IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 30 May 2023, accepted 8 June 2023, date of publication 21 June 2023, date of current version 30 June 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3288330

SURVEY

A Survey of Sybil Attack Countermeasures in Underwater Sensor and Acoustic Networks

ZURIATI AHMAD ZUKARNAIN[1], **OLUWATOSIN AHMED AMODU**[2,3], **(Member, IEEE), CUI WENTING**[1], **AND UMAR ALI BUKAR**[4]

[1]Department of Communication Technology and Network, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia (UPM), Selangor 43400, Malaysia
[2]Department of Electrical, Electronics and Systems Engineering, Universiti Kebangsaan Malaysia (UKM), Bangi, Selangor 43600, Malaysia
[3]Information and Communication Engineering Department, Elizade University, Ilara-Mokin, Ondo State 340271, Nigeria
[4]Centre for Intelligent Cloud Computing (CICC), Faculty of Information Science and Technology, Multimedia University, Bukit Beruang, Malacca 75450, Malaysia

Corresponding authors: Zuriati Ahmad Zukarnain (zuriati@upm.edu.my) and Oluwatosin Ahmed Amodu (amodu_o_a@ieee.org)

This work was supported by the Geran Putra Berimpak (GPB), UPM.

ABSTRACT Underwater sensor and acoustic networks have several unique applications including water quality and ocean life monitoring, as well as ocean navigation and exploration. They also have peculiar physical layer characteristics with respect to operating frequency and attenuation which makes them different from terrestrial wireless sensor communication. Thus, coupled with their large cost of deployment and sensitivity, they are highly vulnerable to security attacks. For instance, a Sybil node could pretend to be at several other locations in the sparse network simultaneously, thereby deceiving legitimate nodes and infringing on the security of transmitted information. Over the last few years, researchers have studied means of preventing, detecting, and mitigating Sybil attacks for safe underwater communication under different assumptions and architectural setups. However, to our knowledge, these efforts have been scattered in the literature and concrete lessons have not been drawn from these efforts via a survey/review on this subject towards achieving safe underwater communication. This motivates the presentation of this paper that provides an exposition of the academic discussion on the solutions for addressing Sybil attacks in underwater wireless communication, with respect to attack prevention, detection and mitigation while identifying some of their limitations. Similarly, proposed methods and technical aspects peculiar to these works are identified, and a wide range of challenges, opportunities, and recommendations are provided.

INDEX TERMS Sybil attacks, trust management, UASN, underwater communication, UWSN.

I. INTRODUCTION

Underwater wireless communication such as sensor and acoustic networks facilitates a variety of applications. Examples include offshore exploration and oil and gas monitoring (especially oil spills) [1]. Underwater sensor networks are also used in the military for mine reconnaissance, i.e., when autonomous underwater vehicles with optical sensors assess objects and detect whether they are actually mine materials [2]. Sensors also monitor land and ocean currents for reliable weather prediction. Thus, climate can be studied and climate change can be measured. With underwater sensor communication, fishes, sunken boats, wrecks, and dangerous objects under the water are tracked. Similarly, sensor-assisted reliable weather prediction makes navigation in the sea easier for boat operators and sailors. Underwater sensors are usually deployed in very harsh environments. The nodes operate unattended in such regions which makes them vulnerable to a lot of security attacks [1], and meeting the major security requirements (see Table 1 based on [3]) becomes challenging.

Underwater environments have other peculiar features [3] such as low bandwidth, stringent power requirement, node mobility with ocean current, and scalability. Radio waves travel very far underwater but at very low frequencies [2], [3]. Furthermore, their data rates vary depending on the type of water (sea water or fresh water) which also determines the application scenarios (varying from autonomous underwater vehicle docking to deep water telemetry) [4]. Based on these characteristics, a number of consequences can be drawn from the security perspective. For example, vital packets that are

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

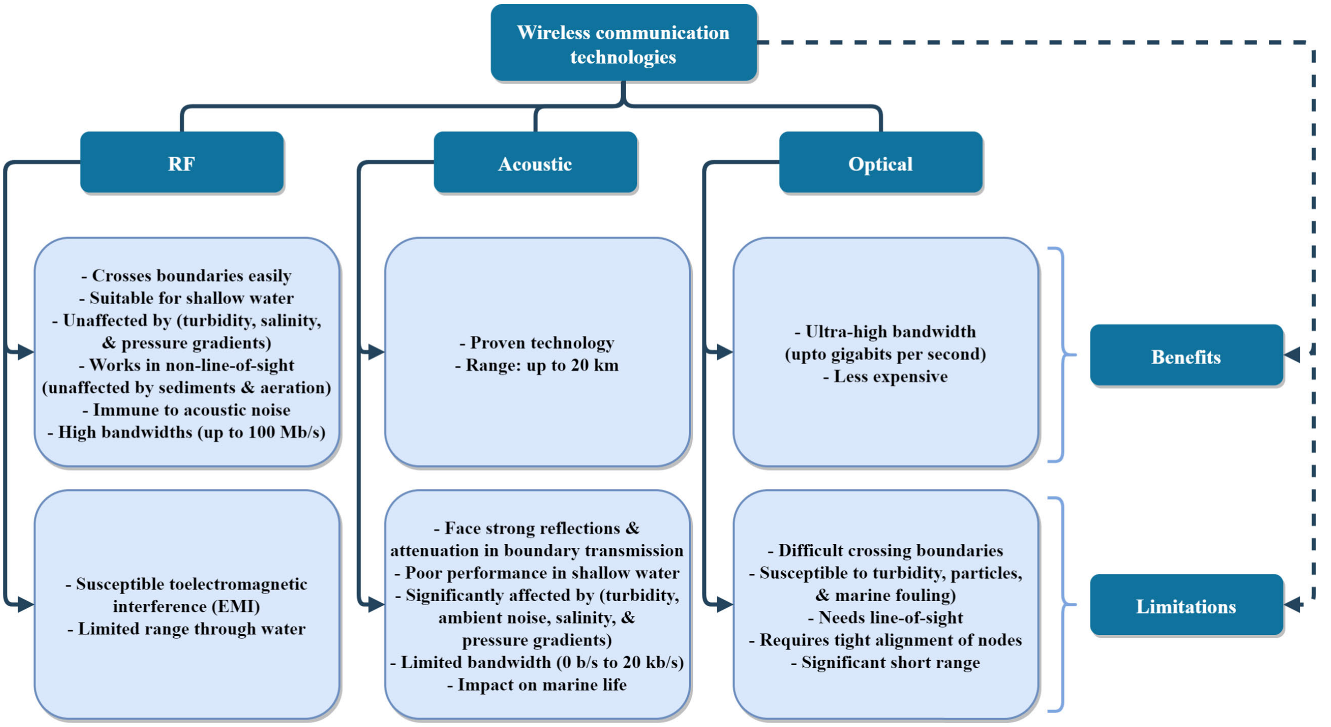
Wireless communication technologies
RF
Acoustic
Optical
- Crosses boundaries easily
- Suitable for shallow water
- Unaffected by (turbidity, salinity, & pressure gradients)
- Works in non-line-of-sight (unaffected by sediments & aeration)
- Immune to acoustic noise
- High bandwidths (up to 100 Mb/s)
- Proven technology
- Range: up to 20 km
- Ultra-high bandwidth (upto gigabits per second)
- Less expensive
Benefits
- Susceptible toelectromagnetic interference (EMI)
- Limited range through water
- Face strong reflections & attenuation in boundary transmission
- Poor performance in shallow water
- Significantly affected by (turbidity, ambient noise, salinity, & pressure gradients)
- Limited bandwidth (0 b/s to 20 kb/s)
- Impact on marine life
- Difficult crossing boundaries
- Susceptible to turbidity, particles, & marine fouling)
- Needs line-of-sight
- Requires tight alignment of nodes
- Significant short range
Limitations

FIGURE 1. Benefits and limitations of various underwater wireless communication technologies based on Che et al. [4].

necessary for achieving security might be lost due to packet errors. This is coupled with the inherently high bit error rates, low propagation delays, critical nature of underwater sensor applications, and vulnerability of underwater environments. Security attacks in such situations become a very serious issue. As a result, the network should be robust to have countermeasures to external attacks when they occur[1] [5]. Efficient and reliable security mechanisms are also required to address security issues such as jamming, replay, wormhole, sinkhole, hello flood, acknowledgment spoofing, selective forwarding, and particularly, Sybil attacks [3].

One of the most dangerous attacks in underwater environments is Sybil attack [6]. To launch a Sybil attack, a malicious node (Sybil node) takes up multiple fake identities at the same time, thus controlling a large portion of the network [6]. This presents a huge threat to the underwater network and many of its applications. This paper aims to present a review of the proposals and methods for addressing Sybil attacks in underwater sensor and acoustic networks to ensure that communication via sensors is free from Sybil attacks.

A. UNDERWATER WIRELESS COMMUNICATION TECHNOLOGIES AND ARCHITECTURE

Underwater wireless communication technologies include radio frequency electromagnetic, acoustic, and optical technologies. Each of these technologies has its prospects (see Figure 1 based on [4]). In view of the potentials of radio frequency electromagnetic and acoustic technologies for underwater wireless sensor networks and acoustic networks coupled with the fact that no studies on Sybil attack mitigation were found for underwater optical wireless communication scenarios, this work is mainly focused on underwater sensor and acoustic networks.

Various devices constitute the underwater network architecture. These include underwater sensors and surface stations mounted on autonomous surface vehicles (ASV), and highly mobile autonomous underwater vehicles (AUVs). Then onshore infrastructure and satellites are typical components of underwater sensor network architecture [7]. As shown in Fig. 2, apart from legitimate nodes, malicious nodes could also be introduced to the network, thus affecting the quality, security, and reliability of information.

B. RELATED SURVEYS

There are a few surveys available on Sybil attack detection and countermeasures. For instance, in ad-hoc networks [8], self-organizing networks (SONs) [9], vehicular networks [10], [11], sensor networks [12] and internet of things (IoT) [13], but none has been carried out on underwater sensors and acoustic networks (refer to Table 2). This section briefs the prior surveys.

In [8], the authors present a comprehensive survey of some of the most potent techniques for defending against Sybil attacks for ad-hoc networks which include random key pre-distribution, central authority for symmetric key sharing, RSSI, neighborhood data, passive ad-hoc Sybil identity (with and without group) detection, and energy trusts systems. The approaches are analyzed by highlighting their merits and demerits with an exposition of the Sybil defense mecha-

[1] Ideally, the network should not allow such attacks without detecting them.

TABLE 1. Security requirements in underwater networks.

Requirement	Application	Description
Confidentiality	Maritime	Ensures information cannot be assessed by unauthorized third parties.
Authentication	Military	Proves that data has not been sent by an adversary.
Integrity	Water quality monitoring	Proves data has not been altered by any adversary.
Availability	Seaquake prediction	Ensure data is available when needed by an authorized user.

TABLE 2. Overview of previous surveys and comparison with this survey.

Ref	Network Type	Description
[8]	MANET	It describes the advantages and disadvantages of random key pre-distribution, symmetric key sharing using central authority, RSSI, neighbor data, passive temporary Sybil identification (vs without group detection), and energy trust system. It also points out the future development direction of Sybil defense.
[13]	WSN IoT	It describes the analysis of recently proposed defense schemes, merits and demerits of encryption, trust, RSSI, and artificial intelligence.
[9]	SONs	It describes the authors' proposed false positive and negative, detection, and untrusted rates for Sybil detection mechanisms, with a special focus on defense mitigation schemes in peer-to-peer and ad-hoc networks.
[10]	VFC-IoT	It describes various Sybil detection mechanisms and gives the future development direction by comparing fault tolerance rate, production cost, operation conditions, and so on.
[12]	WSN	It describes the advantages and disadvantages of the wormhole and Sybil attacks.
[11]	VANET	It describes the effects of Sybil attack in the VANET network.
[14]	VANET	It describes some techniques for detecting Sybil attacks in VANET networks, which have an important impact on reputation systems, secure communications, and the universality of connectivity.
This work	UWSN/UASN	Reviews Sybil attack detection and defense mechanisms in underwater wireless communication.

nisms using diagrams and examples. Then, challenges and future research considerations are drawn for mitigating Sybil attacks.

Another effort is directed at SONs in [9] where the authors studied Sybil detection mechanisms and analyzed its mitigation techniques in peer-to-peer reputation-based systems, social systems, and SONs. The authors used false positive and negative, detection, and non-trustworthy rates for evaluation. They emphasized ways of improving the detection rate and minimizing the false positive and negative rates in the detection and mitigation of Sybil attacks.

The deployment of vehicular fog computing has several security benefits for addressing issues in traditional vehicular adhoc networks (VANETs). Particularly with respect to response time and latency due to the highly frequent interactions between the vehicular network and cloud servers. Nevertheless, attackers can launch Sybil attacks leveraging the anonymity protection mechanism. This motivates the authors in [10] to identify various Sybil attack detection mechanisms, compare and summarize their impact while identifying challenges and research prospects. Similarly, Kaur and Kumar [11] briefly discussed the effect of Sybil attacks in VANETs while [14] discussed some of the techniques for detecting Sybil attacks in VANETs for addressing fundamental issues such as achieving proper node cooperation. These affect secure communication, ubiquity in connectivity, and reputation management.

Designing traditional wireless sensor networks should ideally consider fault tolerance, operating conditions, production cost, hardware constraints, and scalability. Moreover, these networks should be resistant to various attacks such as wormholes and Sybil. In this line, [12] reviews some of the defense mechanisms against these attacks providing a comparison of the merits and demerits.

Several of the wireless sensor network primitives have largely led to the maturity of the Internet of Things (IoT) paradigm where physical objects can send data to a server via an internet gate. Such devices are also quite vulnerable to Sybil attacks due to their distributed nature. Thus, [13] presents a systematic review of some of the recent techniques proposed for defending against Sybil attacks such as encryption, trust, RSSI, and artificial intelligence-based techniques. The paper highlights the merits and demerits of the proposed methods, lessons learned, and future directions.

C. MOTIVATION

The preceding section shows that review papers are needed to improve the knowledge about Sybil attacks and synthesize the proposed solutions in the literature, especially for underwater sensor and acoustic networks. As a result, this study reviews Sybil attack detection and defense mechanisms in underwater wireless communication. Table 2 compares the contributions of prior surveys with this survey based on their focus areas (description) and network type. As shown in Table 2, it is evident that there is no survey/review article on Sybil attacks that helps researchers to (i) understand the existing schemes, (ii) provide a useful classification of these proposals, (iii) identify the research challenges, and

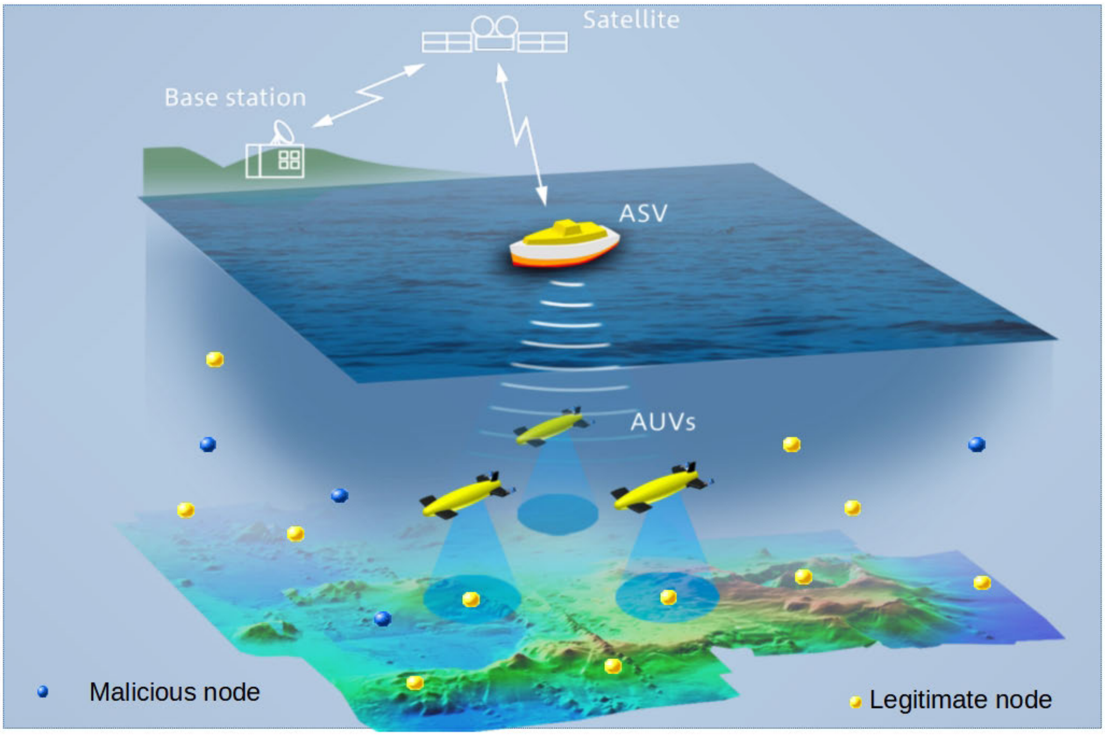

FIGURE 2. Typical architecture of underwater wireless communication with malicious nodes.[2]

(iv) present different future directions. These research gaps motivate the efforts presented in this paper which aims to overview and provide an exposition of existing solutions, unique peculiarities, challenges, and potential future considerations regarding Sybil attacks and countermeasures in underwater acoustic and underwater sensor networks. Thus, this paper presents a comprehensive effort that captures the approaches aimed at preventing, detecting, and mitigating Sybil attacks in underwater sensor and acoustic networks. Moreover, several techniques currently used in this domain such as time synchronization, clustered architectures, encryption, and trust-based techniques are reviewed. The proceeding sections discuss the findings of this study in accordance with the research objectives presented in Section I.

D. OBJECTIVES AND PAPER ORGANIZATION

Since the main aim of the paper is to provide the first comprehensive survey and classification of the current solutions concerning the detection, prevention, and mitigation of Sybil attacks in underwater acoustic and sensor networks, this study focuses on providing a thorough understanding of the techniques and frameworks for addressing Sybil attacks especially due to the unique peculiarities of the underwater environment which makes some of the traditional solutions in terrestrial networks unfeasible in such scenarios. Additionally, we draw lessons from prior solutions in terrestrial networks (with respect to how they can be used to address some of the issues of underwater habitat), open up research gaps in current literature, and indicate new directions for future studies. Specifically, this study achieved the following objectives.

- To identify the approaches adopted to address Sybil attacks in the literature (Section II-E).
- To identify and present the methods and peculiar aspects of Sybil attacks in underwater networks (Section IV).
- To discuss the challenges and future considerations for addressing Sybil attacks in underwater networks (Section V).

Therefore, the rest of this paper is organized as follows: In Section II, a background on the dimensions of Sybil attacks is provided as a precursor to subsequent sections. Section III categorizes the proposed schemes into three and each category is discussed. Section IV discusses some of the methods used, peculiar aspects as well as lessons learned from the proposals aimed to address Sybil attacks in terrestrial networks. Section V discusses current challenges in addressing Sybil attacks and future recommendations while Section VI concludes this paper.

II. OVERVIEW OF SYBIL ATTACKS

In this Section, we provide an overview of Sybil attacks in distributed networks as a background. Details on Sybil attack solutions in underwater communication are provided in the next Section.

A. SYBIL ATTACKS

An attack can be detected through abnormal activities in a system, e.g., increased network delay and packet drop rate. Sybil attacks have two purposes, one is to forge new identities

[2] Picture adapted from hiclipart.com

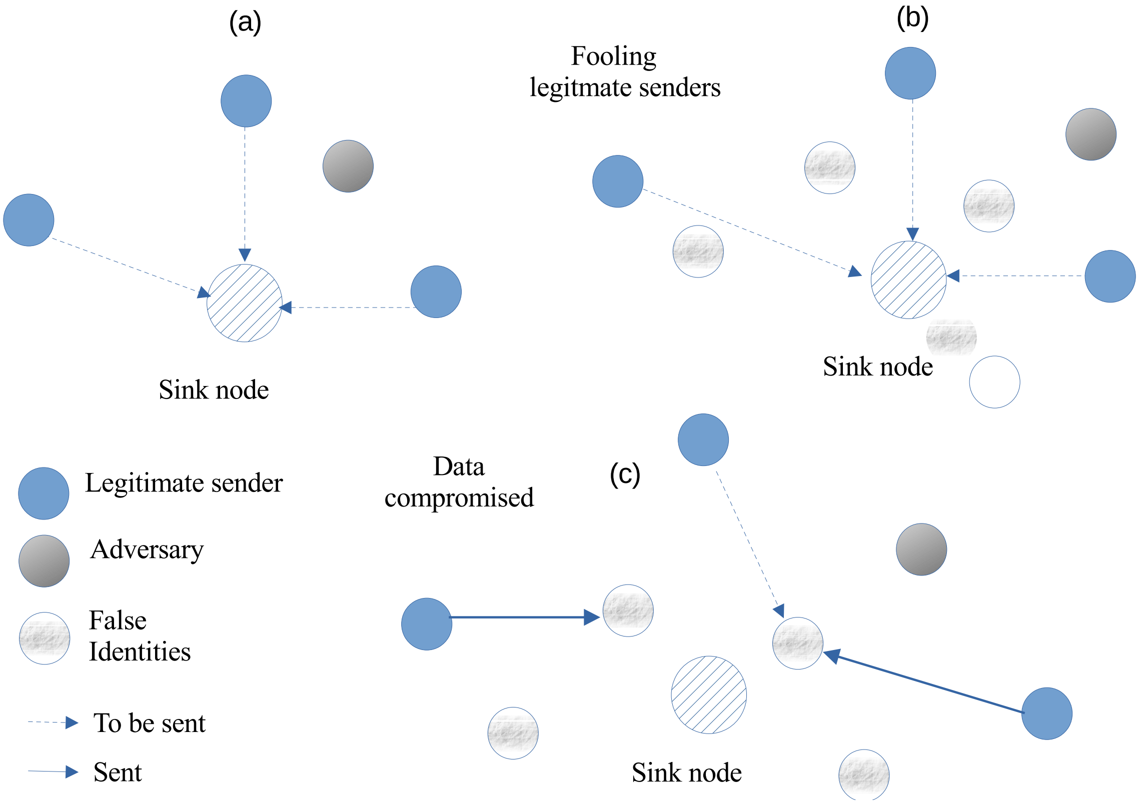

FIGURE 3. Schematic description of a Sybil attack.

and the other is to steal identities from legitimate nodes [15]. This attack could cause a malicious node to gain control over a large portion of the network and maliciously influence the network [8]. This also gives room for several other malicious attacks such as black hole, sinkhole, and byzantine [8] to gain an edge in compromising the network.

Moreover, Sybil attacks are more likely to happen if there are no centralized authorities [6]. Thus, the network can be easily manipulated by adversaries via multiple identities (stolen or fabricated) [16]. For example, consider three nodes intending to send data to the sink (Fig. 3a) while a malicious node creates multiple identities pretending to be in different other locations within the transmission range of the three legitimate nodes, thus fooling them (Fig. 3b). The legitimate nodes think the fake locations are non-malicious and send data to them. This gives the adversary an opportunity to overhear them and the data is compromised (Fig. 3c). Sybil attacks can disrupt several activities [8] in the following ways.

- *Aggregation:* If malicious nodes participate in the aggregation process, they can alter the result of aggregated data.
- *Resource allocation:* In schemes where resource allocation is done on a per-node basis, an adversary can access more resources via its Sybil identities.
- *Vote-based mechanisms:* In this case, malicious node and Sybil identities can vote against a legitimate node. Similarly, an adversary can make Sybil node vote.
- *Routing protocol functionality:* When a Sybil node falls along the route to the destination in location-based routing protocols (such as geographic routing protocol where the position of the immediate neighbor is very important), it alters the routing process. An example is a node sending to a malicious node falsely assuming it is a legitimate multi-path route.
- *Time synchronization*: Since sensor nodes calibrate their clocks using neighbor-broadcasted time stamps, the process can be faulted by Sybil nodes thereby making it difficult for the other nodes to synchronize their clocks.
- *Fault-tolerant schemes:* Sybil attack makes fault tolerant-schemes insignificant. Such schemes might involve distributed storage, topology maintenance, routing, disparity, and multi-path. Location-aware routing requires that nodes share coordinate information with neighbors for geographic routing but Sybil attacks make it seem an adversary is in more than one place at the same time. This adversely affects the *fault-tolerant* scheme because a node might want to leverage the identity of its neighbor not knowing it is an adversary.

B. SYBIL ATTACKS IN DISTRIBUTED NETWORKS

Sybil attacks are common in distributed networks [17] and have been studied in several terrestrial wireless communication systems. For instance, the authors in [8] identified several techniques in the literature to address Sybil attacks

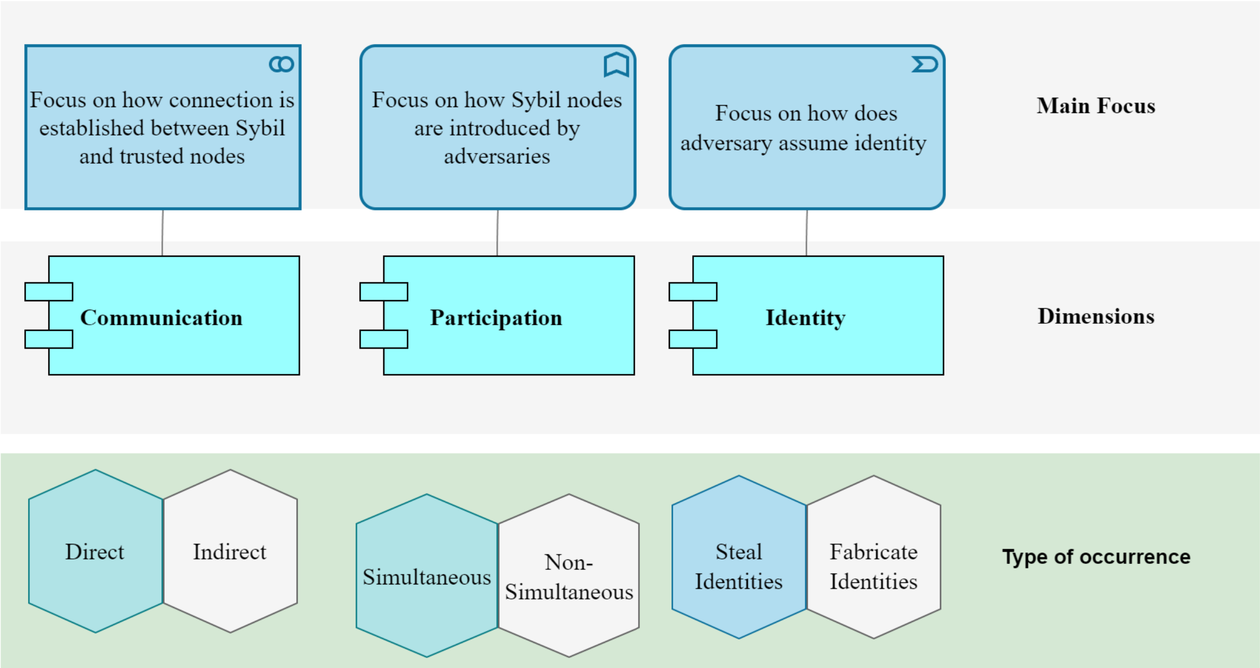
Focus on how connection is established between Sybil and trusted nodes
Focus on how Sybil nodes are introduced by adversaries
Focus on how does adversary assume identity
Main Focus
Communication
Participation
Identity
Dimensions
Direct
Indirect
Simultaneous
Non-Simultaneous
Steal Identities
Fabricate Identities
Type of occurrence

FIGURE 4. The dimensions and main focus of Sybil Attack.

in ad-hoc networks. These include using: (1) a trusted node or center to validate the identity of pairs of nodes intending to communicate; (2) random key-pre-distribution[3] where every node is assigned a key from a large key pool even before they are deployed, such that if two nodes share at least one key, they can communicate securely; (3) radio resource testing on the assumption that every node is equipped with a single radio that can transmit and receive simultaneously on two or more channels; (4) RSSI-based schemes on the premise that multiple Sybil identities of an adversary node can not change their locations [8]. Thus, they will have the same RSSI value [18]; (5) the time difference of arrival between a suspected node and multiple/several detector nodes rather than RSSI; (6) neighbor node information for identifying the presence of Sybil attack in dense networks where two nodes do not have the same set of neighbors; (7) leveraging on node mobility by relying on the fundamental principle that all the Sybil nodes resulting from a single physical node will usually move at the same time with the physical node. So, when such a movement (frequent moving together) is observed, such nodes are suspected as Sybil nodes [19]; and (8) an energy trust system to detect Sybil attack bearing in mind that a legitimate node will have its energy level decreased at a constant rate.

C. DIMENSIONS OF SYBIL ATTACKS

As shown in Fig. 4, Ref. [20] defines three dimensions to Sybil attacks. The first is *communication* which occurs either directly or indirectly. In the former, the legitimate node receives messages from several false identities claiming to be one-hop neighbors while in the latter, the malicious node does not transmit messages through Sybil nodes. In this case, the malicious node claims to have neighbors (which are Sybil nodes) that are not in the communication range of the legitimate node. Thus, the trusted node thinks it can communicate with them through the malicious node. The second is *participation* which can either be simultaneous or non-simultaneous. In the former, an attacker introduces all Sybil nodes at the same time while in the latter, it introduces them at different time intervals. As for *identities*, a Sybil attacker/adversary can assume identities using two techniques, either by stealing or fabricating identities. In the first, identities of the legitimate node that have had their battery drained or have been disconnected are stolen while in the latter, the Sybil nodes fabricate false identities.

D. SYBIL ATTACKS IN UNDERWATER NETWORKS

Sybil attacks in underwater networks basically follow the same philosophy as that of terrestrial networks, i.e., via stealing or falsifying identities. However, underwater sensor network attacks would depend on the architecture which might range between one-dimensional to four-dimensional depending on the sensors' depth, position, and mobility [7]. Moreover, signal processing and network design for prevention, detection, and mitigation would require consideration of far-reaching acoustic signals, long delays, frequency-dependent attenuation, and the sometimes short period of operation of underwater sensing [21].

Successful attack prevention and mitigation mechanisms could leverage the level of mobility of sensor nodes and architecture. Nodes can be static if attached to docks or

[3] The techniques of key distribution varies based on the type of pre-distribution used [8].

anchored buoys. They can also be semi-mobile if they are affected by small-scale distortions such as the precession of buoys on their anchors or the effects of currents or surface waves. They can also be very mobile when attached to AUVS, unpowered drifters or low-power gliders [21]. Other factors peculiar to underwater environments include the different forms of reflections and depth-dependent refractions, small scale and fast variation in instantaneous signal, and slow variation in the propagation medium, e.g., tides and multi-path propagation [21].

E. DESIGN CONSIDERATIONS IN DEVELOPING COUNTERMEASURES TO SYBIL ATTACKS UNDERWATER

Underwater sensor networks are vulnerable to several attacks from the physical to the application layer. It is possible that an adversary sends fake packets or even advertises invalid information by sending a large number of such packets to nodes to reduce system availability. Underwater sensor networks are more prone to external attacks since they exist in an open space. The following are some important peculiar characteristics that are important design considerations in developing countermeasures to Sybil attacks underwater.

1) CHANNEL-BASED ASSUMPTIONS

A number of factors need to be considered in the design of solutions for Sybil attacks in underwater sensor networks. For instance, acoustic channels are characterized by low bandwidth because the link quality is affected by several factors such as refractive properties of sound, fading, and multipath, leading to high bit error rates [3].

2) NOISE

Underwater communication can be grossly affected by noise which could be either natural such as biological activities, currents, seismic, or man-made such as shipping, machinery, etc. Such noise can cause packets to collide which degrades the quality of communication in underwater environments. Similarly, doppler spread could occur due to node mobility and limitations in communication range. Tackling these challenges and developing a protocol resistant to Sybil attacks is thus a major issue in underwater sensor network communication. Note that nodes are energy-constrained and reduced overhead is highly sought after [22].

Noise in underwater acoustic networks is peculiar as it does not follow the traditional Gaussian behavior due to the variance in the noise sources. Thus, signal transmission and detection become quite challenging. Also, sub-optimal performance results could be observed if noise is not properly modeled. These would significantly affect security detection and mitigation schemes [23].

3) ARCHITECTURAL CONSIDERATIONS

Many works assume fixed sensor nodes and sink locations which in many scenarios is not practicable. Some of the metrics used to detect malicious activity include memory space, hop count, and available throughput. In this case, malicious activities can be detected by sensor and sink nodes. Also, some of the assumptions in traditional ad-hoc networks mostly do not hold in underwater wireless communication scenarios, e.g., a static network. As opposed to underwater communication, in traditional terrestrial ad-hoc networks, some of the common assumptions are static networks, synchronized clocks, and dense networks. Due to the movement of ocean current conditions and the high cost of the underwater sensors, few nodes are usually deployed.

4) ENERGY CONSUMPTION

In real-time applications such as oil and gas exploration, implementing UWSNs requires transmitting packets with minimal energy consumption and delay while maximizing the packet delivery ratio as well as guaranteeing security. This implies protection from malicious attacks to protect against loss of critical data [22]. Several works in literature employ expensive cryptographic schemes. Many such schemes are not suitable for UWSN since the schemes are resource-intensive. UWSN can be a victim of either active or passive attacks; the latter is harder to detect.

III. APPROACHES ADOPTED TO ADDRESS SYBIL ATTACKS IN THE LITERATURE

Despite the peculiar characteristics and harsh communication conditions under the water (Table 3), relatively few proposed solutions to underwater Sybil attacks have appeared in the literature (compared to terrestrial networks). Nevertheless, this paper classifies the approaches adopted to address Sybil attacks in underwater sensor and acoustic networks into authentication-based, cluster-based synchronization, encryption-based, and detection-based schemes. The proceeding sections discussed these schemes and their different categories. Some of the approaches adopted to address Sybil attacks in the literature are discussed below.

A. AUTHENTICATION-BASED SCHEMES

Authentication of nodes is very fundamental to addressing Sybil attacks and managing energy waste in the network [5]. Authentication can be achieved using a globally shared key for encryption or via public key cryptography. While the former is prone to attacks, the latter is quite challenging for sensor-based networks due to the resource limitations that make generating and verifying digital signatures cumbersome [36].

1) LIGHT-WEIGHT AUTHENTICATION USING FUZZY LOGIC

Several efforts at addressing security attacks in underwater environments have focused on using complex encryption and decryption-based authentication schemes that consume a significant amount of memory and energy resource. In light of this, the authors in [24] aim to protect the UWSN from Sybil attacks via a simple authentication mechanism that is integrated with the Hierarchical Fuzzy system (HFS)-based trust management model (see Fig. 5) to detect and prevent

TABLE 3. Proposed solutions.

	Ref	Method	Objective	Advantage	Critique	Simulator
UWSN	[24]	Authentication Trust management(HFS)	Detection	Less energy consumption	In this scheme, the node table needs to record the location information of nodes at every moment so, there is a blank time when the location information is not updated.	Xfuzzy-3.5
	[15]	Based on nodes state information	Detection	High detection consumption	The experimental results will result in a large error rate due to the small number of nodes and an unstable network, which will lead to changes in the topology map.	MATLAB
	[25]	Blockchain trust management	Detection	Future development trend	The proposed trust model cannot detect multi-channel attacks, so it needs an artificial intelligence-based model to solve the problem.	Flask
	[26]	TR physical layer authentication	Detection	Effectiveness	This method is limited by spatial and physical dependence. Also, an attacker with an acoustic modem planted on or in the immediate vicinity of a trusted node is not defended against.	-
	[27]	Physical authentication	Prevention	Improves the time synchronization accuracy	In this scheme, CHs will have a centralized bottleneck caused by frequent communication. The hierarchical network topology exposes the mechanism to non-uniform clustering problems. Secondly, public key encryption will cause computer and communication overhead problems.	-
	[28]	True-neighbor algorithm	Mitigation	Fast and efficient calculation	If an attacker obtains the key by hijacking the system, the security of the entire network is compromised because the entire network shares a single key.	Unetstack
	[22]	Multi-factor authentication	Detection	Ensures no modification transition	When the collected network information is biased, the node security cannot be fully guaranteed.	-
	[29]	Encryption	Prevention	Provide security for a tree topology UWAN	The method proposed in this model needs both routing algorithm RE2R and key distribution algorithm to ensure the security.	-
	[30]	Authentication	Detection	Reducing the energy consumption and delay	Although traditional intrusion protection mechanisms can detect external attacks, they cannot defend against internal attacks.	-
	[31]	Trust management	Mitigation	Enhanced privacy	If the CH is damaged, the new node connection process will fail.	MATLAB
UASN	[32]	SecFUN Cryptographic	Mitigation	Reduce delay and energy consumption	However, due to the high computational complexity, the scalability of this scheme is questionable.	-
	[33]	STMS (SVM) Trust model	Detection	High communication and network lifetime	However, the method cannot protect privacy or resist attacks. It does not consider computational overhead and it is not context-aware.	-
	[34]	AoA physical layer authentication	Detection	Effectiveness	The experimental limit is under static UASN and can only be within a certain range of sight.	-
	[35]	TR physical layer authentication	Detection	The node has low overhead and high accuracy	Because the nodes in complex underwater environments are subject to a lot of interference, GMM validation performance data can be biased in the case of complex parameters.	-

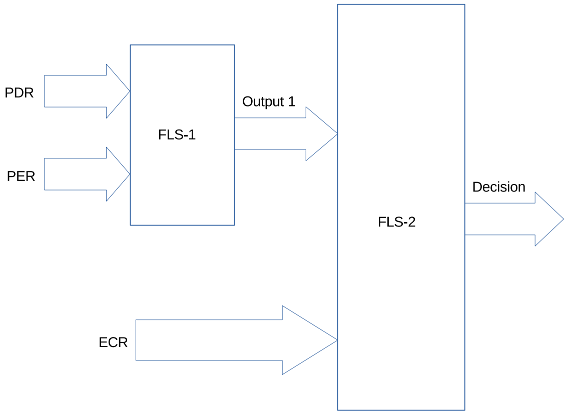

FIGURE 5. HFS-based trust management model comprising of 3 input parameters and 2 fuzzy logic units [24].

Sybil attacks. A hierarchical fuzzy system was used due to the rule explosion and curse of dimensionality that the single-layer fuzzy system suffers from. The proposed solution does not consume resources as much as many other proposed security mechanisms for Sybil attacks based on encryption and decryption.

In the proposed mechanism, sensor nodes sense and store data within a cluster that has a cluster head. Data is transferred to the cluster head by sensor nodes using a routing protocol. The cluster heads transmit their collected data via a surface station to the base station where end users can access data or modify it. An autonomous underwater vehicle (AUV) detects obstacles such as rocks, wrecks, and obstructions. To ensure that a legitimate node is not compromised, the behaviour of sensor nodes is checked to ascertain whether it is malicious via three trust parameters: packet drop rate (PDR), packet error rate (PER) and energy consumption rate (ECR). The proposed scheme achieves data confidentiality and integrity as only authorized nodes can read/extract from the exchanged data. Also, malicious nodes cannot manipulate data via the proposed trust management model. Finally, authentication is ensured as only authorized nodes can communicate. The proposed mechanism for trust management was simulated using Xfuzzy-3.5 and shows significant performance in detecting compromised nodes.

2) MULTI-FACTOR AUTHENTICATION

The underwater sensor network is characterized by path loss, variable speed, high propagation delay as well as constraints in power and bandwidth which makes it very different from terrestrial wireless sensor networks. This necessitates that peculiar security mechanisms are developed for achieving secure UASN. Several existing routing and MAC protocols developed in this context are quite prone to attacks that can affect the quality of the network or disrupt its connection in its entirety. Such attacks can cause catastrophic consequences and network performance degradation in critical applications such as oil and gas spill monitoring. Although some related works have studied underwater network security, they have (mostly) used a predefined threshold beyond which malicious attack detection is not optimal. The authors in [22] are thus motivated to propose a multi-factor authentication model for detecting malicious activities thereby helping to secure UWSN from several attacks. The authors proposed algorithms for both the monitoring, detection, and mitigation of these attacks. One advantage of the proposed method is that no calculations are required and detection and monitoring are the primary means of addressing the Sybil attack issue. Prior schemes to [22] such as [37] use utility functions that depend on hop count and remaining energy which is suitable when the network connectivity is reliable and nodes have relatively sufficient resources as seen in traditional sensor networks. The authors argue that to detect malicious activities these metrics may not be sufficient. This motivates the proposal of a multi-factor authentication mechanism [22] which involves updating the packets' header information by including an identifier based on MAC address (IMAC), direction of arrival, and hop count (HC) for validating incoming packets (See Algorithms 1 and 2). This has several advantages, for instance, accurate time synchronization, accurate localization or further communication to the sink (by sensor nodes) is not required. In the proposed approach, each node extracts the header from packets that it overhears based on its transmission range (TR). The node has stored information about its neighbors which it compares with the header information. Whenever there is a disparity between the two pieces of information, the node labels such packets as malicious and sends an alert to its neighbors while it isolates itself. This way the protocol is less computation-intensive. However, the authors consider a network size with up to 20 nodes and no evaluation and results are found in this work.

Algorithm 1 Monitoring Process in [22]

```
Objective: Listen to incoming packets (within TR)
           and produce a monitoring report.
Input: Source node's IMAC, angle of arrival (AoA),
       HC, Incoming packet
Output: Monitoring report
Initialize: Request identifier to zero
while overhearing packet $\in$ TR do
    for Source node's IMAC, AOA, HC $\in$ TR do
        for Request identifier > 0 and $\leqslant$255 do
            assign Request identifier for each Pkt into
             Monitoring report extract IMAC, AOA,
             and HC from incoming packet  into
             Monitoring report Increment Request
             identifier by 1
        end
    end
end
```

3) CLUSTER-BASED AUTHENTICATION

In underwater sensor networks, it is quite easy for adversaries to manipulate the communication channel and the sensor

Algorithm 2 Detection & Mitigation Process [22]

```
Objective: Detecting and mitigate malicious activities
           in UWSN.
Input: Source node's and neighbour's IMAC, AOA,
       HC, Incoming packet
Output: Accept (for further authentication), reject or
        authenticate incoming packet
while Monitoring report $\neq \oslash$ do
    for Source node's IMAC, AOA, HC $\in$ TR do
        Check the IMAC$_i$,AOA$_i$,HC$_i$ from M$_j$;
        if Monitoring report contains duplicate
        requests then
            Reject packet & execute protection
            mechanism
        else
            Accept packet for further authentication
        end
        Compare the Source node's IMAC, AOA, and
        HC from the Monitoring report with those of
        its neighbors;
        if IMAC, AOA, HC are equal with those of
        the neighbors respectively then
            Incoming packet has been authenticated
        else

        end
        Reject packet & execute protection
        mechanism
    end
end
```

nodes. In this context, data authentication and integrity are very crucial for the network to scale and survive. Thus, the authors in [30] propose a secure authentication and aggregation method for clustered UWSN due to the stability and conciseness provided by clustered arrangements. The gateway authenticates the cluster head in each cluster to ensure that only valid nodes handle each cluster. Also, communication is handled securely to ensure it is not compromised during the network operation. This method is proven to ensure the security of all nodes for safe communication. Similarly, the proposed method improves data reliability as it reduces energy consumption and delay as compared to other state-of-the-art techniques.

4) PHYSICAL-LAYER-BASED AUTHENTICATION

The channel impulse response is one of the physical layer characteristics which has location-specific characteristics useful for authenticating UASN. Another important ingredient that can be used to achieve security in underwater wireless communication is the time-reversal mechanism. Time reversal is a signal processing technique that leverages the reciprocity of the wireless communication channel for achieving spatial and temporal convergence.[4] The authors of [26] proposed a PHY authentication mechanism using TR resonating strength and CIR is used to authenticate nodes before communication is established for data transmission. As opposed to prior literature [39], [40], [41], [42], [43], the mechanism is not limited to line-of-sight and thus, cooperation from neighboring nodes is not needed for an authentication decision to be made. The authentication process is a two-step process: CIR is estimated using a pilot/probe signal, and then by calculating the maximum TR resonating strength, the node is authenticated via the convolution of time-reversed CIR with the CIRS in the database. Via simulations, the result shows that the use of location-specific CIR is simple and effective. The probability of authenticating the receiver correctly (probability of detection), and authenticating the attacker node as the receiver (probability of false alarm) using various thresholds prove the authentication scheme performs well in underwater acoustic sensor networks.

Another effort at using physical layer authentication for underwater sensors using a location-specific feature i.e. angle of arrival (AoA), was proposed by [34]. In a sender-receiver-attacker (Alice, Bob, Eve) scenario, Alice (the sink node) maintains a database of the estimated AoA[5] which is compared with the AoA in the CIR database by computing the Mahalanobis distance[6](with the database). The AoA measurement during the $n-$th time slot is given by $Q(n)$

$$Q(n) = (\hat{\alpha}, \hat{\beta})(n) = (\alpha,\ \beta) + k_{\alpha,\beta}(n) \tag{1}$$

Whenever the distance is less than a threshold value the incoming packets are authenticated as sent by Bob. Both Bob and Eve ensure line-of-sight (LOS) propagation in the 3D underwater environment[7] and can send data to Alice. The authors assume a static LOS underwater acoustic network while considering the probability of detection and the probability of false alarms as metrics. They carry out simulations by providing estimates for 1000 AoAs for both Bob and Eve by varying the SNR. The results show a good trade-off between these two metrics.

[4] A simple TR communication system involves two transceivers A and B. The latter sends a pilot pulse signal (that propagates through scattering and multi-path) to the former to initiate communication. Then transceiver A sends the required information on the time-reversion signal of the waveform received through the same channel. Leveraging the channel reciprocity, the TR retraces all incoming paths and harvests the energy from the multipath environment to focus the signal to the intended receiver both in space and time domains. Thus, it is a low-complexity form of communication [38].

[5] Azimuth and elevation AoA are used for an additional layer of security as the adversary can hardly mimic both features simultaneously.

[6] Mahalanobis distance measures the distance between a point from an unknown sample and a distribution of known samples. It is suitable for classifying data that are multi-dimensional in nature and finding similarities between variables in observation and known collection of a set of variable sets. Such similarity is inversely proportional to the Mahalanobis distance.

[7] NLOS has challenges with respect to multipath phenomena which makes it difficult for the sink to make AoA estimations.

5) AES AND DSS-BASED AUTHENTICATION FRAMEWORK

One major challenge observed in the literature is that security solutions based on the network layer up to the application layer are majorly overlooked despite the diverse amount of proposals on underwater acoustic networks. This motivates the authors in [32] to propose a security framework for UASN called SecFUN which is based on the most effective cryptographic primitives (both symmetric and asymmetric-based cryptography) for authentication. The proposed scheme is shown to be configurable and flexible. It can accommodate different features and security levels which has the potential to satisfy the requirements of the UASN. Particularly, for sending data to the sink by authentication via encryption and digital signatures.

Via SecFUN, data confidentiality, integrity, authentication, and non-repudiation can be achieved since it uses Advanced Encryption Standard (AES) in Galois Counter Mode (GCM) as well as Digital signature-based algorithms as the foundational building block. The proposed scheme is extended to channel-aware routing protocol as a proof of concept to support the cryptographic primitives developed. The approach can provide security requirements such as confidentiality, integrity, and authentication in unicast and flooding-based routing protocols. The overall energy consumption and latency were used as the metric to evaluate the overall performance of the proposal. Results reveal that a comprehensive and flexible solution can be achieved at a reasonable cost while meeting the requirements of UASN. Although AES encryption is simple as it uses peculiar features of GCM, it could be resource-intensive [22].

B. CLUSTER-BASED SECURE SYNCHRONIZATION

One of the primary concerns in a UWSN is achieving secure time synchronization. The authors in [27] propose CLUster-based Secure Synchronization (CLUSS) protocol characterized by accurate synchronization and deployed to achieve security. An underwater sensor network with a large number of uniformly scattered *static* nodes (or nodes with low mobility relative to signal propagation speed) is considered. All nodes have the same transmission range and each node only knows and communicates with its direct neighbors without knowing whether they are malicious or safe. The network mainly consists of ordinary nodes, beacons, and cluster heads. The protocol securely executes cluster formation via cluster consistency checking before time synchronization. Then it performs time synchronization which is divided into three main phases: authentication, intercluster synchronization, and intracluster synchronization. Parts of the last two phases can be executed in a concurrent manner to reduce message overhead in synchronization. Malicious nodes are removed from the network during the first (authentication) phase since nodes need to be authenticated to one another. In the second phase, the cluster heads synchronize themselves with beacons. This is done in sender-receiver mode while in the last phase (intracluster), ordinary nodes synchronize themselves with cluster heads.

CLUSS can detect abnormal end-to-end delay which improves the synchronization time accuracy. Via simulations, the authors show that as compared to traditional protocols CLUSS has the potential to reduce synchronization errors as well as the number of synchronization messages when the underwater network is attacked by malicious nodes. The influence of packet loss and retransmissions was not incorporated in this work and identified as a potential future direction in addition to real ocean experiments.

C. ENCRYPTION-BASED SCHEMES

1) NEIGHBOR DISCOVERY

Sensor node movement in an underwater environment is usually not predictable which makes secure neighbor discovery for a successful exchange of information very challenging. When neighbor discovery is compromised, it is easy to launch an attack (e.g., Sybil and wormhole attacks) which can lead to less throughput and loss of confidentiality. Conventional cryptographic schemes cannot *come to the rescue* because of the peculiar nature of the open acoustic channel and harsh underwater conditions [28].

In view of the above, the authors in [28] aim to mitigate neighboring attacks via a proposed true-neighbor algorithm. The algorithm operates before the actual communication starts to determine whether nodes are malicious or genuine. There is a symmetric key-based encryption mechanism for node authentication with a single key shared throughout the network operation. The senders' location coordinate is encrypted and sent. To prevent a replay attack later, the time of sending the message is timestamped and appended to the information sent.

One of the advantages of symmetric-based encryption is that fast and efficient computations can be performed. Similarly, the protocol [28] is easier to implement since the configuration of the shared key can occur when the nodes are being created and deployed. This way, risks involved with the key exchange are averted despite the unsafe and active underwater environment. However, if the secret key becomes known by the attacker via system hijacking, the security of the entire network is compromised since only a single key is shared throughout the network. The algorithm's performance was evaluated in UnetStack with respect to end-to-end delay. An improvement can be made on the proposed scheme based on diverse systems and application requirements using different encryption algorithms.

In applications where fast computation and minimal hardware complexity are major requirements, lightweight symmetric encryption techniques can be used. Also, various keys can be used between node pairs such that, even if the keys between some pairs of nodes are compromised, the entire system is not affected and it remains intact. Another area for future work is key sharing in real time if the computational requirements and overhead are well managed [28]. A typical flowchart for mitigating neighborship attacks in UnetStack software is demonstrated in Fig. 6.

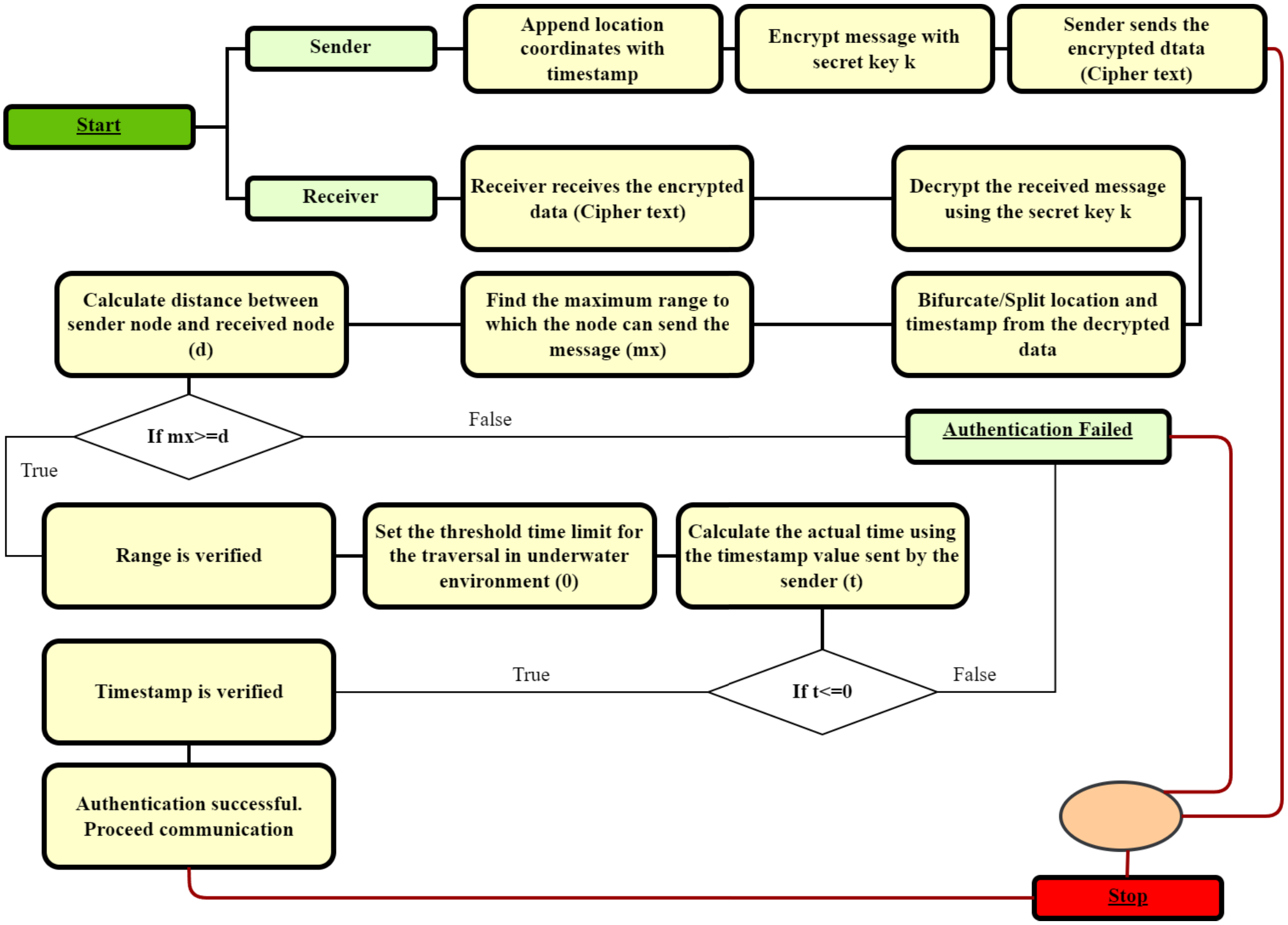
Start
Sender
Append location coordinates with timestamp
Encrypt message with secret key k
Sender sends the encrypted dtata (Cipher text)
Receiver
Receiver receives the encrypted data (Cipher text)
Decrypt the received message using the secret key k
Bifurcate/Split location and timestamp from the decrypted data
Find the maximum range to which the node can send the message (mx)
Calculate distance between sender node and received node (d)
If mx>=d
False
True
Authentication Failed
Range is verified
Set the threshold time limit for the traversal in underwater environment (0)
Calculate the actual time using the timestamp value sent by the sender (t)
If t<=0
True
False
Timestamp is verified
Authentication successful. Proceed communication
Stop

FIGURE 6. Flowchart for mitigating neighbourship attack in UnetStack software [28].

Algorithm 3 Key Generation Process in [29]

```
If there exist two numbers $a$ and $b$ ($a \neq b$) and both $a$ and $b$ are prime
Calculate $= a * b$
Calculate $\phi(n) = (a - 1) * (b - 1)$
Select integer gcd $(\phi(n), e) = 1;\ 1 < e < \phi(\mathrm{n})$
Calculate $e * d = 1 \mod \phi(n)$
Public key $(e, n)$
Private key $(d, n)$
$N$ is sensed data and $Q$ is encrypted data
Encrypt data using private key
$Q = N^d \mod n$
$Q1 = Q^e \mod n\ B$
```

2) ENCRYPTION AND CLUSTER DATA AGGREGATION

Robust data aggregation, encryption, and data transfer are essential requirements in clustered underwater sensor networks. Ref. [29] study a clustered UWSN architecture where sensor nodes and super nodes (located at lowest depths send data to BS while other nodes can function as cluster heads) are first deployed in the network, then, tiers are formed and tier heads are selected. The tier head executes the algorithm for key generation (shown in Algorithm 3). Each sensor node generates the private key, and then senses and encrypts the sensed data. The sensed data is sent in a multihop fashion (via a communication chain constructed by a minimum spanning tree) to the tier head which aggregates all the encrypted data and routes it to the BS where it is decrypted. The use of data aggregation with the cluster (tier head) helps to reduce energy consumption within the network. A minimum spanning tree is constructed in a periodic fashion and thus whenever a node fails or loses connection and cannot contribute to the aggregated data, this does not affect the network negatively since other nodes can construct the communication chain. Similarly, during the aggregation process, the node ID is sent with the encrypted message which makes every node aware of the node ID of a node whose link has failed.

D. DETECTION USING TRUST-BASED SCHEMES

Underwater acoustic networks are prone to attacks and the use of trust models has thus been considered one of the most important tools for responding to attackers. Some of the prior schemes in UASNs used key management and authentication techniques which have been effective for dealing with intruders, but for attackers who have already caused an invasion, they are not capable of handling them. To manage such internal attacks, trust management systems are often resorted to. They are considered efficient and particularly more tolerant of such attacks. However, several key problems remain which are due to the nature of the underwater environment. Such include sparse deployment of underwater sensor nodes, the weak nature of the connection and communication links, narrow bandwidth, and high latency and the non-Gaussian behavior of underwater noise[8] which retards the developments made in this domain. This necessitates the need for investigating the development of efficient trust models that can be used to cope with internal attacks and proper network functionality.

1) BLOCKCHAIN DETECTION

The authors in [25] aim to use blockchain for Sybil attacks detection. This was achieved by incorporating a trust model with a blockchain method to achieve higher resilience to attacks. The network consists of three types of nodes: sensor nodes, cluster heads, and BS. The randomly deployed sensor nodes are low-powered and resource constrained. They sense the environment, collect, and process the data to be transmitted. Sensor nodes can also move with the water current and are not static. Thus, they could join a different cluster at a different time and also communicate with the BS or sink via a hierarchy. CH authenticates with newly joining SNs or excludes nodes that do not pass the authentication phase. For each sensor node, it generates a temporary cluster member ID. It aggregates all collected data and transmits it to the BS either directly or via other CHs. In this case, CHs are authenticated by the BS. The sensor nodes communicate with trusted neighbor nodes within a particular communication range and the data is forwarded to the BS via the CH in a multi-hop fashion. Each node is provided with a permanent and unique node ID at the beginning of network deployment. CH position cannot be taken by regular SNs as CHs are assumed not to be low-powered and are of a higher energy level compared to the regular sensor nodes. As such, it can store different trust values for sensor nodes due to its sufficient memory and processing capability. The proposed system is modeled as a Markov decision process where a source node interacts with its neighbour nodes. Using Adaptive Neuro-Fuzzy Inference System (ANFIS) framework [31], trusted nodes are determined from the neighbour list. With the MDP model, three states are identified: trustworthy, uncertain, and untrustworthy. Using the ANFIS learning rule, the sender node learns about its forwarding node in each state. The node selects a trusted node based on the trustworthiness value learned. This way, the risk of breaching privacy by a malicious or compromised node is reduced completely.

2) NODE STATE INFORMATION-BASED

The authors in [15] present a novel Sybil attack detection scheme that uses the state information of nodes to reduce the vulnerability of underwater sensors. An adversary uses stolen information to replicate nodes. Such cloned nodes are placed in different locations where they communicate with neighbour nodes.

The authors study the malicious behaviours of such Sybil attackers and then propose a scheme for detecting them using node state information. In the proposed schemes, a beacon node is used to judge Sybil nodes with regard to the receipt of reply packets and the relationship between the communication frequency and residual energy of nodes recorded in a list. Then the beacon node makes its evaluation to identify the suspected node and compares the coordinate distances broadcasted by the suspected node to the beacon node and by the suspected node to its neighbor nodes. The authors calculate the detection rate of a malicious node as shown below:

$$q = q_1 q_2 q_3 \tag{6}$$

where q_1 is the random distribution rate of sensor nodes, q_2 is the probability of determining suspicious nodes based on sensor nodes, and q_3 is the rate of detecting malicious nodes based on the algorithm. The proposed scheme was numerically analyzed and evaluated using MATLAB for its detection accuracy and showed that the detection accuracy can be as high as 94%.

3) SVM TRUST-BASED MODEL

Due to the ability of machine learning to adapt to the dynamic underwater environment as opposed to traditional trust calculation techniques, the authors of [33] adopted this powerful artificial intelligence-based tool taking into account the unavailability of labeled training sets in actual applications. Thus, they used $k - means$ algorithm to divide the training set into two labels. In this case, the $k - means$ algorithm is considered attractive because of its simple nature and the speed of solving clustering-based problems. The support vector machine (SVM) is used to train the labeled dataset for generating the prediction model. This is also needed to solve the machine learning problem within the small sample framework. The essence of this proposal is to provide an accurate trust value and efficient malicious node detection. The efficiency of collecting trust evidence is improved by dividing the network into clusters, similarly, a double cluster head approach is deployed to improve the network security and lifetime. The methods and techniques proposed to address similar problems in terrestrial networks are usually unfeasible in the underwater environment particularly because of the peculiarities such as the unreliable nature of the underwater scenarios and their complexity. The authors in [33] aim at achieving an accurate and robust trust evaluation framework for underwater acoustic sensor networks and thus propose a synergetic trust model based on SVM. The authors divided

[8] Including Middleton Class A noise, Middleton Class B noise, and $\alpha-$stable noise wherever applicable. Non-Gaussian noise models are usually deployed for modeling ambient noise in the ocean [44]. Some underwater environments may also experience impulsive noise [45].

the network into interconnected clusters having cluster heads and cluster members that perform their roles in a synergetic fashion (see Fig. 7). The proposed synergetic trust model involves three steps: generation of trust evidence, calculation of the prediction model and cluster head monitoring and updating. In the first part, cluster members generate three kinds of trust evidence to properly reflect the most malicious behaviors. Using simulations the authors show that the proposed scheme was better than similar proposals in a sparse underwater sensor deployment environment and significant results were achieved with respect to the accuracy of detecting malicious nodes and the success rate of communication as well as network lifetime.

SVM is used to train a trust prediction model to evaluate an accurate trust value. The authors suggest the use of double cluster heads to enhance the network security as well as extend the network lifetime. Using simulations, the authors show that the proposed scheme is better than other similar proposals in the sparse underwater sensor deployment environment. Also, significant results are achieved with respect to the accuracy of detecting malicious nodes, the success rate of communication, and network lifetime. However, the complex and inaccessible nature of underwater environments impacts prediction accuracy, so it is important to study the impact of environmental factors and parameters on trust prediction accuracy as well as the exploration of practical trust models.

E. DISCUSSION

The BS carried by a water vehicle or some highly advanced nodes can be deployed within the network to be involved in the detection and mitigation process. Similarly, abnormal network features can be learned and the results could be used in the design of protocols for managing Sybil attacks. It is also evident that there is a need for the development of Simulators to help researchers further understand and solve problems relating to Sybil attacks in different underwater environments. In addition to security, energy consumption, lightweight solutions, and low overhead are some of the characteristics sought after in proposed solutions. The complex and inaccessible nature of underwater environments impacts prediction accuracy, so it is important to study the impact of environmental factors and parameters on trust prediction accuracy as well as the exploration of practical trust models. The next section places more emphasis on methods and aspects relating to these works.

IV. METHODS AND PECULIAR ASPECTS

Identifying methods and distinctive characteristics of Sybil attacks is among the research objectives formulated in this study. Hence, this section identifies and discusses many methods as well as the aspects employed to prevent, detect, and mitigate Sybil attacks. Before dwelling into the classification of key aspects of underwater wireless communication, some peculiar characteristics are summarised and presented in Fig. 8 based on [3] and [5].

TABLE 4. Methodological aspects.

Aspects	Focus	Ref.
Algo Math tools	Markov	[25]
	Adaptive neural fuzzy	[31]
	CSVMs	[27]
	Artificial intelligence	[33]
	K-means + SVM	[33]
Trust	Trust model	[24], [25], [33]
	Trust evidence	[33]
Technologies	Blockchain	[25]
Security techniques	Multi-factor authentication	[22]
	Symmetric encryption	[28], [32]
	128-bit block cipher	[32]
Peculiar	Cross layer	[32]
	Time synchronization	[27]
	Aggregation	[29], [30], [32]
	Hash value	[30]
	Beacon	[15], [27]
	Double CH	[33]
	Cluster identity	[30]
	Time-reversals	[35]

A. METHODS

Several methods have been used in the course of preventing, detecting, and mitigating Sybil attacks in underwater networks (see Table 4). The adaptive neural fuzzy inference system was used to evaluate the reliability of sensor nodes in [31]. In [27], a distributed outlier detection scheme called Central hyper ellipsoid support vector machine (CSVMS) was used to detect end-to-end abnormal delay and identify malicious nodes [27]. Besides the above, $K-means$ and support vector machine algorithm was used in [33] to generate the trust evaluation model to solve the problem of insufficient evidence as a result of scarce/sparse environment.[9]

Blockchain was combined with a trust management model in [25] where it was used with a Hash function to ensure invariance.[10] One form of trust model is the hierarchical trust model which gives the node three chances to authenticate an identity: the first time with the neighbor node, the second time with the neighbor node of the same cluster, and the third request with the base station [24].

Another use of trust models is predicting the trustworthiness of nodes through trust models as done in [25] using hidden Markov model (HMM). The approach used in [33] improves security via the trust framework which leverages SVM. Another use of the trust model appears in [31] where the whole trust model is divided into three components: node profile information, link trust, and node trust. Node profile information is used for authentication while link and node trust were used to evaluate the trustworthiness of nodes.

[9] In other work, artificial intelligence-based schemes were used as they can deploy existing knowledge to improve efficiency and better cope with changing environments.

[10] In underwater wireless networks, blockchain can effectively ensure network **invariance**, privacy, and security [25]. Blockchain support distributed systems/environments and has characteristics such as confidentiality, integrity, authentication, and availability. Any attempt to copy the identity of a legitimate node will be detected in the blockchain.

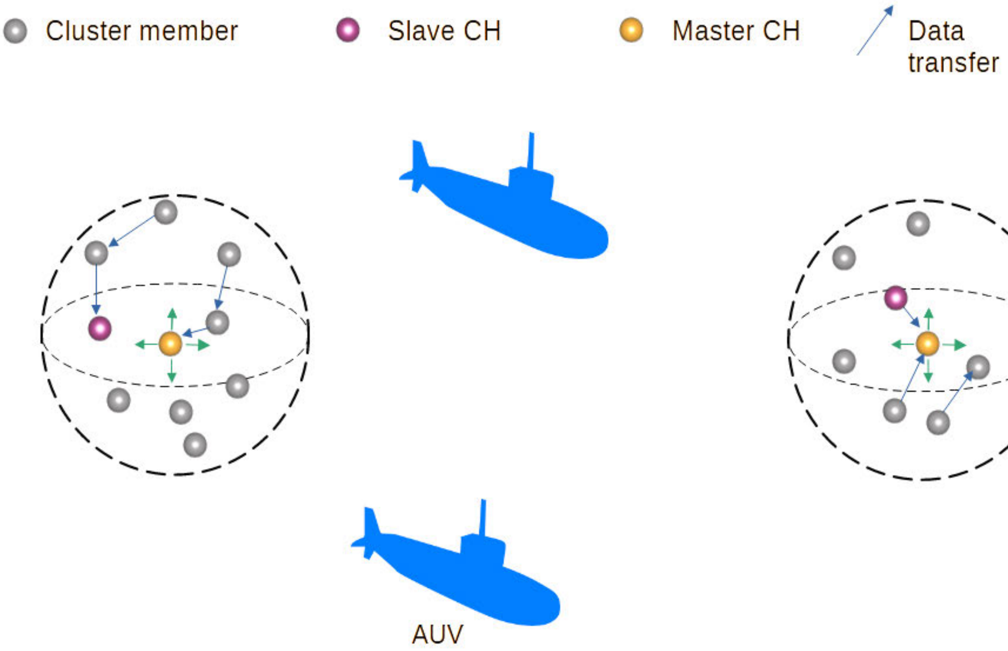

FIGURE 7. 3D clustered network architecture in [33] with BS (not shown) located on the surface of the sea.

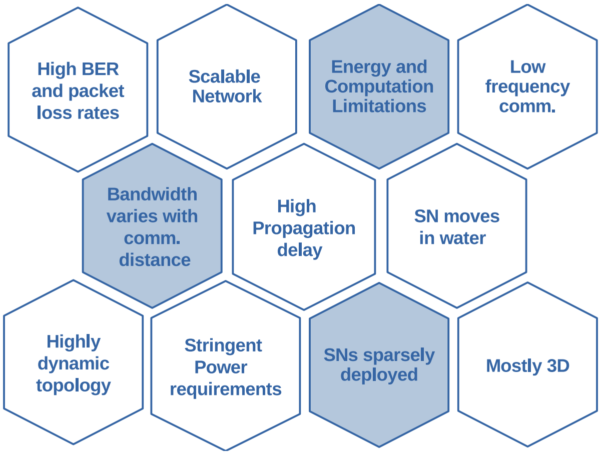
High BER and packet loss rates
Scalable Network
Energy and Computation Limitations
Low frequency comm.
Bandwidth varies with comm. distance
High Propagation delay
SN moves in water
Highly dynamic topology
Stringent Power requirements
SNs sparsely deployed
Mostly 3D

FIGURE 8. Peculiar characteristics of underwater sensor networks.

Authentication is a common approach by which Sybil attacks can be prevented. The multi-factor authentication model based on zero-knowledge proof can better protect WSNs from Sybil attacks and malicious detection as used in [22]. For authentication, two kinds of mechanisms are commonly used: symmetric encryption (secret key) and asymmetric encryption (public key) [32].[11] In SecFUN, Galois counter mode was used as a security building block for encrypting and authenticating data operations using a 128-bit block cipher such as AES [32]. GCM method involves one-time message identity authentication and uses a ciphertext equal in length to the plaintext length, so there is no extra overhead, which makes it suitable for bandwidth-limited devices. In [28], authentication is performed using symmetric encryption. In this case, the location coordinates of the sender are encrypted with a timestamp. CLUSS model proposed in [27] can reduce synchronization error and energy consumption.

The concept of data aggregation has also been used with encryption. For instance, in [29], sensors sense node information from nearby nodes and send it to neighbor nodes. Data aggregation is applied and accepted by cluster head nodes using encryption technology. Another method considered is cluster-based authentication which includes two important aspects, cluster head security authentication and protected data aggregation [30]. Thus, [30] presents a cluster-based security authentication and data aggregation method for WSNs. First, the cluster head authenticates to the gateway to prove that the cluster is now running safely [30]. Then each sensor uses symmetric encryption to send data to the cluster head, and finally aggregate the data back to the base station.[12] This method requires minimal network energy and delay.

Time reversal is another method used with the key features of the channel impulse response for physical layer authentication [26]. Based on this method, nodes can be detected using a threshold range. which has the potential to reduce

[11] Symmetric encryption means that encryption and decryption use the same secret key, but decryption requires two secret keys [32].

[12] The cluster head authenticates the identity of the cluster to ensure its validity and reduce security risks.

overhead [35]. Timestamps can also be used to effectively prevent nodes from bypassing authentication mechanisms and thus inhibiting a breach as exemplified in [28].

Node state information can also be exploited in the course of detecting Sybil attacks with a high detection accuracy and success rate as done in [15].

B. ASPECTS

Some distinctive characteristics of Sybil attacks for distributed networks have been identified earlier in this work. Fig. 9 summarises these aspects based on the knowledge and insight obtained from the current studies regarding Sybil attacks. In these section, more emphasis would be placed on trust management, energy consumption reduction and management.

1) TRUST MANAGEMENT

One way of addressing Sybil attack is to have a trusted agent certify the identities of users [6]. Any update from an untrusted sensor node is considered invalid [22]. Trust management has several advantages and it can be combined with different techniques under diverse frameworks. One of such is blockchain, as done in [25] which was evaluated using the hidden markov model. Others are discussed below.

a: AUTHENTICATION

Trust management can be used to address the sensor leakage problem as solved in [24] where a trust management model of the hierarchical fuzzy system was deployed. The hierarchical trust model gives the cluster head node three ways of authenticating an identity. The CH gets confirmation from its immediate neighbor node about the identity of the required node, the CH could also obtain confirmation from a neighbor node of the same cluster, and finally, the CH could request from the base station. Another fundamental technique for managing Sybil attacks is the use of a central authority to verify trusted nodes. Several other sub-components of this kind of architecture can have different unique aspects. Particularly, for judging whether nodes are trusted, the behavior of a node can be used to determine whether it is legitimate or not. The trust parameter value can also be assigned for judging the credibility of nodes. For instance, in the trust parameter value (see [24]), if the trust factor value increases, it implies lower credibility and thus higher risk. Trust evidence can be used to detect malicious nodes.

b: ANFIS-TRUST MANAGEMENT

One of the techniques adopted to evaluate the trustworthiness of a sensor node is ANFIS. In [31], the whole trust model is divided into three parts: node profile information, link trust, and node trust. Other factors for trust evidence include energy consumption as an observation index. In this case, each node is observed. When a malicious node starts, it consumes more energy than a normal node. A high observation index for a node implies that the node cannot be trusted [31].

c: SVM-TRUST MANAGEMENT

In clustered architectures, both cluster heads and cluster members can be used to effectively predict trust and collect evidence. Cluster members can facilitate trust prediction since they can record the communication behavior of neighboring nodes and send the necessary information to the base station. A typical way of developing a trust evaluation model can involve combining graph-based algorithms and a classification algorithm [33]. For instance, combining $K - means$ and SVM algorithm as done in [33] is useful when there is insufficient evidence. Another technique for defining trust is the interval between successful and unsuccessful communication.

2) ENERGY CONSUMPTION

Energy efficiency is paramount especially since energy is wasted as a result of malicious attacks [5]. Thus, it is important to balance the energy of network nodes in underwater networks. UASN uses acoustic wave communication, so it faces great environmental challenges one of which is high energy consumption as well as low bandwidth and bit rate, and high transmission delay [32]. Thus energy consumption minimization is fundamental in the management of UASNs as well as attack detection, prevention and mitigation.

a: SecFUN

Energy consumption is mainly caused due to message passing and as such the energy required for computation is not a major concern when Sybil attacks are launched. In view of this, [32] emphasized the need for a security framework that ensures security and minimizes additional overhead and its associated energy waste due to the need to transfer extra information. Another technique is using packet buffers, especially at high traffic loads. This can reduce energy consumption and increase packet delivery rates [32].

b: CLUSTER-BASED PROTOCOLS FOR ENERGY REDUCTION

Clustering is another method by which energy consumption can be reduced. The cluster head authenticates the identity of the cluster members to ensure their validity thereby reducing security risks. Each cluster head authenticates the gateway individually so, attacks by malicious nodes controlling the cluster are avoided. As can be observed, the method uses little network energy and reduces delay [30] since authentication is done only within a cluster. Additionally, the use of multiple sinks can reduce long-distance transmissions. This has the potential to reduce excessive energy consumption and communication latency [30].

Cluster-based CLUSS time synchronization protocol [27] helps to reduce energy consumption via a clustered architecture where normal nodes authenticate to the cluster head and the cluster head authenticates to the beacon. Using the approach, time accuracy can be improved and some func-

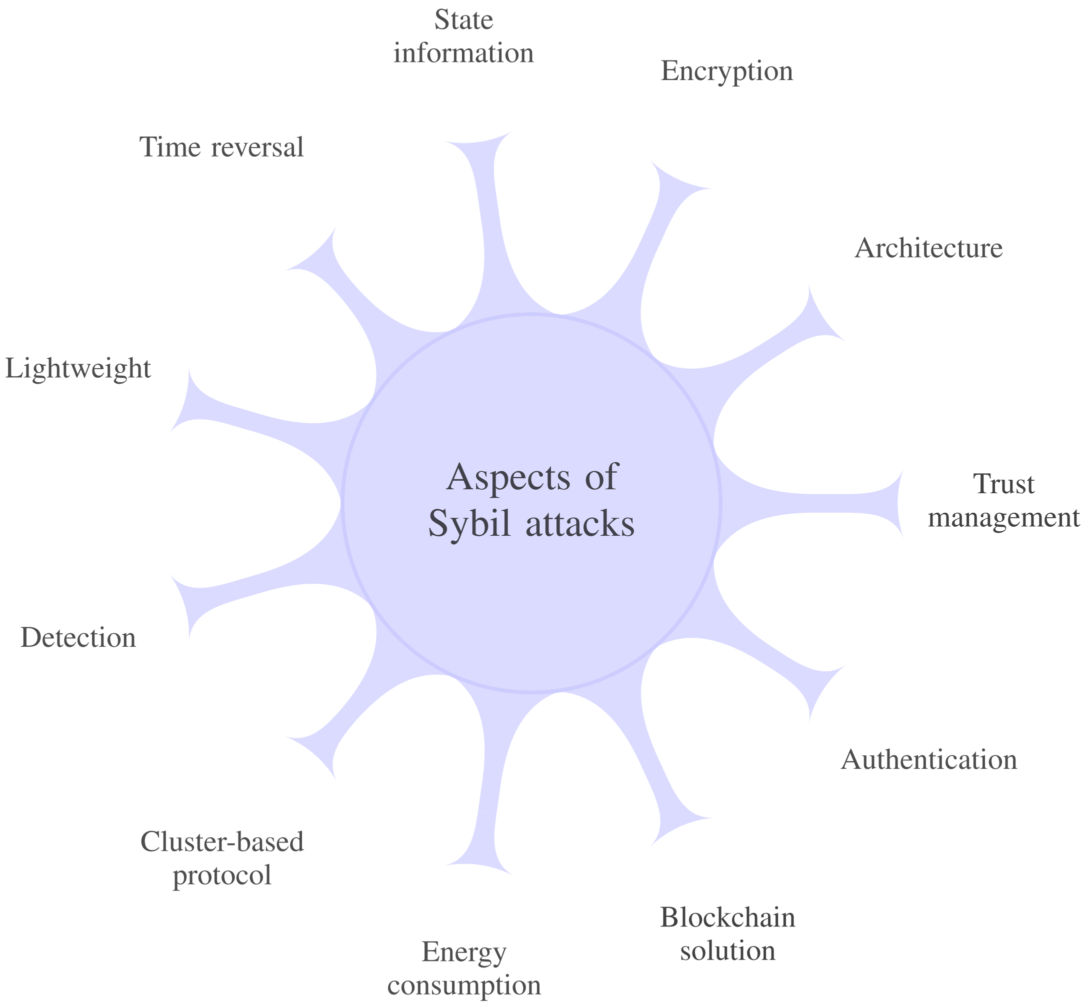

FIGURE 9. Peculiar aspects of Sybil Attacks management techniques in underwater networks identified from literature.

tions can be executed simultaneously to reduce the number of messages required for synchronization. Thus, reducing synchronization error and energy consumption.

C. DETECTION

This study identifies various techniques that are reported in the literature for detecting Sybil attacks. Some of these techniques for detecting Sybil attacks include the use of firewalls, node state information and time reversals. These techniques have been discussed to reflect how they are applied to detect Sybil attacks in underwater wireless networks.

1) FIREWALLS

Firewall rules, isolation of malicious packets, and effective broadcast of information to neighboring nodes can help detect Sybil attacks. If a node receives suspicious packets from multiple neighbors, it creates firewall rules, creates firewall rules, isolates the malicious packets, and broadcasts an alert to neighbouring nodes about the malicious activity [22].

2) NODE HEADER INFORMATION

Another approach is to use nodes' header information for accurate Sybil attack detection. This can be achieved when each node overhears packets within its transmission range and extracts the header information from these packets. The header information is compared with pre-existing stored header information about the neighbour of the nodes. The valid nodes take action by labelling an incoming packet as malicious, generating an alert for neighbouring nodes whenever the stored information does not match with the header information of an incoming packet. The malicious is also isolated [22].

3) TIME REVERSAL

Time-Reversal has a remarkable ability to take advantage of the multi-path energy from underwater environments [35]. It is a signal-processing technique that has been used in a wide spectrum of engineering applications [46]. The communication nodes are distinguished by the spatial dependency of link channel impulse response (CIR),[13] and the nodes are distinguished by comparing the current CIR with the CIR in the database [26]. Suppose there is a sink node, a legitimate node, and a malicious node. The malicious node requests to access the sink node. At this time, the sink node estimates the CIR using the pilot signal of the legitimate node and compares it with the database to verify the type of the node and effectively detect spoofing attacks [35]. The spatial dependency of acoustic link channel impulse response offers a natural signature for each link in UASNs.

D. ARCHITECTURAL ASSUMPTIONS

Several architectural assumptions are made related to node positioning and mobility, clustered and unclustered architectures, the nature of traffic load, single or multiple sinks, and other environmental dynamics. Particularly, static nodes were assumed in [15] while dynamic nodes were considered in [27] in a multi-hop architecture. Dual cluster heads were assumed in [33]. Multiple sink nodes were assumed in [30] while [32] assumed a high traffic load. Also, a dynamic underwater environment was assumed in [28]. This section provides further details on these assumptions.

Li et al. [15] assumed that all nodes are static in their physical locations and are labeled. Node instability was considered in [27] as nodes constantly repeat the process of leaving and joining, which necessitates that more attention be paid to cluster maintenance costs. To cater to the network instability, if a cluster head leaves the network, the system performs, the system performs the process of cluster formation and assigns a new cluster head to a new form of cluster. Ref. [33] also considers a clustered architecture to improve the efficiency of the collection of trust evidence.

In many cases, a single sink cannot cater to the large-sized or widely dispersed underwater sensor network architecture and thus, multiple sinks would be a better option in such cases. Communication may also be facilitated at the level of the sinks if required. The use of multiple sinks can reduce latency and excessive energy consumption [30]. Sometimes, the traffic load is high which could affect performance measures such as packet delivery rates and energy consumption [28]. In such cases, packet-buffering would be a promising approach to manage the situation (see [32]).

V. CHALLENGES AND FUTURE RECOMMENDATIONS

To achieve the fourth research objective of this study, the challenges and future directions are discussed in this section.

A. CHALLENGES

It is important that data transmission in underwater networks are secure to ensure reliable data transfer [47] and an efficient operation of its target application. Generally, security challenges in this context could be associated with routing, data aggregation, localization and intrusion detection [48]. A number of other challenges associated with Sybil attacks in underwater sensor networks are discussed in this section. Fig. 10 summarizes these challenges based on the knowledge and insight obtained from the literature.

1) MEDIUM ACCESS

With a security breach, several functionalities such as medium access become marred. Particularly, the underwater networks are distributed in nature and they communicate using acoustic waves over a wireless medium [49]. Whenever Sybil nodes are introduced into the network, they compete with legitimate nodes for channel access which affects the coordination within the network.

2) DYNAMIC UNDERWATER ENVIRONMENT

Underwater environments are sometimes unpredictable which makes the design of Sybil attack detection and mitigation quite challenging as techniques needed to detect and mitigate Sybil attacks largely depends on the harsh and unique nature of the underwater environment. In addition, the deployment of sophisticated sensors that can partly cushion the effects of the surroundings via power control and long transmission range connections which could be expensive. In general, there is a level of difficulty associated with undersea deployment and design due to the dynamic nature of the environment. This makes recovery difficult and such network deployment is time-consuming and cost-ineffective [7].

3) PROPAGATION CONDITIONS

Challenges experienced by researchers aiming at detecting, preventing, and mitigating Sybil attacks in underwater sensors are related to the propagation conditions, channel peculiarities in the underwater environment, and the different characteristics exhibited by unique water bodies. Also, the environment could negatively affect the propagation of radio signals thus affecting Sybil attack detection accuracy [15], [50]. Particularly, this makes it difficult to directly adapt many of the proposed solutions for addressing the Sybil attack in terrestrial wireless sensor networks. As such, agreement protocols would need a redesign while factoring in the peculiarities of the deployed environment. Hence, not all protocols that can be used on land can be easily adapted to underwater environments.

In relation to the above, Sybil attacks can occur at different layers of the protocol stack such as the MAC, routing, and application layers [32]. The characteristics of these and their considerations differ below waters. For instance, routing and clustering underwater would require 3D-aware protocols and algorithms as opposed to terrestrial communication. Similarly, in ground-based networks, external monitoring devices such as UAVs can easily visit a bounded location whereas the sensors deployed in oceans could be located deep below the

[13] The use of the CIR makes it unnecessary to implement authentication at the upper layer thus resulting in a lightweight solution.

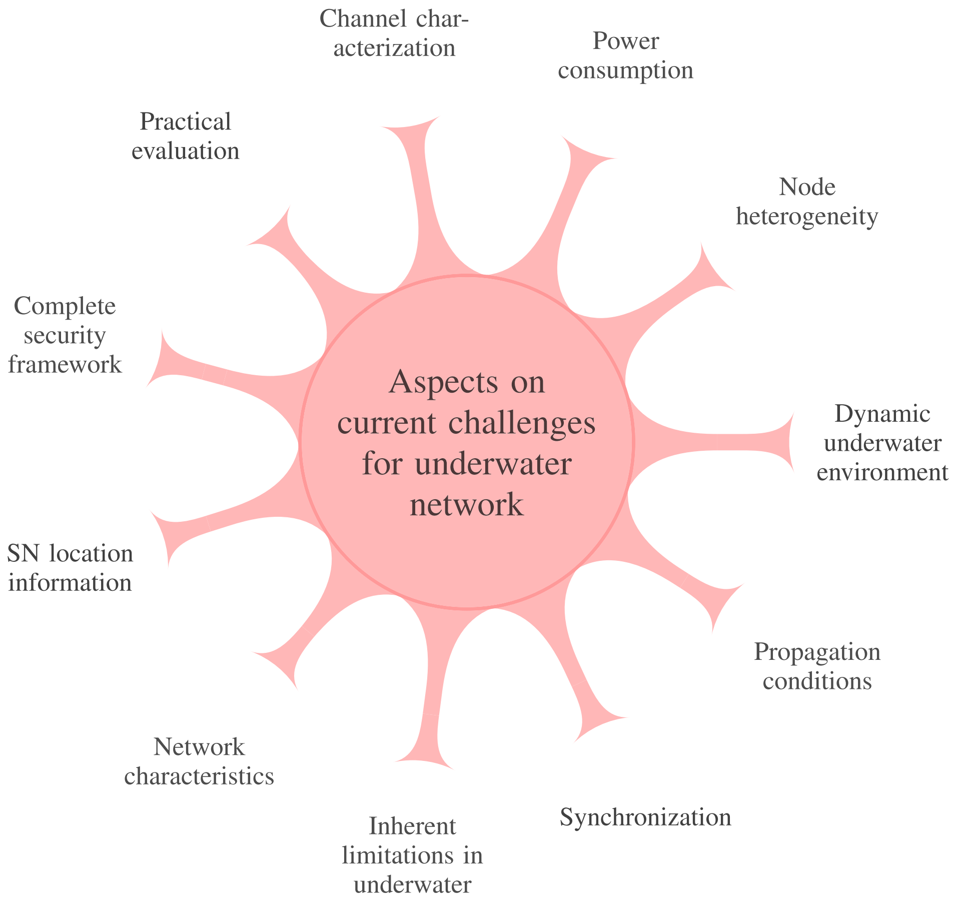

FIGURE 10. Aspects of the technical issues and challenges identified.

sea. Many such nodes are not static due to the movement of the waters. Thus, several aspects of these scenarios would be affected.

4) SYNCHRONIZATION

Another challenge related to propagation conditions is achieving timely, effective, and accurate time synchronization. This is important for detecting and mitigating the Sybil attacks as well as informing other nodes that an attacker has been identified. It is also vital for re-routing, isolating Sybil nodes, and effective network coordination. However, time synchronization mechanisms should be energy-aware to minimally reduce energy consumption in the course of preventing, detecting, or mitigating Sybil attacks. One major factor that would help to achieve a timely synchronization is improving the transmission speed [51]. This is another major challenge due to the well-known transmission limitations of underwater sensors and the unique characteristics of the environment.

5) INHERENT LIMITATIONS IN UNDERWATER ENVIRONMENTS

The environmental challenges faced by underwater acoustic sensor networks are quite significant which generally limits the kinds of Sybil attack prevention solutions that can be developed. For instance, the network is characterized by low bandwidth, transmission delay, low bit rate, and high energy consumption [32]. Furthermore, underwater environments where sensors are deployed vary in depth, and atmospheric conditions including severe weather, different pressure, and underwater layers. Thus, preventing Sybil attacks knowing the characteristics of the potential environment (e.g., sea, lake, wind speed, etc.,) should take top priority for attack prevention. Successful and large Sybil attacks are much more harmful and quite difficult to detect in many cases. Although the Sybil attack can be detected via the level of energy consumed within the network due to the Sybil node's misrepresentation of identities, the network itself requires some energy in the process of detecting such anomalies. Thus, preventing Sybil attacks from the outset should be prioritized to avoid the cost involved in mitigating a devastating attack.

6) NETWORK CHARACTERISTICS

UWSNs have some peculiar characteristics which can be conveniently leveraged. However, this might also create room for launching Sybil attacks even after the initial network deployment. In many cases, the network is scalable and thus, Sybil nodes can be added to the network maliciously. Such additions could make accurate geographic routing difficult coupled with the fact that the use of GPS might not be suitable while providing a solution. Particularly, GPS signals use radar waves in 1.5GHz which do not propagate in water [3]. Although scalability is an advantage in UWSN, malicious Sybil nodes can be added to the network after initial deployment which poses security risks.

7) SENSOR NODE LOCATION INFORMATION

For effective packet delivery in UWSNs, routing is very essential [3]. Nevertheless, geographic routing protocols can be misled due to Sybil attacks as an attacker having several identities can pretend to be at different locations at the same time [3]. To facilitate this, proper knowledge of location information for legitimate and adversary nodes is important. In this case, the noisy environment makes it more challenging to ensure the location is accurately captured in a robust manner. Such noise includes multi-path and fading, and the refractive properties of sound which all lead to a high bit error rate [1].

8) COMPLETE SECURITY FRAMEWORK

Minimizing energy consumption in the course of managing Sybil attacks in UWSNs should be approached within a complete security framework which could be quite challenging. Although mitigating Sybil nodes could result in some overhead with respect to the cost of message exchange, holistically, it could help to reduce the node's energy consumption and prolong the network lifetime while improving the probability of successful transmissions at the same time via the selection of valid routes. In this regard, developing effective solutions to address the Sybil attack problem in underwater sensor and acoustic networks considering potential vulnerabilities in the protocol stack (e.g., using sleep and wake-up schedules, application and network level authentication, and minimizing the exchange of control information) is vital.

9) PRACTICAL EVALUATION

Investigating proposed Sybil attack prevention, detection, and mitigation solutions have been mainly investigated by simulations. It is worthy of note that a comprehensive simulator for studying Sybil attacks in different architectural setups is required to further improve the research prospects of this area. However, there is more to the practical underwater environments that might not be perfectly captured via simulation or analytical techniques. Although quite challenging and expensive, it is important to practically experiment with the underwater sensors to identify some of the salient factors that might hinder the full implementation of some earlier proposed techniques as well as other future solutions. This would provide more promising outcomes as the research community can focus on addressing these salient such as those relating to hardware design and underwater peculiarities. For instance, some water bodies are salty while some might include minerals that can adversely affect sensor materials over time. In any case, salt and algae will damage physical equipment in water as time goes by [7].

10) CHANNEL CHARACTERIZATION

Another challenge is accurate channel characterization of different underwater sensor environments at different depths in order to accurately determine the impact of Sybil countermeasures and the severity of different forms of attacks. This is resourceful in predicting the effectiveness of solutions proposed for such environments. Similarly, it is easier to capture the level of transmission reliability in characterized environments [7]. However, a huge cost and infrastructure are required for characterization especially via practical field tests. In this case, quantifying the number of propagation delays that can be experienced, noise, multi-path, path loss, and Doppler phenomenon would be quite intuitive. Large propagation delays degrade the performance of proposed underwater network protocols [52] and channel-dependent Sybil solutions. In the same vein, noise, multi-path, path loss, and Doppler effects affect the performance of UWSN [47].

11) POWER CONSUMPTION

The underwater acoustic environment consumes more power than terrestrial communication, thus requiring more complex processing at receivers [53]. This implies more impact of a Sybil attack on the system. Moreover, it becomes more pronounced considering that it is difficult to replace the batteries of underwater sensors. In other words, addressing the node energy constraints is vital [51]. The potential of leveraging sleep and wake-up mechanisms to save energy is thus very important. Overall, power consumption optimization should be made a priority to improve the underwater sensor network lifetime.

12) NODE HETEROGENEITY

Another major challenge with regard to the detection and mitigation of Sybil attacks is the heterogeneous nature of sensor nodes and other underwater network devices (such as modems) and their manufacturer-specific technologies. This sometimes makes cooperation and sharing information among them challenging due to the absence of compatible standards. For instance, communication with optical and acoustic modems in an operational setting is difficult because of the lack of a common standard and interface to support communication and message exchange [47]. This could make the practical application of generic proposals for detecting and mitigating Sybil attacks challenging. Thus, emphasizing the need for real-life deployment of proposed solutions. This way, the device specifications and nature of the environment can all be used to benchmark future proposals. The heterogeneity of sensors allows static and mobile nodes to be combined for specific applications but node communication interfaces to maximize data transmission is a problem [47].

B. FUTURE RECOMMENDATIONS

Proposals targeted at securing UASN from Sybil attacks and improving the network lifetime as well as other metrics

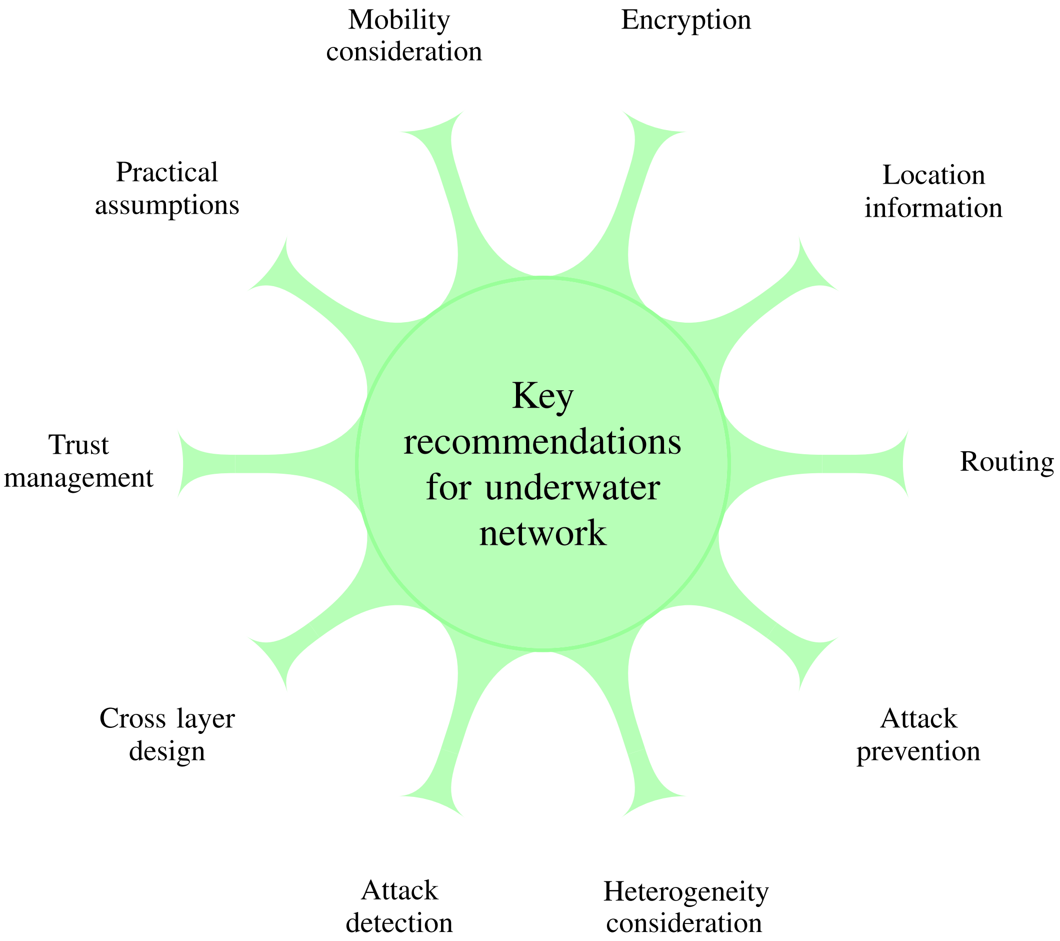

FIGURE 11. Recommendations and considerations for secure data transmission in underwater networks.

should put the peculiarities of the underwater environment in mind as those proposed for terrestrial sensor communication are not suitable due to the unique characteristics of underwater channel propagation. It is also important to comprehensively study the impact of Sybil attacks in different forms of water (like lake and ocean) at different depths, pressures, atmospheric situations, and underwater layers; not just in (almost) perfect conditions. The architecture in this case also differs from that of terrestrial sensor networks [22].

On a general note, proper traffic monitoring, broadcast range optimization, network topology construction, packet transmission and re-transmission regulation, and sleep/wake-up scheduling are all important [5] to protect against attacks in underwater sensor networks; one of which is Sybil attack. Proposed wireless security solutions should be effective to detect Sybil attacks with small or very minimal overheads. They should also be of reasonably low complexity. The information with regards to the depth of the sea should be considered and effective clock synchronization is required, i.e., horizontal and vertical time synchronization.

Here, we discuss key recommendations according to the knowledge and understanding acquired from the existing studies. Similarly, key aspects of these recommendations are presented in Fig. 11.

1) ROUTING

Secure Sybil-resistant routing protocols should meet the security objectives designed for protecting against false identities and ensuring data is safe and secure, especially in terms of the correctness of information as well as unavailability to Sybil nodes. Underwater networks require delay-tolerant communication protocols because the propagation delay underwater is higher [5]. Sometimes, re-transmissions are required due to environmental conditions. Thus, the introduction of Sybil attacks weakens the effectiveness of routing in underwater networks. It is also important to improve channel utilization, reduce routing overhead, explore self-configuring routing, and use the latest routing information while developing the routing algorithms [54].

2) ATTACK PREVENTION

In view of the importance of confidentiality in underwater sensor transmission, it is essential to develop solutions for preserving the confidentiality of data collected by sensors by authenticating nodes/information and protecting against Sybil and other forms of attacks. However, to practically and sustainably achieve this, lightweight solutions are required in view of the resource constraints of underwater sensors in several applications. This is mainly to ensure that the information is not assessed by unauthorized third parties. Such is required in maritime applications [3]. As mentioned earlier, Sybil nodes can intrude on the privacy of legitimate nodes even in the narrow band acoustic channels. To preserve the privacy of underwater sensors and ensure the confidentiality of their information without compromising their location accuracy, it is important to work toward attack prevention. The confidentiality of the packet and its integrity should be protected by making it a top priority. Preventing Sybil attacks ensures data integrity which implies that the data has not been altered by any adversary [3]. This is particularly critical in applications such as those for monitoring water quality in lakes [55]. As such, prevention of Sybil attacks should be prioritized as it is easier to manage as compared to attack mitigation when some damage might have been caused in the network.

3) HETEROGENEITY

The lack of a common standard interface between communicating entities is a fundamental challenge, especially for communication involving node heterogeneity [47]. Besides ordinary sensors, buoys, nodes with special functions (like super nodes), and underwater vehicles need to be equipped with interoperable communication facilities. Also, the allows different devices to be used for specific applications. However, the node communication interface to maximize data transmission is a challenge [47].

4) ATTACK DETECTION

Malicious nodes should be identified using resilient techniques. This also applies to very crucial nodes such as anchor nodes to prevent false dissemination [3]. In this case, the development of intelligent algorithms using advances in machine learning would be resourceful. The algorithm could learn about a safe underwater environmental conditions which can be used to detect possible outliers and attacks in the network where a Sybil node could be present. Particularly, nodes can move with ocean currents and oceanic animals which makes attack detection somewhat complicated [1].

5) CROSS LAYER DESIGN

Cross-layer design of solutions to Sybil attacks are also important such as proper sleep/wake-up schedules [5]. The heterogeneous nature of the security threats in underwater sensors requires a proper cross-layer design. Security protocols should achieve confidentiality, integrity,[14] availability, data/key freshness, authentication, and non-repudiation[15] [32].

6) TRUST MANAGEMENT

Acoustic channels are characterized by poor link quality, high propagation delay, and limitations in channel bandwidth. These make it vulnerable to several security threats. On the other hand, the design of complex but efficient security algorithms and key management solutions is difficult to implement in low-powered sensor nodes due to their effect on the overall network lifetime. In this case, trust management becomes very crucial as it can help to mitigate many forms of attack when properly utilized. Practical trust models should be developed especially those that can be deployed in real and underwater environments. The reputation trust model can be used to analyze the behavior of nodes as trust values can be assigned to ensure nodes are legitimate [5]. The behavior of neighbor nodes can be analyzed using reputation-based schemes. Also, via trust management, routes that involve malicious nodes or selfish nodes can be avoided [3].

7) PRACTICAL ASSUMPTIONS

In reality, underwater sensors are sparsely deployed due to the high cost of underwater hardware [3]. They are also majorly non-static because of water/oceanic movements. This should be accommodated in the design of underwater sensor protocols and security mechanisms as well as in the prevention, detection, and mitigation of Sybil attacks. Similarly, underwater networks are mainly three-dimensional and of a large size. The network is majorly delay-tolerant and thus prevention, mitigation, and detection mechanisms should have minimal additional overhead.

It is also important to have a central entity, especially on initial deployment which could allocate keys to nodes and protect the introduction of Sybil nodes. The challenge, however, is that terrestrial networks could use the base station as the central entity which is majorly not the case for underwater networks especially when they are far from terrestrial systems. Although surface stations can perform a fundamental role in preventing attacks, the potential of integrating UAVs for ensuring underwater network security is also worth investigating.

An autonomous underwater vehicle can also move around to monitor the network and collect information from sensor devices continually due to its higher energy resources, and sensors can be attached to those vehicles if required. Also, it is important to detect malicious attacks from the outset. It should also be noted that there could be many Sybil nodes especially since the underwater terrain is large and deep. Unless nodes are anchored in the ocean or at specific depths, it is difficult to assume detector nodes would not move in the ocean/water body due to the oceanic movements. Proper scheduling would also be required in the implementation of

[14] Integrity can be achieved via a keyed cryptographic tag.

[15] Non-repudiation means a node cannot deny sending a message. This can be achieved via digital signatures.

Sybil attack mitigation and detection mechanisms to prolong the lifetime of the network.

8) MOBILITY

Water currents are sometimes high and the sensors move with water. However, in a few scenarios, some sensors are anchored below the ocean while some sensors are suspended at specific depths [3]. Note that measures should be taken so that adversaries do not take advantage of mobility to attack the network [5] and mobility-aware techniques that can defend against Sybil nodes are required in underwater wireless communication. Node mobility should also be generally factored into the design of security techniques for UWSN [3]. In this context, the peculiarity of low propagation delays and the particular challenges associated with mobility has to be borne in mind [3]. Useful techniques for addressing and even preventing the Sybil nodes from launching attacks could be leveraged. Particularly, while putting the mobility of sensor nodes due to ocean drift into perspective.

9) ENCRYPTION

Underwater wireless sensors often have significant security challenges due to environmental problems. In addition, encryption and decryption methods consume resources [24]. Encryption and authentication should be fast and powerful to prevent intruders. It takes a long time to detect intruders due to the large propagation delays in UWSN. Similarly, it is important to avoid paths containing malicious nodes [3]. Route encryption is a promising technique that has been considered for improving network security under the water while also addressing energy consumption and the bandwidth requirement of many traditional encryption schemes [54] and thus can be explored for addressing Sybil attacks.

10) LOCATION INFORMATION

Algorithms should be better adapted to address the characteristics of the underwater channel and to determine the location of sensor nodes even in the presence of attacks such as Sybil and wormhole attacks [3]. In order to properly tag data, it is important to ensure proper localization. This helps in making accurate route decisions [3]. In other words, it is important to detect attacks and verify the location of sensors in the highly dynamic underwater environment. Accurate node localization in this case is very important for different underwater architectures (clustered or dispersed). Localization accuracy should be improved in cases where a malicious anchor node is introduced. The localization schemes for terrestrial-based sensor networks do not work effectively in underwater environments due to physical characteristics such as multipath, Doppler effect, and fading which causes variation in the acoustic channel in addition to node mobility, bandwidth constraints, and sparse node deployments. Therefore, suitable localization schemes are required [3].

Similarly, in addition to ensuring proper localization and preventing and mitigating the impact of Sybil attacks on routing processes within the network, there are a number of other considerations. For instance, [54] emphasizes the importance of ensuring improved channel utilization, minimal routing overhead, and self-healing routing mechanisms in case of a failure, as well as the use of the latest routing information to improve the entire routing process.

11) ENERGY CONSUMPTION

Nodes save energy by discarding routing table data packets due to suspicious sensor nodes unknown sensor nodes [22]. Moreover, malicious nodes have the tendency to increase energy consumption in the network. This is because trusted nodes might receive the wrong packets due to malicious activities which also increases the packet loss rate within the network [31]. With this, the introduction of Sybil attacks further worsens the energy waste in the network. Thus, the causes of packet loss should be properly inferred using novel techniques tailored to the underwater acoustic channel [53]. Another important consideration is the development of mechanisms to reduce high bit error rates and losses of connectivity at different depths.[16] All these are important since the prevention and management of Sybil attacks can be quite challenging depending on the physical condition of the water. This is especially because sometimes the underwater channel experiences extreme conditions due to salinity, variations in temperature and density [56].

C. DISCUSSION

Underwater sensor networks deployed in oceans experience several dynamics and thus, cannot be assumed to be static or small-sized. Secret keys that are allocated by an external terrestrial entity (whenever available/applicable) or a central authority on the ocean/water should have a higher transmission range to cover a significantly large amount of sensor nodes. Sensor nodes that are not covered may be catered for by a different central entity. In this case, efficient utilization of memory is required. This can be achieved by using two keys (one shared by the central device and the other shared by nodes) to establish a connection. However, a challenge is that in underwater sensor networks, the deployment of nodes is sparse as underwater sensors are more expensive. In this case, each node can possess a unique key that makes it impossible for secret data to be divulged especially when the central device is involved in the communication between any two devices.

Central devices are vital to achieving security in underwater sensor networks. The central devices possesses a record of all prior established connections by node pairs. It can revoke any device that ''misbehaves'' within the network as well as inform other nodes which are connected to such nodes. Similarly, the number of nodes involved in the communication can be controlled. However, the use of a central device can only cover a limited amount of sensor nodes, and

[16] Ocean depth is a strong indication of seawater density as shown in [56].

others outside this range cannot be authenticated. Another problem associated with the scheme is that the central device becomes the main target of compromise. Also, the process of distribution of keys consumes energy, and adding new sensors to the network becomes impossible after the network deployment is completed.

A large pool of keys can also exist such that before deployment each node is pre-assigned keys or key-related information. A secure link can then be established by neighboring nodes with a shared key. The choice of key distribution mechanism and discovery of shared keys might however vary.

Validating keys involves a high overhead especially if all the keys need to be verified. Moreover, identities can also be impersonated. When the identity of a node is stolen, this technique cannot detect such an attack [57]. This method is suitable for reasonably dense networks. However, effectively deploying it for large-scale underwater environments would be very challenging because of the sparse nature of node distribution in the network as well as node mobility due to water tides and the probabilistic nature of the key distribution method.

Nonetheless, a consistent result is a desired characteristic of security mechanisms. Particularly, the robustness of a Sybil mitigation or prevention mechanism could be made to depend on a threshold to ensure the strength of security can be easily increased or tuned based on the network conditions. This is also useful when trade-offs need to be put into consideration. Having unique keys makes authenticating two nodes easy. However, if more than the threshold number of devices required for guaranteed security is compromised, the network becomes highly vulnerable which can also occur when the threshold of the network is too small. The network can be easily compromised with a higher threshold, the number of keys to be maintained becomes higher which increases the overhead in the network.

Using radio resource testing has been confirmed to be effective for addressing Sybil attacks in ground-based networks. This scheme can protect against all forms of Sybil attacks. It requires low memory and has low communication overhead. However, whenever an attacker uses multi-radio devices simultaneously, it can launch a successful attack. Also, it involves high transmission power consumption. During radio resource testing, the battery of legitimate nodes can be drained which makes such nodes unable to transmit over the channel [20]. In the case of underwater communication, the propagation conditions would also affect the effectiveness of these types of schemes.

LESSONS FROM Ad-hoc NETWORKS

Finally, we highlight some of the common assumptions for different kinds of architectures and approaches proposed in ad-hoc networks for mitigating Sybil attacks. The intention, in this case, is that researchers can look into applicable assumptions for future proposals in underwater sensor and acoustic networks.

Prior work on ad-hoc networks has presented the following assumptions [8]: static network, mobile network, small WSN size, the base station allocates keys to all sensor nodes before they are deployed, malicious nodes introduce Sybil nodes by providing false identities, one radio can not transmit on two or more different frequencies at the same time, clocks are synchronized, all nodes are initially trustworthy, and new sensor nodes enter into the network including malicious nodes. Others include: only one Sybil attacker entering into the network after initial deployment, and the network is divided into clusters with a primary detector in a cluster with higher processing and storage capacity. The cluster head leads the cluster while there is another (minimum of two) trusted secondary detector node. In some schemes, three detectors are required, the position of detector nodes is known, nodes are mobile, no specific hardware is required, multiple observer nodes share their data, and a malicious node launches an attack.

VI. CONCLUSION

This paper presents a survey of Sybil attack detection and defense mechanisms in underwater sensor and acoustic networks. The models and assumptions in the proposed schemes were discussed with their unique architectures and peculiar aspects. Cluster-based architectural solutions, energy consumption management, use of firewalls, node status, and time reversal-based mechanisms were all identified. Then the role and nature of assumptions were also emphasized. Aside from these, other important issues were discussed which include Sybil node detection as well as the challenges and future recommendations in light of the peculiar characteristics of underwater wireless communication. One such is trust management and energy consumption. Particularly, effective trust handling and management helps to easily identify distrusted nodes or adversaries within the network. Similarly, secure Sybil-free routing, attack prevention, the need to support heterogeneous entities within the underwater architecture, improved attack detection mechanisms, cross-layer solutions, incorporation of practical assumptions, and addressing the challenge of mobility are some of the future directions identified.

AUTHOR CONTRIBUTIONS

Zuriati Ahmad Zukarnain: project initiation, supervision, and funding acquisition; Oluwatosin Ahmed Amodu: conceptualization, investigation, resources, writing–original draft, writing–review and editing, visualization, and project administration; Cui Wenting: conceptualization, investigation, resources, and writing–original draft; Umar Ali Bukar: writing–review and editing and visualization.

ACKNOWLEDGMENT

The authors would like to thank everyone who provided valuable suggestions and support to improve the content, quality, and presentation of this article.

REFERENCES

[1] H. Li, Y. He, X. Cheng, H. Zhu, and L. Sun, ''Security and privacy in localization for underwater sensor networks,'' *IEEE Commun. Mag.*, vol. 53, no. 11, pp. 56–62, Nov. 2015.

[2] C. Peach and A. Yarali, ''An overview of underwater sensor networks,'' in *Proc. 9th Int. Conf. Wireless Mobile Commun. (ICWMC)*, 2013, pp. 31–36.

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

[4] X. Che, I. Wells, G. Dickers, P. Kear, and X. Gong, ''Re-evaluation of RF electromagnetic communication in underwater sensor networks,'' *IEEE Commun. Mag.*, vol. 48, no. 12, pp. 143–151, Dec. 2010.

[5] 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.

[6] J. R. Douceur, ''The sybil attack,'' in *Proc. Int. Workshop Peer-Peer Syst.* Cham, Switzerland: Springer, 2002, pp. 251–260.

[7] E. Felemban, F. K. Shaikh, U. M. Qureshi, A. A. Sheikh, and S. B. Qaisar, ''Underwater sensor network applications: A comprehensive survey,'' *Int. J. Distrib. Sensor Netw.*, vol. 11, no. 11, Nov. 2015, Art. no. 896832.

[8] A. Vasudeva and M. Sood, ''Survey on sybil attack defense mechanisms in wireless ad hoc networks,'' *J. Netw. Comput. Appl.*, vol. 120, pp. 78–118, Oct. 2018.

[9] A. M. Bhise and S. D. Kamble, ''Review on detection and mitigation of sybil attack in the network,'' *Proc. Comput. Sci.*, vol. 78, pp. 395–401, Jan. 2016.

[10] H. Yang, Y. Zhong, B. Yang, Y. Yang, Z. Xu, L. Wang, and Y. Zhang, ''An overview of sybil attack detection mechanisms in VFC,'' in *Proc. 52nd Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. Workshops (DSN-W)*, Jun. 2022, pp. 117–122.

[11] S. Kaur and A. Kumar, ''Techniques to isolate sybil attack in VANET—A review,'' in *Proc. Int. Conf. Electr., Electron., Optim. Techn. (ICEEOT)*, Mar. 2016, pp. 720–726.

[12] S. Goyal, T. Bhatia, and A. K. Verma, ''Wormhole and sybil attack in WSN: A review,'' in *Proc. 2nd Int. Conf. Comput. Sustain. Global Develop. (INDIACom)*, Mar. 2015, pp. 1463–1468.

[13] A. Arshad, Z. M. Hanapi, S. Subramaniam, and R. Latip, ''A survey of sybil attack countermeasures in IoT-based wireless sensor networks,'' *PeerJ Comput. Sci.*, vol. 7, p. e673, Sep. 2021.

[14] Z. A. Abdulkader, A. Abdullah, M. T. Abdullah, and Z. A. Zukarnain, ''A survey on sybil attack detection in vehicular ad hoc networks (VANET),'' *J. Comput.*, vol. 29, no. 2, pp. 1–6, Jan. 2018.

[15] X. Li, G. Han, A. Qian, L. Shu, and J. Rodrigues, ''Detecting sybil attack based on state information in underwater wireless sensor networks,'' in *Proc. 21st Int. Conf. Softw., Telecommun. Comput. Netw.*, Sep. 2013, pp. 1–5.

[16] F. Medjek, D. Tandjaoui, I. Romdhani, and N. Djedjig, ''Performance evaluation of RPL protocol under mobile sybil attacks,'' in *Proc. IEEE Trustcom/BigDataSE/ICESS*, May 2017, pp. 1049–1055.

[17] R. John, J. P. Cherian, and J. J. Kizhakkethottam, ''A survey of techniques to prevent sybil attacks,'' in *Proc. Int. Conf. Soft-Comput. Netw. Secur. (ICSNS)*, Feb. 2015, pp. 1–6.

[18] M. Demirbas and Y. Song, ''An RSSI-based scheme for sybil attack detection in wireless sensor networks,'' in *Proc. Int. Symp. World Wireless, Mobile Multimedia Networks*, 2006, pp. 570–574.

[19] K.-F. Ssu, W.-T. Wang, and W.-C. Chang, ''Detecting sybil attacks in wireless sensor networks using neighboring information,'' *Comput. Netw.*, vol. 53, no. 18, pp. 3042–3056, Dec. 2009.

[20] J. Newsome, E. Shi, D. Song, and A. Perrig, ''The sybil attack in sensor networks: Analysis & defenses,'' in *Proc. 3rd Int. Symp. Inf. Process. sensor Netw.*, Apr. 2004, pp. 259–268.

[21] J. Heidemann, M. Stojanovic, and M. Zorzi, ''Underwater sensor networks: Applications, advances and challenges,'' *Phil. Trans. Roy. Soc. A, Math., Phys. Eng. Sci.*, vol. 370, no. 1958, pp. 158–175, Jan. 2012.

[22] A. Al Guqhaiman, O. Akanbi, A. Aljaedi, and C. E. Chow, ''Lightweight multi-factor authentication for underwater wireless sensor networks,'' in *Proc. Int. Conf. Comput. Sci. Comput. Intell. (CSCI)*, Dec. 2020, pp. 188–194.

[23] A. Agrawal, R. Kumar, and M. Agrawal, ''Modeling of underwater noise,'' in *Proc. OCEANS*, May 2019, pp. 1–6.

[24] A. A. Islam and K. A. Taher, ''A novel authentication mechanism for securing underwater wireless sensors from sybil attack,'' in *Proc. 5th Int. Conf. Electr. Eng. Inf. Commun. Technol. (ICEEICT)*, Nov. 2021, pp. 1–6.

[25] M. Arifeen, A. A. 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.* Cham, Switzerland: Springer, 2021, pp. 467–476.

[26] M. Khalid, R. Zhao, and X. Wang, ''Node authentication in underwater acoustic sensor networks using time-reversal,'' in *Proc. Global Oceans*, Oct. 2020, pp. 1–4.

[27] 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.

[28] A. Deshmukh, S. Deo, and B. R. Chandavarkar, ''Mitigating neighborship attack in underwater sensor networks,'' in *Proc. 12th Int. Conf. Comput. Commun. Netw. Technol. (ICCCNT)*, Jul. 2021, pp. 1–6.

[29] G. Khan, K. K. Gola, and R. Rathore, ''Robust data aggregation, encryption and data transfer in UWSNs,'' in *Proc. 1st Int. Conf. Next Gener. Comput. Technol. (NGCT)*, Sep. 2015, pp. 403–407.

[30] 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.

[31] M. M. Arifeen, A. A. Islam, M. M. Rahman, K. A. Taher, M. M. Islam, and M. S. Kaiser, ''ANFIS based trust management model to enhance location privacy in underwater wireless sensor networks,'' in *Proc. Int. Conf. Electr., Comput. Commun. Eng. (ECCE)*, Feb. 2019, pp. 1–6.

[32] G. Ateniese, A. Capossele, P. Gjanci, C. Petrioli, and D. Spaccini, ''SecFun: Security framework for underwater acoustic sensor networks,'' in *Proc. OCEANS*, Mar. 2015, pp. 1–9.

[33] G. Han, Y. He, J. Jiang, N. Wang, M. Guizani, and J. A. Ansere, ''A synergetic trust model based on SVM in underwater acoustic sensor networks,'' *IEEE Trans. Veh. Technol.*, vol. 68, no. 11, pp. 11239–11247, Nov. 2019.

[34] M. Khalid, R. Zhao, and N. Ahmed, ''Physical layer authentication in line-of-sight underwater acoustic sensor networks,'' in *Proc. Global Oceans*, Mar. 2020, pp. 1–5.

[35] R. Zhao, M. Khalid, O. A. Dobre, and X. Wang, ''Physical layer node authentication in underwater acoustic sensor networks using time-reversal,'' *IEEE Sensors J.*, vol. 22, no. 4, pp. 3796–3809, Feb. 2022.

[36] 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.

[37] 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)*, May 2015, pp. 1–6.

[38] B. Wang, Y. Wu, F. Han, Y. Yang, and K. J. R. Liu, ''Green wireless communications: A time-reversal paradigm,'' *IEEE J. Sel. Areas Commun.*, vol. 29, no. 8, pp. 1698–1710, Sep. 2011.

[39] 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.*, Oct. 2008, pp. 1838–1841.

[40] L. Xiao, G. Sheng, X. Wan, W. Su, and P. Cheng, ''Learning-based PHY-layer authentication for underwater sensor networks,'' *IEEE Commun. Lett.*, vol. 23, no. 1, pp. 60–63, Jan. 2019.

[41] 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)*, Jul. 2013, pp. 299–304.

[42] W. Aman, M. M. U. Rahman, J. Qadir, H. Pervaiz, and Q. Ni, ''Impersonation detection in line-of-sight underwater acoustic sensor networks,'' *IEEE Access*, vol. 6, pp. 44459–44472, 2018.

[43] R. Diamant, P. Casari, and S. Tomasin, ''Cooperative authentication in underwater acoustic sensor networks,'' *IEEE Trans. Wireless Commun.*, vol. 18, no. 2, pp. 954–968, Feb. 2019.

[44] X. Zhang, W. Ying, P. Yang, and M. Sun, ''Parameter estimation of underwater impulsive noise with the class b model,'' *IET Radar, Sonar Navigat.*, vol. 14, no. 7, pp. 1055–1060, Jul. 2020.

[45] K. Pelekanakis and M. Chitre, ''Robust equalization of mobile underwater acoustic channels,'' *IEEE J. Ocean. Eng.*, vol. 40, no. 4, pp. 775–784, Oct. 2015.

[46] F. Rachidi, M. Rubinstein, and M. Paolone, *Electromagnetic Time Reversal: Application to EMC and Power Systems*. Hoboken, NJ, USA: Wiley, 2017.

[47] S. Fattah, A. Gani, I. Ahmedy, M. Y. I. Idris, and I. A. T. Hashem, "A survey on underwater wireless sensor networks: Requirements, taxonomy, recent advances, and open research challenges," *Sensors*, vol. 20, no. 18, p. 5393, Sep. 2020.

[48] 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, pp. 1–15, Dec. 2021.

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

[50] M. Wen, H. Li, Y.-F. Zheng, and K.-F. Chen, "TDOA-based sybil attack detection scheme for wireless sensor networks," *J. Shanghai Univ.*, vol. 12, no. 1, pp. 66–70, Feb. 2008.

[51] J. Luo, Y. Chen, M. Wu, and Y. Yang, "A survey of routing protocols for underwater wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 1, pp. 137–160, 1st Quart., 2021.

[52] J. Heidemann, Y. Li, A. Syed, J. Wills, and W. Ye, "Underwater sensor networking: Research challenges and potential applications," USC/Inf. Sci. Inst., Marina del Rey, CA, USA, *Tech. Rep., ISI-TR-2005-603*, 2005.

[53] 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.

[54] M. Ayaz and A. Abdullah, "Underwater wireless sensor networks: Routing issues and future challenges," in *Proc. 7th Int. Conf. Adv. Mobile Comput. Multimedia*, Dec. 2009, pp. 370–375.

[55] 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.

[56] D. Makhija, P. Kumaraswamy, and R. Roy, "Challenges and design of MAC protocol for underwater acoustic sensor networks," in *Proc. 4th Int. Symp. Modeling Optim. Mobile, Ad Hoc Wireless Netw.*, 2006, pp. 1–6.

[57] R. Di Pietro, L. V. Mancini, and A. Mei, "Random key-assignment for secure wireless sensor networks," in *Proc. 1st ACM Workshop Secur. Ad Hoc Sensor Netw.*, Oct. 2003, pp. 62–71.

ZURIATI AHMAD ZUKARNAIN received the Ph.D. degree from the University of Bradford, U.K. She was the Head of the Department of Communication Technology and Networks, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia (UPM), where she is currently the Head of the Section for High Performance Computing, Institute of Mathematical Research. She is also a Full Professor with the Faculty of Computer Science and Information Technology, UPM. She is undertaking some national funded projects on QKD protocol for cloud environment and routing and load balancing in the wireless ad hoc networks. She is the Founder of ZA Quantum Sdn Bhd, a start-up company from UPM, to produce a software designing tool for quantum communication known as quantum communication simulator. Her research interests include efficient multiparty QKD protocol for classical network and cloud, load balancing in the wireless ad hoc networks, quantum processor unit for quantum computer, authentication time of the IEEE 802.15.4 with multiple key protocol, intradomain mobility handling scheme for wireless networks, efficiency and fairness for new aimd algorithms, and a kernel model to improve the computation speedup and workload performance. She has actively involved as a member of the editorial board of some international peer-reviewed and cited journals.

OLUWATOSIN AHMED AMODU (Member, IEEE) received the B.Tech. degree in electrical and electronics engineering from the Federal University of Technology, Akure, Nigeria, in 2012, the master's degree in computer science with a specialization in distributed computing from Universiti Putra Malaysia, in 2016, and the Ph.D. degree in wireless communication and network engineering, in 2021. He is currently a Lecturer with Elizade University, Ilara-Mokin, Ondo, Nigeria. He is also a Postdoctoral Fellow with the Wireless Communication and Networks Laboratory, Universiti Kebangsaan Malaysia. His research interests include sensor networks, machine-type communications, device-to-device communication, stochastic geometry, unmanned aerial vehicles, and terahertz communications.

CUI WENTING received the bachelor's degree in information management and information security from Shanghai Sanda University, China, in 2020. She is currently pursuing the master's degree in information security with Universiti Putra Malaysia. Her research interests include data security, network security, network protocols, sensor network security, and underwater network security.

UMAR ALI BUKAR received the B.Sc. degree in business information technology with concentration in e-commerce research and strategy from Greenwich University, U.K., the M.Sc. degree in computer network management from Middlesex University, Dubai, and the Ph.D. degree from the Department of Software Engineering and Information Systems, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, Malaysia. He is currently a Postdoctoral Research Fellow with the Centre for Intelligent Cloud Computing (CICC), Faculty of Information Science and Technology, Multimedia University, Malacca, Malaysia. His contributions have published in prestigious peer-reviewed journals and international conferences. His IT career has included work on several niche projects, with responsibilities ranging from teaching, research, and analysis. His research interests include crisis informatics, data analytics, text analysis, machine learning, and SLR.