks:** Dargahi et al.[14] propose a collaborative strategy for the detection and mitigation of routing attacks. In this study, nodes broadcast discovery packets, silently monitor the channel and store all packets from neighbours. The nodes then search for discrepancies in the communications[14]. They describe methods by which the scheme can detect sinkhole and wormhole attacks and present a scheme to isolate detected malicious nodes. A distributed approach is presented by Wang et al. for detecting wormhole attacks by visualising distortions in the network[31].

c. **Countermeasures to defeat spoofing attacks:** In 2015, Li et al.[34] propose an authentication scheme to detect spoofing attacks based on reinforcement learning. The researchers formulated the interactions between the surface station and the spoofer as a zero-sum game to increase the accuracy of spoofing detection. The simulation results were shown to enhance detection.

d. **Countermeasures to defeat denial of service attacks:** Martin and Rajasekaran[32] propose an adaptive protocol for async channel conditions, and a reactive algorithm to detect and defend against DoS attacks. The authors argue for the adoption of ICN (Information-centric networking) and NDN (Named Data network) in UWSN.

There are other research studies related to UWSN security solutions that are not related to a specific attack, which are summarised in the following.

a. **Authentication:** authentication is one of the core security requirements of any networked system, and it's the same for UWSNs. The proposed authentication solutions are:

- SenseVault – a three-tier authentication framework proposed by Xu and Liu[39]. The three tiers are:
  i. A cubic cluster formation to adapt to dynamic environments using cryptographic hash functions to derive secret keys for authentication[39]
  ii. A lightweight node revocation and authentication key update mechanism based on higher order polynomial (addressing node mobility),
  iii. VPS (Virtual phase shift) a phase quantization approach for key generation at the physical layer[39]
- A low computational complexity scheme is proposed by Yuan et al. in[40] using matrix addition instead of multiplication to reduce computing overhead. The base station generates configuration for each node, reducing memory cost. Zero knowledge proof protocol is used to verify authentication and prevent secret key disclosure[40].
- Yun et al.[38] propose a ticket-based authentication protocol that goes through four phases and involves the collaboration of the cluster head, gateway and base station.
- A protocol for secure authentication of cluster heads (CHs) and protected data aggregation is proposed by Goyal et al[44]. CHs are authenticated to gateways to ensure that the CHs serving each cluster are valid and not compromised. In the second module, each sensor node encrypts the data using symmetric key encryption before communicating to the CH. Data is then securely aggregated and transmitted to the base station[44].

b. **Trust management:** a trust cloud model for UWSNs is proposed by Jiang et al.[41] for malicious node detection, trust value calculation and data transmission. Also, Arifeen et al.[43] propose a trust management model for location privacy. It utilizes Adaptive Neuro Fuzzy Inference System (ANFIS) to asses node trustworthiness and Markov Decision Process (MDP) to select trusted nodes.

c. **Key distribution:** Kalkan et al.[37] propose a key distribution scheme based on Blom's key distribution scheme and applied to nomadic mobility model and meandering mobility model. Symmetric keys are utilized due to low computation overhead.

5 | FUTURE RESEARCH DIRECTIONS FOR UNDERWATER WIRELESS SENSOR NETWORK SECURITY

Based on the results obtained from this systematic literature review and our observations, we present some suggestions for future research on the UWSN security. First, we briefly discuss the main security requirements of UWSNs:

a. **Confidentiality:** This requires that unauthorised nodes are prevented from reading sensitive data, whether it is user data, e.g., military information, or network data such as routing information [13].

b. **Authentication:** This ensures that receiving nodes securely identify the source of data [13,22]. This is enabled by encryption and key exchange schemes [22].

c. **Integrity:** UWSNs rely on the integrity of the data, especially in military [13] and environmental [22] applications. Tampering on data could have severe consequences on the users of the network.

d. **Availability:** Legitimate users should always have access to the network's data, especially in time-sensitive applications such as seaquake prediction [22]. Redundancy should be provided such that the network will function in the event of a failure of some nodes [13].

5.1 | A Standardised Security Architecture for UWSN

Currently, most security measures proposed are experimental and either geared towards a specific threat or a group of threats. We suggest that more work should be done towards creating a robust security architecture consisting of protocols and policies that will provide multi-layer security and serve as a guide towards designing future UWSNs. Input can be taken from existing research works that are demonstrated to be effective. For instance, the scheme by Li Et al. [34] for spoofing detection shows improved detection performance. Also, according to Bagali and Sundaguru [29], their model for reactive jamming detection shows significant improvement over previous models. Another example is SenseVault, a framework proposed by Xu and Liu for UWSN security with contributions such as adapting to dynamic environments, authentication and cryptography [39,50].

5.2 | Energy Sources and Consumption

It has been established that limited energy supply and high energy consumption are both major challenges in UWSNs in general. However, it is also a challenge that is directly tied to security, as energy is required for the necessary computational power used in security. Therefore, it is important for more research into better energy sources to be conducted, as well as creating more energy efficient and low-computation overhead security measures. This will create more options for better security measures that would otherwise be impractical. For example, Yuan et al. propose a low computational complexity scheme for authentication [40]. More effort needs to be put in this area.

5.3 | Physical Experimentation

Majority of the research work presenting security mechanisms are evaluated by simulations, which mostly have preset constraints. Simulations provide a cost and time-effective way of testing new concepts and are definitely valuable for experimental research. However, due to the unpredictable nature of the underwater environment, the simulation software does not capture the actual behaviour and as such leaves room for inaccuracies. More physical experiments can be done to evaluate the efficacy of proposed security solutions. This will provide a more complete result of the performance of these solutions.

6 | CONCLUSION

This research identified available peer-reviewed research papers on the security challenges, threats and detective/mitigative solutions in UWSN. Three research questions were developed based on the objective, and answers were provided using the data extracted from the selected primary studies. The core challenges to UWSN security were identified, as well as the possible attacks and proposed countermeasures. We found that the majority of the existing research focus on DoS attacks. This indicates

that DoS is the most concerning type of attack to UWSNs. This is likely due to the energy constraints of sensor nodes and the unreliable communication of acoustic communication, which could worsen the effects of DoS attacks. Various techniques for detection and mitigation of attacks are proposed in the primary studies, including applying distributed techniques, game theory and machine learning models. In general, all the identified security challenges and attacks are followed by a proposed solution in the primary studies. Key focus areas showed that attack detection and authentication have received more research attention. As UWSNs advance and become more widely utilized, it is essential for security to be a key part of that process. Directions for future research are presented in Section 5 of this study, which could be summarized as the need for a comprehensive security framework for UWSNs composed of proper policies and protocols. Further research should be performed on creating lightweight and energy efficient security protocols. Moreover, a real-world testbed is required to evaluate the performance of the existing and future security mechanisms.

References

1. Felemban E, Shaikh F, Qureshi U, Sheikh A, Qaisar S. Underwater Sensor Network Applications: A Comprehensive Survey. *International Journal of Distributed Sensor Networks* 2015; 11: 1–14.

2. Heidemann J, Ye W, Wills J, Syed A, li Y. Research Challenges and Applications for Underwater Sensor Networking. In: IEEE Wireless Communications and Networking Conference. ; 3–6 April 2006.

3. Murad M, Sheikh A, Manzoor M, Felemban E, Qaisar S. A Survey on Current Underwater Acoustic Sensor Network Applications," A Survey on Current Underwater Acoustic Sensor Network Applications. *International Journal of Computer Theory and Engineering* 2014; 7(1): 51–56,.

4. Stratistics M. *Wireless Sensor Networks (WSN) - Global Market Outlook (2017-2026*. Stratistics MRC . 2019.

5. Pessoa L, Duarte C, Salgado H, et al. Design of an underwater sensor network perpetually powered from AUVs. In: OCEANS 2019. ; 2019.

6. Rahman Z, Hashim F, Rasid M, Othman M, Alezabi K. Normalized Advancement Based Totally Opportunistic Routing Algorithm With Void Detection and Avoiding Mechanism for Underwater Wireless Sensor Network. *IEEE Access* 2020; 8: 67484–67500,.

7. Kumar R, Bhardwaj D, Mishra M. Enhance the Lifespan of Underwater Sensor Network Through Energy Efficient Hybrid Data Communication Scheme. In: 2020 International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC), Pradesh. ; 2020.

8. Javaid N. NADEEM: Neighbor node approaching distinct energy-efficient mates for reliable data delivery in underwater WSNs. *Transactions on Emerging Telecommunications Technologies* 2019: e3805. doi: 10.1002/ett.3805

9. Hussain T, Rehman ZU, Iqbal A, Saeed K, Ali I. Two hop verification for avoiding void hole in underwater wireless sensor network using SM-AHH-VBF and AVH-AHH-VBF routing protocols. *Transactions on Emerging Telecommunications Technologies* 2020; 31(8): e3992. _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/ett.3992doi: 10.1002/ett.3992

10. Ruggeri A. Baiae: A Roman Settlement at the Bottom of the Sea. *BBC* 2020.

11. Matheson R. A battery-free sensor for underwater exploration. *MIT* 2019.

12. Das A, Thampi S. Secure communication in mobile underwater wireless sensor networks. In: 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI. ; 2015.

13. Yang G, Dai L, Si G, Wang S, Wang S. Challenges and Security Issues in Underwater Wireless Sensor Networks. *Procedia Computer Science* 2019; 147: 201–216.

14. Dargahi T, Javadi H, Shafiein H. Securing Underwater Sensor Networks Against Routing Attacks. *Wireless Personal Communications* 2017; 96: 2585–2602,.

15. Kong J, Ji Z, Wang W, Gerla M, Bagrodia R, Bhargava B. Low-cost attacks against packet delivery, localization and time synchronization services in under-water sensor networks. In: 4th ACM Workshop on Wireless Security. ; 2005.

16. Cong Y, Yang G, Wei Z, Zhou W. Security in Underwater Sensor Network. In: International Conference on Communications and Mobile Computing. ; 2010.

17. Ahmed M, Aseeri M, Kaiser M, Zenia N, Chowdhury Z. A novel algorithm for malicious attack detection in UWSN. In: International Conference on Electrical Engineering and Information Communication Technology (ICEEICT). ; 2015.

18. Qiu T, Zhao Z, Zhang T, Chen C, Chen CLP. Underwater Internet of Things in Smart Ocean: System Architecture and Open Issues. *IEEE Transactions on Industrial Informatics* 2020; 16(7): 4297–4307. doi: 10.1109/TII.2019.2946618

19. Mrabet H, Belguith S, Alhomoud A, Jemai A. A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis. In: . 20. ; 2020; Basel, Switzerland.

20. Shahapur S, Khanai R. Localization, routing and its security in UWSN — A survey. In: International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT). ; 2016.

21. Yunus F, Ariffin S, Zahedi Y. A Survey of Existing Medium Access Control (MAC) for Underwater Wireless Sensor Network (UWSN). In: 2010 Fourth Asia International Conference on Mathematical/Analytical Modelling and Computer Simulation. ; 2010.

22. Domingo M. Securing underwater wireless communication networks. *IEEE Wireless Communications* 2011; 18(1): 22–28,.

23. Das A, Thampi S. Fault-resilient localization for underwater sensor networks. *Ad Hoc Networks* 2017; 55: 132–142,.

24. Mian S, Kumar R. Security Analysis and Issues in Underwater Wireless Sensor Auditory and Multipath Network. *The International journal of analytical and experimental modal analysis* 2019; 11(10): 2269–2271,.

25. Zuba M, Shi Z, Peng Z, Cui JH. Launching denial-of-service jamming attacks in underwater sensor networks. In: . WUWNet '11 of *Sixth ACM International Workshop on Underwater Networks*. ; 2011.

26. Xiao L, Zhu Y. Modeling the Wormhole Attack in Underwater Sensor Network. In: International Conference on Wireless Communications, Networking and Mobile Computing. ; 2012.

27. Xie P, Zhou Z, Peng Z, et al. Aqua-Sim: An NS-2 based simulator for underwater sensor networks. In: OCEANS 2009. IEEE; 2009; Biloxi, MS: 1–7

28. Misra S, Dash S, Khatua M, Vasilakos A, Obaidat M. Jamming in underwater sensor networks: detection and mitigation. *IET Communications* 2012; 6(4): 2178–2188,.

29. Bagali S, Sundaraguru R. Efficient Channel Access Model for Detecting Reactive Jamming for Underwater Wireless Sensor Network. In: 2019 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET). ; 2019; Chennai.

30. Xiao L, Li Q, Chen T, Cheng E, Dai H. Jamming Games in Underwater Sensor Networks with Reinforcement Learning. In: 2015 IEEE Global Communications Conference (GLOBECOM). ; 2015.

31. Wang W, Kong J, Bhargava B, Gerla M. Visualisation of wormholes in underwater sensor networks: a distributed approach. *International Journal of Security and Networks* 2008; 3(1): 10–23,.

32. Martin R, Rajasekaran S. Data centric approach to analyzing security threats in Underwater Sensor Networks. In: OCEANS 2016 MTS/IEEE. ; 2016.

33. Khan G, Gola K, Rathore R. Robust data aggregation, encryption and data transfer in UWSNs. In: International Conference on Next Generation Computing Technologies (NGCT), Dehradun. ; 2015.

34. Li Y, Xiao L, Li Q, Su W. Spoofing detection games in underwater sensor networks. In: OCEANS 2015 - MTS/IEEE. ; 2015.

35. Ahmad B, Jian W, Enam R, Abbas A. Classification of DoS Attacks in Smart Underwater Wireless Sensor Network. *Wireless Personal Communications* 2019.

36. Ahmed M, Tahsien S, Aseeri M, Kaiser M. Malicious attack detection in underwater wireless sensor network. In: 2015 IEEE International Conference on Telecommunications and Photonics (ICTP). ; 2015.

37. Kalkan K, Levi A. Key distribution scheme for peer-to-peer communication in mobile underwater wireless sensor networks. *Peer-to-Peer Networking and Applications* 2014; 7: 698–709,.

38. Yun CW, Lee JH, Yi O, Park SH. Ticket-based authentication protocol for Underwater Wireless Sensor Network. In: 2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN). ; 2016.

39. Xu M, Liu L. SenseVault: A Three-tier Framework for Securing Mobile Underwater Sensor Networks. *IEEE Transactions on Mobile Computing* 2018; 17(11): 2632–2645,.

40. Yuan C, Chen W, Zhu Y, Li D, Tan J. A Low Computational Complexity Authentication Scheme in Underwater Wireless Sensor Network. In: 11th International Conference on Mobile Ad-hoc and Sensor Networks (MSN). ; 2015.

41. Jiang J, Han G, Zhu C, Chan S, Rodrigues J. A Trust Cloud Model for Underwater Wireless Sensor Networks. *IEEE Communications Magazine* 2017; 55(3): 110–116,.

42. Yang G, Dai L, Lei Y. A secure and energy balanced clustering protocol for underwater wireless sensor networks. In: 2018 International Conference on Security, Pattern Analysis, and Cybernetics (SPAC). ; 2018; Jinan.

43. Arifeen M, Islam A, Rahman M, Taher K, Islam M, Kaiser M. ANFIS based Trust Management Model to Enhance Location Privacy in Underwater Wireless Sensor Networks. In: 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE). ; 2019; Bangladesh.

44. Goyal N, Dave M, Verma A. SAPDA: Secure Authentication with Protected Data Aggregation Scheme for Improving QoS in Scalable and Survivable UWSNs. *Wireless Personal Communications* 2020; 110.

45. Ansari Z, Ghazizadeh R, Shokhmzan Z. Gradient descent approach to secure localization for underwater wireless sensor networks. In: 24th Iranian Conference on Electrical Engineering (ICEE). ; 2016.

46. Shanthi M, Anvekar D. Secure Localization for Underwater Wireless Sensor Networks Based on Probabilistic Approach. In: 2018 Second International Conference on Advances in Electronics, Computers and Communications (ICAECC). ; 2018.

47. Zhao H, Yan J, Luo X, Guan X. Privacy preserving solution for the asynchronous localization of underwater sensor networks. *IEEE/CAA Journal of Automatica Sinica* 2020: 1–17.

48. Bagali S, RSundaraguru . Maximize resource utilization based channel access model with presence of reactive jammer for underwater wireless sensor network. *International Journal of Electrical and Computer Engineering* 2020; 10(3): 3284–3294,.

49. Mrabet H, Cherifi A, Raddo T, Dayoub I, Haxha S. A Comparative Study of Asynchronous and Synchronous OCDMA Systems. *IEEE Systems Journal* 2020: 1–12.

50. Belguith S, Kaaniche N, Hammoudeh M. Analysis of attribute-based cryptographic techniques and their application to protect cloud services. *Transactions on Emerging Telecommunications Technologies*: e3667.