A Survey on the Security of Routing Protocols for Underwater Acoustic Sensor Networks

Ayman Alharbi[1, *] and Muhammad Muzzammil[2]

[1]Department of Computer Engineering, College of Computer and Information systems, Umm Al-Qura University,
Mecca, ,Kingdom of Saudi Arabia

[2]College of Underwater Acoustic Engineering, Harbin Engineering University, Harbin 150001, China

Summary

Underwater acoustic sensor networks (UASNs) are the most widely adopted technology for a wide range of underwater applications such as monitoring of climate change impacts, monitoring of oil and gas production facilities, pollution monitoring, and military surveillance applications. However, UASNs exhibit various challenges and limitations such as high ocean interference and noise, narrow bandwidth and low data rate, long link delay, dynamic network topology, sparse deployment due to high production cost, and limited powered sensor nodes. Due to these challenges, ensuring the security of the sensor nodes and networking protocols has become more challenging. In this article, we present the results of our comprehensive survey on the security of routing protocols in UASNs. First, various network and routing layer security threats and attacks are presented. Second, the existing countermeasures to various threats and attacks are summarized. Third, the existing attack-resilient routing protocol schemes are compared in terms of their capability to address security requirements and attacks, merits and limitations, mobility, and performance metrics such as end-to-end delay, packet delivery ratio, energy consumption, and network lifetime. Finally, various recommendations and future directions are presented.

Key words:

Routing protocols, localization, security, secure routing, underwater acoustic sensor networks.

1. Introduction

Underwater acoustic sensor networks (UASNs) play a major role in the exploration of vast ocean systems, which are rich not only in marine life but also in other natural resources such as oil, gas, and other mineral deposits. UASNs also enable a wide range of underwater applications such as ocean monitoring, seismic monitoring, environment monitoring, and various military monitoring operations. Despite these impressive advantages and applications, UASNs have greater security challenges than terrestrial wireless sensor networks (TWSNs) due to their special networking environment. The existing security approaches adopted in TWSNs cannot be directly applied in UASNs [1] because underwater acoustic media suffer from long propagation delays, large multipaths, and severe Doppler effect due to the very low (1500 m/s) propagation speed of sound waves [2], [3]. Moreover, the underwater acoustic channel causes large attenuation and absorption, which lead to limited bandwidth and low data rates [4]. Moreover, UASNs are more severely energy-constrained than TWSNs because underwater acoustic modems are mostly battery-operated and consume more energy for transmitting and receiving information [5], [6].

The architecture of UASNs is mostly three-dimensional (3D) because any sensor node that they deploy may not be fixed due to the highly dynamic nature of sea water and because sensor nodes move explicitly with the water current [7]. Considering the dynamic topology of UASNs due to the water current and the high production cost of underwater sensor nodes, UASNs are sparsely deployed. This sparse deployment of sensor nodes causes security threats and provides room for the attackers to attack either the sensor node or the networking protocols. Previous research focused mainly on developing networking protocols that are energy-efficient, have a low end-to-end delay, and are less computationally complex and focused less on the security aspects. Recently, however, efforts have been made to secure networking protocols in open-system interconnection (OSI) layers [7-9]. The fundamental security requirements of UASNs are as follows:

1. *Authentication*: The identity of each communicating node in the network is verified to ensure that a nonlegitimate user/node cannot act as a legitimate one.
2. *Confidentiality*: Data transmitted over the network is protected so that it will be out of the reach of any nonlegitimate party.
3. Integrity: Data transmitted over the network cannot be altered by a nonlegitimate user/node.
4. *Availability*: Data requested by any legitimate user/node is available all the time, and network services operate normally even in cases of attack.

In the last decade, several review papers and surveys related to security in UASNs have been reported [7–15]. Domingo et. al [11] underlined the specific characteristics of underwater wireless communication networks (UWCNs), various possible attacks, and countermeasures to them. The authors highlighted core research challenges in secure time synchronization, localization, and routing. Han et. al [7]

Manuscript received January 5, 2022
Manuscript revised January 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.1.59

presented a survey paper that addressed layer-wise (physical layer, data link layer, network layer, and transport layer) security and identified respective attacks and countermeasures. Li et. al [16] presented security and privacy challenges in the localization of underwater sensor networks by reviewing various existing localization algorithms, identified various localization attacks, and presented countermeasures to secure localization schemes. Jiang et. al [8] comprehensively surveyed UASN security fundamentals and structures, layerwise security threats from the transport layer to the physical layer, countermeasures to various attacks, and cryptographic primitives. Recently, a comprehensive survey paper on routing protocols was reported [17] in which routing protocols were classified into three main categories: energy-based routing protocols, data-based routing protocols, and geography-based routing protocols. However, the paper and the reported routing protocols did not address the security aspect at all.

All these previous studies (summarized in Table 1) on secure UASNs were very general; they focused on UASN security requirements and various attacks related to the transport layer, the network layer, the data link layer, and the physical layer. In this survey paper, we focus on the network (routing) layer, related security threats and attacks, and corresponding countermeasures. First, we will briefly review previously reported UASN security requirements and routing layer security threats and attacks. Second, we will summarize various secure routing protocols presented in literature and classify them based on various routing layer attacks. Third, we will compare the existing secure routing protocols in terms of their methodology, anti-attacks, energy efficiency, complexity, advantages, and limitations. This study will assist the research community in reviewing existing secure routing protocols in one place and building more secure UASNs. The rest of the paper is organized as follows. In Section 2, we present various routing layer security attacks/threats. In Section 3, we summarize existing studies related to secure routing protocols. In Section 4, we compare existing secure routing protocols/schemes based on anti-attack and performance metrics. In Section 5, we highlight various recommendations and future directions. Finally, in Section 6, we conclude this paper.

2. Various Routing Threats and Attacks

In this section, we present various security threats/attacks related to the network/routing layer. These routing layer attacks have been reported but only briefly. We believe there is a need for a detailed presentation that can provide better insights on routing attacks for the research community and support the building of more secure routing protocols for UASNs.

The most reported routing layer attacks in literature are selective forwarding, wormhole attacks, Sybil attacks, sinkhole attacks, and blackhole attacks [10], [11], [18– 20]. These routing attacks are discussed in detail in the next sections.

2.1 Selective Forwarding

In a selective forwarding attack, the routing is restrained by dropping certain messages instead of forwarding them. In this type of attack, there are two important factors: the attacker location and the amount of dropped messages [18]. When the attacker location is near the sink, the maximum traffic will be attracted; and when more messages are dropped, the attacker will have greater energy to attack further. To avoid this attack in UASNs, the receiver should ensure that it is not losing messages due to a shadow zone or due to a selective forwarding attack.

Availability and integrity issues arise with a selective forwarding attack [20]. The countermeasures reported in literature are multipath routing and authentication, but they add to the communication overheads.

2.2 Wormhole Attack

In a wormhole attack, the attacker’s nodes use less propagation delay and a higher bandwidth link by generating a fast connection between two physical locations in the network either by using a radio frequency link above the sea surface or a wired link. Therefore, a fake neighbor relationship is built up between two nonlegitimate nodes [8], [11], [16]. Then the attackers transfer some selected messages from one end to the other through the generated fast wormhole link and reinsert it into the network [21]. Moreover, the routing protocol can choose the wormhole link as a route, which will enable the attacker to delay/drop messages and monitor the network traffic, which can be harmful for the network. The wormhole attack is shown in Figure 1. An out-of-band-connection called a “wormhole link” is shown between two nonlegitimate nodes. The legitimate nodes choose this route because this wormhole link appears to be shorter and faster due to less propagation delay. Therefore, the nonlegitimate nodes can drop or delay messages through this wormhole link. Availability issues arise with a wormhole attack [20].and the reported countermeasures are network topology construction [7], secure location of nodes and monitoring of traffic [20].

Table 1: Margin specifications

Ref. No	Publication Year	Main Objective(s)	Merits	References Cited
[10]	2010	Addressing threats, attacks and various issues	Identifying security requirements (characteristics) and layer wise attacks classification	21
[11]	2011	Survey of security for underwater wireless communication networks (UWCNs) and highlighting research challenges	Attacks on UWCNs and its countermeasures, security requirements and addressing security issues and open challenges for secure time synchronization, localization and routing protocols	17
[12]	2014	Systematic summaries and analysis of existing security attacks	Addressing security requirements, addressing security attacks and its defenses on node, data and network	24
[7]	2015	Comprehensive survey of the emerging topics arising from the secure communication in UASNs	Addressing and classification of secure communication in each OSI layer	13
[13]	2015	Addressing security and privacy in underwater localization	Identifying localization schemes in underwater sensor networks, various security attacks and privacy issues on underwater localization and countermeasures	15
[14]	2016	Addressing future aspects that can improve security in UASNs	Addressing security attacks and proposing possible future solution in terms of software defined cognitive networks, context aware routing and cross-layer communication	25
[15]	2018	Addressing security challenges and various applications of UWSNs	Discussion on security, applications and challenges of UWSNs	7
[8]		Comprehensive survey on security of underwater acoustic networks (UWANs)	Discussion on fundamental of network security, Addressing security threat in each OSI layer, review of countermeasure schemes against the typical security threats, review of securing UWANs protocols, review of cryptographic primitives designed for UWANs and discussion of open security issues	149
[9]	2011	Survey on threats, challenges and security issues of UWSNs	Addressing active and passive attacks, security requirements and security issues such are: key management, intrusion detection, trust management, secure localization, secure synchronization, and routing security	34
[11]	2011	Survey security for underwater wireless communication networks (UWCNs) highlighting research challenges	Presents UWCN attacks and countermeasures, security requirements; addresses security issues and open challenges for secure time synchronization, localization, and routing protocols	17

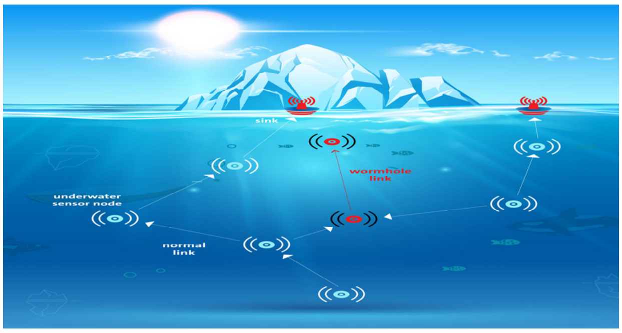

Fig. 1 Wormhole attack

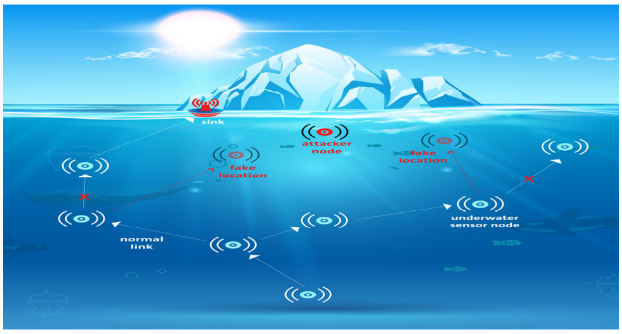

Fig. 2 Wormhole attack

2.3 Sybil Attack

In a Sybil attack, the attacker mimics a fake node location and identity in order to appear to exist in more than one place in the network at a time by compromising the identity of legitimate nodes [11], [18]. This type of attack becomes catastrophic because it targets the multipath routing and topology maintenance and thus, deceives the routing protocols as well [11],[22]. Geographic routing protocols are the most vulnerable routing protocols to Sybil attacks.
A Sybil attack is graphically illustrated in Figure 2. The attacker node advertises two fake locations of sensor nodes that do not physically exist. It is assumed here that all the sensor nodes are within the same communication range. The legitimate nodes will transmit the information to the fake nodes via the red link line shown in Fig. 2 and will avoid the transmission to the legitimate nodes shown by the crossed links. The fake sensor nodes are chosen because their lower depth compared to the sink nodes enables the attacker node to overhear the information transmitted by the legitimate nodes.
Authentication issues arise with a Sybil attack [20]. The countermeasures are authentication and location security [7], [11], [20].

Table 2: Margin specifications

Routing layer attack	Description	Security issue(s)	Defenses	Studies addressing attacks
Selective forwarding	Random dropping of certain messages by the attackers	Availability and integrity	Multipath routing and authentication	
Wormhole	Creation of lower propagation delay and high bandwidth link to tunnel messages from one end to another through dedicated RF/wired links	Availability	Network topology construction, secure location of nodes and traffic monitoring	[20], [24-26]
Sybil	Mimicking of fake node location and identity by the attackers and showing of existence in multiple places in the network	Authentication Authentication	Authentication and location security	
Sinkhole	Fraudulent announcement of the high-quality and shortest path towards the sink node to attract maximum traffic	confidentiality, availability, and integrity	Geographic routing, traffic monitoring, authentication and multipath route	[20], [27], [28]

2.4 Sinkhole Attack

In a sinkhole attack, also called a “blackhole attack” [18], the attacker node fraudulently announces a high-quality and shortest path towards the sink node to attract maximum traffic [11], [23].

Figure 3 shows a sinkhole attack. The attacker node attracts maximum traffic to itself due to its fake announcement of high-quality and shorter-depth information to the sink node. Furthermore, it can be seen that the legitimate sensor node avoids directly sending the information to the sink node despite its shorter range to the sink node. Therefore, a sinkhole attack is harmful for the routing protocols in the UASNs.

Table 2 summarizes routing layer attacks with a brief description of each attack, of security issues that arise, possible defenses/countermeasures, and existing attack resiliency studies in literature. Besides the above-mentioned four attacks, in some previous studies, Hello flood, neglect and greed, homing, spoof/alter, and replay routing info are also classified as network/routing layer attacks [10], [18], [29].

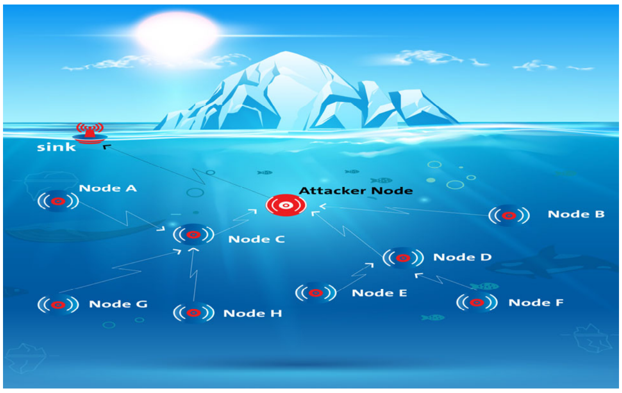

Fig. 3 sinkhole attack

3. Secure Routing Protocol Schemes, Communication Suite, and Frameworks

Underwater acoustic channel and sensor node mobility in UASNs poses significant challenges in designing a secure routing protocol. In literature, many routing protocols are proposed, classified into different categories such as energy-based routing protocols, data-based routing protocols, geographic information-based routing protocols, and cooperative schemes-based routing protocols [17], [30]. Most of these routing protocols are focused on energy efficiency, end-to-end delay, the packet delivery ratio (PDR), and the network lifetime, and there is less discussion of the security of the routing protocols. Recently, efforts to develop secure routing protocols for UASNs have increased.

In this section, we summarize existing secure routing protocols. These routing protocols schemes, approaches, architectures, frameworks, and security suites address different security threats/attacks in the network (i.e., the routing layer) such as wormhole attacks, Sybil attacks, sinkhole attacks, flooding attacks, and black hole attacks.

3.1 Secure Routing Protocol Schemes/Approaches

In this section, we present various schemes and approaches to securing routing protocols by addressing the above-mentioned threats/attacks.

3.1.1 Distributed Visualization of Wormholes (Dis-VoW)

The Dis-VoW approach [24] for the detection of wormhole attacks in UASNs was derived from the multidimensional scaling visualization of wormholes (MDS-VoW) approach [31] after modifying it for the underwater medium. In MDS-VoW, the deployed sensor nodes are assumed to be in a two-dimensional (2D) space and use a centralized approach while keeping in view the free movement of underwater sensor nodes due to the water current and therefore, the dynamic network topology in the underwater medium. Dis-VoW sensor nodes are assumed to be deployed in a three-dimensional (3D) space, and a distributed approach is used to cope with wormhole attacks. Dis-VoW has three building blocks: (1) estimation of the neighboring node distance, (2) localized reconstruction, and (3) wormhole detection.

After the network deployment, each sensor is required to estimate its distance from the neighboring node, which is further used in localized reconstruction. The time of arrival (ToA) approach is used to estimate the distance, and a one-round protocol is proposed for determining the upper and lower bounds of the distance between the two sensor nodes. Then, the two-hop topology will be shared with the neighbors by broadcasting each sensor node's neighbor list and its distance from them. To generate the distance matrix and calculate the shortest distance between sensor nodes, we used the Dijkstra method.

In addition, within two hops network reconstruction will be performed using the classical metric MDS and virtual position calculation for each node. Finally, wormhole attacks are detected using edge length and angle distortions among the neighbor sensor nodes. The fake neighbor link is identified by defining a normalized variable wormhole indicator based on these edge length and angle distortions.

The authors discussed the security of Dis-VoW, how to minimize false positive alarms, and the wormhole detection algorithm conducting frequency. The identified drawbacks of the proposed Dis-VoW approach are increased computational complexity and storage overhead of the sensor nodes. In a Sybil attack, the attacker mimics a fake node location and identity in order to appear to exist in more than one place in the network at a time by compromising the identity of legitimate nodes [11], [18]. This type of attack becomes catastrophic because it targets the multipath routing and topology maintenance and thus, deceives the routing protocols as well [11],[22]. Geographic routing protocols are the most vulnerable routing protocols to Sybil attacks.

A Sybil attack is graphically illustrated in Figure 2. The attacker node advertises two fake locations of sensor nodes that do not physically exist. It is assumed here that all the sensor nodes are within the same communication range. The legitimate nodes will transmit the information to the fake nodes via the red link line shown in Fig. 2 and will avoid the transmission to the legitimate nodes shown by the crossed links. The fake sensor nodes are chosen because their lower depth compared to the sink nodes enables the attacker node to overhear the information transmitted by the legitimate nodes.

3.1.2 Wormhole-resilient Secure Neighbor Discovery (WSND) Protocols

WSND protocols are proposed by (name of author/s) [25] to counter wormhole attacks in UASNs. The advantages of the proposed protocols are that they do not require secure and time synchronization, localization, and a high sensor node density in the network. The only assumption in the proposed protocols is that each sensor node can estimate the direction of arrival (DoA) of the incoming acoustic signals. The authors proposed the following neighbor discovery protocols (NDPs):

1. Basic Neighbor Discovery Protocol (B-NDP): In this protocol, only two sensor nodes are considered and are assumed to be static. All true neighbors need to locate each other to prevent fake neighbors with a high probability of initiating a neighboring relationship.

2. Double-Verification Neighbor Discovery Protocol (DV-NDP): This protocol is the improved version of B-NDP, in which three nodes are considered for initiating mutual neighboring links at the same time to improve wormhole attack defense of B-NDP. At the cost of a few lost links, this protocol blocks fake neighbors with a probability approaching 1 to initiate such mutual neighbor relationship.

3. Strict Double-Verification Neighbor Discovery Protocol (SDV-NDP): DV-NDP may not work properly when the two nodes are close to each other. SDV-NDP, a deterministic scheme, makes sure that any two nodes are not very close to each other and therefore, will not fail to detect any wormhole link. However, the cost is more lost links than with DV-NDP.

4. Mobility-Aware Neighbor Discovery Protocol (MC-NDP): In B-NDP, DV-NDP, and SDV-NDP, the sensor node mobility factors are not considered. In MC-NDP, it is. This protocol can be set up upon the above-mentioned three protocols and can locate wormhole links randomly with a high probability.

3.1.3 Secure Flood (SeFLOOD) Protocol

SeFLOOD [32] is an NDP protocol and an extension of the FLOOD protocol [33] that secures UASNs against network authenticity, integrity, and spoofing attacks. The authors proposed the utilization of a cryptographic suite for NDPs with less message length overhead. SeFLOOD is executed before the FLOOD protocol to secure exchange of information during the FLOOD protocol. In the operation of the SeFLOOD protocol, it is assumed that a link key is shared between two sensor nodes, which can be distributed by the known protocols called the "Elliptic curve Diffie-Hellman" [34] or the "Blundo scheme" [35]. However, a

Link Key Table (LKT) that contains all the link keys is kept with each sensor node to simplify the protection of unicast messages. Further clusters are formed that are subsets of underwater nodes that contain a unique broadcast domain. To secure broadcast messages within those clusters, a Cluster Key Table (CKT) is formed that contains a cluster key generated by each sensor node. Each sensor node encrypts both a cluster key and a shared link key, which it further secretly distributes to its clustering members, and the process of distributing the cluster key is continued until all the members in the cluster have it. The cluster key is distributed by the Cluster Key Distribution Protocol. Broadcast messages are authenticated by each sensor node with the cluster key.

Although the SeFLOOD protocol provides security against spoofing-based integrity and denial-of-service attacks, the study did not present the delay overhead, energy consumption, and broadcast message ratio that SeFLOOD added to the FLOOD protocol in terms of security and left them for future studies.

3.1.4 Resilient Pressure Routing (RPR) Protocol

The RPR protocol [36] was developed to provide security for geographic- or pressure-based routing protocols, which are considered exposed to malicious intrusions such as insider spoofing attacks [37]. This protocol is based on the Depth-based Routing (DBR) protocol [38]. It adopted the packet-forwarding strategies of the DBR protocol but added the feature of robust packet delivery in the presence of the attackers by introducing cryptographic mechanisms, implicit acknowledgments, retransmissions, geographic constraints with a sliding window feature, and randomization. In the packet-forwarding process of RPR, to avoid a malicious intrusion, a sensor node is selected as a forwarder only when it knows the network-wide secret key (NSK) and has a legitimate ID. Moreover, the sliding window thresholding feature blocks the outsider node from forwarding packets when its threshold is outside the current set threshold. However, if it does forward the packets, each sensor node in the network will ignore it because it violates the protocol rules. This sliding window thresholding feature is also important in determining the nodes with fake depth information.

3.1.5 R-CARP (Reputation-based Channel-Aware Routing Protocol

This protocol [27] is the extended version of the channel-aware routing protocol (CARP) [39]. It has features that protect a UASN against insider spoofing attacks such as a sinkhole attack. This protocol is considered the first reputation-based mechanism. It uses Boneh–Lynn–Shacham (BLS), a short digital signature algorithm that provides security against sinkhole attacks. In R-CARP, first, each sensor node in the network needs hop distance information from the sink and also shares the same group key and a unique secret key with the sink. Now, when any sensor node wants to forward data packets, it needs to select the best relay among the neighbors and therefore, broadcasts the request message “PING”. The neighbor nodes that receive this request PING message reply with a PONG message that contains link quality information and hop distance information. This PONG reply message is also authenticated and encrypted, in a way similar to that in [19], to ensure that the message will not be modified by the attackers. Then, the sensor node that sends the PING message calculates the reputation ratio, which is “the total number of messages confirmed by the sink that any sensor node, let’s say x, has forwarded through the relay node y according to recent history. The reputation range of any node is from 0 to 1, but a higher reputation value is desired. In addition, the relay node selection among neighbors is based on the utility function, which is the sum of the hop distance information, link quality information, and reputation value.

The authors concluded that after a few exchanges of PING/PONG messages, the sensor nodes in the network were enabled to exploit any sinkhole activity both in data and confirmation messages and to start avoiding and blocking the compromised node or relay path. The performance of R-CARP was evaluated with performance metrics such as end-to-end latency, PDR, and energy per bit (EPB) both under normal and under-attack scenarios. With only a slight increase in latency, R-CARP outperformed CARP in terms of PDR and EPB.

3.1.6 R-CARP (Reputation-based Channel-Aware Routing Protocol

This protocol [26] was developed to improve the quality of service (QoS) by using four agents: the security agent (SA), routing agent (RA), underwater gateway agent (UWAg), and vehicle agent (VA). The primary goal of these agents is to discover wormhole-resilient neighbor sensor nodes and routing information through a secure path and to provide defense against wormhole, route poisoning, and impersonation attacks. In the operation of this protocol, first, the SA helps to locate secure neighbor sensor nodes by using the RIPEMD-160 authentication mechanism as well as the Node Monitoring Agent (NMOA) and clones of the Secure Node Identification Agent (SNIA). The SA also updates the DOA estimation and neighbor discovery database. Second, the RA establishes the secure route path using static and mobile routing agents. In addition, it uses the Node Manager Agent (NMA) and clones of the Secure Path Discovery Agents (SPDAs) to cross through neighbor sensor nodes and create a secure path route to the surface gateway. Third, the UWAg uses agents to create a secure route path to the sink node, while the Surface Gateway

Manager Agent (SGMA) gathers multipath route information from the source node at the surface gateway. The SGMA further determines the path selection priorities, after which it informs the source nodes of these path selection priorities by transferring clones of the Surface Gateway Path Setup Agents (SGPSAs) to establish connectivity. The UWAg can also perform the key exchange task. Finally, the route maintenance agents are used for route maintenance in case of node/link failure. In this case, Vehicle Traversal Agents (VTAs) are activated to re-establish the link by modifying the directions of the autonomous underwater vehicle (AUV) so that they would surround the isolated sensor nodes.

3.1.7 R-CARP (Reputation-based Channel-Aware Routing Protocol

The new digital short-signature routing scheme [40] is an improved version of the digital short signature algorithm proposed in [41]. It is more efficient because it eliminates the need for an online trusted third party. The source and destination nodes are authenticated with digital signatures, while the anonymity of the communication nodes (source and destination) from the intermediate nodes is built up with the trap door design for routing messages. This secure routing scheme based on anonymity provides resilience against forgery attacks from other nodes and blocks the attack node to determine the identity of the source/forwarding/destination node by interpreting the routing messages. Intermediate nodes are also made anonymous in the routing path with encoding session IDs by the neighboring sensor node based on the multi-protocol label switching (MPLS) technique. The proposed model also provides security against location identification so that an attacking node would not be able to get the location and hop count information of other nodes by analyzing routing messages.

Three tables are maintained in this proposed protocol: the session ID (SID) table for neighboring nodes, the SID table for itself, and the encoding length table.

3.1.8 Distributed Detection and Mitigation Approach

The distributed detection and mitigation approach proposed in [28] was developed to detect and defend networks against routing attacks such as sinkhole attacks, out-of-bound wormhole attacks, and encapsulated wormhole attacks. In this distributed detection and mitigation approach, each sensor node first locates its neighbors through the NDP by using geometric relationships. The signal DOA determines the correct neighboring pair transceivers [25]. Moreover, the pairwise synchronization approach is adopted to synchronize each sensor node’s local clock with that of each of its neighboring sensor nodes. There are two types of pairwise synchronization approaches: receiver-receiver synchronization and sender-receiver synchronization [42], [43]. In this study, the authors used the latter approach as it is considered more suitable in the challenging UASN environment [44]. Moreover, in this approach, each sensor node maintains two sliding windows, W and W’ both with size t , at their local time for each of its neighboring sensor nodes. To conclude, the proposed approach is based on three phases: the discovery phase, the silent monitoring phase, and the detection phase.

The authors further presented various scenarios of the detection of sinkhole attacks, out-of-bound wormhole attacks, and encapsulated wormhole attacks using their proposed approach and then isolated sensor nodes with malicious activities/behavior. In addition, an analytical model was developed to find the node deployment density that guarantees that at least one sensor node can monitor each link in the entire network.

3.1.9 Tic-Tac-Toe AI-MINIMAX Algorithm

The Tic-tac-toe AI-MINIMAX algorithm was proposed in [45]. It is the basic min-max algorithm, which provides an optimal and secure route for UASNs by applying the game theory with the proposed tic-tac-toe AI-MINIMAX algorithm.

The implementation of the minmax algorithm involves mainly two players, Min and Max. They are opposite each other; Min has the lowest score, and Max has the highest score. For implementation in UASNs, the sender is chosen as the Max and the attacker is chosen as the Min.

The algorithm implementation has mainly four steps: (1) optimal route detection, (2) current move better condition, (3) GameOVer state condition, and (4) making AI smarter. In conclusion, the authors suggested that the game theory, artificial intelligence (AI), and the minmax algorithm can provide better results in terms of security and finding optimal routes.

3.1.10 Secure Routing Algorithm for Underwater (SRAU)

The Wormhole and Sybil attack-resilient routing algorithm named “secure routing algorithm for underwater” (SRAU) was proposed in [46]. The operation of SRAU has four phases. In the first phase, the secure neighbor discovery under a wormhole attack is carried out in the network. In the second phase, called the “primary route discovery process”, the reliable forwarding node is chosen from the source to the sink node, which increases the PDR. In the third phase, the attack is detected during the distribution. In the fourth and final phase, the alternate secure route for malicious node detection is determined.

The authors conducted various experiments to evaluate the performance of SRAU with respect to its detection rate, PDR, end-to-end delay, energy consumption, and network lifetime.The Tic-tac-toe AI-MINIMAX algorithm was proposed in [45]. It is the basic min-max algorithm, which provides an optimal and secure route for UASNs by applying the game theory with the proposed tic-tac-toe AI-MINIMAX algorithm.

3.1.11 Secure-capable Multi-user Network Protocol

A secure-capable multi-user network protocol was proposed in [47]. They adopted the energy-efficient Janus-based UASN protocol in a hybrid cellular topology and proposed an optimized flooding routing protocol to increase the PDR and the energy consumption. This study had mainly three main contributions. First, it presented the cellular topology-based hybrid architecture as a primary mode and then introduced the secondary ad hoc topology in case the gateway sink node did not respond. Second, it proposed an optimized flooding routing protocol capable of optimizing the PDR and reducing the energy consumption due to avoidance of excessive packet relay. Third, a lightweight key exchange protocol was developed that secured the transceiver nodes from routing attacks, eavesdropping, and data tampering by creating symmetric key encryption between them.

3.1.12 Secure-capable Multi-user Network Protocol

This protocol was proposed in [48]. It considers energy consumption, security, and the network lifetime. The authors claimed that SEECR has the capability to efficiently utilize the sensor node power resources, and they adopted cooperative schemes that also played a significant role in efficient energy utilization. Moreover, the security algorithms of SEECR for combating active routing attacks did not add significantly to the computational overhead. Therefore, it increased the network lifetime due to its minimum energy consumption. Moreover, in the SEECR protocol, the data packets are forwarded from the source to the destination/sink node via hop by hop (thus, this protocol is sometimes known as the "multi-hop network model"), which is a cooperative mechanism. This protocol is considered immune and capable of detecting active routing attacks that drop packets and block those attacker nodes as well. The author compared the SEECR protocol with the AMCTD protocol performance [49] with and without attack scenarios using the performance metrics of alive nodes in the network, transmission loss, throughput, energy consumption, and end-to-end delay.

3.1.13 Secure-capable Multi-user Network Protocol

SAPDA was proposed in [50] based on a cluster structure that was compact, stable, and extended the network lifetime. The advantages of the SAPDA scheme are secure authentication and safe data aggregation, which are based on real-time parameters; use of multiple sink nodes that can help to reduce the delay, drop packets, and improve the PDR. Moreover, trusted encrypted schemes are applied in this scheme to make it secure and reliable.

The SAPDA scheme has mainly two modules: (1) secure authentication of cluster heads (CHs) and (2) protected data aggregation. The first module is responsible for authenticating CHs to the gateways (GWs) to ensure that each CH is a legitimate node and not a compromised one. In the second module, symmetric encryption is used to secure the data first, after which the securely aggregated data is transmitted to the base station. The compromised data are detected by the base station through time stamps and handled so as not to disrupt safe network operations.

The comparative analysis of the SAPDA scheme was performed with the HaSAFSS [51], ES [52], FDRT [53] and IDACB [54] schemes. The performance metrics for evaluation are average end-to-end delay, average data delivery/reliability ratio, average packet drop, and average energy consumption.

3.2 Secure Underwater Acoustic Communication Suite

A secure communication suite for UASNs composed of both static and mobile sensor nodes was proposed in [55]. It protects the integrity and confidentiality of underwater acoustic (UWA) communication, while considering the UWA channel limitations. A secure routing protocol and a set of cryptographic primitives (i.e., a cipher, a digest, and re-keying) are the two main parts of the suite. The cryptographic suite efficiency depends on the ciphertext expansion. Limiting this expansion can increase the efficiency of the cryptographic suite. A similar approach was used in this study. The author used a secure routing protocol named "SeFLOOD", which was discussed in the previous subsection. The SeFLOOD protocol also meets the computer systems design given by the well-known Lampson's recommendations [56]. In summary, this study had three main contributions. First, it defends the integrity and confidentiality of UWA communications. Second, the communication suite also backs one-to-one and one-to-many communications. Third and last, this study enabled secure reconfiguration in cases of sensor node mobility and entering or leaving the network. The authors of [56] concluded that the proposed secure communication suite had limited communication overhead and less energy consumption.

3.3 Secure Frameworks and Architectures

3.3.1 Security Framework for Underwater Networks (SecFUN)

A security framework, SecFUN, was proposed in [19] It uses Galois Counter Mode (GCM) AES building blocks and a short digital signature algorithm to defend the data integrity, confidentiality, authentication, and non-repudiation. It supports message authentication, relay protection, and confidentiality, along with flexible selection of MAC sizes and message/entity authentication and integrity via digital signatures because of its symmetric and asymmetric cryptography. Symmetric or secret key cryptography uses the same key, while asymmetric or public key cryptography uses different keys for both encryption and decryption. With the support of both cryptographic types, SecFUN provides protection against routing attacks from the link layer to the application layer through suitable (configurable and flexible) selection of security features that can handle specific applications/scenarios. Moreover, in SecFUN, the CARP protocol is extended to support the proposed cryptographic measures. Therefore, two different routing protocols are developed: Se-CARP and Sds-CARP. Se-CARP is the improved version of the basic CARP protocol [39], which supports the AES-GSM encryption with the assumption that the sensor nodes share the same group and a unique secret key within the network. Sds-CARP is also an extended version of the CARP protocol that can support short digital signatures (i.e., BLS [57], ZSS [58] and Quartz [59]) and provides message authentication with the use of such digital signature schemes. The authors assessed the performance of the Se-CARP and Sds-CARP by utilizing the SUNSET framework [60] and performed a comparative analysis of CARP, Se-CARP, and Sds-CARP with the performance metrics: latency and energy consumption.

3.3.2 Architecture of Software-Defined Network-based Hybrid UANs (SUANs)

A Software-Defined Network (SDN)-based hybrid UAN architecture was proposed in [20] to augment the robustness and security of UANs by consolidating various aspects such as the physical layer security (PLS), software-defined networking (SDN), node cooperation, cross-layering, context awareness, and cognition. SUAN architecture is adaptable to environmental changes, the network status, and possible attacks due to the visualization of various strategies at the node and network layer. SUAN architecture has three planes: (1) the application plane, (2) the control plane, and (3) the data plane. Application-related assignments (e.g., data collection, defining QoS requirements and security policies, etc.) are dealt with in the application plane, and the control plane is responsible for running various networking services. These networking services are operational based on the UAN's application demands with the help of logically centralized controllers (primary OF-controllers). The data plane is composed of OF-sensors, an optical fiber-enabled static underwater sensor node, and "OF-AUVs", which are optical fiber-enabled mobile autonomous underwater vehicles. Therefore, the data plane set up the UAN networking infrastructure. The OF-sensors and the OF-AUVs are responsible for data sensing and data forwarding, and the secondary layer of control (the secondary OF-controllers) is also assigned to these nodes and is therefore also capable of performing primary OF-controller tasks.

The security analysis of the SUAN architecture was carried out by considering various attacks such as jamming attacks, wormhole and ID spoofing attacks, blackhole and sinkhole attacks, and replay and resource exhaustion attacks. Moreover, the open design challenges concerning the controller robustness, energy-aware networking, and scalability for the implementation of the SUAN architecture were also presented. The author concluded that the proposed SUAN architecture was not a proven solution but could be the focus of future research on UANs.

4. Comparison of Secure Routing Protocols Schemes/Frameworks/Architectures

In this section, we compare previous secure routing protocol schemes, frameworks, and architectures that we classified into two groups. The first comparison was based on how the protocols address security requirements, besides comparing their anti-attacks, advantages, and limitations. The second comparison was related to the performance evaluation based on the following performance metrics: end-to-end delay, PDR, energy consumption, network lifetime, etc.

4.1 Comparison 1: Anti-attack-based Comparison

In this subsection, we compare the existing secure routing protocol schemes based on their addressing of the fundamental security requirements discussed in Section 1, the various routing security threats/attacks discussed in Section 2, their advantages, and their limitations. The comparison is shown in Table 3. Moreover, for ease of reading, we indicate in the same table the reference and publication year of each secure routing protocol scheme. It can be observed from Table 3 that most of the existing secure routing protocols address mostly one type of routing

Table 3: Comparison of the existing protocols schemes/approaches/frameworks etc. based on the anti-attack

Ref No	Methodology			Security requirement	Routing attack	Merits	Limitations
[24]	Dis-VoW	2008	Distortion visualization of angles and edge lengths	-	Wormhole	Suitable for large scale UASNs and no additional special hardware required	Introduce computational and storage overhead
[25]	WSND	2010	Direction of Arrival estimation	-	Wormhole	No requirements of high density node deployment, secure and accurate time synchronization and localization	Low adjacent wormhole node detection capability
[32]	SeFlood	2011	Cryptographic suite	Authenticity and Integrity	DoS	Protection against spoofing based DoS and integrity attacks	Lack of performance evaluation of the proposed protocol
[55]	Secure underwater communication suite	2012	Cryptographic suite	Confidentiality and integrity	-	Support mobile nodes	-
[36]	RPR	2014	Cryptographic mechanisms	-	Malicious intrusions	Robust packet delivery service in the presence of attackers	Depth information required
[27]	R-CARP	2015	Reputation based mechanism and BLS, a short digital signature algorithm	Authenticity and Integrity	Sinkhole	Low communication overhead	Minor increase in delay
[19]	SecFUN	2015	Short digital signatures, i.e., BLS	Confidentiality, integrity, auntentication and non-repudiation	-	Meet the security requirements	Increase in energy and latency
[26]	SARP	2016	Agent based scheme	Authentication	Wormhole, route poisoning, and impersonation attack	-	-
[40]	Digital short signature routing scheme	2017	Short signature algorithm	Authentication	Forgery attacks	No use of online third party, anonymity and less overhead due to trap door design	More energy consumption
[28]	Distributed detection and mitigation approach	2017	Collaborative detection strategy	-	Wormhole and sinkhole	Less delay and negligible energy consumption	-
[20]	SUAN	2017	Hybrid architecture	-	Jamming, wormhole and ID spoofing, blackhole and sinkhole, replay and resource exhaustion	Adaptable to environmental variations	Facing challenges of energy efficiency, scalability and control overhead
[45]	Tic-tac-toe AI-MINIMAX algorithm	2018	Game theory with Min-Max algorithm	Authentication	Internal and external attacks	Capable of secure optimal move	-
[46]	SARU	2018	Hybrid architecture	-	Eavesdropping and data tempering	Energy efficient	Security feature add additional traffic and latency
[47]	Secure-capable multi-user network protocol	2018	Hybrid cellular Ad-hoc topology	-	Eavesdropping and packet tampering	Secure and energy efficient Janus based UWAN protocol which also increases PDR	Security feature introduce more overhead
[48]	SEECR	2020	Cooperative schemes	-	Routing attacks	Efficiently utilizes energy as well as security against active routing attacks	-

attack and only some of them fulfill part of the fundamental security requirements. Although each secure routing protocol has advantages, they introduce security features at the cost of the performance parameters (energy efficiency, computational ease, and less delay) and introduce several other overheads accordingly. Therefore, based on the comparison table, we can conclude that there are many research gaps that need to be filled in order to fully secure the routing protocols that can tackle most of today's routing threats/attacks at minimum overheads.

4.2 Performance Metrics-based Comparison

To elaborate more on the existing secure routing protocol schemes, we compare them in terms of the performance metrics of end-to-end delay, packet delivery ratio (PDR), energy consumption, network lifetime, and many others mentioned in existing literature. The comparison based on performance metrics is in Table 4. From our analysis of Table 4, we found that either the performance of most of the existing secure routing protocols had not been evaluated or they were evaluated but according to only a few parameters to show the effectiveness of the proposed secure routing schemes. Thus, wide-ranging research needs to be carried out to ensure the secure implementation of UASNs.

this

Table 1: Comparison of the existing protocols schemes/approaches/frameworks etc. based on performance metrics

Protocols	Mobility	Performance metrics				Other metrics
		Delay	PDR	Energy	Network lifetime	
Dis-VoW	×	×	×	×	×	-
WSND	×	×	×	×	×	-
SeFlood	×	×	×	×	×	-
Secure underwater communication suite	✓	×	×	×	×	Average delivery ratio and average round trip time
RPR	×	✓	✓	×	×	Average No. of transmissions
R-CARP	×	✓	✓	✓	×	
SecFUN	×		×		×	
SARP	×	×	✓	✓	×	Probability of success (P_s), probability of failure (P_f) and route maintenance overhead
Digital short signature routing scheme	×	×	✓	✓	×	Throughput
Distributed detection and mitigation approach	×	×	×	×	×	Probability of detection and Probability of isolation
SUAN	×	×	×	×	×	-
Tic-tac-toe AI-MINIMAX algorithm	×	×	×	×	×	-
SARU	×	×	×	×	×	-
Secure-capable multi-user network protocol	✓	×	×	×	×	Forwarding time
SEECR	×	✓	×	✓	×	Number of alive nodes, transmission loss and throughput

5. Conclusion and Future Directions

In this section, we present various recommendations and future directions based on the previous studies mentioned in Sections 3 and 4, where we believe a research gap existed that needs to be addressed to fully secure the routing protocols and UASNs.

Our analysis in Section 4 showed that most of the previous studies did not fulfill the security requirements completely and focused only on one type of routing attack, such as wormhole attacks or sinkhole attacks. Very few studies—among them [20]—addressed various types of attacks. The studies were also silent on the need to address security requirements. While a secure routing protocol needs to be secure from all types of routing attacks, it must also fulfill security requirements. Moreover, most of the previous studies did not evaluate the performance of their proposed technology or approach, or used only a few parameters in their performance analysis. One important challenge that was not properly addressed is node mobility in UASNs due to the dynamic network topology. Therefore, we believe that there is a need for a secure routing scheme that can address all types of security attacks; address the UASN challenges related to power, the network lifetime, mobility, etc.; and fulfill security requirements; and its performance must be evaluated. With the advancement of underwater technologies such as UASNs that operate on various media such as acoustic, EM, optical, and MI media, the ensuing development of various underwater devices such as underwater vehicles and various underwater communication modems enables the technology Internet of Underwater Things (IoUT). Future studies may investigate not only the various challenges of IoUT [29] but also security challenges related to IoUT.

Acknowledgments

The authors would like to thank the Deanship of Scientific Research at Umm Al-Qura University for supporting this work by Grant Code 19-COM-1-01-0019

References

[1] S. Jiang, “Security in uwans,” in Wireless Networking Principles: From Terrestrial to Underwater Acoustic. Springer, 2018, pp. 337–367.

[2] I. F. Akyildiz, D. Pompili, and T. Melodia, “Underwater acoustic sensor networks: research challenges,” Ad hoc networks, vol. 3, no. 3, pp. 257– 279, 2005.

[3] M. Stojanovic and J. Preisig, “Underwater acoustic communication channels: Propagation models and statistical characterization,” IEEE communications magazine, vol. 47, no. 1, pp. 84–89, 2009.

[4] D. Pompili and I. F. Akyildiz, “Overview of networking protocols for underwater wireless communications,” IEEE Communications magazine, vol. 47, no. 1, pp. 97–102, 2009.

[5] I. F. Akyildiz and X. Wang, “A survey on wireless mesh networks,” IEEE Communications magazine, vol. 43, no. 9, pp. S23–S30, 2005.

[6] J. Partan, J. Kurose, and B. N. Levine, “A survey of practical issues in underwater networks,” ACM SIGMOBILE Mobile Computing and Communications Review, vol. 11, no. 4, pp. 23–33, 2007.

[7] G. Han, J. Jiang, N. Sun, and L. Shu, “Secure communication for underwater acoustic sensor networks,” IEEE communications magazine, vol. 53, no. 8, pp. 54–60, 2015.

[8] S. Jiang, “On securing underwater acoustic networks: A survey,” IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 729–752, 2018.

[9] G. Yang, L. Dai, G. Si, S. Wang, and S. Wang, “Challenges and security issues in underwater wireless sensor networks,” Procedia Computer Science, vol. 147, pp. 210–216, 2019.

[10] Y. Cong, G. Yang, Z. Wei, and W. Zhou, "Security in underwater sensor network," in 2010 International Conference on Communications and Mobile Computing, vol. 1. IEEE, 2010, pp. 162–168.

[11] 11. M. C. Domingo, "Securing underwater wireless communication net- works," IEEE Wireless Communications, vol. 18, no. 1, pp. 22–28, 2011.

[12] 12. L. F. Liu and M. D. Ma, "Security issues in underwater sensor networks: Attacks and defenses," in Applied Mechanics and Materials, vol. 644. Trans Tech Publ, 2014, pp. 2689–2698.

[13] G. Han, J. Jiang, N. Bao, L. Wan, and M. Guizani, "Routing protocols for underwater wireless sensor networks," IEEE Communications Magazine, vol. 53, no. 11, pp. 72–78, 2015. Middleware 2009. LNCS, vol. 5896, pp. 83–102. Springer, Heidelberg (2009)

[14] 14. C. Lal, R. Petroccia, M. Conti, and J. Alves, "Secure underwater acoustic networks: Current and future research directions," in 2016 IEEE third underwater communications and networking conference (UComms). IEEE, 2016, pp. 1–5.

[15] S. Kumar, B. Kumari, and H. Chawla, "Security challenges and ap- plication for underwater wireless sensor network," in Proceedings on International Conference on Emerg, vol. 2, 2018, pp. 15–21.

[16] 16. H. Li, Y. He, X. Cheng, H. Zhu, and L. Sun, "Security and privacy in localization for underwater sensor networks," IEEE Communications Magazine, vol. 53, no. 11, pp. 56–62, 2015.

[17] J. Luo, Y. Chen, M. Wu, and Y. Yang, "A survey of routing protocols for underwater wireless sensor networks," IEEE Communications Surveys & Tutorials, vol. 23, no. 1, pp. 137–160, 2021.

[18] A. Modirkhazeni, N. Ithnin, and M. Abbasi, "Secure hierarchal routing protocols in wireless sensor networks; security survey analysis," Inter- national Journal of Computer Communications and Networks (IJCCN), vol. 2, no. 1, 2012.

[19] G. Ateniese, A. Capossele, P. Gjanci, C. Petrioli, and D. Spaccini, "Secfun: Security framework for underwater acoustic sensor networks," in OCEANS 2015-Genova. IEEE, 2015, pp. 1–9.

[20] C. Lal, R. Petroccia, K. Pelekanakis, M. Conti, and J. Alves, "Toward the development of secure underwater acoustic networks," IEEE Journal of Oceanic Engineering, vol. 42, no. 4, pp. 1075–1087, 2017.

[21] L. Buttyan and J.-P. Hubaux, Security and cooperation in wireless net- works: thwarting malicious and selfish behavior in the age of ubiquitous computing. Cambridge University Press, 2007.

[22] S. S. Shahapur and R. Khanai, "Localization, routing and its security in uwsn—a survey," in 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT). IEEE, 2016, pp. 1001–1006.

[23] A. Modirkhazeni, N. Ithnin, and O. Ibrahim, "Secure multipath routing protocols in wireless sensor networks: a security survey analysis," in 2010 Second International Conference on Network Applications, Protocols and Services. IEEE, 2010, pp. 228–233.

[24] W. Wang, J. Kong, B. Bhargava, and M. Gerla, "Visualisation of wormholes in underwater sensor networks: a distributed approach," International Journal of Security and Networks, vol. 3, no. 1, pp. 10–23, 2008.

[25] R. Zhang and Y. Zhang, "Wormhole-resilient secure neighbor discovery in underwater acoustic networks," in 2010 Proceedings IEEE INFO- COM. IEEE, 2010, pp. 1–9.

[26] M. R. Bharamagoudra and S. S. Manvi, "Agent-based secure routing for underwater acoustic sensor networks," International Journal of Communication Systems, vol. 30, no. 13, p. e3281, 2017.

[27] A. Capossele, G. De Cicco, and C. Petrioli, "R-carp: A reputation based channel aware routing protocol for underwater acoustic sensor networks," in Proceedings of the 10th International Conference on Underwater Networks & Systems, 2015, pp. 1–6.

[28] T. Dargahi, H. H. Javadi, and H. Shafiei, "Securing underwater sensor networks against routing attacks," Wireless Personal Communications, vol. 96, no. 2, pp. 2585–2602, 2017.

[29] A. G. Yisa, T. Dargahi, S. Belguith, and M. Hammoudeh, "Security challenges of internet of underwater things: A systematic literature review," Transactions on Emerging Telecommunications Technologies, vol. 32, no. 3,p e4203, 2021.

[30] H. Khan, S. A. Hassan, and H. Jung, "On underwater wireless sensor networks routing protocols: A review," IEEE Sensors Journal, vol. 20, no. 18, pp. 10 371–10 386, 2020.

[31] W. Wang and B. Bhargava, "Visualization of wormholes in sensor networks," in Proceedings of the 3rd ACM workshop on Wireless security, 2004, pp. 51–60.

[32] G. Dini and A. L. Duca, "Seflood: A secure network discovery pro tocol for underwater acoustic networks," in 2011 IEEE Symposium on Computers and Communications (ISCC). IEEE, 2011, pp. 636–638.

[33] H. Rustad, "A lightweight protocol suite for underwater communication," in 2009 International Conference on Advanced Information Networking and Applications Workshops. IEEE, 2009, pp. 1172–1177.

[34] E. B. Barker, D. Johnson, and M. E. Smid, "Recommendation for pair- wise key establishment using discrete logarithm cryptography (revised)," 2007.

[35] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-secure key distribution for dynamic conferences," in Annual international cryptology conference. Springer, 1992, pp. 471–486.

[36] M. Zuba, M. Fagan, Z. Shi, and J.-H. Cui, "A resilient pressure routing scheme for underwater acoustic networks," in 2014 IEEE Global Communications Conference. IEEE, 2014, pp. 637–642.

[37] M. Zuba, M. Fagan, J.-H. Cui, and Z. Shi, "A vulnerability study of geographic routing in underwater acoustic networks," in 2013 IEEE Conference on Communications and Network Security (CNS). IEEE, 2013, pp. 109–117.

[38] H. Yan, Z. J. Shi, and J.-H. Cui, "Dbr: depth-based routing for un- derwater sensor networks," in International conference on research in networking. Springer, 2008, pp. 72–86.

[39] S. Basagni, C. Petrioli, R. Petroccia, and D. Spaccini, "Carp: A channel- aware routing protocol for underwater acoustic wireless networks," Ad Hoc Networks, vol. 34, pp. 92–104, 2015.

[40] X. Du, C. Peng, and K. Li, "A secure routing scheme for underwater acoustic networks," International Journal of Distributed Sensor Net- works, vol. 13, no. 6, p. 1550147717713643, 2017.

[41] X. Chen, F. Zhang, D. M. Konidala, and K. Kim, "New id-based threshold signature scheme from bilinear pairings," in International Conference on Cryptology in India. Springer, 2004, pp. 371–383.

[42] N. Chirdchoo, W.-S. Soh, and K. C. Chua, "Mu-sync: a time synchro- nization protocol for underwater mobile networks," in Proceedings of the third ACM international workshop on Underwater Networks, 2008, pp. 35–42.

[43] J. Liu, Z. Zhou, Z. Peng, J.-H. Cui, M. Zuba, and L. Fiondella, "Mobi-sync: efficient time synchronization for mobile underwater sensor networks," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 2, pp. 406–416, 2012.

[44] Z. Li, Z. Guo, F. Hong, and L. Hong, "E2dts: An energy efficiency distributed time synchronization algorithm for underwater acoustic mo- bile sensor networks," Ad Hoc Networks, vol. 11, no. 4, pp. 1372–1380, 2013.

[45] K. Porkodi and A. ZubairRahman, "Enhanced underwater wireless sensor networks security with tic-tac-toe ai-minimax algorithm in game theory." TAGA J. Graphic Technol., vol. 14, pp. 216–224, 2018.

[46] M. Ahmadi and S. Jameii, "A secure routing algorithm for underwater wireless sensor networks," International Journal of Engineering, vol. 31, no. 10, pp. 1659–1665, 2018.

[47] H. Ghannadrezaii and J.-F. Bousquet, "Securing a janus-based flooding routing protocol for underwater acoustic networks," in OCEANS 2018 MTS/IEEE Charleston. IEEE, 2018, pp. 1–7.

[48] K. Saeed, W. Khalil, S. Ahmed, I. Ahmad, and M. N. K. Khattak, "Seecr: secure energy efficient and cooperative routing protocol for underwater wireless sensor networks," IEEE Access, vol. 8, pp. 107 419–107 433, 2020.

[49] M. R. Jafri, S. Ahmed, N. Javaid, Z. Ahmad, and R. Qureshi, "AMCTD: Adaptive mobility of courier nodes in threshold-optimized dbr protocol for underwater wireless sensor networks," in 2013 Eighth International Conference on Broadband and Wireless Computing, Communication and Applications. IEEE, 2013, pp. 93–99.

[50] 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 Personal Communications, pp. 1–15, 2020.

[51] A. A. Yavuz and P. Ning, "Self-sustaining, efficient and forward-secure cryptographic constructions for unattended wireless sensor networks," Ad Hoc Networks, vol. 10, no. 7, pp. 1204–1220, 2012.

[52] Y. Ren, V. A. Oleshchuk, and F. Y. Li, "Optimized secure and reliable distributed data storage scheme and performance evaluation in unat- tended wsns," Computer Communications, vol. 36, no. 9, pp. 1067–1077, 2013.

[53] N. Goyal, M. Dave, and A. K. Verma, "A novel fault detection and recovery technique for cluster-based underwater wireless sensor net- works," International Journal of Communication Systems, vol. 31, no. 4, p. e3485, 2018.

[54] N. Goyal, M. Dave, and A. K. Verma, "Improved data aggregation for cluster based underwater wireless sensor networks," Proceedings of the National Academy of Sciences, India Section A: Physical Sciences, vol. 87, no. 2, pp. 235–245, 2017.

[55] G. Dini and A. Lo Duca, "A secure communication suite for underwater acoustic sensor networks," Sensors, vol. 12, no. 11, pp. 15 133–15 158, 2012.

[56] B. W. Lampson, "Hints for computer system design," in Proceedings of the ninth ACM symposium on Operating systems principles, 1983, pp. 33–48.

[57] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," Journal of cryptology, vol. 17, no. 4, pp. 297–319, 2004.

[58] F. Zhang, R. Safavi-Naini, and W. Susilo, "An efficient signature scheme from bilinear pairings and its applications," in International Workshop on Public Key Cryptography. Springer, 2004, pp. 277–290.

[59] N. T. Courtois, M. Daum, and P. Felke, "On the security of hfe, hfev- and quartz," in International Workshop on Public Key Cryptography. Springer, 2003, pp. 337–350.

[60] C. Petrioli, R. Petroccia, J. R. Potter, and D. Spaccini, "The sunset framework for simulation, emulation and at-sea testing of underwater wireless sensor networks." Ad Hoc Networks 34 (2015): 224-238.

Ayman Alharbi received his B.Sc. (2006) from Umm Al-Qura University, Saudi Arabia. His M.Sc. (2012) and Ph.D. (2015) degree was obtained in Computer Science and Engineering from the University of Connecticut, USA.

Since 2010, he has been a member with the UConn's Underwater Sensor Networks Laboratory. He was a Chairman of the Computer Engineering Department. He is currently an Associate Professor with Umm Al-Qura University.

Muhammad Muzzammil received the B.S. degree in Electronics from COMSATS Institute of Information and Technology (CIIT), Pakistan in 2012 and M.S. degree in Electronic Engineering from Capital University of Science and Technology (CUST), Pakistan in 2015. In 2017, he joined the College of Underwater Acoustic Engineering, Harbin Engineering University (HEU), China where currently he is pursuing his Ph.D. in Information and Communication Engineering.

Mr. Muzzammil received the Best Poster Award in The 13th ACM International Conference on Underwater Networks & Systems (WUWNet'18) and is also being selected in the OES Student Poster Competition (OCEANS'19). His research interests lie in the areas of wireless communication, magneto-inductive communication and underwater acoustic communication and networking.