A Key Agreement Algorithm for Securing Underwater Acoustic Communications

Roee Diamant[§,*], Paolo Casari[♯], Francesco Ardizzon[♯], Stefano Tomasin[♯],
Thomas Corner[+], Benjamin Sherlock[+], Jeff Neasham[+]

[§]Department of Marine Technologies, University of Haifa, Israel
[♯]DISI, University of Trento, and CNIT
[+]Newcastle University, School of Engineering
[*]Corresponding author, email: roee.d@univ.haifa.ac.il

***Abstract*—With the introduction of standards in underwater acoustic communications, protecting the content of packets sent underwater has become a pressing need. Since underwater devices can be compromised over long-term deployments, navies are reluctant to use encryption devices on the one hand; and on the other hand, they require secure communication without the use of pre-agreed secret keys for flexibility. To answer this demand, here we present a key agreement protocol to generate secret keys from the channel impulse response (CIR) between Alice and Bob. Considering the time-varying nature of the underwater acoustic CIR, our key generator is based on the parameters of the distribution of the random features that characterize the CIR rather than directly on the features themselves. Assuming CIR reciprocity, we estimate the CIR by transmitting probe signals between Alice and Bob, and synchronize the probe transmissions such that signals fly by each other while still respecting the half-duplex constraints of underwater acoustic modems. In turn, Alice and Bob's packets arriving to Eve, the attacker, expose different CIRs and possibly collide. Modeled simulation results show agreement between the keys generated by Alice and Bob, and a significant difference with respect to the keys obtained by Eve.**

I. Introduction and Related Work

UNDERWATER acoustic communication (UWAC) is increasingly perceived as a cost-effective ocean exploration and monitoring means. UWAC devices are left to carry out tasks unattended, possibly for long periods of time, which makes them subject to external attacks. The recent introduction of the North Atlantic Treaty Organization (NATO) standard for UWAC, JANUS, increases the attack surface by standardizing communication signals and packet formats, calling for novel schemes to secure the privacy of underwater communications. In this paper, we focus on defending against an attacker who passively intercepts UWAC messages, aiming to decode them and possibly mimic or replay their transmissions. This challenge poses a severe security problem to applications such as command, control, and communication with underwater autonomous vehicles (AUVs) or divers, including the non-authorized activation of acoustically controlled equipment such as acoustic releases, as well as to the remote sensing and reporting of suspicious activity in the water.

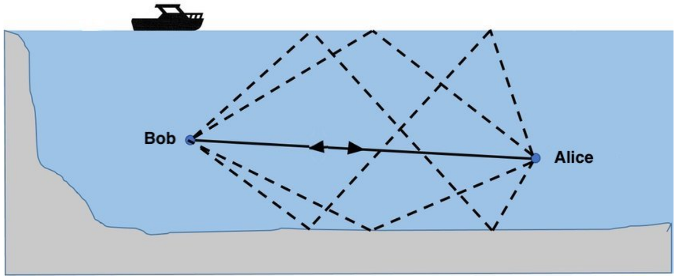

Fig. 1. Illustration of acoustic propagation between two underwater acoustic devices, Alice and Bob.

Secret key agreement is a procedure by which two terminals generate a sequence of bits that remain secret to an eavesdropper. To generate the key, the parties need to share a source of randomness. This can arise from the location-specific and time-varying physical channel features, if the two devices can estimate these quantities and derive values in agreement with each other. This property relies on channel reciprocity, and typically applies to such channel features as the impulse response, the frequency response, as well as transmitter or receiver impairments. Moreover, coding techniques are used to remove estimation errors, and hashing techniques have to be applied to hide the key from eavesdroppers [1].

Secret key agreement has been applied in various contexts, especially on the wireless channel (see [2] and [3] for surveys). A relevant example of secret key agreement is its application to orthogonal frequency division multiplexing (OFDM). In [4], suitable resource allocation strategies for secret key agreement over OFDM are proposed, while in [5] the approach is extended to exploit log-likelihood thresholding and syndrome decoding. A strategy for the advantage distillation step of the secret key agreement involving the cooperation between the legitimate user has been proposed in [6]. Secret key extraction can also be used to perform authentication using cryptographic approaches, and a comparison between direct physical-layer authentication and authentication by secret (physical layer) keys has been proposed in [7]. For the specific application of secret key agreement to underwater scenarios, in [8] the channel frequency response of an OFDM system for underwater communications is exploited for secret key generation. Furthermore, two enhancements are proposed – one is based on adaptively weighting the probing signals to increase the

This work was sponsored in part by the NATO Science for Peace and Security Programme under grant no. G5884 (SAFE-UComm), by the European Union's Horizon Europe programme under UWIN-LABUST project (project number 101086340), and by the Italian Ministry of Economy and Finance through iNEST (Interconnected NordEst Innovation Ecosystem), funded by PNRR (Mission 4.2, Investment 1.5), Next Generation EU (Project ID: ECS 00000043, Digital, Industry, Aerospace).

channel correlation, and the second introduces a block-sliced key verification procedure to deal with channel dynamics and increase key agreement probability. An overview of alternatives for key extraction, information reconciliation, and privacy application is discussed, especially considering its application in an underwater context in [9].

The main challenge in physical key generation for secure UWAC is the need to agree on the key between Alice and Bob. The underwater CIR is spatially-varying. This makes it suitable to conceal keys from the attacker, Eve, who is assumed to be at a different location than that of the communicating partners, Alice and Bob. However, the same spatial changes also lead to a vulnerability, as the CIRs experienced by Alice and Bob may change due to nodes' drift or self motion. Moreover, the fast time-varying nature of the underwater CIR makes it hard to agree on a channel-based key between Alice and Bob. As a result, methods relying on key extraction directly from the channel's or noise characteristics, e.g., [7], [10], are mostly suitable to calm sea conditions with coherent bathymetry where the channel's temporal and spatial changes are slow. In a previous work [11], we proposed to use the packet time-of-arrival while using the propagation delay as a random key generator. However, this is suitable to the setup of a complex network of underwater devices, while only a few secret bits can be drawn for a peer-to-peer scenario.

In this paper, we address the challenge of key generation by taking a statistical approach regarding the characteristics of the UWAC channel. We avoid solutions that require intervening in the modem's architecture and rather rely on information that can be obtained by both Alice and Bob independently. Our solution stems from two main assumptions: 1) that the underwater CIR is reciprocal, and 2) that the channel's features are random with distribution that is fixed over the short period of key agreement. Given that, we build the secret key from the distribution parameters of the channel's features, and reach key agreement by scheduling the key generation simultaneously at Alice and Bob. The result is a collection of random numbers for each channel feature used, which are combined and quantized to obtain a binary key. The underwater CIR is representative of frequency-selective channels, whose fading is considered extremely long, with a delay spread in the order of 5 ms for short-range shallow sea (up to 100 m depth) and can reach 1 s for long-range communications (for distances above 50 km) [12]. The channel exhibits delayed reflections arriving from the sea boundaries: surface, seabed, and volume scatters, see Fig. 1. Hence, we expect the distribution's parameters to yield non-trivial values that are hard to guess.

The remainder of this paper is organized as follows. In Section II, we describe our system model including assumptions about Eve's actions. Section III presents the details of our key agreement protocol. Simulation results are given in Section IV, and conclusions are drawn in Section V.

II. System Model

Our system model includes two underwater devices, Alice and Bob, that aim to securely exchange communication packets in a peer-to-peer connection. The communication includes a periodic key agreement procedure in which Alice and Bob send public probe signals from which the CIR can be estimated. The locations of Bob and Alice are not known, but their communication range can be estimated by measuring the time-difference-of-arrival for a two-way packet exchange.

We assume that the CIR for the Alice-Bob link is reciprocal, but rapidly time-varying. Specifically, we assume that the features of the CIR are random numbers with distributions that are stationary only for the short period of the key exchange (on the order of less than a second). The distribution assumed in this paper is Gaussian, but the method is flexible and can incorporate other types of distributions. As a result of the assumed stationary distribution, the distribution's parameters are considered fixed. We further assume a sufficiently complex CIR, such that the distribution's parameters are not trivial and hard to guess.

The attacker, Eve, is considered to be passive in order to conceal her existence from Alice and Bob. Eve is assumed to overhear and decode all the communication between Alice and Bob. We further assume that Eve can estimate the locations of Alice and Bob via, e.g., an array of receivers and self motion [13], and can thus reconstruct the CIR between Alice and Bob through propagation models such as Bellhop [14]. However, this estimation is considered noisy due to unknown or roughly estimated bathymetry and inaccuracies in the positioning of Alice and Bob.

III. The Key Generation Protocol

A. Key Idea

We model the underwater CIR as a tapped delay line

$$h(t) = \sum_{p} c^p(t)\delta(t - \tau^p) \ , \tag{1}$$

where $h(t)$ is the time-domain CIR, p is the tap's number, $c^p(t)$ is the complex amplitude of the pth tap and τ^p is the tap's delay. Coefficients $c^p(t)$ and τ^p are considered highly location-dependent [15] and are treated as random variables. In particular, $c^p(t)$ is often considered as Racine-distributed whereas τ^p can be modeled as a folded normal distribution [16]. Function $h(t)$ is estimated by Bob/Alice emitting a probe signal that comprises a sequence of wideband chirp signals of known parameters. The receiver, Alice/Bob, apply a channel estimation technique, e.g., orthogonal matching pursuit [17] or even a simple matched filter in case of high signal-to-noise-ratio, to yield a sequence of $h(t)_1, \ldots, h(t)_N$ for all N chirps. For each $h(t)_n$, features of the CIR are derived. The sequence of N such features is then used to statistically evaluate the feature's distribution parameters. These parameters are summed up for all features used and quantized to yield a single binary key.

To agree of a key while facing the channel's temporal variations, we schedule the transmissions of Alice and Bob to start emitting the probe signal simultaneously. As a result, since we assume channel's reciprocity, the two exchanged proes will experience the same CIR. The duration of the probe signal which determines the value of N, is set according to the instantaneous propagation delay between Bob and Alice, minus a guard time to allow the local reverberation following

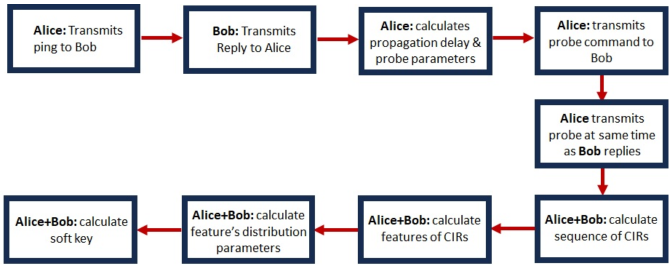
Alice: Transmits ping to Bob
Bob: Transmits Reply to Alice
Alice: calculates propagation delay & probe parameters
Alice: transmits probe command to Bob
Alice transmits probe at same time as **Bob** replies
Alice+Bob: calculate sequence of CIRs
Alice+Bob: calculate features of CIRs
Alice+Bob: calculate feature's distribution parameters
Alice+Bob: calculate soft key

Fig. 2. Block diagram for the secret key generation and exchange.

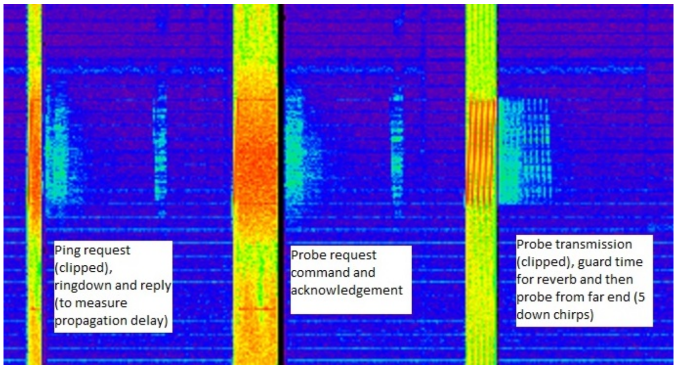

Fig. 3. Sample spectrogram view of the synchronized probe exchange, showing the signal received by Alice.

a transmission to decay to an acceptable level. As proposed in [18], the long propagation delay of the underwater channel can be utilized to increase throughput by letting packets fly by each other. The following protocol is used:

1) Alice sends a "ping request" message to Bob;
2) Bob sends a "ping reply" message enabling Alice to measure propagation delay;
3) Alice calculates the number of chirps in the probe transmission for a given propagation delay, chirp length, guard time, etc.;
4) Alice sends a command to Bob to trigger the transmission of the specified probe;
5) Alice calculates the expected start time of Bob's probe transmission from the known propagation delay;
6) Alice starts the probe transmission at the same time as Bob.

A block diagram of the soft key extraction protocol is given in Fig. 2.

B. Channel's Features and Distribution Analysis

For each received chirp symbol from the probe signal, we estimate the CIR as an array of tap (value,delay) pairs, $(c_n^p, \tau_n^p),\ p = 1, \ldots, P,\ n = 1, \ldots, N$, arranged in sequences, $\bar{\tau_n}$ and $\bar{c_n}$. These sequences are used to evaluate the channel features. We rely on the analysis made in [19] for the CIR's features that both slowly change in time and fast change in space. The former is aimed to fulfil our assumed stationary distribution, while the latter is aimed to conceal the key from Eve. These features include the number of channel's taps

$$\rho_n^1 = N \ , \tag{2}$$

the RMS of the channel's tap delay

$$\rho_n^2 = \sqrt{E(\bar{\tau}_n^2)} \ , \tag{3}$$

the RMS of the channel's tap values

$$\rho_n^3 = \sqrt{E(\bar{c}_n^2)} \ , \tag{4}$$

and the channel's delay spread

$$\rho_n^4 = \frac{\sum_p c_n^p \cdot \tau_n^p}{\sum_p c_n^p} \ . \tag{5}$$

The four sequences of channel features are next analyzed to find their distribution parameters.

Recall we assume stationary distribution for the channel's features. Thus, each feature is derived from the same distribution function. To estimate the parameters of this distribution we use the simple but effective method-of-moments, which statistically computes the moments of a sequence of observation and compare them with the analytical moment to yield a sequence of L equations, one for each moment used. Here, L should be greater than or equal to the number of distribution parameters. To characterize the channel features we choose the Gaussian distribution. However, this way, other types of distribution functions can be easily integrated into the protocol.

C. Modem Configuration

The hardware developed to investigate this protocol in practice is based on the NMv3 miniature spread spectrum acoustic modems developed by Newcastle University [20], operating in the 24-32 kHz frequency band. In order to achieve the time-synchronised exchange of channel probe signals between Alice and Bob, as described in Fig. 2, a PC application was written in C++ to interface to the modems, calculate the required delays and probe parameters, and initiate the transmissions at the correct times via modem commands. Custom firmware was produced for the modems, adding a command to transmit a specified number of chirp signals, with selectable direction (up/down), durations of 2, 5, 10, 20, 40, 50 ms and variable delay between chirps.

The received signal (pre-amplified and filtered) from Alice and Bob's modems is connected to a digital audio card interfaced into the PC at each end, with timestamped recordings to enable correspondence of channel probe signals at each end. The recorded signals, in `.wav` audio format, can then be processed offline to analyse the reciprocal channel responses and perform key generation. Fig. 3 shows a spectrogram view of an example of a synchronised exchange between Alice and Bob in the North Sea over 800m range (viewed from Alice). From left to right we see:

1) Ping request and ping reply used to measure propagation delay;
2) Probe request command sent by Alice and acknowledged by Bob;
3) Alice's probe transmission consisting of 5 up-chirps;
4) Reverberation from Alice's transmission;
5) Reception of Bob's probe transmission consisting of 5 down-chirps;

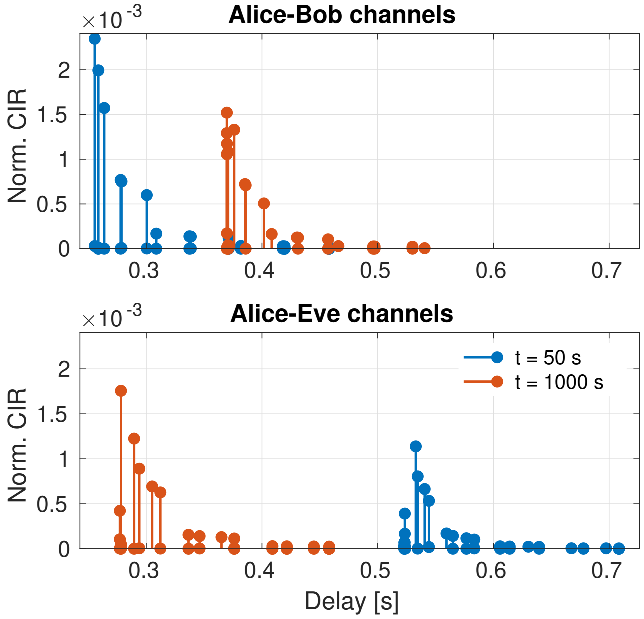

Fig. 4. Examples of Alice-Bob and Alice-Eve channels at different times along a simulated trajectory. Here, after 950 s, Alice has moved farther from Bob and closer to Eve.

This procedure is repeated approximately every 10 seconds with chirp probe parameters automatically adjusted as range, and hence propagation delay, vary.

IV. Performance Evaluation

A. Simulation Model

We have performed Monte-Carlo simulations to evaluate the performance of our key derivation scheme, using the Bellhop ray tracing software to model acoustic propagation realistically. We assume Alice and Bob to move at a prescribed speed within a downward refractive environment with flat bottom and surface. The trajectories of Alice and Bob evolve according to a Gauss-Markov process of self-correlation equal to 0.99, which emulates a mild drift with highly self-correlated trajectories. The initial location of both Alice and Bob is drawn at random within an area of 2×2 km^2, and their depth is chosen at random in the interval $[-45, -25]$ m. Eve is located at random within the same area and remains static throughout the simulation.

Alice and Bob exchange messages while drifting to estimate channels, derive channel feature statistics, and distill bit sequences for key formation. Transmission outcomes are location-dependent, and channel features change over time. For instance, multiple reflections fade away as distance increases, and thus the number of significant channel taps decreases.

We collect a Monte-Carlo set of 10,000 simulation runs, where we execute the key distillation procedures multiple times per run. Throughout each experiment, Eve also attempts to decode the key derived from the messages exchanged by Alice and Bob.

Fig. 4 shows an example of Alice-Bob (top panel) and Alice-Eve channels (bottom panel), 50 s and 1000 s after the start of a simulation, where Alice and Bob move at 0.5 m/s on average. Here, the mobility patterns bring Alice progressively farther from Bob and closer to Eve. This is seen, e.g., from the amplitude of the strongest arrival (which decreases for the Alice-Bob channel and increase for the Alice-Eve ones). In addition, the number of arrivals for each channel and the variation of the delay and power of each of them are significant, and can be used for key distillation purposes, as we discuss below.

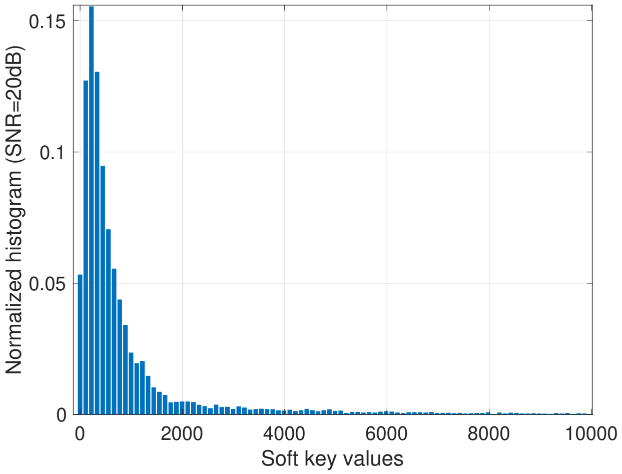

Fig. 5. Histogram for the values of soft secret key derived by Bob.

B. Simulation Results

We analyze the results in terms of the Hamming distance between the keys derived by Alice, Bob, and Eve, as well as by the dynamic range of the soft keys before quantization. We start by exploring the diversity of the channel features to comment on their suitability to serve as random key generators. Fig. 5 shows the histrogram of the accumulated parameters used by Bib as soft secret keys as computed from all 10,000 numerical simulations. We observe a large variation between 0 to 3000 that can translate into 11 bits per quantized value.

In Fig. 6 we show the CDF results of the Hamming distance between the keys derived by Alice and Bob as a function of the SNR. From the results, we observe that the Hamming distance is roughly the same until the SNR is about 10 dB, but greatly deteriorate for lower SNR values. That is, the channel features are stable at both ends of the Alice-Bob link for SNR≥10 dB, but are hard to agree upon for lower SNR values.

Finally, in Fig. 7, we show the cumulative density function (CDF) of the Hamming distance between Bob and Alice for several average simulated drifting speed values of the nodes, normalized by the key length. While the drifting speed effects the coherence of the CIR, we observe to effect on the hamming distance results. This is mainly due to the simultaneous message exchange by Alice and Bob that aims to overcome channel variations.

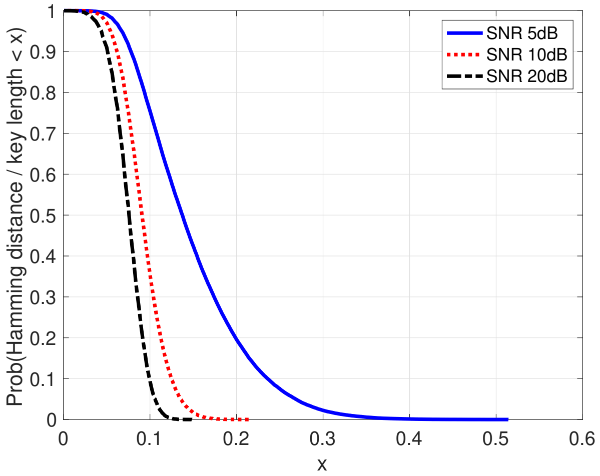

Fig. 6. A CDF of the Hamming distance, normalized by key length, between the secret keys derived by Alice and Bob as a function of the SNR. Speed: 0.1 m/sec.

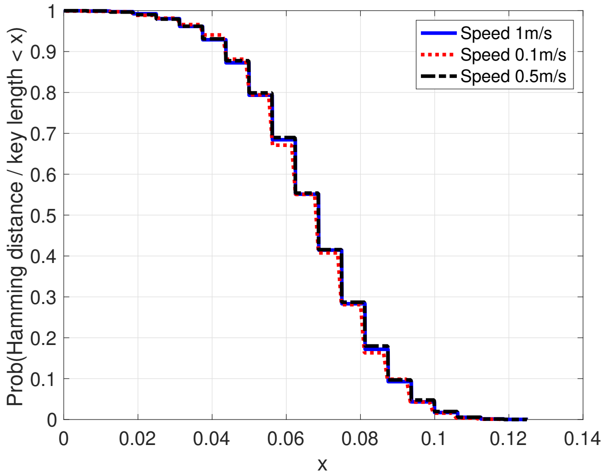

Fig. 7. CDF of the Hamming distance, normalized by the key length, between the secret keys derived by Alice and Bob as a function of the drifting speed. SNR: 20 dB.

V. Conclusions

In this paper, we outline a protocol to generate secret keys for a peer-to-peer underwater acoustic communication. Rather than generating the key based on the direct features of the channel, we offer a more abstract representation of the channel's features to provide high agreement rate between Alice and Bob's keys. This is performed by calculating the distribution parameters of the channel's features. To further enhance the key agreement capability, we schedule the transmissions of Alice and Bob to start simultaneously and determine the size of their packets by the measured propagation delay. This allows packets to propagate through the same reciprocal channel while avoiding packet collisions. Our numerical results demonstrate this key agreement by a small hamming distance between Alice and Bob, that is robust for SNR levels above 10 dB and for various speed of the communicating nodes. Results also show a high diversity of the used keys which reflects on a potential for a large number of secret bits.

References

[1] M. Bloch and J. Barros, *Physical-layer security: from information theory to security engineering*. Cambridge University Press, 2011.

[2] Y. E. H. Shehadeh and D. Hogrefe, "A survey on secret key generation mechanisms on the physical layer in wireless networks," *Security and Communication Networks*, vol. 8, no. 2, pp. 332–341, 2015.

[3] T. Wang, Y. Liu, and A. V. Vasilakos, "Survey on channel reciprocity based key establishment techniques for wireless systems," *Wireless Networks*, vol. 21, pp. 1835–1846, 2015.

[4] S. Tomasin and A. Dall'Arche, "Resource allocation for secret key agreement over parallel channels with full and partial eavesdropper CSI," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 11, pp. 2314–2324, 2015.

[5] A. Dall'Arche and S. Tomasin, "Resource allocation for secret key agreement by LLR thresholding over parallel channels," in *2014 11th International Symposium on Wireless Communications Systems (ISWCS)*. IEEE, 2014, pp. 955–959.

[6] F. Ardizzon, F. Giurisato, and S. Tomasin, "Secret-key-agreement advantage distillation with quantization correction," *IEEE Communications Letters*, vol. 27, no. 9, pp. 2293–2297, 2023.

[7] S. Yıldırım, K. Pelekanakis, G. Sklivanitis, D. A. Pados, P. Paglierani, R. Petroccia, J. Alves, F. Molfese, and F. Cuomo, "Secret underwater acoustic key generation challenged by eve's simulator," *IEEE Journal of Oceanic Engineering*, 2023.

[8] Y. Huang, S. Zhou, Z. Shi, and L. Lai, "Channel frequency response-based secret key generation in underwater acoustic systems," *IEEE Transactions on Wireless Communications*, vol. 15, no. 9, pp. 5875–5888, 2016.

[9] Y. Luo, L. Pu, Z. Peng, and Z. Shi, "RSS-based secret key generation in underwater acoustic networks: advantages, challenges, and performance improvements," *IEEE Communications Magazine*, vol. 54, no. 2, pp. 32–38, 2016.

[10] M. Xu, H. Feng, and L. Liu, "Covert secret-key agreement protocol based on the underwater acoustic channel," *IEEE Wireless Communications Letters*, vol. 11, no. 7, pp. 1384–1388, 2022.

[11] R. Diamant, S. Tomasin, F. Ardizzon, D. Eccher, and P. Casari, "Secret key generation from route propagation delays for underwater acoustic networks," *IEEE Transactions on Information Forensics and Security*, 2023.

[12] W. S. Burdic, "Underwater acoustic system analysis," *(No Title)*, 1984.

[13] T. Alexandri, M. Walter, and R. Diamant, "A time difference of arrival based target motion analysis for localization of underwater vehicles," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 1, pp. 326–338, 2021.

[14] M. B. Porter, "The bellhop manual and user's guide: Preliminary draft," *Heat, Light, and Sound Research, Inc., La Jolla, CA, USA, Tech. Rep*, vol. 260, 2011.

[15] H. Yan, T. Ma, C. Pan, Y. Liu, and S. Liu, "Statistical analysis of time-varying channel for underwater acoustic communication and network," in *2021 International Conference on Frontiers of Information Technology (FIT)*. IEEE, 2021, pp. 55–60.

[16] P. Qarabaqi and M. Stojanovic, "Statistical characterization and computationally efficient modeling of a class of underwater acoustic communication channels," *IEEE Journal of Oceanic Engineering*, vol. 38, no. 4, pp. 701–717, 2013.

[17] Y. Zhou and R. Diamant, "A parallel decoding approach for mitigating near–far interference in internet of underwater things," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 9747–9759, 2020.

[18] R. Diamant, W. Shi, W.-S. Soh, and L. Lampe, "Joint time and spatial reuse handshake protocol for underwater acoustic communication networks," *IEEE Journal of Oceanic Engineering*, vol. 38, no. 3, pp. 470–483, 2013.

[19] R. Diamant, P. Casari, and S. Tomasin, "Cooperative authentication in underwater acoustic sensor networks," *IEEE transactions on wireless communications*, vol. 18, no. 2, pp. 954–968, 2018.

[20] B. Sherlock, N. Morozs, J. Neasham, and P. Mitchell, "Ultra-low-cost and ultra-low-power, miniature acoustic modems using multipath tolerant spread-spectrum techniques," *Electronics*, vol. 11, no. 9, p. 1446, 2022.