# Trust in the Deep: a Survey on Authenticating Acoustic Underwater Communication

Luisa Lux°•, Elmar Padilla°, Jan Bauer°
°Fraunhofer FKIE
Cyber Analysis & Defense
Wachtberg, Germany
•RWTH Aachen University
Research Group IT-Security
Aachen, Germany
{luisa.lux, elmar.padilla, jan.bauer}@fkie.fraunhofer.de

***Abstract*—The increasing capabilities of underwater sensing and wireless networking have led to a growing range of applications in both civilian and military domains. As these underwater systems become more pervasive, the integrity of the collected sensor data – and consequently the authenticity of the communicating entities and the messages exchanged – becomes critical for ensuring trust in the data, its interpretation, and eventually in the envisioned concept of a transparent ocean. Over the past decade, various approaches have been proposed to ensure authentication in underwater acoustic communication, ranging from adaptations of traditional cryptographic mechanisms to novel physical-layer techniques tailored to the underwater environment. This paper provides an overview of these developments, systematically analyzing their advantages and limitations in light of the unique challenges posed by underwater acoustic communication.**

***Index Terms*—Underwater Sensor Networks, Underwater Acoustic Communication, Authentication, Network Security**

## I. Introduction

The interest of governments, organizations, and research in understanding and protecting the oceans has increased in recent decades, driven in particular by their essential role in the profound transformations introduced by anthropogenic climate change. Coupled with technological advancements of underwater equipment, sensors, and communication technologies, this development has led to the deployment of entire underwater networks, unlocking the possibility of making the complex structure of the oceanic ecosystem transparent [1], [2]. Underwater Sensor Networks (UWSNs) are used to collect sensor data monitoring a variety of phenomena, including seismic movements, marine wildlife, and human influences, and transmit accumulated information back to the shore [2]. While the collected data constitutes a valuable resource for close supervision and forecast of events with high systematic relevance like tsunamis, oil spills, or acute coral bleaching, the broadcast nature of UWSNs and their sparse topology in unattended off-shore areas poses the risk of attracting adversaries that seek to compromise the integrity of sensitive data acquired by and processed within UWSNs [3] and thus undermine *trust in the deep*.

At the same time, implementing integrity-protecting procedures in the aquatic environment can be challenging due to the physical communication conditions rendering well-known approaches from terrestrial networks unsuitable. In UWSNs, acoustic communication frequently plays a pivotal role to enable data transmissions between underwater entities. Thus, communication protocols must be efficient due to latency, bandwidth limitations, and ambient noise. Consequently, suitable authentication mechanisms for the protection of data exchanged within these networks must be both reasonably secure as well as tailored to the physical capabilities preset by underwater acoustics. As reconciling these requisites is demanding, approaches in different research directions have been explored.

Even though network security considerations for underwater communications and UWSNs were raised early on during their development, they typically focus on confidentiality through covert communication [4] or encryption [5] but less on integrity protection and communication authenticity. Still, a growing number of works has been exploring approaches in different research directions, with an overview of existing work and guidance on the trade-offs associated with different approaches being missing. To close this gap, we survey existing message authentication approaches for Underwater Acoustic Communication (UAC), work out the main trends, and contribute with a comparative evaluation of the efficacy and feasibility of existing approaches for UWSN deployment.

The remainder of the paper is organized as follows: To acquaint the reader with acoustic underwater communication, we briefly touch on its characteristics and inherent security threats in Section II. After that, we study and group existing state-of-the-art underwater authentication mechanisms in Section III before discussing their efficacy and feasibility within UWSNs in Section IV. Finally, we summarize our key findings in Section V.

## II. Acoustic Communication & Security Threats

Underwater communication poses unique challenges due to the physical properties of water. Electromagnetic and optical signals suffer from severe attenuation and scattering, limiting their effective transmission range to only a few meters. For this reason, acoustic signals are the primary medium for long-range underwater communication, enabling data exchange over several kilometers [1]. Despite its advantages, UAC systems face significant constraints. Key challenges include signal attenuation caused by absorption and spatial spreading, high ambient noise levels, multi-path propagation, and Doppler shifts due to node mobility. Additionally, the propagation speed of sound in water is roughly five orders of magnitude

 DOI: 10.1109/VCC67261.2025.11351213

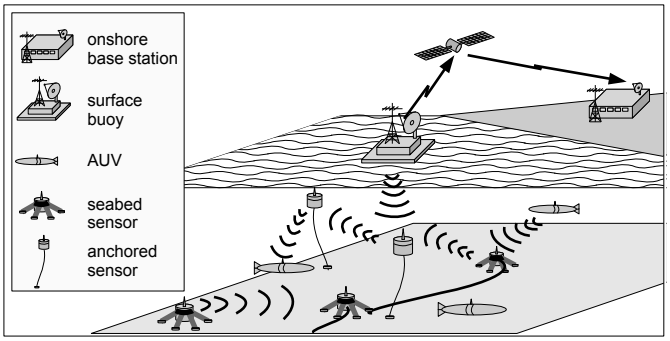


Fig. 1. Oceanic data collection and acoustic transmission in UWSNs, cf. [2].

slower than that of electromagnetic waves, and varies with environmental factors such as temperature, depth-dependent pressure, and salinity [1]. These factors result in limited bandwidth and low data rates, typically in the range of just a few kbps [1].

Nevertheless, continuous advancements across the communication stack have enabled reliable UAC, including efficient multi-hop routing protocols, e.g., [6]. These developments have paved the way for large-scale UWSNs that support robust and energy-efficient data transmission, enabling applications such as oceanic data collection, environmental monitoring, offshore exploration, underwater surveillance, and disaster prevention [2]. As depicted in Figure 1, typical UWSN scenarios consist of both stationary seabed-deployed sensors and mobile nodes such as autonomous underwater vehicles (AUVs) or ocean gliders. These nodes collect oceanographic data and transmit it to surface stations, which are often equipped with satellite links to relay the data to onshore base stations. Topologically, UWSNs are sometimes organized in clusters, where a dedicated cluster head (CH) is responsible for collecting, aggregating, and pre-processing sensor data within its cluster, while additionally often handling network management tasks.

The broadcast nature of acoustic transmission in underwater environments exposes UWSNs to significant security threats. Adversaries with sufficient resources and expertise can effortlessly intercept acoustic signals, especially given the typically unattended and widely distributed deployment of underwater sensors. If the communication protocols are known, attackers may craft and inject forged messages into the network – a practice known as *spoofing* – which compromises data integrity and undermines trust in the system. Spoofed messages can be used to falsify sensor data or hijack control signals, and may serve as a basis for more advanced attacks such as *Sybil* or *wormhole* attacks, cf. [7]. These threats are particularly critical in applications involving sensitive data or mission-critical tasks, making robust authentication mechanisms indispensable. Depending on the method, authenticity can be enforced and verified either on a hop-by-hop or end-to-end (E2E) basis. While a few existing surveys address security in UAC broadly [3], [7], none have yet provided a focused analysis of authentication mechanisms – a gap this paper seeks to address in the following section.

## III. Authentication Approaches

Early underwater authentication approaches adapted cryptographic methods from terrestrial radio-based networks, but their high overhead proved less suitable for resource-constrained UAC. This led to the development of Physical Layer Authentication (PLA), which leverages acoustic channel properties for lightweight and context-aware security. More recently, hybrid Cross-Layer Authentication (CLA) methods have also emerged, combining higher- and physical-layer features to improve robustness and efficiency. An overview of a possible classification is given in Figure 2. Key approaches of each category are now briefly introduced, followed by a comparative analysis in the next section.

### A. Higher Layer Authentication

Higher Layer Authentication (HLA) summarizes a category of approaches relying on non-physical information about network nodes and connections. These approaches can be of a *cryptographic* nature or utilize abstract node information, such as *timestamps* or *identifiers (IDs)* of messages and senders.

*1) Cryptographic HLA:* Cryptographic authentication mechanisms attract increasing attention within the research community. Like conventional cryptographic authentication methods in terrestrial networks, the authenticity of an entity is typically established and proved based on the possession of a secret key. Both symmetric and asymmetric authentication and key establishment procedures have been proposed for UWSNs.

*a) Digital Signatures:* A common approach for message authentication are digital signatures leveraging (asymmetric) public/private key pairs distributed across all network participants [8]. Souza et al. [9] have performed a comparison of pre-selected digital signature schemes as potentially suitable options for lightweight UAC authentication. Concretely, they compare the Zhang-Safavi-Naini-Susilo (ZSS) scheme [10], generating shorter signatures designed for resource-constrained environments, to the Boneh-Lynn-Shacham (BLS) [11] scheme, aggregating multiple signatures into a compact form, and use ECDSA [12] as a baseline. According to their results, the energy saved with smaller signatures exceeds the computational cost required for their generation. A related approach, SecFUN, is presented by Ateniese et al. [13], who extend the standard Channel-aware Routing Protocol (CARP) implementation with an authentication scheme leveraging different lightweight signature

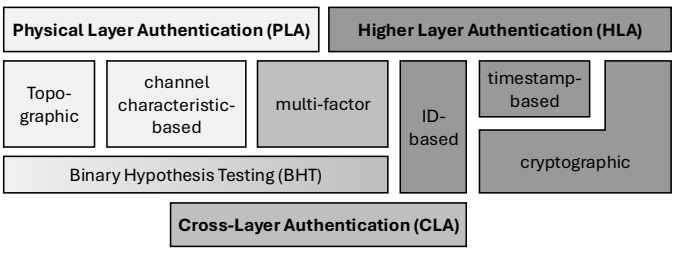


Fig. 2. A classification of various authentication categories and techniques.

schemes, including BLS, ZSS, and Quartz. As part of their evaluation, the authors compare end-to-end latency and energy/bit needed across all three signature schemes and show that BLS is specifically efficient. Note that SecFUN is a hybrid approach that also uses symmetric cryptography (i.e., AES in Galois/Counter Mode) for message authentication. Lastly, Du et al. [14] propose a novel signature scheme tailored to UAC. Their approach includes a trusted third party performing key agreement procedures with each node.

However, asymmetric cryptography and thus digital signatures are generally very computationally intensive. In addition, current schemes are under significant threat from quantum computers that can break cryptographic algorithms, while their symmetric counterpart, discussed in the following section, is less vulnerable to such quantum attacks [15].

*b) Symmetric Key Authentication:* A blockchain-based approach was proposed by Yazdinejad et al. [16], enabling decentralized authentication in cluster-based UWSNs by using a permission-less blockchain as a distributed database accessible across the network. To adapt to the underwater environment, they replace the commonly used proof-of-work mechanism [17] with a proof-of-authentication approach [18]. For performing authentication of nodes with information stored on the blockchain, new nodes have to be registered on the blockchain by their current CH. For the registration, initial authentication of the joining node based on a pre-shared key with the CH is performed. Only after successful authentication, the CH generates a genesis transaction, creating a valid key for the node, and distributes this key to the joining node. In the following, the freshly generated session key can be used for authenticated peer-to-peer communication within the network. If a node shows malicious behavior, its key is revoked, causing a disability to authenticate itself towards any other node within the network, thereby effectively leading to its isolation. A related, but leaner approach based solely on pre-shared key authentication is given by Xu et al. [19]. In their work, the authors describe a network defined by geographic clusters with node authentication performed on the basis of pre-shared cluster keys from which further pairwise keys are derived. Another approach for symmetric key management is proposed by Yuan et al. [20], introducing a modification to Blom's key management system [21]. Authentication is based on pairwise symmetric keys that are generated by a secret polynomial, which is derived based on Vandermonde matrices [22] and orthogonal space. The proposed approach consists of a centralized authentication scheme leveraging a base station to be responsible for creating the polynomial and performing the initial configuration of the nodes. A central advantage of the approach, as emphasized by the authors, is the reduction of memory requirements due to the structured nature of Vandermonde matrices as well as lower computational complexity. Lastly, Dini et al. [23] provide an authentication scheme both for a mutual authentication between a node and a central instance (such as a CH), as well as an authenticity check system based on message digests to verify the integrity of singular messages. By simulations, the authors tested their scheme with the transport layer protocols TCP and UDP, leading to a functional prototype implementation.

*2) Timestamp-based HLA:* A sub-direction explored within HLA is timestamp-based authentication. Such approaches typically integrate timestamps sent along each message and verify whether a certain timestamp falls within an expected time window. However, timing-based approaches are rarely used as standalone authentication mechanisms. More frequently, they are employed as an additional authentication factor, particularly in combination with cryptographic approaches, e.g., to prevent replay attacks as shown by Campagnaro et al. [24]. In a recent approach [25], an authentication scheme for NATO standard JANUS is introduced based on a pre-shared group key. Mutual authentication is performed via an encrypted three-way handshake, where timestamps serve as nonces for the derivation of session keys.

*3) ID-based HLA:* ID-based authentication represents the third pillar of HLA mechanisms explored for UWSNs. In this context, Islam and Taher [26] propose a trust management system leveraging hierarchical fuzzy systems [27] for authentication. Their approach requires a hierarchical network topology, where each node periodically updates a CH on its current one-hop neighbors. Once a node wants to establish communication with another node, it must announce its ID to the CH, triggering an authenticity check to verify the existence of a node with the announced ID.

### *B. Physical Layer Authentication*

At the physical layer, environmental physical properties can be leveraged to prove authenticity. Common for all approaches is their use of a *binary hypothesis testing (BHT)* [28] for decision-making, a statistical method to determine an unknown truth based on observed data within a setting of mutually exclusive binary decisions (e.g., authentic vs. non-authentic). Only if the observed data presents sufficiently strong evidence against a default assumption (i.e., authentic), the alternative hypothesis representing a statistically significant deviation (i.e., non-authentic) is chosen as the binary truth. At which point observed data is considered a significant deviation from the norm, is typically estimated by compressing observations into a numerical trust value that is compared against a predefined threshold. Naturally, the effectiveness of BHT is largely affected by the formulation of this threshold, which is a sensitive factor for the likelihood of inaccuracies in authentication decisions. Common techniques for threshold optimization in the context of PLA include supervised machine learning techniques such as Gaussian mixture models [29], [30], support vector machines [31], [32], or neural networks [32].

*1) Topographical PLA:* Location-specific properties of network nodes and received messages can be used to determine their authenticity. Based on positional information, a receiver checks whether valid messages have previously been received from the spatial vicinity of the alleged sender. Khalid et al. [29]

introduced a novel authentication approach based on Angle of Arrivals (AoAs) of received messages. By maintaining an AoA database of previously received messages from legitimate nodes, current and previous AoAs can be fed into the BHT, where outliers in the observed distance between the measured and estimated sender positions serve as an indicator for potential spoofing. Similarly, Aman et al. [33] combine AoAs with transmission distances to retrieve an estimation of the sender's spatial position. Using these features as a joint transmitter fingerprint, BHT is again applied to determine the likelihood of the sender's authenticity.

*2) Channel-based PLA:* In contrast to methods using the sender's position as a criteria for their legitimacy, channel-based authentication approaches utilize the physical characteristics of the acoustic link between sender and receiver. Frequently used characteristics include the propagation delay spread [31], [34] of the channel as well as the Channel Impulse Response (CIR) [30]. Since these properties are assumed to be unique for each connection, it is challenging for attackers to authentically forge them. However, these channel features are also subject to significant variations caused by UAC's dynamic nature and thus constitute no robust features for authentication [32]. Instead, Casari et al. [32] suggest using the power-weighted average delay and exploit the channel's time variability. As the average delay determines the distance between the sender and receiver, it provides a more reliable signature of the transmitter. To implement their idea, multiple cooperative receivers are integrated to enhance the robustness of the transmitter's signature. Then, a Kalman filter is utilized to manage the mobility of nodes. The difference between the filter's prediction and the observation is finally compared against a BHT threshold. By analyzing different strategies for combining measurements from different receivers, the authors conclude that the simplest form of linear combination leads to similar results as the more complex combinations via neural networks [35] or one-class support vector machines [36]. Similarly, Xiao et al. [37] propose a method leveraging the average received signal power and the delay of the channel's propagation paths into a joint channel vector that can be compared to historic recordings in a BHT. Additionally, they propose deep-learning strategies for smart channel feature estimation that can even further increase the robustness against spoofing attacks. Machine Learning for decision-making was also tested by Bragagnolo et al. [38], who experiment with neural networks and an auto-encoder based on channel features such as number of taps, delay spread, and received power. Both approaches demonstrate fairly good results with respect to precision and recall.

### C. Cross-Layer & Multi-Factor Authentication

CLA leverages authentication factors from both physical and higher layers to establish a multi-factor authentication process. An example is proposed by Guqhaiman et al. [39] who utilize a combination of senders' MAC addresses, physical AoAs, and hop counts of messages for authentication. Authenticity checks for messages can be performed decentrally by each receiver without global synchronization. Since MAC addresses can be forged relatively easily, the authors replace traditional MAC addresses with unique identifiers called IMAC values, which are assigned to each trusted node during initial deployment and stored by neighboring nodes. After deployment, authentication procedures for messages are performed in two phases. First, messages are collected during a monitoring phase, where nodes receive messages and extract the respective message header and AoA for subsequent authenticity checks of the messages. After that, authenticity inspections for all received messages are performed by checking whether the IMAC of a received message belongs to one of the neighboring nodes, and AoA and hop count of the received message coincide. If any discrepancies are found, a node considers the message malicious and alerts its neighbors.

Su et al. [40] introduced another CLA approach focusing on centralized cluster-based UWSNs. Here, the cluster structure is assumed to consist of a designated CH supported by two assisting nodes, which are responsible for authentication management and inter-cluster communication. To establish authentication within its cluster, the CH initially broadcasts a Request-to-Send (RTS) with maximum transmission power, requesting its cluster nodes to respond with their unique identities. For each member node, the CH then calculates the average Time-Reversal Resonating Strength (TRRS) value based on a database of historic CIRs to associate channel-based information accurately with node IDs. To authenticate a node, the CH and its aides collect nodal information across three categories: the TRRS as channel-based evidence, packet forwarding and bit error rate as behavior-based evidence, and the energy consumption rate of nodes. This information is then fused into a trust value to update a node's overall trustworthiness score. If a node's trustworthiness score decreases below a predefined threshold, it is deemed inauthentic, cooperatively causing jamming signals by the nearest legitimate node.

## IV. Comparative Analysis & Discussion

As mentioned in the previous section, early studies on underwater acoustic authentication mostly comprise (cryptographic) HLA approaches attempting to simply transfer established cryptography, such as digital signatures, from the terrestrial domain. This strategy is not only straightforward, but we also assess the security level of cryptographic authentication approaches as very high due to the robustness of their cryptographic building blocks, as can be seen in our final and summarized comparison in Table I.

However, this comes at the cost of significant communication overhead. Most HLA methods require the transmission of additional information on top of payload data. This results either in increased message size due to appended signatures [9], [13], [14], or in increased network traffic due to additional authentication tags and handshaking for symmetric cryptographic HLA schemes [16], [19], [20], [25], [26]. While such considerations are negligible in terrestrial networks, they are afforded much bigger significance in the context of UWSNs.

TABLE I
UAC AUTHENTICATION SURVEY AND ASSESSMENT.

| Categorie | Authors | Year | Ref. | Approach | Description | Synchonization | 3rd Party | Secure Channel | Mobility Support | E2E Support | Feasibility | Security Level |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| HLA | Dini and Duca | 2011 | [23] | cryptographic | symmetric | ○ | ◐ | ● | ■ | ■ | | |
| | Souza et al. | 2013 | [9] | cryptographic | digital signature | ○ | ○ | ● | ■ | ■ | | |
| | Ateniese et al. | 2015 | [13] | cryptographic | digital signature | ○ | ○ | ● | ■ | ■ | | |
| | Yuan et al. | 2015 | [20] | cryptographic | symmetric | ○ | ● | ● | ■ | ■ | | |
| | Du, Peng, & Li | 2017 | [14] | cryptographic | digital signature | ○ | ○ | ● | ■ | ■ | | |
| | Xu and Liu | 2018 | [19] | cryptographic | symmetric | ○ | ◐ | ● | ■ | ■ | | |
| | Yazdinejad et al. | 2019 | [16] | cryptographic | symmetric | ○ | ◐ | ● | ■ | ■ | | |
| | Islam and Taher | 2021 | [26] | ID-based | ID | ● | ◐ | ○ | ■ | □ | | |
| | Téglásy et al. | 2022 | [25] | timestamp/crypto. | symmetric, nonce | ● | ○ | ● | ■ | ■ | | |
| PLA | Aman et al. | 2018 | [33] | topographic | AoA, distance | ● | ○ | ○ | □ | □ | | |
| | Diamant, Casari & Tomasin | 2019 | [31] | channel-based | #taps, power, delay | ◐ | ◐ | ● | □ | □ | | |
| | Xiao et al. | 2019 | [37] | channel-based | power, delay | ○ | ○ | ○ | □ | □ | | |
| | Khalid, Zhao & Ahmed | 2020 | [29] | topographic | AoA | ● | ○ | ○ | □ | □ | | |
| | Bragagnolo et al. | 2021 | [38] | channel-based | #taps, power, delay | ◐ | ◐ | ● | □ | □ | | |
| | Zhao et al. | 2022 | [30] | channel-based | CIR | ○ | ○ | ○ | ◩ | □ | | |
| | Ardizzon et al. | 2022 | [34] | channel-based | #taps, power, delay | ● | ◐ | ● | ◩ | □ | | |
| | Casari, Ardizzon & Tomasin | 2022 | [32] | channel-based | delay, time variability | ● | ○ | ○ | ◩ | □ | | |
| CLA | Al Guqhaiman et al. | 2020 | [39] | ID, topographic | AoA, hop count, ID | ○ | ○ | ○ | □ | □ | | |
| | Su et al. | 2022 | [40] | channel, misc. | CIR, misc. | ○ | ◐ | ○ | ◩ | □ | | |

**Dependencies**: ○ not required, ◐ partly required, ● required; **Features**: □ no, ◩ partial, ■ full; **Results**: low high.

As an innovative response, PLA methods utilizing already existing environmental data for authentication have emerged in the following years (cf. Table I). Compared to HLA, this category of approaches specifically stands out by its lightweightness. As PLA leverages channel and nodal features such as delay or AoA, communication costs in terms of larger or more frequent transmissions are cut. With an increasing number of features that are evaluated for authentication purposes, PLA approaches can become more expensive in terms of memory and processing [32], [37], [38]. However, transmission and computation overhead for cryptographic HLA exceed even the costs of elaborate PLA approaches by far, which makes HLA less feasible (cf. Table I).

Beyond their lightweightness, some approaches from the PLA category even manage without the requirements of a third party, precise time synchronization, secure out-of-band channels, and some even support moderate to rapid mobility of nodes within the network [30]–[32]. These features generally underline the extreme customization of PLA to the narrow requirements of the underwater domain as presented in Section II. In contrast to that, HLA methods often require pre-installed keys [9], [13], [14], [16], [19], [20], [23], cluster architectures [16], [19], [20], [23], [26], or a reliable time synchronization infrastructure [25], [26] making a smooth transfer into practice more cumbersome.

Still, physical layer information can also be forged by intruders manipulating node position data or channel characteristics. Examples of malicious behavior include a closer placement to legitimate nodes, thereby obtaining similar properties of the channel, or the attempt to artificially replicate positional characteristics. Since BHT thresholds might be defined relatively lax to avoid false-positives, a fairly good manipulation of channel characteristics or node positions is sufficient for an attacker to be considered authentic within the network. Because deterministic cryptographic HLA methods are robust against these probabilistic decision-making trade-offs, we find that their potential regarding their security level is higher than that of PLA, despite PLA methods excelling with respect to other criteria (cf. Table I). At the same time, the security level provided by PLA methods might be fully sufficient for civil applications with lower security risks than their military counterparts. In particular, PLA methods combining multiple physical properties [31], [32], [37], [38] and CLA methods leveraging features even across multiple layers [39], [40] raise the bar for attackers trying to circumvent authentication. Nevertheless, applications with elevated security requirements might demand authentication mechanisms that completely eliminate the risk of false classification and moreover, enable E2E authentication. As PLA approaches leverage direct link information between two nodes due to the analysis of either direct neighbor transmission behavior or channel characteristics, PLA cannot be employed for verifying message integrity and authenticity of nodes beyond their one-hop links. Hence, this weakness also extends to the studied CLA approaches utilizing physical layer properties [39], [40].

In summary, one of the major key findings visualized by Table I is the obvious trade-off between the level of protection achieved by an authentication approach and its feasibility for the underwater domain. Underwater use cases requiring a high level of protection thus call for a novel category of approaches combining both the security potential of cryptographic primitives as well as the lightweightness of PLA approaches.

## V. Conclusion

Authentication in underwater acoustic networks requires a careful balance between security strength and communication efficiency. While higher-layer (cryptography-based) approaches offer robust protection, their overhead often exceeds the constraints of underwater environments. In contrast, Physical Layer Authentication (PLA) provides lightweight and domain-adapted alternatives, though at the cost of reduced security. Cross-layer methods attempt to combine the strengths of both, but inherit PLA's limited capability for end-to-end authenticity. Hence, applications with elevated security demands will likely require hybrid approaches that integrate cryptographic primitives with physical-layer efficiency. As our analysis highlights, a cryptography that is truly lightweight in terms of message size and thus, communication overhead remains a key challenge. Developing efficient, low-overhead approaches tailored to the constraints of underwater communication is, therefore, a critical and promising direction for future research.

## Acknowledgments

The authors would like to thank Jonas Koczwara for supporting this work with literature research and an initial overview of existing approaches. They are responsible for the contents of this publication.

## References

[1] 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.

[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] S. Jiang, "On Securing Underwater Acoustic Networks: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 729–752, 2019.

[4] B. Liu, J. Huang, N. Jia, B. Wang, and S. Guo, "Covert Underwater Acoustic Communication Using Marine Ambient Noise Without Detectable Features," *Journal of Marine Science and Engineering*, vol. 12, no. 12, 2024.

[5] C. Peng, X. Du, K. Li, and M. Li, "An Ultra-Lightweight Encryption Scheme in Underwater Acoustic Networks," *Journal of Sensors*, vol. 2016, no. 1, 2016.

[6] M. Goetz and I. Nissen, "GUWMANET – Multicast routing in Underwater Acoustic Networks," in *Proc. of MCC*, 2012.

[7] 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.

[8] Aki, "Digital Signatures: A Tutorial Survey," *Computer*, vol. 16, no. 2, pp. 15–24, 1983.

[9] E. Souza *et al.*, "End-to-end authentication in Under-Water Sensor Networks," *Proc of ISCC*, 2013.

[10] F. Zhang, R. Safavi-Naini, and W. Susilo, "An Efficient Signature Scheme from Bilinear Pairings and its Applications," in *Proc. of PKC*, 2004.

[11] D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from the Weil Pairing," in *Proc. of the International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2001, pp. 514–532.

[12] D. Johnson, A. Menezes, and S. Vanstone, "The Elliptic Curve Digital Signature Algorithm (ECDSA)," *International Journal of Information Security*, vol. 1, pp. 36–63, 2001.

[13] G. Ateniese *et al.*, "SecFUN: Security Framework for Underwater Acoustic Sensor Networks," in *Proc. of OCEANS 2015-Genova*, 2015.

[14] X. Du, C. Peng, and K. Li, "A secure routing scheme for underwater acoustic networks," *Int J Distrib Sens Netw*, vol. 13, no. 6, pp. 1–13, June 2017.

[15] J. Sliwa, K. Wrona, T. Shabanska, and A. Solmaz, "Lightweight Quantum-Safe Cryptography in Underwater Scenarios," in *Proc. of LCN MarCaS*, 2023.

[16] A. Yazdinejad *et al.*, "Energy Efficient Decentralized Authentication in Internet of Underwater Things Using Blockchain," in *Proc. of Globecom Workshops*, 2019.

[17] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the Security and Performance of Proof of Work Blockchains," in *Proc. of SIGSAC*, 2016, pp. 3–16.

[18] D. Puthal, S. P. Mohanty, P. Nanda, E. Kougianos, and G. Das, "Proof-of-Authentication for Scalable Blockchain in Resource-Constrained Distributed Systems," in *Proc. of ICCE*, 2019.

[19] M. Xu and L. Liu, "SenseVault: A Three-tier Framework for Securing Mobile Underwater Sensor Networks," *IEEE Trans Mob Comput*, vol. 17, no. 11, pp. 2632–2645, November 2018.

[20] C. Yuan *et al.*, "A Low Computational Complexity Authentication Scheme in Underwater Wireless Sensor Network," in *Proc. of MSN*, 2015.

[21] R. Blom, "Non-Public Key Distribution," in *Advances in Cryptology: Proceedings of Crypto 82*. Springer, 1983, pp. 231–236.

[22] D. Kalman, "The Generalized Vandermonde Matrix," *Mathematics Magazine*, vol. 57, no. 1, pp. 15–21, 1984.

[23] G. Dini and A. L. Duca, "A Cryptographic Suite for Underwater Cooperative Applications," in *Proc. of ISCC*, 2011.

[24] F. Campagnaro *et al.*, "Replay-Attack Countermeasures for Underwater Acoustic Networks," *Proc. of Global Oceans 2020: Singapore – U.S. Gulf Coast*, 2020.

[25] B. Z. Téglásy, E. Wengle, J. R. Potter, and S. Katsikas, "Authentication of Underwater Assets," *Computer Networks*, vol. 241, p. 110191, 2024.

[26] A. A. Islam and K. A. Taher, "A Novel Authentication Mechanism for Securing Underwater Wireless Sensors from Sybil Attack," in *Proc. of ICEEICT*, 2021.

[27] L.-X. Wang, "Analysis and Design of Hierarchical Fuzzy Systems," *IEEE Transactions on Fuzzy Systems*, vol. 7, no. 5, pp. 617–624, 1999.

[28] J. Neyman and E. S. Pearson, "On the Problem of the Most Efficient Tests of Statistical Hypotheses," *Philosophical Transactions of the Royal Society of London. Series A, Containing Papers of a Mathematical or Physical Character*, vol. 231, no. 694-706, pp. 289–337, 1933.

[29] M. Khalid, R. Zhao, and N. Ahmed, "Physical Layer Authentication in Line-of-Sight Underwater Acoustic Sensor Networks," *Proc. of Global Oceans 2020: Singapore – U.S. Gulf Coast*, 2020.

[30] R. Zhao *et al.*, "Physical Layer Node Authentication in Underwater Acoustic Sensor Networks Using Time-Reversal," *IEEE Sens J*, vol. 22, no. 4, pp. 3796–3809, February 2022.

[31] R. Diamant, P. Casari, and S. Tomasin, "Cooperative Authentication in Underwater Acoustic Sensor Networks," *IEEE Trans Wirel Commun*, vol. 18, no. 2, pp. 954–968, February 2019.

[32] P. Casari, F. Ardizzon, and S. Tomasin, "Physical Layer Authentication in Underwater Acoustic Networks with Mobile Devices," in *Proc. of WUWNet*, 2022.

[33] W. Aman *et al.*, "Impersonation Detection in Line-of-Sight Underwater Acoustic Sensor Networks," *IEEE Access*, vol. 6, pp. 44 459–44 472, August 2018.

[34] F. Ardizzon *et al.*, "Machine Learning-Based Distributed Authentication of UWAN Nodes with Limited Shared Information," in *Proc. of UComms*, 2022.

[35] M. A. Nielsen, *Neural Networks and Deep Learning*. Determination Press San Francisco, CA, USA, 2015, vol. 25.

[36] B. E. Boser, I. M. Guyon, and V. N. Vapnik, "A Training Algorithm for Optimal Margin Classifiers," in *Proc. of the fifth Annual Workshop on Computational Learning Theory*, 1992, pp. 144–152.

[37] L. Xiao *et al.*, "Learning-Based PHY-Layer Authentication for Underwater Sensor Networks," *IEEE Communications Letters*, vol. 23, no. 1, pp. 60–63, January 2019.

[38] L. Bragagnolo *et al.*, "Authentication of Underwater Acoustic Transmissions via Machine Learning Techniques," in *Proc. of COMCAS*, 2021.

[39] A. Al Guqhaiman *et al.*, "Lightweight Multi-factor Authentication for Underwater Wireless Sensor Networks," in *Proc. of CSCI*, 2020.

[40] Y. Su *et al.*, "A Cooperative Jamming Scheme Based on Node Authentication for Underwater Acoustic Sensor Networks," *Journal of Marine Science and Application*, vol. 21, no. 2, pp. 197–209, 2022.