A Deep Dive into Wormhole Attacks in Underwater Acoustic Communication: From Theory to Practice

Luisa Lux
luisa.lux@fkie.fraunhofer.de
Fraunhofer FKIE
RWTH Aachen University
Wachtberg and Aachen, Germany

Jan Bauer
jan.bauer@fkie.fraunhofer.de
Fraunhofer FKIE
Wachtberg, Germany

Eric Wagner
eric.wagner@uni.lu
University of Luxembourg
Luxembourg, Luxembourg

Konrad Wolsing
wolsing@comsys.rwth-aachen.de
RWTH Aachen University
Aachen, Germany

Ulrike Meyer
meyer@itsec.rwth-aachen.de
RWTH Aachen University
Aachen, Germany

Abstract

With growing geopolitical interests in the maritime domain, security research of Underwater Acoustic Networks (UANs) gains momentum. One threat that has been receiving continuous attention for over two decades is the *wormhole attack*. However, despite having proposed multiple detection and prevention mechanisms, the theoretical feasibility of wormhole attacks in underwater scenarios has been motivated solely by the different propagation speeds of sound waves in water and electromagnetic waves in air. To the best of our knowledge, this work provides the first proof-of-concept to confirm the practical feasibility of wormhole attacks in a real UAN. Additionally, we carry out an in-depth analysis of the variables influencing the success of wormhole attacks and demonstrate how different UAN types can fall victim to wormholes depending on their configuration and deployment.

CCS Concepts

• **Security and privacy → Mobile and wireless security**.

Keywords

Underwater Acoustic Networks, Network Security, Wormhole Attack, Proof-of-Concept

ACM Reference Format:
Luisa Lux, Jan Bauer, Eric Wagner, Konrad Wolsing, and Ulrike Meyer. 2026. A Deep Dive into Wormhole Attacks in Underwater Acoustic Communication: From Theory to Practice. In *Proceedings of the 19th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '26), June 30-July 03, 2026, Saarbrücken, Germany*. ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3765613.3811672

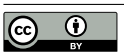
1 Introduction

Terrestrial wireless communication has become the backbone of contemporary society, with decades of research efforts contributing to this status quo. As roughly 70% of our planet is covered by water, the growing interest of governments and academia in transferring this success to underwater communication over the last decades is no surprise [3, 48]. By now, Underwater Acoustic Networks (UANs) are deployed for a wide variety of scientific, industrial, and military applications ranging from homeland security, over offshore critical infrastructures, to marine climate protection [15, 28].

Conventional terrestrial data transmission technologies based on electromagnetic signals are mostly unusable in the underwater domain due to the strong absorption of electromagnetic waves [28]. Instead, acoustic channels leveraging sound waves are preferred for underwater networking [3]. Under water, sound can travel hundreds of kilometers, enabling communication over large distances [3]. But, depending on depth, salinity, and temperature, sound just travels at a speed of 1450–1560 m/s [9]. Thus, under water, acoustic signals propagate five orders of magnitude slower than terrestrial electromagnetic signals ($\sim 3e8$ m/s). This high latency comes with a narrow frequency spectrum at which acoustic underwater hardware operates. Due to the strong absorption of higher-frequency waveforms, only low data rates can be achieved [3].

The long distances that UANs can cover allow their deployment in extremely remote areas that can, in turn, be covertly accessed by adversaries [14]. The combination of handling critical information and being covertly accessible renders UANs an attractive target for adversaries [23], while their ambiguous network structure and limited bandwidth exacerbate their protection. Nevertheless, bandwidth-efficient cryptographic measures, such as truncated authentication tags [40], physical layer key agreement schemes [8], and efficient ciphers [39] can partially protect against attacks threatening data confidentiality and integrity. However, some cyberattacks against underwater communication cannot be prevented by cryptographic measures alone. Probably the most prominent of these attacks are *wormhole attacks* [10, 14, 23]. As sound travels slower than light, *wormhole links* like cables or radio surface channels can be installed in UANs to transport signals faster than the acoustic links below the surface [22]. Due to its exploitation of two different communication mediums (e.g., water and air), we call it a *hybrid wormhole attack*.

Traditionally, a wormhole attack is based on an out-of-band channel, the wormhole link, that outperforms regular communication [22, 45] within the targeted network. It thus constitutes a special variant of the broader category of relay attacks, where attackers



WiSec '26, Saarbrücken, Germany

ACM ISBN 979-8-4007-2201-1/2026/06
https://doi.org/10.1145/3765613.3811672

perform a Man-in-the-Middle (MitM)-attack to bridge a connection between two otherwise disconnected communication partners [41] and replay attacks, where recorded messages are resent within the network [4]. Wormholes were originally introduced in the more general context of Mobile Adhoc Networks (MANETs) [26]. As MANETs are characterized by a dynamic formation, a disproportionately performant wormhole link (e.g., fast, robust, reliable, etc., or pretending to be such) may interfere with neighbor and route discovery as well as localization , and consequently disrupt a wide variety of network services. For terrestrial networks, the practical feasibility of wormhole attacks was demonstrated, e.g., on IEEE 802.15.4 [13, 29] and IEEE 802.11a/b/g networks [46]. Recently, terrestrial ultrasound applications have also been associated with the wormhole attack [18]. This confirmed risk that arises from wormholes launched a series of studies examining wormhole detection and prevention mechanisms [16, 17, 19]. However, these approaches were developed based on the physical properties of terrestrial networks and cannot be naively transferred to the underwater domain. This is due to the non-negligible propagation delay that makes UANs prone to the hybrid wormhole variant, which is not feasible in terrestrial, electromagnetic-based networks, namely *the out-speed of direct links*.

Countermeasures specifically adapted to the features of UANs were more recently investigated [2, 43, 45]. Unfortunately, these detection and prevention methods are (if at all) validated by simulations only. As the success of hybrid wormhole attacks heavily relies on timing effects and physical phenomena, real-world examination, as performed for jamming attacks in UANs by Zuba et al. [49], is crucial to fully understand the potential and limitations of wormholes in UANs. Nevertheless, to the best of our knowledge, no reports on the real-world feasibility of hybrid wormhole attacks have yet been published. Instead, the threat posed by wormhole attacks for UANs has been motivated solely by reference to the physical properties of water and air as communication mediums [9, 22, 43] –without further analyzing the detailed physical preconditions for a successful hybrid wormhole attack. Even analyzing the preconditions for wormholes theoretically is only attempted by a few works, both in terrestrial and underwater networks [22, 38], with none of them providing an exhaustive and systematic investigation of the concrete parameters affecting a difference in the end-to-end delay between wormhole and benign links.

Contributions. To address the missing theoretical and practical analysis of the feasibility of hybrid wormholing attacks, we make the following contributions:

(1) We examine the literature on wormholing in UANs to derive a representative attack model (Section 2).
(2) We formalize wormhole attacks and derive their necessary physical preconditions (Section 3). We concentrate on the – from the attacker's perspective – most challenging direct-benign-link setting. We show that this setting is only feasible in extremely high-latency networks such as UANs.
(3) We apply these insights to off-the-shelf hardware (Section 4) and validate the technical feasibility of hybrid wormholes targeting direct links in a real-world experiment (Section 5).
(4) We abstract these specific experimental results to assess the risk of hybrid wormhole attacks for current state-of-the-art underwater communication hardware (Section 6).

2 Hybrid Wormholes in Literature

As a basis of our theoretical and practical examination, we conducted a systematic literature review (SLR) according to the guidelines by Kitchenham et al. [21]. The review was guided by three research questions:

Q1: What is known on the practical feasibility of wormhole attacks in UANs, and has it been experimentally confirmed?
Q2: How are wormhole attacks in the underwater domain currently characterized?
Q3: How can we synthesize existing attack descriptions into a representative wormhole scenario to theoretically analyze and experimentally implement a Proof-of-Concept (PoC)?

2.1 Setup and Procedure

On November 6th of 2025, we conducted the SLR leveraging *Parsifal* [11]. Our methodology is visualized in Figure 1. The search with keywords *underwater* and *wormhole* ① returned 921 publications and reduced iteratively (②–④) to a final set of 156 works, excluding a significant group of papers dealing with wormholing in other types of sensor networks. As the physical characteristics of terrestrial communication rule out variants of the wormhole attack that are physically feasible only in UANs, hybrid wormholes can cover more attack nuances than non-hybrid wormholes. As the majority of wormhole-related works are not UAN-related, including these works would possibly result in an unrepresentative weighting of attack aspects for hybrid wormholes. We thus decided to exclusively condense our findings to UAN-related wormhole attack literature.

2.2 Evaluation

The selected set of papers shows a rise of publications per year from 2005 (earliest mentioning wormholing in UANs [43]) until 2025, indicating that the topic has gained attention progressively over the last years (cf. Figure 2). In the following, we summarize our findings regarding Q1 and Q2.

2.2.1 Q1: Wormhole Attack against UANs in Practice. Indications for practical implementations of wormhole attacks in UANs were not found in any of the 156 works that were examined. We thus conclude that no scientifically supported implementation of a wormhole attack in UANs has ever been conducted and published. We were especially interested to see how the works, which propose countermeasures for wormhole attacks in UANs, would evaluate their approaches. However, all of them exclusively opted for a

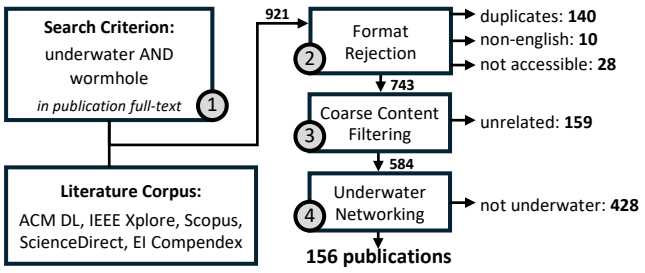


Figure 1: Selection process used in the SLR.

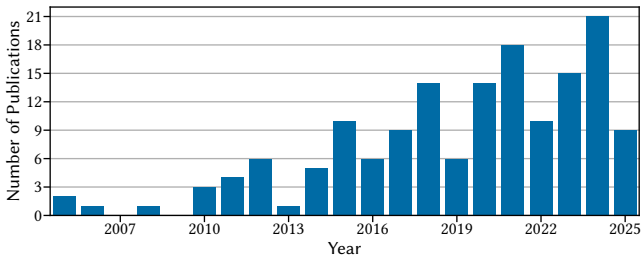


Figure 2: Increase of wormhole attack research in UANs over the last two decades.

simulation-based evaluation. As the modeling of sound in the underwater domain is rather complex and simulations mostly work event-based, they rationalize away factors, e.g., nodal processing, which might be of critical relevance for the success of a wormhole attack. Consequently, the relevance of this attack type cannot easily be assessed purely simulation-based.

2.2.2 Q2: Properties of Wormholes in UANs. Overall, the publications included in our SLR describe wormholes in the underwater domain with respect to four main aspects:

- A1: How and to what extent wormhole nodes infiltrate a network to incorporate their wormhole into a UAN, e.g., as insider or outsider, active attacker, etc.;
- A2: How the wormhole is technically implemented (establishing a wormhole tunnel, intercepting and forwarding messages);
- A3: Which malicious actions are enabled once the wormhole is installed (dropping and manipulating messages, etc.);
- A4: Which network services can be thus disrupted (routing, neighbor discovery, time synchronization, etc.).

We found aspects A1, A3, A4 to be described in many nuances within literature, thus creating a vast amount of attack variations. Agreement seems to be restricted to aspect A2, i.e., the physical installation of a wormhole.

To dive deeper regarding aspect A2, we also filtered examined works for attack descriptions, which could be found in 66 works. In the following, we provide the found number of works regarding an attack description property in parentheses. The three most commonly described properties within these descriptions are: (i) the wormhole being an *out-of-band channel* characterized by (ii) a *high performance* connection between (iii) *at least two colluding nodes*.

(i) Out-of-band channel. In the majority of works that contain an attack description, wormhole links are specified as non-acoustic out-of-band channels (48). We only find three works additionally considering so-called encapsulated wormhole attacks using an existing in-band network path [7, 27, 33]. With regard to the technical options that exist to establish such a non-acoustic out-of-band link in UANs, Kong et al. [22] distinguish between two alternatives: *Surface-level wormholes* connecting two surface-level devices via a radio link and *Underwater wormholes* establishing a wired connection between two underwater nodes. Technically, *underwater wireless wormholes* are also feasible, e.g., by leveraging optical communication, but such channels would be heavily restricted in range.

(ii) High performance. Wormhole links are typically associated with latency advantages. This is reflected in being described as a low-latency channel (17), a time-wise shortcut (4), or more generally as short (15) or efficient (2). However, instead of latency, wormholes can also be perceived as advantageous links due to other desirable characteristics, such as high-bandwidth (9), low hop-count (1), or even reliability.

(iii) Two nodes. In two-thirds of the descriptions, wormholes are explicitly defined as links between at least two colluding nodes (44) with no works contradicting this property. In practical scenarios, wormhole nodes might even have to be connected in series due to communication range constraints of the utilized technology, constituting a multi-hop wormhole.

2.3 Derived Basic Wormhole Scenario

Leveraging on our SLR, we now address Q3 and motivate and describe the basic hybrid wormhole scenario we consider in the rest of this paper. We also briefly discuss what our theoretical and practical analysis of the feasibility and limitations of wormhole attacks in this scenario allows us to conclude with respect to the feasibility of more complex wormhole scenarios.

Our analysis of wormhole attacks focuses on aspect A2. We deliberately refrain from making any assumptions regarding how nodes infiltrate a network to establish a wormhole (A1) and from considering any further malicious actions that can be taken with the help of an already established wormhole (A3) or their impact on network services (A4). Instead, we derive the following generic wormhole setting for UANs as depicted in Figure 3: We consider a scenario comprising four nodes A, B, W_1, W_2 with all neighboring nodes being in acoustic communication range of each other. We assume W_1 and W_2 to be two collaborating malicious nodes that are capable of recording signals broadcasted by A and B and processing them to the respective packet format on the data link layer. Furthermore, we assume that W_1 and W_2 have installed a wormhole link between each other (dashed red path). We found wormhole links to be commonly understood as *out-of-band channels* in Sec. 2.2 with at least one *high performance* feature. For our setup, we stick with the most widely described high-performance feature, namely, low latency. Since special network properties such as sparsity and node mobility render the use of cables cumbersome within UANs, we consider a *surface-level wormhole* (cf. Sec. 2.2) between W_1, W_2 in the rest of this paper. While the choice of technology might play a role from a practical perspective, from a conceptual point of view, these wormhole types mainly differ with respect to the individual latency improvement that they provide. Our setup and analysis can also be carried out for wired connections analogously.

Lastly, we opt for a setting in which only two benign and two wormhole nodes are present such that the basic wormhole setting we analyze incorporates on both paths the least amount of hops possible. As will be analyzed in-detail in Section 6.2.2, additional hops on either path slow down message delivery to the intended receiver. As the hybrid wormhole attack presented here is based on latency advantages, additional-hop cases lead to shifts in the results of our theoretical and practical analysis regarding the concrete environmental parameters needed for a successful attack: While multiple hops on the benign path make the tight timing constraints for the

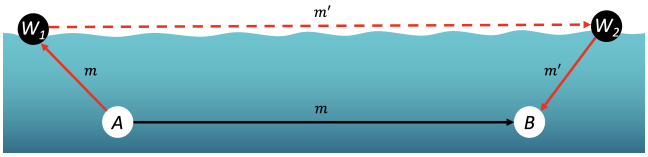


Figure 3: Two-node hybrid wormhole scenario considered comprises four nodes A, B, W_1, W_2 with a direct wormhole link (dotted red path) between W_1 and W_2.

wormhole attack more relaxing, additional hops on the wormhole path spanning over a direct acoustic link cause the opposite. Thus, the chosen setting with minimal hops as sketched in Figure 3 allows for logical propositions on both types of additional-hop cases:

Case 1: Proving the technical feasibility of a two-node wormhole spanning a direct underwater benign link also proves the technical feasibility of such a wormhole spanning a multi-hop benign path.

Case 2: A technical infeasibility of a two-node wormhole in our PoC also results in a technical infeasibility of a wormhole path with more than two nodes that targets a direct acoustic link.

3 Analytic Study

We now move on to analyzing the concrete parameters influencing the success of an attack in the basic wormhole scenario.[1] We start with a brief excursion to the components of end-to-end delay in general and subsequently formalize the wormhole problem. We end this section with an analysis of the concrete parameters influencing the feasibility and success of a wormhole attack in the given scenario before moving on to the practical PoC.

3.1 End-to-end-delay in Networks

In all types of networks, including UANs, end-to-end-delay τ_e is defined as the sum of (1) propagation delay τ_p, (2) transmission delay τ_t, (3) processing delay τ_{proc}, and (4) queuing delay τ_q [6]:

$$\tau_e = \tau_p + \tau_t + \tau_{proc} + \tau_q \tag{1}$$

The propagation delay between two nodes N_i and N_j describes the amount of time it takes for the first bit of the message to travel from one end of the link (sender) to the other end of the link (receiver):

$$\tau_p(d_{N_i,N_j}) = \frac{d_{N_i,N_j}}{v} \tag{2}$$

with d_{N_i,N_j} being the distance between two nodes N_i and N_j and v the signal propagation speed of the communication medium.

The transmission delay refers to the amount of time it takes to bring the complete message m onto the transmission link, depending on a given transmission rate R:

$$\tau_t(m) = \frac{|m|}{R} \tag{3}$$

In contrast to the propagation delay and transmission delay, both the processing delay, referring to the amount of time needed for nodal processing, and the queuing delay, representing the amount of buffer time until the message is processed, cannot be easily formalized. Instead, they need to be measured. Note that an overview on our notation can be found in Table 3 in the Appendix.

[1]This section is not UAN-specific, but can rather be applied to a basic wormholing attack following Figure 3 in any underlying networking technology.

3.2 Formalization of the Wormhole Problem

Considering the network setting in Figure 3, a wormhole attack is successful if the path $A \to W_1 \to W_2 \to B$ is faster than $A \to B$. We denote the original message to be routed from A to B over the path $A \to B$ as m, whereas the copy of the message that is wormholed along the path $A \to W_1 \to W_2 \to B$ is denoted as m' (cf. Figure 3).

We define a wormhole attack as successful only if the complete message m' can be wormholed over $A \to W_1 \to W_2 \to B$ before the first bit of message m sent from $A \to B$ is received at B. Otherwise, a collision at the receiver would occur. Thus, the wormhole attack is successful, if the end-to-end delay (see Section 3.1) on path $A \to W_1 \to W_2 \to B$ for message m' is smaller than the delay on path $A \to B$ for m's first bit:

$$\tau_e(\overrightarrow{A, W_1, W_2, B}) + \tau_t(m) < \tau_e(\overrightarrow{A, B}) \tag{4}$$

Since we assume that malicious nodes do not buffer messages, the queuing delay τ_q is omitted. Furthermore, we can ignore the nodal delays of A and B (processing and queuing) that are irrelevant for the hybrid wormhole in the end-to-end analysis. As a result, we get the following condition that needs to be satisfied for the wormhole to be successful. Note that we refer to the propagation and transmission delay on the out-of-band channel as $\tilde{\tau_t}$ and $\tilde{\tau_p}$:

$$\begin{aligned}\tau_e(\overrightarrow{A, W_1, W_2, B}) + \tau_t(m) = \\ \tau_p(d_{A,W_1}) + \tau_t(m) + \tau_{proc}(W_1) + \tilde{\tau_t}(m') + \tilde{\tau_p}(d_{W_1,W_2}) \\ + \tau_{proc}(W_2) + \tau_p(d_{W_2,B}) + \tau_t(m') + \tau_t(m) \\ < \tau_p(d_{A,B}) + \tau_t(m) = \tau_e(\overrightarrow{A, B})\end{aligned}$$

We can further reduce this formula and obtain the following formalization of the wormhole problem:

$$\begin{aligned}\iff \tau_p(d_{A,W_1}) + \tilde{\tau_p}(d_{W_1,W_2}) + \tau_p(d_{W_2,B}) + \tau_t(m') + \tilde{\tau_t}(m') \\ + \tau_t(m) + \tau_{proc}(W_1) + \tau_{proc}(W_2) < \tau_p(d_{A,B})\end{aligned} \tag{5}$$

Insight Wormholes targeting direct links are feasible iff networks' propagation delay $\tau_p(d_{A,B})$ is non-negligible and the attacker has an out-of-band channel with a lower delay.

3.3 Wormhole Performance Parameters

Analyzing parameters that govern the success of a wormhole attack further, we distinguish between parameters that we consider to be fixed, those that an attacker may control, and those that are variable, but controlled by the network.

3.3.1 Fixed parameters. Fixed parameters include the **speed of propagation** v (cf. Equation 2), both in the network medium and the medium of the out-of-band channel. While both propagation speeds depend on the communication forms used, they can neither be directly influenced by the benign nor the wormhole nodes.

3.3.2 Attacker-controlled Parameters. Parameters that we assume to be attacker-controlled are those that are independent of the benign network. This includes the **processing time** τ_{proc} of the wormhole nodes, which depends largely on the processing units

of the hardware involved as well as program run-times and serial transmissions within hardware components. These can be influenced by code optimization and high baud rates, as well as the choice of generally high-performant hardware. Secondly, the attacker can influence the parameters constituting the transmission delay $\tilde{\tau}_t(m')$ of the attacker-controlled out-of-band channel, the **message size** and **transmission rate on the out-of-band channel**. Considering Equation 3, we find that short message sizes and high transmission rates are desirable for a wormhole success as they effectively reduce $\tilde{\tau}_t(m')$. While the message size is subject to a lower bound provided by the payload size on the acoustic links, the attacker influences the length of preamble, header, and CRC size on the out-of-band channel. Lastly, the attacker can also impact the propagation delay on the links to the wormhole end-points. While propagation delay is typically negligible in networks operating with the speed of light, this is not the case in networks with slower wave propagation (i.e., UANs). Considering Equation 5, in these cases, the feasibility of a wormhole attack is facilitated by short **distances to the wormhole endpoints** d_{A,W_1} and $d_{W_2,B}$. Thus, the propagation delay, adding on the end-to-end delay of the wormhole path, can be effectively reduced by placing W_1, W_2 as close as possible to A and B respectively.

3.3.3 Network-controlled Parameters. Besides attacker-controlled parameters that can be configured as optimally as possible for the attacker, depending mostly on the attacker's resources, network-controlled parameters are variable and can be configured either in favor of the attacker or not. Given a specific attacker-controlled parameter set, a triad of three parameters influences whether the wormhole attack becomes feasible. This includes both the **message size** $|m|$ (cf. Equation 3) and the **transmission rate** R (cf. Equation 3) on the acoustic links. As for the out-of-band channel, we find that short message sizes and high transmission rates on the acoustic links are desirable for a wormhole success as they effectively reduce the transmission times $\tau_t(m')$ on the links to the wormhole endpoints. Their configuration varies depending on modem choice and application context, impacted by message formats including headers, CRC, error correction, and minimal payload length, as well as transmission parameters such as modulation, preamble length, and robustness considerations. Regarding the feasibility of a wormhole attack, this leads to a special relevance of the third network-influenced parameter, namely the **distance between benign nodes** $d_{A,B}$. As it considerably increases the propagation delay on the benign link (cf. Equation 2), a large distance $d_{A,B}$ on the benign link facilitates the attack.

Insight Wormhole attacks become more feasible with small message sizes $|m|$ and high data rates R as well as a large distance $d_{A,B}$.

Assuming that message sizes, transmission rates, processing delays, and distance to the wormhole endpoints are configured in a certain combination, this results in a minimal wormhole distance ω_{min} between nodes A and B at which the attack starts to become feasible. At the same time, it explains why the only wormhole variant feasible in the given wormhole setting (cf. Figure 3) is a hybrid wormhole due to the necessity of a non-negligible propagation delay. If we presume attacker-controlled parameters to be optimized within given resource limits, as well as message size and transmission rate within the network to be fixed and adapted to the network's application context, the length of $d_{A,B}$ is thus the prime driver for attack success with

$$\tau_e(\overrightarrow{A, W_1, W_2, B}) + \tau_t(m') < \tau_e(\overrightarrow{A, B}) \text{ then } \omega_{min} < d_{A,B} \quad (6)$$

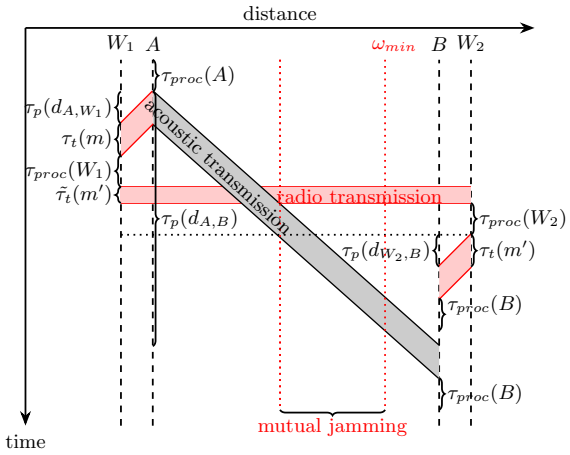


Figure 4: Components of end-to-end delay of messages m and m' until message reception at receiver B.

Insight If, dependent on the configuration of other network-controlled and attacker-controlled parameters, a wormhole attack against the link between A and B is feasible, there exists a minimal wormhole distance $\omega_{min} < d_{A,B}$.

We have visualized the composition of the delays for the given wormhole setting in Figure 4, showcasing the importance of the propagation delay between nodes A and B and including ω_{min}.

4 Application to Specific Hardware

We now apply our analyses of the parameters influencing the feasibility of a wormhole attack in the basic scenario (Figure 4) to the specific hardware setting we selected for our PoC. We first describe our hardware setup and then discuss how individual delay components and parameters influence ω_{min} to practically confirm our calculations. It also enables us to efficiently optimize hardware settings to reduce ω_{min} and facilitate the practical experiment within the possible communication range of our setup.

4.1 Hardware Setup

Wormholes are particularly dangerous if they can be carried out with off-the-shelf, low-cost equipment. For our PoC, we used hardware that can be freely purchased for under 1000 EUR per node.

Our setup comprises four underwater nodes, each consisting of a RaspberryPi connected with an underwater acoustic modem, an AS-1 hydrophone [1], a GPS receiver, and a power source. As an out-of-band channel for the wormhole link, two RaspberryPis were equipped with LoRa hats used for surface communication. We

chose LoRa as it is frequently deployed in marine applications due to its energy efficiency, robustness, and its ability to transmit over large distances [24, 34]. The underwater hardware used comprises four ahoi modems [32], which are well-documented open-source research modems developed by the University of Hamburg. The data rate of these modems is 250–4500 bps with a reported and tested communication range of 300 m. In our testbed setting, we use the high-speed wide-band configuration with a necessary spreading factor of $S = 3$ [32], resulting in a data rate of 1562.5 bps. The ahoi message format consists of a preamble, a header of 6 bytes, a payload of arbitrary byte length, and a CRC. For our PoC, we used the smallest possible payload size of 1 B. As LoRa hats, we use the Waveshare SX1262 868M LoRa HAT [44] operating in the 868 MHz frequency band with SF7 and a bandwidth of 125 kHz.

4.2 Preliminary Lab Measurements

To obtain a realistic estimation of ω_{min} for the PoC setup, we apply the wormhole formalization of Equation 5 (Section 3.2) to the selected hardware specifics. We provide concrete values for all parameters as introduced in Section 3.3. In Table 1, we summarize our lab findings showing both our measurements of the processing and transmission delays for the hardware used as well as the calculations for transmission and propagation delays based on the formulas introduced in Section 3.1. As the LoRa physical layer is proprietary, we leveraged the LoRa calculator by Semtech [35] to calculate LoRa transmission delays. For the manual measurements of transmission times, we used an oscilloscope of type Multi-ComP Pro MP720025 [25] which allowed us to determine the values approximately, apart from minor errors due to sound reflection and resonance in the water tank. Processing delays were measured based on round-trip times on the same RaspberryPi, subtracting measured transmission times and calculated propagation delays assuming a speed of sound under water of 1500 m/s and a negligible radio propagation delay in air $\tilde{\tau_p}$. As propagation delays, we assumed a distance of at least 5-7 m between nodes A, W_1 and W_2, B to avoid acoustic signal clipping [32]. To visualize the influences of the end-to-end delay components on ω_{min}, we also converted the measured delays into acoustic distances under water. Adding up these distances results in $\omega_{min} \approx 447–482$ m. The calculated minimal wormhole distance ω_{min} needed for the given hardware configuration, therefore, does not lie within the confirmed communication range r_{max} of the utilized modem.

> **Insight** The feasibility of a two-node hybrid wormhole attack (cf. Figure 3) is limited by acoustic communication distance and requires $r_{max} > \omega_{min}$.

4.3 Optimization of Parameters for Lake Trials

We find the transmission delays of the underwater links and the LoRa connection to particularly drive up the required minimal wormhole distance ω_{min}. Therefore, we opted for both the LoRa hats and the underwater modems to run in implicit header mode [36]. While implicit header mode is a standardized technique for LoRa, this was not the case for the ahoi modems and required a manual hardcoding of the ahoi header into the modem firmware. As illustrated in Table 1, sending the message payload without the header results in a large reduction of the transmission times, leading to a reduced $\omega_{min} \approx 215–250$ m. This design choice was made to enable the wormhole attack within the modems' communication range. Note that commercial and non-academic modems typically have higher communication ranges [5, 20, 37, 47] allowing to perform hybrid wormhole attacks within their comfortable range even without having to artificially shorten messages. Details regarding the modem configuration are summarized in Table 4.

5 Proof-of-Concept

Our analysis in Section 4 shows that a hybrid wormhole attack cannot be carried out in a lab setting. We therefore conducted our experiments in a nearby lake with our final lake experiments being conducted on November 14th, 2025, between 10:30 am to 5 pm. The reported outdoor temperature was at 16 °C.

5.1 Experiment Setup

In our experiments, A, acted as the sender, broadcasting messages with a payload of 1 B every 5 s. Its position in the middle of the lake (cf. Figure 5) was relatively static as it was moored at a buoy.

W_1 acted as the wormhole start point. It constantly listened on its acoustic channel. Once A sent a message, the hydrophone of W_1 picked it up, the modem processed it, and then sent it over its serial connection to the RaspberryPi, which broadcasted the message over its LoRa channel. W_1 was roped together with A such that the underwater distance between A and W_1 was around 5 m. W_2 acted as wormhole endpoint. It constantly listened on its LoRa channel. Once it received a message from W_1, the message was forwarded over the serial connection to the modem, which then transmitted it acoustically over its hydrophone. W_2 was roped together with B. As B was mobile, the distance between W_2 and B varied between approximately 3 m and 5 m. Finally, B acted as receiver and constantly listened on its acoustic channel, logging incoming messages of A and W_2. Its position was mobile on a stand-up paddling board, either due to slow wind drift or cautious paddling. The wormhole endpoints were tied to benign nodes in order to keep conditions largely constant during the experiment; however, fixed distances are not a prerequisite for carrying out the attack.

Two rounds of experiments were performed. The first one was conducted between 10:30 am to 12:20 pm with a windspeed of 5.7–7.6 m/s, which allowed for a slow but steady drift without having to use paddles. In the second one, between 3 pm to 5 pm, the wind speed slowed down to 3.1–4.3 m/s, necessitating more paddling. GNSS routes and experiment setup are shown in Figure 5.

5.1.1 Mutual jamming avoidance. As wormhole nodes try to outpace the receipt of the original message m, an attack success becomes more likely with increasing $d_{A,B}$. However, before ω_{min} is reached, the two messages m and m' collide due to their transmission times overlapping. This leads to a range in which m' effectively jams m. Thus, the formalization of the wormhole problem as defined in Equation 5 (Section 3.2) takes a collision phase $\tau_t(m')$ into consideration. To showcase this effect, we ran the experiment with two different setups: While we conducted a real wormhole setting in the afternoon experiment run, during which this mutual jamming (cf. Figure 4) effect takes place, the morning experiment introduced a fixed delay of 2 s within the wormhole node W_2 before

Table 1: Lab measurements and calculations of delay components (cf. Sec. 3.1) converted into acoustic distance under water.

Description	Parameter	Approximation [ms]	Measurement [ms]	Acoustic Dist. [m]
Propagation time under water (≈10 m)	$\tau_p(d_{A,W_1}) + \tau_p(d_{W_2,B})$	6.9–9.3	–	**10–14**
Propagation time in air (≈300 m)	$\tilde{\tau_p}(d_{W_1,W_2})$	<0.000001	–	0
Transmission time under water with header (based on [32])	$\tau_t(m') = \tau_t(m)$	117.76	118–122	177
Transmission time LoRa with header (based on [35])	$\tilde{\tau_t}(m')$	30.97	30.9	46
Sum of processing time	$\tau_{proc}(W_1)+\tau_{proc}(W_2)$	–	25–45	**37–68**
Transmission time under water **implicit header**	$\tau_t(m') = \tau_t(m)$	46.08	47–50	**69**
Transmission time LoRa **implicit header**	$\tilde{\tau_t}(m')$	25.85	20.1	**30**

Assumption: v_a ≈1500 m/s, v_c ≈300 000 000 m/s; (underlined values used for estimation of acoustic distance).

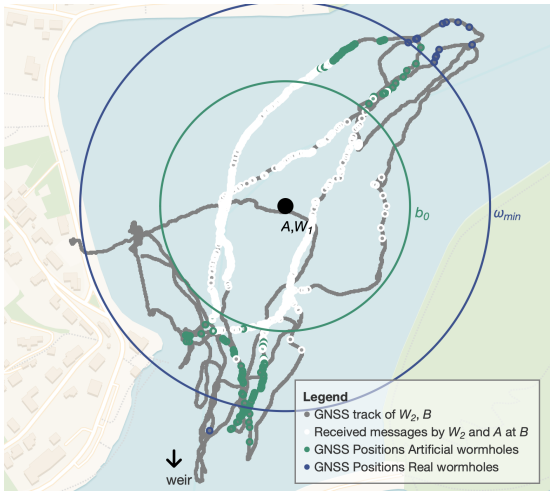


Figure 5: GNSS positions of the 102 artificial wormhole events and 13 real wormhole events

m' was forwarded to B, that was subtracted at B upon reception. This avoids the collision of m and m' and enabled a fine-grained analysis of the distance, where $\tau_e(\overrightarrow{A, W_1, W_2, B}) = \tau_e(\overrightarrow{A, B})$, practically resulting in a reception time difference $\Delta t(m, m') = 0$ at B. We refer to this boundary as b_0. As the wormholes measured in the morning do not necessarily meet Equation 5, we call them *artificial wormholes* in the following.

5.2 Experimental Results

We now present the results of the lake experiments described in the last section. The data is analyzed with a special focus on the proven feasibility of the attack as well as the recorded minimal wormhole distance ω_{min} to validate our theoretical analysis in Section 3. Furthermore, we provide data regarding the communication range and the packet delivery ratio (PDR) observed.

5.2.1 Link Quality. As expected and confirmed by Figure 6, the PDR (brown dots) measured over the entire day declined with increasing distance between nodes A and B. Regarding the single links between the nodes, Table 2 also draws a consistent picture for both experiment series and for the overall day: The PDRs of the links in the morning and afternoon are similar, with all links being slightly more stable in the morning. We suspect the mobility of nodes W_2 and B to be responsible for the lower PDR on link $W_2 \rightarrow B$ compared to the ones observed on link $A \rightarrow W_1$. We attribute the generally lower PDRs on all links in the afternoon to the additional noise caused by more intense paddling. The *mutual jamming avoidance* in the morning seemed to have a major positive effect on the PDR on both links $W_2 \rightarrow B$ and $A \rightarrow B$.

Table 2: Link quality, wormhole successes, and wormhole distances measured during the lake test. The measured ω_{min} of 221.5 m matches the calculated ω_{min} of 215–250 m.

Measurements	Morning	Afternoon	Entire Day
PDR $A \rightarrow B$ [%]	40.10	21.77	30.11
PDR $A \rightarrow W_1$ [%]	99.55	97.16	98.25
PDR $W_1 \rightarrow W_2$ (LoRa) [%]	98.56	92.25	95.16
PDR $W_2 \rightarrow B$ [%]	72.90	67.08	69.86
Measured r_{max} [m]	270.5	277.6	277.6
# successful wormholes	102	13	115
Measured $\omega_{min}[m]$	–	221.5	221.5
Wormhole success ratio [%]	60.00	81.25	60.85

5.2.2 Communication Range. Table 2 also shows that the maximally measured communication range between A and B was quite similar in the morning (270.5 m) and in the afternoon (277.6 m). This lies slightly below the reported communication range of the ahoi modems (300 m [32]). However, we did not actively attempt to reproduce these reported distances and reckon that the range limit we observed could be caused by noise from a weir in the vicinity of our experiments (cf. Figure 5, arrow). Furthermore, the S-shaped curve of the lake is transected by a steep shipping canal, resulting in an uneven bathymetry, which could have further impacted our reception in the opposite direction.

5.2.3 Wormhole Occurrences. During the two experiment runs, we logged 115 instances in total, in which the wormhole attack succeeded. Wormhole occurrences were events in which the timestamp of the wormholed message m' at node B was smaller than the timestamp of the original message m. Events, in which only m' was received by B, but not the corresponding m, were not counted as wormhole occurrences. Out of these 115 wormholes, 102 wormholes were logged during the morning measurements, constituting

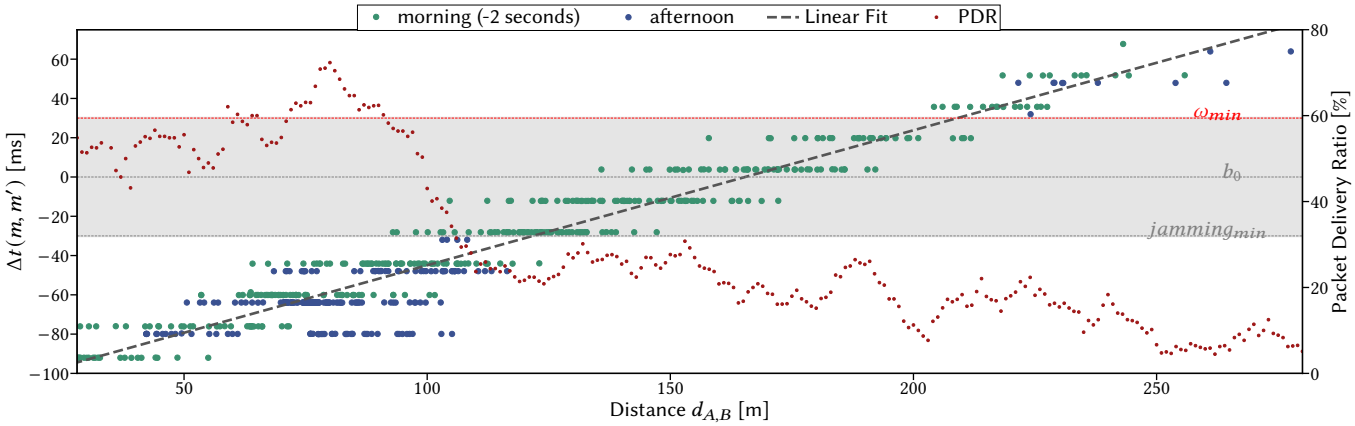


Figure 6: Measured delay between the reception of m and m' and PDR with increasing distance $d_{A,B}$. In the collision area (gray), no reception events of m and m' without mutual jamming avoidance (blue dots) were measured.

artificial wormholes as explained in Section 5.1. Another 13 successful wormhole attacks were logged during the afternoon experiment, constituting *real wormholes*.

> **Insight** Executing a hybrid wormhole attack in a UAN test setting is practically feasible.

5.2.4 Wormhole Distances. The distance b_0 was 135.8 m, measured during the experiment run in the morning. The geographical locations at which wormhole occurrences, both for artificial (green dots) and real wormholing (blue dots) took place are visualized in Figure 5. As expected and depicted in Figure 6, the reception time difference $\Delta t(m, m')$ at B (green and blue points) increases linearly with an increasing distance between nodes A and B. The distinct stair pattern in the time differences between m' and m can be explained by the ~16 ms-cyclic nature of the serial connection between modem and RaspberryPi, leading to a discretization of the time differences. The predicted mutual jamming effect in the afternoon experiment run shows in the gap of messages received between -30 ms and 30 ms visualized by the gray belt around the zero line representing b_0. With the underwater transmission delay $\tau_t(m)$=46.08 ms subtracted, the cyclic serial communication patterns of ~16 ms, this belt represents the timing area during which both messages are on the medium and thus collisions between m' and m can occur. Only if the wormhole message m' is significantly faster than the outpaced original message m (at least ~30 ms faster) by reaching the minimal wormhole distance ω_{min}, both messages are successfully received by B and a wormhole event is logged. Due to the cyclic serial communication effect, we expected the difference between ω_{min} and b_0 to be 30–62 ms resulting in a difference of approximately 45–93 m. This expectation was met by our measurements: the minimal wormhole distance ω_{min} measured in the afternoon was 221.5 m and thus 86 m larger than b_e measured in the morning experiments.

As visible in Figure 6, 27 artificial wormhole events additionally show a time offset of m' preceding m that is larger than 30 ms (green dots above the gray belt). Thus, they would have been real wormholes even without the jamming protection. This can also be seen in Figure 5 by the green dots outside the blue ω_{min} circle.

Considering that the experiment runs were conducted with implicit headers (cf. Section 5.1), measurements of b_0 provide guidance as to whether the experiment setup would have worked with headers as well. The additionally needed transmission time for messages in the ahoi format, including both payload and header, is 71.68 ms. As the measured b_0 was 135.8 m an additional time delay of 71.68 ms and 189.44 ms respectively would have resulted in a necessary distance of ≈250 m and ≈420 m for the artificial and real wormholes respectively. As the maximally measured communication range between the modems during our lake experiment was 277.6 m, the required minimal wormhole distance ω_{min} for real wormholes would have been much higher than the maximal communication range of the modems.

> **Insight** The measurements of the distances b_0 and ω_{min} match the analytic prognosis of Section 4.

6 Generalization to other UAN Hardware

Having demonstrated the technical feasibility of a basic hybrid wormhole within a concrete experimental setup in the previous section, we now assess the feasibility of such an attack in UANs more generally. As described in Section 3.3, variable *network-controlled* parameters influence ω_{min}. Especially, the data rates vary greatly between different underwater modem types. We therefore further examine how the choice of the modem influences the risk for wormholing in UANs. In particular, for each modem type, we determine the required ω_{min} based on its data rate and compare ω_{min} to its maximal communication range r_{max}. Additionally, we take additional-hop cases (cf. Section 2.3) into consideration.

6.1 Reference Data

To determine ω_{min} for different modems, we synthesize standalone publications, surveys [5, 20, 37, 47], and technical data sheets into a set of 144 underwater modems (cf. Appendix, Table 5). This covers

50 commercially available high-performance high-cost modems as well as 94 research modems developed as prototypes for academia. We explicitly exclude modem types not designed for acoustic communication (e.g., optical and radio modems) and acoustic modems that reported distances below 3 m, as these ultra-short distances are not the usual application cases of acoustics. As the majority of documents collected did not report specific message sizes, we use the message format of the JANUS communication standard [31] as a reference. Note that the ahoi message format and the JANUS message format have the same message size of 144 bits if we assume the smallest possible payload for both formats:

- JANUS: 64 information bits + 8 zeros with 1/2 convolutional encoder = 144 bits,
- ahoi: 6 header bytes + 1 byte header CRC + 1 byte payload + 1 byte payload CRC with (8/4) Hamming-Code = 144 bits.

As listed in Section 4.2, acoustic underwater communication typically uses preambles. We use the JANUS standardized preamble of 200 ms in the following. Compared to the ahoi preamble of 25.6 ms, this is relatively long. As references for the *attacker-controlled* variables (cf. Section 3.3), we use the measurements taken in Section 4.2.

6.2 Results

Based on the data rates collected in the last section and the measurements of Table 1, we can determine ω_{min} for each modem according to Equation 9 in the Appendix and evaluate whether $\omega_{min} < r_{max}$. Fixing all variables except for the data rate R, for JANUS, we obtain:

$$\Omega_{min}(R) := \left(2 \cdot \left(\frac{144\,\text{bits}}{R\,\text{bps}} + 200\,\text{ms}\right) \; + \; 54.4\,\text{ms}\right) \cdot 1500\,\text{m/s}$$

6.2.1 Basic Setting. The minimal wormhole distance needed is inversely proportional to the data rate and forms a hyperbolic curve. We thus present Figure 7 using a log-log scale. The combination of data rate and maximal communication range of each modem is marked (commercial modems with ⧫, research modems with •). Markers above the curve indicate that these modems are at risk for a hybrid wormhole when using link lengths larger than ω_{min} for the data rate of the given modem type. Figure 7 shows that a basic hybrid wormhole, as conducted in Section 5 is technically feasible for 63 modems. This is specifically the case for 80% of commercial modems due to their extensive communication ranges.

6.2.2 Additional-Hop Settings. Wormholes can also span multiple underwater hops or consist of more than two nodes on the wormhole path itself. This leads to shifts on either side of the Equation 5 as additional hops lead to additional transmission and processing delay. If we assume the wormhole path $W_1 \rightarrow W_2$ to be a multi-hop link with n hops and the same processing delay per node, then

$$\begin{aligned}\tau_e(\overrightarrow{A, W_1, ..., W_n, B}) = \tau_p(d_{A,W_1}) + \tau_p(d_{W_n,B}) + \tilde{\tau_p}(d_{W_1,W_n}) \\ + \tau_t(m) + \tau_t(m') + (n-1) \cdot \tilde{\tau_t}(m') + n \cdot \tau_{proc}(W_1) \quad (7)\end{aligned}$$

Hence, multi-hop wormholes need higher ω_{min} and are thus not of advantage for the attacker. Furthermore, we argue that even though surface communication is subject to a practical maximal communication range (reliable LoRa range ≈ 2 km [30], heavily depending e.g., on antenna gain, orientation, and position), this does not necessitate multiple hops to cover the entire underwater link longer than this restriction. Instead, an attacker can also increase the underwater distance of the two-node wormhole endpoints to their victims (d_{A,W_1} and $d_{W_2,B}$) to only cover a part of the underwater link that is just long enough, i.e., $\geq \omega_{min}$.

Proof. Assume the existence of a node B' on the link between A and B such that $d_{A,B'} < d_{A,B}$ and for which a two-node wormhole as described in Section 5 is feasible. Then, we can deduce:

$$\begin{aligned}\exists(W_1, W_2) : \tau_e(\overrightarrow{A, W_1, W_2, B'}) + \tau_t(m') < \tau_e(\overrightarrow{A, B'}) \\ \overset{d_{A,B'} < d_{A,B}}{\Longrightarrow} \tau_e(\overrightarrow{A, W_1, W_2, B'}) + \tau_t(m') + \tau_p(d_{B',B}) \\ < \tau_e(\overrightarrow{A, B'}) + \tau_p(d_{B',B}) \\ \Longleftrightarrow \tau_e(\overrightarrow{A, W_1, W_2, B}) + \tau_t(m') < \tau_e(\overrightarrow{A, B})\end{aligned}$$

□

On the other hand, also the underwater path $A \rightarrow B$ can be a multi-hop link with n hops via additional nodes $N_1, ..., N_{n-1}$. Assuming all nodes causing the same processing delay $\tau_{proc}(N)$:

$$\tau_e(\overrightarrow{A, N_1, ..., N_{n-1}, B}) \geq \tau_p(d_{A,B}) + n \cdot \tau_t(m) + (n-1) \cdot \tau_{proc}(N) \quad (8)$$

with = instead of ≥, if all N_i lie on the direct line between A and B. Otherwise, the distance $d(\overrightarrow{A, N_1, ..., N_{n-1}, B})$ increases, which consequently leads to a greater propagation delay.

As additional processing and transmission delay add up on the underwater path, routing over multiple hops introduces longer end-to-end delays, effectively reducing ω_{min}. This is highly relevant for a large subset of research modems that communicate with low data rates, resulting in very high τ_t, and a very small r_{max} such that $r_{max} < \omega_{min}$ (cf. Figure 7, solid line —). Thus, they would not be considered vulnerable to a hybrid wormhole when only considering single links. If these modems are, however, connected in a multi-hop series, ω_{min} is reduced and the underwater routing over n hops stretches r_{max} potentially to $r_{max} \cdot n$. As a consequence, hybrid wormholes remain a threat. This also holds for modems with large communication ranges that are deployed to communicate over distances shorter than ω_{min}. If we determine ω_{min} over one additional underwater hop (using Appendix, Equation 10 with $n = 2$), we find that for 84/144 modems, the communication ranges of in-series connected modems well overlap with the respective ω_{min} (cf. Figure 7, dashed line - -). Note that for visualization reasons, we plot Ω_{min}/n in Figure 7 instead of inserting each modem multiple times with $r_{max} \cdot n$. For two additional underwater hops (cf. Figure 7, dotted line ···), we see that 94% of the examined modems are potentially vulnerable to hybrid wormholes. This can be explained by a high overhead on the underwater path due to the sum of processing delays and the long JANUS preamble, even if the transmission delay decreases due to high data rates underwater. For 4-hop underwater paths, we find that hybrid wormhole attacks become feasible for all modem types as $\omega_{min} = 0$ (cf. Appendix, Equation 10). Thus, we conclude that variations of the wormhole attack are technically feasible for all of the modems analyzed and are especially feasible when underwater routing over multiple hops takes place.

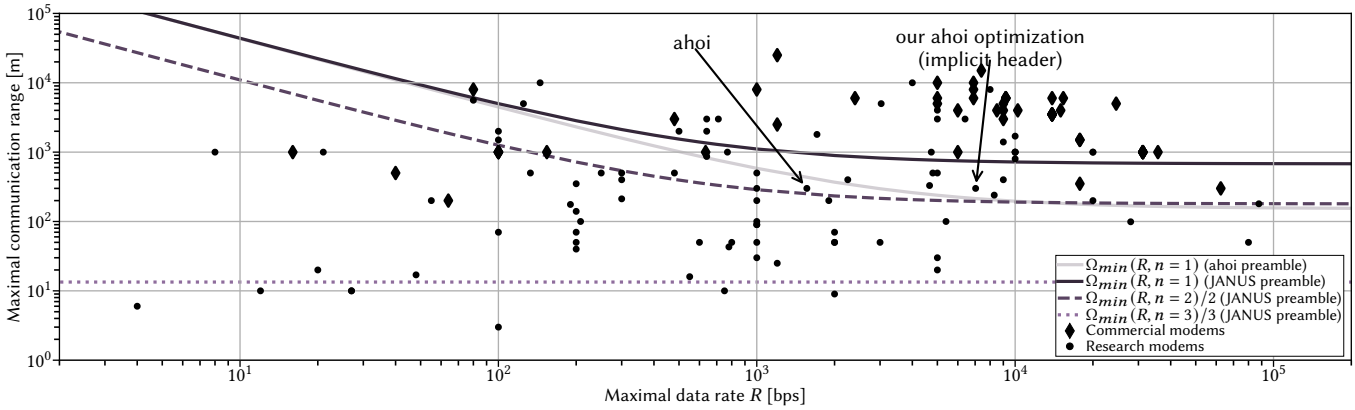


Figure 7: Commercial modems and research modems (cf. Appendix, Table 5) represented as a combination of their data rate R and r_{max} as well as the necessary ω_{min} for increasing data rates depending on the number of hops of the underwater link.

> **Insight** Solely shortening link range while bridging consistently long end-to-end underwater distances sets the stage for hybrid wormholes targeting multi-hop routes.

As analyzed in Section 3.3, parameters that facilitate hybrid wormholes are small message sizes $|m|$, high data rates R, and long distances $d_{A,B}$. This is further demonstrated in Figure 7 via the ahoi modem, which was lifted above ω_{min} (cf. solid line —) by virtually increasing its data rate (cf. Section 4.3). At the same time, in particular, the increase of data rates and the extension of communication ranges are major research goals for communication and networking. This brings us to our final insight.

> **Insight** Technical advancements, including higher data rates and longer communication ranges, will make UANs more vulnerable to wormholing in the future.

7 Impact and Countermeasures

Traditionally considered a routing attack in MANETs, wormholes can affect multiple network services. Dynamic underwater routing protocols such as SUN [42] and GUWMANET [12] are specifically vulnerable as their routing metrics are based on minimal hop count, maximal path signal-to-noise ratio, and shortest end-to-end delay, all of which would favor hybrid wormhole links as presented in this paper. This opens the door for a variety of post-attack behavior, even if packets are cryptographically encrypted and authenticated.

Existing wormhole detection approaches based on neighborhood monitoring [2] aim at detecting internal nodes that manipulate the routing protocol to establish themselves as wormhole endpoints. These countermeasures are not able to detect the existence of a hybrid wormhole link itself, but rather its impact. Approaches based on angle-of-arrivals of messages can reveal wormhole endpoints depending on their relative location [45] and, thus, could disclose the existence of W_2 in our scenario. Lastly, topology-based approaches such as those proposed by Wang et al. [43] can also detect hybrid wormhole links. However, this approach might come with high overhead due to the necessity of regular RTT measurements throughout the entire network. Another detection approach in our PoC would be the identification of an increased number of duplicate messages, since the original message m still reaches the recipient. However, attackers capable of jamming this message could evade detection.

Alternatively, based on the findings in Section 6.2, networks might also be configured preventively with wormhole-resilient parameters, e.g., reducing end-to-end distance of paths within the network given a specific hardware to use or extending packet lengths and adjusting transmission rates accordingly given a geographic area to be covered. However, this would come with serious limitations regarding communication properties, e.g., decreasing PDR, and might not be feasible in practice.

8 Conclusion

Even though the technical feasibility of hybrid wormholes within UANs constitutes a consensus across existing work, this paper finally provides a practical PoC, clearly confirming this widespread belief. Besides providing in-depth descriptions of a exemplary attack setup, we also abstract from the findings of this setup and provide a detailed theoretical analysis of which parameters influence the success of this attack. Furthermore, we analyze the risk potential for a large set of underwater modems in use. Our findings show that all modem types examined can fall victim to hybrid wormholes, calling for an increased focus on the practical implementation of wormhole countermeasures into existing underwater communications standards and protocols. The need to strengthen underwater surveillance due to the current geopolitical situation and the expected increase in physical attacks on (critical) underwater infrastructures makes this necessity more urgent than ever.

Ethical Considerations

The attack and all experiments conducted in this work were performed with specially procured research hardware. No operational networks were targeted. All procedures complied with applicable local and national regulations.

Acknowledgments

The authors would like to thank Prof. B.-C. Renner for his valuable support and technical expertise regarding the ahoi modems.

References

[1] Aquarian Hydrophones. 2025. AS-1 Hydrophone. https://www.aquarianaudio.com/as-1-hydrophone.html (last accessed: Dec 2025).

[2] M. R. Bharamagoudra and S. S. Manvi. 2017. Agent-based secure routing for underwater acoustic sensor networks. *Int. Journal of Communication Systems* 30, 13 (2017). doi:10.1002/dac.3281

[3] A. Boukerche and P. Sun. 2021. Design of Algorithms and Protocols for Underwater Acoustic Wireless Sensor Networks. *ACM Computing Surveys (CSUR)* 53, 6 (2021). doi:10.1145/3421763

[4] Filippo Campagnaro et al. 2020. Replay-Attack Countermeasures for Underwater Acoustic Networks. In *Global Oceans 2020: Singapore – U.S. Gulf Coast.* doi:10.1109/IEEECONF38699.2020.9389259

[5] F. Campagnaro et al. 2024. Affordable underwater acoustic modems and their application in everyday life: a complete overview. In *Proc. of WUWNet.* doi:10.1145/3631726.3631734

[6] B.-Y. Choi et al. 2004. Analysis of Point-To-Point Packet Delay In an Operational Network. In *Proc. of INFOCOM.* doi:10.1109/INFCOM.2004.1354590

[7] T. Dargahi, H. H.S. Javadi, and H. Shafiei. 2017. Securing Underwater Sensor Networks Against Routing Attacks. *Wireless Personal Communications* 96 (2017). doi:10.1007/s11277-017-4313-1

[8] R. Diamant et al. 2023. Secret Key Generation From Route Propagation Delays for Underwater Acoustic Networks. *IEEE Transactions on Information Forensics and Security* 18 (2023). doi:10.1109/TIFS.2023.3280040

[9] M. C. Domingo. 2011. Securing Underwater Wireless Communication Networks. *IEEE Wireless Communications* 18, 1 (2011). doi:10.1109/MWC.2011.5714022

[10] M. C. Domingo. 2012. An overview of the internet of underwater things. *Journal of Network and Computer Applications* 35, 6 (2012). doi:10.1016/j.jnca.2012.07.012

[11] V. Freitas. 2013. Parsifal. https://parsif.al/ (last accessed: Jan 2026).

[12] Michael Goetz and Ivor Nissen. 2012. GUWMANET – Multicast routing in Underwater Acoustic Networks. In *Proc. of MCC.*

[13] J. Ramírez Gómez et al. 2018. Implementation of a Wormhole Attack on Wireless Sensor Networks with XBee S2C Devices. In *Proc. of CCC.* doi:10.1007/978-3-319-98998-3_8

[14] G. Han et al. 2015. Secure Communication for Underwater Acoustic Sensor Networks. *IEEE Communications Magazine* 53, 8 (2015). doi:10.1109/MCOM.2015.7180508

[15] J. Heidemann et al. 2012. Underwater sensor networks: applications, advances and challenges. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 370, 1958 (2012). doi:10.1098/rsta.2011.0214

[16] L. Hu and D. Evans. 2004. Using Directional Antennas to Prevent Wormhole Attacks. In *Proc. of NDSS.*

[17] Y. Hu, A. Perrig, and D. B. Johnson. 2003. Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks. In *Proc. of INFOCOM.* doi:10.1109/INFCOM.2003.1209219

[18] David Inyangson et al. 2025. SoK: Security in the Inaudible World. In *Proc. of WiSec.* doi:10.1145/3734477.3734715

[19] I. Khalil, S. Bagchi, and N. B. Shroff. 2005. LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks. In *Proc. of DSN.* doi:10.1109/DSN.2005.58

[20] A. Khan et al. 2020. Modem design for underwater acoustic networks: Taxonomy, capabilities, challenges, applications and future trends. *Journal of Intelligent & Fuzzy Systems: Applications in Engineering and Technology* 39, 6 (2020). doi:10.3233/JIFS-189137

[21] B. Kitchenham and S. Charters. 2007. *Guidelines for performing Systematic Literature Reviews in Software Engineering.* Technical Report. EBSE-2007-01.

[22] J. Kong et al. 2005. Low-cost Attacks against Packet Delivery, Localization and Time Synchronization Services in Under-Water Sensor Networks. In *Proc. of WiSe.* doi:10.1145/1080793.1080808

[23] C. Lal et al. 2017. Toward the Development of Secure Underwater Acoustic Networks. *IEEE Journal of Oceanic Engineering* 42, 4 (2017). doi:10.1109/JOE.2017.2716599

[24] D. Magrin et al. 2020. Collaboration of LoRaWAN and Underwater Acoustic Communications in Sensor Data Collection Applications. In *Proc. of Global Oceans 2020: Singapore – U.S. Gulf Coast.* doi:10.1109/IEEECONF38699.2020.9389248

[25] MultiComP Pro. 2025. MultiComP Pro MP720025. https://multicomp-pro.com/ (last accessed: Dec 2025).

[26] A. Nadeem and M. P. Howarth. 2013. A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks. *IEEE Communications Surveys & Tutorials* 15, 4 (2013). doi:10.1109/SURV.2013.030713.00201

[27] V. Obado et al. 2012. Hidden Markov Model for Shortest Paths Testing to Detect a Wormhole Attack in a Localized Wireless Sensor Network. *Procedia Computer Science* 10 (2012). doi:10.1016/j.procs.2012.06.140

[28] A. Pal et al. 2022. Communication for Underwater Sensor Networks: A Comprehensive Summary. *ACM Transactions on Sensor Networks* 19, 1 (2022), 44 pages. doi:10.1145/3546827

[29] P. Perazzo et al. 2018. Implementation of a Wormhole Attack Against a RPL Network: Challenges and Effects. In *Proc. of WONS.* doi:10.23919/WONS.2018.8311669

[30] J. Petajajarvi et al. 2015. On the Coverage of LPWANs: Range Evaluation and Channel Attenuation Model for LoRa Technology. In *Proc. of ITST.* doi:10.1109/ITST.2015.7377400

[31] J. Potter et al. 2014. The JANUS Underwater Communications Standard. In *Proc. of UComms.* doi:10.1109/UComms.2014.7017134

[32] B.-C. Renner, J. Heitmann, and F. Steinmetz. 2020. ahoi: Inexpensive, Low-power Communication and Localization for Underwater Sensor Networks and μAUVs. *ACM Transactions on Sensor Networks (TOSN)* 16, 2 (2020). doi:10.1145/3376921

[33] K. Saeed et al. 2023. A Comprehensive Analysis of Security-Based Schemes in Underwater Wireless Sensor Networks. *Sustainability* 15, 9 (2023). doi:10.3390/su15097198

[34] G. Schneider et al. 2023. Design and Implementation of a Gateway Buoy for the Underwater-IoT. In *Proc. of MarCaS.* doi:10.1109/LCN58197.2023.10223369

[35] Semtech. 2025. LoRa Calculator. https://www.semtech.com/design-support/lora-calculator (last accessed: Feb 2026).

[36] Semtech. 2025. SX1261/SX1262 Datasheet. https://www.semtech.com/products/wireless-rf/lora-connect/sx1262 (last accessed: Dec 2025).

[37] S. Sendra et al. 2016. Underwater Acoustic Modems. *IEEE Sensors Journal* 16, 11 (2016). doi:10.1109/JSEN.2015.2434890

[38] F. Shi et al. 2011. Time-based Detection and address of Wormhole Attacks in Wireless Ad Hoc Networks. In *Proc. of TrustCom.* doi:10.1109/TrustCom.2011.240

[39] J. Sliwa et al. 2023. Lightweight quantum-safe cryptography in underwater scenarios. In *Proc. of MarCaS.* doi:10.1109/LCN58197.2023.10223321

[40] E. Souza et al. 2013. End-to-end Authentication in Under-Water Sensor Networks. In *Proc. of ISCC.* doi:10.1109/ISCC.2013.6754963

[41] Paul Staat et al. 2022. Analog Physical-Layer Relay Attacks with Application to Bluetooth and Phase-Based Ranging. In *Proc. of WiSec.* doi:10.1145/3507657.3528536

[42] Giovanni Toso et al. 2018. Revisiting Source Routing for Underwater Networking: The SUN Protocol. *IEEE Access* 6 (2018). doi:10.1109/ACCESS.2017.2779426

[43] W. Wang et al. 2008. Visualisation of wormholes in underwater sensor networks: a distributed approach. *Int. Journal of Security and Networks* 3, 1 (2008). doi:10.1504/IJSN.2008.016198

[44] Waveshare. 2025. Waveshare SX1262 868M. https://www.waveshare.com/wiki/SX1262_868M_LoRa_HAT (last accessed: Dec 2025).

[45] R. Zhang and Y. Zhang. 2010. Wormhole-Resilient Secure Neighbor Discovery in Underwater Acoustic Networks. In *Proc. of INFOCOM.* doi:10.1109/INFCOM.2010.5462093

[46] J. Zhou et al. 2012. Analysis and Countermeasure for Wormhole Attacks in Wireless Mesh Networks on a Real Testbed. In *Proc. of AINA.* doi:10.1109/AINA.2012.81

[47] M. Y. I. Zia et al. 2021. State-of-the-Art Underwater Acoustic Communication Modems: Classifications, Analyses and Design Challenges. *Wireless Personal Communications* 116, 2 (2021). doi:10.1007/s11277-020-07431-x

[48] M. Zuba. 2014. Connecting with Oceans Using Underwater Acoustic Networks. *XRDS: Crossroads, The ACM Magazine for Students* 20, 3 (2014). doi:10.1145/2590642

[49] M. Zuba et al. 2011. Short Paper: Launching Denial-of-Service Jamming Attacks in Underwater Sensor Networks. In *Proc. of WUWNet.* doi:10.1145/2076569.2076581

A Appendix

Determination of ω_{min}. The minimal wormhole distance for underwater single-hop links can be determined by:

$$\Omega_{min}(R) := \left(\tau_p(d_{A,W_1}) + \tau_p(d_{W_2,B}) + \left(\frac{|m|}{R} + \tau_t(\text{preamble})\right) + \left(\frac{|m'|}{R} + \tau_t(\text{preamble})\right) + \tilde{\tau}_t(m') + 2\cdot\ \tau_{proc}(W_1)\right)\cdot v_a \quad (9)$$

and generalized to multi-hop underwater links using:

$$\Omega_{min}(R,n) := \max\left(0, \left(\tau_p(d_{A,W_1}) + \tau_p(d_{W_2,B}) + \left(\frac{|m|}{R} + \tau_t(\text{preamble})\right) + \left(\frac{|m'|}{R} + \tau_t(\text{preamble})\right) + \tilde{\tau}_t(m') + 2\cdot\ \tau_{proc}(W_1) - (n-1)\cdot\left(\left(\frac{|m|}{R} + \tau_t(\text{preamble})\right) + \tau_{proc}(N)\right)\right)\cdot v_a\right) \quad (10)$$

Table 3: Overview of notation.

Symbol	Description
$N_i, i \in \mathbb{N}$	Network nodes
A, B	Source and destination node
$W_i, i \in \{1, 2\}$	Wormhole endpoints
m, m'	Message and copy of message m with size $\|m\|$
R	Transmission rate
v	Signal propagation speed (v_c EM, v_a acoustic)
d_{N_i,N_j}	(Physical) distance of the link between N_i and N_j
$\tau_e(\overrightarrow{N_1, ..., N_n})$	End-to-end-delay of the path $\overrightarrow{N_1, ..., N_n}$
$\tau_p(d_{N_i,N_j}) = \frac{d_{N_i,N_j}}{v}$	Propagation delay of the link between N_i and N_j
$\tau_t(m) = \frac{\|m\|}{R}$	Transmission delay of message m for a given R
τ_q	Queuing delay (ignored in our analysis)
τ_{proc}	Nodal processing delay (experimentally determined)
$\Delta t(m, m')$	Time difference between m's and m''s reception
b_0	Distance, such that $\tau_e(A, W_1, W_2, B) = \tau_e(A, B)$
r_{max}	Maximal communication range
ω_{min}	Minimal two-node wormhole distance
$\Omega_{min}(R, n)$	ω_{min} as a function of R and number n of hops

$\tilde{\tau}$ variants and $\tilde{r}_{max}$ refer their electromagnetic (EM) counterparts, i.e., the LoRa-based surface channel.

Table 4: Modem configuration during experiments.

Parameter	Value	Parameter	Value
Symbol duration T_s	1.28 ms	Receive Gain at M_1	0
Bits per Symbol C	6 bits	Receive Gain at B	18
Spreading Factor S	3	Transmit Gain at A, M_2	18
Packet Length	1 B	Automatic Gain Control	OFF

All parameter variables are named according to [32].

Table 5: Specifications of 144 acoustic underwater modems.

Commercial modems (model name)	Data rate [bps]	Range [km]	Product [bps × m]
Waterlinked M64	64	0.2	
Waterlinked M16	16	1	
Tritech Micron Data Modem	40	0.5	
Blueprint SubSea SeaTrac {X150, X110, X010}	100	1	
Desert Star SAM-1	154	0.1	
DiveNET Microlink	634	1	
DiveNET: Sealink {C,S}	80	8	
DSP AquaComm	480	3	
DiveNET Sealink R	1,200	2.5	
Kongsberg cNode MiniS 34-180	6,000	1	
LinkQuest UWM1000	17,800	0.35	
DSPComm Aquacomm Gen2	1,000	8	
Teledyne Benthos Atm9xx	2,400	6	
EvoLogics S2CM HS	625	0.3	
Kongsberg cNode MiniS 34-40V	6,000	4	
LinkQuest UWM3000	5,000	5	
LinkQuest {UWM2000H, UM2000}	17,800	1.5	
Sonardyne Modem 6 Mini	9,000	3	
LinkQuest UWM3000H	5,000	6	
GPM 3000 Acoustic Modem	1,200	25	
EvoLogics {S2CR 48/78USBL, S2CR 42/65USBL, S2CM 48/78, S2CM 42/65, S2CR 42/65}	31,200	1	
LinkQuest UWM4000	8,500	4	
LinkQuest UWM2200	35,700	1	
Sonardyne Modem 6 Sub-Mini	9,000	4	
Popoto low-power modem	10,240	4	
EvoLogics S2CR 7/17USBL	6,900	6	
Sonardyne Modem 6 Standard	9,000	5	
EvoLogics {S2CR 18/34, S2CR 18/34 DUSBL, S2CR 18/34 HUSBL, S2CM 18/34 USBL, S2CR 18/34 D}	13,900	3.5	
LinkQuest UWM10000	5,000	10	
EvoLogics S2CR {12/24USBL, 15/27USBL, 15/27}	9,200	6	
EvoLogics S2CR 7/17WUSBL	6,900	8	
Subnero M25M	15,000	4	
EvoLogics S2CR 7/17DUSBL	6,900	10	
EvoLogics S2CM 15/27	13,900	6	
Teledyne Benthos Atm9xx	15,360	6	
Sercel MATS 3G 12 kHz	7,400	15	
Sercel MATS 3G 34 kHz	24,600	5	
Research Modems (title of publication, abbreviated with clickable web links)	**Data rate [bps]**	**Range [km]**	**Product [bps × m]**
Digital acoustic modem design for narrowband UW vehicle comm.	4	0.006	
Software Acoustic Modems for Short Range Mote-based USNs	12	0.01	
Dolphin Sounds-Inspired Covert UAC and Micro-Modem	27	0.01	
Design of a Reconfigurable Acoustic Modem for USNs	27	0.01	
An Ultrasonic Sensor Based LP Ac. Modem for UW Comm.in UWSNs	100	0.003	
A Compact Acoustic Comm. Module for Remote Control Underwater	20	0..02	
Software Modems for Underwater Sensor Networks	48	0.017	
Design and impl. of a low-cost and small-size UW acoustic modem	100	0.07	
An off-line software modem for UAC and its field evaluation results	750	0.01	
Implementation of a micro-modem for UWSNs	200	0.04	
An Omni-directional Underwater Acoustic Modem Based on Cortex-M3	200	0.04	
Impl. of multi-hop bidir. comm. link w/ time sync. on test bed of UASN	8	1	
A physical layer implementation on reconfigurable UW acoustic modem	550	0.016	
Software Defined Modem for Interconnection of Terrestrial and UAN	200	0.05	
Evaluating Acoustic Comm. Perf. of Micro AUV in Confined Space	55	0.2	
Design and Impl. of an Omni-Dir. UW Ac. Micro-Modem	200	0.07	
Low-Power Low-Cost Acoustic Underwater Modem	2,000	0.009	
The Design and Impl. of a UW Multimode Acoustic Modem for AUVs	208	0.1	
Underwater wireless inpipe communications system	21	1	
Proteus II: Design and eval. of an integrated power-efficient UW SN	200	0.14	
Implementation of a Low-Power Acoustic Modem for UWSNs	1,000	0.03	
Hydroacoustic modem for autonomous underwater vehicle	1,200	0.025	
Design and eval. of a low-cost, DIY-inspired, UW platform	600	0.05	
First in-field exp. with a UW ac. modem supporting the JANUS standard	190	0.176	
Poster: Affordable Acoustic Modem for Small-Sized AUVs	780	0.043	
Acoustic modem for micro AUVs: design and practical evaluation	800	0.05	
Low-Power Microcontroller-based Ac. Modem for UW Robot Comm.	1,000	0.05	
Implementation of a high reliable chirp underwater acoustic modem	300	0.212	
An underwater acoustic telemetry modem for eco-sensing	133	0.5	
Design of a Low-Cost Underwater Acoustic Modem	200	0.35	
Coralcon: An open source low-cost modem for UW IoT applications	1,000	0.09	
Utilizing JANUS for Very High Frequency Underwater Acoustic Modem	1,000	0.09	
Demo: Run-time Reconfigurable Underwater Broadband Modem	2,000	0.05	
A low cost and high efficient acoustic modem for USNs	1,000	0.1	
A First-of-its-kind Low Size, Weight, Power Run-Time Reconf. Modem	2,000	0.05	
Poster abstract: A point-to-multipoint acoustic modem for UWSNs	5,000	0.02	
AquaNodes: An underwater sensor network	300	0.4	
Low cost adaptive UW acoustic modem for the Black Sea environment	250	0.5	
Packet-based ranging with an LP low-cost ac. modem for micro AUVs	2,000	0.07	
Robot Control Using an Underwater Acoustic Modem	5,000	0.03	
Rake Receiver with Interference Cancellation for a UW ac. modem	3,000	0.05	
Underwater Acoustic Micromodem for Underwater Internet of Things	300	0.5	
Dev. of the "Seatrac" miniature ac. modem and USBL positioning units	100	1.5	
Design of a low-cost, UW ac. modem for short-range sensor networks	100	2	
An Ultra-LP and Flex. Ac. Modem Design to Dev. Energy-Effi. USNs	1,000	0.2	
Character. of UW ac. modem perf. for real-time horizontal data trans.	480	0.5	
Underwater Acoustic Modem for a MOrphing Distributed AUV (MODA)	1,000	0.3	
Designing an adaptive acoustic modem for underwater sensor networks	1,900	0.2	
Acoustic communications under shallow shore-fast Arctic Ice	80	5.6	
ahoi: Inexpensive, Low-power Communication and Localization for Underwater Sensor Networks and μAUVs	1,562.5	0.3	
Design and impl. of a bidir. ac. micro-modem for UW comm. systems	1,000	0.5	
Eff. UW comm. modem for harsh and highly non-stat. chan. conditions	5,400	0.1	
UW Positioning System Based on Drifting Buoys and Acoustic Modems	640	0.866	
A General Embedded UAC System Based on Advance STM32	125	5	
DSP based real-time single carrier UACs using freq. dom. turbo equal.	770	1	
SeaModem: A low-cost UW acoustic modem for shallow water comm.	22,500	0.4	
UAN node design and anechoic pool network exp. with five nodes	500	2	
Ultra-LC and ultra-LP, min. ac. modems using spread-spectrum tech.	640	2	
Spread-Spectrum Techniques for Bio-Friendly UACs	145	10	
Matching pursuits channel estimation for an UW ac. OFDM modem	4,664	0.33	
Reconfigurable underwater acoustic modem based on chirp modulation	640	3	
UW Ac. Modems (S2CR Series) for Sync. of UAN Clocks	8,300	0.24	
Full-duplex, multi-user and parameter reconfigurable UAC modem	710	3	
Research and dev. of an acoustic modem for UW bio-mimetic fish robots	4,800	0.5	
Micro-Modem for Short-Range UW Mobile Comm. Systems	5,000	0.5	
Design of A Software-def. UW Ac. Modem with Real-time PHY Adap.	28,000	0.099	
Implementation of an UW acoustic modem with network capability	1,710	1.8	
The UNET-2 modem – An extensible tool for UW networking research	9,000	0.4	
A high data-rate, software-defined underwater acoustic modem	80,000	50	
A Channel-Aware Adaptive Modem for UACs	2,000	0.2	
Research and Development of a Highly Reconfig. OFDM MODEM	4,737	1	
A robust OFDM modem for underwater acoustic communications	10,000	0.8	
Using multi-freq. modul. in a modem for trans. of near-realtime video	10,000	1	
Underwater acoustic modem using multicarrier modulation	10,000	1	
Dev. of a Low-Cost Reconfigurable UW Ac. Modem for AUV Apps.	10,000	1	
Towards a video-cap. wireless UW modem: Doppler tol. broadband	1,000,000	0.012	
Dev. of a 1 Mbps low power acoustic modem for UW comms.	1,000,000	0.012	
Design and Impl. of Real-Time UW Ac. Multimedia Trans. Modem	9,000	1.4	
MIMO OFDM Underwater Acoustic Communications	5,000	3	
HEU OFDM-modem for UAC and Networking	3,030	5	
HERMES – A High Bit-Rate UW Ac. Modem Oper. at High Freq.	87,768	1.8	
High data rate acoustic modem for underwater applications	1,000,000	0.016	
A Real-Time Coded OFDM Ac. Modem in Very Shallow UW Comms.	10,000	1.7	
A Modem Design for UW Acoustic Networking in the High North	96	200	
DSP based receiver implementation for OFDM acoustic modems	6,400	3	
The design and experiment of a software-defined ac. modem for USN	20,000	1	
Underwater acoustic modem with streaming video capabilities	1,000,000	0.02	
A Janus compatible software-def. UW ac. MIMO modem	20,000	1	
A compact underwater acoustic modem	5,000	4.025	
High data rates in the high frequency acoustic channel	380,000	0.08	
Open-water, real-time, high data-rate, UW acoustic modem testing	380,000	0.1	
Impl. of UW acoustic modem based on the OMAP-L138 processor	4,000	10	
A High-Rate SW-Def. UW Ac. Modem With Real-Time Adapt. Cap.	260,000	0.2	
Modularized real-time comm. modem design based on SDR of UAN	8,000	8	
Experimental results with HF UW ac. modem for high bandwidth apps.	1,000,000	0.1	

Modems/publications are sorted by the *product* of their data rates and communication ranges.