IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 12 September 2024, accepted 26 October 2024, date of publication 1 November 2024, date of current version 11 November 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3490498

SURVEY

Securing Underwater Wireless Sensor Networks: A Review of Attacks and Mitigation Techniques

KHAWAJA MASOOD AHMED[1], REHAN SHAMS[1], (Senior Member, IEEE), FOZIA HANIF KHAN[2], AND MIGUEL-ÁNGEL LUQUE-NIETO[3]

[1]Department of Telecommunication Engineering, Sir Syed University of Engineering and Technology, Karachi 75300, Pakistan
[2]Department of Mathematics, University of Karachi, Karachi 75300, Pakistan
[3]Institute of Oceanic Engineering Research, University of Malaga, 29010 Málaga, Spain

Corresponding author: Rehan Shams (r.shams@hotmail.com)

This work was supported in part by the Institute of Oceanic Engineering Research of the University of Malaga.

ABSTRACT In recent years industry's pursuit of Underwater Wireless Sensor Networks (UWSN) has surged because of UWSN's advancements in commercial and military applications as well as monitoring marine life. Owing to its capabilities, open acoustic channel, and hostile undersea environment, additionally, it is susceptible to many different types of malicious attacks and threats. Although secure interaction and communication is necessary for many UWSN-based applications, attackers can readily exploit vulnerabilities to steal data while the application is in use. However, most of UWSN research to date has not taken security into account. Due to these factors, the objective of this research is to present a thorough review of UWSN security by going over security requirements as well as the primary UWSN security threats according to layered classification. This paper discusses different security concerns and examines countermeasure schemes against UWSN security attacks and strategies created specifically for UWSNs that discuss several security issues. The aim of this study is to discuss various security concerns and examines countermeasure schemes against UWSN security attacks and strategies created specifically for UWSNs that discuss several security issues. The goal of this study is to recommend future lines of inquiry for UWSN research. The proposed study discusses different strategies that had already addressed the security issues. However, how these schemes are still lacking in the performance and what countermeasures can be considered by different techniques such as confidentiality, integrity, authenticity and many more, in order to fulfill the security issues in under water sensors networks. The goal of this study is to recommend future lines of inquiry for UWSN research. Comparisons of different techniques in terms of energy efficiency, latency, and detection accuracy with other major factors have also been done as a guideline for new research.

INDEX TERMS Underwater wireless sensor networks (UWSNs), security attacks, attack mitigation, security mechanism.

I. INTRODUCTION

Wireless communication and Information security are correlated. Data obtained from any unprotected wireless network, whether it be under the sea or terrestrial, is useless in modern applications. The field of UWSN has seen significant research activity over the past 30 years, ranging from advancements in MAC and routing protocols. The cutting-edge areas that appear to be least concentrated are hybrid network architectures, underwater information security, and alternatives to acoustic underwater communication media. Security for underwater networks is one of these three extremely sensitive domains [18]. One possible explanation for why information security has always been assigned the lowest priority by researchers is the difficulties associated with underwater communication mediums, which will be covered in section II.

The increased adoption of underwater wireless sensor networks (UWSN) for surveillance, catastrophe monitoring, and oil and gas operations by government agencies underscores the importance of giving information security of these networks a similar emphasis. The development of Protocol stack

The associate editor coordinating the review of this manuscript and approving it for publication was Peter Langendoerfer.

standardization, localization mechanism, sensors' time synchronization, routing strategy design, hardware, and other related aspects, have all contributed to the momentum of this trend. As a matter of fact, information security cannot be replaced using sophisticated networking solutions; rather, to create a complete networking solution, security algorithms and protocols must be implemented [100].

As illustrated in Figure 2. The primary purpose of underwater sensors is to send sensed data to the surface gateway for additional processing and interpretation. while simultaneously gathering real-time data from a specified tracking range. Typically, these networks are positioned in isolated areas and are not monitored. To safeguard them from dangers like black holes, Sybil attacks, denial of service (DoS), eavesdropping, tampering, and other threats, security mechanisms must be installed on them [101]. However, as mentioned in [8] sensor nodes in UWSNs are appropriate for tiny message transmission because of their limitations concerning processing power, storage, and battery life, whereas transmission without encryption or authentication is unsafe [91]. The identification of several attacks on UWSN security, including as wormholes, jamming, sinkholes, spoofing, eavesdropping, and so forth, has been the focus of current research. These attacks are primarily motivated by two factors: (i) the various underwater applications create enormous amounts of confidential information, and (ii) As discussed in [18], Because UWSN has recently become more standardized, attackers now have an easier time creating models or attack plans for underwater networks.

Popular security techniques in UWSNs mostly rely on encryption, namely symmetric/secret key and asymmetric/ public key schemes, to maintain security against the attacks outlined above as well as to safeguard confidentiality, integrity, and enable authentication. But because of the padding and extra data that must be added for encryption, they result in ciphertext growth. However, higher layer encryption techniques suffer from significant computational complexity, particularly in UWSNs with severe resource constraints [92], [93], [94]. Especially when it comes to public-key cryptosystems like the Rivest-Shamir-Adleman scheme (RSA), which are frequently utilized for authentication and digital signature, they are nearly useless in UWANs, [95], [96].

Besides many challenges, Blockchain based network can also be seen as one of the most prominent solutions for underwater communication [114]. It is a distribute and decentralized technology that can able to provide differential integral features for the underwater applications which mainly includes management of sharing trusted data, tracking and monitoring of several of resources, secure routing mechanism and traceability. By using the block chain technology under water communication could be more secure without the intervention of any third party [115]. Blockchain is also beneficial in decision making required due to unreliable connection with the outside base station. Due to the smart contract, it gives the autonomous decision making.

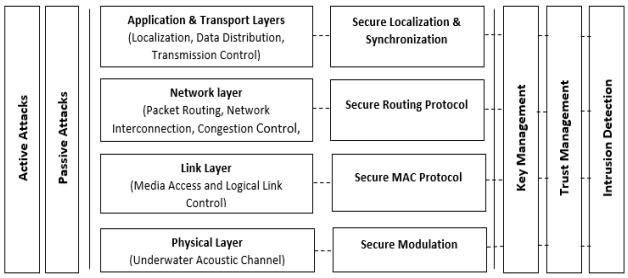


FIGURE 1. Security architecture of UWSNs.

As compared to other centralized record keeping technologies. Blockchain can built the trust along with the transparency and gives transmission without failure. It structure consist of six levels namely: network, data, consensus, contract, incentive, and application layers.

The primary unit of Blockchain perform the transaction which has been done by structured in the block. Each block generates the cryptographic hash to verify the immediate precedent block, this hash is able to generate the sequential link between all the blocks in the blockchain structure. This mechanism assuring the data integrity irreversibility.

As a result, before UWSN deployment, it is necessary to give security techniques special attention. With the exception of elliptic-curve encryption, the majority of TWSN information security techniques cannot be applied straight to UWSN [1]. A creative approach or rethinking of the security techniques employed for TWSN is necessary to design a security scheme to deliver an all-encompassing approach for UWSN. In accordance with open system interconnection (OSI) layer model the security issues pertaining to the UWSNs are rationally divided into distinct layers. The physical layer, link layer, network layer, and application & transport layer are the four layers that constitute the security architecture of UWSNs, as depicted in Figure 1. In this paper, layered-wise attacks will be discussed in detail, and will review numerous security issues in UWSNs.

Numerous research findings have been published to address the unique characteristics of UWSNs for information security; numerous reviews are included in this study, including [3], [9], [10] [97], [98], [99] [100], [102], [103]. Reference [3] reviews five solutions that have been developed to prevent potential attacks on UWANs. In [98], several aspects of underwater acoustic communication security are briefly discussed, along with potential layer-by-layer attacks and three countermeasure strategies against jamming and wormhole attacks.

In [97], another survey is carried out wherein ten countermeasure strategies are reviewed without any discussion of encryption algorithms. Reference [99] examines 21 methods of countermeasure strategies. A more comprehensive analysis, reviewed in [90], examines 35 suggestions that concentrate on potential attacks and defenses of the lowest three levels; no discussion is found of the high tiers' mechanisms, such as transport and application. This research objective is to

present a detailed survey of the layered wise attacks and the most recent defense mechanism for UWSN security. It will accomplish this by reviewing over 40 mechanisms, many of which have not been covered in the surveys listed above. The study focuses on typical security threats in UWSNs from all tiers, as shown in Figure. 1, and countermeasure techniques against them as well as schemes to identify and mitigate security attacks specifically targeted at UWANs.

Main Contributions:

The proposed study's contributions are as follows,

- An overview of the background and the state of art concept related to the security and underwater communication are discussed.
- A study of different challenges in the current underwater communication system and corresponding security techniques is analyzed.
- Efficient utilization of cryptographic concept in the design of underwater sensor networks is studied.
- To investigate and propose an appropriate platform for the implementation of underwater sensors networks applications.
- Highlight open research challenges of UWSNs as a guideline for future research to drive innovative development in various fields.
- Comparative analysis of various studies and algorithms/techniques related to the secure communication in underwater acoustic is performed to analyze the research gap, challenges and future directions.
- A discussion of different types of attacks related to underwater acoustic networks and how these attacks can be countermeasures.

This is the first comprehensive review on UWSN security as far as the author's understanding. It can give professionals the state of the art in this sector and learners an overview of UWAN security solutions. The following is the order of the remaining sections of the paper:

In Section II, the unique characteristics and environments of UWSNs are presented. The Security requirements and concerns in UWSNs are addressed in Section III. The security attacks and countermeasures are explained in Section IV. The security mechanisms to identify and mitigate security attacks are covered in Section V. Section VI covers the Discussion. Section VII highlights the Future gaps and challenges. The paper is finally concluded in Section 8.

II. UNDERWATER ACOUSTIC CHANNELS CHARACTERISTICS

Underwater acoustic channels have the following characteristics.

A. UNDERWATER COMMUNICATION CHANNEL

WSNs don't usually interact with acoustic signals for communication; UWSN nodes do [104]. Compared to WSNs, this leads to a smaller bandwidth, an increased bit error rate, and a slower propagation speed [36]. The amount of useful acoustic bandwidth is far lower than the amount of useful RF bandwidth [105]. Furthermore, an attacker can easily capture or prevent messages sent across this channel due to its open nature [65].

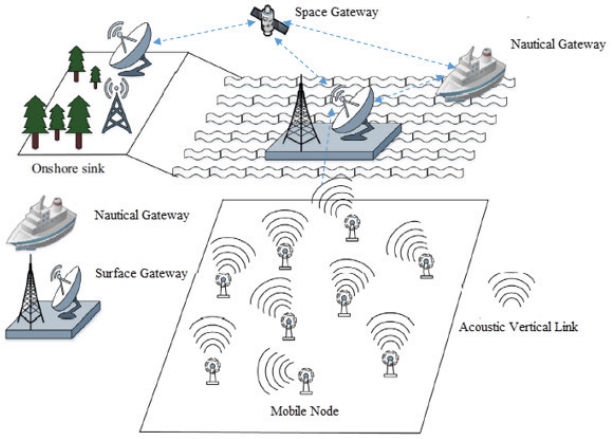


FIGURE 2. A scenario of UWSNs connected with other networks.

B. OPERATING ENVIRONMENT

The network topology is dynamic due to the movable nature of the sensor nodes caused by ocean currents [48]. The accuracy of data transmission and data routing may be impacted by changes in network topology [104]. Node mobility emphasizes the need for precise and secure localization as well as time synchronization. In addition, compared to their terrestrial equivalents, UWSNs are sparsely populated means have lower density, which results in longer distances between nodes.

C. ENERGY AND HARDWARE

Energy, computational power, and storage capacity are all constrained on UWSN nodes. Moreover, UWSNs use more power because of their longer range and intricate signal processing that takes signal attenuation into consideration [104]. Although WSNs can be easily charged with solar energy, when deployed UWSNs are submerged, making maintenance and recharge more difficult [104]. This further tightens energy restrictions, which affects security by limiting the kinds of security measures that can be used.

The aforementioned explanation and Table 1's list of UWSN features imply that it is challenging to implement security algorithms for data communication that occurs underwater. ''Enhancing the security efficacy of the underwater network by conserving the underwater nodes resources'' is the most challenging task, in our opinion. Presumably, if more algorithms need to be executed for security, this will increase node power consumption. This presents a challenge in the process of designing a secure data communication link. In UWSN communication, cryptographic algorithms have to remain efficient in terms of message length and quantity. As a result, several adjustments must be made when using conventional methods in an underwater environment, such as ciphers and digital signatures.

TABLE 1. Characteristics comparison between communication mediums of UWSN.

S.No.	Characteristics	Radio Waves	Acoustic Waves
1.	Attenuation	Maximum, since attenuation rises with frequency (3.5–5 dB/m)	Moderate; attenuation varies with distance (0.1–4 dB/km).
2.	Bandwidth	Low	Moderate because it depends on the distance. a few kHz
3.	Data rate	Moderate in Mbps	Low in Kbps
4.	Latency	Moderate	High
5.	Speed of Propagation	3 x 10^8 m/s	1500 m/s
6.	Dispersing Phenomena	Absent	Absent
7.	Cost	High	High
8.	Energy Usage	High	High
9.	Doppler Effect	Insignificant	Significant
10.	Type of Water	Ideally in shallow water	Primarily in deep water

III. SECURITY IN UWSN

Because UWSN communication occurs underwater, there is a chance that an adversary could jeopardize UWSN security. The sensor nodes are susceptible to several types of security breaches in UWSNs. Hence, the first consideration in the design of any UWSN mechanism should be security. UWSNs use acoustic channels for communication, which have a high latency and a low bandwidth. The energy usage in underwater acoustic communication is higher than in RF waves in WSNs because of the characteristics of acoustic channels used in UWSNs. As such, consumption of energy is necessary to consider while developing security methods for UWSNs [2], [3], [4].

A. SECURITY REQUIREMENTS OF UWSNS

The following are the general objectives that security ought to accomplish: i) guarantee the confidentiality and integrity of the sensed data transferred across the network; ii) ensure that the sensed data is delivered to the intended locations; iii) Secure the network-connected systems against attacks; and iv) Potential attack sources must be identified. In order to do this, the following security features are typically put into practice, assuming that the network infrastructure is stable enough to support regular network activities [2], [3], [5].

1) CONFIDENTIALITY

Confidentiality means information is kept secret so that individuals with malicious intentions cannot access it. This has to deal with preventing illegitimate nodes from accessing sensitive data, such as identities and keys. The resilience of the user's information (such as tactical or strategic military information) and the resilience of the MAC, routing data, etc. are all included in the definition of confidentiality. A malicious attacker must not be able to access or alter this confidential information. Implementing a low-power-efficient encryption approach that works well with UWSNs can help achieve confidentiality. Typically, UWSNs use a lightweight encryption method called cipher text theft [6].

2) AUTHENTICATION

Authentication refers to transferring data to a recipient or destination and ensuring its secure authentication. Since each user maintains a unique authentication, the attacker can easily access the sender's message or the recipient's data, and the source of the data can be rapidly identified within the network. Because of this, this kind of authentication is employed across numerous industries, especially in UWSN applications pertaining to military data transmission and safety and security [7].

3) INTEGRITY

Various UWSNs applications, such as aquatic ecosystem monitoring and monitoring of water quality, demand extremely reliable data, it indicates that any adversary would not be able to readily breach the system. Integrity is essential in the aforementioned applications because it safeguards sensitive information from being modified by outside parties. To ensure the data integrity of received underwater data, for instance, a message integrity check can be performed. Additionally, in the UWSN context, software and log integrity are examples of auto-integrity-checking methods that can be employed to confirm the device software and logs integrity, respectively [8].

4) AVAILABILITY

Availability serves as a guarantee that the network is sufficiently strong. The system will be able to continue operating even in the event that certain nodes malfunction or are attacked. UWSNs can be made available by self-healing, auto recovery, and appropriate redundancy techniques [8].

5) FRESHNESS

Freshness checks are performed to ensure that the data being received is actually new and not just legacy data being retransmitted. Real-time routing updates ought to be provided. A significant amount of actual information could be lost as a result of the update messages' delay, which could indicate an incorrect network state [9], [10].

6) PRIVACY

Regarding UWSNs, privacy pertains to the data or service that a specific user or device is able to access. To shield the data from hackers, a strong privacy strategy must be implemented for UWSN. The following categories list the many privacy strategies that should be taken into account in UWSNs [9], [10]:

- **UWSN data privacy**

Data privacy is required in UWSN naval applications to prevent adversaries, such as enemy submarine attacks

and covert message passing from accessing confidential communications.

- **UWSN device privacy**

Device/node identification is typically used in UWSNs to monitor and send data to endpoint nodes. Since a node's identity can be traced, information theft by attackers is made easier. To secure the node's identity from hostile nodes in this situation, a strong identity protection strategy is required.

- **UWSN location privacy**

In UWSNs, the node's location information is required to monitor UWSN node mobility. For data to be transmitted among the nodes, the node's location data must be available. Furthermore, it is difficult to hide a node's position based on necessity. Therefore, a privacy-based location-sharing method must be ported to UWSN devices.

7) ISOLATION

The purpose of isolation is to make sure nodes can recognize unusual activity and separate out hostile nodes. Additionally, MAC and data routing protocols ought to be safe from hostile attacks. Malicious nodes can be isolated using lightweight cryptography techniques and appropriate trust management [9], [10].

8) SELF-STABILIZATION

The goal of self-stabilization is to guarantee that nodes can recover from attacks on their own, autonomously in real time without the need for outside help. A node that is capable of self-stabilizing against malicious attacks can return to its normal condition on its own, even in the event that the attacker remains within the network [9], [10].

9) SURVIVABILITY

This refers to the system's ability to promptly complete its task even in the event of a fault, malfunction, hack, or hostile attack. Its purpose is to guarantee that, even in the event of a partial network destruction, the network can continue to provide and restore critical services both during and after hostile attacks [9], [10].

10) AUDITABILITY

To deliver high-quality services in UWSNs, security procedures, operations, and performance analysis are required. One possible approach to evaluate the security systems in the UWSN is to use an auto-auditing or self-auditing model [9], [10].

B. SECURITY CONCERNS

Mechanisms for detecting and mitigating attacks in UWSNs should be proposed using a variety of security techniques and technologies to fulfill the requirements of security outlined above. Routing security, intrusion detection, key management, trust management, secure localization, and time synchronization are the primary security concerns, as shown in Figure. 1.

1) ROUTING SECURITY

Basic transit and connection security techniques applied to individual routing protocols and sensors comprise routing security. Furthermore, nodes must use any of the routing protocols and transmit neighbor data to build the network architecture. Secure data transfer and secure routing are two components of routing security. Secure routing needs nodes must work together to exchange precise information of routing and maintain network connectivity. Secure transmission of data should protect information communications from being manipulated, dropped, or altered by unauthorized person.

2) LOCALIZATION SECURITY

Location approximation is essential for origin identification and monitoring applications. Underwater sensors gather location and velocity data from moving nodes even in the process of localization, which is employed to choose the most efficient intermediary node for data transmission. The lack of position data prevents the base station from identifying the source of the received signal. The unique features of underwater channels make it impossible to implement suggested WSN localization approaches to underwater operations [37].

3) SYNCHRONIZATION SECURITY

MAC protocol sequencing and several other underwater operations require synchronization. Furthermore, achieving accurate time synchronization in underwater scenarios is highly challenging. While security is crucial in underwater applications, still it is not considered in any of the existing time synchronization algorithms [108], [109].

4) KEY MANAGEMENT

The fundamental objective of key management and encryption are data secrecy, data integrity, validity and authenticity. Thanks to encryption, unauthorized individuals cannot view or alter sensitive data or transmit it over insecure underwater channels. Nevertheless, there are certain issues with the encryption and key management systems in use today, like extensive computation and ciphertext enlargement. Data padding and codes extend the text after encryption is applied and increase energy consumption during processing and transfer [106]. Usually, a digital signature is employed to verify messages. The addition of a signed, validated message causes message expansion and connection latency [107].

5) INTRUSION DETECTION

To detect, recognize, and isolate intruders both inside and outside of the network, intrusion detection techniques are employed. On the other side, most intrusion detection systems operate only after malicious attacks have occurred and been identified. It can be difficult to spot suspicious intruders early on in an attack. Authentic detecting methods need to be improved and researched as a result. Conversely, systems can be protected while letting malicious intruders to exist by using

intrusion tolerance techniques. To further enhance UWSN privacy, techniques, and systems for intrusion detection have previously been proposed.

6) TRUST MANAGEMENT

One important aspect of encryption security that offers significant advantages in intrusion detection is the trust management technique. Because of UWSNs' distinct features and limitations, developing trust management techniques in UWSNs has more challenges [43]. Now a days, three flavors of trust management systems exist: distributed, centralized, and hierarchical. In a centralized system, a base station or root node provides trust management to all nodes in the channel. Centralized systems don't work for UWSNs. Trust value transfers between base station and ordinary nodes demand plenty of energy since it is an expensive constraint. In a distributed system, every ordinary node is liable for establishing and preserving the trust level of channel. In hierarchical systems, the evaluation and transmission of trust levels are carried out sequentially. The lowest layer's trust levels are transferred up to the highest layer and merged.

IV. SECURITY ATTACKS IN UWSN

Underwater data transmission has drawn plenty of research interest, which has resulted in the creation of numerous applications. Of these, 90% are used for national security, oceanographic research, and industrial purposes. The significance of transmitting data underwater has grown due to these developments in the underwater realm, making data security risks and threats increasingly pressing concerns. The deliberate destruction of underwater networks via various attack techniques is a threat that has alarmed the scientific community as well as many developers of underwater applications. Thus, in order to safeguard against future attacks on underwater networks, it is crucial to investigate various security risks. Every kind of attack within every layer of the UWSN is depicted in Figure 3. The terms used to describe attacks on UWSNs are nearly identical to those used for terrestrial sensor networks. But there's a big difference in the way the attack is carried out and the approach taken. Unidentified threats and their related attacks may still exist, making UWSN vulnerable. Therefore, some preventive steps to make UWSN resistant to security threats include developing advanced-level security algorithms to ensure secrecy, integrity, authentication, increased secure key generation, secured routing, and synchronization. In this paper, these attacks and defenses were thoroughly examined and researched. These attacks are primarily divided into four categories based on the behaviors of the malicious attacker: host-based, Protocol Stack, attacker capabilities, and information in transit.

A. CHALLENGES TO ATTACKERS

Certain characteristics of UWSNs present difficulties for attackers and can be partially utilized in the development of security mechanisms. These characteristics which are listed

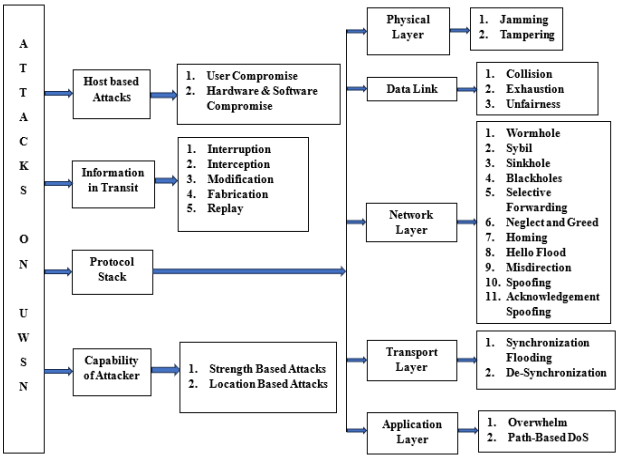


FIGURE 3. Classification of UWSN attacks.

below consist of the distribution of spare nodes, low network node heterogeneity, and a well-planned deployment of network with already configured security features [11], [12], [13].

(i) Determining the size and distribution of a UWSN in a sparse UWSN without prior knowledge is difficult, it can be challenging to identify a specific node to attack.

(ii) It is difficult to covertly deploy a massively sized, energy-hungry disrupting device in the operational region of a UWSN that is being attacked. Because underwater acoustic communication is wideband, techniques like channel jamming are rendered less successful if the attacker is unaware of the frequency that UWSNs are using. If the bandwidth of a communication system is lower than 1% of the signal's center frequency, it is classified as narrowband., wideband if it is between 1% and 20% of the center frequency of the signal, and ultra-wideband (UWB) if it is greater than that [14].

(iii) An attacker needs to put in a significant amount of time deciphering the secret information due to the low-rate acoustic channel as explained in [17]. The relatively narrow acoustic channel contributes to the inefficiency of some attacks, including denial of service (DoS) and attacks via repetitive trials. Similarly, distributed DoS (DDoS) attacks are challenging due to sparse node distributions, on the other hand, When DoS attacks are launched above the physical layer, a channel with a rate substantially lower than a node's computation capacity serves as a bottleneck.

To reduce cost, applications' security requirements should be considered, and the aforementioned features should be taken advantage of by the UWSN security mechanism.

B. ATTACK MODELLING

Threat and attack are two distinct ideas, they must be discussed individually. To put it simply, an attack is a fact that happens as a realized threat, whereas a threat is merely the

TABLE 2. Layered-based analysis of malicious threats & attacks.

Malicious Threats	Attacks	Description	Layer
Network unavailable (Resource Depletion)	Denial of Service (DoS), Host-based & Exhaustion	Intentional disruption of nodes and communication.	Transport layer
Loss of reliability during data transmission	Sinkhole, Wormhole, Blackhole & Spoofing	Processing of false or unauthentic data input by legitimate node.	Network layer
Larger delays during data transmission	The adversary transmits messages with false path data. Sybil, Wormhole & Misdirection	No verification of identification. Longer time required for intruder detection.	Network layer
Network integrity violation	Spoofing-based DoS	Creation of incorrect routing information.	Network layer
Compromised neighbor discovery phase	Blackhole	No verification of identification.	Datalink layer
Increased energy consumption i.e. shorter battery life	Power depletion, Flooding & Overwhelm	Deliberate depletion of nodes' energy.	Datalink layer
Data packet alteration	Data tampering	Violation of confidentiality.	Physical layer
Cluster head hacking	Homing & Jamming	Sabotage the whole cluster of nodes and freshness of data, causes more harm.	Physical layer Network layer
Tampering	Node capturing physically	Alteration to the node's internal memory. No data auditing is done.	Physical layer

chance of something horrible happening. Attacks are now conducted when there is anything to gain or damage or obvious reasons. With UWSN, an attacker can obtain confidential digital data sent over underwater networks and harm adversarial nations' national security. In Figure 3, the attacks are categorized into many groups. Consequently, to lower the risk, it is vital to come up with advanced security mechanisms that are better understood and based on the layered study of different underwater threats and attacks, as Table 2 illustrates.

1) HOST-BASED ATTACKS

A host-based attack is one that targets a single system, or host or node. The three main parts of every machine are the hardware, software, and user [53]. Thus, host-based attacks are further classified into three types based on these components, which are listed below,

(a) User/Operator Compromise: The user of UWSN, an offshore facility located on the ground, gets compromised by this type of attack. Critical network data, including passwords and sensor node keys, are disclosed by tricking users.

(b) Hardware Compromise: The sensor node's hardware is the target of this attack. The goal of the attack is to break into the sensor node's hardware to obtain data, program code, and keys.

(c) Software Compromise: The attack causes the sensor nodes' operating software to malfunction. Software threats include buffer overflow as one of their examples.

A network-based attack is one that is carried out by devices on the network with the goal of using it [53]. Network-based attacks primarily cause the network protocol to deviate from how it is designed to function.

2) INFORMATION IN TRANSIT ATTACK

Transmission of information is the primary goal for network development in UWSN. Attackers are drawn to wirelessly transmitted data packets because they frequently contain confidential data related to underwater applications. Therefore, it's imperative to research the different attacks carried out throughout the data in the transit phase. There are primarily five types of attacks that can be detected whenever the data is in the transmission phase, as Figure. 3 illustrates.

(a) Interruption: The attack aims to transmit bogus information with the objective of disrupting the communication channel. The primary goal of an interruption attack is to render network services unavailable [18].

(b) Interception: Targeting network nodes and, indirectly, data stored in memory chips, the attacker eavesdrops on the sensor node in order to obtain unauthorized access. The purpose of this application layer attack is to compromise data confidentiality while it is in transit [18].

(c) Modification: As the term implies, intercepting data packets during their transmission phase and subsequently modifying their content in order to deceive legitimate nodes and jeopardize data integrity [18].

(d) Fabrication: During the transmission phase, the attacker inserts a stream of bogus data in an attempt to lose data authentication [18].

(e) Replay: Replay attack is the forced repetition of outdated data packets in an attempt to deplete a node's battery and decrease the freshness of the message [18], [19].

3) ATTACKS ON PROTOCOL STACK

The different attacks made at different tiers of the UWSN protocol stack are mentioned in Figure 3. Any attack on a layer compromises the protocol stack's perfect operation, hence layer-by-layer attacks must be addressed in order to develop appropriate security mechanisms.

a: ATTACKS ON THE PHYSICAL LAYER

Well-known attacks on the physical layer include jamming and tampering.

(i) Jamming

To occupy the communication channel and sabotage the authentic real time communications, an undesired signal is injected into the channel during a jamming attack [20], [21], [22], [23]. Networks are particularly vulnerable to jamming attacks since they don't require specialized hardware, can be carried out at low cost, and can be made more intelligent by interfering with open communication channels [20].

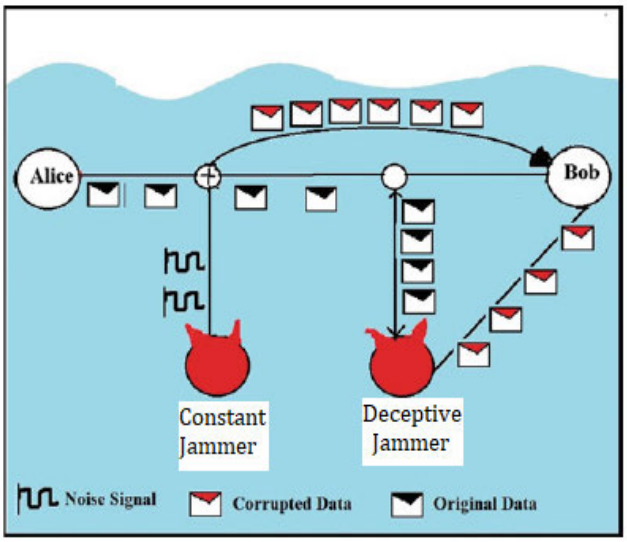


FIGURE 4. Overview of jamming attack.

Jamming can shorten the network's lifespan by draining the batteries in sensor nodes, in addition to disrupting communications [22]. Jamming is a kind of denial-of-service (DoS) attack and falls into four categories:

- Constant jamming: Similar to Figure. 4, the jammer continuously feeds noise into the channel in an attempt to corrupt packets or congest the network [20].
- Deceptive jamming: As illustrated in fig.4, the jammer uses legitimate packets rather than noise to disrupt the network because it is aware of some of the protocols. [20], [23].
- Random jamming: At random intervals, the jammer alternates between sleeping and injecting packets [20].
- Reactive jamming: Reactive jamming involves listening to communications, staying still until it detects activity, and then sending out jamming signals [20], [23].

To detect jamming, Bagali et al. offered a unique cross-layer method and an effective channel assignment method for collaborative communication. A learning-based power control method to counter jamming assaults is provided by Xiao et al. [22] in situations where the attacker's channel characteristics are unknown. Furthermore, they apply a jamming game-theoretic investigation to UWSN. Two jamming games are used to model the communications between a reactive jammer and a UWSN. Misra et al. [23] offer a jamming detection system in which nodes strategically exchange acknowledgment and discovery packets.

(ii) Tampering

In a tampering attack [24], Before getting complete control of the compromised node, the attacker modifies or destroys the capabilities of the sensor node. To obtain unauthorized access to confidential underwater transfers of data, he can also decode sensitive data, including encryption keys. This attack alters the hardware, leading to a loss of functionality and altered internal memory. Through the use of appropriate key management techniques, hiding nodes, and frequent encryption key changes, the attack is thwarted.

b: ATTACKS ON DATA LINK LAYER

In data link layer, multiple access control (MAC) techniques are employed to ensure fair and efficient channel sharing among various devices because of limited bandwidth of the underwater wireless channel. However, the primary goals of attackers at the MAC layer are regrettably connected to communication channels, such as lengthening channel access times, lengthening propagation delays, deteriorating channel quality, and so forth. A significant danger that deliberately damages UWSN systems is the denial-of-sleep attack, which shortens the lifetime of the network.

(i) Collision Attack

Strong multipath effects are the primary cause of collision attacks in UWSN. The complex underwater landscape, where the UWSN architecture varies quickly, and the potential of acoustic waves to propagate through two or more paths are the reasons for multipath. The increased error rate and decreased communication quality are indirectly caused by the collision attack. With less chance of detection and less transmission energy used than jamming, this technique is more beneficial for the attacker [25]. A collision attack can be protected by reducing a colluding collision strategy. When colluding in an attack causes packets to be interrupted during transmission [26]. Collisions can be avoided in a practical way by using an error-correcting code.

(ii) Battery-oriented/Exhaustion Attack

Through the introduction of a rogue node into the network, this type of attack draws attention to the data communication link and uses up node energy. It can start from the attacker's own program code on a compromised node or from the attacker directly. Another kind of fatigue attack is when a compromised node sends join requests or RTS/CTS notifications to force the recipient node to send and receive. To prevent distributed node depletion assaults, the author in [27] describes a fuzzy logic-based technique. A sensible method would be to impose rate limits on each network node and suggest an anti-distributed-node-exhaustion method based on fuzzy logic.

(iii) Unfairness

This kind of denial-of-service attack is weaker because it does not entirely stop the authorized sensor nodes from connecting the communication link, the attacker just lowers the network's performance. To cut down on time, a minor frames approach is applied. It is susceptible to additional disparity. Instead of just pausing at random, an attacker might, for instance, transmit at a quicker rate [28]. By restricting the speed of transmission, dividing packets into brief frames, and using error detection code, the majority of above-mentioned denial of service (DoS) attacks on the data link layer are preventable. One way to reduce the time needed is to use the small frames method. The effectiveness is sacrificed in

favor of a lesser impact when employing this method. It is also available for exploitation in the future. An attacker could retransmit at a faster rate rather than waiting aimlessly. Most of the above-discussed denial of service (DoS) attacks on the datalink layer can be countered by packet slicing, error detection codes, and rate limiters.

(iv) Denial of Sleep

In the event of a denial of sleep attack, battery-operated devices will run short of energy [29]. Two techniques are available to carry out the attack: the first is the use of collision threats; the second is the repeated handshaking exchange of the clear-to-send (CTS) and request-to-send (RTS) flow control messages. The node is kept from entering a sleep state by doing this.

c: ATTACKS ON NETWORK LAYER

Data packets are routed via numerous intermediary nodes to their destination, which is the primary function of the network layer. Additional services offered by the layer include packet switching, flow control, packet sequence control, connection service, and more. As a result, attackers are focusing to target network layer services, which are the backbone of the whole network. As Figure 3 illustrates, there are several attacks at the network layer.

(i) Wormhole Attack

As depicted in Figure 5, between two or more malicious nodes, The attacker constructs an alluring tunnel or wormhole link with low latency and high bandwidth [30]. The attacker then uses this wormhole link to launch devastating attacks such as total interruption of routing [31], localization, and synchronization services [32]. In addition, the link is utilized to initiate man-in-the-middle and DoS attacks, as well as to selectively drop and modify packets. This is categorized as routing and localization attacks. Azimuth measuring technology is the basis for Junqing et al.'s proposed wormhole attack detection technique in the Underwater Acoustic Communication Network, which is examined in [112]. Azimuth makes the determination that a wormhole attack exists.

(ii) Blackhole Attack

A malicious node discards packets and tries to masquerade as a destination node to prevent them from reaching their destination, as depicted in Figure 6, or may attempt to forge route reply packets delivered to the source node [33], [34], [35]. Blackhole is a kind of denial-of-service (DoS) attack. A method to counteract blackhole attacks is presented by Zala et al. in [111]. It involves grouping nodes into clusters and choosing coordinator nodes from each cluster to determine whether any blackholes are present in that cluster. To authenticate and validate nodes, we employed the challenge-response technique along with public-key cryptography.

(iii) Sinkhole Attack

To trick other nodes into using a malicious node more frequently, it poses as the best route to the base station [36], [37]. A high-performance external device or a compromised

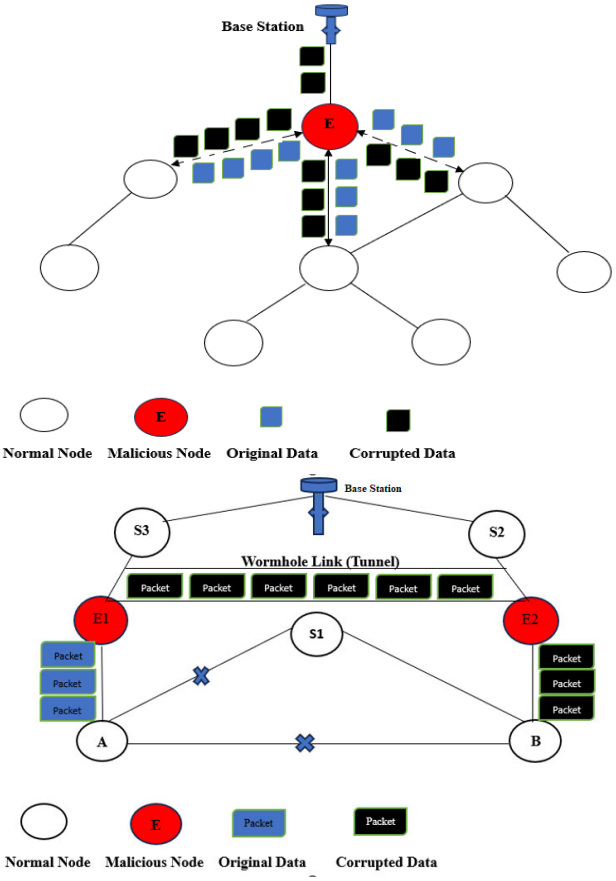


FIGURE 5. Scenario of wormhole attack.

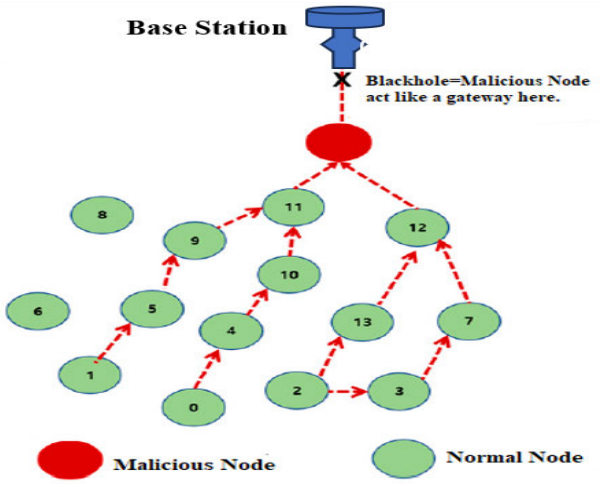


FIGURE 6. Scenario of blackhole attack.

insider node can be used to carry out a sinkhole attack [36]. The goal of the sinkhole assault, as illustrated in Fig. 7, is to stop the buoy at the water's surface from getting the full and accurate sensed data from underwater sensor nodes. We classify this as a routing attack. To counter such assaults in UWSN, reputation-based and multi-level trust techniques have been developed. Two methods to counteract sinkhole attacks are to authenticate nodes that exchange

routing messages or to route data packets from sensor nodes to multiple buoys positioned at the sea's surface.

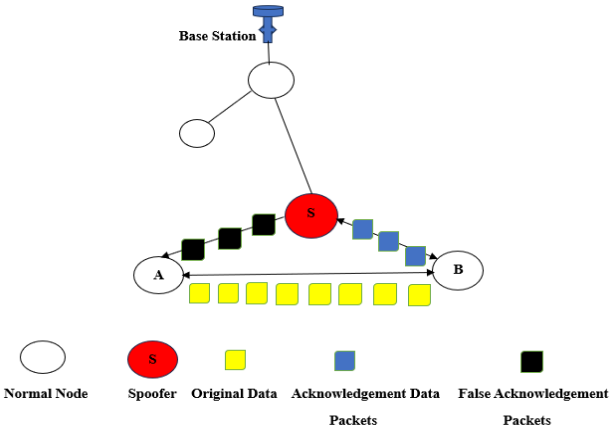


FIGURE 7. Scenario of sinkhole attack.

(iv) Sybil Attack

The strategy behind the Sybil attack is that an attacker creates a single malicious node and it pretends to be in numerous places at once with different identities [37], [38]. This generates a fictitious situation of multiple relay nodes and deceives routing protocols [3], [37]. These identities are either freshly established by the attacker or are a spoof of an authentic node. We classify this as a routing attack. Fig. 8 illustrates that the malfunctioning node, or Sybil node, E1, has several false identities. It is also evident that the sybil node serves as the intermediary in all communication routes among nodes A and B. Node A waits for the response after sending query packets throughout her transmission region. Node E1 may be designated as a Sybil node if it is not noted in Node A's list of neighbors as responding to her. However, there may also be a contradictory scenario in which a node with authorization asserts that S3 does not respond to node A because it runs out of battery life and becomes a dead node. Therefore, we are unable to remove S3 from the Sybil node and designate them as a sybil node.

To stop the sybil attack in the UWSN system, appropriate localization and message authentication techniques are required. Arifeen et al. [110] presented an approach for the detection for blockchain-based sybil attack in UWSN in 2021. To strengthen it against the detection of attacks, they have also combined a trust model with a blockchain-based technique.

(v) Selective Forwarding Attack

The rogue node in these attacks is situated close to the UWSN network gateway. When certain packets are identified, the legitimate nodes will choose a different route to relay the data to the gateway. In this attack, the rogue node has the ability to drop some packets before they reach the target, as seen in Figure 9. In UWSN networks, it really results in packet loss [9]. In [42], node capture efforts utilizing the Dempster–Shafer theory of integrated multiple

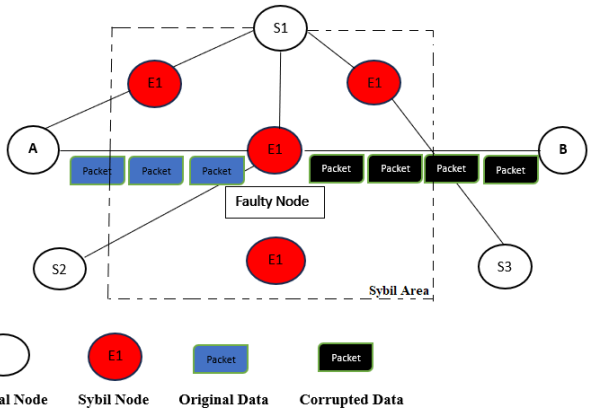


FIGURE 8. Overview of sybil attack.

facts are identified through empirical research. Such attacks are detectable and can be eliminated from the network by employing reputation methods and trust management techniques that rely on behavior evaluation [43]. Figure 9 illustrates the overview of selective forwarding attack.

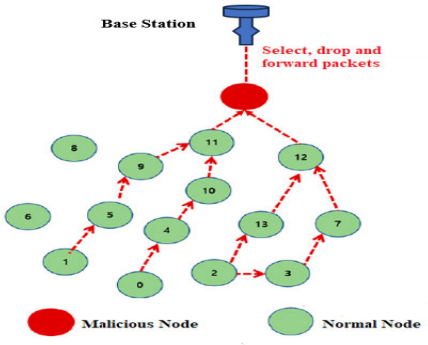


FIGURE 9. Overview of selective forwarding attack.

(vi) Neglect and Greed Attack

A variant of the selective forwarding threat where the attacker can arbitrarily discard incoming packets while offering high priority or acknowledgment to data packets coming from the source node [39], [40]. A practical countermeasure against this type of attack is to send messages repeatedly announcing different routing pathways, but this would require more power during the conversation, putting UWSNs at the highest risk of energy shortages.

(vii) Homing Attack

To identify and target nodes doing certain functions, such cluster heads or sinkholes, a potential hacker may observe network traffic in a homing attack. In addition, the hacker might carry out more denial-of-service attacks in order to disable or block these particular nodes. An anti-traffic analysis technique that uses "dummy packets" helps conceal the base station's location from observers [44]. Unfortunately, these dummy packets consume a significant amount of node energy, especially for UWSNs. It should therefore only be applied when it is essential to prevent traffic analysis.

(viii) Hello Flood Attack

An attacker can launch a "hello flood attack" by bombarding the network with hello packets. Generally speaking, all of the neighboring nodes get notified of an authorized node's existence through hello data packets. In order for all nodes in the network to view the malicious node as their neighbor, the attacker broadcasts these hello packets to every single node in the entire network. As a result, many nodes transmit data packets to fictitious neighbors [37]. This is a routing attack. Consequently, one way to defend against such attacks is to authenticate neighboring nodes. Figure 10 demonstrates that rogue nodes use strong signal HELLO packets to entice legitimate nodes [113].

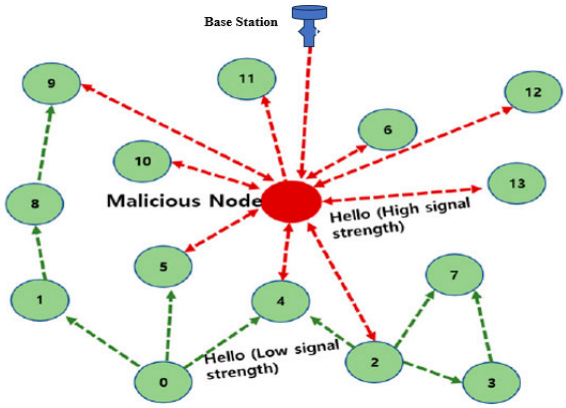


FIGURE 10. Overview of hello flood attack.

(ix) Misdirection Attack

A misdirection attack entails sending packets to a captured node, altering the routes, or rerouting them to unreachable destinations. By altering the route path, an attack can be countered which includes the source route in every packet [45]. The attacker changed the path to go to node F, even though the typical route, as shown in Figure 11, should go from node A to node D.

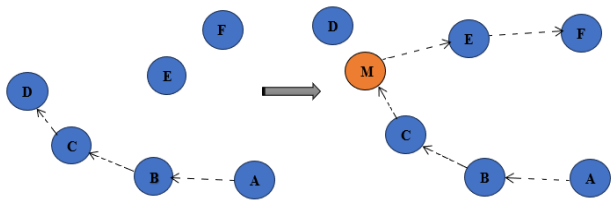


FIGURE 11. Overview of misdirection attack.

(x) Spoofing Attack

In order to enable more attacks, a malicious node impersonates another node by obtaining unauthorized access or utilizing a fictitious MAC address [46]. Figure 12 depicts that Node A believes the spoofer node to be an authorized neighbor, it is transmitting all of its data packets to it. However, in order to disrupt traffic and cause congestion, the spoofer subsequently modifies and replays all of the routing information. The application of reinforcement learning techniques or the addition of an authentication code to every transmission are the countermeasures against such attacks.

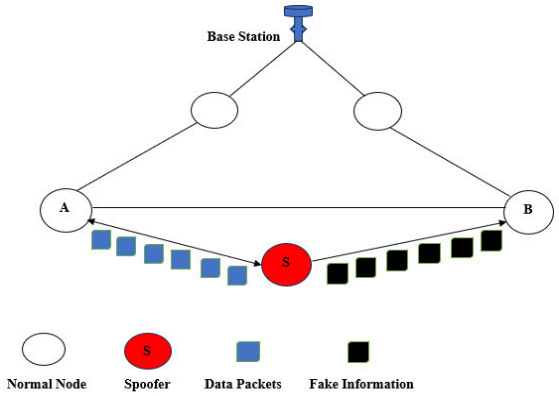


FIGURE 12. Overview of spoofing attack.

(xi) Acknowledgment Spoofing Attack

The malicious node in this attack listens in on the packets that the neighboring nodes send. The malicious node spoofs the link layer's acknowledgment by using the information at its disposal in order to introduce a weak link or shadow zone link [4], [47]. This can be classified as a denial-of-service (DoS) attack. The scenario shown in Figure 13, Node B is supposed to respond to the data packets that node A is transmitting by sending acknowledgment data packets back to node A. However, the spoof in the middle sends a bogus acknowledgment data packet to node A by pretending to be node B. Such attacks can be prevented by encrypting communications and authenticating all data frames coming into and going out of the node.

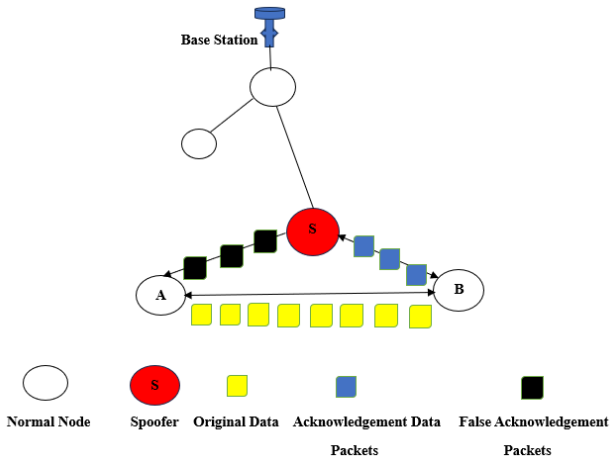


FIGURE 13. Overview of acknowledgment spoofing attack.

d: ATTACKS ON TRANSPORT LAYER

The dependable transmission of packets in UWSNs is the responsibility of the transport layer. At this layer,

desynchronization and synchronization flooding attacks are common DoS attacks.

(i) Synchronization Flooding Attack

Since the flooding attack directly targets network connections, it takes place at the transport layer. An attacker uses the flooding attack to overwhelm nodes with connection requests in an attempt to exhaust their resources [38], [48]. This is a denial-of-service (DoS) attack. Restricting the number of connections is one kind of defense against this kind of attack.

(ii) Desynchronization Attack

Malicious users can cause destination desynchronization by sending bogus data packets with fictitious control signals or sequence numbers, they disrupt the connection between nodes and launch a desynchronization attack. In addition to being difficult to use, synchronization is essential for UWSNs, furthermore, the Global Positioning System (GPS) is also useless [47].

e: ATTACKS ON APPLICATION LAYER

Because there are no known protocols for UWSN, its application layer is very different from that of terrestrial networks. The desktop computers at offshore stations or surface stations (buoys or surface ships) are where the underwater application software is directly installed. By employing a variety of strategies to stop data packets from reaching base stations, the attacker in these layers attempts to compromise the apps. The two attacks that take place in the application layer are overwhelm and path-based denial-of-service.

(i) Overwhelm Attack

In overwhelm attack, the attacker wants to overwhelm each and every network nodes and force them to send a significant volume of data packets to the surface gateway or the base station. In addition to using network bandwidth, the overwhelm attack depletes node energy [49].

(ii) Path-Based DOS Attack

In this attack, no other node is able to send sensed data to the surface gateway because the rogue node uses up all the resources on the path to the surface gateway or base station. The adversary feeds bogus data packets into the network to carry out this attack, starving it of legitimate network traffic [50].

4) CAPABILITY OF ATTACKER-BASED ATTACKS

Water in the surrounding environment presents numerous obstacles for underwater wireless networks. As a result, UWSN has numerous limitations, including reduced battery life, unreliable data transmission, a restricted capacity for data transmission, low processing power, and non-replaceable sensor nodes. Underwater networks are susceptible to several security breaches and threats because of their broadcasting nature and these limitations. As seen in Figure. 14, there are another type of malicious attacks that are contingent upon the attacker's capability. In this sense, ''capability'' refers to an attack's reliance on the strength of the attacker, such as the location of the attacking node or the attacking node's hardware and processing capacity, which might intensify the attack.

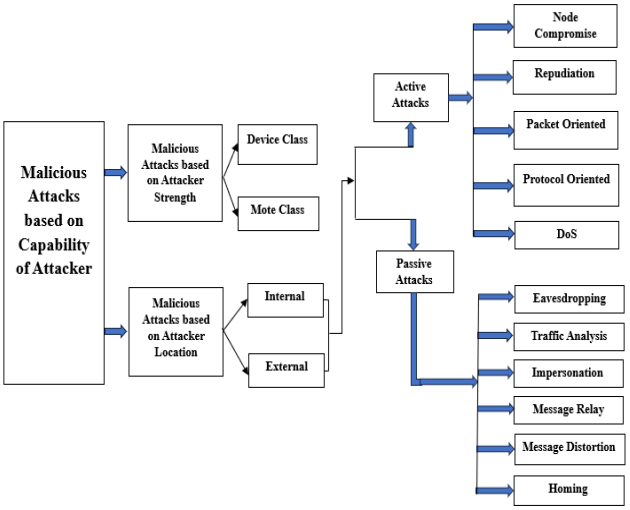


FIGURE 14. Classification of capability of attacker based attacks.

a: ATTACKS BASED ON ATTACKER STRENGTH

Attacks can be classified into two groups according to the strength of the attacker: device class and mote class [102].

(i) Device Class Attack

In the device class, the attacker uses a specifically made sensor node, such as ROV or an AUV, that has a large memory, a long battery life, high transmit power, and high computational power to conduct an attack.

The goals of device class attacks are to disguise the legitimate sender, to steal confidential information, and disrupt the network operations.

(ii) Mote Class Attack

In contrast to device class attacks, mote class attacks try to initiate an attack by gaining access to an already existing sensor node. Such attacks are constrained because the attacker exploits the capacity of another node to cause disruption to the network.

b: ATTACKS BASED ON LOCATION OF ATTACKER

An attacker may come from two locations, i.e. internal and external.

(i) External or Outsider Attack

Nodes outside of the UWSNs are responsible for this attack, which is known as an outsider or external attack. Surreptitiously listening to data transmission, the external attacker injects bogus data packets into the network to cause a denial of service (DoS) attack and waste network resources [13].

(ii) Insider or Internal Attack

Nodes that are a part of the UWSNs can launch an internal or insider attack. The underwater network's authorized sensor nodes are forced to exhibit strange behavior from the start by the insider attacker. Since insider attacks have access to

critical and confidential network information, they are more dangerous than exterior attacks [13].

(iii) Active Attacks

In active attacks, attackers attempt to add, delete, alter, or distort data that is transmitted over a network [51]. Active attacks can keep an eye on data and attempt to influence or remove packets that hostile actors from the outside or inside can execute. Since external attacks are carried out by non-network nodes, they are easier to detect and prevent. Inner nodes are responsible for internal attacks, which have the capacity to do serious damage. Therefore, internal attacks have dire repercussions as they are harder to recognize. Using security measures like authentication, cryptography, and trust management is the simplest way to avoid this problem. The classification of active attacks based on their goal is as follows [54].

- Node Compromise

Underwater sensor nodes could be placed in unsupervised and unsecured or hazardous maritime environments. Furthermore, the UWSN may have hundreds or even thousands of nodes that are far dispersed, making it impossible for it to guarantee the security of every node. An attacker may capture, breach, and seize control of nodes to access and alter data from memory. For monitoring or disruption purposes, the compromised nodes could be added into the UWSN as legitimate nodes, which could result in more serious harm. To Protect UWSN networks from node compromise attacks requires modifying mechanisms including data management, configuration management, trustworthiness, and a high-level hardware protection system.

- Repudiation

In repudiation attacks, malicious nodes disclaim the exchange of information with other nodes or any involvement in a specific operation. Refers to a node's decision of rejection from involvement in all or a portion of a communication, whether or not the communication is harmful.

- Packet Oriented

When a malicious adversary initiates a packet-oriented attack, the goal is to either destroy the packet data or interfere with the packet's data transmission. Among the most frequent active attacks are injection, modification, and interception attacks.

- Protocol Oriented

Attacks are launched by the malicious adversary with the intention of damaging the operation of particular protocols. Attacks on media access control (MAC) protocols and attacks on routing protocols are the two main subcategories of these attempts. Routing protocols attacks have the potential to stop packets from reaching their destination node and potentially stop the network from functioning altogether. These attacks, which include packet replication, rushed attacks, routing table overflow, and poisoning, are launched against the routing protocols. Attackers can lure packets, examine them, or even drop them at will by using these malicious behaviors. MAC protocol attacks are designed to interfere with the system that grants nodes access to the channel. The channel might be persistently occupied by malicious attackers to prevent legitimate nodes from sending packets. Furthermore, sending a request to send (RTS) and clear to send (CTS) packets repeatedly for handshake of MAC protocol would drain nodes' batteries, making it a straightforward method to launch attacks. Using UWSN-compatible encryption, authentication, and trust management techniques is a workable way to ward off these kinds of attacks.

- Denial of Service (DoS) Attacks

Denial of Service (DoS) attacks aim to prevent legitimate nodes from accessing resources and services. The attacker attempted to block legitimate nodes from using network services in order to accomplish this purpose. DoS attacks can be executed in a variety of methods and can be either active or passive manner. When these attacks are merged with other active or passive attacks, it becomes more challenging to identify and fend off them. DoS is attained by flooding and jamming. As a result, DoS attacks include blackhole, wormhole, and jamming. Any OSI model layer could become the target of a DoS attack. A reactive approach to identify and thwart denial-of-service (DoS) attacks was also proposed by Martin et al. [34] along with an adaptive protocol for async channel situations.

(iv) Passive Attack

Rogue nodes seek to identify the kind of actions conducted and gather data that is transmitted over the network by employing a passive attack [52], which prevents them from interfering with the network's ability to function. Additionally, the attacker can track data transfer, identify interacting hosts, forecast transmission patterns, and identify the source by capturing data and analyzing the resulting traffic. Since these passive attacks don't affect the network's functionality, they can be challenging to detect. The following is a classification of passive attacks based on their intended purpose.

Table 3 provides an overview of the attacks based on the description provided.

- Eavesdropping Attack

Eavesdropping in this attack [55] does not compromise the integrity of the channel. In the functional network, the information is detected by the illegitimate node. The hackers eavesdrop on the data to determine the transmission path and jeopardize network security. Eavesdropping is the most frequent violation of data security.

- Traffic Analysis Attack

The attacker looks at the patterns of transmission that were followed in this attack [56]. In order to damage and facilitate the destruction of the network through active attack, the attacker gains access to the data sequence because the intruder allows it. The network is constantly monitored over to prevent this threat.

- Impersonation Attack

To hide the required number of nodes, the attacker [57] employs this tactic by posing as a regular node in the sensor

TABLE 3. Overview of both active and passive attacks.

Types of Threat	Active or Passive	Summary	Defense Mechanism
Jamming	Active	Limit the sources' ability to send messages or prevent them from sending valid messages.	Jamming methods, region mapping
DoS	Active	Unavailability of the facilities and services. Shut off or divert the infrastructure's function.	Message prioritization, monitoring, and encryption techniques.
Physical	Active	Permanently destroyed the node	Proofing against tamper
Tampering	Active	The seize nodes is completely taken over, and its ability to function is compromised.	Regular key updates and appropriate key management methods should be used.
Neglect and Greed	Active	It selects the quickest path for transmission by transferring packets to a malicious node.	Authentication methods, redundancy.
Homing	Active	To carry out any active attacks, ascertain the networks' insight sources.	Cryptography
Node Capture	Active	To launch the repeated attacks. Several nodes are taken down and then redeployed.	Secure Authentication
Node Outage	Active	All transmission links and all parental and ordinary sensor nodes are entirely turned off.	Powerful Computations, Time Protocols
Eaves dropping	Passive	It listens to data in an active network	Surveillance of the network
Traffic Analysis	Passive	The attacker gives the defender the sequence to cause harm and facilitate destruction.	Surveillance of the network
Impersonation	Passive	As a result, the packets are being misdirected to other links of communication.	Privacy Analysis
Rushing	Active	Via a different tunnel, the data from the nearby node is quickly transmitted to the other target node.	Adding a nodes list
Clock skewing	Active	By modifying the relaying messages' time. The adversary imitates the targeting clock skew	Interval of variable time synchronization
Vampire	Active	The network is destroyed, and the sensor batteries are exhausted by this type Denial of Service (DoS) attack	Methods for validation
Cloning	Active	When a hacker can easily get, compromise, and install an infinite number of copies on the sensor network's captured nodes.	Intrusion detection

network. Transmissions are therefore diverted to alternative connection pathways.

- Message Relay Attack

Within such attacks [9], [18], In order to transmit identical data that was previously transferred by the source node, the attacker either impersonates the identity of the source node or uses hacking to purposefully pause the data transfer.

- Message Distortion

The attacker may modify the data that is transferred from one node to another in these attacks [9], [18]. By forwarding the end consumers' incorrect information, this could cause confusion.

- Homing Attack

This attack [51] does not directly alter the messages; instead, the adversary looks the network for insight sources, which are subsequently used to execute any active attacks. Cluster chiefs are also known as cryptographic key administrators employ header encoding and network behavior monitoring to locate and attack nodes in order to prevent assaults of this nature.

V. MECHANISMS TO DETECT AND MITIGATE SECURITY ATTACKS

Security schemes and sets of procedures must address concerns such as secure localization & synchronization, authentication, key management, trust management, intrusion detection, and secure routing to meet the security criteria and maintain the security of the UWSN, as shown in Figure 1. The common strategies suggested to identify and mitigate UWSN attacks are reviewed in this section. To deal with each concern, many state-of-the-art security techniques have been developed for UWSN. A brief summary of the several security techniques in use, along with the defensive attacks that go along with them, is provided in Table 4.

A. ENCRYPTION ALGORITHMS

This section includes an analysis of several different methods of encryption that the researchers have proposed for the UWSN environment. Table 4 presents the analysis in tabular form as well.

1) LIGHTWEIGHT CRYPTOGRAPHIC ALGORITHM FOR UWSNS

Specifically designed for underwater wireless sensor networks (UWSNs), a lightweight encryption algorithm was developed in [60]. To ensure data security during transmission in UWSNs, the algorithm makes use of symmetric key encryption, error-correcting codes, and message authentication codes (MACs). The paper's main focus is on the necessity of secure communication in UWSNs. However, it is difficult to apply conventional encryption techniques on UWSNs due to their peculiar characteristics, which include high latency, poor bandwidth, and unstable communication routes. This study's primary contribution is the creation of a lightweight encryption technique that is well suited to the limitations and specifications of UWSNs. It is demonstrated that the method maintains minimal computational and energy costs while offering a high degree of security. The article covers a number of possible UWSN attacks, including message manipulation, impersonation, and eavesdropping. The suggested technique offers message authentication, data integrity, and confidentiality protection against these types of assaults. Any UWSN

that transmits data using acoustic communication can apply the suggested algorithm.

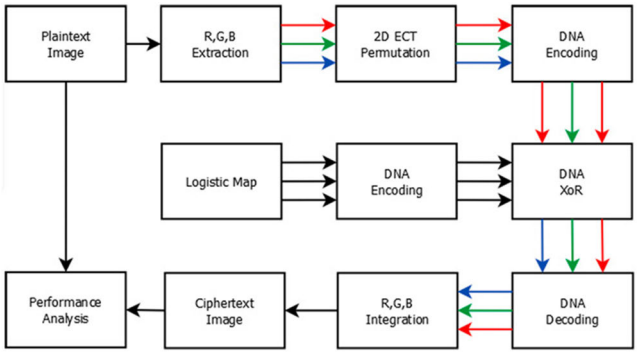


FIGURE 15. Encryption approach [60].

2) EFFICIENT ENCRYPTION ALGORITHM FOR UWSN

Efficient encryption mechanisms were recommended by the study conducted in [58] to safeguard integrity and confidentiality in the context of UWSNs. An alternative method is used to modify the traditional advanced encryption standard AES-128. The traditional advanced encryption standard (AES) is inappropriate for the UWSN setting since it needs more energy when using the S-Box. Consequently, an 8-round block cipher technique has been employed in place of S-Box in the context of UWSNs. The research's suggested technique is resistant to several attacks, including brute force. By adjusting the number of iteration rounds, the suggested algorithm allows the key space to be expanded. Increasing the number of iteration rounds from 8 to 10 is one way to further expand the key space. Brute force attacks cannot defeat the round key. Additionally, a secure network architecture for the UWSN environment was suggested by the research's authors. The suggested scheme is contrasted with the current schemes, including PRESENT, AES-128, and Blowfish. The findings show that the proposed technique is both energy effective and secure, when compared to the other current methods. The suggested encryption technique has less overhead, making it appropriate for the UWSN environment, as confirmed by the simulation results. In the future, the accuracy of the suggested encryption algorithm can be verified by testing it in a real UWSN environment. Figure 16 shows the algorithm routine of an efficient encryption algorithm for UWSNs.

3) ENCRYPTION SCHEME FOR UWSNS

This study [59] examined the encryption algorithm based on its applicability to the UWSN context. In the protocol stack of UWSN which consists of five layers, each layer appends its header with data, when data goes from an upper layer to a lower layer. The encryption procedure includes the security header, which has security parameters for the recipient to get the data. The authors recommended using the exact same key for decryption as well as encryption because symmetric keys have small key sizes. The message is put into the

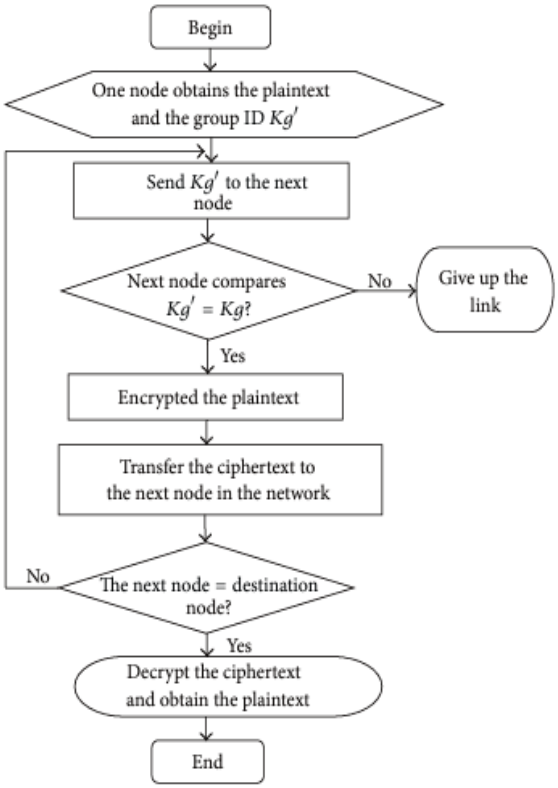


FIGURE 16. Algorithm routine of efficient encryption for UASNs [58].

message authenticated code once the headers have been applied. The shared key and message authenticity are ensured via the message integrity code (MIC). The message integrity code (MIC) and message are encrypted by encryption. The recipient computes and contrasts the two MIC. The message is accepted or rejected depending on whether the values of the two MICs are equivalent or not. This study suggests that the CMVP method be used in conjunction with minimum overhead to provide security in UWSNs. The procedure of data encryption and decryption is depicted in Figure 17.

B. SECURE ROUTING

The different secure routing algorithms that the research community has proposed for the UWSN environment are analyzed in this section. Table 4 presents the analysis in tabular form as well.

1) NEW ENERGY-EFFICIENT SECURE ROUTING IN UWSNS

A novel multi-objective routing protocol called Boltzmann Ant Colony Optimization Routing Protocol (MO-CBACORP) was proposed by authors in [66]. By reducing sensor node energy consumption in UWSN routing, MO-CBACORP can effectively reduce network delay and greatly improve the security of routing. The algorithm's convergence is much accelerated and the problem of being trapped in local optimal solutions is successfully prevented because

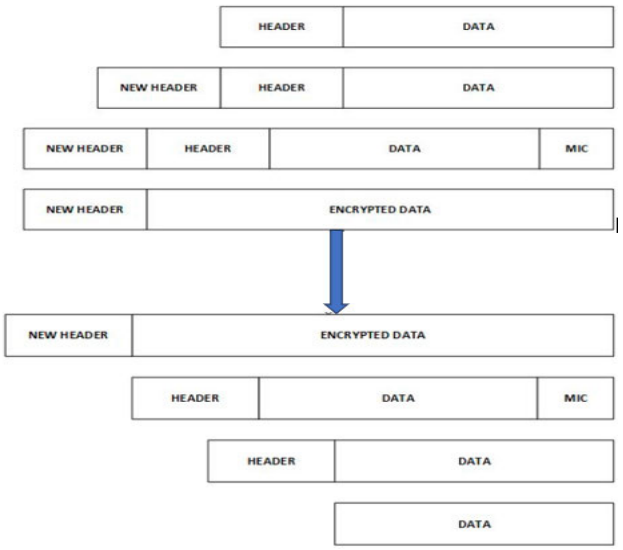


FIGURE 17. Procedure of encryption and decryption [59].

to MO-CBACORP's innovative suggestions for the Boltzmann selection strategy and chaos operator throughout the routing optimization process. Furthermore, a novel experiment that precisely imitates attack scenarios and underwater monitoring settings is provided for use in underwater monitoring environments. With a minimum parameters improvement of 9.31 % 7.68%, and 7.25% regarding consumption of energy, delay, and route security, respectively, the experimental results demonstrate that MO-CBACORP outperforms the most recent modern research, such as MAP-ACO, ACO-MCMC, and THOA-MHR. In order to accurately detect hostile nodes and account for variations in physical parameters such as consumption of energy, delay, and system security, this study proposes a novel Quality of Service (QoS) secure routing method for UWSN. Simultaneously, by merging direct and indirect trust, the developed model can assess the trustworthiness of sensor nodes quickly, precisely, and thoroughly in the network. The flowchart of MO-CBACORP is depicted in Figure 18.

2) SECURE ROUTING IN UWSNS

The fusion technique of the firefly algorithm (AFSA) and the ant colony optimization algorithm (ACOA) is the basis of the secure routing algorithm for underwater wireless sensor networks (UWSNs) that the authors propose in [61]. The main contribution of this study is a secure routing system that may ensure the availability, integrity, and confidentiality of data transfer in UWSNs. It is based on the AFSA-ACOA fusion mechanism. ACOA is used to improve the security of the chosen paths and AFSA to optimize the routing path selection. The paper covers a variety of attack methods, including replay, sybil, and packet-dropping attacks, that can be used against UWSNs. Various software and hardware platforms can be used to implement the method, depending on the particular needs of the application.

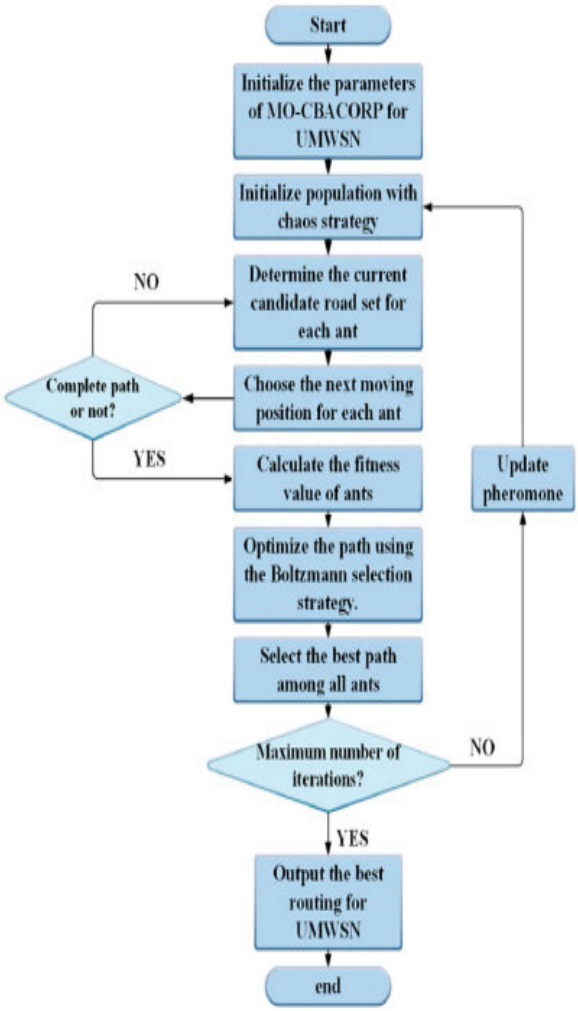


FIGURE 18. Flowchart of MO-CBACORP [66].

3) SECURE ENERGY-EFFICIENT LAYERED ROUTING IN UWSNS

To increase energy efficiency and transmission reliability, authors in [67] presented the secure energy-efficient layered routing approach (DESLR) for UWSNs. To characterize the node behaviors, the DESLR develops a trust model which is trust-based that considers both direct as well as indirect trust variables. The reliability of the acoustic channel is a critical factor to take into account when identifying malicious nodes since different channel conditions can have a big impact on packet transmission. In order to find energy-efficient and low-latency routing paths, an enhanced Ant Colony Optimization Algorithm (ACOA) is presented, which balances the consumption of energy and routing distance. A two-layer fuzzy logic approach combined with a Layered Clustering method is also used by DESLR to organize nodes into clusters and selects cluster heads (CH) that stay away from hotspots and guarantee even distribution of energy. The simulation's findings demonstrate that DESLR outperforms previous similar work in terms of data packet loss, average latency, and

usage of energy, and may identify defective nodes by studying unusual behaviors.

4) SECURE ROUTING SCHEME FOR UWSNS

A secure routing approach was designed by the researchers in [62] for the UWSN environment. Since establishing a trustworthy third party in UWSNs might be difficult, a concise signature strategy is recommended for establishing a secure route between the source and the destination node. A signature scheme that strengthens security and is resistant to forging and other forms of attacks was recommended by the authors. The suggested method can operate without the assistance of a trusted online third party. Utilizing a trapdoor strategy, the authors suggested, would allow sensor nodes to remain anonymous. This research's recommended routing strategy avoids the issue of fake identity within sensor nodes, provides security for interaction in the UWSN environment, and to ensure anonymity and two-way authentication between the source and destination nodes, use digital signatures and bilinear map trap doors. In the proposed method, the trap door lowers the overhead associated with large-scale pre-shared key management. It takes one bilinear mapping and one hash operation to open the trap door. The proposed scheme's performance was assessed by simulations conducted with the ns2 simulator and the UWSN aqua-sim simulation program. The performance of GPNC and LB-AGR is examined with respect to throughput, usage of energy, and packet delivery ratio (PDR). The results show that the recommended approach performs far better in terms of network security and efficiency. The UWSN secure routing system is shown in Figure 19.

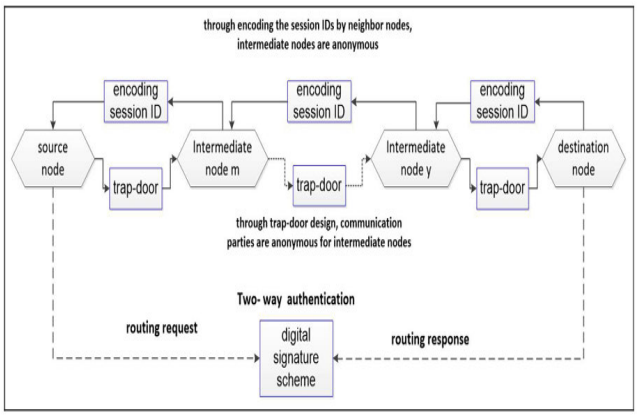


FIGURE 19. Design of secure routing scheme [62].

5) SECURING THE COOPERATIVE ROUTING SCHEME FOR UWSNS

For application in UWSN context authors in [63] suggested the scheme known as energy efficient and secure cooperative routing (SEECR). SEECR features an integrated defense system and efficient energy usage. Using several performance evaluation factors, an AMCTD is used to compare the performance of SEECR. The findings showed that, with regard

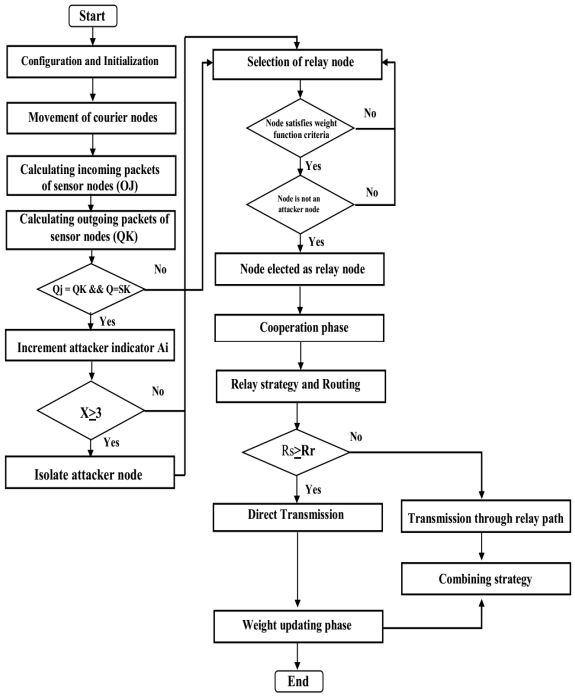


FIGURE 20. Flowchart of SEECR scheme for UWSNs [63].

to every performance evaluation criterion, the SEECR protocol outperforms the AMCTD protocol. The performance of SEECR is superior to AMCTD, according to the results. SEECR improves throughput by up to 9%, decreases transmission loss by more than 50%, lowers energy cost by up to 23%, and shortens end-to-end latency by 25%. It also improves the number of living nodes by 9%.

6) SECURING UWSNS FROM ROUTING ATTACKS

In the setting of UWSNs, the authors of [36] presented a distributed defensive approach against specific routing-related attacks. Using the suggested mechanism, sinkhole and wormhole attacks on routing protocols can be identified. Silent surveillance and identification are the two phases of the suggested approach. For the purposes of prevention and identification, the sensor nodes listen in on the messages transmitted by neighboring sensor nodes. To find its neighbor as soon as it is deployed, every node uses the secure neighbor discovery protocol. Monitoring neighbors' activity helps identify malicious activity occurring within UWSNs. The sinkhole attack may cause receiving packets to be tampered with or dropped. This research's suggested that to identify sinkhole attacks compare each neighbor sensor node's incoming and outgoing traffic. The signatures will not match if the malicious node modifies or deletes the packets, allowing for the detection of an attack. The suggested mechanism by the research may detect active attacks, but it cannot detect passive ones. The suggested mechanism will not be able to identify such an attack if an illegitimate node records data traffic for analysis without altering or dropping it. By examining

the signatures, the recommended approach can also identify encapsulated wormhole threats and out-of-bound threats. Utilizing an isolation method, a hostile node discovered within the UWSN environment is isolated and cut off from the network. Because of this, the rogue node is unable to interfere with UWSN operations or stop the routing process.

7) SECURING THE NEIGHBOR DISCOVERY IN UWSNS

A secure neighbor discovery approach was put forward by the authors of [64], [65], [66], [67], [68], [69], [70], [71], [72], [73], [74], [75], [76], [77], [78], [79], [80], [81], [82], [83], [84], [85], [86], [87], [88], [89], [90], [91], [92], [93], [94], [95], [96], [97], [98], [99], [100], [101], [102], [103], [104], [105], [106], [107], [108], [109], [110], [111], [112], [113], [114], [115], [116], [117], [118], [119], and [120] in the context of UWSNs. An invader has the ability to conduct a wormhole attack in a hostile setting by finding a neighbor who is vulnerable to one. The wormhole attack has unintended consequences that encryption solutions are unable to handle. The methods proposed in this paper provide wormhole-resistant secure neighbor discovery techniques for UWSNs. The arrival signals' direction of approach determines the approaches that the research recommends. The proposed strategy can fend off wormhole attacks. The following four procedures make up the proposed scheme: (a) B-NDP requires two nodes; (b) DV-NDP requires three nodes; (c) SDV-NDP enhances DV-NDP; and (d) MA-NDP allows node mobility in neighbor discovery. Evaluation outcomes of the following four procedures are listed: (a) There is a very high probability that B-NDP will prevent fake neighbors from forming neighbor connections. The true neighbors in B-NDP are able to find each other. (b) Fake neighbors can be prevented from forming neighbor relationships by DV-NDP with a probability close to 1 and at a low cost in terms of links lost. (c) SDV-NDP can detect every wormhole; nevertheless, compared to DV-NDP, SDV-NDP loses a lot of links. (d) MA-NDP is able to regulate node movement and identify highly probable random placements of wormhole links. The B-NDP and MA-NDP protocols should be used in applications where end-to-end latency and connection quality are the main concerns. Low-density network environments can also benefit from them. Applications requiring wormhole resilience and a high node density should use the DV-NDP and SDV-NDP protocols.

8) SECURE COMMUNICATION SUITE FOR UWSNS

For the UWSN environment, in [8], the authors presented a security suite consisting of mobile and stationary sensor nodes. The security suite includes cryptographic primitives and secure routing methods. The authors originally proposed the FLOOD technique. The technique discussed above has a secure variation known as secure flood (SeFLOOD). The amount of overhead introduced to the FLOOD protocol in order to ensure its security was measured by testing the performance of the SeFLOOD protocol. According to Figure 22, the testbed consists of a gateway (GW),

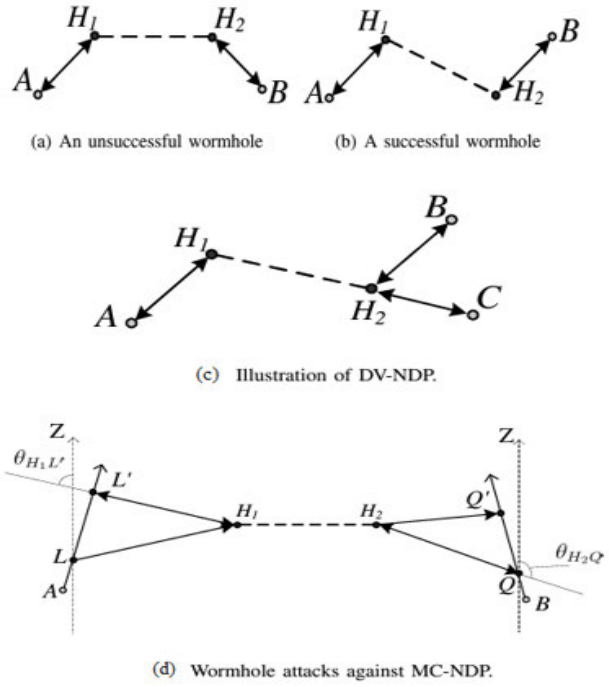


FIGURE 21. Protocol proposed to resist wormhole attack in secure neighbor discovery [64].

two fixed nodes (FN1 and FN2), two unmanned aerial vehicles (UAVs), and their respective software. The trials' results show that the suggested suite works well in the UWSN context. The suggested protocol suite's main achievements are shown below. (a) The small impact of the cipher text expansion makes the suggested suite efficient. (b) Compared to an unsecured protocol, the discovery phase of a secure protocol produces 6% less overhead. When comparing the reconfiguration stage of the secure protocol to the unsecured protocol, (c) no extra overhead was incurred (d) Lampson's recommendations for computer system design were adhered to in the creation of the secure protocol.

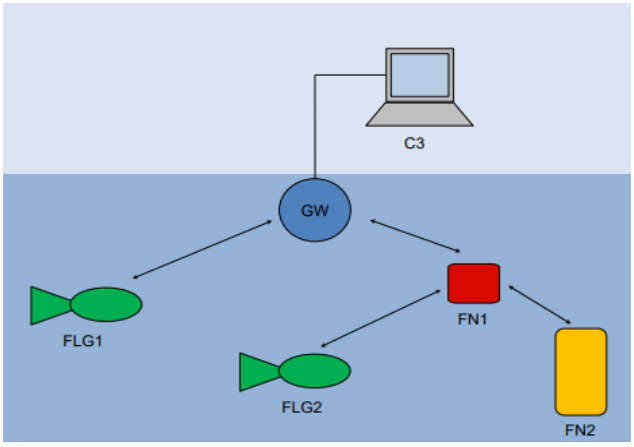


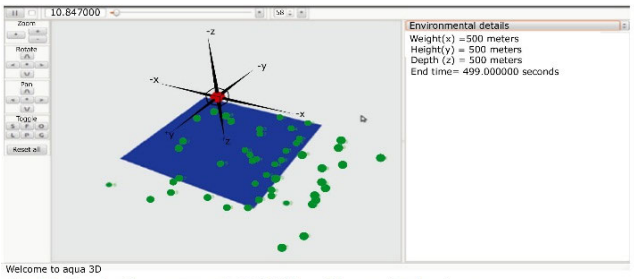
FIGURE 22. Testbed formation in secure communication suite [8].

9) SECURE COMMUNICATION IN MOBILE UWSNS

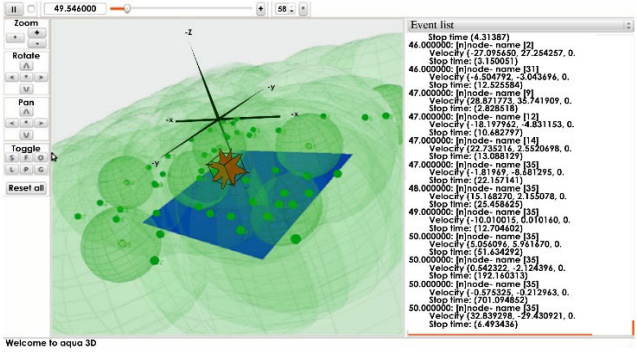
DoS attacks were the main focus of research in [65]. DoS attacks include flooding, demolition attempts, and man-in-the-middle (MITM) attacks. An MITM attack recorded the information shared between sensor nodes in UWSNs. Wormhole, Sybil, and selective forwarding attacks are examples of potential MITM attacks in the context of UWSNs. An excessive number of packets are delivered to the base station by the malicious node(s) in a flooding attack, which causes congestion. The flooding attack degraded the overall network efficiency. A demolition attack destroys the network by modifying or tampering with a sensor node's configuration. Physical security is crucial for thwarting attacks. Issues such as incorrect neighbor identification and out-of-coverage concerns are encountered by mobile sensor nodes in a UWSN scenario. To simulate their findings, the authors of this study used Aqua-Sim. In order to protect mobile UWSNs from DoS assaults, this study creates secure UWSNs with self-localization and intelligent sensor nodes. Figure 23 depicts the aqua 3D visualization of flooding attack (a) node deployment with single base and (b) packet transfer while there is a flood node present.

C. KEY MANAGEMENT FRAMEWORKS FOR UWSNS

The several key management frameworks created by the researchers for the UWSN environment are examined in this section. The analysis is also shown in tabular form in Table 4.



(a) Node deployment of UWSN with a single base

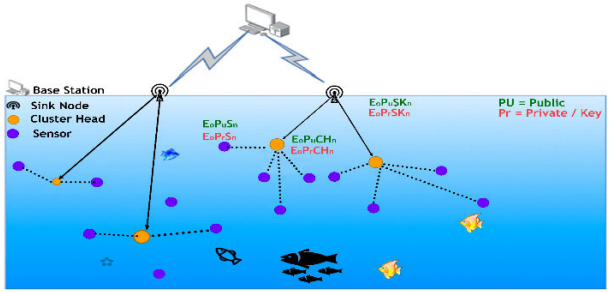


(b) packet transfer in the presence of flood node

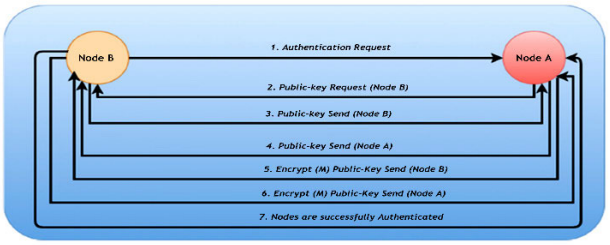
FIGURE 23. Aqua 3D visualization of flooding attack [65].

1) SECURING KEY MANAGEMENT SYSTEM FOR UWSNS

A secure lightweight key management system for UWSNs is suggested in [68]. Along with lightweight implementation, scalability, and authentication procedures, the suggested framework also incorporates key distribution, revocation, and generation. For key distribution, authors employ an elliptic curve-based technique and for key revocation employ the certificate revocation list (CRL). Authors additionally assess the effectiveness of the suggested system considering the overhead for communication and the degree of security. In comparison to the most advanced computationally significant frameworks, the findings of the simulation demonstrate that ECC-based lightweight methods decreased the overhead of computation and communication to extend network lifespan and enhance the security and scalability of UWSNs. Figure 24(a) depicts the key management paradigm, while Figure 24(b) depicts a lightweight approach.



(a) Proposed Key management model fot UWSNs.



(b) Proposed lightweight approach

FIGURE 24. Key management model & authentication approach [68].

2) COMPUTATIONALLY EFFICIENT SIGNATURE SYSTEM FOR UWSNS

The computational overhead of signature verification can be reduced by 90% using the online/offline computationally effective signature approach [69], which makes use of batch verification and elliptic curve cryptography (ECC). The signature scheme's model is depicted in Figure 25. The paper's focus is on the requirement for efficient and secure signature systems in UWSNs. Conventional signature methods are not appropriate for underwater sensor nodes (UWSNs) due to their processing constraint and consumption of energy. The creation of a computationally effective online/offline signature technique is the paper's main contribution, especially adapted to the needs and limitations of UWSNs. The study addresses many attack vectors against UWSNs, including message modification and node compromise attacks. The suggested signature system is made to offer data integrity and authenticity defense against these kinds of attacks. The suggested signature scheme is applicable to any UWSN that

generates and verifies signatures using ECC. In an environment of limited resources such as UWSNs, the approach is specifically intended to function well.

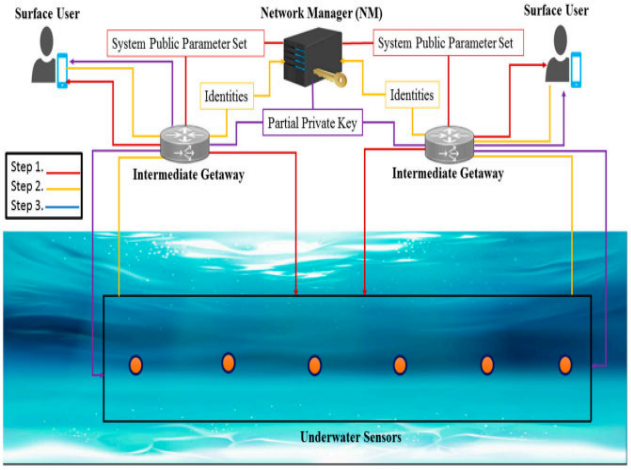


FIGURE 25. Network model of signature scheme [69].

3) KEY AGREEMENT MECHANISM FOR UWSNS

Researchers in [70] presented the key agreement mechanism for the UWSN ecosystem. It is a unique and energy-efficient mechanism. To reduce communication overhead, in the system that is suggested, clusters are created from the sensor nodes. The task of gathering, aggregating, and transmitting observational data falls to each cluster's H-node, also known as the cluster head. Not only do the S-nodes transmit the observation data to the H-nodes, they are also responsible for observation. When it comes to capacity, compute, and communication power, H-nodes outperform S-nodes and are higher-performing nodes overall. Attacks like replay, spoofing, Sybil, and node replication attacks can be thwarted by using the suggested key agreement approach. The public and private keys of the sensor node incorporate the location and identity, strengthening the suggested mechanism's defense against attacks. The reason for the lower overhead in the suggested approach is that Tate pairing decomposition problems were not used. When it comes to computation and communication duties, low-performing nodes receive help from high-performing nodes. High-performance sensor nodes actively engage in tasks related to communication and computation, resulting in a dramatic drop in the energy usage of low-performance sensor nodes. The suggested method suggests updating the session key of underperforming sensor nodes periodically to strengthen the security and resilience of the UWSN environment. The outcomes of the simulation demonstrate how the suggested mechanism outperforms the others in terms of network security and performance. The sensor nodes with poor performance saw a considerable decrease in energy consumption when the proposed key agreement mechanism was implemented. Figure 26 displays the key management scheme's network model.

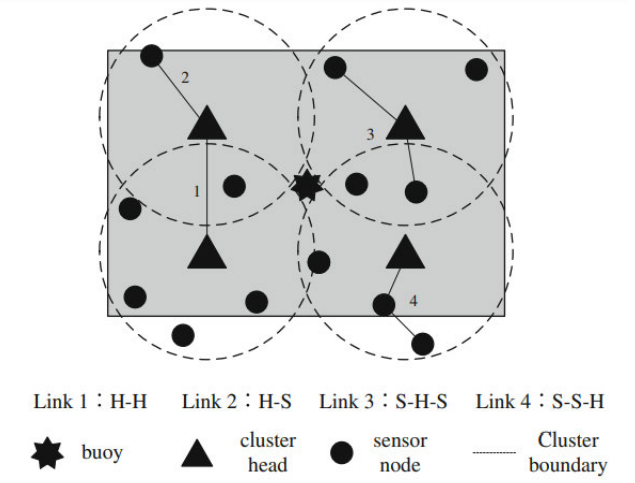


FIGURE 26. Network model of key management scheme [70].

4) KEY DISTRIBUTION MECHANISM FOR MOBILE UWSNS

The study undertaken in [71] produced a key distribution mechanism for UWSNs. In mobile UWSNs, the suggested study aims to facilitate peer-to-peer communication. This research makes use of models of meandering and nomadic mobility. The meandering model is accurate since it is dependent on ocean movement. Vertical movement is not taken into consideration by this two-dimensional model. The idea of hierarchical meandering is applied across large regions, like thousands of meters. The paradigm of nomadic mobility is three-dimensional and hierarchical. This mobility strategy works well in certain coastal areas. According to the nomadic mobility model, each sensor node moves a little bit autonomously and randomly after floating to a destination as a group. According to the suggested plan, each sensor node travels slightly to a new location after the group does. The research's findings indicate certain connectivity problems. Mobility is the cause of the connectivity problem, but the suggested solution promptly resolved it. The research's suggested strategy demonstrates that even if an adversary manages to seize some sensor nodes, resilience performance remains significantly higher. In this instance, the number of compromised links is very low. The results reported also show that the suggested approach has improved security and minimal energy use.

5) KEY MANAGEMENT BASED ON CLUSTER TECHNIQUE FOR UWSNS

The cluster-based key management protocol (CKP) was suggested by the authors in [72] in the context of UWSNs to tackle the issue of mobility and security. In the suggested method, to offer varying degrees of security in the mobile environment different types of keys are employed at various points in time. The sensor nodes in hierarchical networks form clusters of competent sensor nodes. In this study, a novel communication architecture is put forth, and it facilitates

the effective management of sensor node mobility. Additionally, the impact of self-node compromise is reduced. CKP offers integrity, freshness, secrecy, and verification. The findings of this study demonstrate that CKP is energy- and storage-efficient since each sensor node only keeps a minimum quantity of keys on its file. Additionally, the resilience of CKP against the various security risks is also examined in this study.

6) DIGITAL SIGNATURE BASED END-TO-END AUTHENTICATION IN UWSNS

The authors of this study assessed several digital signature techniques for UWSNs [73]. End-to-end authentication techniques are used, and evaluation is based on energy consumption. The authors of this study found that because UWSN nodes have very limited resources and RSA requires a lot of computation, typical digital signature algorithms like it are not appropriate for the UWSN environment. This study's conclusion shows that while some strategies worked well in WSN environments, UWSNs' particular qualities may prevent these schemes from working well there. The authors of this study disclosed several attributes of digital signature methods that make them appropriate for use in UWSN environments. Three digital signature techniques like ECDSA, ZSS and BLS are assessed. Based on the amount of power consumed, an evaluation is conducted. ECDSA, ZSS and BLS have respective signature generation times of 134 ms, 229 ms and 302 ms. ECDSA, ZSS and BLS have signature sizes of 40 bytes, 21 bytes and 21 bytes, respectively. This study came to the conclusion that the primary factors influencing energy efficiency in the UWSN environment are aggregate and signatures that are small in size.

7) SECURE AUTHENTICATION IN CLUSTER-BASED UVWSNS

As an underwater vehicular wireless network (UVWSN) that has the capacity to fully identify network-wide malicious node attacks (MNA), the authors of this study [74] examine UWSN and underwater vehicle (UV) optimization. Therefore, using the UVWSN-deployed SDAA (secure data aggregation and authentication) protocol, the suggested methodology resolves MNA that opens the UWSN channel and initiates MNA. For secure data exchange, the SDAA protocol is crucial, even in cases where the cluster-based network design (CBND) network architecture produces a network that is simplified, reliable, and energy-efficient. In order to ensure that a legitimate UWSN is in charge of every cluster deployed in the UVWSN, which is securely set up to provide privacy and trustworthiness, the base station (BS) or the gateway (GW) authenticate the cluster head (CH) in this study. Furthermore, because the network's improved SDAA models ensure secure data transmission, the UVWSN network's communication data guarantees this. The primary contribution of this study is a new secure multi-mobile sink (MMS) approach for cluster-based network design (CBND). MMS minimizes communication overhead, including ships, and is utilized to organize suitable vehicle routes. This method minimizes latency/delay, improves the packet delivery ratio, and guarantees energy efficiency provision in UWSNs (underwater wireless sensor nodes).

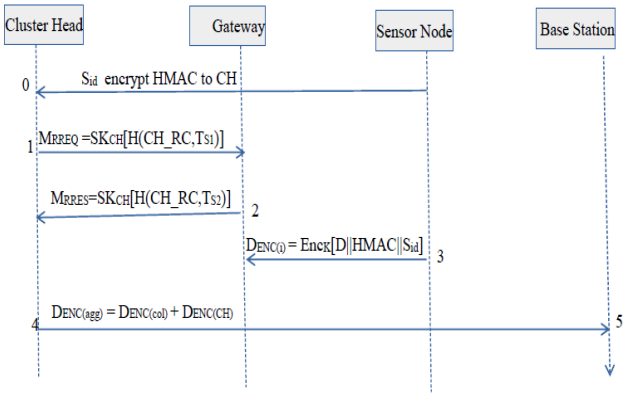


FIGURE 27. Process flow of SDAA [74].

This is in contrast to secure MAC protocols like SEFSC, SDA, and EEST, which don't take network energy efficiency into account and merely detect packet failures and delays. Using trusted encryption and decryption schemes to improve security, this scheme proposes a novel underwater vehicular sensor network (UVWSN) composed of underwater vehicles (UV) deployed in the network with the capability to identify and thwart malicious node attacks (MNA) in order to provide beneficial wireless sensor monitoring applications for the UV. Furthermore, the UVWSN guarantees total reliability, privacy, and integrity protection within the network.

8) SECURE AUTHENTICATION IN UWSNS

A secure data authentication and aggregation approach was suggested by the researchers in [75] for the UWSN cluster-based structure because cluster-based design creates a simplified and stable network. To make sure that legitimate nodes are managing each cluster, each cluster head is authenticated through a surface gateway. Secure handling of the data being communicated within the network will also help to prevent data compromise during network operations. This ensures that every node is secure, and that network communication is safe. This method lowers energy consumption and delay, which increases network data reliability. The primary contribution of this work is that the experiment reflects that SAPDA operates on real-time parameters. Increasing the number of sink nodes decreases latency and packet drop while increasing packet delivery ratio. Using trusted encryption techniques and a cluster-based approach that extends network lifetime, SAPDA demonstrates its dependability and security.

D. INTRUSION DETECTION

The research community's various intrusion detection systems for the UWSNs environment are analyzed in this section. Table 4 presents the analysis in tabular form as well.

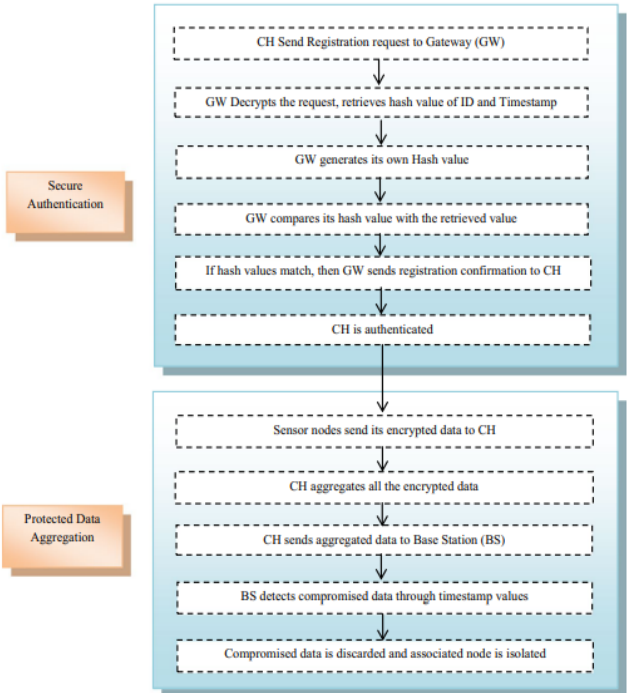


FIGURE 28. Block diagram of SAPDA [75].

1) SECURE INTRUSION DETECTION SYSTEM FOR UWSNS

The authors [76] provide details of a novel intrusion detection system that assigns real-time neighbor monitoring duties using Long Short-Term Memory (LSTM) and Integrated Secure MAC concepts. To keep data transmission protected, the proposed system applies Secure LSTM-MAC principles and Generative Adversarial Network (GAN) enabled UWSN channel assessment framework. The proposed approach in this study uses trained distributed agents to develop the intrusion detection system (IDS). These agents come equipped with the new LSTM-MAC engine, intrusion dataset, rule-based monitoring techniques, Two Fish algorithm, secure hashing algorithm-3 (SHA-3), and packet filtering capabilities, which are installed in every genuine sensor node. Adaptive MAC channel operations are driven by the suggested agent-based and LSTM model to prevent malicious traffic from reaching legal nodes. Furthermore, signal jamming, neighbor-based packet monitoring, and alert messaging protocols are employed in this work to construct dependable security systems that fend off various forms of threats. The suggested strategy outperforms the most current procedures across a variety of metrics, according to the outcomes of the experiments and observations, by 5% to 10%.

2) INTRUSION DETECTION FOR ROUTING IN UWSNS

A unique approach to intrusion detection known as DOIDS is suggested by research published in [78]. The core of this approach is density-based spatial clustering of applications with noise (DBSCAN). DOIDS is intended to identify and mitigate the attacks against opportunistic routing (OR)

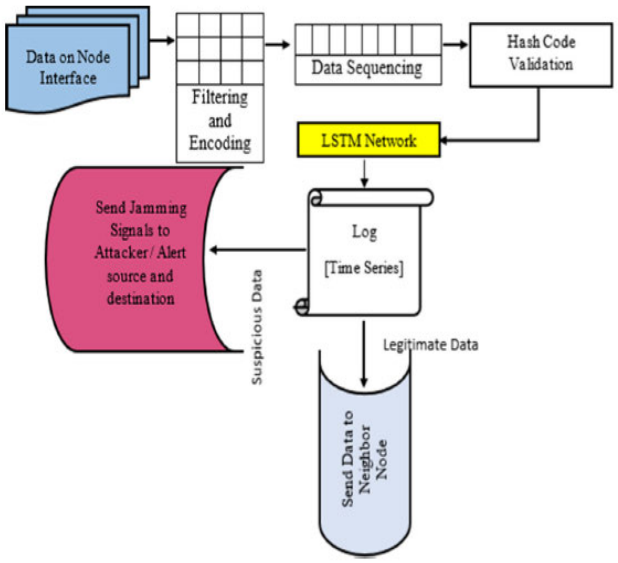


FIGURE 29. Supervising network data [76].

methods. The paper's main focus is on successfully identifying and mitigating the impact of a number of attack vectors that can be used against OR systems in UWSNs, such as Sybil, wormhole, selective forwarding and sinkhole attacks. The technique has been designed to be efficient against the attacks of both types such as random and selective and can be employed in a range of UWSN applications. Depending on the particular needs of the application, the plan can be executed on a variety of hardware and software platforms.

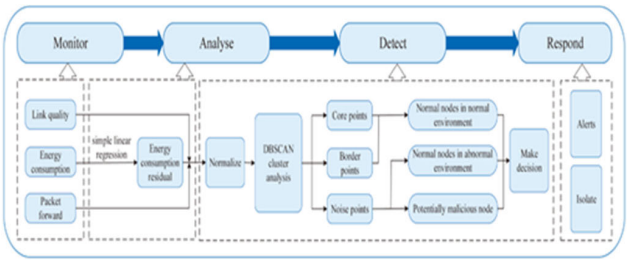


FIGURE 30. Framework for DOIDS [78].

3) INTRUSION DETECTION MODEL FOR UWSNS

In [77], authors presented an intrusion detection approach to protect underwater sensor networks from different types of attacks. Initially, neighborhood rough sets are used by cluster head nodes to extract features, and to minimize node processing, the reduced dimensional data is subsequently sent to sink nodes. Moreover, the data set is balanced, more minority class samples are included, and the minority class assault detection rate is raised with the application of the synthetic minority oversampling method (SMOTE). Ultimately, ascertain a node's trustworthiness based on the cluster head node's trust value. The classifier should then be trained using

the random forest technique to identify the kind of assault; this approach is not very good at detecting various kinds of intrusions. This study's primary contribution is that sensor nodes gather data from UWSNs, which will in fact gather an excessive amount of redundant and pointless data which will unavoidably burn up too much node energy. To address this issue, a neighborhood rough sets feature extraction technique is suggested, which lowers the dimensionality of security data and removes features that aren't really important. By employing the SMOTE synthetic minority oversampling approach to use the collected set of near-neighbor samples to interpolate the minority-type samples, it is possible to increase the number of minority-type samples in the imbalance data and enhance the detection accuracy of imbalance types. The issue where some data types' numbers differ excessively from those of other data types is resolved in this way. According to simulation results, the model can detect imbalance classes with an accuracy of more than 99% and enhance the effectiveness of intrusion detection of multi-type attacks.

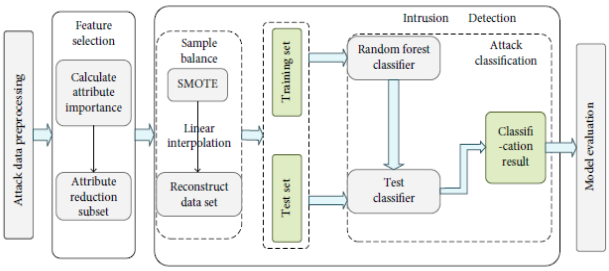


FIGURE 31. Schematic diagram of intrusion detection model process [77].

E. SECURE MAC TECHNIQUES FOR UWSNS

An examination of different secure MAC strategies put forth by researchers in relation to UWSNs is provided in this section. Furthermore, Table 4 presents the analysis tabularly.

1) MODES BASED SECURE MAC FOR UWSNS

A secure MAC protocol was proposed by the authors in [79]. In the context of UWSNs, the secure MAC technique aims to protect data confidentiality, and ensure authenticity, and integrity from attacks with less energy consumption. The fundamental working principle is that node A transmits RTSA to node B to occupy the channel before sending data to node B. After receiving RTSA, node B transmits CTSB back to node A, indicating that it is available for receiving. Here, node A sends out signals such as RTSA, which are detected by a malicious node C. Node A transmits data to node B, which node C receives as well once node B sends it the CTSB. However, the data is encrypted. Because node A and node B alone have the necessary security information, node C is unable to decode the data. Based on algorithms such as AES and ARIA, this study employs the CCM-UW mode. Comparing the proposed MAC protocol in this study to the existing MAC approaches, it is efficient in terms of transmission time and consumption of energy. The comparison is done using algorithms and security levels. Using a fish robot, the suggested process is put into practice in a real environment. The research's findings also demonstrate that while the results are not optimal, they may still be utilized as a starting point and offer enough information to support future study and the implementation of network security in the context of UWSNs. Figure 32 shows the secure MAC protocol's basic functionality.

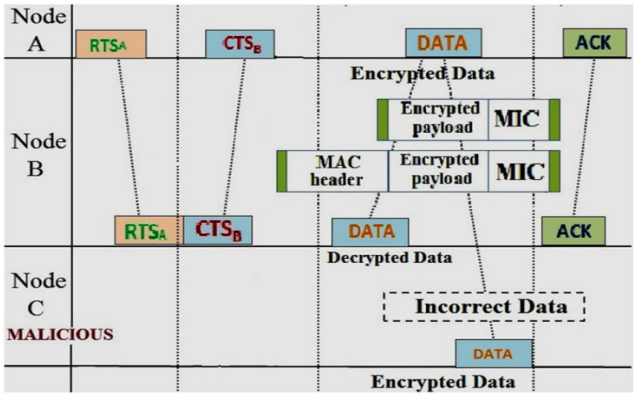


FIGURE 32. Basic operation of secure MAC [79].

2) CLUSTER-BASED SECURE MAC FOR UWSNS

A secure cluster-based MAC technique called SC-MAC was proposed by the authors of [80] for use in UWSN environments. Under hostile and difficult UWSN situations SC-MAC ensures security of data transmission. Replay, Sybil, and message manipulation attacks are all countered by SC-MAC. SC-MAC allows for the secure and dynamic creation and updating of clusters. For the purpose of extending the network's lifespan, the MAC layer data are utilized by taking into consideration the modem's battery and residual energy. Data transmission can be protected by the sensor nodes in different clusters when mutual authentication is successfully completed. An Aqua-Sim simulator is used to conduct the simulation for this study. The research's findings show that the suggested SC-MAC outperforms the current MAC protocols in terms of delivery ratio, network performance, and energy usage.

F. SECURITY FRAMEWORKS FOR UWSNS

The researcher's many frameworks and models for the UWSN environment are analyzed in this section. Table 4 presents the analysis in tabular form as well.

1) SECFUN

For UWSNs, the authors of [81] suggested the SecFUN security framework. The suggested framework combines the advanced encryption standard (AES) with the short digital signature algorithms, namely ZSS, Quartz, and BLS, in Galois counter mode (GCM) to provide the secure

authentication, non-repudiation, integrity, and confidentiality. To counter these threats, the researchers recommended implementing cross-layer security measures. The security framework in this study employs highly efficient cryptographic primitives. The recommended architecture is flexible and can be configured with different security settings to meet UWSN security requirements. The functionality of the channel-aware routing protocol (CARP) was extended in this work. The study's conclusions showed how effective the CARP secure version is in terms of latency and energy usage. Additional processing is required to implement security, but the UWSN environment has limited resources. As a result, energy-efficient security methods are needed for the UWSN environment in order for the solutions to remain usable there. In addition, it is imperative for the researchers to establish equilibrium between security and energy efficiency.

2) CRYPTOGRAPHIC SUITE FOR UWSNS

In [82], a cryptography suite is suggested for a clustered UWSN with mobile and stationary nodes in addition to a gateway. It is tried and examined further for an underwater vehicle team's group communication. It seeks to facilitate secure reconfiguration to manage node mobility, enabling a node to connect the network, begin a mission, and depart without difficulty following the event. Together with a set of cryptographic primitives (cipher, digest, and re-keying), the suite includes a secure routing protocol to enable secure underwater communication in one-to-one and one-to-many modes via the gateway. This is done while taking into consideration the characteristics of underwater acoustic channels, which are detailed below. The field testing' findings demonstrate how little energy and communication overhead the security measures cause. The encryption method in the suggested suite, called cipherText Stealing, modifies just the final two blocks of a plaintext's processing. In short, it basically "steals" a small amount of the ciphertext from the second-last block to pad the final plaintext block, which is then encrypted consistently without increasing the ciphertext size. By shortening the actual hash function value to 4 bytes, it minimizes overhead to roughly 4.4% of a standard UWAN message without compromising security. As seen in Fig. 33, a key-chain scheme including a collection of symmetric keys each one being the hash value of the key that before it in the key creation process lays the foundation for group key management. In other words, all prior keys in the key-chain can be computed given a key, but not the reverse ones. Here, the cluster keys are distributed using the SeFlood [8]. Additionally, it enables mobile nodes without increasing message overhead. Because nodes must periodically emerge in order to synchronize with GPS, it is believed that nodes are weakly time synchronized. The gateway eliminates the hacked node from the routing tables after canceling the group key and recalculates the relevant routes for secure data delivery.

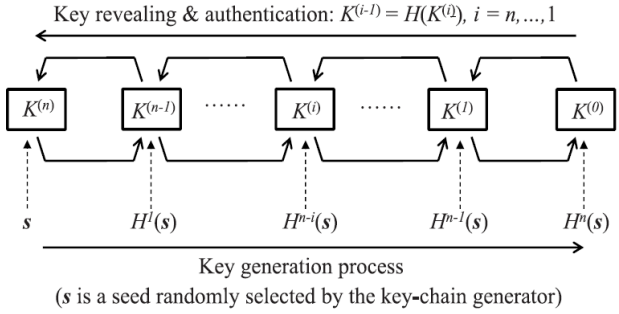


FIGURE 33. Key generation process [82].

3) REINFORCEMENT LEARNING-BASED TRUST MODEL

TUMRL is a novel reinforcement learning-based trust updating technique for UWSNs, according to the study's authors [83]. Using a specific environment model that oversees the trust score update process, the influence of the underwater environment is first measured. Next, the idea of key degree is presented as a means of protecting critical nodes by raising their strength of detection sensitivity to hostile attacks, given that the network's most significant nodes may be more susceptible to malicious attacks. Finally, by integrating reinforcement learning, the whole approach is integrated into a decision-making trust score update mechanism to accomplish efficient trust updating. The idea of key degree, which makes key nodes in the network more sensitive to trust and reduces losses from malicious attacks, and the environment model, which quantifies the abstract environmental influence as a probabilistic variable and is utilized to mitigate trust misclassification caused by environmental factors rather than offensive attacks, are the two main contributions of this research. Reinforcement learning is integrated into the environment model and the key degree approach to enhance the efficacy and adaptability of the trust update mechanism. The TUMRL workflow diagram is displayed in Figure 34.

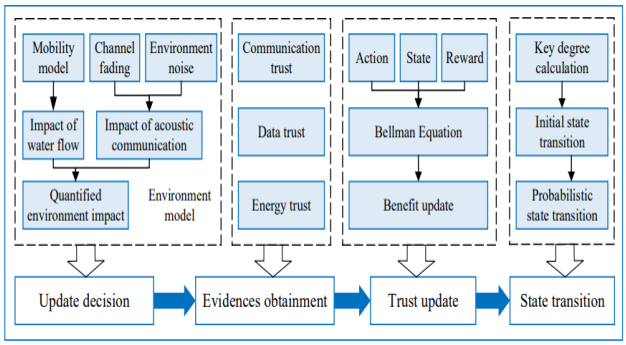


FIGURE 34. TUMRL Workflow Diagram [83].

4) FAULT-TOLERANT BASED TRUST MODEL FOR UWSNS

To guarantee secure and reliable data transmission in underwater acoustic sensor networks (UWSNs), the authors in [84] suggested a fault-tolerant trust model against hybrid attacks.

By fusing fault-tolerant data fusion with trust assessment, the model finds hostile nodes in the network and reduces their impact. Because UWSNs have particular obstacles because of the underwater environment, conventional trust models are inappropriate for these environments. The creation of a fault-tolerant trust model that is especially adapted to the needs and limitations of UWSNs represents the research's principal accomplishment.

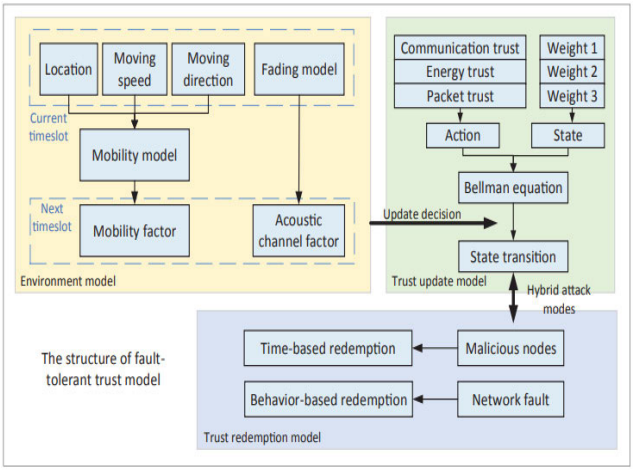


FIGURE 35. Architecture of fault-tolerant trust model [84].

It is demonstrated that the model is successful in identifying and reducing the impact of sensor node failures as well as single and coordinated attacks. The paper covers a variety of attack methods, including wormhole, selective forwarding, and node compromise attacks, that can be used against UWSNs. Even when there are malicious nodes present, the suggested trust architecture is made to provide secure and consistent data delivery, thwarting these types of attacks. Any UWSN that transmits data via acoustic communication can employ the suggested trust model. The model is appropriate for usage in a variety of UWSN applications since it is specially designed to be fault-tolerant and capable of functioning against both types of threats such as random and selective. The architecture of the fault-tolerant trust model is reflected in Figure 35.

5) TRUST CLOUD MODEL FOR UWSNS

A trust model known as TCM was suggested by the study done in [43] for the UWSN context. The available trust management strategies were thoroughly examined by the researchers. Based on trust calculation methodologies and concepts, the current trust management systems are divided into seven categories. These trust management strategies are based on fuzzy logic, probability, D-S evidence, entropy theory, subjective logic, cloud theory, and Bayesian theory. Owing to their unique characteristics, UWSNs cannot be effectively managed by the current trust management mechanism. TCM measures the degree of trust among sensor nodes. The sensor nodes can only transmit data through trustworthy sensor nodes since they can determine each other's trustworthiness based on measured results. The following factors are taken into consideration while evaluating TCM's performance: data transmission performance, trust value computation performance, and malicious node detection performance. TCM outperforms the other two trust models that are currently in use, according to the data. The architecture of the trust cloud model is depicted in Figure 36.

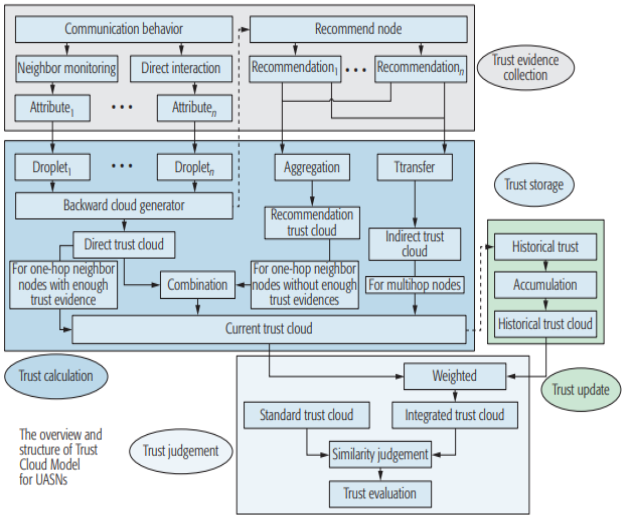


FIGURE 36. Architecture of TCM [43].

G. LOCALIZATION AND TIME SYNCHRONIZATION SECURITY

The various localization and time synchronization strategies put forth by the research community for the context of UWSNs are analyzed in this section. Table 4 presents the analysis in tabular form as well.

1) SECRET

The authors of this paper [85] proposed SecRET, an Evidence Theory-powered Secure Range-based localization technique for UWSNs. The proposed SecRET system uses trust-based computations to enable the unlocalized nodes to choose the most dependable collection of anchors with the least amount of resource consumption. As a result, the suggested plan can adapt to a variety of attacks in the context of UWSN. An NS-3 based performance study found that SecRET guarantees secure and effective localization even in the presence of compromised nodes vulnerable to various threats while maintaining the energy efficiency of the deployed nodes. This study's primary contribution is the authors' use of a DST-based trust model to model how anchor nodes and unlocalized nodes interact. For secure localization in UWSNs, the plan enables anchors to be independently discovered that are trustworthy and reliable. To assess a node's trust multi-dimensional trust metrics are used, including recommendations from surrounding nodes, residual energy, direct communication behaviors between nodes, and location data

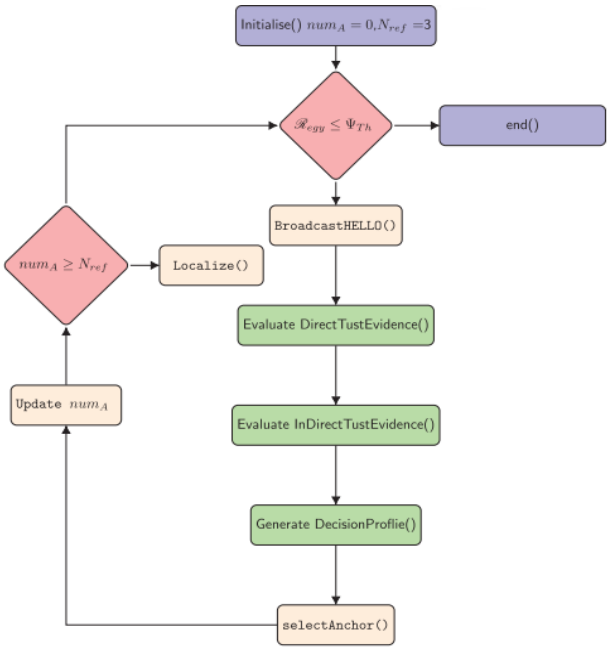


FIGURE 37. Flowchart representation of SecRET [85].

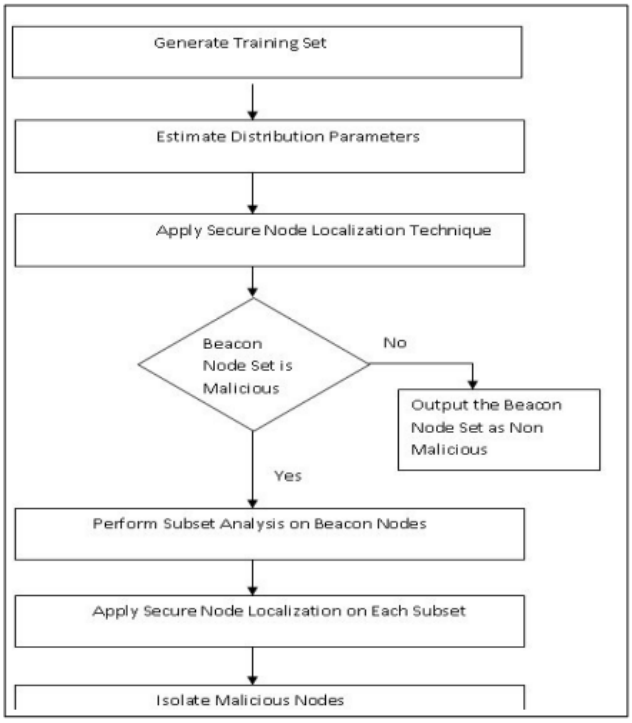


FIGURE 38. Secure localization flow diagram [86].

integrity. This procedure guarantees the suggested scheme's robustness. The suggested method successfully identifies malfunctioning nodes and achieves a high degree of security against a few significant threats in the hostile environment in UWSNs. The nodes in SecRET can retain energy efficiency while consuming less in the way of compute and communication. To meet the energy-efficiency requirements, the packet size is kept to a minimum by choosing appropriate and pertinent metrics for the trust evaluation. Figure 37 shows a flow representation of SecRET.

2) SECURE LOCALIZATION FOR UWSNS

The authors of this research paper [86] provide a secure localization framework based on a probabilistic model. This framework has a probabilistic system at its core. Furthermore, there are various challenges in the localization of underwater sensors networks discussed by [118] and [119]. The necessary training set is generated in order to estimate the parameters of the probabilistic scheme. The suggested probabilistic approach and PSO technique are used to carry out the malicious node isolation. The suggested framework is put into practice in MATLAB and contrasted empirically with the current framework. The suggested approach performs significantly better in terms of accuracy in isolating malicious nodes than the current mechanism. Figure 38 displays the secure localization flow diagram.

3) SECURE LOCALIZATION BASED ON GRADIENT DESCENT TECHNIQUE

By using a gradient descending technique, the authors of this study [87] enhanced the performance of a secure localization for underwater wireless sensor networks (UWSNs). The suggested approach uses a cooperative localization technique to lower the localization error in a noisy underwater environment by having each node determine its position based on the information it has received. Based on the data received from anchor nodes, each node may determine its location using the cooperative localization approach and then broadcast that location to its neighbors. This method, in addition to obtaining information about anchor nodes, each node can determine the distance it is from certain neighbor nodes whose location is already known. Consequently, the node can use the gradient descent technique and more information to decrease its localization error and locate itself. The distance between the anchor and regular nodes can be ascertained using any of the following methods: TOA, TDOA, hop count and RSS. Some other techniques have also been discussed by [116] and [117]. Emerging data aggregation techniques are given by [120]. Based on transmission losses, authors use the Lambert function to determine the distance between regular nodes and anchor nodes. The method's efficiency is demonstrated by the simulation results.

4) CLUSS

In this study [88], to provide synchronization security in hostile underwater environments against a range of attacks, including replay, Sybil, delay, and message manipulation attacks, a CLUster-based Secure Synchronization (CLUSS) protocol is presented. The three stages of CLUSS's time synchronization process are the authentication, intra- and inter-cluster synchronization, and synchronization phases. During the authentication procedure, regular nodes authenticate to

TABLE 4. Analysis of security mechanisms in UWSNs.

S.No.	Technique	Issue Addressed	Major Contribution	A	B	C	D	Protection from Attacks
1.	**Efficient Channel Access Model for Detecting Reactive Jamming for Underwater Wireless Sensor Network [21]**	Cooperative Detection of Reactive Jammer in UWSN	Presented an innovative cross-layer design for cooperative communication for detecting jamming and an effective channel allocation scheme.	Yes	yes	No	yes	Jamming
2.	**Mitigating Blackhole attack of Underwater Sensor Networks [111]**	Identify the presence of Black holes	Suggested a method for preventing blackhole attacks that involves grouping nodes into clusters and choosing coordinator nodes from each cluster to determine whether any blackholes are present in that cluster. To authenticate and confirm nodes, we employed the challenge-response technique and public-key cryptography.	No	yes	No	yes	Blackhole
3.	**Wormhole Attack Detecting in Underwater Acoustic Communication Networks [112]**	Detection of Wormhole	An analysis is conducted on the suggested wormhole attack detection technique in the Underwater Acoustic Communication Network, which utilizes azimuth measurement technology. Azimuth or distance outliers are used to assess the existence of wormhole attacks.	No	Yes	No	NO	Wormhole
4.	**A Blockchain-Based Scheme for Sybil Attack Detection in Underwater Wireless Sensor Networks [110]**	Sybil attack detection	Suggested a Sybil attack detection system for UWSN based on blockchain technology. To strengthen it against the detection of attacks, the authors have additionally combined the blockchain-based approach with a trust management model based on the Hidden Markov model.	No	No	No	No	Sybil
5.	**Data centric approach to analyzing security threats in Underwater Sensor Networks [34]**	Denial of Service	Suggested using a specific algorithm to identify and disconnect any potentially malicious nodes. In addition, the authors present machine learning methods for assessing detection criteria over time in order to better withstand numerous mobile attackers.	No	No	Yes	Yes	Denial of Service (DoS)
6.	**A Lightweight Cryptographic Algorithm for Underwater Acoustic Networks [60]**	Addressed secure communication by using encryption in UASNs.	Developed a cryptographic method that is lightweight and especially designed to meet the needs and limitations of UWSNs. It is demonstrated that the method maintains minimal computational and energy costs while offering a high degree of security.	No	yes	No	No	Eavesdropping, message Modification, and Impersonation attacks

cluster heads and cluster heads authenticate to beacons. In the intra-cluster and inter-cluster synchronization phases, CLUSS isolates the propagation delay of uplink due to node mobility from that of downlink to improve the precision of time synchronization. Furthermore, to minimize the number of messages created during synchronization, portions of these two stages may be carried out concurrently. Through simulations, we show that CLUSS can, under various conditions, reduce both synchronization errors and energy usage when compared to standard protocols.

TABLE 4. *(Continued.)* **Analysis of security mechanisms in UWSNs.**

7.	**An Ultra-Lightweight Encryption Scheme in Underwater Acoustic Networks [58]**	Addressed the issue of lightweight encryption algorithm for UASNs environment.	A lightweight cryptographic technique is proposed for the context of UWSNs. AES modification to enable UWSN compatibility. The suggested method is energy-efficient and offers strong security with little overhead.	No	Yes	Yes	Yes	Brute force and other Adverse attacks.
8.	**Security in Underwater Acoustic Sensor Network: Focus on Suitable Encryption Mechanisms. [59]**	Addressed suitability of algorithms for UWASNs environment.	Discussed appropriate algorithms for UWASN security. The authors recommended a less amount of data overhead while implementing security in UWASNs. suggested use the CMVP algorithm.	No	Yes	Yes	No	Attacks on Encryption in UWSNs.
9.	**MO-CBACORP: A new energy-efficient secure routing protocol for underwater monitoring wireless sensor network [66]**	Addressed the issue of routing security with energy efficiency for UWSNs environment.	Presented MO-CBACORP, a novel multi-objective chaotic Boltzmann ant colony optimization routing protocol. This can considerably improve routing security and reduce system latency by minimizing the energy consumption of sensor nodes in UWSN routing.	No	No	No	Yes	Black hole attack in UWSNs.
10.	**Secure routing in underwater acoustic sensor networks based on AFSA-ACOA fusion algorithm [61]**	Addressed the issue of secure routing in UWSNs.	Created a secure routing method that can guarantee the availability, confidentiality, and integrity of data transmission in UWSNs. This algorithm is based on the AFSA-ACOA fusion technique.	No	No	No	No	Packet Dropping, Sybil and Replay attacks
11.	**DESLR: Energy-efficient and secure layered routing based on channel-aware trust model for UASNs [67]**	Addressed the issue of secure routing in UWSNs	Utilizing a two-layer fuzzy logic method to choose CHs and fuse data, a unique layered clustering strategy is developed and used to group nodes into clusters. Furthermore, a channel-based trust prediction technique that takes into consideration both direct and indirect trust metrics is employed to identify malicious nodes. Lastly, an energy-efficient and low-latency routing method based on an improved ACOA is suggested in order to find the best routing path.	No	Yes	Yes	Yes	Insider attacks and Identification of malicious nodes.
12.	**A Secure Routing Scheme for Underwater Acoustic Networks [62]**	Addressed the issue of a secure routing approach for UWSNs.	Suggested a secure route for UWSNs. For source and destination node authentication, a signature scheme is suggested. A trap-door mechanism is employed to ensure the nodes' anonymity.	No	Yes	Yes	Yes	Forgery attacks and improves the overall security.

5) WATER SYNC

This study's authors [89] proposed the water quality monitoring system (water) model, which is low-energy, scalable, and delay-tolerant. What sets the water model apart from terrestrial radio sensor networks is its mobility, lengthy propagation delay, and high variability. The authors suggest a lightweight time synchronization system in order to obtain satisfactory timestamp accuracy in the vertical direction. However, among other network attack methods, malicious actors can trick water quality monitoring in water platforms via replay, wormhole, sybil, and byzantine assaults. In order to identify nodes executing internal assaults that

TABLE 4. *(Continued.)* **Analysis of security mechanisms in UWSNs.**

13.	**SEECR: Secure energy efficient and cooperative routing protocol for underwater wireless sensor networks [63]**	Addressed the issue of secure and energy efficient routing approach for UWSNs.	A secure and energy-efficient routing technique for UWSNs is suggested. Taking into account the constrained resources of UWSNs, minimum calculations are employed.	No	No	No	Yes	Attacks that Drop Packets
14.	**Securing underwater sensor networks against routing attacks [36]**	Addressed combating routing attacks in UWSNs via distributed approach.	Suggested a centralized method for managing vulnerabilities in UWSN configuration attacks. To capture the interplay between the many contributing factors, an analytical model is developed. This study, however, does not address how to identify and address additional security flaws in UWSNs.	Absent	No	No	Yes	Wormhole and Sinkhole attack
15.	**Wormhole-Resilient Secure Neighbor Discovery in Underwater Acoustic Networks [64]**	Addressed the issue of secure neighbor discovery in UASNs.	A suite of protocols is suggested for UWSNs' secure neighbor discovery. The direction of arrival (DoA) signals approach serves as the foundation for the suggested methods.	No	Yes	Yes	No	Wormhole
16.	**A Secure Communication Suite for Underwater Acoustic Sensor Networks [8]**	Addressed the issue of secure routing for UASNs.	Cryptographic primitives and secure routing protocol are part of the proposed SeFLOOD scheme. Because of its low overhead and power consumption, the proposed protocols suite is appropriate for use with UWSNs.	Yes	No	Yes	No	Provide Integrity and Confidentiality in UASNs against attacks.
17.	**Secure Communication in Mobile Underwater Wireless Sensor Networks [65]**	Addressed various DoS attacks in mobile UWSNs environment	A simulated flooding attack on UWSNs is conducted, and the effects it has on the networks' performance are examined. It has been determined that methods appropriate for a WSN setting are inappropriate for a UWSN setting.	No	Yes	No	No	Various DoS attacks such as Man in the Middle attack, and Flooding attack
18.	**Enhancing Security and Efficiency in Underwater Wireless Sensor Networks: A Lightweight Key Management Framework [68]**	Addresses the issue of Key generation, distribution and revocation.	A lightweight secure key management system for UWSNs is suggested. Along with lightweight implementation and scalability, the proposed framework contains mechanisms for key distribution, revocation, authentication, and creation. Leverages the Certificate Revocation List (CRL) for key revocation and an elliptic curve-based technique for key distribution.	No	Yes	No	Yes	Prevent unauthorized access. Ensures Confidentiality, Integrity and Non-Repudiation.
19.	**A Computationally Efficient Online/Offline Signature Scheme for Underwater Wireless Sensor Networks [69]**	Secure and efficient signature schemes in UWSNs.	Design of an online/offline signature system that is specifically suited to the needs and limitations of UWSNs and is computationally efficient. It is demonstrated that, in comparison to conventional signature methods, the scheme may decrease the computing overhead of signature verification by up to 90%.	No	Yes	Yes	Yes	Provide protection against Node Compromise attack and Message Modification attack by providing data Integrity and Authenticity

TABLE 4. *(Continued.)* **Analysis of security mechanisms in UWSNs.**

20.	**An Energy-Efficient Key Agreement Mechanism for Underwater Sensor Networks [70]**	Energy efficient key agreement mechanism having less overhead designed for UWSNs.	Resistance towards various active attacks. Produced positive outcomes in terms of network security and performance. Low-performance nodes' energy usage was greatly decreased.	No	Yes	Yes	Yes	Sybil attack, Spoofed attack, Node replication and Replay attack.
21.	**Key Distribution Scheme for Peer-to-Peer Communication in Mobile Underwater Wireless Sensor Networks [71]**	Addressed the key distribution problem of UWSNs.	Utilized two mobility models meandering and nomadic. Increased security performance.	No	Yes	Yes	Yes	When sensor nodes are captured by an adversary the resiliency performance is good. Reduces the number of links compromised.
22.	**A Cluster-based Key Management Scheme for Underwater Wireless Sensor Networks [72]**	Addressed the mobility and security issues in the UWSN environment.	A novel communication architecture is suggested to effectively manage the mobility of sensor nodes. CKP offers integrity, freshness, confidentiality, and authentication.	NO	Yes	No	Yes	Minimize the effect of self-compromised nodes and resist against insider threats.
23.	**End-to-End Authentication in under-Water Sensor Networks [73]**	Addressed the authentication problem of UWSNs environment	Analyzed ZSS, ECDSA, and BLS, three distinct digital signature methods. It is found that the primary factor influencing UWSN energy efficiency is the use of both aggregate and brief signatures.	No	No	No	Yes	End-to-end authentication.
24.	**SDAA: Secure Data Aggregation and Authentication Using Multiple Sinks in Cluster-Based Underwater Vehicular Wireless Sensor Network [74]**	Addressed the authentication issue in cluster-based UVWSNs	Using MMS (multiple mobile sinks) in the cluster-based network design (CBND), suggests a novel secure SDAA technique. MMS is used for proper vehicle path planning, particularly on ships. It eliminates latency and delay, avoids communication overhead, and ensures energy efficiency, all of which enhance packet delivery ratio and lower packet drop in the network. Reliability is also ensured. Attacks by malicious nodes of any kind can be identified and stopped using this strategy.	No	Yes	No	Yes	Detect and prevent all forms of malicious node attacks.
25.	**SAPDA: Secure authentication with a protected data aggregation scheme for improving QoS in scalable and survivable UWSNs [75]**	Addressed the authentication issue in cluster-based UWSNs	Real-time parameters are the foundation of Secure Authentication and Protected Data Aggregation (SAPDA), and they are also used in experiments. Using sink nodes several times improves the packet delivery ratio and lowers latency and packet drop. Its use of reputable encryption techniques demonstrates its dependability and security. Utilizing the cluster-based strategy extends the life of the network.	No	No	Yes	No	Node Compromise attack.

are distinct from external attacks in that they necessitate the complete disclosure of keying materials, a correlation-based security model is presented by authors for detecting outlier timestamp data. Our time synchronization protocol's dependability is reinforced by this model. Assuming the attackers have already obtained the water sensors and are aware of the keying materials, the correlation-based security approach can also foil numerous insider attacks. Extensive

TABLE 4. *(Continued.)* **Analysis of security mechanisms in UWSNs.**

26.	**Secure and optimized intrusion detection scheme using LSTM-MAC principles for underwater wireless sensor networks [76]**	Addressed intrusion detection technique that can detect attacks in UWSNs.	The capabilities for neighbor-based packet monitoring, signal jamming, and the use of warning messaging protocols to create dependable security services against various attack types are the main benefits of the suggested intrusion detection system.	No	yes	Yes	No	Selective Jamming and Neighbor-based attack monitoring.
27.	**DOIDS: An Intrusion Detection Scheme Based on DBSCAN for Opportunistic Routing in Underwater Wireless Sensor Networks [78]**	Addressed effective intrusion detection schemes that can detect and mitigate attacks in OR schemes in UWSNs.	Designed the DOIDS intrusion detection system, which is intended to identify and mitigate attacks in UWSNs' OR schemes. It is demonstrated that the plan is successful in identifying and mitigating the impact of a variety of attacks, such as wormhole, sinkhole, and selective forwarding assaults.	Yes	No	Yes	Yes	Selective forwarding attacks, Sinkhole attacks, Wormhole attacks, and Sybil attacks.
28.	**Research on the Intrusion Detection Model of Underwater Sensor Networks [77]**	Addressed intrusion detection technique that can detect attacks in UWSNs.	Four potential attack types are investigated in the proposed model, which successfully identifies different kinds of attack risks in wireless sensor networks. Additionally, a random forest-based intrusion is included. The suggested detection technique aims to enhance the detection accuracy of various sorts of attacks and efficiently identify a multitude of attack means.	No	Yes	No	No	DoS, Blackhole, Grayhole, Flooding and Selective Forwarding attacks
29.	**CCM-UW Security Modes for Low-Band Underwater Acoustic Sensor Networks [79]**	Addressed the issue of secure MAC protocol for UASNs.	Recommended MAC protocol, appropriate for UWSNs and secure. The proposed protocol is energy-efficient and secure in terms of transmission time.	No	Yes	yes	yes	Replay Attack
30.	**Towards a Secure Medium Access Control Protocol for Cluster-Based Underwater Wireless Sensor Networks [80]**	Addressed the issue of secure MAC protocol for UWSNs	Suggested secure MAC protocol for cluster-based UWSNs. SC-MAC guarantees data security during transmission in challenging and severe UWSN conditions.	No	yes	Yes	No	Replay, Sybil, and Message Manipulation attacks.
31.	**SecFUN: Security framework for underwater acoustic sensor networks [81]**	Addressed confidentiality, integrity, authentication, and non-repudiation in UASNs.	SecFUN is a suggested security framework for UWSNs. The suggested secure version of CARP is effective in terms of latency and energy efficiency.	Yes	No	Yes	Yes	Sybil, Hello flood, Acknowledgement spoofing, Replay attack, Exhaustion, Selective forwarding, and Sinkhole attack.
32.	**A cryptographic suite for underwater cooperative applications [82]**	Addressed the problem of secure cooperation among UWAVs.	Presented a cryptographic tool capable of minimizing the message overhead that security adds. Vehicle authentication, message integrity and secrecy, and key management are all provided by the cryptography suite.	Yes	No	No	Yes	DoS, Spoofing and Snooping attacks.

tests ensure security methods' effectiveness. Underwater sensor systems used by the military and navy depend heavily on the proposed secure time synchronization technique or WATERSYNC.

TABLE 4. *(Continued.)* **Analysis of security mechanisms in UWSNs.**

33.	**A Trust Update Mechanism Based on Reinforcement Learning in Underwater Acoustic Sensor Networks [83]**	Addressed the issue of trust management among underwater sensor nodes.	The suggested method detects compromised nodes with reliability. With higher densities, the suggested design is more energy-efficient and has a reduced false alert rate.	Yes	No	No	Yes	DoS, Selective forwarding and Packet tampering
34.	**The fault-tolerant trust model for hybrid attack mode in underwater acoustic sensor networks [84]**	Addressed the need for a fault-tolerant trust model for UASNs.	Created a fault-tolerant trust architecture especially suited to the limitations and needs of UASNs. It is demonstrated that the model is successful in identifying and mitigating the impact of sensor node failures as well as isolated and coordinated attacks.	Yes	No	No	Ye	Protect Node Compromise attacks, Selective forwarding attacks, and Wormhole attacks.
35.	**A trust cloud model for underwater wireless sensor networks [43]**	Addressed the trust establishment problem among nodes in UWSNs.	TCM trust model for UWSNs is proposed. TCM models perform significantly better than LCT and CBTM models.	No	Yes	Yes	No	Malicious sensor node in UWSNs.
36.	**SecRET: Secure Range-based Localization with Evidence Theory for Underwater Sensor Networks [85]**	Addressed the issue of localization security	The suggested plan can adapt to a wide range of UWSN environment attacks. NS-3-based performance study shows that, even in the presence of compromised nodes targeted by different attacks, SecRET preserves the deployed nodes' energy efficiency while guaranteeing efficient and secure localization.	No	Yes	Yes	No	Denial-of-service (DoS), Selective forwarding, Impersonation and Data modification attacks.
37.	**Secure Localization for Underwater Wireless Sensor Networks Based on Probabilistic Approach [86]**	Addressed the issue of false localization information threat problem.	A probabilistic model-based secure localization framework is proposed and shown. Empirical evidence shows that the suggested localization framework performs significantly better in terms of security efficacy than the current paradigm.	No	Yes	Yes	Yes	False Localization Information threat, Location Spoofing
38.	**Gradient descent approach to secure localization for underwater wireless sensor networks [87]**	Addressed the issue of false localization information threat problem.	Suggested a secure localization plan using a gradient descent technique that included a stage for selective pruning to get rid of inaccurate data from the underwater sensor network. We proposed a cooperative framework where regular nodes assist each other in localizing in order to reduce localization error.	No	Yes	No	No	False Localization Information threat, Location Spoofing

VI. DISCUSSION

A significant portion of the primary research discusses novel algorithms [8], [60], [66] and security models [73], [79], [83] in order to handle a specific threat or class of attacks. The remaining papers address security issues and major research challenges [3], [10], [48], [90], [90], as well as the demonstration and classification of threats and attacks, including denial-of-service (DoS), localization, and routing attacks [30], [32], [33], [90]. For the most part, simulations are used to assess these investigations. The peculiarities of UWSN, which significantly distinguish its operation and security issues from those of its terrestrial counterpart in terms of location, node mobility, consumption of energy and maintenance, are a recurring theme in most of the primary

TABLE 4. *(Continued.)* **Analysis of security mechanisms in UWSNs.**

39.	**A cluster-based secure synchronization protocol for underwater wireless sensor networks [88]**	Addressed the issue of false time synchronization information threat problem.	Suggested the use of a CLUster-based Secure Synchronization (CLUSS) protocol to protect synchronization against a variety of attacks, such as replay, delay, Sybil, and message manipulation attacks, while operating in hostile underwater environments.	No	Yes	Yes	Yes	Desynchronization, Sybil, Replay, message Manipulation, Delay, and Modification attacks
40.	**Correlation-based security in time synchronization of sensor networks [89]**	Addressed the issue of false times synchronization information threat problem.	Suggested a scalable, energy-efficient, and secure WATER time synchronization service that can withstand significant and wildly fluctuating acoustic propagation delays. By using a correlation-based security model to identify nodes performing insider attacks and detect outlier timestamp data, this approach seeks to make our time synchronization protocol secure.	No	Yes	No	No	Desynchronization, Sybil, Replay, Wormhole and Manipulation attacks

A: Cross-Layer Design **B:** energy consumption
C: latency **D:** detection accuracy under attack scenario

research. Most researchers concur that terrestrial WSN security measures are not always transferable to UWSNs. Because UWSNs operate over greater distances and require more sophisticated signal processing than their terrestrial equivalents, they are more power-hungry and have limited hardware resources (computation, energy, and storage capacity) [10]. In addition, the unstable communication route resulting from the acoustic channel's smaller bandwidth combined with unprotected and sometimes unmonitored makes channels more vulnerable to hostile and eavesdropping assaults [10]. Numerous strategies, such as game theory, encryption, statistics, machine learning and modification of pre-existing networking algorithms, have been put forth to address the issues.

A. PHYSICAL EXPERIMENTATION

The majority of research projects that proposed security methods are assessed using simulations, most of which have predetermined constraints. Simulations are unquestionably useful for experimental research since they offer a time-effective and economical way to test novel ideas. However, the simulation software does not accurately represent the actual behavior due to the unpredictability of the underwater environment, which allows for errors. It would be feasible to do further physical experiments to assess the effectiveness of the suggested security measures. This could provide a more comprehensive outcome of these solutions' performance.

B. EFFECT OF SECURITY ON OTHER SYSTEM PARAMETERS

It is important to remember that enhancing a system's security will inevitably result in more overhead and implications. Any system's overall performance is the result of a complex interplay between many system parameters, so it's critical to examine how security affects pertinent performance metrics like reliability, energy efficiency, and throughput. As given by the table 4 security related algorithm does not address all the issues related to underwater networks, such as energy consumption cross-layer design and latency. Enhancing the security sometimes increase the computational overhead, which may cause the latency. Additionally, mechanisms should be developed, and the compromise between security measures and energy, throughput, and spectrum efficiency should be carefully examined in order to determine how much it will cost to implement a security measure at the desired level of security.

C. CRYPTOGRAPHIC SUITES

The objective of the developed UWSN secure communication suites is to improve the authenticity, confidentiality and integrity of data within the nodes and during transmission. However, due to the insecure exchange of the secret keys needed for encryption and decryption, spoofing attacks continue to occur against these protocols. It is important for any crypto suit that how it works under different attacks, a nicely design encryption technique is one that can able to handle different types of attacks. Given by table 4 not all the algorithm can able to give security under many attacks. Therefore, it is necessary to create a cryptographic suite that is more effective than the ones that are already in use.

D. UPPER LAYER UWSN SECURITY

Applications or transport layers can offer upper-layer security. The aforementioned discussion demonstrates that, while

taking into consideration unique UWSN properties, UWSN security schemes examined thus far have mostly focused on the low three levels (Physical, Data, and Network). It is challenging for the lower layers to provide end-to-end security on their own, though. In addition to making intermediate nodes' job of securing UWSNs easier, an effective upper-layer security scheme can offer customized security services that are made to meet the unique needs of every application. But as was already indicated, the complexity of the current upper-layer security techniques increases with cipher expansion, leading to increased bandwidth and energy consumption.

E. CROSS-LAYER

As the discussion above demonstrates, single layer security techniques are the subject of 95% of security algorithm research conducted in UWSN. The algorithms for layer security are limited to a single layer. It is not possible to say that these layer-specific algorithms have completely defensive methods because cross-layer attacks occur on the network. The use of single layer security methods for UWSN has a number of disadvantages, such as the rapid depletion of network resources if countermeasures against an attack are calculated independently for every layer. The inability of single layer security algorithms to react to alterations in UWSN topology, failure of node, and other related issues is another disadvantage of the technology. Since node's energy is a valuable resource for UWSN, it is crucial to design cross-layer security mechanisms while maintaining a comprehensive network perspective.

F. SECURE LOCALIZATION & TIME SYNCHRONIZATION

Since there are no Global Positioning System (GPS) signals underwater, localization and time synchronization remain a crucial concern for underwater nodes. Localization attacks like Sybil and Wormhole, which have been revealed recently, have the ability to inflict great harm by using or altering the localization data. Cryptographic techniques must be designed with efficiency and effectiveness to prevent the injection of false localization information into UWSNs [85], [86]. On the other hand, appropriate cryptographic algorithms must be created in order to protect against attacks on time synchronization, such as manipulation, replay and masquerading [88].

VII. CONCLUSION

This study examines the different security mechanisms for detection and mitigation in UWSNs, which are typically installed in challenging underwater conditions with significant energy usage and limited network resources. This study addresses prevalent attacks, classification of attacks using a layered approach and their countermeasures, strategies for secure MAC and Secure routing, encryption algorithms framework that require less computing power and cryptographic overhead, key management schemes practical for UWSNs, Intrusion detection, and trust management models. Some UWSN characteristics also present difficulties for attackers and ought to be used to strengthen UWSN security. The issues addressed, significant contributions, and potential avenues for future research are thoroughly explored. Keep in mind that most of the strategies are based on theoretical research. UWSN conditions are dynamic and complicated, making it challenging to model them effectively. Field testing is the most reliable way of validation. As a result, more study with real-world testing is required because UWSN security research is still in development. Various applications have different security needs, that must be taken into consideration while developing workable UWSN security schemes. In this situation, a strategic approach for effective coordination between different tiers is crucial to optimize the consumption of resources to achieve the security strength that is required and ensure the sustainability of the solution for the UWSN environment. A UWSN may be tailored for a specific application.

A. FUTURE GAPS AND CHALLENGES

Now a days under water sensors networks has gained a lot of attentions and that is why a numerous growth can be seen in this area. But still there a chance of improvement in UWSNs mainly its implementation of the wide area or huger environment. For the large area networks, it is required by the researchers to apply more algorithms that can produced more accurate solutions. The experiments should be performed in large surroundings to see the effect of network connectivity that should long-lasting. It is very important in UWSNs that the neighborhood range should be wider with better coverage, low energy consumption.

A study in future should focus on the underwater vehicles with the improved communication in terms of autonomy level and channel bandwidth. A models should be generated for these underwater vehicles that analyzes the environment of UWSNs in wide range of experimental area. Also, the study should be done for high level of planning layer to match with the surroundings of the vehicles. It is also required by the researcher that try to design the experimental setup in more complex environment that consider multipath, shadowing and mobility and see the results. Analysis of results in more complex networks should be done to see its effects related to surroundings.

The idea of using the deep learning technique for the localization in underwater could be more reliable as compare to the existing techniques.

UWSNs can be used for many different purposes, such as military, civic, and more. The application and study of UWSNs are becoming more and more common in industry and academia. There are still a lot of unanswered questions after looking at recent advancements, studies, and research gaps that were previously mentioned. These are covered in brief in the subsections that follow.

In the last, it more important to see effect of hybrid harvesting energy in the ocean environment. The application of

harvest can bring more stability and reliability in the hostile marine environment.

REFERENCES

[1] J. Heidemann, W. Ye, J. Wills, A. Syed, and Y. Li, "Research challenges and applications for underwater sensor networking," in *Proc. Wireless Commun. Netw. Conf.*, Apr. 2006, pp. 228–235.

[2] C. Yuan, W. Chen, and D. Li, "A hierarchical identity-based signcryption scheme in underwater wireless sensor network," in *Proc. China Conf. Wireless Sensor Netw.* Berlin, Germany: Springer, 2017, pp. 44–54.

[3] M. C. Domingo, "Securing underwater wireless communication networks," *IEEE Wireless Commun.*, vol. 18, no. 1, pp. 22–28, Feb. 2011.

[4] S. S. Kasture and N. Gudpelliwar, "Securing underwater wireless communication networks-literature," *Int. J. Sci. Eng. Res.*, vol. 7, no. 2, pp. 73–78, 2018.

[5] R. Hunt, "Network security—Systems and architecture 2003," in *Proc. Total Focus Conf.*, Singapore, Mar. 2003, pp. 729–752. [Online]. Available: http://www.cosc.canterbury.ac.nz

[6] Y. W. Law, J. Doumen, and P. Hartel, "Survey and benchmark of block ciphers for wireless sensor networks," *ACM Trans. Sensor Netw.*, vol. 2, no. 1, pp. 65–93, Feb. 2006.

[7] Y. Liu, J. Jing, and J. Yang, "Secure underwater acoustic communication based on a robust key generation scheme," in *Proc. 9th Int. Conf. Signal Process.*, Beijing, China, Oct. 2008, pp. 1838–1841.

[8] G. Dini and A. L. Duca, "A secure communication suite for underwater acoustic sensor networks," *Sensors*, vol. 12, no. 11, pp. 15133–15158, Nov. 2012.

[9] D. R. K. Mary, E. Ko, S.-G. Kim, S.-H. Yum, S.-Y. Shin, and S.-H. Park, "A systematic review on recent trends, challenges, privacy and security issues of underwater Internet of Things," *Sensors*, vol. 21, no. 24, p. 8262, Dec. 2021, doi: 10.3390/s21248262.

[10] G. Yang, L. Dai, and Z. Wei, "Challenges, threats, security issues and new trends of underwater wireless sensor networks," *Sensors*, vol. 18, no. 11, p. 3907, Nov. 2018.

[11] Y. Z. Dong and P. X. Liu, "Security considerations of underwater acoustic networks," in *Proc. Int. Congr. Acoust. (ICA)*, Sydney, NSW, Australia, Aug. 2010, pp. 1–4.

[12] D. Yangze and L. Pingxiang, "Security analysis on underwater acoustic networks," in *Proc. Oceans*, Yeosu, South Korea, May 2012, pp. 1–4.

[13] Y. Dong, H. Dong, and G. Zhang, "Study on denial of service against underwater acoustic networks," *J. Commun.*, vol. 9, no. 2, pp. 135–143, 2014.

[14] P. A. van Walree and R. Otnes, "Ultrawideband underwater acoustic communication channels," *IEEE J. Ocean. Eng.*, vol. 38, no. 4, pp. 678–688, Oct. 2013.

[15] J. A. Catipovic, "Performance limitations in underwater acoustic telemetry," *IEEE J. Ocean. Eng.*, vol. 15, no. 3, pp. 205–216, Jul. 1990.

[16] J. Catipovic, D. Brady, and S. Etchemendy, "Development of underwater acoustic modems and networks," *Oceanography*, vol. 6, no. 3, pp. 112–119, 1993.

[17] C. Karlof, N. Sastry, and D. Wagner, "TinySec: A link layer security architecture for wireless sensor networks," in *Proc. 2nd Int. Conf. Embedded Networked Sensor Syst.*, Baltimore, MD, USA, Nov. 2004, pp. 162–175.

[18] P. N. Mahalle, P. A. Shelar, G. R. Shinde, and N. Dey, "Threats and attacks in UWSN," in *The Underwater World for Digital Data Transmission*. Singapore: Springer, 2021, pp. 43–53.

[19] V. V. Kimbahune, A. V. Deshpande, and P. N. Mahalle, "Lightweight key management for adaptive addressing in next generation internet," *Int. J. Ambient Comput. Intell.*, vol. 8, no. 1, pp. 50–69, Jan. 2017.

[20] M. Zuba, Z. Shi, Z. Peng, and J.-H. Cui, "Launching denial-of-service jamming attacks in underwater sensor networks," in *Proc. 6th ACM Int. Workshop Underwater Netw.*, 2011, pp. 1–5.

[21] S. Bagali and R. Sundaraguru, "Efficient channel access model for detecting reactive jamming for underwater wireless sensor network," in *Proc. Int. Conf. Wireless Commun. Signal Process. Netw. (WiSPNET)*, Mar. 2019, pp. 196–200.

[22] L. Xiao, Q. Li, T. Chen, E. Cheng, and H. Dai, "Jamming games in underwater sensor networks with reinforcement learning," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2015, pp. 1–6.

[23] S. Misra, S. Dash, M. Khatua, A. V. Vasilakos, and M. S. Obaidat, "Jamming in underwater sensor networks: Detection and mitigation," *IET Commun.*, vol. 6, no. 14, p. 2178, 2012.

[24] P. Dewal, G. S. Narula, V. Jain, and A. Baliyan, "Security attacks in wireless sensor networks: A survey," in *Cyber Security* (Advances in Intelligent Systems and Computing), vol. 729, 2018, pp. 47–58.

[25] W. Znaidi, M. Minier, and J.-P. Babau, "An ontology for attacks in wireless sensor networks," Ph.D. thesis, Unité de Recherche INRIA Rhône-Alpes, Montbonnot Saint-Ismier, France, Unité de Recherche INRIA Futurs Parc Club Orsay Université—ZAC des Vignes, INRIA, 2008.

[26] C. Pu, S. Lim, B. Jung, and M. Min, "Mitigating stealthy collision attack in energy harvesting motivated networks," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Baltimore, MD, USA, Oct. 2017, pp. 539–544.

[27] S. Kamalesh and P. G. Kumar, "Fuzzy based secure intrusion detection system for authentication in wireless sensor networks," *J. Comput. Theor. Nanosci.*, vol. 14, no. 5, pp. 2465–2472, May 2017.

[28] F. Stajano and R. J. Anderson, "The resurrecting duckling," in *Proc. 7th Int. Workshop Secur. Protocols*, Cambridge, U.K., Apr. 1999, pp. 1–240.

[29] F. Stajano and R. Anderson, "The resurrecting duckling: Security issues for ubiquitous computing," *Computer*, vol. 35, no. 4, pp. 22–26, Apr. 2002.

[30] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks," in *Proc. 22nd Annu. Joint Conf. IEEE Comput. Commun. Societies*, vol. 3, Apr. 2003, pp. 1976–1986.

[31] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad Hoc Netw.*, vol. 1, nos. 2–3, pp. 293–315, Sep. 2003.

[32] C. Yuan, W. Chen, Y. Zhu, D. Li, and J. Tan, "A low computational complexity authentication scheme in underwater wireless sensor network," in *Proc. 11th Int. Conf. Mobile Ad-hoc Sensor Netw. (MSN)*, Dec. 2015, pp. 116–123.

[33] F. Yunus, S. H. S. Ariffin, and Y. Zahedi, "A survey of existing medium access control (MAC) for underwater wireless sensor network (UWSN)," in *Proc. 4th Asia Int. Conf. Math./Anal. Modelling Comput. Simulation*, Shanghai, China, May 2010, pp. 544–549.

[34] R. Martin and S. Rajasekaran, "Data centric approach to analyzing security threats in underwater sensor networks," presented at the *Proc. OCEANS MTS*, Washington, DC, USA, Sep. 2016.

[35] G. Khan, K. K. Gola, and R. Rathore, "Robust data aggregation, encryption and data transfer in UWSNs," presented at the 1st Int. Conf. Next Gener. Comput. Technol. (NGCT), Sep. 2015.

[36] T. Dargahi, H. H. S. Javadi, and H. Shafiei, "Securing underwater sensor networks against routing attacks," *Wireless Pers. Commun.*, vol. 96, no. 2, pp. 2585–2602, Sep. 2017.

[37] S. S. Shahapur and R. Khanai, "Localization, routing and its security in UWSN—A survey," presented at the Int. Conf. Electr., Electron., Optim. Techn. (ICEEOT), Seattle, WA, USA, Mar. 2016.

[38] S. Mian and R. Kumar, "Security analysis and issues in underwater wireless sensor auditory and multipath network," *Int. J. Anal. Exp. Modal Anal.*, vol. 11, no. 10, pp. 2269–2271, 2019.

[39] C. Ioannou and V. Vassiliou, "The impact of network layer attacks in wireless sensor networks," in *Proc. IEEE Int. Workshop Secure Internet Things (SIoT)*, Heraklion, Greece, Sep. 2016, pp. 20–28.

[40] I. Khan, M. A. Khan, S. Khusro, and M. Naeem, "Vehicular lifelogging: Issues, challenges, and research opportunities," *J. Inf. Commun. Technol. Robot. Appl.*, vol. 8, no. 2, pp. 30–37, 2017.

[41] P. Pandarinath, "Secure localization with defense against selective forwarding attacks in wireless sensor networks," in *Proc. 3rd Int. Conf. Electron. Comput. Technol.*, vol. 5, Kanyakumari, India, Apr. 2011, pp. 112–117.

[42] M. R. Ahmed, M. Aseeri, M. S. Kaiser, N. Z. Zenia, and Z. I. Chowdhury, "A novel algorithm for malicious attack detection in UWSN," in *Proc. Int. Conf. Electr. Eng. Inf. Commun. Technol. (ICEEICT)*, Dhaka, Bangladesh, May 2015, pp. 1–6.

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

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

[45] M. Saini, R. Kumar, and J. Kaur, "To propose a novel technique for detection and isolation of misdirection attack in wireless sensor network," *Indian J. Sci. Technol.*, vol. 9, no. 28, pp. 1–7, 2016.

[46] Y. Li, L. Xiao, Q. Li, and W. Su, "Spoofing detection games in underwater sensor networks," in *Proc. OCEANS*, Oct. 2015, pp. 1–12.

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

[48] Y. Cong, G. Yang, Z. Wei, and W. Zhou, "Security in underwater sensor network," in *Proc. Int. Conf. Commun. Mobile Comput.*, vol. 1, Shenzhen, China, Apr. 2010, pp. 162–168.

[49] J. Chen, Y. Zhang, Y. Zhou, and Z. Li, "Mitigating overwhelm attacks in underwater sensor networks: A distributed clustering and threshold-based approach," *IEEE Trans. Veh. Technol.*, vol. 67, no. 2, pp. 1227–1237, Feb. 2018.

[50] R. Singh, A. Sharma, and M. Jones, "Thwarting the depths: Mitigating path-based denial-of-service attacks in underwater sensor networks," *ACM Trans. Sensor Netw.*, vol. 17, no. 2, pp. 1–18, Aug. 2021.

[51] R. Verma and S. Bharti, "A survey of network attacks in wireless sensor networks," in *Information, Communication and Computing Technology* (Communication and Computing Technology), 2020, pp. 50–63.

[52] I. Butun, P. Österberg, and H. Song, "Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 616–644, 1st Quart., 2020.

[53] S. Palisetti, B. R. Chandavarkar, and A. V. Gadagkar, "Intrusion detection of sinkhole attack in underwater acoustic sensor networks," in *Proc. 12th Int. Conf. Comput. Commun. Netw. Technol. (ICCCNT)*, Kharagpur, India, Jul. 2021, pp. 1–7, doi: 10.1109/ICCCNT51525.2021.9580148.

[54] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54–62, Oct. 2002.

[55] D.-L. Vu, T.-K. Nguyen, T. V. Nguyen, T. N. Nguyen, F. Massacci, and P. H. Phung, "A convolutional transformation network for malware classification," in *Proc. 6th NAFOSTED Conf. Inf. Comput. Sci. (NICS)*, Dec. 2019, pp. 234–239.

[56] D.-T. Do, T. Anh Le, T. N. Nguyen, X. Li, and K. M. Rabie, "Joint impacts of imperfect CSI and imperfect SIC in cognitive radio-assisted NOMA-V2X communications," *IEEE Access*, vol. 8, pp. 128629–128645, 2020.

[57] L. Zhen, A. K. Bashir, K. Yu, Y. D. Al-Otaibi, C. H. Foh, and P. Xiao, "Energy-efficient random access for LEO satellite-assisted 6G Internet of Remote Things," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5114–5128, Apr. 2021, doi: 10.1109/JIOT.2020.3030856.

[58] C. Peng, X. Du, K. Li, and M. Li, "An ultra-lightweight encryption scheme in underwater acoustic networks," *J. Sensors*, vol. 2016, pp. 1–10, Jan. 2016.

[59] J. E. Kim, N. Y. Yun, S. Muminov, S. H. Park, and O. Y. Yi, "Security in underwater acoustic sensor network: Focus on suitable encryption mechanisms," in *Proc. Asian Simulation Conf.*, Shanghai, China. Berlin, Germany: Springer, 2012, pp. 160–168.

[60] S. B. Goyal, R. V. Ravi, C. Verma, M. S. Raboaca, and F. M. Enescu, "A lightweight cryptographic algorithm for underwater acoustic networks," *Proc. Comput. Sci.*, vol. 215, pp. 266–273, Jan. 2022.

[61] Z. Wang, J. Du, Z. Xia, C. Jiang, Z. Fang, and Y. Ren, "Secure routing in underwater acoustic sensor networks based on AFSA-ACOA fusion algorithm," in *Proc. IEEE Int. Conf. Commun.*, May 2022, pp. 1409–1414.

[62] X. Du, C. Peng, and K. Li, "A secure routing scheme for underwater acoustic networks," *Int. J. Distrib. Sensor Netw.*, vol. 13, no. 6, Jun. 2017, Art. no. 155014771771364.

[63] K. Saeed, W. Khalil, S. Ahmed, I. Ahmad, and M. N. K. Khattak, "SEECR: Secure energy efficient and cooperative routing protocol for underwater wireless sensor networks," *IEEE Access*, vol. 8, pp. 107419–107433, 2020.

[64] R. Zhang and Y. Zhang, "Wormhole-resilient secure neighbor discovery in underwater acoustic networks," in *Proc. IEEE INFOCOM*, San Diego, CA, USA, Mar. 2010, pp. 1–9.

[65] A. P. Das and S. M. Thampi, "Secure communication in mobile underwater wireless sensor networks," in *Proc. Int. Conf. Adv. Comput., Commun. Informat. (ICACCI)*, Aug. 2015, pp. 2164–2173.

[66] M. Zhang, J. Xie, Z. Wang, L. Liang, P. Gu, P. Jin, and J. Zhou, "MO-CBACORP: A new energy-efficient secure routing protocol for underwater monitoring wireless sensor network," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 35, no. 9, Oct. 2023, Art. no. 101786, doi: 10.1016/j.jksuci.2023.101786.

[67] R. Zhu, A. Boukerche, X. Huang, and Q. Yang, "DESLR: Energy-efficient and secure layered routing based on channel-aware trust model for UASNs," *Comput. Netw.*, vol. 234, Oct. 2023, Art. no. 109939, doi: 10.1016/j.comnet.2023.109939.

[68] S. Shah, A. Munir, A. Waheed, A. Alabrah, M. Mukred, F. Amin, and A. Salam, "Enhancing security and efficiency in underwater wireless sensor networks: A lightweight key management framework," *Symmetry*, vol. 15, no. 8, p. 1484, 2023, doi: 10.3390/sym15081484.

[69] S. S. Ullah, S. Hussain, M. Uddin, R. Alroobaea, J. Iqbal, A. M. Baqasah, and R. Alsaqour, "A computationally efficient online/offline signature scheme for underwater wireless sensor networks," *Sensors*, vol. 22, no. 14, p. 5150, 2022, doi: 10.3390/s22145150.

[70] Y. Zhao, B. Tian, Z. Chen, Y. Liu, and J. Ding, "An energy-efficient key agreement mechanism for underwater sensor networks," in *IT Convergence and Security 2017*. Berlin, Germany: Springer, 2018, pp. 146–158.

[71] K. Kalkan and A. Levi, "Key distribution scheme for peer-to-peer communication in mobile underwater wireless sensor networks," *Peer-Peer Netw. Appl.*, vol. 7, no. 4, pp. 698–709, Dec. 2014.

[72] S. Verma and Prachi, "A cluster based key management scheme for underwater wireless sensor networks," *Int. J. Comput. Netw. Inf. Secur.*, vol. 7, no. 9, pp. 54–63, Aug. 2015, doi: 10.5815/ijcnis.2015.09.07.

[73] E. Souza, H. C. Wong, I. Cunha, Ì. Cunha, L. F. M. Vieira, and L. B. Oliveira, "End-to-end authentication in under-water sensor networks," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Split, Croatia, Jul. 2013, pp. 299–304.

[74] S. K. Erskine, H. Chi, and A. Elleithy, "SDAA: Secure data aggregation and authentication using multiple sinks in cluster-based underwater vehicular wireless sensor network," *Sensors*, vol. 23, no. 11, p. 5270, Jun. 2023, doi: 10.3390/s23115270.

[75] N. Goyal, M. Dave, and A. K. Verma, "SAPDA: Secure authentication with protected data aggregation scheme for improving QoS in scalable and survivable UWSNs," *Wireless Pers. Commun.*, vol. 113, no. 1, pp. 1–15, Jul. 2020.

[76] S. Rajasoundaran, S. V. N. S. Kumar, M. Selvi, K. Thangaramya, and K. Arputharaj, "Secure and optimized intrusion detection scheme using LSTM-MAC principles for underwater wireless sensor networks," *Wireless Netw.*, vol. 30, no. 1, pp. 209–231, Jan. 2024, doi: 10.1007/s11276-023-03470-x.

[77] H. Huang, N. Liu, D. Chen, Q. Yang, and X. Huang, "Research on the intrusion detection model of underwater sensor networks," *J. Sensors*, vol. 2022, pp. 1–17, May 2022, doi: 10.1155/2022/2323747.

[78] R. Zhang, J. Zhang, Q. Wang, and H. Zhang, "DOIDS: An intrusion detection scheme based on DBSCAN for opportunistic routing in underwater wireless sensor networks," *Sensors*, vol. 23, no. 4, p. 2096, Feb. 2023, doi: 10.3390/s23042096.

[79] M. Ibragimov, J.-H. Lee, M. Kalyani, J.-I. Namgung, S.-H. Park, O. Yi, C. H. Kim, and Y.-K. Lim, "CCM-UW security modes for low-band underwater acoustic sensor networks," *Wireless Pers. Commun.*, vol. 89, no. 2, pp. 479–499, Jul. 2016.

[80] M. Xu, G. Liu, and J. Guan, "Towards a secure medium access control protocol for cluster-based underwater wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 11, no. 5, May 2015, Art. no. 325474.

[81] G. Ateniese, A. Capossele, P. Gjanci, C. Petrioli, and D. Spaccini, "SecFUN: Security framework for underwater acoustic sensor networks," in *Proc. OCEANS*, Genova, Italy, May 2015, pp. 1–9, doi: 10.1109/OCEANS-Genova.2015.7271735.

[82] G. Dini and A. L. Duca, "A cryptographic suite for underwater cooperative applications," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jun. 2011, pp. 870–875.

[83] Y. He, G. Han, J. Jiang, H. Wang, and M. Martínez-García, "A trust update mechanism based on reinforcement learning in underwater acoustic sensor networks," *IEEE Trans. Mobile Comput.*, vol. 21, no. 3, pp. 811–821, Mar. 2022, doi: 10.1109/TMC.2020.3020313.

[84] G. Han, Y. He, J. Jiang, H. Wang, Y. Peng, and K. Fan, "Fault-tolerant trust model for hybrid attack mode in underwater acoustic sensor networks," *IEEE Netw.*, vol. 34, no. 5, pp. 330–336, Sep. 2020.

[85] S. Misra and T. Ojha, "SecRET: Secure range-based localization with evidence theory for underwater sensor networks," *ACM Trans. Auto. Adapt. Syst.*, vol. 15, no. 1, pp. 1–26, Mar. 2020, doi: 10.1145/3431390.

[86] M. B. Shanthi and D. K. Anvekar, "Secure localization for underwater wireless sensor networks based on probabilistic approach," in *Proc. 2nd Int. Conf. Adv. Electron., Comput. Commun. (ICAECC)*, Bangalore, India, Feb. 2018, pp. 1–6, doi: 10.1109/ICAECC.2018.8479451.

[87] Z. Ansari, R. Ghazizadeh, and Z. Shokhmzan, "Gradient descent approach to secure localization for underwater wireless sensor networks," in *Proc. 24th Iranian Conf. Electr. Eng. (ICEE)*, Shiraz, Iran, May 2016, pp. 103–107, doi: 10.1109/IranianCEE.2016.7585498.

[88] M. Xu, G. Liu, D. Zhu, and H. Wu, "A cluster-based secure synchronization protocol for underwater wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 10, no. 4, Apr. 2014, Art. no. 398610.

[89] F. Hu, S. Wilson, and Y. Xiao, "Correlation-based security in time synchronization of sensor networks," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Mar. 2008, pp. 2525–2530.

[90] S. Jiang, "On securing underwater acoustic networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 729–752, 1st Quart., 2019, doi: 10.1109/COMST.2018.2864127.

[91] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, 1996.

[92] I. Krikidis, J. S. Thompson, and S. Mclaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.

[93] S. Basagni, M. Conti, S. Giordano, and I. Stojmenovic, "Advances in underwater acoustic networking," in *Mobile Ad Hoc Networking: The Cutting Edge Directions*, S. Basagni, M. Conti, S. Giordano, and I. Stojmenovic, Eds., Hoboken, NJ, USA: Wiley, 2013, ch. 2, pp. 804–852.

[94] H. Kulhandjian, T. Melodia, and D. Koutsonikolas, "Securing underwater acoustic communications through analog network coding," in *Proc. 11th Annu. IEEE Int. Conf. Sens., Commun., Netw. (SECON)*, Singapore, Jun. 2014, pp. 266–274.

[95] H. Yan, Z. J. Shi, and Y. Fei, "Efficient implementation of elliptic curve cryptography on DSP for underwater sensor networks," in *Proc. 7th Workshop Optimizations DSP Embedded Syst.*, Seattle, WA, USA, Mar. 2009, pp. 7–15.

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

[97] G. Han, J. Jiang, N. Sun, and L. Shu, "Secure communication for underwater acoustic sensor networks," *IEEE Commun. Mag.*, vol. 53, no. 8, pp. 54–60, Aug. 2015.

[98] M. A. Habib, M. J. Uddin, and M. Islam, "Safety aspects of enhanced underwater acoustic sensor networks," *Int. J. Emerg. Technol. Adv. Eng.*, vol. 2, no. 8, pp. 385–390, Aug. 2012.

[99] K. Saeed, W. Khalil, A. S. Al-Shamayleh, S. Ahmed, A. Akhunzada, S. Z. Alharthi, and A. Gani, "A comprehensive analysis of security-based schemes in underwater wireless sensor networks," *Sustainability*, vol. 15, no. 9, p. 7198, Apr. 2023.

[100] I. Ahmad, T. Rahman, A. Zeb, I. Khan, I. Ullah, H. Hamam, and O. Cheikhrouhou, "Analysis of security attacks and taxonomy in underwater wireless sensor networks," *Wireless Commun. Mobile Comput.*, vol. 2021, no. 1, Jan. 2021, Art. no. 1444024, doi: 10.1155/2021/1444024.

[101] S. P. K. Deepak and M. B. M. Krishnan, "Survey on security systems in underwater communications systems," in *New Trends in Computational Vision and Bio-inspired Computing*. Cham, Switzerland: Springer, 2020, pp. 1153–1163, doi: 10.1007/978-3-030-41862-5_117.

[102] P. A. Shelar, P. N. Mahalle, and G. Shinde, "Secure data transmission in underwater sensor network: Survey and discussion," in *Internet of Things, Smart Computing and Technology: A Roadmap Ahead. Studies in Systems, Decision and Control* (Studies in Systems, Decision and Control), vol. 266, N. Dey, P. N. Mahalle, P. M. Shafi, V. V. Kimabahune, and A. E. Hassanien, Eds., Cham, Switzerland: Springer, 2020, pp. 323–360, doi: 10.1007/978-3-030-39047-1_15.

[103] S. Kumari, K. K. Singh, P. Nand, G. S. Mishra, and R. Astya, "A comparative study of security issues and attacks on underwater sensor network," in *Proc. 3rd Int. Conf. Comput., Commun., Cyber-Secur.*, in Lecture Notes in Networks and Systems, vol. 421, P. K. Singh, S. T. Wierzchoń, S. Tanwar, J. J. P. C. Rodrigues, and M. Ganzha, Eds., Singapore: Springer, pp. 59–74, doi: 10.1007/978-981-19-1142-2_5.

[104] G. Yang, L. Dai, G. Si, S. Wang, and S. Wang, "Challenges and security issues in underwater wireless sensor networks," *Proc. Comput. Sci.*, vol. 147, pp. 210–216, Jan. 2019.

[105] J. Kong, Z. Ji, W. Wang, M. Gerla, R. Bagrodia, and B. Bhargava, "Low-cost attacks against packet delivery, localization and time synchronization services in under-water sensor networks," in *Proc. 4th ACM workshop Wireless Secur.*, Dhaka, Bangladesh, Sep. 2005, pp. 87–96.

[106] G. B. Rajendran, U. M. Kumarasamy, C. Zarro, P. B. Divakarachari, and S. L. Ullo, "Land-use and land-cover classification using a human group-based particle swarm optimization algorithm with an LSTM classifier on hybrid pre-processing remote-sensing images," *Remote Sens.*, vol. 12, no. 24, p. 4135, Dec. 2020.

[107] A. Boukerche and D. Turgut, "Secure time synchronization protocols for wireless sensor networks," *IEEE Wireless Commun.*, vol. 14, no. 5, pp. 64–69, Oct. 2007.

[108] J. Liu, Z. Wang, M. Zuba, Z. Peng, J.-H. Cui, and S. Zhou, "DA-sync: A Doppler-assisted time-synchronization scheme for mobile underwater sensor networks," *IEEE Trans. Mobile Comput.*, vol. 13, no. 3, pp. 582–595, Mar. 2014.

[109] J. Liu, Z. Wang, Z. Peng, M. Zuba, J.-H. Cui, and S. Zhou, "TSMU: A time synchronization scheme for mobile underwater sensor networks," in *Proc. IEEE Global Telecommun. Conf.*, Dec. 2011, pp. 1–6.

[110] M. M. Arifeen, A. Al Mamun, T. Ahmed, M. S. Kaiser, and M. Mahmud, "A blockchain-based scheme for Sybil attack detection in underwater wireless sensor networks," in *Proc. Int. Conf. Trends Comput. Cogn. Eng.*, in Advances in Intelligent Systems and Computing, vol. 1309, M. S. Kaiser, A. Bandyopadhyay, M. Mahmud, and K. Ray, Eds., Singapore: Springer, 2021, pp. 467–476.

[111] D. Zala, D. Thummar, and B. R. Chandavarkar, "Mitigating blackhole attack of underwater sensor networks," in *Proc. 12th Int. Conf. Comput. Commun. Netw. Technol. (ICCCNT)*, Kharagpur, India, Jul. 2021, pp. 1–8.

[112] Z. Junqing, Z. Gangqiang, and L. Junkai, "Wormhole attack detecting in underwater acoustic communication networks," in *Proc. OES China Ocean Acoust. (COA)*, Harbin, China, Jul. 2021, pp. 647–650.

[113] P. Kaur and J. S. Gurm, "Detect and prevent HELLO FLOOD attack using centralized technique in WSN," *Int. J. Comput. Sci. Eng. Technol.*, vol. 7, no. 8, pp. 379–381, 2016.

[114] A. Kumar, N. J. Ahuja, M. Thapliyal, S. Dutt, T. Kumar, D. A. De Jesus Pacheco, C. Konstantinou, and K.-K. R. Choo, "Blockchain for unmanned underwater drones: Research issues, challenges, trends and future directions," *J. Netw. Comput. Appl.*, vol. 215, Jun. 2023, Art. no. 103649.

[115] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasurbramanian, "A lightweight blockchain based framework for underwater IoT," *Electronics*, vol. 8, no. 12, p. 1552, Dec. 2019.

[116] M. Nain and N. Goyal, "Localization techniques in underwater wireless sensor network," in *Proc. Int. Conf. Advance Comput. Innov. Technol. Eng. (ICACITE)*, Mar. 2021, pp. 747–751.

[117] M. Chaudhary, N. Goyal, A. Benslimane, L. K. Awasthi, A. Alwadain, and A. Singh, "Underwater wireless sensor networks: Enabling technologies for node deployment and data collection challenges," *IEEE Internet Things J.*, vol. 10, no. 4, pp. 3500–3524, Feb. 2023.

[118] O. Gupta, M. Kumar, A. Mushtaq, and N. Goyal, "Localization schemes and its challenges in underwater wireless sensor networks," *J. Comput. Theor. Nanosci.*, vol. 17, no. 6, pp. 2750–2754, Jun. 2020, doi: 10.1166/jctn.2020.9116.

[119] A. M. Pandith and N. Goyal, "Emerging data aggregation state-of-art techniques with comparative analysis in UWSN," in *Proc. 2nd Int. Conf. Adv. Comput. Innov. Technol. Eng. (ICACITE)*, Apr. 2022, pp. 28–29.

[120] M. Kumar, N. Goyal, and V. Khullar, "Emerging node localization state-of-art techniques classification with comparative analysis in UWSNs," in *Proc. 2nd Int. Conf. Advance Comput. Innov. Technol. Eng. (ICACITE)*, Apr. 2022, pp. 1824–1828, doi: 10.1109/ICACITE53722.2022.9823574.

[121] B. Chen, J. Hu, Y. Zhao, and B. K. Ghosh, "Finite-time observer based tracking control of uncertain heterogeneous underwater vehicles using adaptive sliding mode approach," *Neurocomputing*, vol. 481, pp. 322–332, Apr. 2022, doi: 10.1016/j.neucom.2022.01.038.

KHAWAJA MASOOD AHMED is currently pursuing the Ph.D. degree in electronic engineering with the Sir Syed University of Engineering and Technology, with a focus on optimization of security algorithms in underwater wireless sensor networks. This review presented here is part of his research work.

REHAN SHAMS (Senior Member, IEEE) is currently an Associate Professor with the Department of Telecommunication Engineering, Sir Syed University of Engineering and Technology, Karachi, Pakistan. He is the author of over 25 papers in refereed international journals and conference proceedings and the book *Underwater Wireless Sensor Networks* (2022). His research interests include cybersecurity, network security, and underwater wireless sensor networks.

FOZIA HANIF KHAN received the Ph.D. degree in operations research from the University of Karachi, Karachi, Pakistan, in 2012. She held a postdoctoral position with the University of Malaga, Spain, in September 2019. She is currently an Assistant Professor with the Department of Mathematics, University of Karachi. Her research interests include cryptography, graph theory, optimization network security, wireless sensors networks, and underwater sensor networks.

MIGUEL-ÁNGEL LUQUE-NIETO was born in Córdoba, Spain, in 1971. He received the Ingeniero de Telecomunicación and Ph.D. degrees from the Universidad de Málaga, Málaga, Spain, in 1996 and 2018, respectively. He was an ensign with Spanish Air Force, from 1996 to 1998. In 1998, he joined the Escuela Técnica Superior de Ingeniería de Telecomunicación (ETSIT), Universidad de Málaga, as an Assistant Professor. He is currently an Associate Professor with ETSIT and a Principal Researcher with the Institute of Oceanic Engineering Research, Universidad de Málaga. His research interests include underwater acoustic communications networks, especially protocols, wireless communications, and image processing.