Quantum Key Distribution for Secure Encryption in Underwater Networks

Jacopo Lazzarin, Filippo Campagnaro, Matteo Padovan, Edoardo Rossi, Ilektra Karakosta-Amarantidou,
Francesco Picciariello, Francesco Vedovato, Giuseppe Vallone, Paolo Villoresi, Michele Zorzi

Department of Information Engineering, University of Padova, via Gradenigo 6/B, 35131 Padova, Italy

***Abstract*—Security is a crucial aspect of underwater acoustic networks, that are often used in mission critical scenarios, such as coastal surveillance, rapid environmental assessment and mine countermeasure applications. The broadcast nature of the acoustic channel makes it vulnerable to a variety of attacks, such as spoofing, men-in-the-middle and jamming. Moreover, the lack of a standardized key distribution system makes data confidentiality challenging. In this paper we investigate the use of quantum key distribution (QKD) in underwater networks, in order to ensure confidentiality and integrity of the communication.**

While in the terrestrial domain the use of the one-time-pad protocol (requiring the key length to be equal to the message length) is limited by the low rate of the QKD rate compared to the bitrate of radio transmissions, in the underwater domain the limited bandwidth of the acoustic channel makes QKD a valid approach also for the one-time-pad protocol. The system is tested both with an emulator and a field test: results show that QKD can be a valuable system to secure underwater acoustic networks.

***Index Terms*—Quantum key distribution, underwater acoustic networks, DESERT Underwater.**

I. Introduction and State of the Art

Underwater Acoustic Networks (UANs) have been recognized as an enabling technology for various applications in the maritime domain, including prediction of natural disasters, monitoring and maintenance of Oil & Gas pipelines and offshore infrastructures, water quality assessment in bathing and aquaculture sites, coastal erosion monitoring, and military applications like coastal surveillance [1]. The broadcast wireless nature of the acoustic medium makes UANs vulnerable to spoofing and Denial Of Service (DoS) attacks. Moreover, UANs are often used in mission-critical scenarios (such as coastal surveillance), hence a DoS attack can cause severe damages not only to the equipment, but also to the safety of the people. Nevertheless, security aspects of UANs started to be addressed only a few years ago, and are now a hot topic in the research community [2].

The challenges imposed by the underwater acoustic channel, characterized by low bandwidth, long propagation delay, low bitrate and poor performance in case of shallow water transmissions and in the presence of shipping and wind noise [3], make the use of security mechanisms used in wireless terrestrial networks impractical. In fact, DoS attacks can be performed at different levels of the protocol stack. Jamming attacks consist of a malicious node transmitting a strong signal that causes interference at the receiver, preventing the correct reception of the packets. While in terrestrial wireless networks solutions based on frequency hopping are often applied, the small bandwidth available in the underwater channel makes solutions based on packet-level coding and randomizing the packet transmission times the only ones applicable to UANs scenarios (e.g., in [4] randomization parameters and strength of the coding scheme are optimally selected with Game Theory). The lack of standardization of the protocol stack does not only cause interoperability issues, but is also a source of vulnerabilities that can be exploited by replay, sinkhole, sibyl and other resource exhaustion attacks [5]. In fact, research groups and companies often develop their own Medium Access Control (MAC) and routing algorithms by themselves, and, although performing an enormous effort ensuring that the network is fully operational in normal working conditions, do not have enough resources to verify all possible security aspects of the developed protocols. In addition to DoS attacks, there are also important vulnerabilities on the integrity and the confidentiality of the data. Specifically, the lack of a key-distribution infrastructure and of standards for security in UANs make the deployment of a secure underwater network even more difficult. Recent studies propose a peer-to-peer key generation system that uses the estimated channel impairments as a shared secret to generate the keys [6], [7]. While this method works quite well in a controlled environment, the time varying nature of the acoustic channel makes the channel non-reciprocal, hence the failure rate of this mechanism is quite high, making it not directly applicable to date.

The recent advances in non-acoustic underwater communications, including magneto-inductive, radio frequency, and optical [1], enable the possibility to establish short range broadband links. In the case of optical communication, the use of a collimated optical beam from transmitter to receiver would

F. Campagnaro, corresponding author (email: campagn1@dei.unipd.it). This work was supported in part by the FSE REACT EU, PON Research and Innovation 2014-2020 (DM 1062/2021). I. K.-Amarantidou acknowledges funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 956071 AppQInfo - Applications And Hardware For Photonic Quantum Information Processing. E. Rossi acknowledges funding from the European Union's PON Ricerca e Innovazione 2014-2020 Azioni IV.4 "Dottorati e contratti di ricerca su tematiche dell'innovazione" e Azione IV.5 "Dottorati su tematiche Green." — DM 1061/2021 (project ID: DOT1319501-4). A special thanks to F. Bragato, R. Francescon and A. Montanari for the help with the underwater network deployment.

prevent eavesdroppers from overhearing the communication. On the other hand, water has strong intrinsic absorption, with a minimum that is spectrally varying with the water condition. Moreover, the crucial procedure of alignment of the receiver with the transmitter is harder underwater than in free space, and mechanisms akin to those used to align quantum signals from Earth to satellites, between satellites [8], or between airborne vehicles [9], should be employed. Nevertheless, long range communication can be performed only with acoustic modems, making underwater optical communication only suitable in the presence of mobile nodes, such as Autonomous Underwater Vehicles (AUVs), that can use optical links as soon as they approach a submerged node, acting as mules in data retrieval or docking operations. Since optical communication alone is insufficient in most maritime scenarios, such as Intelligence gathering, Surveillance & Reconnaissance (ISR), Mine Counter-Measures (MCM), and Rapid Environmental Assessment (REA) [10], it is mostly used together with acoustic communication, hence forming an underwater multimodal network [11]. These types of networks, however, are not immune to eavesdropping and spoofing attacks, and possible countermeasures should be analyzed.

The idea at the core of this work is to equip the underwater communication with keys generated via Quantum Key Distribution (QKD) [12]. QKD is a quantum communication protocol allowing two parties to share the same key, that can then be used for cryptographic applications, as secure communication via One-Time-Pad (OTP) [13] or to feed Advance Encryption Standard (AES) [14] modules which require the refresh of a 128- or 256-bit long symmetric key [15]. QKD is already commercially available for fiber communication links [16], and has been demonstrated also along free-space channels [17], [18] and satellite-to-ground links [19]. It is worth noticing that there are also recent studies in the literature investigating the possibility to realize quantum communication and QKD exploiting different encodings with underwater optical communication, as in [20]–[22], up to a distance of 55 m.

The main contribution of this work is to show a demonstration result of the combination of underwater communication with free-space QKD. In our scenario, depicted in Figure 1, we assume a network composed of AUVs, Autonomous Surface Vessels (ASVs), buoys, bottom nodes and ships. All the nodes can exchange data with underwater acoustic or optical modems, while surface nodes, including ASVs and buoys, can also be equipped with quantum communication terminals for QKD and, in principle, be able to deploy the keys to the other nodes via directive optical communication links. A trusted AUVs sent from the main ships can even be used to deploy or update the key to nodes that are not in optical range with surface nodes.

This paper is structured as follows. Section II describes the system architecture, including the QKD system, the underwater network and the software interface between the two components. Section III proves the effectiveness of the system in an emulated environment, while the results of the field test demonstration are discussed in Section IV. Section V, finally, concludes the paper.

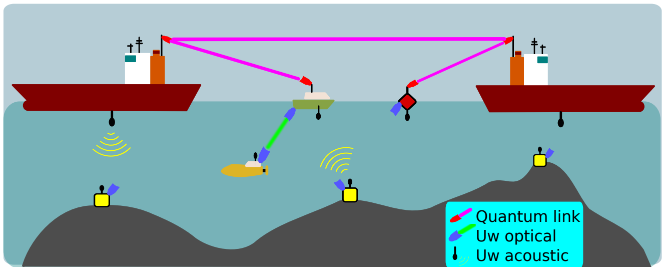


Fig. 1. Scenario of interest, where ships deploy quantum keys in surface and mobile nodes.

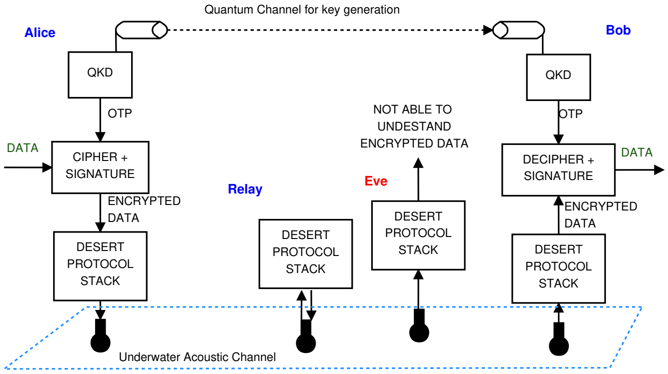


Fig. 2. System Architecture, where Alice and Bob exchange a secure key with QKD and then cipher and decipher the data before transmitting it through the acoustic network.

II. System Architecture

In this section we present the system architecture (depicted in Figure 2) developed to deploy a secure UAN: the complete system is composed of an above water QKD mechanism (Section II-A), an underwater network part (Section II-B), and the interface between the two components, also responsible of ciphering the data with the secure key (Section II-C). With this structure, data can be securely transmitted through the acoustic network as only the transmitter (Alice) and the receiver (Bob) can decipher the messages. Other nodes in the network (e.g., a relay) can receive and forward the packets along the correct route, but cannot decipher the original data.

A. Quantum Key Distribution Framework

QKD enables the creation of a shared secret bit-string between distant parties, typically referred to as Alice and Bob, which communicate through both a quantum channel and a classical authenticated channel. The security of this process relies on the principles of quantum mechanics, which prevent the faithful copying of an unknown quantum state. Moreover, any attempt by an eavesdropper, named Eve, to get information about the exchanged quantum states can be revealed by monitoring the noise in the quantum channel, the so-called Quantum Bit Error Rate (QBER). If the QBER exceeds a certain threshold, indicating potential eavesdropping, the protocol is aborted. Otherwise, a partially correct and partially secret key, named the raw-key, is established and shared between Alice and Bob. To enhance privacy and correctness, classical postprocessing algorithms, such as information reconciliation and privacy amplification, are used on the raw key, leading to the final secure key [12], [23].

The QKD system closely resembles the one outlined in [24], implementing the 3-state efficient BB84 protocol [25] with polarization modulation and the 1-decoy technique [26]. The transmitter consists mainly of a 1550 nm laser emitting pulses at a repetition rate of 50 MHz, an intensity modulator for adjusting the mean photon number required for decoys, and a polarization modulator based on the iPOGNAC scheme [27]. Subsequently, the pulses are attenuated below the single-photon level using a variable optical attenuator before entering the quantum channel. The electronic components are composed of a System-on-a-Chip (SoC) with an FPGA and CPU, with a detailed architecture description available in [28].

Post-generation, the attenuated laser pulses are directed to the free-space system, which has already been successfully used in the past for free-space QKD demonstrations in urban environments and is described in greater detail in [29], [30]. It consists of two compact telescope terminals and a Pointing, Acquisition and Tracking (PAT) system at the receiver, necessary to ensure the coupling of the incoming laser beam into a Single-Mode Fiber (SMF).

The free-space transmitter is equipped with a terminated SMF fiber channel/physical contact (FC/PC) adapter, which is mounted on a linear stage and positioned in the back focus of a 2-inch (50.8 mm) lens. This arrangement aims to generate a collimated beam with a waist of approximately 25 mm. In addition, two extra beacon lasers—one operating at 980 nm and the other at 1545 nm—are merged into the same SMF using wavelength multiplexing. The fine-alignment process between the free-space transmitter and receiver terminals takes advantage of these two beacons and is implemented on the receiver side.

The presence of an SMF at the receiver is crucial as it serves as a spatial filter enabling operation in daylight conditions. However, incorporating it in the system comes with certain constraints on the design of the receiver terminal [31]. Adhering to these limitations, the free-space receiver is optimized for a maximum working distance of 1 km. It includes a 6× beam reducer with a 2-inch aperture, followed by a fast-steering mirror (FSM), and a dichroic mirror (DM) for separating the 980 nm beam from those in the telecom C-band (QKD signal and 1545 nm-beacon). To address angle-of-arrival (AoA) fluctuations in the incoming beam, the FSM is employed, utilizing feedback from a position-sensitive detector (PSD) positioned on the focal plane of a 300 mm lens. Meanwhile, the C-band beams are directed to the FC/PC-terminated SMF.

After the fiber coupling, the receiver employs a time-multiplexing scheme for state decoding, introducing an additional 3 dB of losses but significantly enhancing system compactness and cost-effectiveness. The system features only one InGaAs/InP single-photon avalanche diode (SPAD), specifically a PDM-IR from Micro Photon Devices S.r.l., providing 15% quantum efficiency. Time tags corresponding to photon arrivals are recorded by a quTAU time-to-digital converter from qutools GmbH and transmitted to a computer for subsequent data processing. To further streamline architecture requirements, the QKD system utilises the Qubit4Sync algorithm [32] for time synchronisation between the transmitter and the receiver, eliminating the need for a dedicated system to distribute the clock reference.

Ultimately, a custom QKD key manager application is deployed to oversee the management of shared secure keys and distribute the identical set of keys to the relevant applications at the communication endpoints. The APIs are specified in accordance with the ETSI GS QKD 004.

B. Underwater Network Protocol Stack

The DESERT Underwater Framework [33] is a complete suite of protocols for underwater networks. This open-source tool can be used to build the desired network protocol stack and test it in simulation, emulation and sea trials. In fact, in addition to the various models available to simulate the physical propagation in different sea conditions, real modems can be plugged to DESERT in place of the simulated physical layer, hence the same network configuration tested in simulation can be used in real networks. DESERT can also be used with modem emulators, in order to verify the correct operation of the network before the sea trial. Following a layered structure similar to the ISO/OSI standard, its protocol stack is usually composed of five main components, namely:

- the application layer(s), generating the data;
- the transport layer (usually UDP-like), that forwards the received packets to the correct application;
- the network layer, that sets the path followed by the packets to reach the proper destination;
- the MAC layer, that orchestrates the channel access and ensures that the packet reaches the next hop on the route;
- the physical layer, that sets the rate, the bandwidth, modulation and coding schemes, etc.

A simulated channel is then used to compute the propagation delay between the transmitter and the other nodes in the network. At the physical layer, then, the bit error rate is computed, observing path loss, noise and interference. In simulation, an event-based scheduler is used, and the time requested for a simulation run depends on the number of events and not on the simulated time. On the other hand, for the sea experiment a realtime event scheduler is used: this scheduler is synchronized with the clock of the computing unit (e.g., a laptop or a pc on-board) used in the sea test. Given that in this paper we focus on emulations and field experiments, some additional modules are introduced to convert the packets generated by the network simulator to actual packets transmitted by real modems. Specifically, the final DESERT stack used in the underwater network is structured as follows:

- Application layer: `UwApplication` is used to transmit real data generated from an external application (connected via socket to `UwApplication`). The data is encapsulated in packets with a fixed size and generated with a fixed period.

- Transport layer: `UwUDP`, a UDP-like transport layer that delivers the packet to the proper process at the destination with a best effort policy.
- Network layer: `UwStaticRouting`, where the routing table of every node is known at deployment time.
- MAC layer: `UwCSMA-Aloha`, a carrier sensing MAC layer inspired by Carrier Sense Multiple Access (CSMA).
- Adaptation layer: `UwAL` is used to serialize and deserialize all the packets, converting them in a format that can be transmitted in the real channel.
- Physical layer: `UwEvologicsS2C`, software drivers that interface DESERT with the Evologics S2C modems.

C. Secure UANs

The security aspects of the communication are implemented through a Python script at the application level, in order to ensure confidentiality and integrity of the data being sent. Confidentiality is obtained by using OTP, a well known block cipher that under the Claude Shannon conditions [34] can achieve perfect secrecy. Message integrity, instead, is reached by means of a checksum, described in [35], that is ciphered and appended after the end of the payload of a packet.

The script works in two phases that mimics our scenario of interest, presented as follows.

1) An initial key setup phase where each application connects with its respective QKD key manager entity and obtains one OTP.
2) Once every application has obtained the required key, it detaches itself from the QKD infrastructure network, connects to DESERT Underwater and begins transmission or reception activities.

We recall that perfect secrecy can be obtained with OTP as long as the same portion of the key is used to cipher the data being sent only once. In our scenario the nature of the communication between the underwater nodes is characterized by messages of fixed size and a best effort policy for packet delivery. Specifically, given that the underwater acoustic channel often has a high Packet Error Rate (PER), a 16-bit index i_{otp} indicating which block of the OTP is used to cipher the packet payload is used. Although i_{otp} is sent unciphered and can in principle be modified by a malicious forwarder, the 16-bit checksum inserted at the end of the payload and then encrypted before the transmission is computed using also i_{otp} in order to ensure data integrity. The structure of the application packet is summarized in Figure 3.

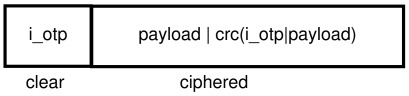


Fig. 3. Application packet structure.

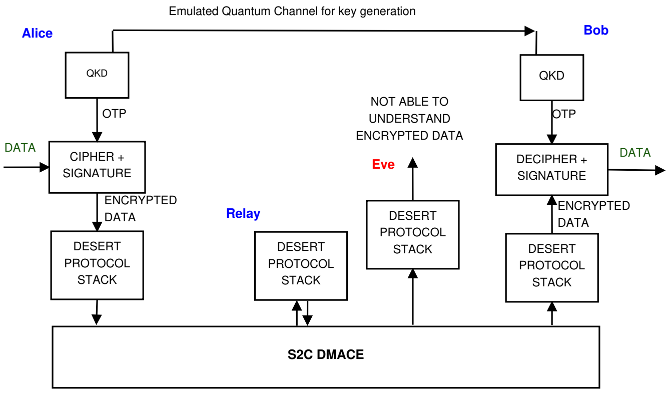


Fig. 4. System Architecture with emulated quantum key distribution and emulated acoustic modems.

III. Emulation Results

In this section, we test the secure architecture presented in Section II using an acoustic modem emulator. The Evologics S2C acoustic modems come with an emulator called S2C DMACE [36], provided by the manufacturer for testing all software components before actual deployment. We aim to simulate an underwater channel with two pairs of nodes communicating. Each pair has a pre-shared cryptographic key, mimicking the keys that will be generated by the QKD devices in the field test. The system setup, including pre-shared QKD keys and emulated acoustic modems, is shown in Figure 4.

A. Scenario and Settings

In the emulated scenario, depicted in Figure 5, we assume two ships to first exchange one OTP for each data stream (phase 1). By definition, each OTP shall be as long as the data that will be transmitted by the underwater nodes. In this use-case scenario, Alice (A) and Bob (B) are located on ship 1, while Carol (C) and Dave (D) on ship 2: after phase 1 terminates, A and C will share a common OTP, named `OTP_AC`, to exchange secure data between each other, while B and D will share the key `OTP_BD`. Then, in phase 2, the two ships will deploy the nodes under water. After deployment, A and B can transmit secure data to C and D, respectively. Therefore, even if Eve (E), a potential eavesdropper, tries to overhear the channel, they will not be able to get the original content transmitted by A and C.

B. Results

The emulation experiments allowed to test each component of the system architecture, as well as to test our scenario of interest in a controlled environment. The final emulation was executed on a desktop PC connected to DMACE, with one instance of DESERT and one ciphered application running for each node in the scenario. All applications were connected to the same QKD emulator, that distributed pregenerated keys to each node. Each application was configured to send 100 packets with 20 B of payload each, for a total of 2200 B ciphered with OTP sent in each communication stream.

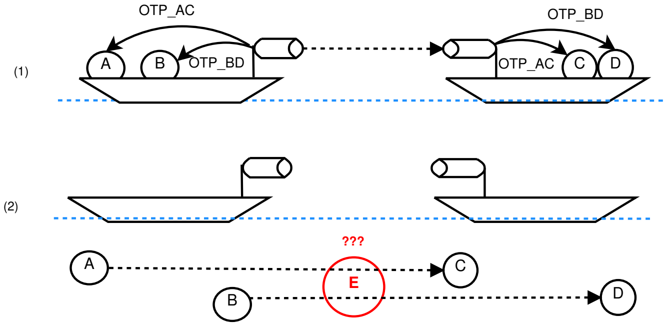
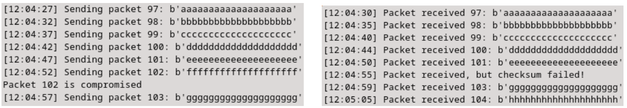


Fig. 5. The two phases of the emulated scenario, with QKD performed in phase 1 (1) and secure data exchange between submerged nodes in phase 2 (2), where nodes A and B transmit secure data to C and D, while E cannot understand the data as it lacks the key.



```
[12:04:27] Sending packet 97: b'aaaaaaaaaaaaaaaaaaaa'
[12:04:32] Sending packet 98: b'bbbbbbbbbbbbbbbbbbbb'
[12:04:37] Sending packet 99: b'cccccccccccccccccccc'
[12:04:42] Sending packet 100: b'dddddddddddddddddddd'
[12:04:47] Sending packet 101: b'eeeeeeeeeeeeeeeeeeee'
[12:04:52] Sending packet 102: b'ffffffffffffffffffff'
Packet 102 is compromised
[12:04:57] Sending packet 103: b'gggggggggggggggggggg'
```

(a) Transmitter's log.

```
[12:04:30] Packet received 97: b'aaaaaaaaaaaaaaaaaaaa'
[12:04:35] Packet received 98: b'bbbbbbbbbbbbbbbbbbbb'
[12:04:40] Packet received 99: b'cccccccccccccccccccc'
[12:04:44] Packet received 100: b'dddddddddddddddddddd'
[12:04:50] Packet received 101: b'eeeeeeeeeeeeeeeeeeee'
[12:04:55] Packet received, but checksum failed!
[12:04:59] Packet received 103: b'gggggggggggggggggggg'
[12:05:05] Packet received 104: b'hhhhhhhhhhhhhhhhhhhh'
```

(b) Receiver's log.

Fig. 6. Communication sample between two nodes. Packet 102's corruption is detected at the receiver's side.

To test the correctness of the checksum check algorithm, we decided to modify the behavior of the transmitter by making it corrupt a portion of some packets selected according to a uniform random variable. Specifically, a packet to be transmitted was corrupted with a probability of 10%: this allowed us to mimic the presence of an attacker corrupting packets without the need to set up a third malicious node. In Figure 6 it is possible to see a meaningful extract of the communication: the received data is successfully deciphered by the application with the exception of the packet corrupted by the transmitter, which failed the checksum as expected.

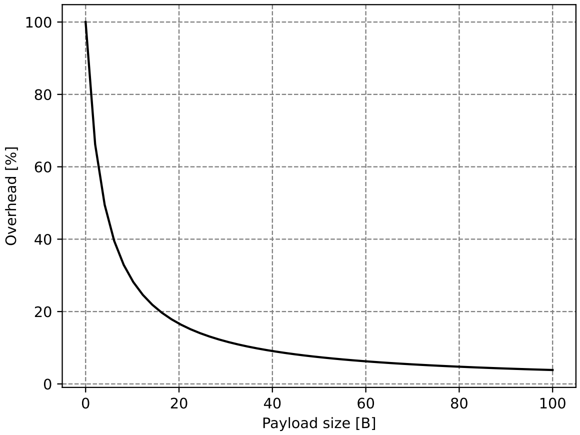


Fig. 7. Relationship between payload size and overhead.

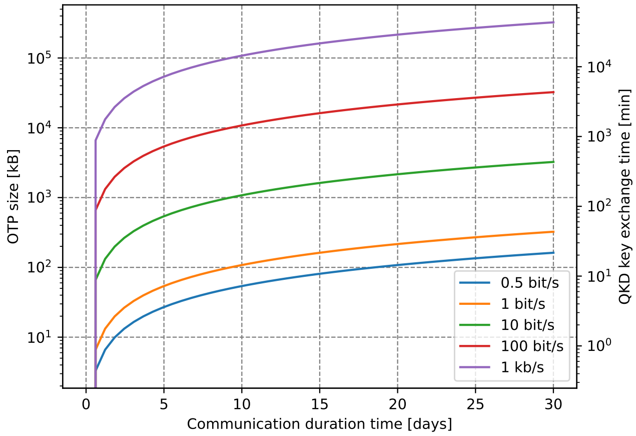


Fig. 8. Size of OTP key and its generation time for supporting a mission deployment of a certain duration with different traffic generation rates.

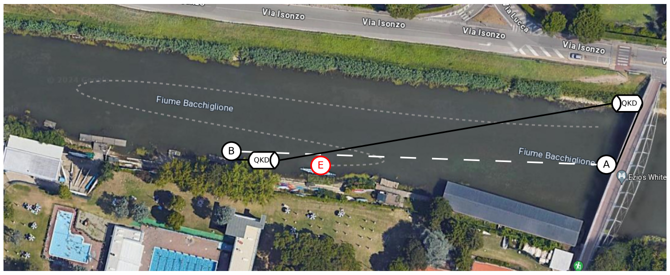


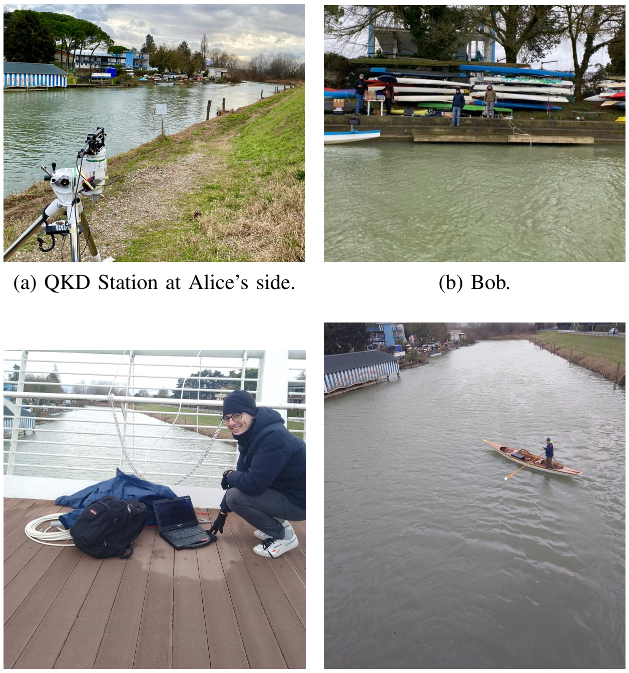
Fig. 9. Deployment area in the Bacchiglione River, Padova, Italy.

As shown in Figure 7, increasing the payload size is useful in reducing the impact of the application header overhead, but with the consideration that the final packet size, that includes also the DESERT header, does not surpass the 64 B maximum size of the Evologics' instant messages.

Finally, Figure 8 depicts the size of the OTP key to support up to one month of mission duration, considering different traffic generation rate of the acoustic nodes, assuming that QKD has an average generation rate of 1 kbit/s. While in terrestrial networks the traffic rate usually prevents OTP from being used, the nature of underwater networks, where the packet generation rate is typically very low, OTP can still be used in some practical scenarios.

IV. River Test

After the emulation, the complete system was deployed in a river test, to prove that the presented concept works also in a real environment. While in emulation we tested a more complex network, in the river test we deployed only two underwater nodes and one eavesdropper, as this was the minimal setup required to test QKD and prove that the proposed paradigm works in a real deployment. The rest of this section is structured as follows: Section IV-A presents the deployment setup, while the results are discussed in Section IV-B.



(a) QKD Station at Alice's side.

(b) Bob.

(c) Alice.

(d) Eve.

Fig. 10. Some pictures of the deployment in the Bacchiglione River.

A. Deployment area

The system deployment was performed on the 18^{th} of January 2024 in the Bacchiglione River in Padova, Italy. The area of the river used for the test (Figure 9) is 37 m wide and has a depth between 2 and 4 meters. The test was performed during a cold rainy and windy day, in order to prove the effectiveness of the proposed solution also in non-ideal conditions.. The underwater channel was realized with EvoLogics S2C 18/34 acoustic modems used with the DESERT Underwater framework. The two QKD stations, described in Section II-A, were installed on the two sides of the river, one close to the pedestrian and bicycle bridge and one close to the jetty of the Rari Nantes rowing association: the distance between the two QKD devices was 150 m. The authenticated classical channel for the QKD protocol was realized with two Radio Frequency (RF) antennas. A and B, the two underwater nodes, were deployed from the the Rari Nantes rowing association's jetty (Figure 10b) and the bridge (Figure 10c), respectively, and got the OTP from the QKD device closer to their location. The distance between A and B was approximately 140 m. The obtained keys were deployed to the nodes A and B equipped with the underwater modems, emulating the key distribution from the two main ships to the underwater nodes before their deployment. Finally, the underwater nodes were able to establish secure communication links thanks to OTP.

E is a malicious mobile node that was deployed from a Mascareta (the typical Venetian rowboat in Figure 10d) and initially located close to B. Then, it moved around the deployment area. E does not have any key, therefore cannot decode the data but can still overhear the channel. In this scenario, E represents a classical eavesdropper who operates solely on the classical channel secured by the QKD shared keys, without any interference on the quantum channel. The absence of Eve on the quantum channel is guaranteed by the fact that the QKD protocol does not abort after the parameter-estimation phase [12], [23].

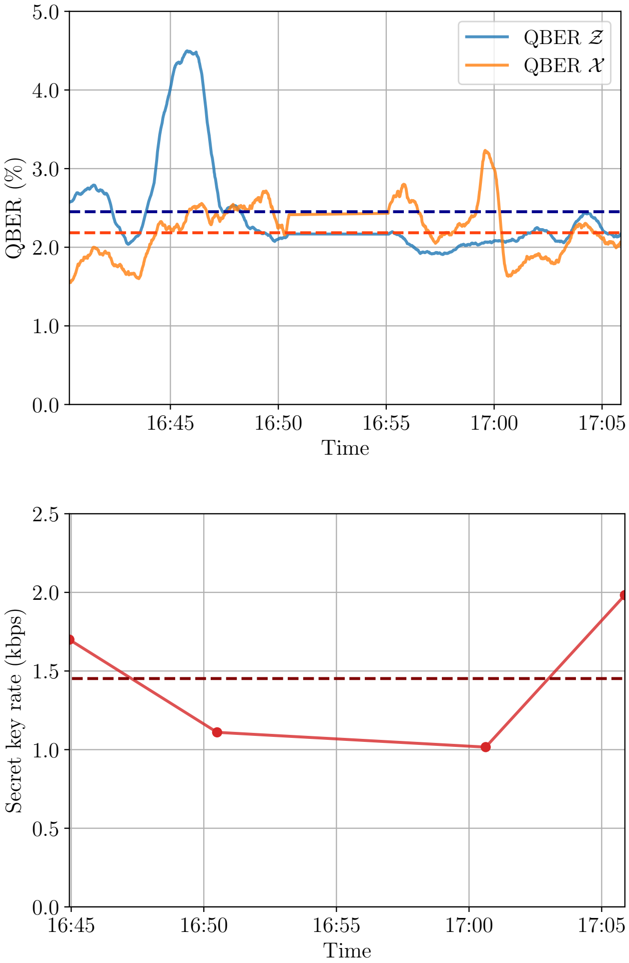
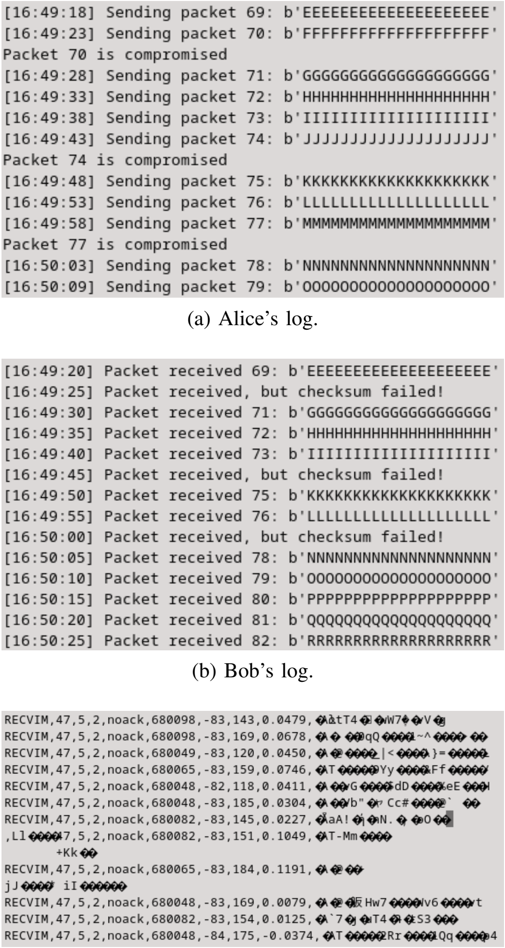


Fig. 11. Summary of the performance of the QKD system in terms of Quantum Bit Error Rate (QBER) and Secret Key Rate (SKR). Dashed lines are the average values, which are 2.45%, 2.18% and 1.45 kbps for the QBER in $\mathcal{Z}$ basis, QBER in $\mathcal{X}$ basis, and SKR respectively.

B. Results

During the demonstration, the QKD system successfully generated 2.2 Mb of secure key within a 30-minute generation timeframe. Fig. 11 illustrates the performance of the QKD system. The overall estimated channel losses were 15 dB and the average QBER was 2.45% for the $\mathcal{Z}$ basis and 2.18% for the $\mathcal{X}$ basis.

For what concerns the underwater network, we performed three batches of experiments. In each batch we performed two transmissions of 200 packets carrying a payload of 20 B each,



```
[16:49:18] Sending packet 69: b'EEEEEEEEEEEEEEEEEEEE'
[16:49:23] Sending packet 70: b'FFFFFFFFFFFFFFFFFFFF'
Packet 70 is compromised
[16:49:28] Sending packet 71: b'GGGGGGGGGGGGGGGGGGGG'
[16:49:33] Sending packet 72: b'HHHHHHHHHHHHHHHHHHHH'
[16:49:38] Sending packet 73: b'IIIIIIIIIIIIIIIIIIII'
[16:49:43] Sending packet 74: b'JJJJJJJJJJJJJJJJJJJJ'
Packet 74 is compromised
[16:49:48] Sending packet 75: b'KKKKKKKKKKKKKKKKKKKK'
[16:49:53] Sending packet 76: b'LLLLLLLLLLLLLLLLLLLL'
[16:49:58] Sending packet 77: b'MMMMMMMMMMMMMMMMMMMM'
Packet 77 is compromised
[16:50:03] Sending packet 78: b'NNNNNNNNNNNNNNNNNNNN'
[16:50:09] Sending packet 79: b'OOOOOOOOOOOOOOOOOOOO'
```

(a) Alice's log.

```
[16:49:20] Packet received 69: b'EEEEEEEEEEEEEEEEEEEE'
[16:49:25] Packet received, but checksum failed!
[16:49:30] Packet received 71: b'GGGGGGGGGGGGGGGGGGGG'
[16:49:35] Packet received 72: b'HHHHHHHHHHHHHHHHHHHH'
[16:49:40] Packet received 73: b'IIIIIIIIIIIIIIIIIIII'
[16:49:45] Packet received, but checksum failed!
[16:49:50] Packet received 75: b'KKKKKKKKKKKKKKKKKKKK'
[16:49:55] Packet received 76: b'LLLLLLLLLLLLLLLLLLLL'
[16:50:00] Packet received, but checksum failed!
[16:50:05] Packet received 78: b'NNNNNNNNNNNNNNNNNNNN'
[16:50:10] Packet received 79: b'OOOOOOOOOOOOOOOOOOOO'
[16:50:15] Packet received 80: b'PPPPPPPPPPPPPPPPPPPP'
[16:50:20] Packet received 81: b'QQQQQQQQQQQQQQQQQQQQ'
[16:50:25] Packet received 82: b'RRRRRRRRRRRRRRRRRRRR'
```

(b) Bob's log.

```
RECVIM,47,5,2,noack,680098,-83,143,0.0479,�AtT4� �wW7��vV�g
RECVIM,47,5,2,noack,680098,-83,169,0.0678,�A� ��qQ����~^���� ��
RECVIM,47,5,2,noack,680049,-83,120,0.0450,�A�����_|<����}=�����
RECVIM,47,5,2,noack,680065,-83,159,0.0746,�AT�����Yy����Ff�����
RECVIM,47,5,2,noack,680048,-82,118,0.0411,�A���G����dD����eE���
RECVIM,47,5,2,noack,680048,-83,185,0.0304,�A���b"�� Cc#����`  ��
RECVIM,47,5,2,noack,680082,-83,145,0.0227,�aA!��N.� �O��
,Ll����47,5,2,noack,680082,-83,151,0.1049,�AT-Mm����
      +Kk��
RECVIM,47,5,2,noack,680065,-83,184,0.1191,�A���
jJ���� iI������
RECVIM,47,5,2,noack,680048,-83,169,0.0079,�A��Hw7����v6����t
RECVIM,47,5,2,noack,680082,-83,154,0.0125,�A`7��T4���S3���
RECVIM,47,5,2,noack,680048,-84,175,-0.0374,�AT�����Rr����Qq����4
```

(c) Eve's log.

Fig. 12. Sample output at the three nodes during one of the experiments.

with an application generation traffic of 38.4 b/s. The first OTP key requested was previously exchanged by the QKD nodes in our laboratories, since we were unsure that the weather conditions would prove favorable for an outdoor exchange, and was used for the first two batches. In the last batch we were able to use a new OTP key exchanged on site.

The experiments proved successful, with Figure 12 showcasing the different nodes outputs. Alice (Figure 12a) and Bob (Figure 12b) were able to securely exchange data, while Eve (Figure 12c) was only able to detect the presence of a communication. Surprisingly, the measured channel conditions were ideal, with a measured PER of 0% for all the experiments.

V. Conclusions and Outlook

In this paper we presented a secure architecture for underwater acoustic networks, where a quantum channel is used to distribute OTP keys between nodes before deployment. The proposed architecture has been evaluated both in an emulated environment and in a river test. The demonstration allowed to asses the actual key exchange needed for secure communications in the UAN network in different configurations and levels of data traffic. In this paper we showcased how QKD can be used to secure underwater acoustic communication links, highlighting how this system can practically be used in ISR and REA scenarios, moving a step forward towards secure underwater wireless networks.

References

[1] A. Pal, Filippo Campagnaro, K. Ahraf, R. Rahman, A. Ashok, H. Guo, "Communication for underwater sensor networks: A comprehensive summary," *ACM Transactions on Sensor Networks (TOSN)*, vol. 19, no. 1, pp. 1–44, Nov. 2022.

[2] C. Lal, R. Petroccia, M. Conti, and J. Alves, "Secure underwater acoustic networks: Current and future research directions," in *Proc. UComms*, Aug. 2016.

[3] M. Stojanovic, "On the relationship between capacity and distance in an underwater acoustic communication channel," *ACM Mobile Comput. and Commun. Review*, vol. 11, no. 4, pp. 34–43, Oct. 2007.

[4] A. Signori, F. Chiariotti, F. Campagnaro, and M. Zorzi, "A game-theoretic and experimental analysis of energy-depleting underwater jamming attacks," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 9793–9804, Oct. 2020.

[5] D. Tronchin, R. Francescon, F. Campagnaro, A. Signori, R. Petroccia, K. Pelekanakis, P. Paglierani, J. Alves, and M. Zorzi, "A secure cross-layer communication stack for underwater acoustic networks," in *IEEE/MTS OCEANS San Diego – Porto*, 2021.

[6] K. Pelekanakis, C. M. G. Gussen, R. Petroccia, and J. Alves, "Robust channel parameters for crypto key generation in underwater acoustic systems," in *MTS/IEEE OCEANS Seattle*, 2019.

[7] A. Giuliani, F. Ardizzon, and S. Tomasin, "Ml-based advantage distillation for key agreement in underwater acoustic channels," in *2023 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2023, pp. 703–708.

[8] C. Xu, T. Yang, and E. Rojas, "Agile beaconless laser beam alignment with adaptive mm-wave beamforming for inter cubesat communication," in *IEEE International Conference on Space Optical Systems and Applications (ICSOS)*, 2022, pp. 218–223.

[9] V. V. Mai and H. Kim, "Beam control and tracking techniques for high-altitude airborne free-space optical communication systems," in *IEEE International Topical Meeting on Microwave Photonics ("MWP")*, 2020, pp. 5–8.

[10] H. Dol, "EDA-SALSA: Towards smart adaptive underwater acoustic networking," in *IEEE/MTS OCEANS 2019 - Marseille*, 2019.

[11] F. Campagnaro, R. Francescon, P. Casari, R. Diamant, and M. Zorzi, "Multimodal underwater networks: Recent advances and a look ahead," in *Proc. International Conference on Underwater Networks & Systems (WUWNet)*, Halifax, Canada, November 2017.

[12] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," *Adv. Opt. Photon.*, vol. 12, no. 4, pp. 1012–1236, Dec 2020. [Online]. Available: https://opg.optica.org/aop/abstract.cfm?URI=aop-12-4-1012

[13] G. S. Vernam, "Cipher printing telegraph systems: For secret wire and radio telegraphic communications," *Journal of the A.I.E.E.*, vol. 45, no. 2, pp. 109–115, 1926.

[14] J. Daemen and V. Rijmen, "The block cipher rijndael," in *Smart Card Research and Applications*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2000, pp. 277–284.

[15] F. Picciariello, F. Vedovato, D. Orsucci, P. Dominguez, T. Zechel, M. Avesani, M. Padovan, G. Foletto, L. Calderaro, D. Dequal *et al.*, "Quantum-secured time transfer between precise timing facilities: a field trial with simulated satellite links," *GPS Solut*, vol. 28, no. 48, 2024.

[16] "Thinkquantum s.r.l," https://www.thinkquantum.com, accessed: 2022-12-20.

[17] M. Avesani, L. Calderaro, M. Schiavon, A. Stanco, C. Agnesi, A. Santamato, M. Zahidy, A. Scriminich, G. Foletto, G. Contestabile *et al.*, "Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics," *Nature npj Quantum Information*, vol. 7, no. 1, pp. 1–8, 2021.

[18] M. T. Gruneisen, M. L. Eickhoff, S. C. Newey, K. E. Stoltenberg, J. F. Morris, M. Bareian, M. A. Harris, D. W. Oesch, M. D. Oliker, M. B. Flanagan, B. T. Kay, J. D. Schiller, and R. N. Lanning, "Adaptive-optics-enabled quantum communication: A technique for daytime space-

to-earth links," *Phys. Rev. Appl.*, vol. 16, p. 014067, Jul 2021. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevApplied.16.014067

[19] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu *et al.*, "Satellite-relayed intercontinental quantum network," *Physical review letters*, vol. 120, no. 3, p. 030501, 2018.

[20] F. Hufnagel, A. Sit, F. Bouchard, Y. Zhang, D. England, K. Heshami, B. J. Sussman, and E. Karimi, "Investigation of underwater quantum channels in a 30 meter flume tank using structured photons," *New Journal of Physics*, vol. 22, no. 9, p. 093074, sep 2020. [Online]. Available: https://dx.doi.org/10.1088/1367-2630/abb688

[21] C.-Q. Hu, Z.-Q. Yan, J. Gao, Z.-Q. Jiao, Z.-M. Li, W.-G. Shen, Y. Chen, R.-J. Ren, L.-F. Qiao, A.-L. Yang, H. Tang, and X.-M. Jin, "Transmission of photonic polarization states through 55-m water: towards air-to-sea quantum communication," *Photon. Res.*, vol. 7, no. 8, pp. A40–A44, Aug 2019. [Online]. Available: https://opg.optica.org/prj/abstract.cfm?URI=prj-7-8-A40

[22] Y. Chen, W.-G. Shen, Z.-M. Li, C.-Q. Hu, Z.-Q. Yan, Z.-Q. Jiao, J. Gao, M.-M. Cao, K. Sun, and X.-M. Jin, "Underwater transmission of high-dimensional twisted photons over 55 meters," *PhotoniX*, vol. 1, pp. 1–11, 2020.

[23] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," *Reviews of Modern Physics*, vol. 92, no. 2, p. 025002, 2020.

[24] M. Avesani, G. Foletto, M. Padovan, L. Calderaro, C. Agnesi, E. Bazzani, F. Berra, T. Bertapelle, F. Picciariello, F. B. L. Santagiustina, D. Scalcon, A. Scriminich, A. Stanco, F. Vedovato, G. Vallone, and P. Villoresi, "Deployment-ready quantum key distribution over a classical network infrastructure in Padua," *IEEE/OSA Journal of Lightwave Technology*, vol. 40, no. 6, pp. 1658–1663, Jan 2022.

[25] C.-H. F. Fung and H.-K. Lo, "Security proof of a three-state quantum-key-distribution protocol without rotational symmetry," *Physical Review A*, vol. 74, no. 4, p. 042342, Oct 2006.

[26] D. Rusca, A. Boaron, F. Grünenfelder, A. Martin, and H. Zbinden, "Finite-key analysis for the 1-decoy state QKD protocol," *Applied Physics Letters*, vol. 112, no. 17, p. 171104, Apr 2018. [Online]. Available: https://doi.org/10.1063%2F1.5023340

[27] M. Avesani, C. Agnesi, A. Stanco, G. Vallone, and P. Villoresi, "Stable, low-error, and calibration-free polarization encoder for free-space quantum communication," *Optics Letters*, vol. 45, no. 17, p. 4706, Aug 2020.

[28] A. Stanco, F. B. L. Santagiustina, L. Calderaro, M. Avesani, T. Bertapelle, D. Dequal, G. Vallone, and P. Villoresi, "Versatile and concurrent FPGA-based architecture for practical quantum communication systems," *IEEE Transactions on Quantum Engineering*, vol. 3, pp. 1–8, 2022.

[29] F. Vedovato, F. Picciariello, I. Karakosta-Amarantidou, D. Scalcon, M. Avesani, E. Rossi, A. Scriminich, G. Foletto, M. Padovan, A. Lorenzetto *et al.*, "Realization of intermodal fiber/free-space quantum key distribution networks," in *Quantum Computing, Communication, and Simulation III*, vol. 12446. SPIE, 2023, pp. 153–159.

[30] F. Picciariello, I. Karakosta-Amarantidou, E. Rossi, M. Avesani, G. Foletto, L. Calderaro, G. Vallone, P. Villoresi, and F. Vedovato, "Intermodal quantum key distribution field trial with active switching between fiber and free-space channels," *arXiv preprint arXiv:2310.17441*, 2023.

[31] A. Scriminich, G. Foletto, F. Picciariello, A. Stanco, G. Vallone, P. Villoresi, and F. Vedovato, "Optimal design and performance evaluation of free-space quantum key distribution systems," *Quantum Science and Technology*, vol. 7, no. 4, p. 045029, 2022.

[32] L. Calderaro, A. Stanco, C. Agnesi, M. Avesani, D. Dequal, P. Villoresi, and G. Vallone, "Fast and simple qubit-based synchronization for quantum key distribution," *Physical Review Applied*, vol. 13, no. 5, p. 054041, May 2020.

[33] F. Campagnaro *et al.*, "The DESERT underwater framework v2: Improved capabilities and extension tools," in *Proc. UComms*, Lerici, Italy, Sep. 2016.

[34] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[35] "Internet Protocol," RFC 791, Sep. 1981. [Online]. Available: https://www.rfc-editor.org/info/rfc791

[36] "S2C DMAC Emulator," Last time accessed: Dec. 2023. [Online]. Available: https://evologics.de/emulator