sustainability

MDPI

Article

A Comprehensive Analysis of Security-Based Schemes in Underwater Wireless Sensor Networks

Khalid Saeed [1], Wajeeha Khalil [2], Ahmad Sami Al-Shamayleh [3], Sheeraz Ahmed [4], Adnan Akhunzada [5], Salman Z. Alharthi [6,*] and Abdullah Gani [7]

1 Department of Computer Science, Shaheed Benazir Bhutto University, Sheringal Dir Upper 18000, Pakistan
2 Department of Computer Science & Information Technology, University of Engineering and Technology, Peshawar 25000, Pakistan
3 Department of Networks and Cybersecurity, Faculty of Information Technology, Al-Ahliyya Amman University, Amman 19328, Jordan
4 Department of Computer Science, Iqra National University, Peshawar 25000, Pakistan
5 College of Computing & IT, University of Doha for Science and Technology, Doha P.O. Box 24449, Qatar; adnan.adnan@udst.edu.qa
6 Department of Information System, College of Computers and Information Systems, Al-Lith Campus, Umm AL-Qura University, P.O. Box 7745, AL-Lith 21955, Saudi Arabia
7 Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur 50603, Malaysia; abdullah@um.edu.my
* Correspondence: szharthi@uqu.edu.sa

Abstract: Underwater wireless sensor networks (UWSNs) are comprised of sensor nodes that are deployed under the water having limited battery power and other limited resources. Applications of UWSNs include monitoring the quality of the water, mine detection, environment monitoring, military surveillance, disaster prediction, and underwater navigation. UWSNs are more vulnerable to security attacks as compared to their counterparts such as wireless sensor networks (WSNs). The possible attacks in UWSNs can abrupt the operation of entire network. This research work presents the analysis of relevant research done on security-based schemes in UWSNs. The security-based schemes are categorized into five sub-categories. Each technique in each category is analyzed in detail. The major contribution in each security-based scheme along with technique used, possible future research issues and implementation tool are discussed in detail. The open research issues and future trends identified and presented in this research can be further explored by the research community.

Keywords: security; encryption algorithms; secure routing; key management schemes

Citation: Saeed, K.; Khalil, W.; Al-Shamayleh, A.S.; Ahmed, S.; Akhunzada, A.; Alharthi, S.Z.; Gani, A. A Comprehensive Analysis of Security-Based Schemes in Underwater Wireless Sensor Networks. *Sustainability* **2023**, *15*, 7198. https://doi.org/10.3390/su15097198

Academic Editor: Juan Miguel Navarro

Received: 17 January 2023
Revised: 14 April 2023
Accepted: 19 April 2023
Published: 26 April 2023

1. Introduction

The ocean covers more than 70% of the planet, making underwater wireless sensor networks (UWSNs) highly significant. In the past ten years, UWSNs have received considerable attention [1,2]. Sensor nodes in UWSNs communicate with each other to determine the most suitable path based on certain selection criteria. This path is then used to transfer data from the bottom of the water to the surface and beyond. UWSNs serve a range of purposes underwater, including resource exploration, information exchange, surveillance, and disaster prevention [3–6]. Environmental sustainability in UWSNs is important because communication technologies have significant impact on wildlife [7]. UWSNs differ significantly from wireless sensor networks (WSNs) because of their limited resources. Additionally, the environmental challenges associated with UWSNs are distinct from those found in WSNs [8].

There are numerous challenges associated with communication in UWSNs, leading to unpredictable outcomes [9]. The characteristics of the underwater environment, such as scattering, high attenuation, and absorption, render radio wave communication unfeasible. Instead, acoustic communication is the preferred method for data transmission in UWSNs.

However, the limited spectrum of useful frequencies available for acoustic waves imposes a range limitation [10]. Unlike radio communication, acoustic communication is much slower, with a propagation speed of only 1500 m/s, resulting in long end-to-end and propagation delays within the UWSNs environment. The available bandwidth for acoustic communication is also limited, being below 100 kHz. Although sensor nodes in UWSNs are typically considered static, they can move at speeds ranging from 1 to 3 m/s [8,11–13]. The architecture of UWSNs is illustrated in Figure 1.

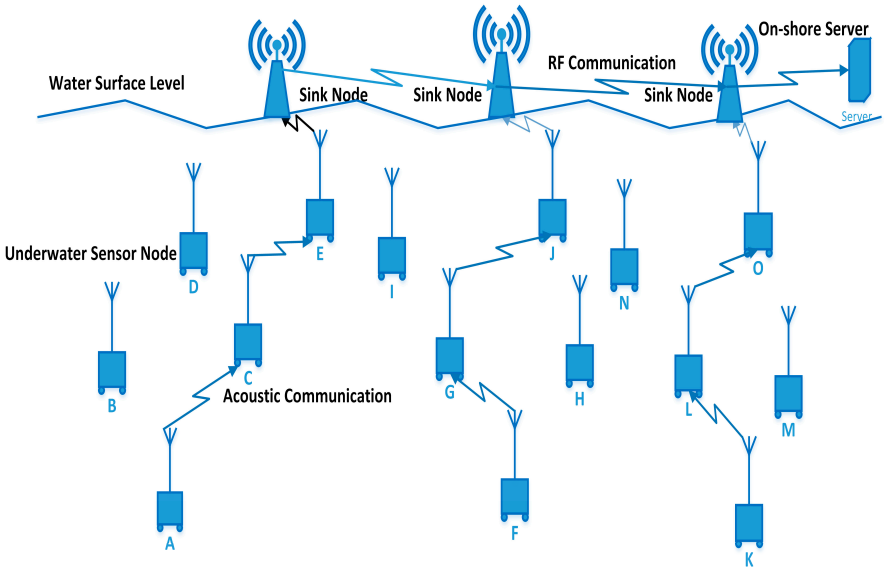

Figure 1. UWSNs architecture.

Figure 1 reflects the basic architecture of UWSNs environment, whereas A, B, C . . . O are the sensor nodes deployed in UWSNs environment. The communication among sensor nodes in UWSNs environment is multi-hop which means the data reach from source to sink via multiple sensor nodes. The communication in underwater environment is acoustic whereas the communication between sink nodes is via radio waves.

UWSNs Applications

UWSNs have a diverse range of applications, including monitoring, military, disaster prevention, assisted navigation, and sports, as shown in Figure 2. In UWSNs, monitoring involves the deployment of sensor nodes to monitor the physical environment, which is further classified into water quality, exploration, and habitat monitoring. Exploration includes natural resources, pipelines, and cables, while habitat monitoring includes marine life and fish farms. Disaster prevention applications of UWSNs include flood, oil spill and volcano, earthquake, and tsunami monitoring. UWSNs also have military applications, which are further classified into mines, submarines, and surveillance [14–28].

Graphical classification of UWSNs can be broadly categorized into three types: network architecture, deployment strategy, and communication protocol. Network architecture can be further classified into centralized, distributed, and hybrid. The deployment strategy of UWSNs can be classified into static and mobile. The communication protocol of UWSNs can be classified into three types: acoustic, optical, and hybrid [14,29].

Rest of the research paper is structured as follows: Section 2 includes detail regarding related surveys; motivation of research is discussed in Section 3; challenges in UWSNs are discussed in Section 4; Section 5 is regarding security in UWSNs; research contribution on security in UWSNs are discussed in detail in Section 6; Section 7 includes detail discussion on current challenges and future trends; Section 8 contains conclusion.

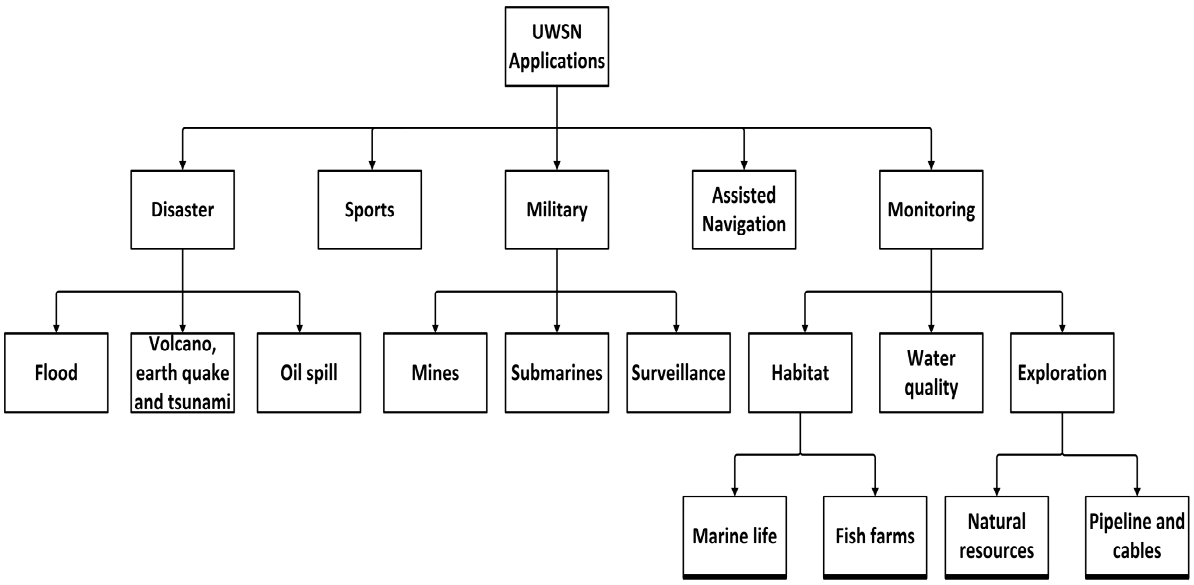

Figure 2. UWSNs applications [14].

2. Related Surveys

There are some related research articles and surveys published by the research community so far. The researchers in [30–32] conducted a survey on the applications and challenges of UWSNs. The authors in [33] conducted a survey on advances and challenges in UWSNs. The research conducted in [34] focused on security challenges and applications for UWSNs environment. Authors in [35] conducted survey on the challenges and techniques in underwater localization; authors of [36] explored the architectural challenges in UWSNs; authors of [37] discussed the challenges and security issues in UWSNs; authors of [38] discussed the issues and challenges regarding the implementation of UWSNs; authors of [39] conducted survey on security infrastructure for UWSNs; authors of [7] conducted survey on UWSNs and discussed open research challenges; an exhaustive study on UWSNs modems is presented in [40]; the classification of UWSNs modems, analysis, as well as design challenges are presented in [41]. The researchers in [42–46] conducted a survey on routing protocols in UWSNs; authors of [47] conducted a survey on multi-path routing protocols for UWSNs. The research conducted in [48] conducted a survey on security issues in UWSNs. They focused on attacks and defenses. They analyzed in detail the possible attacks on node, attacks on data, and attacks on network. The authors in [49] conducted a survey on security in UWSNs; authors of [50] conducted a survey on security attacks in UWSNs. They discussed the characteristics and vulnerabilities of UWSNs. They discussed the possible attack and their countermeasures in UWSNs. The attacks include jamming attack, wormhole attack, swallow hole attack, and sybil attack. They also mentioned the security requirements and security challenges for UWSNs environment.

3. Motivation

So far, the focus of research community in UWSNs addressed the energy efficiency-related issues due to the built-in and limited lifetime of sensor node' battery. The researchers in [51–60] focused on energy efficiency in routing protocol for UWSNs; authors of [61] focused on energy-efficient MAC as well as routing protocols for sustainable UWSNs. Security in UWSNs plays an important role and it cannot be ignored. There are some research articles published by the research community that addressed security in UWSNs but analysis of security-based schemes in UWSNs is not yet addressed by the research community. Therefore, to address the security in UWSNs this research includes analysis of the relevant research done on security in UWSNs. The research work done on security in UWSNs is divided into different categories such as key management schemes, encryption schemes, secure routing schemes, frameworks/models, and secure mac algorithms for

UWSNs environment. Each mechanism in the mentioned categories is analyzed in detail. The major contribution made in each research, along with the attack types addressed and simulation environment are analyzed in detail. Research articles from reputed journal/conferences and relevant to above five sub-categories are analyzed in this research. This research will help the research community to evaluate the research contribution on security in UWSNs. To the best of our knowledge this is the first research work regarding analysis of security-based schemes in UWSNs environment.

4. Challenges in UWSNs

The UWSNs environment presents several challenges, such as noise, channel attenuation, limited bandwidth, acoustic wave speed, short network lifespan, MAC issues, channel utilization, localization, routing difficulties, and packet size selection [62,63].

4.1. Underwater Noise

Underwater communication quality is adversely affected by the presence of underwater noise, which leads to a preference for paths with lower noise levels. This noise can be divided into two categories—human noise and ambient noise. Human noise is generated by activities such as the use of heavy machinery, fishing, shipping, aircraft, sonar, and military operations, and can even be caused by human beings themselves [63]. Ambient noise, also known as background noise, is also a contributing factor. It is important to address these issues to improve underwater communication. The ambient noise in the underwater environment is usually constituted by the following four components such as thermal noise (N_{th}), wave noise (N_{wv}), shipping noise (N_{sh}), and turbulence noise (N_{tb}) [64]. These noises are modeled in Equation (1).

$$N = N_{th} + N_{wv} + N_{sh} + N_{tb} \quad (1)$$

4.2. Channel Attenuation

The channel attenuation is defined as the wave energy that is converted into heat energy and absorbed by the medium that has been used. The heat is absorbed by the underwater environment. Attenuation is direction proportional to distance and frequency [65]. The channel attenuation in UWSNs is due to the absorption loss and it significantly reduces the strength of signals. Due to the channel attenuation, it becomes severely difficult while extracting the desired data from the signal at the destination [64]. The channel attenuation is modeled as shown in Equation (2).

$$A\ (d, f) = A_o d^k\ a(f)^d \quad (2)$$

where A_o is constant known as normalizing constant, k represents the factor such as spreading factor, a(f) is known as the absorption coefficient.

4.3. Limited Bandwidth

The medium of underwater communication is harsh; therefore, specific frequencies of the acoustic spectrum can be used for carrying information [64]. The available bandwidth becomes restricted due to which there are restrictions regarding the design of the acoustic systems. The bandwidth in acoustic communication is very limited. The routing protocol in the UWSNs has to consider the limited bandwidth and have to select the optimal path for the delivery of the packets to the destination. The transmission range of applications in underwater communication is inversely proportional to the bandwidth [64].

4.4. Speed of Acoustic Waves

The speed of the acoustic waves in underwater communication is significantly less as compared to the radio waves in traditional WSNs. Moreover, the speed of acoustic waves in underwater communication varies with temperature, salinity, and depth of the water. Due to the variation in speed of acoustic waves, there is also variation in the time

taken for the delivery of data. The speed of acoustic waves is very significant in some critical applications such as rescue operation, military surveillance, disaster prediction, and disaster prevention etc., [62,66].

4.5. Shorter Network Life Time

The limited battery power of the sensor node in UWSNs results in a short lifetime [67]. The replacement of battery in sensor node deployed under the water is not an efficient solution. Due to the depletion of battery power of sensor nodes, the dead nodes are increased in UWSNs which significantly degrades the performance of the network [62].

4.6. Channel Utilization

The design of highly utilizing channel is a challenging task due to the characteristics of UWSNs environment. The characteristics of UWSNs environment include multipath propagation which causes phase fluctuations and fading. Due to the movement of sensor and receiver nodes, another problem is observed known as doppler effect. Underwater noise and speed of sound etc., are other factors that influence the acoustic channel's performance [68].

4.7. Routing Issues

Energy saving is the major issue that affects UWSNs. The mobility of nodes in UWSNs environment is another challenge. There are different routing protocols for land-based sensor networks but due to the mobility of nodes and rapid change in the topology the routing protocols of sensor networks are not suitable for UWSNs environment [69]. Routing is the main concern of almost all categories of networks. The routing protocols are used for discovering and maintaining paths for the transmission of data [70]. Energy efficiency and secure routing are challenging areas of research in UWSNs environment.

5. Security in UWSNs

The communication in UWSNs is under the water and public due to which it is possible for an adversary to compromise the security in UWSNs. The sensor nodes in UWSNs are vulnerable to different security attacks. Therefore, security should be the main concern while designing any mechanism for UWSNs. The communication in UWSNs is done using acoustic channel in which the bandwidth is low, and latency is high. Due to the features of acoustic channels in UWSNs, the energy consumption is more in acoustic communication as compared to radio waves in WSNs. The security mechanisms designed for WSNs cannot be used in UWSNs because the resources are limited in UWSNs environment. Therefore, energy consumption should be considered while designing security mechanisms for UWSNs [71–73].

5.1. Security Requirements in UWSNs

The basic requirements of security in UWSNs environment are authentication, confidentiality, integrity, and availability [71,72].

5.1.1. Authentication

Authentication refers to the identification of sensor node. If there is no authentication, then the malicious node can participate in the operations of UWSNs and can abrupt the operations. If the malicious node obtains ID information and packet information through wiretapping, then the data can be compromised by the falsification of data [72–74].

5.1.2. Confidentiality

Confidentiality refers to the encryption of data communicated between sensor nodes in UWSNs. If the data communicated among sensor nodes in UWSNs are not encrypted, then malicious nodes can capture and retrieve the data. Therefore, proper encryption

should be used in UWSNs environment so that if the malicious nodes capture the traffic still it cannot be useful because it will be in encrypted form [72,73].

5.1.3. Integrity

Integrity ensures that the data has not been modified by the adversaries. Moreover, in UWSNs integrity refers to identifying tampering of data communicated among sensor nodes in UWSNs. There are some applications of environmental preservation such as monitoring the quality of water relying on the integrity of the data [72,73,75].

5.1.4. Availability

It means that the system should be able to provide services even when the network is under attack by malicious nodes. Moreover, the data should be available according to the need of the legitimate users. DoS attack affects the availability due to which time-critical applications such as predictions of the seaquakes are badly affected [72,73].

5.2. Security Attacks in UWSNs

Security attacks can be launched in UWSNs environment. The first possibility is to attack the sensor node, but it is least likely due to the difficulty in accessing the sensor node deployed under the water. The second possibility is to attack the protocol used for communication in UWSNs. If during attack the protocol used for communication is compromised, then it has impact on the whole network [76]. The research work in [77], focused on the classification of DoS attack in UWSNs environment. The attacks can be generally divided into two broad categories such as passive attacks and active attacks. There are some attacks possible in UWSNs. These attacks include but are not limited to jamming attack, wormhole attack, sinkhole attack, acknowledgement spoofing attack, sybil attack, and selective forwarding attack etc., Some of these attacks are briefly discussed as follows.

5.2.1. Jamming Attack

In jamming attack, the attackers interrupt the communication among sensor nodes. This jamming attack works by sending useless signals to the genuine sensor nodes by utilizing the same band of frequency. Since UWSNs uses a narrow frequency band therefore, UWSNs environments are more vulnerable to the jamming attack [76,78].

5.2.2. Wormhole Attack

In wormhole attack, the malicious node creates a connection at two points in a network. The malicious node receives some packet at one end and transfers them to the other end of the wormhole by utilizing out of band connection and then these packets are injected again in the network. Due to the presence of wormhole attack, the wormhole links will be selected by protocols for communication because these links appear as shorter links. The consequences of wormhole attack can be traffic captured, dropped, and modified by the attacker [73,79].

5.2.3. Sybil Attack

In this attack an attacker with multiple identities pretends to be at multiple places at the same time. Authentication as well as position verification mechanism can be used to detect such type of attack but position verification in UWSNs can be a challenging task due to the mobility of sensor nodes [73].

5.2.4. Selective Forwarding Attack

In this attack instead of forwarding all messages the malicious nodes drop some messages. Authentication and multipath routing can be used to handle such type of attack [73].

5.2.5. Sinkhole Attack

In this type of attack malicious node deceives the neighbor nodes by advertising itself as the best route toward the base station. The neighbor nodes are deceived because they use the route of malicious node frequently. The malicious node can damage the operation of network by tampering the data [73].

5.2.6. Acknowledgement Spoofing Attack

In this attack the malicious node overhears the packets which are sent by the neighbor nodes. By utilizing the available information, the malicious node spoofs the acknowledgment of link layer for the purpose of injecting weak link or shadow zone link [73,80].

5.2.7. Hello Flood Attack

In this attack, a sensor node receives packets from the malicious node may interpret the adversary is in the neighborhood. This assumption is not correct if high power is used for transmission by the adversary. In order to protect against such attack bidirectional link verification mechanism can be used. Moreover, authentication is also a possible means of defense [81].

6. Research Contributions on Security in UWSNS

There are some research articles contributed by the research community in UWSNs but some of them focused on routing protocols for UWSNs and some focused on other problems in UWSNs. To the best of our knowledge this is the first research article that addressed security-based schemes in UWSNs. The research focus of this research is to address the relevant research work done so for on security in UWSNs. The research contribution on security-based schemes in UWSNs is divided into five categories as reflected in Figure 3.

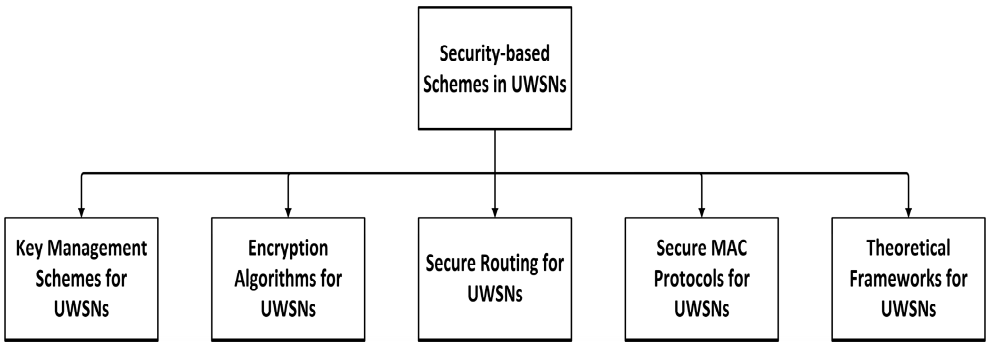

Figure 3. Classification of security-based schemes in UWSNs.

6.1. Key Management Schemes for UWSNs

This section includes analysis of different key management schemes proposed by the research community for UWSNs environment. The analysis is also presented in tabular form in Table 1.

Table 1. Analysis of different key management schemes for UWSNs.

Technique	Issue Addressed	Major Contribution	Attack Type	Implementation Environment
Computationally Efficient Signature Scheme for UWSNs [82]	Secure and efficient signature schemes in UWSNs.	Development of a computationally efficient online/offline signature scheme that is specifically tailored to the requirements and constraints of UWSNs. The scheme is shown to reduce the computational overhead of signature verification by up to 90% compared to traditional signature schemes.	Provide protection against node compromise attack and message modification attack by providing data integrity and authenticity.	MATLAB
Key agreement mechanism for UWSNs [83]	Energy efficient key agreement mechanism having less overhead designed for UWSNs.	Resistance against different active attacks. Produced good results regarding networks performance and security. Energy consumption of low-performance nodes significantly reduced.	Resist against sybil attack, spoofed attack, node replication attack, and replay attack.	System level implementation
Key distribution scheme for Mobile UWSNs [84]	Addressed the key distribution problem of UWSNs.	Two mobility models meandering and nomadic. Better performance in terms of security.	When some of the sensor nodes are captured by an adversary the resiliency performance is good. Reduces the number of links compromised.	Visual studio 2010 and C# for coding
End-to-End authentication mechanism for UWSNs [85]	Addressed the authentication problem of UWSNs environment.	Evaluated three different digital signature schemes such as ZSS, ECDSA and BLS. It is observed that using short as well as aggregate signatures have main role in the energy efficiency in UWSNs.	Resist against attacks on end-to-end authentication.	Implementation tool not used.
Cluster Based Key Management Scheme for UWSNs [86]	Addressed the mobility and security issues in UWSNs environment.	A new communication architecture is proposed to handle the mobility of sensor nodes efficiently. CKP provides authentication, confidentiality, freshness, and integrity.	Minimize the effect of self-compromised node and resist against insider threats.	Implementation tool is not mentioned.

6.1.1. Computationally Efficient Signature Scheme for UWSNs

Authors in [82] proposed signature scheme that is a computationally efficient online/offline signature scheme designed for use in underwater wireless sensor networks (UWSNs). The scheme uses elliptic curve cryptography (ECC) and a batch verification technique to reduce the computational overhead of signature verification. The primary issue addressed by the paper is the need for secure and efficient signature schemes in UWSNs. Traditional signature schemes are not well-suited for UWSNs due to the limited computational resources and energy constraints of underwater sensor nodes. The major contribution of the paper is the development of a computationally efficient online/offline signature scheme that is specifically tailored to the requirements and constraints of UWSNs. The scheme is shown to reduce the computational overhead of signature verification by up to 90% compared to traditional signature schemes. The paper discusses several types of attacks that can be launched against UWSNs, such as node compromise attacks and message modification attacks. The proposed signature scheme is designed to protect against these attacks by providing data integrity and authenticity. The proposed signature scheme can be implemented in any UWSN that uses ECC for signature generation and verification. The scheme is specifically designed to be efficient in resource-constrained environments, such as UWSNs.

6.1.2. Key Agreement Mechanism for UWSNs

The researchers in [83] proposed the mechanism of key agreement for UWSNs environment. The proposed mechanism is novel and energy efficient. The key agreement mechanism is proposed by considering the limited resources of UWSNs environment.

The proposed mechanism bears minimum overhead and is specifically designed for the UWSNs environment. In the proposed mechanism the sensor nodes are grouped into clusters to decrease the overhead of communication. The cluster head known as H-node in each cluster is liable for the collection, aggregation, and sending of observing data. The S-nodes are liable for observation as well as sending the observation data to H-nodes. Among H-nodes and S-nodes, the H-nodes have larger capacity, stronger communication and computation capacities, and high-performance nodes as compared to S-nodes. The proposed key agreement mechanism can counterattack against sybil attack, replay attack, node replication attack, and spoofed attacks etc. For enhancing the capability of the proposed mechanism, the geographical as well as the identity are included to the private key and public key of sensor node for resistance against attacks. The proposed mechanism has less overhead because it did not adopt Tate pairing decomposition problems. The nodes having high performance assist those nodes having low performance in computing and communication tasks. The high-performance sensor nodes actively participate in the computing and communication tasks and as a result the energy consumption significantly decreases for low performance sensor nodes. According to the proposed mechanism, the session key of the sensor node having low performance can be updated on periodical basis to improve the robustness and security of UWSNs environment. The simulation results demonstrate improved performance of the projected mechanism regarding security and network performance. The proposed key agreement mechanism significantly reduced energy utilization of the sensor nodes whose performance is not good.

6.1.3. Key Distribution Scheme for Mobile UWSNs

The research conducted in [84] offered key distribution scheme for UWSNs. The proposed scheme is for the purpose of peer-to-peer communication in the mobile UWSNs. Meandering and nomadic mobility models are utilized while carrying out this research. Meandering model is truthful because it relies upon the ocean movement. Vertical movement is not considered in this model, and it is designed as a two-dimensional model. Meandering model is hierarchical in structure and is used for big areas such as in kilometers. The nomadic mobility model is three dimensional, hierarchical in nature. This mobility model is suitable for limited areas on the seashore. In nomadic mobility model, the sensor nodes are floated together to a location and afterwards each sensor node moves slightly in random manner and independently. In the proposed scheme, the group moves to a new location and afterwards each sensor node moves marginally to a new place. The outcomes obtained in this research show some connectivity issues. The connectivity issue arises due to mobility, but the proposed mechanism managed the issue of connectivity on time. The scheme recommended in this research shows that when an adversary captures some sensor nodes, the resiliency performance is still much better. Very few numbers of links are compromised in this case. The produced results further reveal minimum energy consumption as well as better security in the proposed scheme.

6.1.4. End-to-End Authentication in UWSNs

The researchers in [85] evaluated several digital signature schemes for UWSNs. The schemes are for end-to-end authentication and the evaluation is done on the basis of consumption of energy. In this research the authors revealed that the traditional digital signature schemes such as RSA are not suitable for UWSNs environment because there is heavy computation involved in RSA and the nodes deployed in UWSNs have very inadequate resources. The outcome of this study demonstrates that there are certain schemes which performed good in WSNs environment, but it is not necessary that these schemes will perform well in UWSNs because of the UWSNs unique characteristics. In this research, the authors revealed some characters of the digital signatures schemes for the purpose of suitability in the environment of UWSNs. ZSS, ECDSA, and BLS are the three digital signatures schemes which are evaluated in this research. The evaluation is done based on consumption of power. The time of signature generation for ZSS, ECDSA,

and BLS are 229 ms, 134 ms, and 302 ms respectively. The signatures size of ZSS, ECDSA, and BLS are 21 bytes, 40 bytes, and 21 bytes respectively. This research concluded that aggregate as well as signature short in size have the main role in the energy efficiency in UWSNs environment.

6.1.5. Cluster-Based Key Management Scheme for UWSNs

The research conducted by the authors of [86] addressed the mobility and security issue in UWSNs environment. They proposed a cluster-based key management protocol (CKP) for the UWSNs environment. In the proposed scheme, different kinds of keys are used in order to provide diverse security levels in the mobile atmosphere at different stages. In hierarchical networks the sensor nodes make cluster of capable sensor nodes. New communication architecture is proposed in this research and with the help of proposed architecture the mobility of sensor nodes is handled efficiently. The effect of self-node compromise is also minimized. CKP provides authentication, confidentiality, freshness, and integrity. The results obtained in this research show that CKP is storage effective as well as energy effective because the minimum number of keys are stored in a sensor node. Moreover, in this research, survivability of CKP is investigated against different security threats.

6.2. Encryption Algorithms for UWSNs

This section includes the analysis of different encryption algorithms proposed by the research community for UWSNs environment. The analysis is also presented in tabular form in Table 2.

Table 2. Analysis of encryption schemes for UWSNs.

Technique	Issue Addressed	Major Contribution	Attack Type	Implementation Environment
Encryption scheme for UASNs [87]	Addressed the issue of lightweight encryption algorithm for UASNs environment.	Proposed lightweight cryptographic algorithm for UASNs environment. Modification in AES to make it suitable for UASNs. Proposed mechanism provides good security with limited overhead and is energy efficient.	Resist against brute force and other adverse attacks.	AquaSeNT OFDM modem, computer-based simulation.
Encryption scheme for UWASNs [88]	Addressed suitability of algorithms for UWASNs environment.	Discussed suitable algorithms for security in UWASNs. Authors suggested minimum amount of overhead for data when applying security in UWASNs. Recommended the use of CMVP algorithm.	Resist against attacks on encryption in UWSNs.	Theoretical idea provided in the conducted research and implementation tool is not used.
Lightweight cryptographic Algorithm for UASNs [89]	Addressed secure communication in UASNs.	Developed a lightweight cryptographic algorithm that is specifically tailored to the constraints and requirements of UANs. The algorithm is shown to provide a high level of security while maintaining low computational and energy costs.	Resist against eavesdropping, message modification, and impersonation attacks.	Python

6.2.1. Efficient Encryption Algorithm for UASNs

The research conducted in [87] recommended efficient cryptographic mechanism for the protection of confidentiality as well as integrity in UASNs environment. Traditional AES-128 is modified by utilizing an alternate approach. The S-Box which is used in the traditional AES consumes more energy and therefore it is not suitable for the UASNs environment. Therefore, in this research, instead of S-Box an 8 round block cipher algorithm has been used in the UASNs environment. The mechanism proposed in this research has resistance against brute force and some other attacks. The key space in the proposed algorithm can be increased by changing the number of iterations rounds e.g., by raising the value of iterations rounds from 8 to 10 the key space is further increased. The round key is resistant to brute force attack. The authors in this research also proposed network

architecture which is secure in nature for UASNs environment. The scheme that is recommended is compared with the existing schemes such as Blowfish, AES-128, and PRESENT. The outcomes obtained reveal that the recommended scheme is secure as well as energy efficient compared to the other existing schemes. In this research encryption and decryption are carried out using the proposed encryption algorithm and it has been observed that the proposed encryption algorithm is secure. The simulation findings indicate that the recommended encryption algorithm has produced less overhead and thus it is suitable for UASNs environment. In future the encryption algorithm proposed in this research can be tested in real UASNs environment to check its efficiency in the real environment. Flow chart of efficient encryption algorithm for UASNs is reflected in Figure 4.

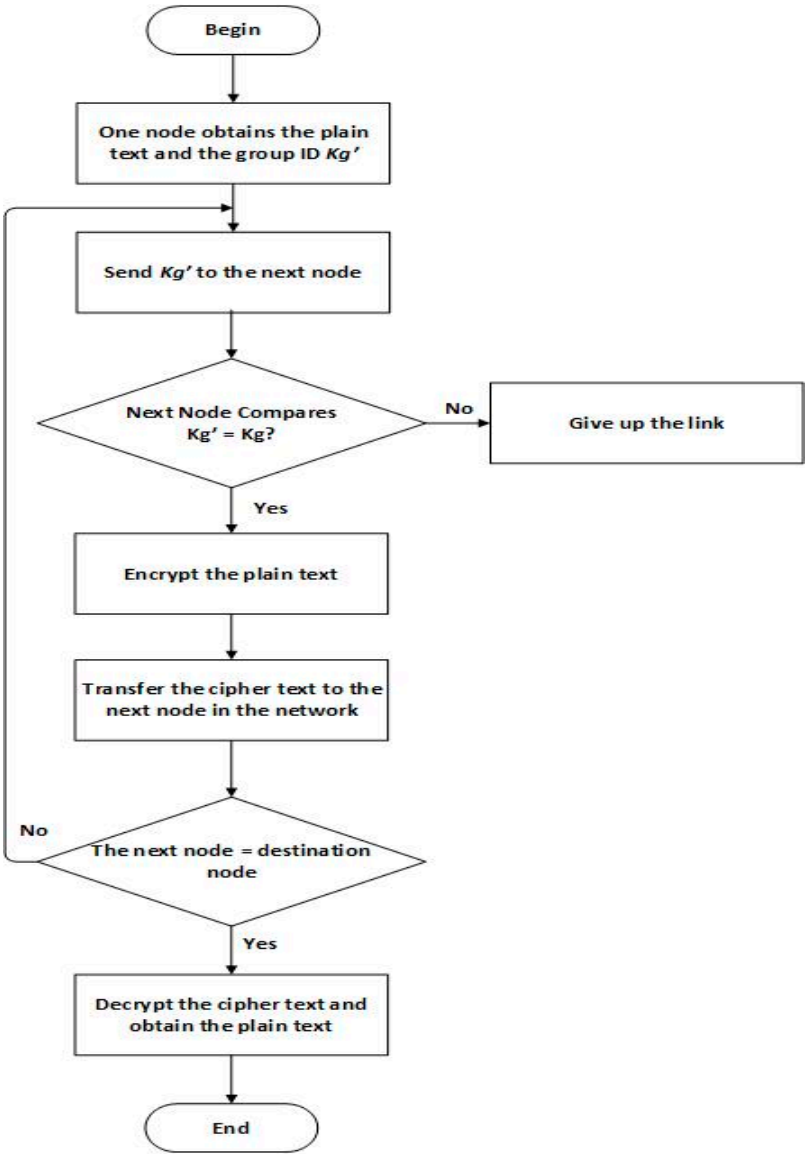

Figure 4. Flow chart of efficient encryption algorithm for UASNs [87].

6.2.2. Encryption Scheme for UWASNs

The researchers in [88] considered the security and requirements issues of the UWASNs environment. For data confidentiality and integrity in UWASNs environment there is a need of proper security mechanism and algorithm. This research investigated the encryption algorithm based on suitability for the UWSNs environment. The protocol stack of UWASNs includes five layers such as (i) application layer, (ii) transport layer, (iii) network layer, (iv) MAC layer, and (v) physical layer. The header is added at each layer when the data

moves from the higher layer to the lower layer. The security header is included in the encryption process which contains parameters of security for retrieving the data by the receiver. The authors suggested utilizing the same key for encryption as well as decryption due to the small key size in symmetric key. After adding the headers, the message is entered to message authenticated code. Message integrity code (MIC) is utilized for ensuring the authenticity of the message and shared key. Encryption is done to encrypt both message and MIC. Receiver calculates and compares both MIC. The message is accepted if both the values of both MIC are equal otherwise the message is discarded. It is recommended in this research to use minimum overhead for security in UWASNs and recommended the use of CMVP algorithm for it. Data encryption and decryption process is reflected in Figure 5.

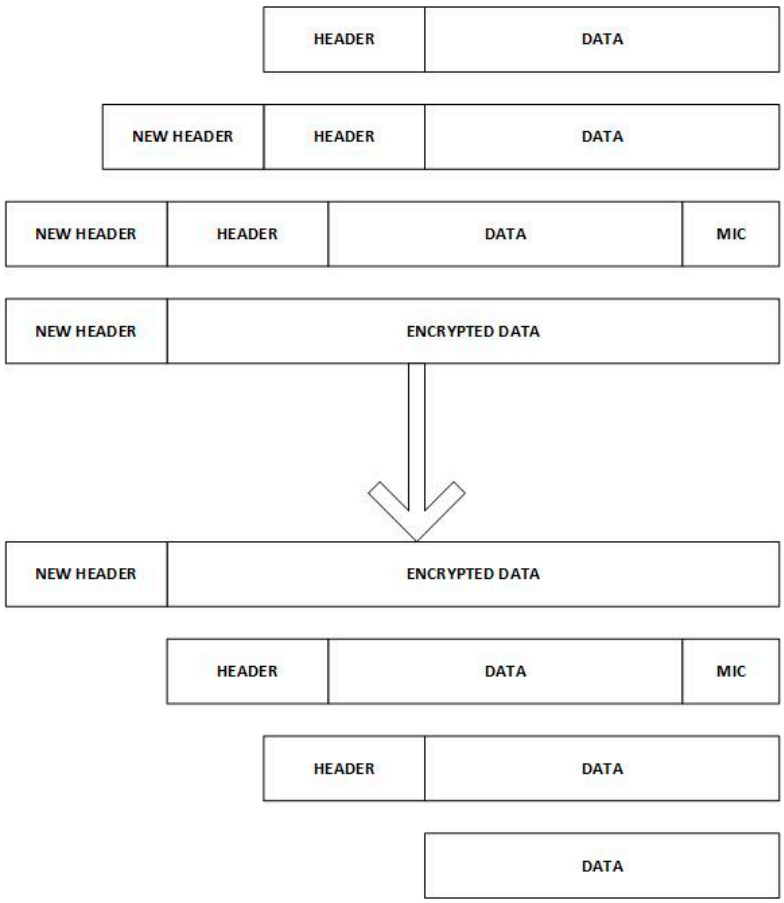

Figure 5. Data encryption and decryption [88].

6.2.3. Lightweight Cryptographic Algorithm for UASNs

Research conducted in [89] proposed an algorithm that is a lightweight cryptographic algorithm designed specifically for use in underwater acoustic networks (UANs). The algorithm uses a combination of symmetric key cryptography, error-correcting codes, and message authentication codes (MACs) to provide security for data transmission in UANs. The primary issue addressed by the paper is the need for secure communication in UANs, which are increasingly being used for a variety of applications such as oceanographic research, underwater surveillance, and oil exploration. However, the unique properties of UANs, such as high latency, low bandwidth, and unreliable communication channels, make it challenging to implement traditional cryptographic algorithms. The major contribution of the paper is the development of a lightweight cryptographic algorithm that is specifically tailored to the constraints and requirements of UANs. The algorithm is shown to provide a high level of security while maintaining low computational and energy costs. The paper discusses several attacks that can be launched against UANs, such as eavesdropping, message modification, and impersonation attacks. The proposed algorithm is designed to

protect against these attacks by providing data confidentiality, data integrity, and message authentication. The proposed algorithm can be implemented in any UAN that uses acoustic communication for data transmission.

6.3. Secure Routing for UWSNs

This section includes analysis of different secure routing schemes proposed by the research community for UWSNs environment. The analysis is also presented in tabular form in Table 3.

Table 3. Analysis of secure routing schemes for UWSNs.

Technique	Issue Addressed	Major Contribution	Attacks	Implementation Environment
Secure routing in UWSNs [90]	Addressed secure routing in UASNs.	Developed a secure routing algorithm based on the AFSA-ACOA fusion technique that can ensure the integrity, confidentiality, and availability of data transmission in UASNs.	Resistant against packet dropping attacks, Sybil attacks, and replay attacks.	MATLAB
Secure routing scheme for UASNs [91]	Addressed the issue of secure routing approach for UASNs.	Proposed secure routing for UASNs. Signature algorithm is proposed for authentication between source and destination node. A trap-door scheme is used for achieving anonymity of the nodes.	The proposed scheme can resist against forgery attacks and improves the overall security.	NS2 with UWSNs package Aqua-Sim
Secure energy efficient and cooperative routing for UWSNs [92]	Addressed the issue of secure and energy efficient routing approach for UWSNs.	Proposed secure and energy efficient routing protocol for UWSNs. Minimum computations are used considering the limited resources of UWSNs.	The proposed scheme can resist active attacks that drop packets.	MATLAB
Securing UWSNs from routing attacks [93]	Addressed combating routing attacks in UWSNs via distributed approach.	Proposed distributed approach for detecting and mitigating the routing attacks in UWSNs. An analytical model is proposed for the said purpose.	Proposed mechanism can detect wormhole and sinkhole attack in UWSNs.	Castalia simulator based on OMNET++
Secure neighbor discovery in UASNs [94]	Addressed the issue of secure neighbor discovery in UASNs.	Proposed protocols suite for secure neighbor discovery in UASNs. The proposed protocols are based on the direction of arrival (DoA) signals approach.	Wormhole resilient secure neighbor discovery	C++ programming language
Secure communication suite for UASNs [95]	Addressed the issue of secure routing for UASNs.	The proposed scheme includes secure routing protocol and cryptographic primitives. Proposed protocols suite has limited power consumption and overhead that's why it is suitable for UASNs.	Proposed solution is efficient for providing integrity and confidentiality in UASNs against attacks.	Experiments based on real data
Secure communication in mobile UWSNs [96]	Addressed various DoS attacks in mobile UWSNs environment.	Flooding attack in UWSNs is simulated and its impact is analyzed on the performance of UWSNs. It has been concluded that techniques suitable for WSN environment are not suitable for UWSNs environment.	Various DoS attacks such as man in the middle attack, and flooding attack.	Aqua-Sim
An IDS for Opportunistic Routing in UWSNs [97]	Addressed effective intrusion detection schemes that can detect and mitigate attacks in OR schemes in UWSNs.	Developed the DOIDS intrusion detection scheme, which is specifically designed to detect and mitigate attacks in OR schemes in UWSNs. The scheme is shown to be effective in detecting and mitigating the effects of several types of attacks, including selective forwarding attacks, sinkhole attacks, and wormhole attacks.	Provide protection against selective forwarding attacks, sinkhole attacks, wormhole attacks, and Sybil attacks.	MATLAB

6.3.1. Secure Routing in UWSNs

The authors in [90] propose a secure routing algorithm for underwater acoustic sensor networks (UASNs) based on the adaptive firefly algorithm (AFSA) and ant colony optimization algorithm (ACOA) fusion technique. The proposed algorithm uses AFSA to optimize the selection of routing paths and ACOA to enhance the security of the selected paths. The primary issue addressed by the paper is the need for secure routing in UASNs. Due to the unique characteristics of the underwater acoustic channel, such as low bandwidth and high error rates, traditional security measures are not effective in UASNs. Therefore, there is a need for secure routing algorithms that can ensure the integrity, confidentiality, and availability of data transmission in UASNs. The major contribution of the paper is the development of a secure routing algorithm based on the AFSA-ACOA fusion technique that can ensure the integrity, confidentiality, and availability of data transmission in UASNs. The proposed algorithm is shown to be effective in optimizing routing paths while also enhancing the security of the selected paths. The paper discusses several types of attacks

that can be launched against UASNs, including packet dropping attacks, Sybil attacks, and replay attacks. The proposed secure routing algorithm is designed to protect against these attacks by ensuring the integrity and confidentiality of data transmission in UASNs. The proposed secure routing algorithm can be implemented in any UASN that uses acoustic communication for data transmission. The algorithm is specifically designed to be effective in the presence of various types of attacks, making it suitable for use in a wide range of UASN applications. The algorithm can be implemented using a range of hardware and software platforms, depending on the specific requirements of the application.

6.3.2. Secure Routing Scheme for UASNs

The researchers in [91] designed secure routing scheme for UASNs environment. Since establishment of the trusted third party is difficult in UASNs therefore a short signature algorithm is suggested for the purpose of secure route establishment among source and the destination node. The authors proposed signature scheme which improves security and can resist attacks such as forgery attacks. The proposed scheme does not require an online trusted third party. For achieving anonymity among sensor nodes, the authors presented a trapdoor scheme. With the help of digital signature as well as bilinear map trap door the suggested routing approach in this research achieves anonymity as well as two-way authentication between origin and target nodes, evades the problem of identity deception among the sensor nodes and delivers security for the interaction in UASNs environment. The trap door in the suggested scheme reduces the overhead for managing pre-shared keys in large numbers. One hash operation as well as one bilinear mapping is included in opening trap door. For performance evaluation of the suggested scheme, simulations were done using NS2 simulator with UWSNs simulation package known as Aqua-Sim. Performance comparison is done with GPNC and LB-AGR using throughput, energy consumption and PDR. The results show improved performance of the proposed scheme regarding security and network performance. The secure routing scheme for UASNs is reflected in Figure 6.

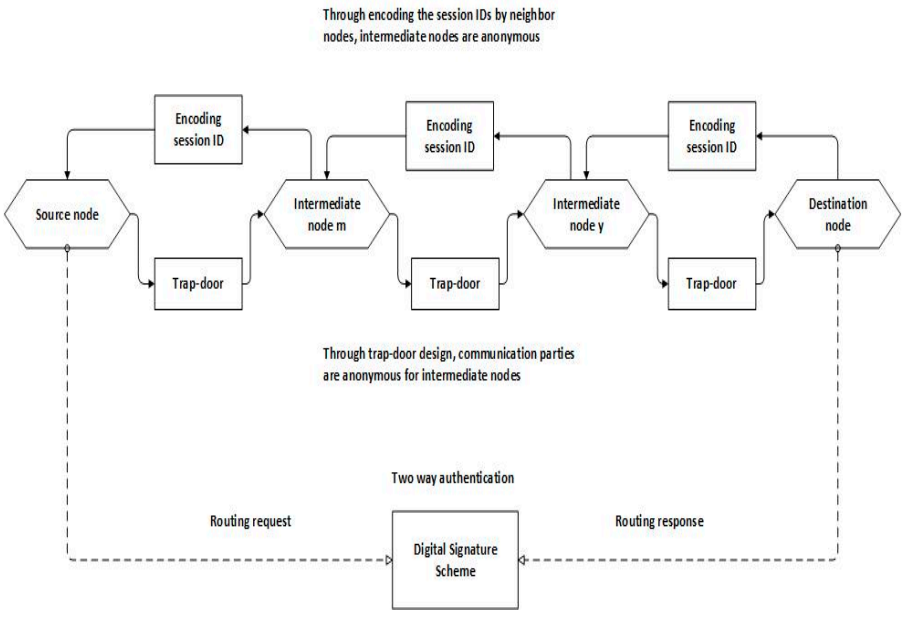

Figure 6. Secure routing scheme for UASNs [91].

6.3.3. Secure Energy Efficient and Cooperative Routing Scheme for UWSNs

Authors in [92] proposed secure energy efficient and cooperative routing (SEECR) protocol for UWSNs environment. SEECR efficiently utilizes energy consumption and has a built-in defense mechanism. Performance comparison of SEECR is carried out with AMCTD using different performance evaluation parameters. The results obtained revealed that

SEECR protocol beats AMCTD protocol in terms of all performance evaluation parameters. The results revealed that the performance of SEECR is better as compared to AMCTD. SEECR shows 9% improvement in number of alive nodes, reduces transmission loss more than 50%, up to 9% improvement in throughput, reduces energy tax up to 23%, and reduces end-to-end delay by 25%.

6.3.4. Securing UWSNs from Routing Attacks

Authors in [93] suggested distributed mechanism to combat specific attacks related to routing in UWSNs environment. The proposed mechanism can detect active and internal attacks on routing protocols such as sinkhole and wormhole attack. Silent monitoring and detection are the two phases used in the proposed mechanism. For mitigation and detection, the sensor nodes overhear the messages of neighbor sensor nodes. Immediately after deployment, each sensor node discovers the neighbor using secure neighbor discovery protocol. The purpose of tracking the activities of neighbors is to detect malicious activities in UWSNs. The consequence of the sinkhole attack is that it can tamper as well as drop the received packets. The solution proposed in this research can detect sinkhole attack by comparing the outgoing as well as the incoming traffic of each neighbor sensor node. If the malicious node has dropped or tampered the packets, then the signatures will not match and in this way an attack will be detected. The mechanism proposed in this research can detect active attack but cannot detect passive attack such as if the malicious node captures the traffic for analysis but do not tamper or drop it then the proposed mechanism cannot detect such type of attack. The proposed mechanism can also detect out of bound as well as encapsulated wormhole attack by checking the signatures. When a malicious node is detected in UWSNs environment then the malicious node is separated using isolation scheme from the network. As a result, the malicious node cannot participate in the activities of the UWSNs and cannot abrupt the routing operation. The idea presented in this research has been implemented using Castalia simulator which is based on OMNET++. In future this research can be extended by designing mechanism for other attacks in the UWSNs environment. Figure 7 reflects the two types of Wormhole attack such as an encapsulated attack channel and out-of-band attack channel. The attacker nodes A and B can communicate despite having more distance among them. Figure 8 reflects Sinkhole attack in which the attacker node is sending the received packets to the base station.

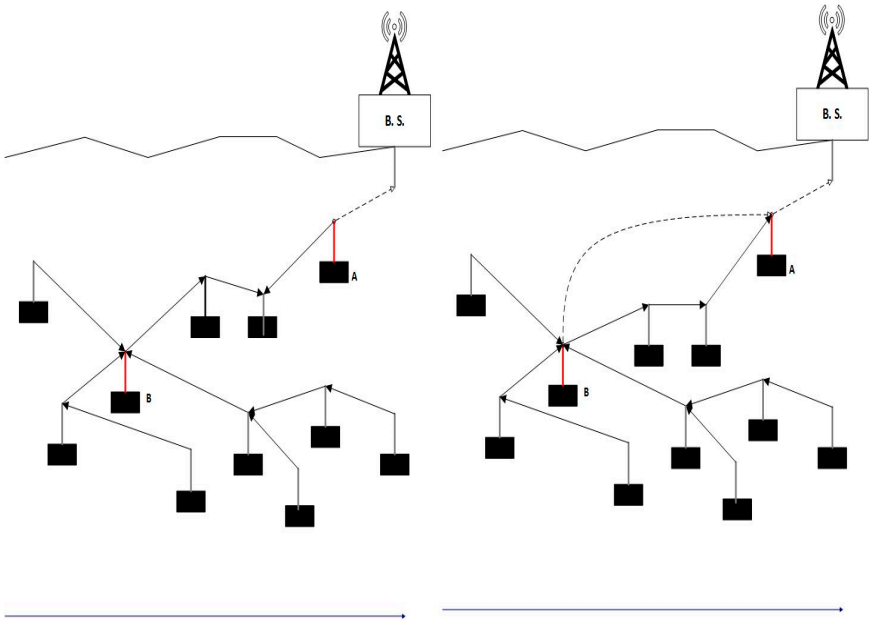

Figure 7. Wormhole attack [93].

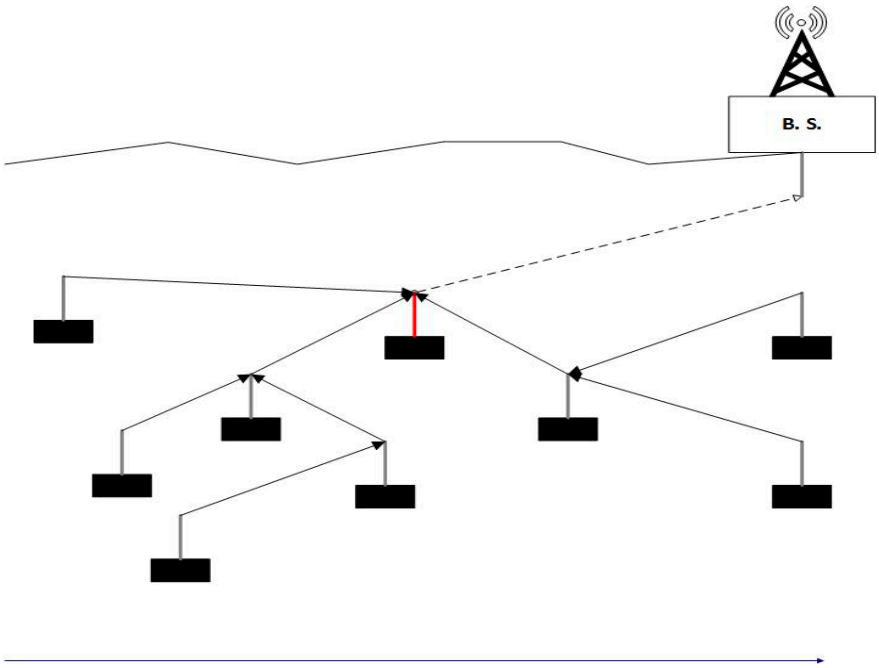

Figure 8. Sinkhole attack [93].

6.3.5. Secure Neighbor Discovery in UASNs

The authors in [94] suggested a scheme of secure discovery of neighbors in UASNs environment. In a hostile environment, the attacker can launch wormhole attack such as the discovery of neighbor is susceptible to wormhole attack. Consequences of the wormhole attack are undesirable results, and these consequences cannot be resolved by cryptographic approaches. This research proposed a suite of protocols which performs secure discovery of neighbor that is resilient to wormhole in UASNs. The recommended protocols in this research are established on the direction of arrival signals approach. The proposed scheme has the capability to resist wormhole attacks. The proposed scheme consists of the following four protocols: (i) B-NDP requires two nodes in neighbor discovery, (ii) DV-NDP has the requirement of three nodes, (iii) SDV-NDP improves DV-NDP and (iv) MA-NDP which accommodate the mobility of node. The evaluation results of the following four protocols are as follows: (i) B-NDP has the capability to stop fake neighbors from establishing neighbor relationship with extremely high-level probability. The genuine neighbors can find out each other in B-NDP. (ii) DV-NDP has the capability to stop fake neighbors from establishing neighbor relationship with probability near to 1 and with few links lost as cost. (iii) SDV-NDP has the capability to identify every wormhole, but the link lost is much in SDV-NDP as compared to DV-NDP. (iv) MA-NDP has the capability to detect wormhole links which are randomly positioned with high probability and can manage node mobility. B-NDP and MA-NDP protocols are appropriate for those applications having connectivity as well as end-to-end delay as their main concern. They are also appropriate for an environment having low density. DV-NDP and SDV-NDP protocols are proper for those applications that have high-level density of node and wormhole resilience needs.

6.3.6. Secure Communication Suite for UASNs

The authors in [95] suggested a security suite which consists of static as well as mobile sensor nodes for UASNs environment. The purpose of the security suite is to achieve confidentiality and integrity in the UANSs environment. The security suite includes secure routing protocols and cryptographic primitives. The researchers first proposed FLOOD protocol. The secure version of the mentioned protocol is introduced known as the secure flood (SeFLOOD). The performance evaluation of SeFLOOD protocol was carried out to evaluate the amount of overhead added to FLOOD protocol to make it secure. The

testbed is comprised of two nodes that are fixed i.e., FN1 and FN2, gateway (GW), two unmanned aerial vehicles (UAVs) such as FLG1 and FLG2 as shown in Figure 9. The results of experiments reveal suitability of the proposed suite for UASNs environment. The proposed suite bears less communication overhead and power consumption. The following are the key accomplishments of the proposed protocol suite. (i) The proposed suite is efficient because of the limited effect of the cipher text expansion. (ii) The discovery phase of the secure protocol produces less additional overhead i.e., 6% as compared to the unsecure protocol. (iii) The phase of reconfiguration in the secure protocol did not produce extra overhead as compared to unsecure protocol. (iv) Lampson's recommendations for the design of the computer system have been followed in the design of secure protocol.

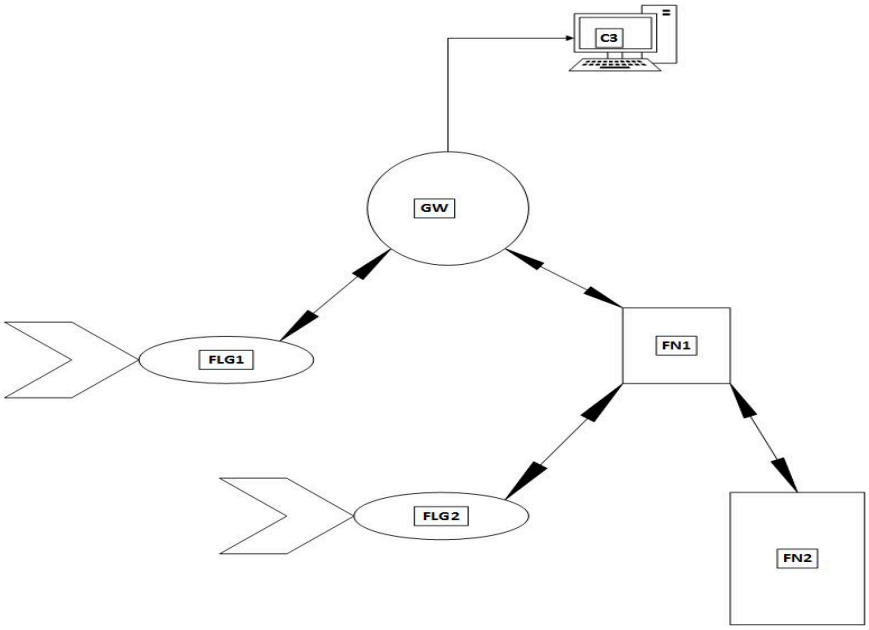

Figure 9. Testbed [95].

6.3.7. Secure Communication in Mobile UWSNs

Researchers in [96] focused on DoS attack. Classification of the DoS attack includes flooding, man-in-the-middle (MITM), as well as demolishing attack. MITM attack in UWSNs captured the data transferred among sensor nodes. The possible MITM attacks in UWSNs environment are selective forwarding, wormhole, and sybil attack. Inside flooding attack, the malicious node(s) causes congestion by sending stream of packets to the base station. The flooding attack worsens the performance of entire network in UWSNs environment. Demolishing attack in UWSNs includes modifying or tampering the configuration of sensor node which results in the destruction of the entire network. Physical security plays an important role in the demolishing attack. The mobile sensor nodes in UWSNs environment face issues such as out of coverage issue and false neighbor identification issue. In this research, the authors used Aqua-Sim for simulation. The results obtained show that due to the performance variation among mobile UWSNs and WSNs the security mechanism suitable for mobile WSNs is not suitable for mobile UWSNs. The possible future work of this research can be designing secure UWSNs with intelligent sensor nodes and self-localization for combating DoS attacks in mobile UWSNs.

6.3.8. An IDS for Opportunistic Routing in UWSNs

Research conducted in [97] proposes a novel intrusion detection scheme called DOIDS, which is based on the density-based spatial clustering of applications with noise (DBSCAN) algorithm. DOIDS is designed to detect and mitigate attacks on opportunistic routing (OR) schemes in underwater wireless sensor networks (UWSNs). The primary issue addressed by the paper is the need for effective intrusion detection schemes that can detect and

mitigate attacks on OR schemes in UWSNs. Traditional intrusion detection schemes are not well-suited for UWSNs due to the unique challenges posed by the underwater environment. The major contribution of the paper is the development of the DOIDS intrusion detection scheme, which is specifically designed to detect and mitigate attacks on OR schemes in UWSNs. The scheme is shown to be effective in detecting and mitigating the effects of several types of attacks, including selective forwarding attacks, sinkhole attacks, and wormhole attacks. The paper discusses several types of attacks that can be launched against OR schemes in UWSNs, including selective forwarding attacks, sinkhole attacks, wormhole attacks, and Sybil attacks. The proposed DOIDS scheme is designed to protect against these attacks by detecting and mitigating their effects. The proposed DOIDS scheme can be implemented in any UWSN that uses OR for data transmission. The scheme is specifically designed to be effective in the presence of both random and targeted attacks, making it suitable for use in a wide range of UWSN applications. The scheme can be implemented using a range of hardware and software platforms, depending on the specific requirements of the application.

6.4. Frameworks/Models for UWSNs

This section includes analysis of different frameworks/models proposed by the research community for UWSNs environment. The analysis is also presented in tabular form in Table 4.

Table 4. Analysis of frameworks/models for UWSNs.

Technique	Issue Addressed	Major Contribution	Attack Type	Implementation Environment
Fault-Tolerant Trust Model for UASNs [98]	Addressed the need for a fault-tolerant trust model for UASNs.	Developed a fault-tolerant trust model that is specifically tailored to the requirements and constraints of UASNs. The model is shown to be effective in detecting and mitigating the effects of both isolated and coordinated attacks, as well as sensor node failures.	Provide protection against node compromise attacks, selective forwarding attacks, and wormhole attacks.	MATLAB
Security framework for UASNs [99]	Addressed confidentiality, integrity, authentication, and non-repudiation in UASNs.	Proposed security framework called SecFUN for UASNs. The proposed secure version of CARP is efficient in terms of energy efficiency as well as latency.	Resistant against sybil attack, hello flood attack, acknowledgement spoofing, replay attack, exhaustion, selective forwarding attack, and sinkhole attack.	Gumstix verdex pro platform
TCM for UWSNs [100]	Addressed the trust establishment problem among nodes in UWSNs.	Proposed TCM trust model for UWSNs. The performance of TCM is much better than LCT and CBTM models.	Proposed mechanism detects malicious sensor node in UWSNs.	MATLAB

6.4.1. Fault-Tolerant Trust Model for UASNs

The authors in [98] proposed a fault-tolerant trust model that is designed to provide secure and reliable data transmission in underwater acoustic sensor networks (UASNs) in the presence of hybrid attacks. The model uses a combination of trust evaluation and fault-tolerant data fusion to detect and mitigate the effects of malicious nodes in the network. The primary issue addressed by the paper is the need for a fault-tolerant trust model that can provide secure and reliable data transmission in UASNs, even in the presence of hybrid attacks. Traditional trust models are not well-suited for UASNs due to the unique challenges posed by the underwater environment. The major contribution of the paper is the development of a fault-tolerant trust model that is specifically tailored to the

requirements and constraints of UASNs. The model is shown to be effective in detecting and mitigating the effects of both isolated and coordinated attacks, as well as sensor node failures. The paper discusses several types of attacks that can be launched against UASNs, including node compromise attacks, selective forwarding attacks, and wormhole attacks. The proposed trust model is designed to protect against these attacks by providing secure and reliable data transmission, even in the presence of malicious nodes. The proposed trust model can be implemented in any UASN that uses acoustic communication for data transmission. The model is specifically designed to be fault-tolerant and able to operate in the presence of both random and targeted attacks, making it suitable for use in a wide range of UASN applications.

6.4.2. SecFUN

The authors in [99] proposed a security framework named SecFUN for UASNs. The proposed framework implements advanced encryption standard (AES) in Galois counter mode (GCM) and digital signature algorithms which are short i.e., ZSS, Quartz, and BLS to deliver the features of confidentiality, integrity, non-repudiation, and authentication. In this research the authors mentioned some attacks possible in UWSNs environment. The authors recommended applying cross layer security mechanism to combat these attacks. In this research, the cryptographic primitives selected for the security framework are most effective. The proposed framework is flexible and can be configured with different security levels to meet the needs of UASNs security. This research extended operation of the channel aware routing protocol (CARP). The results obtained in this research revealed that CARP secure version is efficient in consumption of energy as well as latency. For implementing security there must be additional processing but the resources in UASNs environment are limited due to which there is a demand of energy-efficient security mechanisms for UASNs environment so that the solutions remain applicable for the said environment. Moreover, the researchers must keep a balance between energy efficiency and security.

6.4.3. TCM for UWSNs

The research conducted in [100] recommended trust model called TCM for UWSNs environment. The authors discussed in detail the available trust management mechanisms. The existing trust management mechanisms are split into seven groups based on methods and theories to calculate trust. These are: trust management based on subjective logic, Bayesian theory, probability, fuzzy logic, D-S evidence, entropy theory, and cloud theory. Because of the distinctive qualities of UWSNs, the existing trust management mechanisms are not suitable for UWSNs. TCM quantifies the trust relationship between sensor nodes. The sensor nodes based on quantified results can decide about trustworthiness of other sensor nodes and can transmit data only via trusted sensor nodes. For performance evaluation of TCM, the subsequent aspects are used: performance of malicious nodes detection, performance of trust value calculation, performance of data transmission. The results obtained show that TCM has better results as compared to the other two existing trust models. The workflow of trust cloud model is reflected in Figure 10.

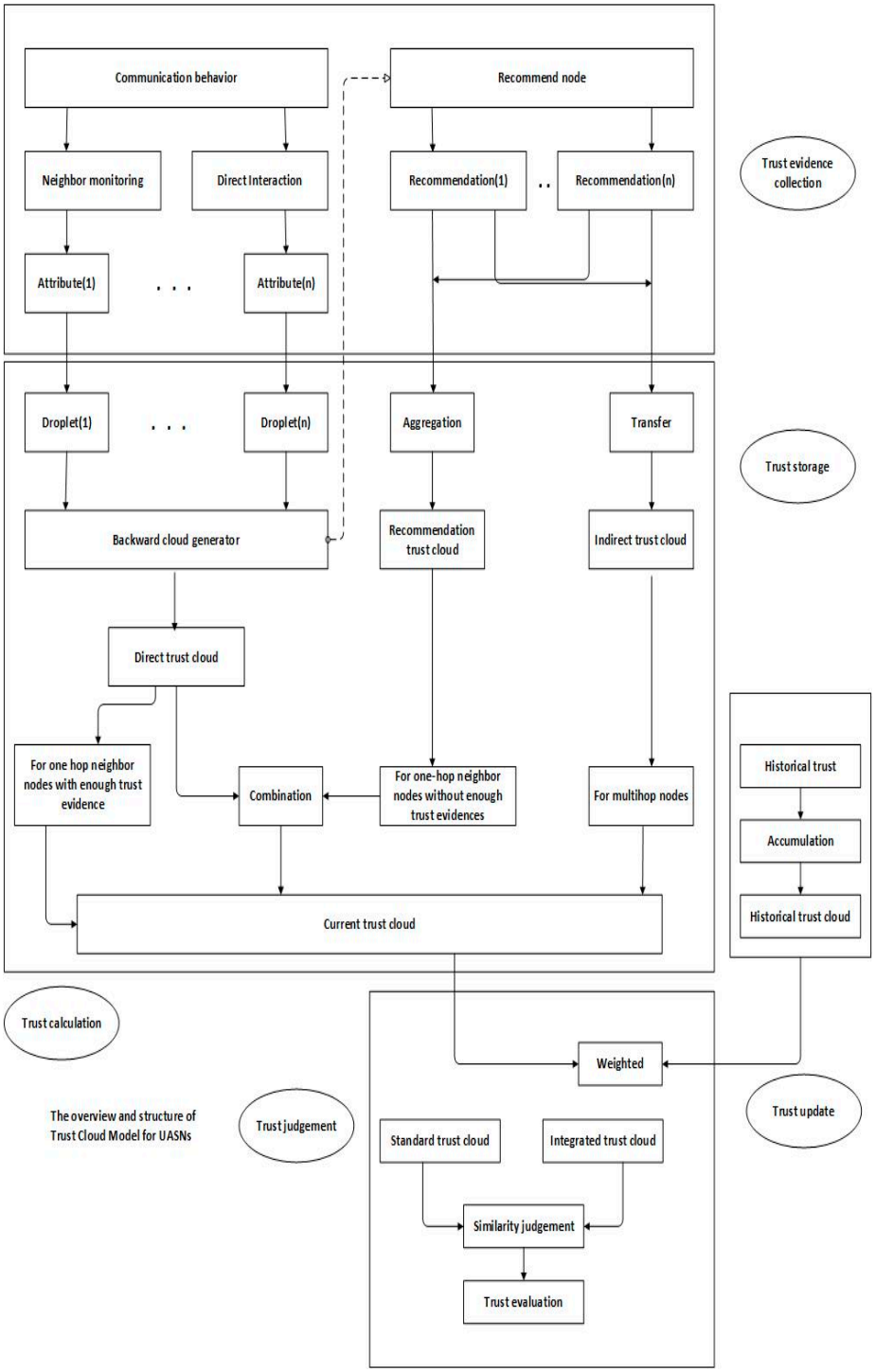

Figure 10. Workflow of trust cloud model [100].

6.5. Secure MAC Protocols for UWSNs

This section includes the analysis of different secure MAC protocols proposed by the research community for UWSNs environment. The analysis is also presented in tabular form in Table 5.

Table 5. Analysis of secure MAC protocols for UWSNs.

Technique	Issue Addressed	Major Contribution	Attack Type	Implementation Environment
Security modes for UASNs [101]	Addressed the issue of secure MAC protocol for UASNs.	Suggested MAC protocol which is secure and suitable for UASNs. Suggested protocol is secure, efficient regarding energy consumption and transmission time.	It can resist against replay attack.	Real environment implementation with fish robot
SC-MAC for UWSNs [102]	Addressed the issue of secure MAC protocol for UWSNs	Proposed cluster based secure MAC protocol for UWSNs. SC-MAC ensures secure transmission of data under hostile and harsh UWSNs environment.	SC-MAC can resist against replay, sybil, and message manipulation attack.	Aqua-Sim

6.5.1. Security Modes for UASNs

The authors in [101] proposed a secure MAC protocol. The purpose of the secure MAC protocol is reliability of data, energy efficiency, confidentiality of data, authenticity, and anti-attacker prevention in the UASNs environment. According to basic operation, first node A sends RTSA to node B to occupy the channel before sending data to node B. When node B receives RTSA, it sends CTSB back to node A which means that the recipient node B is available. In this scenario a malicious node C pays attention to the signals from node A such as RTSA. After receiving CTSB from node B by node A, node A broadcasts data for node B which will also be received by node C, but the data will be in encrypted form. Node C cannot decrypt the data because the security information required is with node A and B only. In this research, CCM-UW mode that is based on algorithms such ARIA and AES is used. Comparison is carried out with the existing MAC protocols and the MAC protocol proposed in this research is efficient regarding consumption of energy as well as transmission time. The comparison is carried out based on security levels and algorithms. The implementation of the proposed mechanism is carried out in a real environment with a fish robot. The findings obtained reveal that the proposed MAC protocol is better than the existing solutions because it is efficient and secure. The results in this research further show that the obtained results are not optimized but these results can be used as a base, and it provides sufficient data in order to carry out research and deploy network security in the UASNs environment. Basic operation of secure MAC protocol is presented in Figure 11.

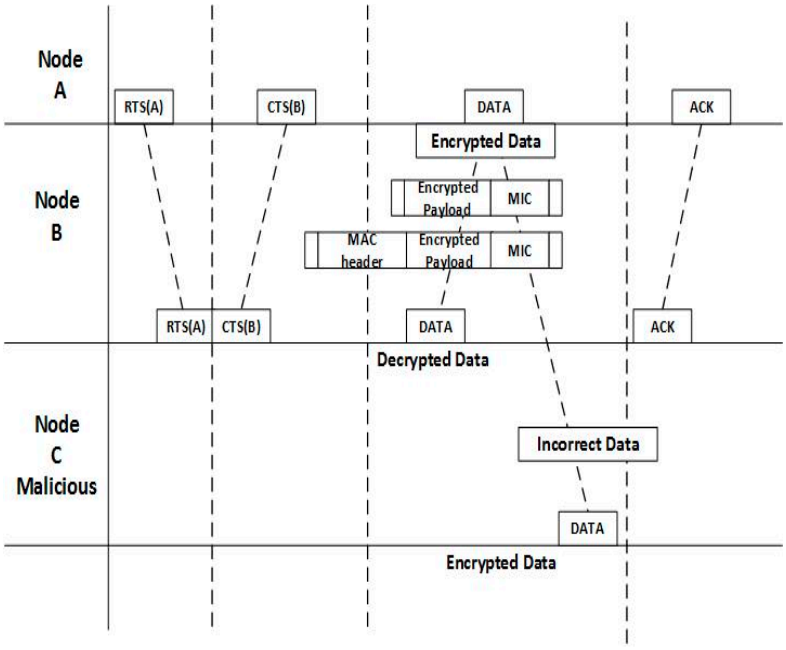

Figure 11. Basic operation of secure MAC [101].

6.5.2. SC-MAC for UWSNs

The research conducted by authors in [102] suggested a secure MAC protocol known as SC-MAC for the UWSNs environment. SC-MAC is cluster-based, and it ensures secure transmission of data under hostile and harsh UWSNs environment. SC-MAC can resist replay attack, sybil attack, and message manipulation attack. The clusters in SC-MAC are formed as well as updated securely and dynamically. To extend the lifespan of the network, the MAC layer data are leveraged by taking into account the residual energy and link quality of the modem's battery. When the mutual authentication is successfully carried out among the sensor nodes, the nodes that are in different clusters can protect the transmission of data. The simulation in this research is carried out using an Aqua-Sim simulator. The value of the sensor nodes is set to 50, the value of the sink nodes is set to 8, malicious nodes ratio is set to 10%, and the simulation area is set to 2 km $\times$ 2 km $\times$ 2 km. The results obtained in this research shows that the suggested SC-MAC executes well in comparison to the present MAC protocols in delivery ratio, network throughput, and consumption of energy.

7. Current Challenges and Future Trends

In UWSNs, increasing the overall network lifetime is the main area of research focused so far by the research community. Some current challenges and future trends are as follows.

Developing more efficient communication techniques that can balance the need for high throughput and real-time communication with the limited energy resources of UWSNs. Exploring and implementing more robust security mechanisms for UWSNs to ensure the confidentiality, integrity, and availability of the data transmitted and processed by the network. Investigating the use of different cryptographic algorithms and techniques, such as block cipher algorithms for improving the security of UWSNs.

Acoustic waves are mostly used in UWSNs for communication but there are some applications that cannot use acoustic waves because they need high throughput as well as real-time communication. In this case, magneto-inductive (MI) is recommended especially for the Internet of UW things. In MI wireless power of transfer is enabled efficiently that increases the operating lifetime of UWSNs. The use of heterogenous channels can be useful based on MI and acoustic channels. The acoustic channel can be utilized for long communication range and low data rate. MI channel can be used for short communication range and high data rate [103].

Due to the energy constrained UWSNs environment the mechanism designed for WNSs environment is not suitable for the environment of UWSNs. The research community mostly focused on energy efficiency related issues whereas security issues along with security mechanisms are not properly explored. Research conducted in [84] proposed key distribution scheme for UWSNs which is applied on two mobility models namely meandering mobility model and nomadic mobility model. Further research exploration in this area can be to propose key distribution scheme having support for different mobility models in the UWSNs environment. Research conducted in [87] proposed modifications in AES to make it suitable for UASNs. Further research exploration in this research area can propose more energy-efficient secure solutions for UWSNs because the environment of UWSNs is resource constrained. Research conducted in [96] discussed various DoS attacks in mobile UWSNs. Further research exploration in this area can be designed for secure UWSNs with intelligent sensor nodes and self-localization for combating DoS attacks in mobile UWSNs.

Research conducted in [100] proposed a trust model called TCM for underwater environment. Further research exploration in this research area can be to establish the trust when the nodes are moving in underwater environment, establishment of trust when the sensor nodes are sparsely deployed, and they are far away from each other. Research conducted in [88] discussed algorithms for security in UWASNs considering suitability for UWASNs environment. They proposed the use of CMVP for the mentioned purpose. Further research exploration in this research area can be carried out by considering block

cipher algorithms such as ARIR and SEED for UWASNs environment. Research conducted in [101] proposed MAC protocol that is secure and suitable for UASNs. Further research exploration in this research area can be carried out by using the technology for underwater security with other network system such as IEEE 802.15.3 (UWB), IEEE 802.11 (WLAN), IEEE 802.15.4 (ZigBee). Research conducted in [104] suggested an algorithm known as Tic-Tac-Toe AI-MINIMAX. The purpose of proposed algorithms is for establishing secure and optimal paths for routing in the UWSNs environment. Further research exploration in this research area can be to use AI models for reducing intelligent attacks in the network for leading to robust systems. According to the research conducted in [96], transfer rate of packets in UWSNs environment can be reduced by utilizing intelligent sensor nodes that are self- localized. In order to address the DoS problem in UWSNs environment, secure UWSNs having intelligent sensor nodes and self- localization should be designed.

8. Conclusions

Security plays an important role in almost every field of computing including UWSNs. In this research, an analysis of security-based schemes in UWSNs is presented. It includes the relevant research work done on security in UWSNs. Research carried out on security in UWSNs so far includes security framework/models for UWSNs, proposed encryption mechanisms for UWSNs, secure routing solutions for UWSNs, key management schemes for UWSNs, and secure MAC algorithms for UWSNs. The research work carried out by the research community regarding security in UWSNs is analyzed in detail. The problem addressed, major contributions, and possible future research directions are discussed in detail. The possible future research directions identified in this research can be explored by the research community. It is observed in this research that security mechanisms designed for WSNs are not suitable for UWSNs due to the constrained resources in UWSNs environment. Moreover, it is also concluded that the research community should consider computation cost in terms of energy while designing secure solution so that the solution remains sustainable for UWSNs environment.

Author Contributions: Conceptualization, K.S. and W.K.; methodology, K.S., S.A. and A.A.; software, K.S.; validation, K.S. and A.S.A.-S.; formal analysis, K.S. and S.Z.A.; investigation, A.A.; resources, S.Z.A. and S.A.; data curation, A.G., A.S.A.-S. and S.Z.A.; writing—original draft preparation, K.S., S.A. and W.K.; writing—review and editing, K.S., W.K., A.A. and S.Z.A.; visualization, K.S and S.Z.A.; supervision, W.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: We would like to extend our appreciation to Umm AL-Qura University, Al-lith Campus, Kingdom of Saudi Arabia and Al-Ahliyya Amman University and, for providing all necessary support to conduct this research work.

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

References

1. Sun, N.; Wang, X.; Han, G.; Peng, Y.; Jiang, J. Collision-Free and Low Delay MAC Protocol Based on Multi-Level Quorum System in Underwater Wireless Sensor Networks. *Comput. Commun.* **2021**, *173*, 56–69. [CrossRef]
2. Khasawneh, A.M.; Kaiwartya, O.; Abualigah, L.M.; Lloret, J. Green Computing in Underwater Wireless Sensor Networks Pressure Centric Energy Modeling. *IEEE Syst. J.* **2020**, *14*, 4735–4745. [CrossRef]
3. Lu, Q.; Liu, F.; Zhang, Y.; Jiang, S. Routing Protocols for Underwater Acoustic Sensor Networks: A Survey from an Application Perspective. In *Advances in Underwater Acoustics*; InTech Open: Rijeka, Croatia, 2017; p. 23.
4. Ahmed, S.; Javaid, N.; Khan, F.A.; Durrani, M.Y.; Ali, A.; Shaukat, A.; Sandhu, M.M.; Khan, Z.A.; Qasim, U. Co-UWSN: Cooperative Energy-Efficient Protocol for Underwater WSNs. *Int. J. Distrib. Sens. Netw.* **2015**, *11*, 891410. [CrossRef]

5. Heidemann, J.; Ye, W.; Wills, J.; Syed, A.; Li, Y. Research Challenges and Applications for Underwater Sensor Networking. In Proceedings of the IEEE Wireless Communications and Networking Conference, 2006 (WCNC 2006), Las Vegas, NV, USA, 3–6 April 2006; Volume 1, pp. 228–235.
6. Pompili, D.; Melodia, T. Three-Dimensional Routing in Underwater Acoustic Sensor Networks. In Proceedings of the 2nd ACM International Workshop on Performance Evaluation of Wireless ad Hoc, Sensor, and Ubiquitous Networks, Montreal, QC, Canada, 10–13 October 2005; pp. 214–221.
7. Fattah, S.; Gani, A.; Ahmedy, I.; Idris, M.Y.I.; Targio Hashem, I.A. A Survey on Underwater Wireless Sensor Networks: Requirements, Taxonomy, Recent Advances, and Open Research Challenges. *Sensors* **2020**, *20*, 5393. [CrossRef]
8. Jodeh, H.; Mikkawi, A.; Awad, A.; Othman, O. Comparative Analysis of Routing Protocols for Under-Water Wireless Sensor Networks. In Proceedings of the 2nd International Conference on Future Networks and Distributed Systems, New York, NY, USA,, 26–27 June 2018; pp. 1–7.
9. Waite, A.D. *Sonar for Practising Engineers*; Wiley: Hoboken, NJ, USA, 2002.
10. Robert, J.U. *Principles of Underwater Sound for Engineers*; McGraw-Hill Book Company: New York, NY, USA, 1967.
11. Chen, K.; Zhou, Y.; He, J. A Localization Scheme for Underwater Wireless Sensor Networks. *Int. J. Adv. Sci. Technol.* **2009**, *4*, 9–16. Available online: https://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=042608D7A4B2F0749F1139CA5222C7F9?doi=10.1.1.178.3027&rep=rep1&type=pdf (accessed on 17 January 2023).
12. 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*, 213012. [CrossRef]
13. Ahmed, S.; Javaid, N.; Ahmad, A.; Ahmed, I.; Durrani, M.Y.; Ali, A.; Haider, S.B.; Ilahi, M. SPARCO: Stochastic Performance Analysis with Reliability and Cooperation for Underwater Wireless Sensor Networks. *J. Sens.* **2016**, *2016*, 7604163. [CrossRef]
14. Felemban, E.; Shaikh, F.K.; Qureshi, U.M.; Sheikh, A.A.; Qaisar, S.B. Underwater Sensor Network Applications: A Comprehensive Survey. *Int. J. Distrib. Sens. Netw.* **2015**, *11*, 896832. [CrossRef]
15. Cui, J.-H.; Kong, J.; Gerla, M.; Zhou, S. The Challenges of Building Mobile Underwater Wireless Networks for Aquatic Applications. *IEEE Netw.* **2006**, *20*, 12–18.
16. Babu, A.V.; Joshy, S. Maximizing the Data Transmission Rate of a Cooperative Relay System in an Underwater Acoustic Channel. *Int. J. Commun. Syst.* **2012**, *25*, 231–253. [CrossRef]
17. Cai, S.; Gao, Z.; Yang, D.; Yao, N. A Network Coding Based Protocol for Reliable Data Transfer in Underwater Acoustic Sensor. *Ad Hoc Netw.* **2013**, *11*, 1603–1609. [CrossRef]
18. Chen, Y.-S.; Lin, Y.-W. Mobicast Routing Protocol for Underwater Sensor Networks. *IEEE Sens. J.* **2012**, *13*, 737–749. [CrossRef]
19. Harris, A.F., III; Zorzi, M. Modeling the Underwater Acoustic Channel in Ns2. In Proceedings of the 1st International ICST Workshop on Network Simulation Tools, Nantes, France, 16 May 2010.
20. Khasawneh, A.; Latiff, M.S.B.A.; Kaiwartya, O.; Chizari, H. A Reliable Energy-Efficient Pressure-Based Routing Protocol for Underwater Wireless Sensor Network. *Wirel. Netw.* **2018**, *24*, 2061–2075. [CrossRef]
21. Ren, Y.; Seah, W.K.; Teal, P.D. Performance of Pressure Routing in Drifting 3D Underwater Sensor Networks for Deep Water Monitoring. In Proceedings of the seventh ACM International 'Conference on Underwater Networks and Systems, Los Angeles, CA, USA, 5–6 November 2012; Volume 284, pp. 1–8. [CrossRef]
22. Tsai, C.S.; Yang, C.F. A novel energy efficient joint dynamic emissive location-based routing scheme for SOFAR channel underwater sensor networks. In *Applied Mechanics and Materials*; Trans Tech Publications Ltd.: Bäch SZ, Switzerland, 2013; Volume 284, pp. 2001–2004.
23. Vieira, L.F.M. Performance and Trade-Offs of Opportunistic Routing in Underwater Networks. In Proceedings of the 2012 IEEE Wireless Communications and Networking Conference (WCNC), Paris, France, 1–4 April 2012; pp. 2911–2915.
24. Wahid, A.; Kim, D. Connectivity-Based Routing Protocol for Underwater Wireless Sensor Networks. In Proceedings of the 2012 International Conference on ICT Convergence (ICTC), Jeju, Republic of Korea, 15–17 October 2012; pp. 589–590.
25. Watfa, M.K.; Selman, S.; Denkilkian, H. UW-MAC: An Underwater Sensor Network MAC Protocol. *Int. J. Commun. Syst.* **2010**, *23*, 485–506. [CrossRef]
26. Zhang, S.; Li, D.; Chen, J. A Link-State Based Adaptive Feedback Routing for Underwater Acoustic Sensor Networks. *IEEE Sens. J.* **2013**, *13*, 4402–4412. [CrossRef]
27. Khasawneh, A.; Abd Latiff, M.S.B.; Kaiwartya, O.; Chizari, H. Next Forwarding Node Selection in Underwater Wireless Sensor Networks (UWSNs): Techniques and Challenges. *Information* **2016**, *8*, 3. [CrossRef]
28. Karpagam, M.; Prabha, D. Underwater Wireless Sensor Network Based Marine Environment Monitoring System. *Int. J. Ocean. Oceanogr.* **2019**, *13*, 269–276.
29. Nain, M.; Goyal, N. Localization techniques in underwater wireless sensor network. In Proceedings of the 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 4–5 March 2021; pp. 747–751.
30. Gkikopouli, A.; Nikolakopoulos, G.; Manesis, S. A Survey on Underwater Wireless Sensor Networks and Applications. In Proceedings of the 2012 20th Mediterranean conference on Control & Automation (MED), Barcelona, Spain, 3–6 July 2012; pp. 1147–1154.

31. Heidemann, J.; Li, Y.; Syed, A.; Wills, J.; Ye, W. Underwater Sensor Networking: Research Challenges and Potential Applications. In Proceedings of the Technical Report ISI-TR-2005-603, USC/Information Sciences Institute. 2005. Available online: https://www.isi.edu/~johnh/PAPERS/Heidemann05b.pdf (accessed on 17 January 2023).
32. Davis, A.; Chang, H. Underwater Wireless Sensor Networks. In Proceedings of the 2012 Oceans, Hampton Roads, VA, USA, 14–19 October 2012; pp. 1–5.
33. Brighty, S.P.S.; Brinda, S.J.; Hemagayathri, R. Recent Advances and Challenges in Underwater Sensor Networks-Survey. *Intl. Jol. Innov. Eng. Technol. (IJIET)* **2017**, *8*, 111–117.
34. Kumar, S.; Kumari, B.; Chawla, H. Security Challenges and Application for Underwater Wireless Sensor Network. In Proceedings of the International Conference on Emerging Trends in Expert Applications & Security Emer, Jaipur, India, 17–18 February 2018; Volume 2, pp. 15–21. Available online: https://www.jecrcfoundation.com/jf-data/Conference/IC/CS/JECRC-ICETEAS%202018.pdf (accessed on 17 January 2023).
35. Tan, H.-P.; Diamant, R.; Seah, W.K.; Waldmeyer, M. A Survey of Techniques and Challenges in Underwater Localization. *Ocean Eng.* **2011**, *38*, 1663–1676. [CrossRef]
36. Shi, Z.J.; Fei, Y. Exploring Architectural Challenges in Scalable Underwater Wireless Sensor Networks. In Proceedings of the Proceedings of Annual Boston Area Computer Architecture Workshop (BARC) University of Rhode Island Kingston, Kingston, RI, USA, 3 February 2006; Volume 2006, pp. 38–42. Available online: https://www.ele.uri.edu/barc2006/BARC-2006-Proceedings.pdf (accessed on 17 January 2023).
37. 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]
38. Bansal, R.; Maheshwari, S.; Awwal, P. Challenges and Issues in Implementation of Underwater Wireless Sensor Networks. *Opt. Wirel. Technol.* **2018**, *472*, 507–514.
39. Venkateswara Rao, P.V.; Mohan Krishna Varma, N.; Sudhakar, R. A Systematic Survey on Software-Defined Networks, Routing Protocols and Security Infrastructure for Underwater Wireless Sensor Networks (UWSNs). In *Emerging Research in Data Engineering Systems and Computer Communications*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 551–559.
40. Sendra, S.; Lloret, J.; Jimenez, J.M.; Parra, L. Underwater acoustic modems. *IEEE Sens. J.* **2015**, *16*, 4063–4071. [CrossRef]
41. Zia, M.Y.I.; Poncela, J.; Otero, P. State-of-the-art underwater acoustic communication modems: Classifications, analyses and design challenges. *Wirel. Pers. Commun.* **2021**, *116*, 1325–1360. [CrossRef]
42. Li, N.; Martínez, J.F.; Meneses Chaus, J.M.; Eckert, M. A survey on underwater acoustic sensor network routing protocols. *Sensors* **2016**, *16*, 414. [CrossRef]
43. Anwar, A.; Sridharan, D. A Survey on Routing Protocols for Wireless Sensor Networks in Various Environments. *Int. J. Comput. Appl.* **2015**, *112*, 5.
44. Han, G.; Jiang, J.; Bao, N.; Wan, L.; Guizani, M. Routing Protocols for Underwater Wireless Sensor Networks. *IEEE Commun. Mag.* **2015**, *53*, 72–78. [CrossRef]
45. Luo, J.; Chen, Y.; Wu, M.; Yang, Y. A survey of routing protocols for underwater wireless sensor networks. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 137–160. [CrossRef]
46. Khan, H.; Hassan, S.A.; Jung, H. On underwater wireless sensor networks routing protocols: A review. *IEEE Sens. J.* **2020**, *20*, 10371–10386. [CrossRef]
47. Shovon, I.I.; Shin, S. Survey on Multi-Path Routing Protocols of Underwater Wireless Sensor Networks: Advancement and Applications. *Electronics* **2022**, *11*, 3467. [CrossRef]
48. Liu, L.F.; Ma, M.D. Security Issues in Underwater Sensor Networks: Attacks and Defenses. In *Applied Mechanics and Materials*; Trans Tech Publ: Stafa-Zurich, Switzerland, 2014; Volume 644, pp. 2689–2698.
49. Vetrivendan, L.; Viswanathan, R.; Punitharaja, K. Security in Underwater Wireless Communication. *Int. J. Eng. Res. Comput. Sci. Eng.* **2018**, *5*, 154–159.
50. Ahmad, I.; Rahman, T.; Zeb, A.; Khan, I.; Ullah, I.; Hamam, H.; Cheikhrouhou, O. Analysis of security attacks and taxonomy in underwater wireless sensor networks. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 1–15. [CrossRef]
51. Wahid, A.; Lee, S.; Jeong, H.-J.; Kim, D. Eedbr: Energy-Efficient Depth-Based Routing Protocol for Underwater Wireless Sensor Networks. In Proceedings of the International Conference on Advanced Computer Science and Information Technology, Seoul, Republic of Korea, 27–29 September 2011; Springer: Berlin/Heidelberg, Germany, 2011; pp. 223–234.
52. Ali, T.; Jung, L.T.; Faye, I. End-to-End Delay and Energy Efficient Routing Protocol for Underwater Wireless Sensor Networks. *Wirel. Pers. Commun.* **2014**, *79*, 339–361. [CrossRef]
53. Al Salti, F.; Alzeidi, N.; Arafeh, B.R. EMGGR: An Energy-Efficient Multipath Grid-Based Geographic Routing Protocol for Underwater Wireless Sensor Networks. *Wirel. Netw.* **2017**, *23*, 1301–1314. [CrossRef]
54. Javaid, N.; Shakeel, U.; Ahmad, A.; Alrajeh, N.; Khan, Z.A.; Guizani, N. DRADS: Depth and Reliability Aware Delay Sensitive Cooperative Routing for Underwater Wireless Sensor Networks. *Wirel. Netw.* **2019**, *25*, 777–789. [CrossRef]
55. Gomathi, R.M.; Martin Leo Manickam, J. Energy Efficient Shortest Path Routing Protocol for Underwater Acoustic Wireless Sensor Network. *Wirel. Pers. Commun.* **2018**, *98*, 843–856. [CrossRef]
56. Hao, K.; Shen, H.; Liu, Y.; Wang, B. An Energy-Efficient Localization-Based Geographic Routing Protocol for Underwater Wireless Sensor Networks. In Proceedings of the International Wireless Internet Conference, Tianjin, China, 16–17 December 2017; Springer: Berlin/Heidelberg, Germany, 2017; pp. 365–373.

57. Anuradha, D.; Srivatsa, S.K. Energy Effectual Reconfigurable Routing Protocol (E2R2P) for Cluster Based Underwater Wireless Sensor Networks. *J. Ambient. Intell. Humaniz. Comput.* **2019**, *10*, 1–8. [CrossRef]
58. Bhattacharjya, K.; Alam, S.; De, D. CUWSN: Energy Efficient Routing Protocol Selection for Cluster Based Underwater Wireless Sensor Network. *Microsyst. Technol.* **2022**, *28*, 543–559. [CrossRef]
59. Venkateswarulu, B.; Subbu, N.; Ramamurthy, S. An Efficient Routing Protocol Based on Polar Tracing Function for Underwater Wireless Sensor Networks for Mobility Health Monitoring System Application. *J. Med. Syst.* **2019**, *43*, 1–8. [CrossRef]
60. Khisa, S.; Moh, S. Survey on recent advancements in energy-efficient routing protocols for underwater wireless sensor networks. *IEEE Access* **2021**, *9*, 55045–55062. [CrossRef]
61. Khan, Z.U.; Gang, Q.; Muhammad, A.; Muzzammil, M.; Khan, S.U.; Affendi, M.E.; Khan, J. A comprehensive survey of energy-efficient MAC and routing protocols for underwater wireless sensor networks. *Electronics* **2022**, *11*, 3015. [CrossRef]
62. Khan, A.; Ali, I.; Ghani, A.; Khan, N.; Alsaqer, M.; Rahman, A.U.; Mahmood, H. Routing Protocols for Underwater Wireless Sensor Networks: Taxonomy, Research Challenges, Routing Strategies and Future Directions. *Sensors* **2018**, *18*, 1619. [CrossRef]
63. 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]
64. Underwater Acoustic Sensor Networks by Yang Xiao | Perlego. Available online: https://www.perlego.com/book/1604650/underwater-acoustic-sensor-networks-pdf (accessed on 15 January 2023).
65. Lanbo, L.; Shengli, Z.; Jun-Hong, C. Prospects and Problems of Wireless Communication for Underwater Sensor Networks. *Wirel. Commun. Mob. Comput.* **2008**, *8*, 977–994. [CrossRef]
66. Mackenzie, K.V. Nine-term equation for sound speed in the oceans. *J. Acoust. Soc. Am.* **1981**, *70*, 807–812. [CrossRef]
67. Heidemann, J.; Stojanovic, M.; Zorzi, M. Underwater Sensor Networks: Applications, Advances and Challenges. *Philos. Trans. R. Soc. A Math. Phys. Eng. Sci.* **2012**, *370*, 158–175. [CrossRef] [PubMed]
68. Xiang-ping, G.; Rong-lin, H. Analyzing the Performance of Channel in Underwater Wireless Sensor Networks (UWSN). *Procedia Eng.* **2011**, *15*, 95–99. [CrossRef]
69. Cui, J.-H.; Kong, J.; Gerla, M.; Zhou, S. Challenges: Building Scalable and Distributed Underwater Wireless Sensor Networks (UWSNs) for Aquatic Applications. *Channels* **2005**, *45*, 22–35.
70. Ayaz, M.; Baig, I.; Abdullah, A.; Faye, I. A Survey on Routing Techniques in Underwater Wireless Sensor Networks. *J. Netw. Comput. Appl.* **2011**, *34*, 1908–1927. [CrossRef]
71. Yuan, C.; Chen, W.; Li, D. A Hierarchical Identity-Based Signcryption Scheme in Underwater Wireless Sensor Network. In *Proceedings of the China Conference on Wireless Sensor Networks*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 44–54.
72. Domingo, M.C. Securing Underwater Wireless Communication Networks. *IEEE Wirel. Commun.* **2011**, *18*, 22–28. [CrossRef]
73. Kasture, S.S.; Gudpelliwar, N. Securing Underwater Wireless Communication Networks-Literature. *Int. J. Sci. Eng. Res* **2013**, *4*, 73–78.
74. Liu, Y.; Jing, J.; Yang, J. Secure Underwater Acoustic Communication Based on a Robust Key Generation Scheme. In Proceedings of the 2008 9th International Conference on Signal Processing, Beijing, China, 8 December 2008; pp. 1838–1841.
75. Hu, F.; Wilson, S.; Xiao, Y. Correlation-Based Security in Time Synchronization of Sensor Networks. In Proceedings of the 2008 IEEE Wireless Communications and Networking Conference, Las Vegas, NV, USA, 31 March–3 April 2008; pp. 2525–2530.
76. Han, G.; Jiang, J.; Sun, N.; Shu, L. Secure Communication for Underwater Acoustic Sensor Networks. *IEEE Commun. Mag.* **2015**, *53*, 54–60. [CrossRef]
77. Ahmad, B.; Jian, W.; Enam, R.N.; Abbas, A. Classification of DoS Attacks in Smart Underwater Wireless Sensor Network. *Wirel. Pers. Commun.* **2021**, *116*, 1055–1069. [CrossRef]
78. Wood, A.D.; Stankovic, J.A. A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks. *Handb. Sens. Netw. Compact Wirel. Wired Sens. Syst.* **2004**, *739*, 763.
79. Buttyan, L.; Hubaux, J.-P. *Security and Cooperation in Wireless Networks: Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing*; Cambridge University Press: Cambridge, UK, 2007.
80. Akyildiz, I.F.; Pompili, D.; Melodia, T. Underwater Acoustic Sensor Networks: Research Challenges. *Ad Hoc Netw.* **2005**, *3*, 257–279. [CrossRef]
81. Shahapur, S.S.; Khanai, R. Localization, Routing and Its Security in UWSN—A Survey. In Proceedings of the 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, India, 3–5 March 2016; pp. 1001–1006.
82. Ullah, S.S.; Hussain, S.; Uddin, M.; Alroobaea, R.; Iqbal, J.; Baqasah, A.M.; Alsaqour, R. A Computationally Efficient Online/Offline Signature Scheme for Underwater Wireless Sensor Networks. *Sensors* **2022**, *22*, 5150. [CrossRef] [PubMed]
83. Zhao, Y.; Tian, B.; Chen, Z.; Liu, Y.; Ding, J. An Energy-Efficient Key Agreement Mechanism for Underwater Sensor Networks. In *IT Convergence and Security 2017*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 146–158.
84. Kalkan, K.; Levi, A. Key Distribution Scheme for Peer-to-Peer Communication in Mobile Underwater Wireless Sensor Networks. *Peer-Peer Netw. Appl.* **2014**, *7*, 698–709. [CrossRef]
85. Souza, E.; Wong, H.C.; Cunha, Í.; Cunha, Í.; 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; pp. 000299–000304.
86. Verma, S. A Cluster Based Key Management Scheme for Underwater Wireless Sensor Networks. *Int. J. Comput. Netw. Inf. Secur.* **2015**, *7*, 54. [CrossRef]

87. Peng, C.; Du, X.; Li, K.; Li, M. An Ultra-Lightweight Encryption Scheme in Underwater Acoustic Networks. *J. Sens.* **2016**, *2016*, 8763528. [CrossRef]
88. Kim, J.E.; Yun, N.Y.; Muminov, S.; Park, S.H.; Yi, O.Y. Security in Underwater Acoustic Sensor Network: Focus on Suitable Encryption Mechanisms. In Proceedings of the Asian Simulation Conference, Shanghai, China, 27–30 October 2012; Springer: Berlin/Heidelberg, Germany, 2012; pp. 160–168.
89. Goyal, S.B.; Ravi, R.V.; Verma, C.; Raboaca, M.S.; Enescu, F.M. A Lightweight Cryptographic Algorithm for Underwater Acoustic Networks. *Procedia Comput. Sci.* **2022**, *215*, 266–273. [CrossRef]
90. Wang, Z.; Du, J.; Xia, Z.; Jiang, C.; Fang, Z.; Ren, Y. Secure routing in underwater acoustic sensor networks based on AFSA-ACOA fusion algorithm. In Proceedings of the ICC 2022-IEEE International Conference on Communications, Seoul, Republic of Korea, 16–20 May 202; pp. 1409–1414.
91. Du, X.; Peng, C.; Li, K. A Secure Routing Scheme for Underwater Acoustic Networks. *Int. J. Distrib. Sens. Netw.* **2017**, *13*, 1550147717713643. [CrossRef]
92. Saeed, K.; Khalil, W.; Ahmed, S.; Ahmad, I.; Khattak, M.N.K. SEECR: Secure energy efficient and cooperative routing protocol for underwater wireless sensor networks. *IEEE Access* **2020**, *8*, 107419–107433. [CrossRef]
93. Dargahi, T.; Javadi, H.H.; Shafiei, H. Securing Underwater Sensor Networks against Routing Attacks. *Wirel. Pers. Commun.* **2017**, *96*, 2585–2602. [CrossRef]
94. Zhang, R.; Zhang, Y. Wormhole-Resilient Secure Neighbor Discovery in Underwater Acoustic Networks. In Proceedings of the 2010 Proceedings IEEE INFOCOM, San Diego, CA, USA, 14–19 March 2010; pp. 1–9.
95. Dini, G.; Duca, A.L. A Secure Communication Suite for Underwater Acoustic Sensor Networks. *Sensors* **2012**, *12*, 15133–15158. [CrossRef] [PubMed]
96. Das, A.P.; Thampi, S.M. Secure Communication in Mobile Underwater Wireless Sensor Networks. In Proceedings of the 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Kochi, India, 10–13 August 2015; pp. 2164–2173.
97. Zhang, R.; Zhang, J.; Wang, Q.; Zhang, H. DOIDS: An Intrusion Detection Scheme Based on DBSCAN for Opportunistic Routing in Underwater Wireless Sensor Networks. *Sensors* **2023**, *23*, 2096. [CrossRef] [PubMed]
98. 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]
99. Ateniese, G.; Capossele, 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.
100. Jiang, J.; Han, G.; Zhu, C.; Chan, S.; Rodrigues, J.J. A Trust Cloud Model for Underwater Wireless Sensor Networks. *IEEE Commun. Mag.* **2017**, *55*, 110–116. [CrossRef]
101. Ibragimov, M.; Lee, J.-H.; Kalyani, M.; Namgung, J.; 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]
102. Xu, M.; Liu, G.; Guan, J. Towards a Secure Medium Access Control Protocol for Cluster-Based Underwater Wireless Sensor Networks. *Int. J. Distrib. Sens. Netw.* **2015**, *11*, 325474. [CrossRef]
103. Jouhari, M.; Ibrahimi, K.; Tembine, H.; Ben-Othman, J. Underwater wireless sensor networks: A survey on enabling technologies, localization protocols, and internet of underwater things. *IEEE Access* **2019**, *7*, 96879–96899. [CrossRef]
104. Porkodi, K.; ZubairRahman, A.M. Enhanced Underwater Wireless Sensor Networks Security with Tic-Tac-Toe AI-MINIMAX Algorithm in Game Theory. *TAGA J. Graph. Technol.* **2018**, *14*, 216–224.