DOI: 10.61782/fa.2023.0615

PRACTICAL SECURITY FOR UNDERWATER ACOUSTIC NETWORKS: PUBLISHED RESULTS FROM THE SAFE-UCOMM PROJECT

Paolo Casari[1,2,*] **Roee Diamant**[4] **Stefano Tomasin**[1,3]
Jeff Neasham[5] **Lutz Lampe**[6]

[1] CNIT, Italy [2] DISI, University of Trento, Italy [3] DEI, University of Padova, Italy
[4] University of Haifa, Israel [5] Newcastle University, UK [6] UBC, Canada

ABSTRACT

The emergence of commercial underwater acoustic modems from different manufacturers and the promulgation of interoperability standards (e.g., JANUS) broadens the application scenarios of underwater acoustic telemetry and communications. At the same time, security concerns call for authentication and privacy-enforcing schemes. However, compute- or communication-intensive methods for terrestrial networks do not adapt well to bandwidth-constrained acoustic communications. In this context, we discuss the findings of the NATO SPS SAFE-UComm project, which involves research teams from Italy, Israel, Canada, and the UK. The project investigates and realizes practical security schemes that exploit the randomness of physical acoustic communication processes for security, and evaluates the potential of biomimicry and the capability of biomimetic signal detectors. After discussing the concept of SAFE-UComm, we survey its approaches to security through a number of results related to authentication, privacy, and biomimicry functions. Our results, based on several field experiments, show the feasibility of the project's design in relevant scenarios.

Keywords: *Underwater acoustic communications, physical-layer security, biomimicry, field experiments*

1. INTRODUCTION

Underwater acoustic networks (UWANs) are becoming cost-effective instruments to explore and monitor the oceans, but may become vulnerable to external attacks when operating unattended for long periods of time. Recent standards such as JANUS [1] offer a common acoustic communication format, and may make attacks more likely. Computing performance limitations tend to discourage encryption and authentication schemes, leaving the UWAN exposed to external attackers. Security mechanisms tailored to underwater acoustic communications (UWAC) constraints are thus gaining momentum, as terrestrial radio security rarely translates to UWANs [2].

Current work on cybersecurity for UWAC considers: the challenges of protection against denial-of-service attacks like jamming [3, 4]; covert communications using low-probability-of-detection (LPD) signals or biomimicry [5]; data integrity and message authentication; and key exchange protocols for cryptography [6]. Yet, underwater acoustic channels offer specific characteristics that can be exploited for security. For instance, the channel's spatial dependency and the long propagation delay offer a diversity gain that enables the exchange of cryptographic keys [7–9] or authentication [10], e.g., through physical layer security (PLS) schemes; the complex mobility patterns of drifting nodes and the time-varying channel impulse response could help prevent interception attacks; and the strong attenuation leads to sparse logical topologies that increase security by splitting communications across disjoint wireless links [11].

In the NATO SPS SAFE-UComm project, whose conclusion is planned in Feb. 2024, we aim to design a cybersecurity framework for underwater acoustic communications. With reference to Fig. 1, we investigate novel and practical solutions for authentication, secret key exchange, analysis of bounds for low probability of detection and interception, as well as the use and detection of biomimetic signals attempting to resemble natural under-

[*] ***Corresponding author***: *paolo.casari@unitn.it.*

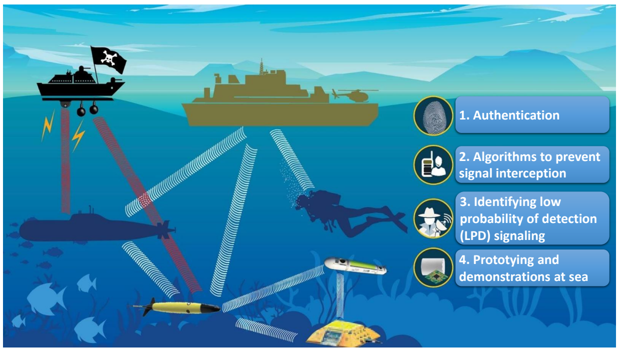
1. Authentication
2. Algorithms to prevent signal interception
3. Identifying low probability of detection (LPD) signaling
4. Prototyping and demonstrations at sea

Figure 1. Concept of the SAFE-UComm project.

water fauna sounds. With a view towards practical systems, we build upon existing UWAC modems, rather than intervening in the modem's design.

In this paper, we overview the main results and conclusions in the above fields. We show that UWAC enables a number of PLS and low-probability of detection (LPD) approaches, and that biomimicry is a feasible communication medium when properly designed, although some biomimetic signal characteristics [12] as well as the operations of electro-acoustic transducers [13] can jeopardize it. In all cases, we discuss preliminary experiments, including tests with a flexible, low-power underwater modem that will be used in the final trials. We start with PLS approaches to underwater communications security in §2, explore biomimetic approaches and detectors thereof in §3, present preliminary results on our transceivers in §4, and discuss conclusions in §5.

2. PHYSICAL LAYER SECURITY

2.1 Authentication

Those features of the impulse response of underwater acoustic channels that vary significantly with a device's location, while remaining coherent over time, offer a good basis for authentication [10]. Consider a typical deployment where nodes transmit data to a sink node, and an attacker tries to pass forged packets as legitimate, while a set of trusted nodes helps the sink detect forging by processing the measured channel features (e.g., number of channel taps, relative root mean-square delay, average tap power, etc.). Because different features may be correlated, we deploy a machine learning scheme based on autoencoders (AEs), a specific type of neural network (NN) that learns the correlation among input features and projects them onto a latent space from which they can be recovered with minimal error. All trusted nodes run their local AE upon receiving a packet, and communicate M latent space features to the sink (over an authenticated channel). The sink then decides on authenticity [14].

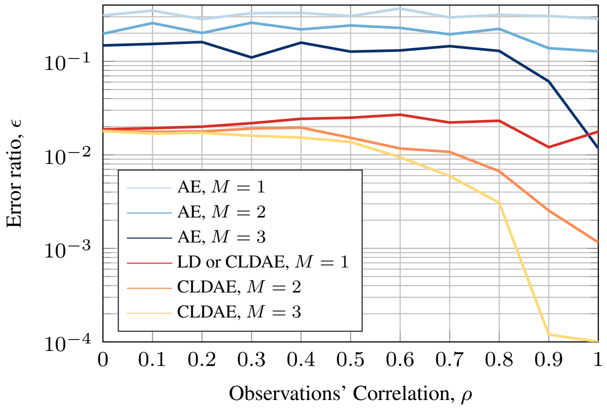

Figure 2. PLS authentication: error ratio vs. the correlation among observations at the trusted node [14].

To train the AEs, we consider (i) a distributed approach, where each trusted node and the sink separately train a local AE; (ii) local decision making (LD), where only the decision is communicated to the sink; (iii) a combination of (i) and (ii), named CLDAE, that separately trains different AEs to extract the M latent space features and make a final decision, and is thus more practical from a complexity and training data collection standpoint.

Our results are based on real UWAC measurements taken in Eilat, Israel, in Jan. 2022, where three stationary buoys act as the trusted nodes, and four drifters represent three legitimate transmitters and one attacker. Fig. 2 shows the classification error ratio ϵ vs. the correlation α among the trusted nodes' measurements. We observe that exploiting the correlation of the channel features makes classification more accurate: $M = 3$ latent space features improve considerably over the $M = 1$ case, whereas further increasing M yields negligibly better results. Moreover, the mixed CLDAE approach outperforms both AE and LD, since it is targeted towards the hypothesis testing problem. Lastly, note that the error probability decreases as α increases: this is due to observing different statistics at different sensors, whereby multiple, highly correlated measurements help reduce the decision uncertainty.

The above scheme requires zero to mild drift-like mobility. For faster, intentional mobility, channel features decorrelate faster over time. We thus expand our approach to explicitly account for the mobility of the legitimate node, and help avoid that authentication fails or that NN training loses relevance over time [15]. Here, we consider the power-weighed average delay of the channel taps as the authentication parameter, which is correlated with the distance between the transmitter and the receiver. We then track the mobility of the legitimate node via a Kalman filter. The difference between the Kalman tracking and the observation of the features provides a good basis for authentication: a good matching indicates a likely authentic packet, whereas bad matching hints at forging.

To evaluate our idea, we consider an attacker that can precode its transmissions to reproduce any channels, even at all of the trusted nodes simultaneously, but makes an error when localizing the legitimate transmitter. This implies that the channel the attacker reproduces may not be fully adequate to impersonate a legitimate network device. Fig. 3 shows false alarm (FA) vs. missed detection (MD) probabilities from a set of simulation carried out with the realistic underwater acoustic ray tracer Bellhop, considering an area of 6×6 km^2 and varying bathymetry. We compare single-sensor authentication (SSA) to three approaches that merge outputs from multiple trusted nodes, namely a linear classifier (LC) against a trained AE and a one-class support vectore machine (OC-SVM). All schemes collect 3 readings per trusted node before making a decision. The results show that higher localization errors improve the capability of the system to differentiate legitimate and forged transmissions. Moreover, due to fast feature decorrelation LC outperforms machine learning approaches. These results prove that PLS yields reliable authentication and leads to practical schemes, based on simple channel impulse response measurements.

2.2 Secret Key Generation

To avoid the scalability issues that arise from pre-installing shared keys and ciphers on a set of devices, a possible secrecy solution is PLS-based key agreement. By exchanging generic probing signals, a legitimate transmitter (Alice) and receiver (Bob) can collect a dataset of channel measurements, e.g., including the channel features described in [10]. Under an (at least partial) channel reciprocity assumption, Alice's and Bob's measurements are correlated and can be processed to extract a common key. The fast time variability of underwater channels then yields different keys over time, from which Alice and Bob can accrue a higher number of secret bits: this approach fits any deployment whose time frame exceeds a few minutes of operations. Moreover, it becomes hard for an eavesdropper (Eve) to predict channel measurements and guess the key.

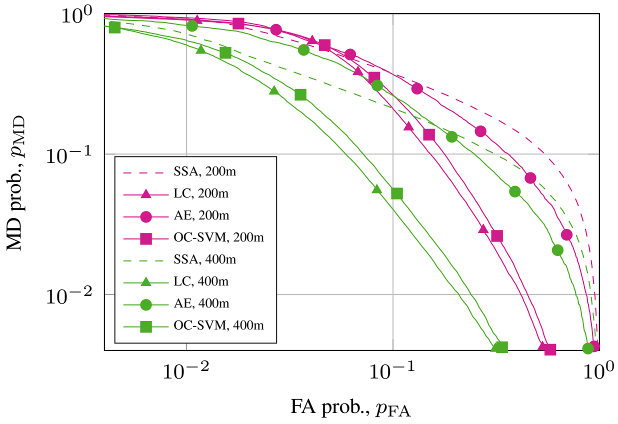

Figure 3. FA vs. MD probability when tracking the feature innovation metric via a Kalman filter [15].

We now discuss new techniques for the advantage distillation step of PLS key agreement. In this step, Alice and Bob (and Eve) quantize channel measurements [11] to extract a bit sequence, that will be the input of the channel reconciliation and privacy amplification steps. Instead of naively quantizing the channel measurements, we propose to exploit channel knowledge to design Alice's and Bob's quantizers and (i) increase Alice's and Bob's reciprocity while (ii) reducing Eve's knowledge about the extracted sequence. We proposed two approaches: one based on quantizer optimization and a second one based on an AE.

2.2.1 *Quantizer Optimization Approch*

In [16] we presented a technique where Alice and Bob jointly optimize their quantizers to maximize the lower bound on the secret key capacity

$$C_{\mathrm{sk}}^{\mathrm{low}} = I(\boldsymbol{s}_{\mathrm{A}};\boldsymbol{s}_{\mathrm{B}}) - \min\left\{I(\boldsymbol{s}_{\mathrm{A}};\boldsymbol{s}_{\mathrm{E}}), I(\boldsymbol{s}_{\mathrm{B}};\boldsymbol{s}_{\mathrm{E}})\right\} \;, \quad (1)$$

where $\boldsymbol{s}_{\mathrm{A}}$, $\boldsymbol{s}_{\mathrm{B}}$, and $\boldsymbol{s}_{\mathrm{E}}$ represent the bit sequence obtained from the quantizers of Alice, Bob, and Eve, and $I(\cdot,\cdot)$ denotes mutual information. In more detail, to converge quickly and save energy, quantizer thresholds are placed in a divide-and-conquer fashion. Quantizers are designed via an adversarial strategy, where Eve and the Alice-Bob pair optimize their quantizers in turns. First

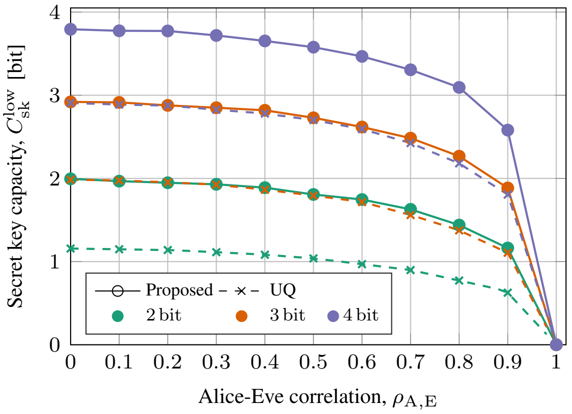

Figure 4. Secret key capacity considering the proposed strategy (solid lines) and a uniform quantizer (dashed), for $b = 2$, 3 and 4 bit, as a function of the correlation between Alice and Eve [16].

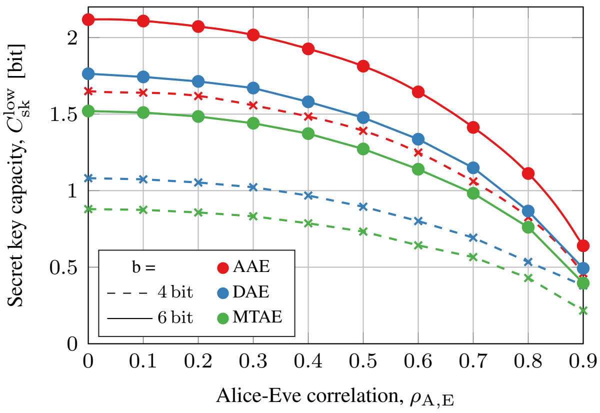

Figure 5. $C_{\mathrm{sk}}^{\mathrm{low}}$ obtained as a function of the correlation between Alice and Eve, for correlation between Alice and Bob, $\rho_{\mathrm{AB}} = 0.9$ for the AAE, DAAE, and MTAE solutions, for b =4 bit and 6 bit [16].

Eve designs her quantizer to minimize (1), thus increasing her knowledge about Alice's (or Bob's) extracted bit sequence. Next, Alice and Bob jointly set their quantizers to maximize (1), increasing the reciprocity between their bit sequences while at the same time making such sequences as different from Eve's as possible.

Fig. 4 shows the secret key capacity as a function of the correlation between Alice's and Eve's observations, ρ_{AE}, considering the average tap power as the quantized channel feature, and extracting $b = 2$, 3, and 4 bit per channel observation. Our quantizer adapts and takes advantage of the common information between Alice and Bob's observations. Moreover, the secret key capacity decreases when ρ_{AE} increases. Still, the proposed strategy outperforms the uniform quantizer for all considered values of ρ_{AE}: for $\rho_{\mathrm{AE}} = 0.9$ and $b = 3$ bit, Alice and Bob harvest 1 more secret key capacity bit using our strategy.

2.2.2 *Autoencoder Approach*

In [17] we proposed an adversarial autoencoder (AAE) approach based on multitask learning: we extract the bit sequence from an NN trained to strike a balance among (i) the reciprocity between Alice's and Bob's measurements, (ii) the uniformity of the extracted bit sequence, and (iii) the eavesdropper leakage, where accounting for the latter reduces the correlation with the sequence extracted by Eve. Training the NN via a uniformity loss function ensures that no information is lost when concatenating the encoder with a uniform quantizer. Fig. 5 compares our AAE to the state-of-the-art domain-AAE (DAE) [18] and the multi-task autoencoder (MTAE) [19] for $b = 4$ and 6 bit. While the secret key capacity expectedly decreases for high ρ_{AE}, our AAE achieves the best results for all considered values of b.

3. BIOMIMICRY

3.1 Biomimetic signal detection and identification

LPD techniques face a key challenge in underwater acoustic communications: the limited bandwidth available often enables interception using energy detection. Even noise-like signals may expose the covert transmitter, because they can be traced by an interceptor to a single location, e.g., via beamforming, whereas ambient noise is assumed to be isotropic. By way of contrast, recent schemes propose biomimetic communications, which hide information in signals that resemble the vocalization of marine mammals. This enables transmissions at high power, as an attacker would believe to be receiving biological sounds. Modulated biomimetic signals have a similar structure as marine mammal vocalizations (e.g., chirplets, clicks, or calls), all of which have a rich, time-varying frequency content.

Detecting biomimetic signals requires an interceptor to classify whether a received vocalization is genuine or forged. Regardless of the communication protocol, the main goal is to find a metric that can tell real and biomimetic signals apart. In the following, we focus on intercepting biomimetic dolphin whistles, although our scheme applies to a broader range of biomimetic signals.

The design of our detector [12] starts from observing that a biological signal's phase is much more diverse compared to biomimetic signals, and even to played-back biological sounds, as acoustic transducers have a limited damping factor. The first step of our procedure is to detect the presence of a whistle-like signal. This can be done with a prior detection procedure such as PAMGuard. Then we extract the statistics of the signal's phase as a clustering metric. We use a phase-locked loop (PLL) to estimate the phase of the signal and calculate its approximate entropy, which quantifies the logarithmic likelihood that sequences of patterns that are close for m observations remain close on next comparisons as well. Such a metric does not depend on an estimate of the signal's probability density function, and can detect breaks in the signal's regularity. Because the energy and phase of whistle-like signals vary over both frequency and time, the PLL can effectively track the phase of the signal only if it operates at a high frequency compared to the signal's bandwidth. This can be guaranteed through passband modulation.

We evaluated the performance of our method by analysing a database of real whistles, and by projecting and receiving biomimetic signals during a sea experiment (both playbacks of real recorded dolphin whistles and synthetic whistle-like signals). A false alarm, in terms of detecting a biomimetic signal, is evaluated by running the interceptor over the real dolphin's whistles. The results are shown in Fig. 6, and show that our method can distinguish well between the real and biomimetic whistles. To the best of our knowledge, this is the first interception technique that can separate between biomimetic UWAC signals and real biological ones.

We also investigated an effective prior detection technique for dolphin whistles, by considering a convolutional NN (CNN). We created a large-scale database of sound recordings via a custom, low-power acoustic recorder anchored at a depth of 50 m, 1.5 m above the seabed, 200 m away from the dolphin's reef in Eilat, Israel. We recorded 27 days of audio during the summer of 2021. Through a quality assurance procedure, we removed sporadic cutoffs, extensive noise periods, and noise transients. We then filtered the frequency range between 5 and 20 kHz (which fits most dolphin whistles) and applied a whitening filter to correct for ripples in the hydrophone's open circuit voltage response and the sound card's sensitivity.

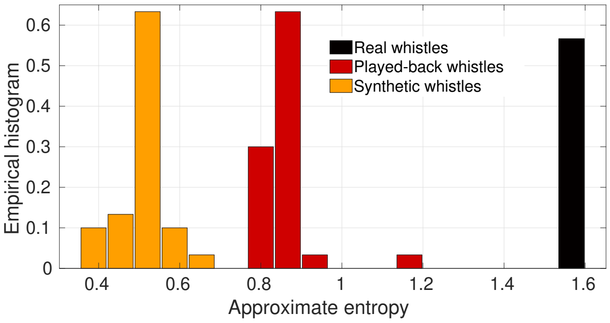

Figure 6. Distribution of the entropy of real, synthetic, and played-back dolphin whistles [12].

Through short-time fast Fourier transforms, we created dolphin whistle spectrograms and manually tagged them to yield a ground-truth dataset. For classification, we considered both a vanilla CNN and a pre-trained CNN based on VGG-16, where we exploited transfer learning and replaced the top layers with two fully-connected layers with 50 and 20 neurons, respectively. Our results show that the vanilla CNN already achieves a remarkable mean detection accuracy of 80.6% (outperforming PAMGuard, which achieves 66.4%). The transfer learning CNN, instead, achieves an accuracy of 92.3%. Although the number of true negatives was comparable across different methods, the number of true positives was significantly higher for deep learning models, especially for the transfer learning architecture.

Finally, in our recent work [20], we extended the approach of using well-known image classification networks as a pre-trained component for dolphin whistle detection. The ultimate objective is to perform automated whistle detection for recording from different underwater environments with as little need for (re-)training of a detector as possible. For this purpose, in [20] we compared detectors using different image classification networks and developed models which perform comparably to or better than existing methods. Our designs use minimal data pre-processing and instead rely on the generalization capabilities of the neural network to adapt to the environmental conditions. This was shown to be more effective than applying, e.g., noise reduction techniques. We tested our approach on the dataset described above and a dataset from the 8th DCLDE workshop [21]. In particular, we pre-trained the detector model on one data set, retrained it with a small amount of data from the second data set, and tested on the second data set. Our results show that the benefit of pre-training is an increasingly more stable detection and false-alarm rate performance for increasing size of the retraining data set. Our approach supports the idea that transfer learning from one dataset to another is likely taking place.

3.2 Generative approaches to biomimicry

Biomimetic signal generation methods for covert communications typically fall into one of two categories. The first uses analytical models to represent modulated biological sounds that carry data. Data modulation would be applied in terms of shaping the waveform and/or the timing of successive waveforms while retaining similarity with the biological sounds, e.g., [22–24]. In the second category, original waveforms are used to directly generate biomimetic signals [25], possibly after denoising. This retains a great level of waveform authenticity, albeit detection is possible due to the properties of acoustic projectors [13].

In our work, we pursue a learning-from-data approach for biomimetic signal generation that lies in between the two above categories. We use machine learning models trained on biological waveforms to generate biomimetic signals. The first potential benefit of our approach is a greater versatility in mimicking biological signals. Moreover, it can improve over plain replay by also accounting for projector characteristics, i.e., via pre-distortion.

A few choices need to be made when applying learning. First, what data is used for learning? Recorded acoustic waveforms or their transformations could be used as input. For the latter, spectrograms seem to be a reasonable choice, as spectrogram-based signal detection has been shown to be highly effective. Second, how are waveforms extracted from recordings? One could train a model with the original recordings, but background noise would effect the training process. Alternatively, extraction or denoising techniques could be applied. The latter is attractive for effective training, but it may introduce distortions to the original waveform.

Generative adversarial networks (GANs) [26] and their variants seem to be a natural choice. However, our experience with GANs for the case of dolphin whistles and training based on spectrograms has been unsatisfactory. It seems that the sparse nature of the time-frequency representation of the waveform is a challenge for GANs. We are therefore focusing on alternative generative models that use efficient latent variable models to capture the basic signal structure and use it for generation.

4. TRANSCEIVERS FOR UNDERWATER CYBERSECURITY

The SAFE-UComm project aims to practically demonstrate some of the security concepts described above using low cost, ultra-low power acoustic modems [27] developed for Internet of Underwater Things (IoUT) applications. These spread spectrum modems, although software defined, have limits on available processing power and memory, so algorithms must be computationally light. Key enablers for physical layer security are i) rapid and accurate measurement of the channel impulse response (CIR) between two network nodes; and ii) simultaneous bidirectional channel estimation for reciprocal channel features.

The existing modems did not require channel estimation in the receiver so this function had to be added. It was also desirable to achieve this without adding overhead for additional channel probing waveforms in the transmitted data packets. The initial implementation relies on the cross correlation of header symbols at the start of data packets, consisting of random binary phase shift keyed (BPSK) chips. This approach delivers useful CIR for most purposes but, since the chip sequence has non-ideal autocorrelation properties, sidelobe artefacts appear, which also vary with the header data. These are a potential problem for channel-based authentication or key generation.

A better approach has proven to be a simple direct adaptive filter model [28] using the header data as a training sequence. Figs. 7 and 8 show a comparison of the two methods on a relatively benign channel, where the reduction in artefacts is obvious. This leads to clearer discrimination of channel features, such as RMS delay spread, with range shown in Figs. 9 and 10 from North Sea experiments. This approach is also computationally light and being incorporated in code for upcoming experiments.

For authentication or key generation, it is important that the channels observed by the two nodes involved in an exchange are as closely matched (reciprocal) as possible. Hence protocols have been developed to enable a synchronized channel estimation message exchange. In this case, short acoustic packets cross each other in the medium, enabled by the low propagation speed of sound, to ensure that the channel is observed by both nodes at the same point in time. This exploits the modem's built-in ranging function, which can measure time of flight to a resolution of 62.5 µs, to calculate transmission time offsets for a synchronized exchange.

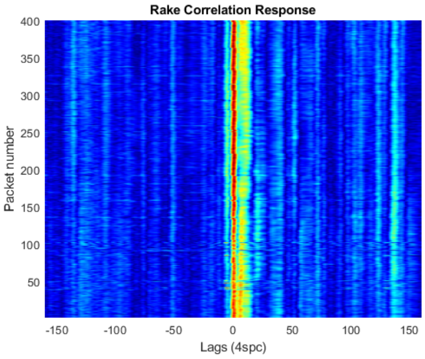

Figure 7. Time evolution of CIR by correlation.

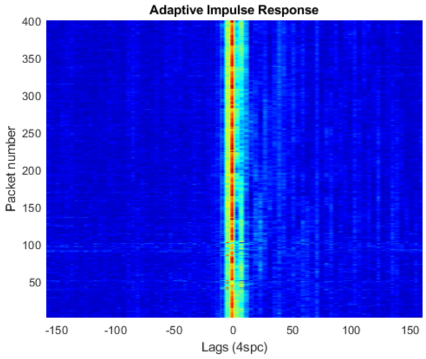

Figure 8. Time evolution of CIR adaptive model.

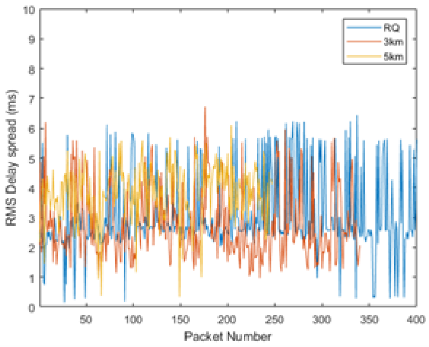

Figure 9. Channel feature by correlation.

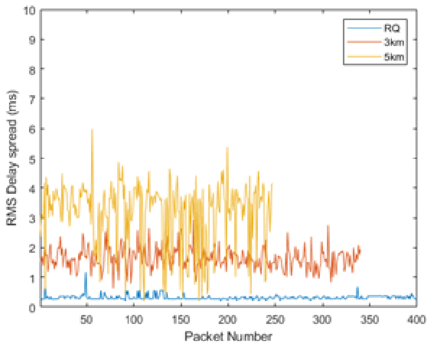

Figure 10. Channel feature by adaptive model.

5. DISCUSSION AND CONCLUSIONS

The ever-increasing capabilities of underwater sensors and autonomous devices makes security issues more pressing. The NATO SPS SAFE-UComm project tackled these issues by targeting distributed authentication and privacy techniques, that make use of physical layer security rather than relying on closed-box cyphers. Moreover, the project investigated the reliable generation and detection of biomimetic signals, where security lies in the low probability of identifying information-carrying signals disguised as natural sounds. A number of preliminary results so far confirm the effectiveness of these approaches and their applicability in practical scenarios.

For the final demonstration of SAFE-UComm, scheduled at the end of September 2023, we plan to close the loop between theory and practice. Thanks to the embedded CIR measurement capabilities of Newcastle University's underwater acoustic modems, we plan to extract secret keys from the parameters of their statistical distribution of CIR features. According to our experience in [10], this choice increases the likelihood that independent measurements by Alice and Bob align.

6. ACKNOWLEDGMENT

This work was sponsored in part by the NATO Science for Peace and Security Programme under grant no. G5884 (SAFE-UComm), 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).

7. REFERENCES

[1] J. Potter *et al.*, "The JANUS underwater communications standard," in *Proc. UCOMMS*, Sept. 2014.

[2] G. Han *et al.*, "Secure communication for underwater acoustic sensor networks," *IEEE Trans. Mobile Comput.*, vol. 53, pp. 54–60, Aug. 2015.

[3] M. Zuba *et al.*, "Vulnerabilities of underwater acoustic networks to denial-of-service jamming attacks," *Wiley Security and Commun. Netw.*, vol. 8, Nov. 2015.

[4] A. Signori *et al.*, "A geometry-based game theoretical model of blind and reactive underwater jamming," *IEEE Transactions on Wireless Communications*, vol. 21, no. 6, pp. 3737–3751, 2022.

[5] G. Qiao *et al.*, "Biologically inspired covert underwater acoustic communication: a review," *Phys. Commun.*, vol. 30, Oct. 2018.

[6] Y. Huang *et al.*, "Channel frequency response-based secret key generation in underwater acoustic systems," *IEEE Trans. Wireless Commun.*, vol. 15, Sept. 2016.

[7] Z. Shen *et al.*, "A local pilot auxiliary key generation scheme for secure underwater acoustic communication," *Information Sciences*, vol. 473, 2019.

[8] K. Pelekanakis *et al.*, "Physical layer security against an informed eavesdropper in underwater acoustic channels: Feature extraction and quantization," in *Proc. UCOMMS*, 2021.

[9] M. Xu *et al.*, "Multi-party secret key generation over underwater acoustic channels," *IEEE Wireless Commun. Lett.*, vol. 9, July 2020.

[10] R. Diamant *et al.*, "Cooperative authentication in underwater acoustic sensor networks," *IEEE Trans. Wireless Commun.*, vol. 18, Feb. 2019.

[11] R. Diamant *et al.*, "Topology-based secret key generation for underwater acoustic networks," in *Proc. UCOMMS*, 2021.

[12] I. Davidesco and R. Diamant, "Detection of dolphin whistle-like biomimicking signals by phase analysis," *IEEE Access*, vol. 10, 2022.

[13] P. Casari *et al.*, "Acoustic projectors make covert bioacoustic chirplet signals discoverable," *Sci. Rep.*, vol. 13, 2023.

[14] L. Bragagnolo *et al.*, "Authentication of underwater acoustic transmissions via machine learning techniques," in *Proc. IEEE COMCAS*, 2021.

[15] P. Casari *et al.*, "Physical layer authentication in underwater acoustic networks with mobile devices," in *Proc. ACM WUWNet*, 2022.

[16] F. Ardizzon *et al.*, "Adversarial learning for advantage distillation in secret key agreement over UWAC," in *Proc. IEEE ICC Workshops*, 2023. In press.

[17] A. Giuliani *et al.*, "ML-based advantage distillation for key agreement in underwater acoustic channels," in *Proc. IEEE ICC Workshops*, 2023. In press.

[18] J. Zhou *et al.*, "Physical-layer secret key generation based on domain-adversarial training of autoencoder for spatial correlated channels," *Applied Intelligence*, vol. 53, June 2022.

[19] J. Zhou *et al.*, "Physical layer secret key generation for spatially correlated channels based on multi-task autoencoder," in *Proc. ICSP*, pp. 144–150, 2022.

[20] X. Lu *et al.*, "Transfer learning of image classification networks in application to dolphin whistle detection," in *Proc. MTS/IEEE OCEANS*, 2023.

[21] "8th DCLDE workshop – dataset challenge," 2018. http://sabiod.lis-lab.fr/DCLDE/challenge.html.

[22] S. Liu *et al.*, "Biologically inspired covert underwater acoustic communication using high frequency dolphin clicks," in *MTS/IEEE OCEANS*, pp. 1–5, 2013.

[23] A. ElMoslimany *et al.*, "An underwater acoustic communication scheme exploiting biological sounds," *Wireless Commun. Mobile Comput.*, vol. 16, no. 15, pp. 2194–2211, 2016.

[24] G. Qiao *et al.*, "Biologically inspired covert underwater acoustic communication—A review," *Phys. Commun.*, vol. 30, pp. 107–114, 2018.

[25] J. Jia-jia *et al.*, "Bio-inspired steganography for secure underwater acoustic communications," *IEEE Commun. Mag.*, vol. 56, no. 10, pp. 156–162, 2018.

[26] I. Goodfellow *et al.*, "Generative adversarial nets," in *Proc. NIPS*, pp. 2672–2680, 2014.

[27] B. Sherlock *et al.*, "Ultra-low-cost and ultra-low-power, miniature acoustic modems using multipath tolerant spread-spectrum techniques," *Electronics*, vol. 11, 2022.

[28] B. Widrow *et al.*, *Adaptive Signal Processing*. Prentice-Hall, 1985.