2021 Fifth Underwater Communications and Networking Conference (UComms) | 978-1-7281-9315-1/21/$31.00 ©2021 IEEE | DOI: 10.1109/UCOMMS50339.2021.9598102

Physical Layer Security against an Informed Eavesdropper in Underwater Acoustic Channels: Feature Extraction and Quantization

Konstantinos Pelekanakis[1], Seçkin Anıl Yıldırım[1], Georgios Sklivanitis[2],
Roberto Petroccia[1], João Alves[1] and Dimitris Pados[2]

[1] NATO STO Centre for Maritime Research and Experimentation, La Spezia 19126, Italy
[2] Center for Connected Autonomy and AI, Florida Atlantic University, FL 33431, USA

***Abstract*—During the Rapid Environmental Picture 2018 (REP18) sea trial, two underwater acoustic nodes (Alice and Bob) exchanged 897 channel probes over different ranges and environmental conditions. In this short paper, Alice and Bob independently process their received probes offline with the aim to generate a cryptographic key based on Physical Layer Security (PLS). Using their estimated Channel Impulse Responses (CIRs), they compute and quantize four pre-agreed channel features. Eve is a simulated eavesdropper who is aware of the PLS algorithm, the 3D positions of Alice and Bob and the acoustic properties of the environment. Eve uses the *de facto* standard Bellhop acoustic simulator to predict the bi-directional CIRs between Alice and Bob and compute her own quantized features. We calculate the Bit Disagreement Ratio (BDR), which is a function of the number of disagreeing bits between a pair of nodes. Our results confirm that the proposed features are robust enough to yield a lower BDR between Alice and Bob than that for Eve. The BDR impact on reconciliation and secret key generation is studied in a subsequent paper [1].**

I. Introduction

We focus on the challenges of symmetric crypto-systems for ad-hoc Underwater Acoustic Networks (UANs). A widely-used symmetric crypto-system is the Advanced Encryption Standard [2], which supports key lengths of 128, 192 or 256 bits. Such a key is typically pre-loaded among all trusted nodes of a network to encrypt/decrypt messages. This approach is inflexible when a new node joins the network because the key should not be shared in the public channel. In addition, in the event that the key is compromised, the entire network is not secure any more.

Physical Layer Security (PLS) aims to generate a key between two authenticated nodes (Alice and Bob) without the need to share the actual key. In theory, this is possible due to channel reciprocity in waveguide propagation. Reciprocity is valid under two assumptions: (a) the transmitting transducer and the receiving hydrophone on a node are co-located; (b) the channel coherence time is sufficiently longer than the propagation time. This assumption can be easily met in radio/optical channels [3], yet, in acoustic channels the travel time is not only non-negligible but often larger than the channel coherence time. Hence, the name of the game shifts towards finding ways to exploit the bi-directional channel correlation [4].

One way to generate a symmetric key based on PLS is to apply four steps [5], [6]: (a) channel feature extraction; (b) quantization; (c) reconciliation; (d) privacy amplification. In this paper, we elaborate on the first two steps while the final two steps and the generated key are presented in a separate manuscript [1]. It is important to note that only recently PLS studies have received attention in the field of underwater acoustic communications [7]–[9].

PLS assessment usually assumes an eavesdropper (Eve) who knows the key generation algorithm and tries to generate the same key from the intercepted channel probes. Our working assumption is that Eve needs to be “sufficiently” far away from the operational area of Alice and Bob to minimize the risk of being noticed. This brings up an important research question: could Eve generate the same key if she had accurate knowledge of the Alice-Bob 3D positions, the bathymetry as well as the sound speed profile? To answer this question we equip Eve with the Bellhop acoustic simulator [10]. Alice and Bob use real data from the Rapid Environmental Picture 2018 (REP18) sea trial. Based on their respective Channel Impulse Responses (CIRs), Alice, Bob and Eve estimate four channel features and quantize their values based on channel-dependent thresholds. We confirm that our methodology exploits the inherent bi-directional channel correlation. Furthermore, we demonstrate that the assumed level of sophistication of Eve is not sufficient to yield a lower Bit Disagreement Ratio (BDR) than that between Alice and Bob.

II. Feature Extraction and Quantization

Assuming a probe signal exchange of bandwidth W, Alice and Bob calculate their respective baseband CIR snapshots represented by a complex-valued vector:

$$\boldsymbol{h}(n) = \left[h_0(n) \cdots h_i(n) \cdots h_{I-1}(n)\right]^{\mathrm{T}}, \qquad (1)$$

where $n \in \mathbb{N}$ denotes the sampled absolute time and $i \in [0, I-1]$ denotes the sampled multipath delay. The value of $h_i(n)$ is the sum of all acoustic rays arriving within the delay window $\tau_i \pm 0.5/W$, where $\tau_i = \tau_0 + i/W$ and τ_0 is a fixed reference delay in seconds. Furthermore, the maximum amplitude of $\boldsymbol{h}(n)$ is normalized to unity (0 dB) to prevent discrepancies between the power amplifiers of Alice and Bob.

We define the index set $\mathscr{L}(n)$ with entries that correspond to local maxima (peaks) of $|\boldsymbol{h}(n)|$ under the condition that these maxima are above a threshold of α dB. The purpose

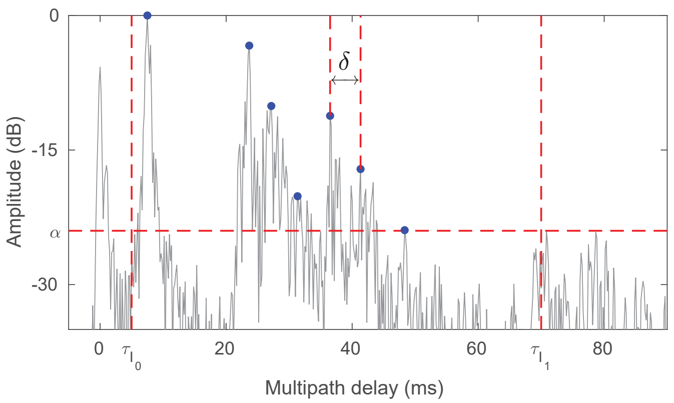


Fig. 1: Calculation of the set $\mathcal{L}(n)$ based on a snapshot of $|\boldsymbol{h}(n)|$. The parameters are chosen as $\alpha = -24$ dB, $I_0 = 31$ ($\tau_{I_0} = 5$ ms), $I_1 = 421$ ($\tau_{I_1} = 70$ ms) and $\delta = 5$ ms.

of the threshold parameter α is to isolate weak multipath components since they tend to have a negative effect on the two-way channel correlation in the event of asymmetric SNRs.

A subset of $\mathscr{L}(n)$, denoted as $\mathcal{L}(n)$, is defined as follows:

$$\mathcal{L}(n) = \left\{\forall i \in \mathscr{L}(n) \;\middle|\; I_0 \leq i \leq I_1,\; \tau_i - \tau_{i-1} \geq \delta\right\}, \quad (2)$$

where parameters I_0 and I_1 define the lower and upper end of a multipath delay window, respectively, and δ aims to isolate peaks based on a minimum delay criterion. To provide insight on how these parameters dictate $\mathcal{L}(n)$, Fig. 1 illustrates an example based on a measured magnitude of a CIR snapshot. Note that the blue circles correspond to peak values $|h_i(n)|$ whose index value i belongs to $\mathcal{L}(n)$.

Based on (2), we define the following four CIR-based features:

1) The L_0 norm feature,

$$L(n) = \left|\mathcal{L}(n)\right|, \quad (3)$$

which is also equal to the number of multipath arrivals that satisfy the specific conditions in (2).

2) The channel sparseness feature defined as:

$$B(n) = \frac{\tilde{I}}{\tilde{I} - \sqrt{\tilde{I}}}\left(1 - \frac{\sum_{i\in\mathcal{L}(n)} \left|h_i(n)\right|}{\sqrt{\tilde{I}}\sqrt{\sum_{i\in\mathcal{L}(n)} \left|h_i(n)\right|^2}}\right), \quad (4)$$

where $\tilde{I} = I_1 - I_0$. It can be shown that $B(n) \in (0, 1]$ and sparser CIRs yield $B(n)$ closer to one.

3) The L_2 norm feature defined as:

$$E(n) = \sqrt{\sum_{i\in\mathcal{L}(n)} \left|h_i(n)\right|^2}. \quad (5)$$

4) The delay spread feature defined as:

$$\Phi(n) = \max_{i\in\mathcal{L}(n)} \tau_i - \min_{i\in\mathcal{L}(n)} \tau_i. \quad (6)$$

Each feature is turned into a bit vector based on a quantizer with $2M + 2$ quantization levels, where $M \in \mathbb{N}$ is a free parameter. Hence, each feature yields $\log_2(2M + 2)$ bits. The quantization levels are channel-dependent and defined as:

$$\left[\mu, \mu \pm \frac{\sigma}{K}\right], \left[\mu \pm \frac{\sigma}{K}, \mu \pm \frac{2\sigma}{K}\right], \ldots, \left[\mu \pm \frac{M\sigma}{K}, \pm\infty\right], \quad (7)$$

where μ and σ are the mean and standard deviation of each feature, respectively, and K is a positive real number that determines the width of the partition interval. We consider that part of the key generation process is to allow Alice and Bob to exchange a pre-agreed number of probes in order to compute μ and σ of each feature before quantization. We emphasize that the pre-agreed free parameters α, I_0, I_1, δ, M and K may be different for each of the four features. These parameters depend on the specific environment, the choice of the channel probe signal, the SNR, to name a few, yet, it is beyond the scope of this work to provide insight on how to select them. On the one hand, the role of the free parameters is to enhance the correlation between Alice and Bob and on the other hand to minimize the correlation of Alice-Eve and Bob-Eve. In our analysis below, Eve has knowledge of the decided parameters.

For the remainder of this paper, the Alice-Bob and Bob-Alice CIRs are represented by $\boldsymbol{h}_{\text{AB}}(n)$ and $\boldsymbol{h}_{\text{BA}}(n)$, respectively. To assess how well each CIR-feature quantizer exploits the correlation between Alice and Bob, we invoke the BDR defined as

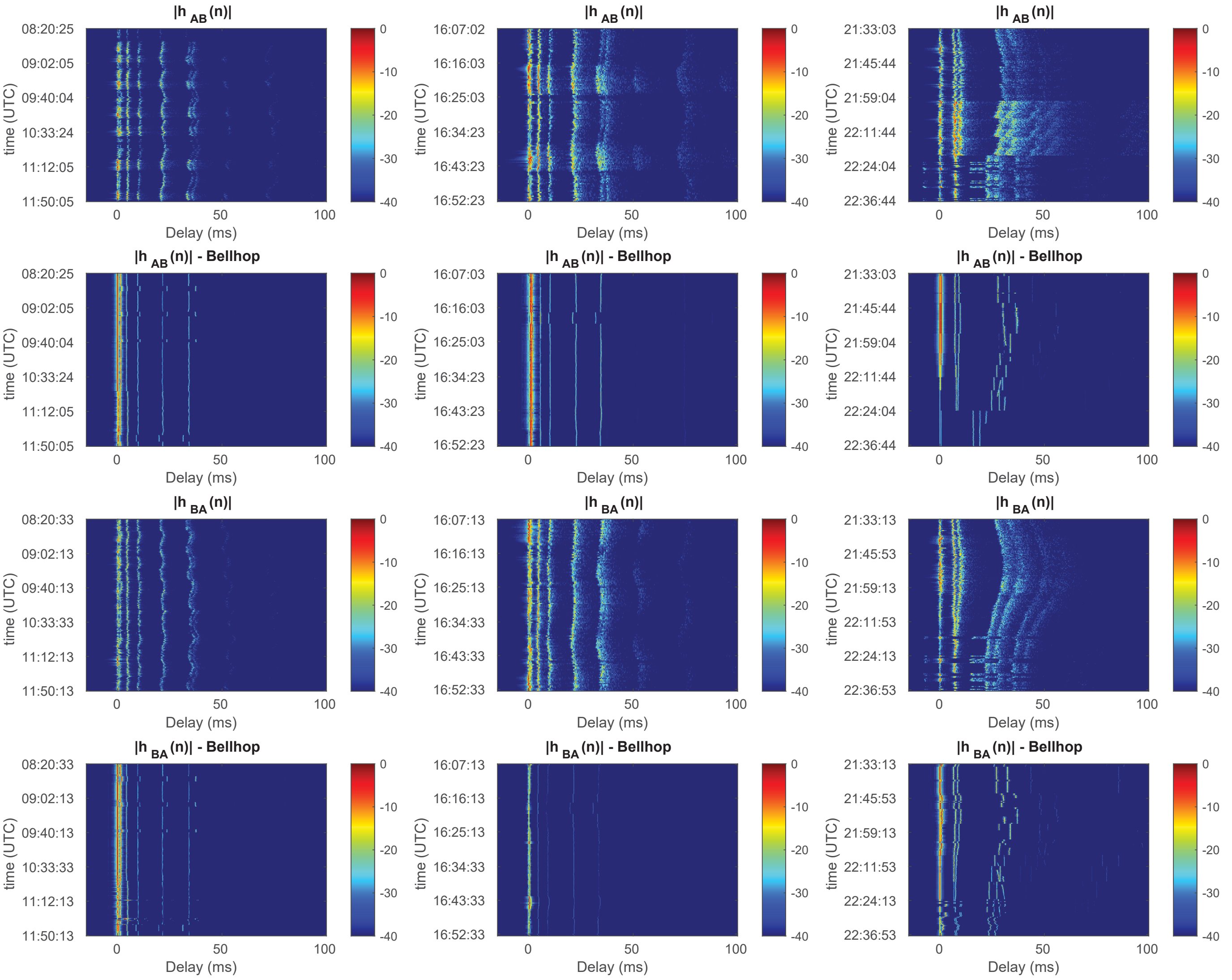
$$\text{BDR}_{\text{AB}} = \frac{\text{Alice-Bob disagreeing bits}}{\log_2(2M + 2)}. \quad (8)$$

It is straightforward to define the average BDR over all four features. Similarly, we define the BDRs between Alice-Eve (BDR_{AE}) and Bob-Eve (BDR_{BE}).

III. Results

We evaluate the proposed feature extraction and quantization method based on off-line processing of acoustic recordings acquired during the REP18 sea trial. The REP18 trial was conducted off the coast of Portugal, between Sines and Sesimbra. The sea depth varied between 100 and 150 m (based on the General Bathymetric Chart of the Oceans (GEBCO) [11]) and acoustic propagation was dictated by a warm surface layer (15-20 m) followed by the thermocline (50-60 m). Three assets were used to establish underwater acoustic links: the NRP Alm. Gago Coutinho hydrographic vessel, a Liquid Robotics Wave Glider, and a sea-surface floating buoy. Table I summarizes the established Alice-Bob links. The link ranges are estimated from the assets' GPS logs and the link velocities are estimated from the Doppler frequency shifts. The latter is achieved after performing matched filtering and searching for the maximum output value in the delay-Doppler plane. Note that the link variability in terms of range, SNR, and mobility was substantial within each day of the experiment.

Alice and Bob exchanged a linear up-sweep chirp (sweeping from 10 kHz to 15 kHz in one second). Alice was programmed to send the chirp at $t_o, t_o + 20s, \ldots$ and Bob was programmed to send the chirp at $t_o + 10s, t_o + 30s, \ldots$. In total, 897 probes were exchanged over three days. Figure 2 illustrates the 897 baseband CIRs Alice and Bob estimated during the



(a) (b) (c)

Fig. 2: Amplitudes of experimental and Bellhop-simulated baseband CIRs: (a) 07-Sept-2018; (b) 08-Sept-2018; (c) 09-Sept-2018. The horizontal axis represents multipath delay and the vertical axis represents absolute time (20 s resolution). The amplitude is in dB scale.

experiment. For each day, the CIRs are stacked along the y-axis. The common x-axis represents the multipath delay whose maximal delay is 100 ms. The 0-ms delay corresponds to the arrival for which the receiver is synchronized. Note that there are a few cases (especially on September 9th) where the receiver is not synchronized to the fastest arrival but to later ones. This happens because our synchronization algorithm has a non-zero probability to miss a weak arrival and lock onto a stronger one. Multipath correlation between $\boldsymbol{h}_{\mathrm{AB}}(n)$ and $\boldsymbol{h}_{\mathrm{BA}}(n)$ can be easily observed despite platform mobility and the non-symmetric SNR levels at Alice and Bob receiver ends.

Figure 2 also includes the synthetic baseband CIRs generated by Eve based on the Bellhop ray tracer. The process of generating a synthetic CIR involves two steps. In the first step, Bellhop identifies the significant eigenrays that connect Alice and Bob. To do so, the following information is used: the Alice-Bob link geometry, sound speed vs. depth, the bathymetry [11] and the geoacoustic parameters for clay-seabed type (bottom density = $1.5\ \mathrm{g/cm^3}$, compressional attenuation = $0.2\ \mathrm{dB/m-kHz}$, compressional speed = $1500\ \mathrm{m/s}$). In the second step, we construct the baseband CIR as follows:

$$h(\tau)=\sum_{q=1}^{Q} a_q e^{-j2\pi f_c \tau_q} b_q\left(\tau-\tau_q\right) \tag{9}$$

where q denotes the q-th eigenray connecting Alice and Bob, a_q and τ_q are the Bellhop complex-valued multipath

TABLE I: REP18 underwater acoustic links.

Date time	Asset depth (Alice)	Asset depth (Bob)	min-max range min-max SNR avg. link velocity
7-Sept-2018 8:19-11:50 (UTC)	Buoy 78 m	Wave Glider 35 m	1.044 - 1.158 km 2.4 - 40.3 dB 0.26 m/s
8-Sept-2018 16:07-16:53 (UTC)	Buoy 78 m	Waveglider 35 m	1.046 - 1.158 km 0.4 - 48.9 dB 0.27 m/s
9-Sept-2018 21:33-22:37 (UTC)	Buoy 78 m	Ship 15 m	0.905 - 1.546 km 7.5 - 44.8 dB 0.42 m/s

gains and delays and $b_q(\tau)$ is the *baseband equivalent* of the ray-dependent sound absorption filter computed over the $[f_c - W/2, f_c + W/2]$ band. For our computations, f_c = 12500 Hz and $W = 5000$ Hz.

As can be observed in Fig. 2, the Bellhop-CIRs are correlated with the ones measured in the field, yet, obvious discrepancies can be seen. These discrepancies are attributed to the fact that the acoustic environment is not known at spatial scales close to the employed wavelengths (10 cm). In addition, measurements of the sound speed profile were taken three times per day and not at every probe exchange. These are limitations that Eve would face in real-world deployment.

Our analysis below uses 20 probe exchanges for deriving the quantization intervals and two probe exchanges to generate quantization vectors. This 20-2 split of the data is called a batch and is selected so because the channel features are time varying and frequent estimation of the quantization levels is needed. For each day of the experiment, we generate a batch for every 20 consecutive probe exchanges, i.e., there is an overlap of two exchanges for two successive batches. Hence, the entire dataset of 897 probe exchanges results into 43 batches, which is sufficient to derive BDR statistics.

Table II shows the judiciously chosen parameters for each feature. All four quantizers are designed to have $M = 63$ (i.e., 7 bits per feature) and $K = 1.7$. Based on the selected parameters, Table II summarizes the average BDR per feature where the average is computed over 43 batches. Note that each batch gives 56 quantization bits. Moreover, Eve has two quantization vectors to consider at each batch, one generated from Alice's probe and another generated from Bob's probe. We consider the worst-case scenario, namely,

$$\mathrm{BDR}_{\mathrm{Eve}} = \min\left(\mathrm{BDR}_{\mathrm{AE}}, \mathrm{BDR}_{\mathrm{BE}}\right). \tag{10}$$

Our BDR analysis shows that all features yield a lower $\mathrm{BDR}_{\mathrm{AB}}$ than that of $\mathrm{BDR}_{\mathrm{Eve}}$.

Figure 3 shows the average BDR per batch number, where the average is computed over all four features. Note that the $\mathrm{BDR}_{\mathrm{AB}}$ is smaller than that of Eve for most batches. There are two cases (batches 3-7 and 22-26) where $\mathrm{BDR}_{\mathrm{AB}} < \mathrm{BDR}_{\mathrm{Eve}}$ for five consecutive batches. However, Eve never succeeds to have a lower BDR for three consecutive batches. Hence, a mechanism that would require $\mathrm{BDR}_{\mathrm{AB}} < \mathrm{BDR}_{\mathrm{Eve}}$ for three or more consecutive batches would be a good starting point for a secure crypto-key generation. Indeed, we show that this is possible and the analysis is deferred to [1].

TABLE II: Free parameter configuration and avg. BDR results.

Feature	α (dB)	$[\tau_{I_0}, \tau_{I_1}]$ (ms)	δ (ms)	avg. $\mathrm{BDR}_{\mathrm{AB}}$	avg. $\mathrm{BDR}_{\mathrm{Eve}}$
L_0 norm	-24	[30,100]	2	0.34	0.42
Ch. sparseness	-24	[0,100]	2	0.31	0.36
L_2 norm	-40	[30,100]	0.17	0.30	0.37
Delay Spread	-10	[0,100]	2	0.35	0.42

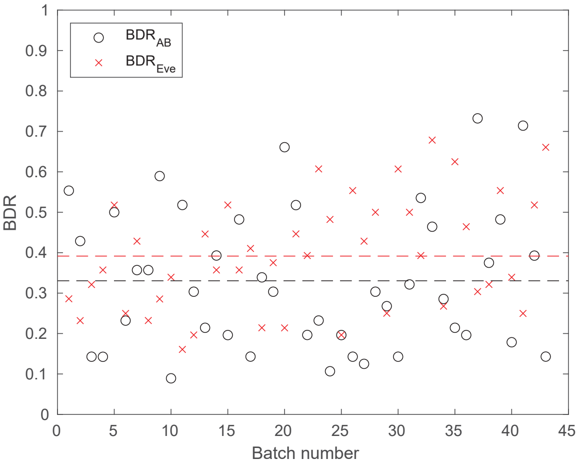


Fig. 3: BDR vs. batch number for Alice, Bob and Eve. Each BDR is averaged over all features. The black and red dashed lines correspond to the average BDR of Alice-Bob and Eve, respectively, computed over all batches.

IV. Conclusions

Dynamic generation of symmetric keys could significantly aid key management in UANs. To this end, an experimental bi-directional link was designed and 897 channel probes were exchanged over three days between two underwater nodes (Alice and Bob). In addition, a simulated Eve was considered to have knowledge of the key generation algorithm, the environment and the true 3D positions of Alice and Bob. With that knowledge, Eve approximated the Alice-Bob link based on the de facto standard Bellhop simulator. Our analysis showed that the proposed four CIR features were robust enough to harvest the two-way channel correlation between Alice and Bob, despite the long chirp duration and the long time difference between Alice and Bob probe exchanges. Moreover, Eve did not manage to beat Alice-Bob in terms of the average BDR despite her high level of intelligence. In our follow-up paper [1], we propose a mechanism that leverages on the BDR advantage of Alice and Bob to derive the crypto-key in a secure way.

Acknowledgment

This work is funded by NATO Allied Command Transformation (ACT) Future Solutions Branch under the Autonomous Security Network Programme and the Office of Naval Research Global under grant no N62909-17-1-2093. The REP18-Atlantic sea trial was co-organized by the Portuguese Navy, FEUP, and CMRE. The authors would like to thank the Captain and crew of the NRP Gago Coutinho for the excellent support during the experiments.

References

[1] G. Sklivanitis, K. Pelekanakis, S. A. Yıldırım, R. Petroccia, J. Alves, and D. Pados, "Physical Layer Security against an Informed Eavesdropper in Underwater Acoustic Channels: Reconciliation and Privacy Amplification," in *2021 IEEE Fifth Underwater Communications and Networking Conference (UComms)*, (accepted).

[2] F. I. P. S. P. 197, "Announcing the ADVANCED ENCRYPTION STANDARD (AES)," November 26 2001, United States National Institute of Standards and Technology (NIST).

[3] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Communications*, vol. 18, no. 4, pp. 6–12, 2011.

[4] K. Pelekanakis, C. M. G. Gussen, R. Petroccia, and J. Alves, "Robust Channel Parameters for Crypto Key Generation in Underwater Acoustic Systems," ser. OCEANS 2019 MTS/IEEE SEATTLE, Seattle, WA, USA, 2019, pp. 1–7.

[5] K. Zeng, "Physical Layer Key Generation in Wireless Networks: Challenges and Opportunities," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 33–39, 1 2015.

[6] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key Generation From Wireless Channels: A Review," *IEEE Access*, vol. 4, pp. 614–626, 2016.

[7] C. Wang and Z. Wang, "Signal Alignment for Secure Underwater Coordinated Multipoint Transmissions," *IEEE Transactions on Signal Processing*, vol. 64, no. 23, pp. 6360–6374, 11 2015.

[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] 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, 2019.

[10] M. B. Porter and H. P. Bucker, "Gaussian beam tracing for computing ocean acoustic fields," *The Journal of the Acoustical Society of America*, vol. 82, no. 4, pp. 1349–1359, 1987.

[11] "General Bathymetric Chart of the Oceans (GEBCO)." [Online]. Available: http://www.gebco.net