Physical Layer Authentication via Underwater Acoustic Multipath Channel Crafting

Davide Eccher
Dept. of Information Engineering and Computer Science
University of Trento
Trento, Italy
davide.eccher-1@unitn.it

Paolo Casari
Dept. of Information Engineering and Computer Science
University of Trento
Trento, Italy
paolo.casari@unitn.it

***Abstract*—With the increasing number of actors in the underwater environment and the development of new applications, such as large-scale monitoring and autonomous underwater vehicle control, securing underwater communications is becoming a primary necessity. Security was not prioritized in the past due to the constraints of underwater acoustic communications, which cannot sustain the overhead of typical cryptographic techniques. In this paper, we propose a method to authenticate a network device by exploiting the physical properties of the acoustic channel. In particular, our method hinges on the uniqueness and quasi-reciprocity of the channel, from which the authenticator (Alice) node can extract several parameters such as the number of multipath channel components, their delay and amplitude. These values are similar on both ends of a link between Alice and a legitimate transmitter (Bob), and can be used as a seed to craft a new artificial channel, that is then applied to transmissions from Bob to Alice. With this procedure, Alice can distinguish Bob from an impersonating attacker (Eve), given a previous message exchange history. Eve can try to bypass the protocol by estimating the channel parameters and by trying to replicate Bob's signal by crafting a similar channel. In our tests, we observe that the estimation error for Eve, caused by her wrong channel estimates, becomes significant even for short distances betwen Eve and Bob. This error results in a discrepancy between the signal generated by Eve and the one expected by Alice, and reveals Eve as an attacker.**

***Index Terms*—Underwater acoustic networks; physical layer security; authentication; channel crafting; simulation; performance evaluation**

I. Introduction

Underwater wireless acoustic communications and networks can enable many key applications, such as marine environment monitoring, diving and navigation safety, sensor data telemetry, coordination among underwater vehicles, and the protection of strategic infrastructure. In several cases, these applications may include mission-critical or security-critical operations, that must be protected against external intrusion or eavesdropping. This, necessitates the development of new solutions and protocols that provide security features, a need that becomes more pressing as the first standards for underwater acoustic modem interoperability emerge. A notable example is JANUS [1], which provides a common modulation format, and facilitates the coordination of communication settings between modems to enable the transmission and decoding of packets among different systems. The presence of standards increases the attack surface for potential malicious actors, but it also offers an opportunity to create and rapidly disseminate effective security standards.

Several functions must be implemented to ensure that an underwater network can operate normally even in the event of external attacks. The main functions typically provided include [2]:

- Authentication: Verifying that a communicating device or user is a legitimate network member.
- Confidentiality: Protecting the privacy of transmitted information.
- Integrity: Identifying or correcting errors and data tampering during transmissions.
- Non-repudiation: Preventing a sender from denying that it had performed a transmission.

In this paper, we focus on the development and evaluation of a protocol aimed at the authentication of nodes in an underwater acoustic network. The typical methods used in terrestrial wireless networks primarily rely on cryptographic functions which, although highly secure, require substantial computational power and add significant communication overhead. Typically, an underwater node lacks these capabilities. Underwater device design usually prioritizes energy efficiency to ensure prolonged unattended operations and reduce power supply or maintenance costs. Additionally, since acoustic waves are used for packet transmission, bandwidth is limited, necessitating protocols that minimize overhead.

For the above reasons, traditional cryptographic methods cannot be straightforwardly applied to underwater networks. The literature approaches the problem in two main ways. The first is by means of lighter cryptographic functions that can be executed by the hardware of an underwater node [3]. Simplifying these functions may make them less robust against attacks with respect to their computationally more complex terrestrial network counterparts. However, they may be still applicable and effective in those scenarios where a potential attacker has a similar computational power as that of legitimate network nodes. The second approach leverages the characteristics of the underwater acoustic channel, and specifically its quasi-reciprocity, fast decorrelation over time, and negligible correlation in space [4]. Such properties make it possible to use

the channel characteristics as a common source of randomness for two communicating parties to extract a shared secret in a physical layer security fashion [5], [6], and replaces the use of higher-layer cryptographic functions.

Our proposed method in this paper aligns with the second approach. We consider a scenario where an underwater device (conventionally, Alice) receives a message from another device (Bob) and needs to authenticate Bob's identity. The main novelty of our scheme is that Bob and Alice communicate by crafting a completely new channel impulse response (CIR) that distorts the transmitted signals before they pass through the physical channel. In order to do so, the legitimate nodes perform channel measurements and derive the pre-distorting CIR from a seed obtained by processing the amplitude and delay of each multipath component in the measured channel responses. As the legitimate nodes likely observe similar communication channels, it will be easy for them to recognize and remove the pre-distortion. On the contrary, an external attacker (Eve) would observe practically uncorrelated channels, and would not be able to impersonate a legitimate node by replicating the correct crafted channel.

Assuming that the reception of the message from Bob is successful from a communications standpoint, Alice now needs to authenticate Bob's identity. To do so, she compares the received signal against an estimate of the signal she *would* receive from Bob, given a history of previous communications. Having such a history available, Alice can use the channel measurements from previous transmissions and generate the artificial CIRs that Bob would use to pre-distort the signal, under the assumption that previously measured channel realizations are at least partly representative of current channel conditions. Alice can then authenticate Bob by ensuring that the locally generated signal and the received signal are not exceedingly different.

Because underwater channels may vary over time, we design an authentication function that is robust to such changes, under the assumption that the entity of channel variations over time will be significantly smaller than the difference between channels measured at different locations. This method provides robustness against attack attempts made by transmitting signals from locations different from Bob's.

In this paper, we present and analyze two different channel crafting methods. The first involves quantizing the delay and amplitude values of the most significant taps of an observed underwater channel realization. These values are passed through a hash function and then used to generate the multipath components of the crafted underwater channel. Quantization helps reduce channel measurement differences due to the channel variations or measurement inaccuracies. The second method, instead of eliminating these errors, aims to amplify the estimation errors made by an external attacker. The delay and amplitude values are passed through a continuous periodic function designed to maintain locality, thereby being robust to small discrepancies while being difficult to invert.

We show that Eve's channel estimation error leads to a significant error in the creation of the crafted channel, even when Eve is located at a short distance from Bob. We exploit the discrepancy that ensues to identify Eve and authenticate Bob, balancing the trade-off between identification accuracy and authentication probability.

The remainder of this paper is organized as follows, in Section II we briefly present the state of the art in authentication for underwater acoustic networks, in particular physical layer authentication methods. In Section III we describe our proposed method with a focus on the channel crafting process (Section III-D). Then, we explain how the simulations were conducted and we show the obtained results in Section IV, before drawing conclusions in Section V.

II. Related work

Common encryption solutions currently implemented in terrestrial radio networks cannot be straightforwardly ported to the underwater environment, mainly due to the limited computational resources and data rates available to underwater devices. These limitations primarily originate from the instability of the underwater channel and from the limited bandwidth available for acoustic transmissions, which constrain the communication bit rate. Moreover, the hardware of the underwater devices typically prioritizes energy efficiency and infrequent maintenance during underwater operations, resulting in computational constraints.

A potential solution is to employ cryptographic methods that require fewer resources to operate, typically by accepting a reduced degree of robustness. If an attacking underwater node cannot count on heavy computational resources these reduced-complexity cryptographic methods can be considered a viable alternative. An example of this approach is presented in [3], where the authors implement a key exchange protocol that does not require resource-intensive algorithms like RSA. Once the keys are obtained, more traditional authentication and encryption methods can be utilized that match the needs of underwater communications.

Furthermore, physical layer security methods have been proposed as a valid alternative to directly embed security functions into communication signals. Besides imposing a low computational overhead, practical physical layer security solutions should also be aware of the high acoustic channel variability and of its dependency on the water conditions, bathymetry, and seabed. Several recent works, such as [6] and [5], proved that is possible to exploit the acoustic CIR to generate a shared secret starting, e.g., from the number, power, and delay of the multipath channel components. This is possible thanks to the uniqueness and quasi-reciprocity of the CIR perceived by two communicating nodes. Previous solutions described in [7] and [8] exploit the channel impulse response properties to distinguish between two different transmitting nodes. In this case, the scheme authenticates the node by comparing the received channel parameters against previous values stored in a table. Other techniques found in the literature leverage machine learning algorithms for authentication. For instance, in [9], the same physical channel parameters used in previous solutions are used as input to a model that is

trained to distinguish signals between a legitimate node and an attacker. Another approach, shown in [10], aims to compensate for channel variability by predicting the channel's evolution, thereby enabling a more effective comparison between the received and the expected signals. This prediction is carried out using a recurrent neural network (RNN) that takes as input the channel characteristics from previous transmissions and extrapolates the trend of its evolution. Additional solutions to the authentication problem can be found through the use of supplementary hardware. The method described in [11] utilizes specialized hardware to measure the angle of arrival of a signal, which is then used as a comparison parameter for authentication, similar to how the channel multipath component are used in the previously discussed methods. Another possibility involves using multiple nodes to perform authentication cooperatively, as demonstrated in [4]. This makes it significantly more challenging for an attacker to estimate and mimic multiple channels simultaneously across different receiver nodes.

Unlike the approaches in [11] and [4], our objective is to develop a protocol that does not rely on specialized hardware or an external infrastructure for the authentication process. Therefore, we employ a method that leverages physical layer security. However, unlike other physical channel-based authentication methods, we do not compare the instantaneous channel measurement with an estimation made by the node based on prior receptions. Instead, we compare differences between crafted channels. The crafting methods are based on the statistics of the channel's multipath components that are temporally more stable than their instantaneous values, thus mitigating the volatility of the underwater acoustic channel.

III. Proposed method

A. Key idea

While the authentication protocol we propose in this paper is also based on underwater channel properties, we resort to *manipulating* such properties rather than just measuring them. Our solution combines the comparison of received CIRs against previously measured CIRs [7], and the generation of a shared secret that can be verified by the receiver.

We rely on the statistics the multipath components' amplitude and delay, which are proven in [4] to be resilient to the constantly changing nature of the acoustic channel. Moreover, we use only the most significant arrivals of the channel impulse response to obtain even more stable parameters and avoid small fluctuations. These values are used as a seed to craft a new CIR, which will constitute the shared secret. Thanks to this configuration, we achieve a high probability that the CIRs match at both the legitimate transmitter and receiver, while being very difficult to predict by an attacker located elsewhere. We detail the transmitter- and receiver-side operations of our method in the following.

B. Preliminary assumptions

We assume that Alice and Bob communicate using a typical signal format where a broadband preamble (e.g., a full-band chirp) precedes the modulated symbols for receiver wake-up, synchronization or channel estimation purposes. We also assume that Alice and Bob have initially authenticated each other via a higher-layer method and that they possess a (short) history of previously authenticated communications. Both Alice and Bob maintain a local estimate of CIR features measured from their respective received signals. These estimates are recorded in a table that contains the n sets of pairs (c_j, τ_j), $j = 1, \ldots, n$, one for each of the n strongest multipath components detected, where c_j represents the complex amplitude of the jth component, and τ_j the arrival delay of the jth component relative to the delay of the earliest arrival. These tables are called $\mathcal{M}_a$ and $\mathcal{M}_b$ at Alice and Bob, respectively. In order to extract these n components, Alice and Bob apply a correlation filter with respect to a reference signal and then find the most significant peaks corresponding to the multipath components.

For each newly acquired channel estimate, e.g., from the preamble of a received packet, Alice and Bob update the above quantities by means of exponentially weighed moving averages. For instance assume that, after the kth channel estimate, Alice has extracted the n strongest multipath components having amplitude and delay (c_j^*, τ_j^*), $j = 1, \ldots, n$. Alice then updates its local table $\mathcal{M}_a$ as

$$\begin{aligned} c_j[k] &= (1-\alpha)c_j[k-1] + \alpha c_j^* \ , \\ \tau_j[k] &= (1-\alpha)\tau_j[k-1] + \alpha \tau_j^* \ . \end{aligned} \tag{1}$$

In the following, we focus on Alice having to authenticate a transmission received from Bob.

Finally, we assume that no CIRs or features thereof are ever transmitted from Alice to Bob or vice-versa, to avoid disclosing identity-sensitive information that would improve the probability of successful impersonation attacks.

C. Authentication procedure

When Bob has to transmit a signal to Alice, he applies a crafting function $\mathcal{C}(\cdot)$ which takes $\mathcal{M}_b$ as an input. The result is the crafted CIR $h_{\text{craft}}(t, \mathcal{C}(\mathcal{M}_b))$ starting from the channels measured from past signals sent by Alice. Assume for the moment that $h_{\text{craft}}(t, \mathcal{C}(\mathcal{M}_b))$ is available to Bob. We delay the discussion on how to obtain it to Section III-D.

Bob transmits a pre-distorted signal by convolving it with the crafted CIR as

$$s(t) = u(t) * h_{\text{craft}}(t, \mathcal{C}(\mathcal{M}_b)) \ , \tag{2}$$

where $u(t)$ is the non-distorted transmit signal (including both the preamble and the modulated symbols), and $*$ denotes convolution. The signal that Alice receives undergoes further distortion from the impulse response $h_{\text{ba}}(t)$ of the physical acoustic channel between Bob and Alice:

$$r(t) = s(t) * h_{\text{ba}}(t) + n(t) \ , \tag{3}$$

where $n(t)$ represents additive noise at the receiver. Assuming that Alice receives the modulated symbols correctly and decodes the corresponding bits, she is now in a position to

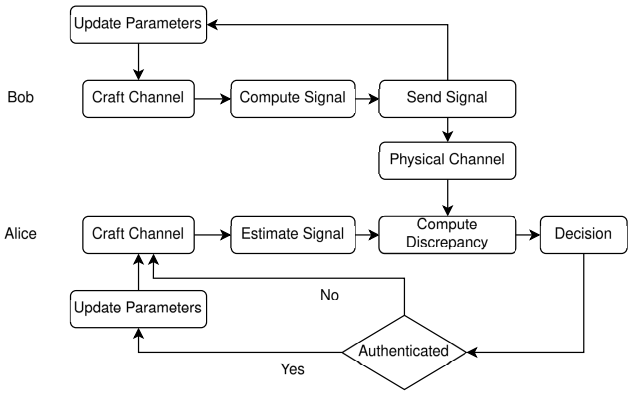

Fig. 1. Block diagram showing the steps of the proposed method.

prepare an estimated copy $\hat{h}_{\text{craft}}\left(t, \mathcal{C}\left(\mathcal{M}_a\right)\right)$ of the original signal transmitted by Bob

$$\hat{r}(t) = u(t) * \hat{h}_{\text{craft}}\left(t, \mathcal{C}\left(\mathcal{M}_a\right)\right) * \hat{h}_{\text{ba}}(t) \ , \tag{4}$$

In (4), Alice exploits a local estimate of $h_{\text{ba}}(t)$ obtained from the preamble of the received signal, and relies on the history of previous communications with Bob in order to derive the crafted multipath components $\mathcal{M}_a$. We note that Alice obtains $\mathcal{M}_a$ by measuring the Bob→Alice channel, whereas Bob computes $\mathcal{M}_b$ by measuring channels from Alice→Bob transmissions. This implies at least an assumption of quasi-reciprocity between the CIRs in the two directions, which must be accounted for during channel crafting operations. Doing so ensures that $\mathcal{M}_a$ and $\mathcal{M}_b$ agree, and at the same time avoids leaking CIR information to attackers.

Then, Alice measures the difference between the received signal and the estimated one, by sampling both signals and computing a mean squared error (MSE) as

$$e = \frac{1}{n}\sum_{i=1}^{n}(r[i] - \hat{r}[i])^2 \ . \tag{5}$$

Alice then computes the mean μ_e and variance σ_e^2 of the MSE over a window of k previous values, and authenticates Bob by comparing the current MSE e against a threshold as

$$\theta = \mu_e + \beta\sigma_e^2 \ , \tag{6}$$

where β can be tuned to increase the tolerance of the authentication process to discrepancies between Bob's crafted channel and Alice's estimate thereof. Only if Bob is finally authenticated, does Alice proceed to update $\mathcal{M}_a$ per the procedure in Section III-B.

D. Channel crafting

We propose two different methods to implement the crafting function $\mathcal{C}\left(\cdot\right)$ starting from a measured CIR. The first method quantizes the values of the amplitude and delay of each detected multipath component, concatenates such values into a single seed, and passes the seed through a hash function $H(\cdot)$ as

$$H\left(\bar{c_1}|\bar{\tau_1}|\bar{c_2}|\bar{\tau_2}|\cdots|\bar{c_n}|\bar{\tau_n}\right) \ , \tag{7}$$

where the bar on top of a quantity indicates quantization and $|$ denotes the concatenation of the corresponding bit sequences. Here, we resort to an implementation of the SHA-256 function. The delays and amplitudes are generated through an iterative process. Starting from an initial delay of zero, each step generates a new amplitude and a new delay, which is added to the previous one. This process continues until it reaches a predefined maximum delay or a maximum number of taps. These values are generated using the previously introduced hash function, specifically employing an incremental salt for each new value. The results are then passed through a module function, establishing a maximum window for both the amplitude and the distance between consecutive taps. Finally, the amplitude values are normalized. We remark that the above quantization approach is a commonplace baseline, but it increases the likelihood of discrepancies between the crafted channels of Alice and Bob [12], thereby hindering a successful authentication outcome without a reconciliation overhead [13]. To solve this issue, we now present a different approach that focuses on maintaining locality, so that a small change in the input CIR will cause a small change in the crafted one. In order to preserve the desirable property that inverting this transformation should be computationally challenging, we exploit the following continuous periodic function

$$f(x) = \left|\text{mod}(x, W) - \frac{W}{2}\right| \ , \tag{8}$$

where, with a little abuse of notation, we define M as an arbitrarily large number, and indicate the modulus of a real number x with respect to a window W as the remainder of the integer division between Mx and W, divided by M.

As for the first method, multipath component values are input to $f(x)$ and the results are used as a seed to generate the new channel. In particular, this seed is composed of the amplitude and delay components of the original channel to which $f(x)$ is applied. Subsequently, each new delay and amplitude value is calculated by applying the module function within a specified window. This window is derived from the sum of the components of the original channel, with each tap using a different, predefined fraction of it. Finally, all values are summed with weights proportional to the original amplitudes, thereby preventing minor components from causing excessive changes in the crafted channels and helping maintain locality. All channels generated by this function have a fixed number of taps. It is not feasible to ensure a high probability that the generated number matches at both ends of the channel without using quantization or leaking information about the original channel, such as its original number of taps. However, our method is designed not to seek perfect correspondence (e.g., unlike secret key generation methods) but rather to minimize discrepancies between Alice's expected channel parameters and Bob's crafted channels, while amplifying the differences against an attacker that does not possess a sufficiently accurate estimate of the channel parameters.

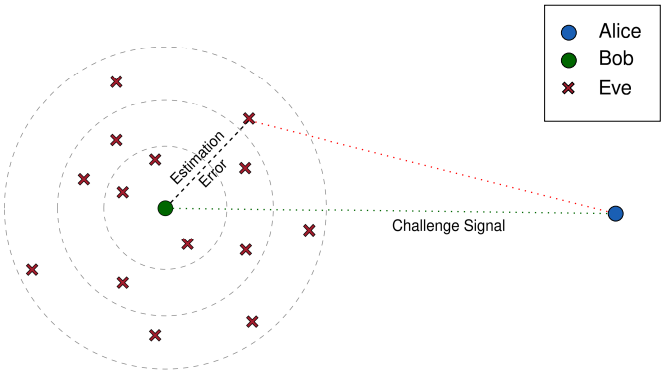

Fig. 2. Simulation scenario. An attacker, Eve, sends a challenge signal to Alice attempting to craft the same impulse response that Bob would craft, but its capability to replicate Bob's signal is affected by errors caused by acoustic channel de-correlation in space.

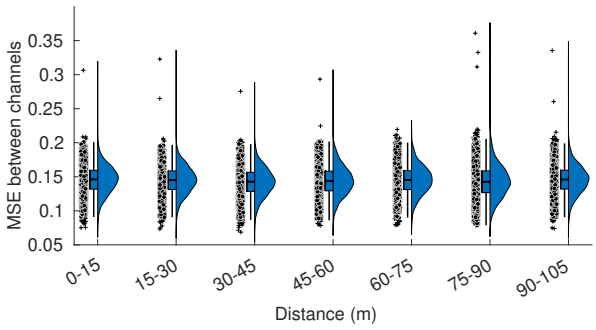

Fig. 3. Error distribution between the estimated signal and the received one from Eve at different distances.

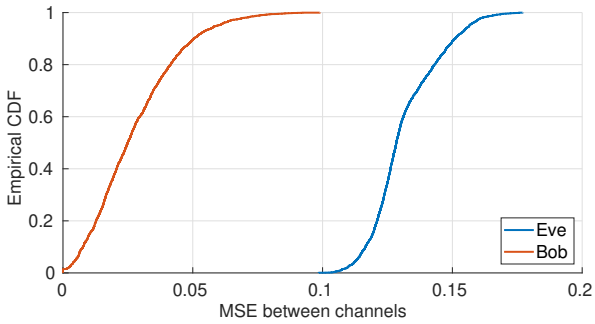

Fig. 4. Empirical CDF of the MSE between Alice's expected CIR and the CIR measured from Bob's signal (red) and from Eve's signal (blue).

E. Attacker model

In order to break the protocol, the impersonating attacker Eve must reproduce the same signal that Bob transmits to Alice. For this, it must estimate the channel between Bob and Alice, which is not trivial even at short distances from the nodes due to the vanishing spatial correlation of underwater acoustic channels. This operation is needed for Eve to compute the same shared secret and finally generate the signal that the Alice expects. In our simulations, the attacker positions itself close to Bob in order to attempt replicating its channel conditions, using the measured CIR as an estimate of the CIR between Bob and Alice.

IV. Simulations Results

A. Simulation setup

In our simulations, we generated random CIRs based on simulated acoustic channels in the San Diego Bay Area. In every scenario, we draw the location of the transmitter (Bob) and of the authenticating receiver (Alice) at random within an area of size 2 km×2 km. We also draw the location of the attacker (Eve) uniformly at random within a ring of increasing radius around the Bob (see Fig. 2).

In the simulations, the nodes move according to a Gauss-Markov mobility model with high self-correlation, such that the trajectory of each node emulates a gentle drift. Each simulation is composed of multiple time instances where the positions of the nodes and then the channel impulse response between the nodes are computed, so as to complete the exchange of messages required by our authentication approach. The simulation alternates transmission by Bob and by Eve and the final performance is evaluated based on Alice's capability to distinguish Bob's transmissions from Eve's.

When not otherwise stated, we set $\alpha = 0.25$ in (1), $\beta = 1.5$ in (6), and $k = 15$.

B. Results

We start from Fig. 3, which shows the MSE between the channel Alice expects given Bob's past transmissions, and the channel measured from Eve's signal. The figure shows boxplots (where the box spans the interval between the 1st and 3rd quartiles of the MSE distribution, and the whiskers span the 10th-90th percentile interval), along with the empirical distribution of the data and a scatterplot that highlights data concentration intervals (dots) and outliers ("+" markers). Different distance ranges between Eve and Bob are considered on the x-axis.

We observe that the MSE has a similar distribution irrespective of the distance between Eve and Bob. However, the mean MSE tends to increase slightly with increasing distance and its statistical dispersion also increases, with additional outliers representing higher MSE values. The consistency of the error that Eve makes is due to the spatial decorrelation of the acoustic channel, which increases the difference between the delays and amplitudes of the taps already whenever Eve is not positioned exactly at Bob's location.

Having observed that Eve makes errors when attempting to reconstruct Bob's crafted CIR, we now check whether this error is significant by comparing it against the error Alice measures between her expected CIR and the one she estimates from Bob's signal. This comparison is shown in Fig. 4, which depicts the empirical cumulative distribution function (CDF) of the MSE of Bob and Eve. The figure shows that the error Alice measures upon receiving a transmission from Eve distributes to greater values than the error due to a reception from Bob. The two CDFs are almost perfectly separate, showing

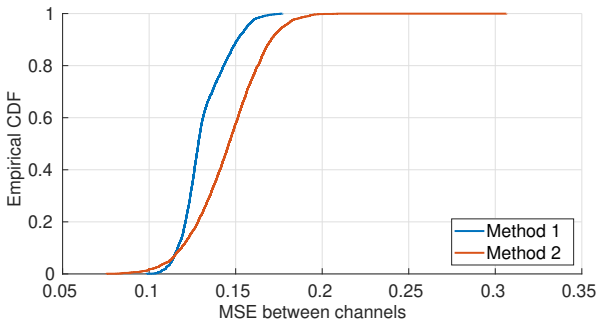

Fig. 5. CDF of the channel MSE after a reception from Eve using the two different channel crafting methods proposed.

that our channel crafting method facilitates the discrimination between legitimate and impersonating transmissions.

As a last comparison, we now discuss the performance of the two channel crafting methods (Fig. 5), by noting that method 2 yields a broader dispersion of the MSE between the channel expected by Alice and that crafted by Eve, including much larger maximum values. This helps in the authentication process and is a consequence of the use of the periodic function in (8), which tends to amplify small discrepancies between the amplitude and delay of expected and crafted multipath channel components. Conversely, with method 1, sufficiently small channel crafting errors by Eve may be rounded off as a result of quantization, yielding a higher probability that the expected and crafted channels match.

Finally, simulations show that the noise level does not significantly affect the authentication performance, as long as it allows the devices to identify the most significant taps of the measured acoustic channels.

V. Conclusions

We have presented a protocol that leverages the multipath characteristics of the underwater acoustic channel to enable a device, Alice, to authenticate a transmitter, Bob, while detecting an impersonating attacker, Eve. The protocol exploits the reciprocity and uniqueness of the multipath phenomena, enabling us to use the statistics of the multipath channel components, in particular their delay and amplitude, as a proxy for the transmitter's identity. Our approach implements a novel method to exploit this secret shared by Bob and Alice. We use the secret as a seed to craft a new channel that will be applied to a reference signal sent by Bob. Upon reception, Alice compares the received signal against an expected channel realization computed from a history of previous communications.

Our results indicate that Eve makes a relevant error in the estimation of the channel between Bob and Alice, even when it is located at a relatively short distance from Bob. This error leads to significant differences in the crafted channel, which are observed both when using the hash-based and when employing the locality-preserving channel crafting functions, where the latter further amplifies the estimation errors. By managing the trade-off between accuracy and robustness, these discrepancies enable the authentication of Bob and the rejection of Eve. Future work will explore different metrics and decision techniques that are more robust against channel instability, with the overarching goal of enhancing accuracy.

Acknowledgment

The authors warmly thank EvoLogics for the support and discussion on this research topic. This work was partially supported by the European Union under the Italian National Recovery and Resilience Plan (NRRP) of NextGenerationEU, partnership on "Telecommunications of the Future" (PE00000001 - program "RESTART").

References

[1] J. Potter, J. Alves, D. Green, G. Zappa, I. Nissen, and K. McCoy, "The janus underwater communications standard," in *2014 underwater communications and networking (UComms)*. IEEE, 2014, pp. 1–4.

[2] S. Jiang, "On securing underwater acoustic networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 729–752, 2018.

[3] S. Zhang, X. Du, and X. Liu, "A secure remote mutual authentication scheme based on chaotic map for underwater acoustic networks," *IEEE Access*, vol. 8, pp. 48 285–48 298, 2020.

[4] R. Diamant, P. Casari, and S. Tomasin, "Cooperative authentication in underwater acoustic sensor networks," *IEEE Trans. Wireless Commun.*, vol. 18, no. 2, pp. 954–968, 2018.

[5] K. Pelekanakis, C. M. Gussen, R. Petroccia, and J. Alves, "Robust channel parameters for crypto key generation in underwater acoustic systems," in *Proc. MTS/IEEE OCEANS*. IEEE, 2019, pp. 1–7.

[6] L. Junkai, Z. Gangqiang, and Z. Junqing, "Key generation technology based on multipath structure of underwater acoustic channel," in *2021 OES China Ocean Acoustics (COA)*. IEEE, 2021, pp. 636–641.

[7] R. Zhao, M. Khalid, O. A. Dobre, and X. Wang, "Physical layer node authentication in underwater acoustic sensor networks using time-reversal," *IEEE Sensors Journal*, vol. 22, no. 4, pp. 3796–3809, 2022.

[8] P. Casari, F. Ardizzon, and S. Tomasin, "Physical layer authentication in underwater acoustic networks with mobile devices," in *Proceedings of the 16th International Conference on Underwater Networks & Systems*, 2022, pp. 1–8.

[9] L. Bragagnolo, F. Ardizzon, N. Laurenti, P. Casari, R. Diamant, and S. Tomasin, "Authentication of underwater acoustic transmissions via machine learning techniques," in *2021 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS)*. IEEE, 2021, pp. 255–260.

[10] F. Ardizzon, P. Casari, and S. Tomasin, "A RNN-based approach to physical layer authentication in underwater acoustic networks with mobile devices," *Computer Networks*, vol. 243, p. 110311, 2024.

[11] M. Khalid, R. Zhao, and N. Ahmed, "Physical layer authentication in line-of-sight underwater acoustic sensor networks," in *Proc. MTS/IEEE OCEANS*. IEEE, 2020, pp. 1–5.

[12] K. Pelekanakis, S. A. Yıldırım, G. Sklivanitis, R. Petroccia, J. Alves, and D. Pados, "Physical layer security against an informed eavesdropper in underwater acoustic channels: Feature extraction and quantization," in *Proc. UComms*, 2021, pp. 1–5.

[13] ——, "Physical layer security against an informed eavesdropper in underwater acoustic channels: Reconciliation and privacy amplification," in *Proc. UComms*, 2021, pp. 1–5.