A Geometry-Based Game Theoretical Model of Blind and Reactive Underwater Jamming

Alberto Signori, *Student Member, IEEE*, Federico Chiariotti, *Member, IEEE*, Filippo Campagnaro, *Member, IEEE*, Roberto Petroccia, *Senior Member, IEEE*, Konstantinos Pelekanakis,*Senior Member, IEEE*, Pietro Paglierani, *Senior Member, IEEE*, João Alves, *Senior Member, IEEE*, Michele Zorzi, *Fellow, IEEE*

***Abstract*—Security is a critical consideration in Underwater Acoustic Networks (UANs) due to the importance of the applications in which these types of networks are often employed, from military applications to marine natural disaster prevention. Furthermore, even simple Denial of Service (DoS) attacks such as jamming can be very effective in disrupting the communication, with significant negative consequences for these critical applications. While jamming has been widely studied in the context of terrestrial networks, the peculiarities of propagation in UANs, such as the low propagation speed, the multipath, and the high delay spread, need to be considered: the relative positions of the jammer, transmitter, and receiver can have a huge impact on the feasibility and impact of reactive jamming, opening the way for the exploitation of other jamming models. In this paper, we analyze the effectiveness of a reactive and a blind jammer through a game theoretical framework, comparing them for different geometries of the scenario. We assess the impact of the different jammers, employing different active and evasive strategies, where the first type of countermeasure implies the use of additional energy to protect the communication, while the second tries to avoid the jamming signals by randomizing the transmission pattern.**

***Index Terms*—Reactive jamming, game theory, underwater acoustic communications, security in underwater networks**

I. Introduction

Underwater sensor networks have seen significant development over the last few years due to their extreme usefulness for both military and civilian applications [1]. Underwater sensor networks can be used in many application scenarios, such as oil and gas platform and pipeline maintenance, coastal and critical infrastructure surveillance, and environmental monitoring. In the underwater environment, both radio and optical signals are greatly attenuated and hence, acoustic waves are the preferred way for wireless communications beyond about 50 m. In addition, underwater acoustic communications exhibit high latency due to the relatively slow speed of sound (1500 m/s, on average), high packet loss rate due to extended time-varying multipath, and low throughput due to distance-dependent bandwidth [2].

A. Signori (email: signoria@dei.unipd.it), F. Campagnaro (email: campagn1@dei.unipd.it), and M. Zorzi (email: zorzi@dei.unipd.it) are with the Department of Information Engineering, University of Padova, 35131 Padova, Italy. F. Chiariotti (email: fchi@es.aau.dk) is with the Department of Electronic Systems, Aalborg University, 9220 Aalborg, Denmark. R. Petroccia (email: roberto.petroccia@cmre.nato.int), K. Pelekanakis (email: konstantinos.pelekanakis@cmre.nato.int), P. Paglierani (email: pietro.paglierani@cmre.nato.int), and J. Alves (email: joao.alves@cmre.nato.int) are with the NATO STO Centre for Maritime Research and Experimentation, 19126 La Spezia, Italy. M. Zorzi is also with Consorzio Futuro in Ricerca,44122 Ferrara, Italy.

As the propagation environment is already hostile for underwater acoustic transmissions, Denial of Service (DoS) jamming attacks can be very effective at disrupting communications [3]. The simplest jamming attacks involve the transmission of a high-power signal that interferes with the legitimate signal in the same band and prevents its correct decoding. The significant differences between terrestrial networks, in which most jamming techniques and countermeasures have been studied, and Underwater Acoustic Networks (UANs) can lead to very different trade-offs [4] that might help or hinder the attacker. For example, the use of high-power jammers with no battery constraints is impossible in most underwater networks: such a jammer would require a large-scale operation using a boat or submarine, which would be detected long in advance and stopped from entering the area [5]. On the other hand, jamming is possible if the jammer is a small Autonomous Underwater Vehicle (AUV), but this limits both the jamming power and the battery due to size and cost concerns. However, AUVs have another advantage, as they can remain almost silent except for the jamming signal and flee at low speed, remaining almost undetectable after the jamming operation, which may last only a few minutes [5]. For this reason, detecting the presence of a jammer might not always be enough for the network to defend itself [6], particularly when there is a single receiver and triangulation is very difficult. This can be the case for many network deployments with a single "leader" floating node gathering data from multiple sensors and transmitting them to a boat or control station using above-surface electromagnetic communications [7].

Most of the radio-frequency literature on jamming countermeasures assumes that the jammer is *reactive*, sensing the packet transmission and jamming it with negligible delay [8]. As a consequence, it focuses on what we call *active* defense. In broad terms, active countermeasures aim at overcoming the jamming signal by strengthening the transmission, and involve an additional energy expenditure by the transmitter. There are three main types of active countermeasures that a transmitter can take to protect a message, potentially combining them to increase their effectiveness:

- *Power control*: the transmitter increases the transmission power [9], consequently increasing the Signal to Interference plus Noise Ratio (SINR) and so increasing the decoding probability, at the cost of spending more energy per packet;
- *Modulation and Coding Scheme (MCS) adaptation*: the

transmitter can select a more robust modulation or a lower coding rate [10], thus reducing the data rate while increasing the probability of correct decoding. However, more energy is required to achieve the same SINR due to the longer duration of a packet transmission;

- *Packet-level coding*: the transmitter can encode the data packets and add some redundant packets [11], ensuring that the transmission is successful as long as a sufficiently large subset of packets is correctly decoded. This countermeasure does not change the power or duration of a packet transmission, but still increases the energy cost of each information packet, as the energy to transmit the redundant packets must be added to the tally.

However, there is also another type of countermeasure, which depends on the peculiar nature of underwater communications. Unlike in terrestrial networks, the long propagation delay of acoustic waves makes it possible for the transmitter to try avoiding the jamming signal entirely or partially. Indeed, depending on the link geometry, the malicious node might only be able to reactively jam part of each packet, or even not at all, reducing its effectiveness. In this case, the jammer can increase its chance to disrupt the transmission by acting *blind*, i.e., not reacting to sensed transmissions but proactively jamming the communication resources that it expects the transmitter to use [11]. However, this makes another type of defense possible: if the legitimate transmitter can use multiple time slots or frequency channels for its transmission, it can try to avoid the jamming signal by randomizing its transmission pattern in time and frequency to increase the probability of transmitting its packets when the jammer is not active.

We call this type of countermeasure *evasive* defense: naturally, evasive defense has no effect against a reactive jammer, which can know exactly when a packet is being transmitted, albeit with some delay. In general, evasive defense can be applied over any kind of wireless communication, including radio-frequency electromagnetic communications. However, in these cases reactive jamming is almost always the best choice, as at the speed of light the propagation delay is much smaller, lower than 1 μs if the communication radius is below 300 m. In this case, the transmission time for each packet is often far longer than the propagation delay, making reactive jamming almost perfect and evasive defense a less attractive proposition. On the other hand, acoustic waves, which are often the only available medium for underwater communications over long distances due to the high electromagnetic attenuation of water, have a low bitrate and high propagation delays, making the trade-off between reactive and blind jammer less trivial than in terrestrial radio-frequency networks. In UANs, the propagation delay can also be higher than or comparable to the packet transmission time, resulting in lower effectiveness of a reactive jammer and making the blind solution more attractive. For these reasons, the geometry of the network affects the ability of a reactive jammer to promptly react to a transmission, making this problem completely different from its counterpart in terrestrial networks and well worth studying.

As stated above, evasive defense can be performed in both time and frequency, but there are two critical reasons to avoid frequency hopping. First, the bandwidth available for long-range acoustic transmissions is already very low in underwater scenarios, making it impractical to further reduce it by dividing it into subchannels. This is especially true for those modems that spread the signal over the whole bandwidth in order to mitigate the multipath distortion caused by the signal reflections with the sea surface and the sea bottom [12], [13]. Secondly, dividing the bandwidth to hop between different subchannels increases the transmission times for each packet, making it easier for a reactive jammer to listen for the transmission and jam it. Conversely, transmitting over the whole available bandwidth ensures the minimum transmission time, giving little time to a reactive jammer to detect and disrupt the transmission, and as long as the total number of resources in time and frequency are the same, the effectiveness of the evasive defense against the blind jammer does not change. Continuous jamming could also be an option: the jammer could send a blanket jamming signal all the time, which would be impossible to evade. However, performing this kind of jamming with enough power to effectively disrupt the legitimate transmission would require a significant energy expense from the jammer, and would not be feasible for the battery-powered nodes that we consider.

In this work, we enhance what is presented in [11] by considering both active and blind jamming and by investigating the effect of active and evasive defenses. We define a game theoretical model to address the selection of the best defense, which depends on the network geometry, the conducted attack and the available resources. Indeed, due to the peculiarities of underwater acoustic propagation, finding the optimal strategies against different jammer models becomes non-trivial and, to the best of our knowledge, has never been investigated before. The proposed game theoretical analysis, when carried out before an actual deployment, helps identify network vulnerabilities by discovering the critical areas where a reactive jammer can cause severe network disruption. This type of analysis is unique to UANs and does not apply in the usual deployment of a terrestrial radio-frequency network, where the trade-off becomes trivial in favor of a reactive jammer. In addition, the game theoretical framework helps predict how many packets an attacked node can send to the destination before depleting its battery. The proposed solution has been validated via simulations employing real acoustic data, recorded during the CMRE Littoral Acoustic Communications Experiment 2017 (LACE17) [14] sea trial in the Gulf of La Spezia, Italy. More specifically, Bit Error Rate (BER) measurements recorded during LACE17 have been used in our simulation to model the quality of the communication link. Although LACE17 was not conducted to model a jamming attack, the data can be adapted to our scenario with limited assumptions: the different transmission power and SINR settings explored in the dataset were taken to represent a communication channel with and without the presence of a jamming signal. In the LACE17 dataset, the jamming signal is modeled as an Additive White Gaussian Noise (AWGN) noise: however, it is possible for a jammer to use a different modulation, which might have a better chance of disrupting the communication [15]. However, this is irrelevant to the design of our model, as it would only affect the bit error probability of

a jammed packet, changing the resulting strategies but not the procedure to solve the game. Our simulation results show that the geometry of the underwater scenario is a critical factor in determining the optimal jamming and defense strategies in our scenario, including evasive as well as active countermeasures.

The rest of the paper is divided as follows: Section II presents an overview of the related work on underwater jamming attacks. The proposed game theoretical jamming model is detailed in Section III, while Section IV describes the algorithm to find the Nash Equilibrium (NE) solution. Section V describes the simulation setting and parameters, while simulation results are discussed in Section VI. Finally, Section VII concludes the paper with some remarks on possible avenues for future work.

II. Related Works

Physical layer jamming is a well-studied and common DoS attack technique, in both terrestrial and underwater networks [16]. Its basic principle is particularly intuitive: in order to block the reception of a packet, the attacker increases the noise level at the receiver by injecting a single-tone or white Gaussian noise signal [15] into the channel in the same frequency band as the transmitter. More sophisticated attacks can target the packet preamble [17] in order to affect the synchronization and metadata decoding processes, which can be vulnerable to more targeted jamming attacks, saving the attacker energy as it does not need to jam the longer body of the packet. All these techniques can be adapted to prevent the transmitter from escaping the jamming using spread spectrum modulation or frequency hopping [18], and more flexible approaches can involve power and modulation control from the jammer to maximize the effectiveness of the attack. One such example is pulsed jamming [19], which aims at blocking the header of a packet or saturating the receiver electronics, making its Automatic Gain Control (AGC) reduce the receiver gain. However, in order to avoid amplifying the environmental noise caused, for instance, by ship propellers [20], snapping shrimps [21], wind waves and rain [22], underwater acoustic modems are often only equipped with manual on/off gain control, making them far less vulnerable to pulsed attacks. For a more comprehensive taxonomy of jamming attacks and defenses, we refer the reader to [23].

Defense techniques have evolved in parallel with jamming attacks, as network designers adapt their solutions to potential attacks, which are then updated in a continuous arms race. While jamming attacks can make easy prey of unaware transmitters that use simple duty cycling to save energy [24], the literature on jamming countermeasures involves active reactions such as power control [25] and channel-hopping [26]. Game theory is a tool that can be employed to model a scenario in which both the jammer and the transmitter have some adaptive capabilities and can adapt to each other. As we described in the introduction, the main drawback of active defense strategies is that they require more energy, reducing the lifetime of the nodes. So-called "vampire" attackers can then exploit this to deplete the transmitter's battery. In this case, the game theoretical model needs to include energy consumption, either as an explicit constraint [27] or by considering nodes with a limited battery [28]. The latter case can be solved by applying dynamic programming techniques [29], as there is a limited number of possible energy states, which can only decrease if the nodes have no energy harvesting capabilities.

Some recent works have analyzed jamming with game theory in an underwater context, exploiting the peculiar nature of UANs. For example, [30] considers a mobile transmitter which can change its position as well as its transmission power to respond to the jamming attack, and [31] investigates friendly jamming as a potential help for the transmitter in preventing eavesdropping. In [32], the authors study the effect of different types of jamming models, such as random, reactive, constant and white noise jammers, using real commercial and prototype modems. Other works in this area are described in [33], which surveys the recent literature on underwater jamming. However, to the best of our knowledge our previous work [11] is the first one to consider the long propagation delays that characterize acoustic transmission as a sort of natural defense against jamming. In [34], the authors address the effects of propagation delay on the detection of reactive jamming, but do not analyze the impact of this delay on defensive countermeasures.

While reactive jamming, in which the attacker only transmits the jamming signal if it senses a packet being transmitted, is the standard assumption in terrestrial wireless networks, the long propagation delay might make it impossible for the jammer to sense the packet and jam it in time. In this case, the jammer needs to adopt a blind strategy, jamming at random instants and hoping to block a packet transmission. This can be modeled as a discoordination game [35], where the transmitter tries to avoid choosing the same transmission times as the jammer, while the jammer does the opposite. This paper expands on the concepts of blind and reactive jamming, analyzing the effects of the geometry of the scenario on the optimal strategies for the jammer and transmitter when both of them are battery-limited.

III. Game Theoretical Model

In this work, we consider a scenario in which an underwater node needs to periodically transmit updates to a receiving node through an underwater acoustic channel. We denote the transmitting node as T, the receiver as R, and the jammer as J. Both T and J are battery-powered nodes. The distance between T and R is denoted with d_{TR}, while d_{JR} represents the distance between J and R. The objective of the jammer is to impair the reception of messages at R and to force T to deplete its battery faster by applying defensive strategies. The main notation used in the paper is summarized in Table I. Each update transmitted by T is composed of K packets of L_0 bits, and both active or evasive countermeasures can be employed. We define θ, the angle between the segment between R and T and the segment between R and J: if θ is 0 and $d_{JR} \leq d_{TR}$, the jammer is between the transmitter and the receiver, while if $\theta = \pi$, J and T are on opposite sides of the receiver. Fig. 1 displays different scenarios when θ varies from 0 to π and with $d_{JR} = d_{TR}/2$.

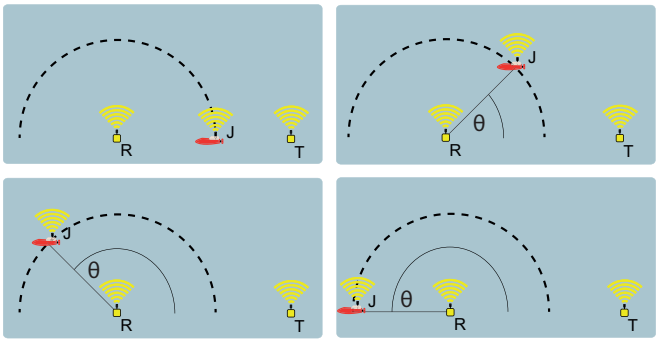


Fig. 1: Example of analyzed topologies for the reactive and blind jammer scenario with different angle θ ($\theta = 0$ top-left; $\theta = \pi/4$ top-right; $\theta = 3\pi/4$ bottom-left; $\theta = \pi$ bottom-right). In this example $d_{JR} = d_{TR}/2$.

In the following, we assume that the transmitter can select the MCS $M \in \mathcal{M}$, the transmission power $P \in \mathcal{P}$, and the number of encoded messages $N \in \mathcal{N}$ (with $\mathcal{N} = \{K, K+1, \ldots, N_{\max}\}$) for each update. The set of possible configurations is then $\mathcal{M} \times \mathcal{P} \times \mathcal{N}$, and the specific selection depends on the target scenario. We assume that J always transmits at the same power. A reactive jammer can choose the number of sensed packets that it will jam, as it is able to sense incoming packets and choose whether to jam all or just a fraction of them. On the other hand, the blind jammer does not know how many packets will be transmitted, or in which time slots, and as such, the only decision it can make is the number of communication resources, i.e., time slots, over which it will send the jamming signal. In the following, we assume a slotted time model, which is favorable to a blind jammer, as it will be able to block packets completely. Indeed, since the node positions are known to both T and J, we assume J to be able to synchronize its slots in order to be able to jam the whole packet. This is not entirely realistic, as the jammer might not be able to know the position of the other nodes precisely, or might suffer from drift due to currents and imprecise positioning; we do not handle this directly in our model, but we perform a sensitivity analysis showing that the strategies are robust to positioning errors.

We consider a zero-sum multistage game between T and J, in which each stage represents the transmission of an update. We consider the two nodes' batteries to be quantized in terms of the maximal common divisor of the possible packet energy costs, so that the state can be discretized. The two nodes start from battery levels $B_{T,0}$ and $B_{J,0}$, and keep playing until the transmitter's battery does not allow it to send any more updates.

In each subgame i, the transmitter will choose M_i, P_i, and N_i, and the jammer will select its jamming strategy. The value of M_i is known in advance to the jammer, as we assume that T sends a control message to R before the beginning of the update, which the jammer can listen to. Of course, this may not be true for all underwater networks, but we consider this assumption to be a worst-case scenario for transmission. In some networks, encrypted information may be exchanged between legitimate transmitter and receiver. If the jammer has less information, the scenario becomes easier for the defender, tilting the game its way and improving the transmission performance. However, there are cases where this information is sent in clear before the data transmission. This is true for both proprietary protocols implemented by underwater acoustic modem manufacturers [36], [37] or solutions where the JANUS standard [38] is used for coordination [39], [40]. In both these cases, control packets can be easily overheard and exploited by the attacker to make the jamming more successful. The reward $u_{T,i}$ for the transmitter is 1 if the transmission is successful, i.e., if at least K of the N_i packets are received and decoded correctly, and 0 otherwise. As the game is purely adversarial, the reward for the jammer is $u_{J,i} = -u_{T,i}$. After the subgame, the battery levels of the two nodes are decreased for the next subgame, to take the energy consumption into account.

In order to model the long-term consequences of energy consumption, and to encourage the nodes to maximize their lifetime, we model the payoff of the users as the expected reward for the next Γ subgames. The players' payoffs in the multistage game are given by:

$$U_T(\Gamma) = \sum_{i=1}^{\Gamma} \lambda^i \mathbb{E}[u_{T,i}], \tag{1}$$

where the parameter $\lambda \in [0, 1]$ is a discount factor that can be tuned to manage the level of foresightedness of the nodes. Naturally, the same goes for the jammer, whose long-term payoff is $U_J(\Gamma) = -U_T(\Gamma)$. In the following, we compute the expected payoff for the reactive and blind jammer separately, considering the effect of the scenario geometry on their performance.

A. Expected payoff with reactive jamming

If the jammer is reactive, there could be a partial overlap between the transmitted packet and the jamming signal. As we described above, T, J, and R form a triangle. The distance between T and R is d_{TR}, the distance between J and R is d_{JR}, and the angle at the receiver is θ. In this case, the jammer's action is the choice of the number of packets to jam, which we denote as $S \in \mathcal{S}_{\text{re}}$, with $\mathcal{S}_{\text{re}} = \{0, 1, \ldots, N_{\max}\}$.

The overlap between the packet and the interference depends on the relative position between transmitter, jammer and receiver. Indeed, the jammer needs to overhear the packets sent by the transmitter before starting to jam the signals and then the jamming signal needs to cover the distance between the jammer and the receiver. The delay Δ_d after which the interference from the jammer arrives at the receiver, computed with respect to the transmitted packet, is equal to

$$\Delta_d(\theta) = \frac{d_{TJ} + d_{JR}}{c} - \frac{d_{TR}}{c} + \tau_h, \tag{2}$$

where c is the speed of sound, and τ_h is the time required for the jammer's half-duplex model to switch from receiving to transmitting. In our scenario d_{JR} and d_{TR} are fixed and known while d_{TJ} depends on θ. Carnot's theorem can be used to find the distance d_{TJ}

$$d_{TJ}^2 = d_{TR}^2 + d_{JR}^2 - 2 d_{TR} d_{JR} \cos\theta. \tag{3}$$

Symbol	Meaning	Symbol	Meaning
T	Transmitter	J	Jammer
R	Receiver	d_{mn}	Distance between nodes m and n
K	Number of packets in an update	L_0	Length of a packet in bits
θ	Angle between segments RT and RJ	$\mathcal{M}$	Set of MCSs
$\mathcal{P}$	Set of transmission power levels	$\mathcal{N}$	Set of packet-level coding choices
$p_{b,c}(M,P)$	Clear channel BER	$p_{b,j}(M,P)$	Jammed channel BER
$B_{n,0}$	Initial battery level for node n	$u_{n,i}$	Instantaneous reward for node n
$U_n(\Gamma)$	Long-term reward for node n	λ	Discount factor
$\mathcal{S}_{\text{re}}$	Set of reactive jammer moves	Δ_d	Delay for the jamming signal
$F(\theta,M)$	Fraction of a packet affected by reactive jamming	$R(M)$	Bitrate for MCS M
$\psi(M)$	Maximum number of bit errors for MCS M	$p_e(P,M,F)$	Packet error probability
$\mathcal{S}_{\text{bl}}$	Set of blind jammer moves	C	Number of packets that avoid jamming
ε	Final state for the game	$\mathcal{B}$	Set of battery states
Γ	Horizon for the strategy	Φ_n	Strategy for node n
T_0	Transmission time for a packet with BPSK	τ_h	Switching time for half-duplex modems
E_q	Energy quantum	$E_{\text{tx}}(M)$	Energy consumption for a packet

TABLE I: Notation.

We define $F(\theta, M)$ as the portion of a packet affected by the jamming signal, with $F \in [0,1]$ depending on the modulation and on the position of the three nodes. Its value is therefore

$$F(\theta, M) = \max\left(0, 1 - \frac{\Delta_d(\theta) R_b(M)}{L_0}\right), \tag{4}$$

where $R(M)$ is the bitrate of the selected MCS. A more robust modulation will reduce the rate, decreasing the effectiveness of the jamming signal, but increasing the overlap at the same time. We define the BERs for a clear channel and for a jammed channel with MCS M and transmission power P as $p_{b,c}(P,M)$ and $p_{b,j}(P,M)$, respectively. As the MCS includes a channel code, packets are protected from errors as long as the number of flipped bits does not go over the correction capability of the code, which we denote as $\psi(M)$ and corresponds to half of the code's minimum Hamming distance [41]. Based on the overlap between the transmission and the jamming signal, we get the packet error probability $p_e(P,M,F)$:

$$\begin{aligned} p_e(P,M,F) =& 1 - \sum_{e_j=0}^{\min(\psi(M), FL_0)} \text{Bin}(e_j; FL_0, p_{b,j}(P,M)) \\ & \times \sum_{e_c=0}^{\min((1-F)L_0, \psi(M)-e_j)} \text{Bin}(e_c; (1-F)L_0, p_{b,c}(P,M)), \end{aligned} \tag{5}$$

where $\text{Bin}(k; N, p)$ is the binomial probability mass function, defined as:

$$\text{Bin}(k; N, p) = \binom{N}{k} p^k (1-p)^{N-k}, \quad 0 \le k \le N. \tag{6}$$

We can then compute the probability that at least K of the N packets are correctly received, given that the jammer jams S of them (with $S \le N$ in the reactive jamming scenario):

$$\begin{aligned} \mathbb{E}_{\text{re}}[u_T | M, N, S] = & \sum_{r_j=0}^{S} \text{Bin}(r_j; S, p_e(P, M, F(M,\theta)) \\ & \times \sum_{r_c=K-r_j}^{N-S} \text{Bin}(r_c; N-S, p_e(P,M,0)). \end{aligned} \tag{7}$$

The $N - S$ packets that are not jammed can be considered as having zero overlap with the jamming signal.

B. Expected payoff with blind jamming

In this case, we assume that there are $N_{\max}$ time slots, and that the blind jammer can perfectly synchronize with the packets. In this case, the optimal action for T is to use random slots to send its packets, and the possible actions for J are, again, the number of jammed slots, which we also denote as $S \in \mathcal{S}_{\text{bl}}$, with the same set $\mathcal{S}_{\text{bl}} = \{0, 1, \ldots, N_{\max}\}$. As we assume synchronization, the error probability for jammed packets is $p_e(M, 1)$. We can then compute the probability mass function (pmf) of the number of packets C that are transmitted without interference from J, which follows a hypergeometric distribution as proven by Vandermonde's Identity [42]:

$$p(C|N,S) = \frac{\binom{N}{C}\binom{N_{\max}-N}{S-(N-C)}}{\binom{N_{\max}}{S}}. \tag{8}$$

Once we know the number of packets without interference, we can compute the expected payoff for a given move S by the blind jammer:

$$\begin{aligned} \mathbb{E}_{\text{bl}}[u_T | M, N, S] = & \sum_{C=0}^{N} p(C|N,S) \sum_{r_c=K-r_j}^{C} \text{Bin}(r_c; C, p_e(M,0)) \\ & \times \sum_{r_j=0}^{N-C} \text{Bin}(r_j; N-C, p_e(M,1)). \end{aligned} \tag{9}$$

IV. Analytical solution of the game

In the case of complete information, dynamic programming can be used to determine the NE. The system state can be completely represented by the tuple (B_T, B_J), as the battery evolution is the only change in this scenario. The state space is limited by the initial battery levels, so the initial state is $(B_{T,0}, B_{J,0})$. The full state space is $\mathcal{B} = \{0, \ldots, B_{T,0}\} \times \{0, \ldots, B_{J,0}\}$. The payoff is then computed by considering the next Γ subgames, during which the system state will move to progressively lower values as the two nodes deplete their batteries. If the transmitter does not have enough energy to transmit the update with any MCS, the game is over. We can

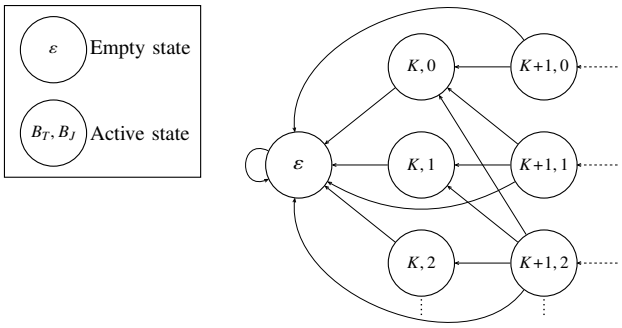


Fig. 2: State transitions for the multistage game.

aggregate all states that satisfy the ending condition into a final state ε and define its payoff as:

$$U_T(\Gamma|B_T = \varepsilon) = 0 \quad \forall \Gamma\,. \tag{10}$$

We can then recursively compute the payoff for each state, starting from the base case in the final state and moving gradually upwards. The recursive formula for the payoff is:

$$\begin{aligned} U_n(\Gamma|B_T, B_J) =& \mathbb{E}[u_n|B_T, B_J] + \sum_{B'_T=0}^{B_T} \sum_{B'_J=0}^{B_J} U_n(\Gamma - 1|B'_T, B'_J) \\ & \times p(B'_T, B'_J|B_T, B_J), \quad n \in \{T, J\}, \end{aligned} \tag{11}$$

where the transition probability $p(B'_T, B'_J|B_T, B_J)$ depends on the players' choices. We define a strategy Φ_T as a probability distribution over T's action space, and do the same for Φ_J. For a given set of strategies Φ_J, the transition probability is:

$$\begin{aligned} p\left(B'_T, B'_J|B_T, B_J\right) = & \sum_{(M,P,N)\in\mathcal{M}\times\mathcal{P}\times\mathcal{N}} \Phi_T\,(N, M, P)\,\delta\left(\frac{NPL_0}{R(M)} + B'_T - B_T\right) \\ & \times \sum_{S\in\mathcal{S}} \Phi_J\,(S)\,\delta\left(\frac{SP_J L_0 F(M,\theta)}{R(M)} + B'_J - B_J\right), \end{aligned} \tag{12}$$

where $\delta(\cdot)$ is the delta function, equal to 1 if the argument is 0 and 0 otherwise, and where $F(M, \theta)$ is always 1 for the blind jamming case. Fig. 2 shows the state transition graph for the multistage game $\mathbb{G}$. Transitions are allowed from bottom to top and from right to left, as a consequence of nodes T or J consuming energy to send packets or jam slots, respectively.

By substituting (12) into (11), we have a full recursive formulation for the expected long-term payoff $\mathbb{E}[U_n^{(m)}(\Gamma)]$ for any strategy pair. Once the payoff bimatrix is thus constructed, the Lemke-Howson algorithm can be used to find the mixed NE [43].

V. Simulation setup

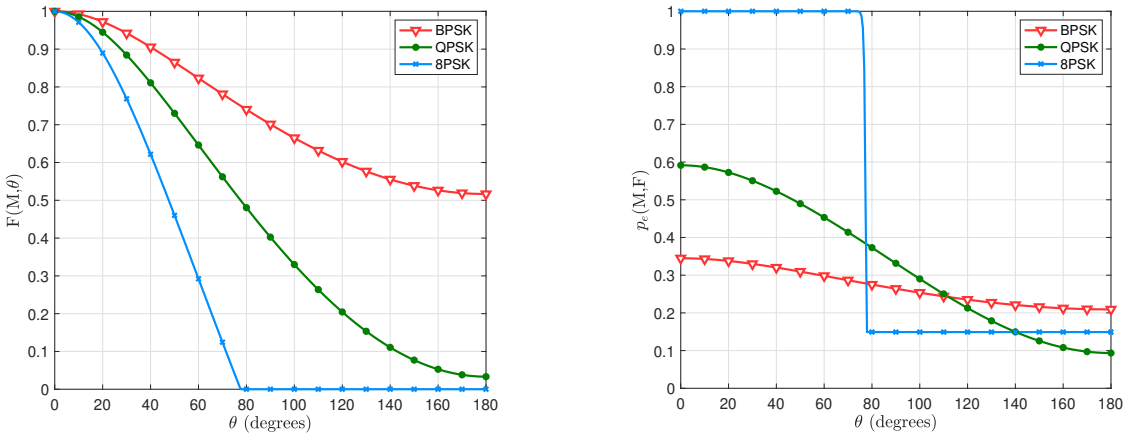
We analyze the performance of the transmitter and jammer using all the three possible modulations available in the LACE17 dataset: Binary Phase-Shift Keying (BPSK), Quadrature Phase-Shift Keying (QPSK), Eight Phase-Shift Keying (8PSK). The length L_0 of the packet, expressed in bits, is constant for all the modulations. Each modulation M corresponds to a different bitrate $R(M)$ and, consequently, to a different packet transmission time $T(M) = \frac{L_0}{R(M)}$. The modulations use channel coding to protect their content, with different rates: if we define the bitrate for a BPSK modulation as $R(\text{BPSK}) = R_0$, we have $R(\text{QPSK}) = 2R_0$ and $R(\text{8PSK}) = 4R_0$ (uncoded 8PSK would only have a bitrate 3 times larger than BPSK, but the MCS also uses a code with less redundancy). The higher modulations use Trellis Coded Modulation (TCM), while BPSK uses a convolutional code. In the next section we will consider whether it is better for the transmitter to use a high bitrate which reduces the packet transmission time (making the system less prone to reactive jamming) and also the energy consumption at the price of a higher BER, or to use a more robust modulation which increases the packet duration, and the energy consumption, and makes the system more prone to reactive jamming.

TABLE II: Modulation and coding schemes used in the LACE17 dataset [14].

Modulation	Bitrate	Code type	Code rate
BPSK	116 bit/s	Convolutional	1/2
QPSK	232 bit/s	TCM	1/2
8PSK	464 bit/s	TCM	2/3

We consider a scenario with a packet size $L_0 = 192$ bit and with a bitrate $R_0 = 116$ bit/s for a BPSK modulation, as in the LACE17 dataset. The modulation and coding schemes are summarized in Table II. The distances of T and J from R in the scenario are equal to $d_{TR} = 1200$ m and $d_{JR} = 600$ m, respectively, while d_{TJ} depends on the angle θ and can be computed according to Equation (3).

Using these values, we are able to simulate a scenario where 8PSK packets cannot be reactively jammed for high values of θ, the QPSK packets can always be reactively jammed (although only for a small portion of the packet for θ around 180 degrees), and the BPSK packets can always be reactively jammed with an overlap higher than 50%. This choice of the parameters enables us to analyze the case in which the packet transmission duration is of the same order of magnitude as the propagation delay, which is unique to the underwater scenario and has a non-trivial strategy that depends on the geometry of the problem and on the communication parameters. In addition, we consider $\tau_h = 0$, which is the setting that is most advantageous to a reactive jammer: furthermore, in most practical scenarios, in which the duration of a packet and the propagation delay will be measured in seconds, τ_h has a negligible effect. Indeed, the two extreme scenarios in which the packet transmission time is far longer (or shorter) than the propagation delay has been already well-studied. In the former, reactive jamming is always the best choice, as the jammer can avoid wasting energy on jamming an empty channel and still be sure to block any packet transmission. In the latter, reactive jamming is impossible, as the jammer will only sense the packet when it is too late to jam any significant portion of it, unless it is directly between the transmitter and the receiver. The purely blind jammer case corresponds to the one we analyzed in our previous work [11], while the purely reactive jammer is well analyzed in the relevant literature [8],



(a) Overlap $F(M, \theta)$ between the signals.

(b) Jammed packet error rate.

Fig. 3: Transmission parameters as a function of θ, for the three considered modulations.

[44], [45].

Fig. 3a shows the overlap between the jamming signal and the packet transmitted by T for the three considered modulations, while varying the value of θ. Fig. 3b displays instead the resulting jammed packet error rate.

Although our framework can support a wide set of strategies, i.e., of parameters that each player can choose, the evaluation was performed considering the information available in the LACE17 dataset. For this reason, we could not consider power control, i.e., the transmitter can use only one possible power level P and the same power level is also used by J. We consider each update to be composed of $K = 4$ information packets, and the maximum number of packets that can be transmitted at each subgame to be equal to $N_{\max} = 2K$, considering the additional redundant packets generated by the packet-level code. In our simulation, the action space for the transmitter is then $\mathcal{M}\times\mathcal{P}\times\mathcal{N}$, where $\mathcal{M} = \{\text{BPSK}, \text{QPSK}, \text{8PSK}\}$, $\mathcal{P} = \{P\}$, and $\mathcal{N} = \{K, K+1, \ldots, 2K\}$. This corresponds to a scenario in which the transmitter can use MCS control and packet-level coding as defense mechanisms, but not power control. The transmitter can also choose the slots in which to transmit over the $N_{\max}$ available slots, using a random strategy to maximize its chances of avoiding a blind jammer. Naturally, evasive defense is not effective against a reactive jammer.

We assume the same initial battery level for both T and J, i.e., $B_{T,0} = B_{J,0}$. The battery levels are quantized according to an energy quantum E_q such that each packet can be transmitted using an integer number of energy quanta $E_{\text{tx}}(M) = Q(M)E_q$. $Q(M)$ depends on the employed modulation and is equal to $Q(M) = \frac{8T(M)}{T_0}$ for 8PSK, QPSK, BPSK, respectively. Consequently, the transmission of a packet with BPSK takes 8 energy quanta, while the transmission with 8PSK only takes 2. We consider $B_{T,0} = B_{J,0} = 400E_q$. This choice allows us to study a sufficiently long game where both nodes can play any strategy for most of the game, while maintaining a low computational complexity. This poses a limit to the maximum number of packets that can be transmitted in the whole game, and therefore on the maximum number of subgames that can be played. Considering the 8PSK modulation, and the lowest possible number of packets that has to be transmitted in each subgame, i.e., $N = K = 4$ packets (i.e., no packet-level coding), the maximum number of subgames is limited to 50. For this reason, we set the time horizon $\Gamma = 50$ to let T and J play with full foresight of the rest of the game.

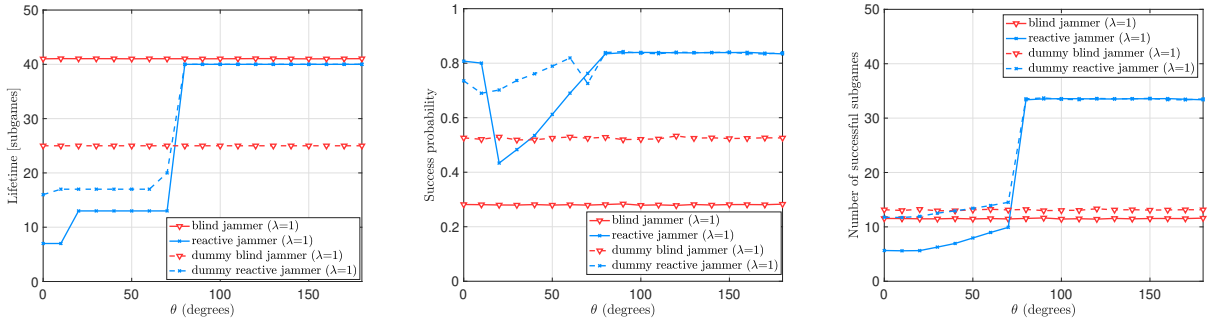
VI. Results

In this section, we compare blind and reactive jammer performance while changing the geometry of the scenario, i.e., varying the angle θ from 0 to π. The goal is to understand for which scenario reactive jamming is more effective than blind jamming.

The framework presented in Section III allows us to compare the two jammer types for different distances and angle θ obtaining the strategies for each player and then analyzing the results through Monte Carlo simulation. First, we analyze in detail the performance and the strategies for both jammer types considering the distance $d_{JR} = \frac{d_{TJ}}{2} = 600$ m as described in Section V. Clearly, the obtained trade-offs are specific for the considered scenario, but similar analysis and considerations also apply for a different choice of the distances between the nodes. Then, to make our study more general, we analyze how the trade-off changes for different distances between jammer and receiver showing the threshold on the angle θ that makes one jammer type more effective than the other. Finally, we perform a sensitivity analysis considering imperfect information on the jammer position.

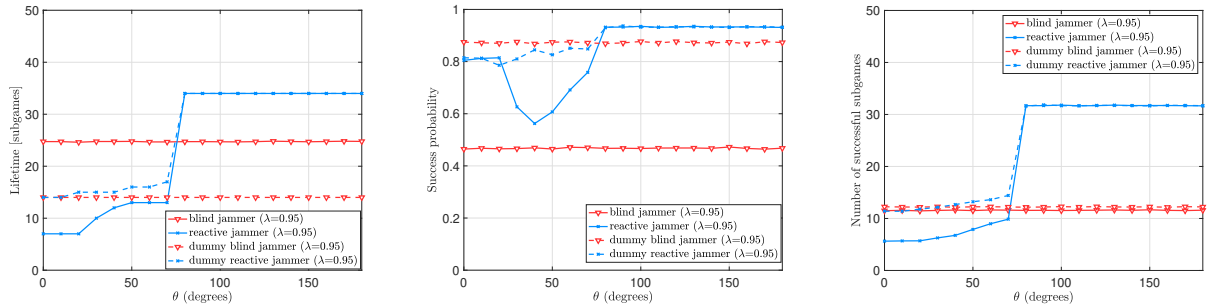
A. Performance analysis

The geometry of the scenario does not affect the performance of the blind jammer, while the reactive scenario depends on the geometry due to the different portion of the packet that the jammer can damage. In this section, we present the lifetime, i.e., the number of played subgames, as a function of θ (Fig. 4a and Fig. 5a), the corresponding subgame success probability (Fig. 4b and Fig. 5b), i.e., the number of subgames



(a) Lifetime of the transmitter. (b) Transmission success probability (c) Number of successful subgames.

Fig. 4: Performance against a reactive and blind jammer, considering optimal and dummy strategies with λ=1, varying the geometry and considering optimal and dummy strategies.



(a) Lifetime of the transmitter. (b) Transmission success probability (c) Number of successful subgames.

Fig. 5: Performance against a reactive and blind jammer, considering optimal and dummy strategies with $\lambda = 0.95$, varying the geometry and considering optimal and dummy strategies.

won with respect to the number of subgames played, and finally the overall number of subgames won by the transmitter (Fig. 4c and Fig. 5c).

Fig. 4a and Fig. 5a show the lifetime computed as the number of subgames played before the transmitter runs out of battery. Specifically, Fig. 4a represents the results without discount factor, i.e., with $\lambda = 1$, for the blind and reactive jammer, while Fig. 5a shows the result with a discount factor $\lambda = 0.95$. As mentioned in Section III, the discount factor makes the player more short-sighted, by letting future rewards for successive subgames count less than the present one.

The consequence of using a discount factor less than 1 is to let T play more aggressively, sending more packets and with a more robust modulation to protect itself from J, with the results of reducing T's lifetime while increasing its subgame success probability (Fig. 4b). As mentioned above, the blind jammer scenario does not depend on the angle θ, while the reactive jammer's performance changes as θ changes.

In the considered scenario with $d_{JR} = \frac{d_{TJ}}{2} = 600$ m, Fig. 4c shows that when $\theta < 80$ degrees, a reactive jammer is more effective than a blind one. In particular, when $\theta < 20$ the reactive jammer can immediately counteract each transmission by almost completely overlapping each packet. In this case, the presence of a reactive jammer forces T to transmit with a robust modulation, such as BPSK, for which the jamming effectiveness is much lower than for the other modulations, adding also redundancy to protect the data, at the price of a fast battery depletion, thus obtaining a lifetime lower than 10 subgames. This increases the probability that T will win each subgame (i.e., make a successful transmission) to over 0.8, but, due to the small number of subgames played, the overall number of T's updates successfully received by R is smaller than 10. Increasing the angle θ, the QPSK modulation also becomes a valid option for the transmitter, since the portion of the packet that J is able to jam decreases, thereby decreasing the reactive jammer's effectiveness. Indeed, Fig. 4b shows a drop in the subgame success probability caused by a change in the modulation strategies from a more robust modulation (BPSK) to a less robust one (QPSK). However, using QPSK results in spending less energy for each transmission, and thus gives T the possibility to increase the lifetime and the overall number of subgames won in the whole game. As soon as the angle increases, the shorter transmission time and shorter collision window for the reactive jammer enable T to achieve a higher success probability.

On the other hand, when $\theta \geq 80$ degrees, it is more convenient for the jammer to play blind, since the number of successful subgames for the transmitter increases up to 34 subgames against a reactive jammer (while it is just 15 against a blind one). In the reactive case, with $\theta \geq 80$ degrees, the jammer is no longer able to jam the 8PSK packets, as shown in Fig. 3a. Therefore, the transmitter always chooses

a strategy involving 8PSK modulation and only fights against the channel. For example, in the scenario with $\lambda = 1$, T always protects the update with one additional redundant packet, i.e., transmitting $N = 5$ overall packets with 8PSK modulation. This is confirmed by Fig. 4a where the lifetime for the reactive jammer scenario with $\theta \geq 80$ is equal to 40 subgames. Considering a discount factor $\lambda = 0.95$, shown in Fig. 5, the transmitter has a lower foresight and becomes more aggressive in terms of energy spent in each subgame, reducing its lifetime while increasing the subgame success probability, with the overall effect of decreasing the total number of successful subgames.

We also compare the results with two dummy policies, in which the blind jammer always tries to jam K packets for each update, while the reactive jammer jams enough packets to let the transmitter send only $K - 1$ in a clear channel, regardless of the MCS used. These strategies are often used in practice and can be effective, as the performance for the blind jammer shows, but they are always suboptimal, as the jammer cannot react to the strategy of the transmitter. This is visible in Fig. 4c, as the number of successful subgames is the metric that the players are optimizing for. Interestingly, the relatively small difference between the NE of the blind jammer and of the dummy is not due to a similarity in the strategies: the dummy jammer spends much more energy and makes the transmitter protect its transmissions in a far more expensive way, reducing the lifetime significantly, but it lets through about 85% of packets, while the game played by the NE nodes is much slower, with lower success probabilities and less energy expended per round, but a far longer lifetime for both nodes.

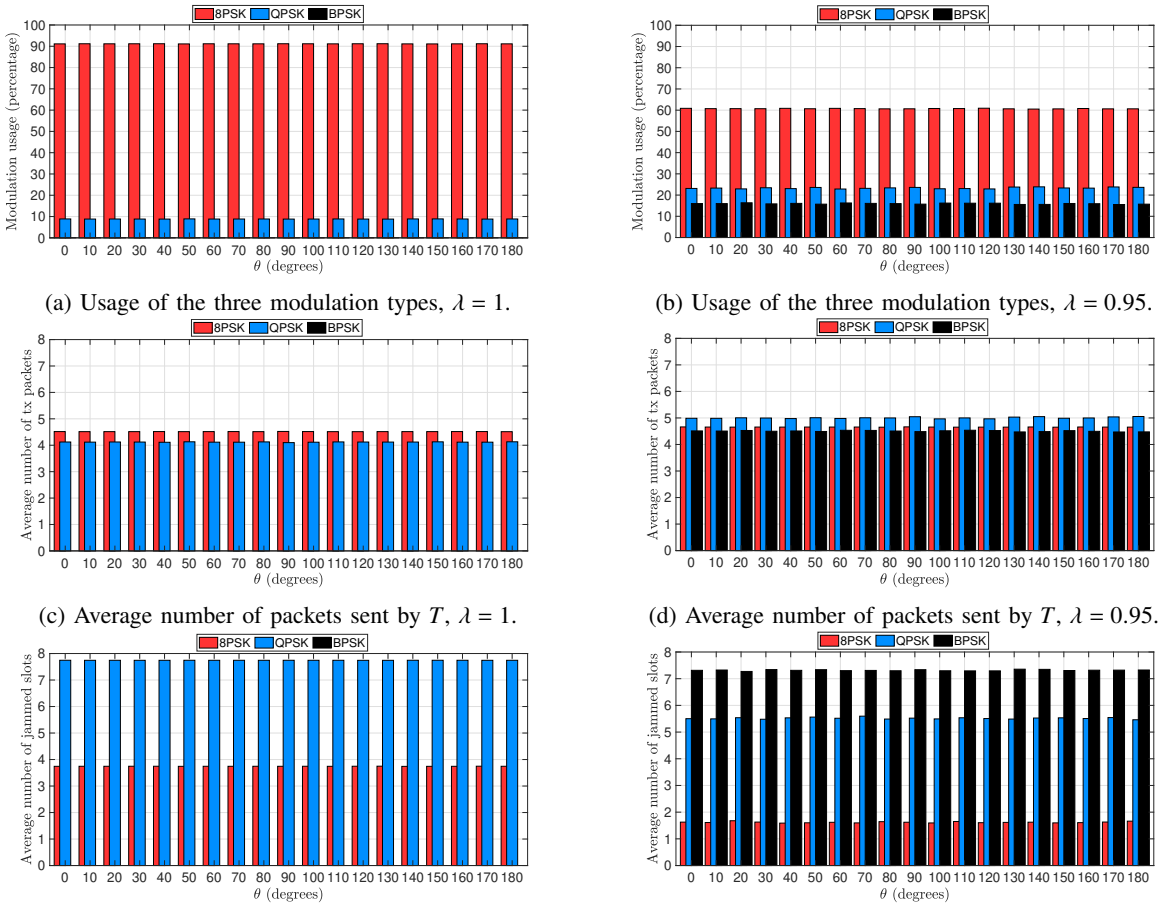
This result clearly depends on the specific distances and MCSs used in this scenario, and choosing a different geometry or different settings for the transmission might change the value of θ at which it is convenient for the jammer to switch to blind jamming, but a general rule holds: the lower the angle θ, the better reactive jamming works, while blind jamming is unaffected by θ as long as the slots can be synchronized (i.e., if the jammer knows the position of all nodes). Reactive jamming is more energy-efficient, as the jammer never wastes energy, transmitting the jamming signal only when it senses a legitimate transmission. Naturally, this means that it needs to deal with the delay, and that it can become ineffective, particularly over long distances.

B. Strategies

In this Section we analyzed in more detail the strategies employed in the scenario with $d_{JR} = \frac{d_{TJ}}{2} = 600$ m. Fig. 6 delves deeper into the choices that the two agents make when the jammer is blind, with $\lambda = 1$ and $\lambda = 0.95$. As expected, the strategies in this case are not affected by the angle θ, as the jammer *proactively* jams part of the slots instead of reacting to the transmitter: by compensating for the different propagation delays of the legitimate and jammed signal, the jammer effectively synchronizes them, but has to give up any knowledge of whether there is a transmission in a given slot or it is just jamming an empty channel. We remind the reader that there are $N_{\max} = 2K$ slots in which T can transmit, and that the blind jammer needs to decide how many to jam. The choice of the slots is random for both nodes, as this is the optimal strategy in an anti-coordination game. Fig. 6a shows that the transmitter uses 8PSK most of the time, with some redundancy to protect itself from the jammer. About 10% of the time, the transmitter uses QPSK with no redundancy. When using QPSK, the jammer is more aggressive, as seen in Fig. 6e: if the transmitter uses QPSK, it is almost always active, i.e., it jams almost all the $N_{\max}$ slots employed for the update, while it is only active approximately half the time when the transmitter uses 8PSK, as being able to jam only few packets is enough to cause the loss of the update. We want to remind the reader that a blind jammer is able to jam the whole packet since J infers the modulation employed from the control messages sent by T before the beginning of a subgame. If we set $\lambda = 0.95$, the transmitter considers the current packet more than future ones, using more energy: as Fig. 6b shows, this causes it to use 8PSK less often, using QPSK 25% of the time and BPSK 15% of the time. For all the three employed modulations, a low level of redundant packets (or zero redundant packets) is used. Correspondingly, the jammer is more active: when the transmitter uses BPSK, it is almost always actively jamming all the slots, while it jams approximately 60% of the available slots in a subgame when the transmitter uses QPSK. The jammer is correspondingly less aggressive against the lightly protected 8PSK transmissions, which happens mostly as the transmitter's battery gets low, and it has to reduce its energy consumption to avoid depleting its battery prematurely. In all cases, the position of the jammer does not matter: as the blind jammer can synchronize with the transmission opportunities, the only parameter related to the geometry of the scenario that affects its performance is its distance from the receiver, while the angle θ does not have any effect.

This is not true if the jammer is reactive: in this case, as Fig. 7 shows, the effectiveness of the jammer is strictly dependent on how quickly it can sense packets, i.e., on the value of the angle θ. If the angle between the jammer and the transmitter is small, the transmitter is forced to spend more energy to defend itself, using BPSK and sending 3 or 4 redundant packets for protection. On the other hand, the jammer tries to overcome the defenses by jamming all the available slots, increasing the chances of packet loss. As the angle grows, the jammer becomes less effective: from 30 to 70 degrees, the transmitter can use QPSK most of the time, still adding several redundant packets. Once $\theta \geq 80$, the jammer is completely harmless, as the jamming signal reaches the receiver only when the packet transmission is already complete. In this case, the transmitter is free to act as if the jammer were not there, using the efficient 8PSK with only one extra packet to protect the transmission from channel errors.

Fig. 7b depicts the strategies for the reactive scenario with $\lambda = 0.95$. As for the blind jammer case, short-sighted players tend to concentrate on the current transmission, so the transmitter adds more redundancy and uses more conservative modulations more often. This is not true if the angle is 20 degrees or lower, as in that case the transmitter with $\lambda = 1$ already used the most conservative settings. This is also true



(a) Usage of the three modulation types, $\lambda = 1$.

(b) Usage of the three modulation types, $\lambda = 0.95$.

(c) Average number of packets sent by T, $\lambda = 1$.

(d) Average number of packets sent by T, $\lambda = 0.95$.

(e) Average number of slots jammed by J, $\lambda = 1$.

(f) Average number of slots jammed by J, $\lambda = 0.95$.

Fig. 6: Strategies with a blind jammer.

for $\theta \geq 80$, as the transmitter adds more redundancy with packet-level coding: even if it just has to contend with the environment noise, it still privileges short-term success over a longer battery lifetime.

C. Analysis as a function of the jammer distance

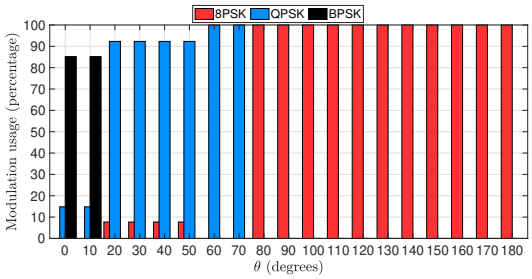
As stated above, all the results presented before depend on the considered distances between the nodes. However, the same analysis can be repeated changing the distances and obtaining similar trade-offs between reactive and blind jammer. As last step, we provide a general analysis of the trade-off between reactive and blind jammer, showing how the threshold on the angle θ depends on the jammer's distance.

To this purpose, Fig. 8 shows when it is more convenient for the transmitter to play against a reactive (blue square) or a blind (red square) jammer as a function of the distance between the jammer and the receiver. Specifically, we analyzed whether the overall number of subgames won by T is larger against a reactive or a blind jammer, for different angles θ and distances between jammer and receiver d_{JR}. When $d_{JR} = 300$ m, it is always better for the transmitter to play against a blind jammer, even for higher values of θ. Indeed, in this case the reactive jammer is always able to reactively jam the packet with all the considered modulations, even if partially. When $d_{JR} \geq 1650$ m, the reactive jammer is not able to jam any of the employed modulations at any angle. Therefore, T plays against an empty channel most of the time, even with $\theta = 0$: in this case, with $d_{JR} \geq 1650$ m, T is placed between R and J, and therefore the jamming signal needs to travel a longer distance than the legitimate packet, becoming unable to jam it.

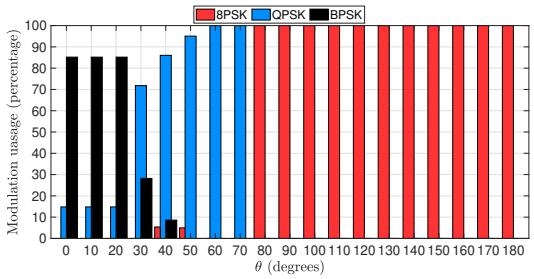
D. Imperfect position information: sensitivity analysis

The assumption of perfect information can be unrealistic in UANs, as underwater localization is often less than perfect, particularly if the jammer is trying to remain unobserved. In the following, we then perform a short sensitivity analysis for the examined strategies, in which we put the jammer at a disadvantage by reducing the precision of its localization. On the other hand, the transmitter has perfect information about the jammer, and the jammer knows the exact location of the legitimate nodes.

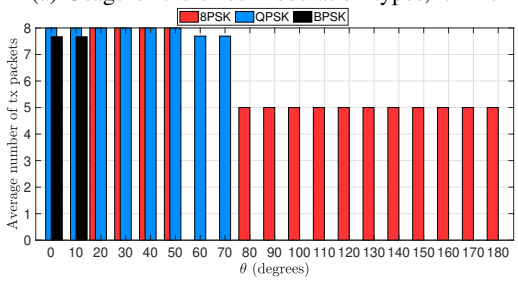
Naturally, this scenario is also not fully realistic, as the transmitter will likely have some uncertainty over the position of its adversary, but we consider this extreme case as the most advantageous for the transmitter. We then include a bivariate Gaussian noise $w \sim \mathcal{N}(0, I\sigma^2)$ on the jammer's estimate of its own position, where σ is the standard deviation and I is



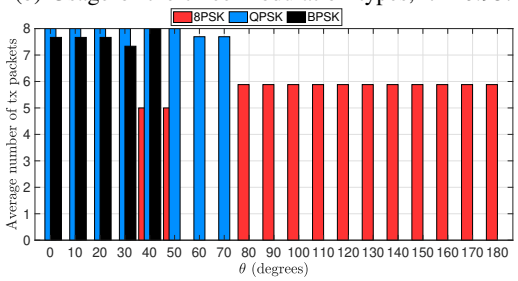
(a) Usage of the three modulation types, $\lambda = 1$.



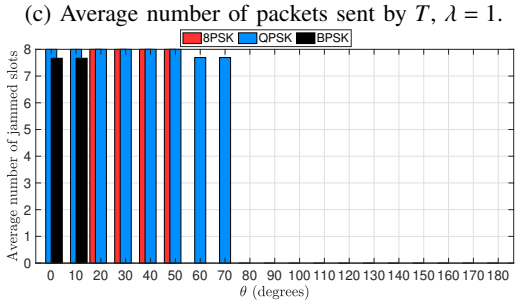
(b) Usage of the three modulation types, $\lambda = 0.95$.



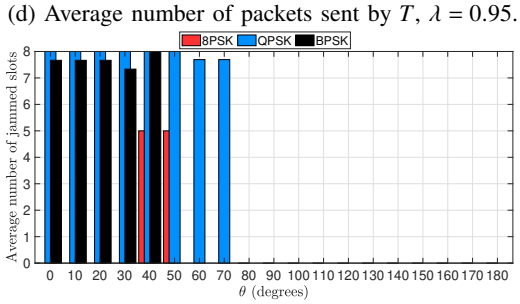
(c) Average number of packets sent by T, $\lambda = 1$.



(d) Average number of packets sent by T, $\lambda = 0.95$.



(e) Average number of packets jammed by J, $\lambda = 1$.



(f) Average number of packets jammed by J, $\lambda = 0.95$.

Fig. 7: Strategies with a reactive jammer.

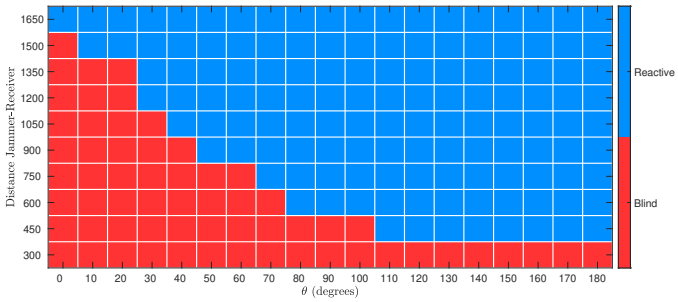


Fig. 8: Analysis as a function of the angle θ and of the distance between jammer and receiver, while keeping constant $d_{TR} = 1200$ m. Blue squares mean that it is more convenient, in terms of overall number of subgames won, for T to play against a reactive jammer. Conversely, red squares mean that it is more convenient for T to play against a blind jammer.

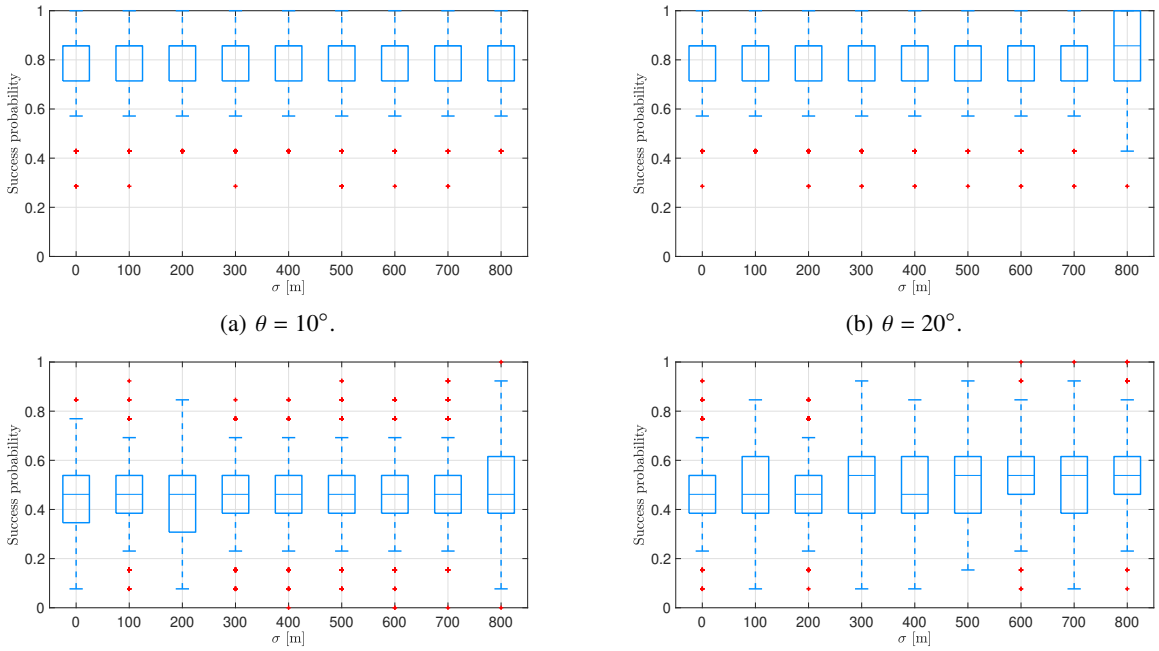
the identity matrix. This error affects both the estimate of the distance between the jammer and the receiver and the estimate of the delay between the legitimate and jamming signal, affecting the synchronization of the signals. The jammer signal will then be poorly synchronized with the legitimate packets, often overlapping with the previous or next slot. We consider this effect in the Monte Carlo simulations, whose results for a reactive jammer are shown in Fig. 9.

The reactive jammer is only slightly affected by the positioning error, particularly at low angles: if the two nodes are aligned, the precise distance matters less than getting the correct strategy, and the jamming is still effective even with some imprecision in the slot synchronization. On the other hand, Fig. 9d shows that, as θ gets closer to the cutoff value, the fraction of the packet that is jammed is increasingly small, and making intelligent decisions based on correct information becomes extremely important. In this case, the positioning error can affect the strategy, as even relatively small errors can significantly increase the success probability for the transmitter, reducing the jammer's payoff.

On the other hand, the blind jammer is almost unaffected by positioning errors, as its strategy is always the same at any angle, as Fig. 10 shows. In general, our results should hold if the information available to the nodes is imperfect, although we leave a more extensive analysis for future work.

VII. Conclusions

In this paper, we analyzed an underwater jamming scenario using game theory, exploring the effectiveness of using reactive and blind jamming. Reactive jamming is hard to implement in UANs due to the high latency caused by the small propagation speed of sound. In acoustic networks with



(a) $\theta = 10°$.

(b) $\theta = 20°$.

(c) $\theta = 40°$.

(d) $\theta = 50°$.

Fig. 9: Boxplot of the success probabilities in the reactive jammer scenario for different σ and at different angles θ.

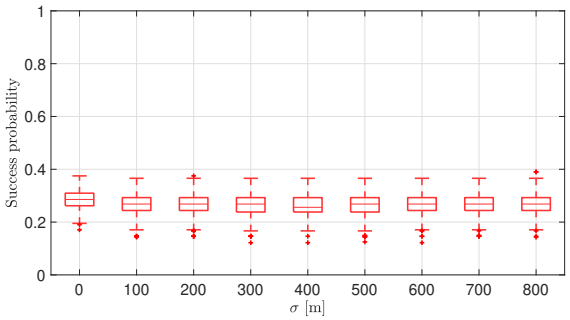


Fig. 10: Boxplot of the success probabilities in the blind jammer scenario for different σ. The blind strategy does not depend on θ.

a slotted time framework, blind jamming may become a valid jamming technique. We compared these two techniques in scenarios with different network geometries, corresponding to different levels of overlap between legitimate and jamming signals in the reactive jammer case. We compared the two jamming models using a game theoretical framework, obtaining the Nash Equilibrium for different network topologies, i.e., for different values of the angle θ, to understand where a blind jammer is more effective than a reactive one. We thoroughly investigated the strategies selected by the two players, i.e., the modulation choice and the level of redundancy, as well as how this choice changes as a function of the geometry for a given distance between transmitter and receiver to show the trade-offs between the strategies against blind and reactive jammer. Then we make a more general study, showing how the threshold on the angle θ changes as a function of the distance between the jammer and the receiver.

Our analyzed scenario shows that when the angle θ is below a certain threshold, equal to 80 degrees in our reference scenario with $d_{JR} = \frac{d_{TJ}}{2}$, a reactive jammer is always more effective than a blind one, forcing the transmitter to use a more robust modulation and spending more energy, at the cost of lowering its battery duration but increasing the chance of correctly delivering an update. Conversely, for larger values of θ the reactive technique becomes less favorable to the jammer, as 8PSK can no longer be reactively jammed. In addition, the general analysis for different distances between jammer and receiver shows that the blind strategy becomes the most convenient one for larger distances. We also performed a sensitivity analysis to understand the impact of the assumption of perfect localization information. The results obtained considering a Gaussian error on the information of the jammer about its own position show that, while a blind jammer is almost unaffected by position errors, for the reactive jammer precise information becomes more important as θ gets closer to the threshold value.

As future works, we will focus on a further investigation of the underwater jamming scenario combining the game theoretical framework with reinforcement learning techniques, that will allow us to investigate more complex strategies that include deception and planning for the adversary's changing belief over unknown parameters. We will also considering Bayesian games as a theoretical tool to model the uncertainty of the nodes about their respective positions and distances, so that the jammer and transmitter can gradually learn their own and the other's position over the course of the game. Another possibility is to extend the game to multiple receivers, so that the jammer needs to optimize its actions for the different positions and angles of all other receiving nodes as well.

ACKNOWLEDGMENT

The authors acknowledge the use of acoustic data that was acquired by CMRE during the LACE17 sea trial. This work was supported in part by the NATO Allied Command Transformation (ACT) Future Solutions Branch under the Autonomous Security Network Program and the Office of Naval Research Global under grant no N62909-17-1-2093.

REFERENCES

[1] G. Tuna and V. C. Gungor, "A survey on deployment techniques, localization algorithms, and research challenges for underwater acoustic sensor networks," *International Journal of Communication Systems*, vol. 30, no. 17, Nov. 2017, e3350.

[2] J. Heidemann, M. Stojanovic, and M. Zorzi, "Underwater sensor networks: applications, advances and challenges," *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 370, no. 1958, pp. 158–175, Jan. 2012.

[3] M. Zuba, Z. Shi, Z. Peng, J.-H. Cui, and S. Zhou, "Vulnerabilities of underwater acoustic networks to denial-of-service jamming attacks," *Security and Communication Networks*, vol. 8, no. 16, pp. 2635–2645, Nov. 2015.

[4] G. Han, J. Jiang, N. Sun, and L. Shu, "Secure communication for underwater acoustic sensor networks," *IEEE Communications Magazine*, vol. 53, no. 8, pp. 54–60, Aug. 2015.

[5] H. Luo, K. Wu, and F. Hong, "Ocean barrier: A floating intrusion detection ocean sensor networks," in *12th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN)*. IEEE, Dec. 2016, pp. 390–394.

[6] S. Bagali and R. Sundaraguru, "Efficient channel access model for detecting reactive jamming for underwater wireless sensor network," in *International Conference on Wireless Communications Signal Processing and Networking (WiSPNET)*. IEEE, Mar. 2019, pp. 196–200.

[7] F. Campagnaro, R. Francescon, P. Casari, R. Diamant, and M. Zorzi, "Multimodal underwater networks: Recent advances and a look ahead," in *12th International Conference on Underwater Networks & Systems (WUWNET)*. ACM, Nov. 2017.

[8] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 4, pp. 42–56, Dec. 2009.

[9] L. Xiao, X. Wan, W. Su, Y. Tang *et al.*, "Anti-jamming underwater transmission with mobility and learning," *IEEE Communications Letters*, vol. 22, no. 3, pp. 542–545, Jan. 2018.

[10] J. Lin, W. Su, L. Xiao, and X. Jiang, "Adaptive modulation switching strategy based on Q-learning for underwater acoustic communication channel," in *13th International Conference on Underwater Networks & Systems (WUWNET)*. ACM, Dec. 2018, pp. 1–5.

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

[12] "Evologics underwater acoustic modems," last visited: July 2021. [Online]. Available: https://evologics.de/acoustic-modems

[13] B.-C. Renner, J. Heitmann, and F. Steinmetz, "ahoi: Inexpensive, low-power communication and localization for underwater sensor networks and AUVs," *ACM Transactions on Sensor Networks*, vol. 16, no. 2, Jan. 2020.

[14] K. Pelekanakis and L. Cazzanti, "On adaptive modulation for low SNR underwater acoustic communications," in *Proc. MTS/IEEE OCEANS*, Charleston, SC, Oct. 2018.

[15] L. Ma, C. Fan, W. Sun, and G. Qiao, "Comparison of jamming methods for underwater acoustic DSSS communication systems," in *IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)*, Mar. 2018.

[16] C. Lal, R. Petroccia, M. Conti, and J. Alves, "Secure underwater acoustic networks: Current and future research directions," in *3rd Underwater Communications and Networking Conference (UComms)*. IEEE, Aug. 2016.

[17] M. Samir, M. Kowalski, S. Zhou, and Z. Shi, "An experimental study of effective jamming in underwater acoustic links," in *11th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*. IEEE, Oct. 2014, pp. 737–742.

[18] M. C. Domingo, "Securing underwater wireless communication networks," *IEEE Wireless Communications*, vol. 18, no. 1, pp. 22–28, Feb. 2011.

[19] D. Torrieri, "The performance of five different metrics against pulsed jamming," *IEEE Transactions on Communications*, vol. 34, no. 2, pp. 200–204, Feb. 1986.

[20] E. Coccolo, F. Campagnaro, A. Signori, F. Favaro, and M. Zorzi, "Implementation of AUV and ship noise for link quality evaluation in the DESERT Underwater framework," in *13th International Conference on Underwater Networks & Systems (WUWNET)*. ACM, Dec. 2018.

[21] M. Chitre, J. Potter, and S.-H. Ong, "Optimal and near-optimal signal detection in snapping shrimp dominated ambient noise," *IEEE Journal of Oceanic Engineering*, vol. 31, no. 2, pp. 497–503, Oct 2006.

[22] M. Stojanovic, "On the relationship between capacity and distance in an underwater acoustic communication channel," in *1st International Conference on Underwater Networks & Systems (WUWNET)*. ACM, Sep. 2006, pp. 41–47.

[23] K. Grover, A. Lim, and Q. Yang, "Jamming and anti–jamming techniques in wireless networks: a survey," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 17, no. 4, pp. 197–215, Jan. 2014.

[24] M. Brownfield, Y. Gupta, and N. Davis, "Wireless sensor network denial of sleep attack," in *6th Annual SMC Information Assurance Workshop (IAW)*. IEEE, Jun. 2005.

[25] L. Chen and J. Leneutre, "Fight jamming with jamming–a game theoretic analysis of jamming attack in wireless networks and defense strategy," *Computer Networks*, vol. 55, no. 9, pp. 2259–2270, Mar. 2011.

[26] G. Alnifie and R. Simon, "A multi-channel defense against jamming attacks in wireless sensor networks," in *3rd Workshop on QoS and Security for Wireless and Mobile Networks (Q2SWinet)*. ACM, Oct. 2007.

[27] R. K. Mallik, R. A. Scholtz, and G. P. Papavassilopoulos, "Analysis of an on-off jamming situation as a dynamic game," *IEEE Transactions on Communications*, vol. 48, no. 8, pp. 1360–1373, Aug. 2000.

[28] B. DeBruhl, C. Kroer, A. Datta, T. Sandholm, and P. Tague, "Power napping with loud neighbors: Optimal energy-constrained jamming and anti-jamming," in *7th Conference on Security and Privacy in Wireless & Mobile Networks (WiSec)*. ACM, Jul. 2014.

[29] F. Chiariotti, C. Pielli, N. Laurenti, A. Zanella, and M. Zorzi, "A game-theoretic analysis of energy-depleting jamming attacks with a learning counterstrategy," *ACM Transactions on Sensor Networks (TOSN)*, vol. 16, no. 1, pp. 1–25, Nov. 2019.

[30] L. Xiao, D. Jiang, Y. Chen, W. Su, and Y. Tang, "Reinforcement-learning-based relay mobility and power allocation for underwater sensor networks against jamming," *IEEE Journal of Oceanic Engineering*, vol. 45, no. 3, pp. 1148–1156, May 2019.

[31] Y. Ye, Z. Peng, and X. Hong, "Active jamming for eavesdropping prevention in underwater wireless networks," in *14th International Conference on Underwater Networks & Systems (WUWNET)*. ACM, Oct. 2019.

[32] M. Zuba, Z. Shi, Z. Peng, and J.-H. Cui, "Launching denial-of-service jamming attacks in underwater sensor networks," in *6th International Conference on Underwater Networks & Systems (WUWNET)*. ACM, Dec. 2011.

[33] G. Yang, L. Dai, and Z. Wei, "Challenges, threats, security issues and new trends of underwater wireless sensor networks," *Sensors*, vol. 18, no. 11, p. 3907, Nov. 2018.

[34] M. Khatua and S. Misra, "CURD: Controllable reactive jamming detection in underwater sensor networks," *Pervasive and Mobile Computing*, vol. 13, pp. 203–220, Aug. 2014.

[35] A. Rubinstein, A. Tversky, and D. Heller, "Naive strategies in competitive games," in *Understanding Strategic Interaction*. Springer, Berlin, Heidelberg, 1997, pp. 394–402.

[36] O. Kebkal, M. Komar, K. Kebkal, and R. Bannasch, "D-MAC: Media access control architecture for underwater acoustic sensor networks," in *Proc. IEEE/OES OCEANS*, Santander, Spain, Jun. 2011.

[37] L. Wu, J. Trezzo, D. Mirza, P. Roberts, J. Jaffe, Y. Wang, and R. Kastner, "Designing an adaptive acoustic modem for underwater sensor networks," *IEEE Embedded Systems Letters*, vol. 4, no. 1, pp. 1–4, Mar. 2012.

[38] J. Potter, J. Alves, D. Green, G. Zappa, I. Nissen, and K. McCoy, "The JANUS underwater communications standard," in *1st Underwater Communications and Networking Conference (UComms)*. IEEE, Sep. 2014.

[39] R. Petroccia, G. Cario, M. Lupia, V. Djapic, and C. Petrioli, "First in-field experiments with a bilingual underwater acoustic modem supporting the JANUS standard," in *OCEANS Conference*. IEEE/MTS, May 2015.

[40] R. Petroccia, J. Alves, and G. Zappa, "Janus-based services for operationally relevant underwater applications," *IEEE Journal of Oceanic Engineering*, vol. 42, no. 4, pp. 994–1006, Oct. 2017.
[41] W. W. Peterson and E. J. Weldon, *Error-Correcting Codes*. MIT Press, Cambridge, MA, 1972.
[42] R. Askey, *Orthogonal Polynomials and Special Functions*. SIAM, Philadelphia, PA, Jan. 1975.
[43] C. E. Lemke and J. T. Howson, Jr, "Equilibrium points of bimatrix games," *Journal of the Society for Industrial and Applied Mathematics*, vol. 12, no. 2, pp. 413–423, Jun. 1964.
[44] L. Xiao, Q. Li, T. Chen, E. Cheng, and H. Dai, "Jamming games in underwater sensor networks with reinforcement learning," in *Global Communications Conference (GLOBECOM)*. IEEE, 2015, pp. 1–6.
[45] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, May 2016.

Alberto Signori [S'19] received the B.Sc degree in information engineering and the M.Sc degree in telecommunication engineering from the University of Padova, Italy, in 2015 and 2017, respectively. In January 2018, he joined the SIGNET research group, within the Department of Information Engineering of the same university, as a research engineering. He is currently pursuing the Ph.D. degree in information engineering, at the University of Padova, under the supervision of Prof. M. Zorzi. His current research interests include the design, the analysis and the implementation of novel communication protocols and architectures for underwater networks, and network security for underwater communications. His current work involves software development for the DESERT Underwater framework. He currently collaborates with the MarTERA RoboVaaS project and with the European Defence Agency project SALSA. In 2019, he received the Best Student Paper Award at International Conference on Underwater Networks & Systems (WUWNet). In 2020, he received the Best Paper Award at IEEE INFOCOM International Workshop on Wireless Communications and Networking in Extreme Environments (WCNEE).

Federico Chiariotti [S'15-M'19] is currently a post-doctoral researcher at the Department of Electronic Systems, Aalborg University, Denmark. He received his Ph.D. in information engineering in 2019 from the University of Padova, Italy. He received the bachelor's and master's degrees in telecommunication engineering (both *cum laude*) from the University of Padova, in 2013 and 2015, respectively. In 2017 and 2018, he was a Research Intern with Nokia Bell Labs, Dublin. He has authored over 40 peer-reviewed papers on wireless networks and the use of artificial intelligence techniques to improve their performance. He was a recipient of the Best Paper Award at several conferences, including the 2020 IEEE INFOCOM WCNEE Workshop. His current research interests include network applications of machine learning, transport layer protocols, Smart Cities, bike sharing system optimization, and Age of Information.

Filippo Campagnaro [M'19] received the B.Sc. and the M.Sc. degrees from the University of Padova, Italy, in 2012 and 2014, respectively. In 2014, he joined the SIGNET Group, within the Department of Information Engineering of the same university, as a Research Engineer. In October 2019 he completed the Ph.D. program in Information Engineering and joined the same department as a post-doctoral researcher and lecturer of ICT master courses. His Ph.D. thesis involves the design and the evaluation of multimodal underwater optical and acoustic networks, with a particular focus on simulation and field experimentation (defence scheduled for February 2020). Filippo has joined many sea trials with the NATO STO CMRE (La Spezia, Italy), EvoLogics GmbH (Berlin, Germany), ENEA (Rome, Italy), the IMDEA Network Institute (Madrid, Spain), and the University of Haifa (Israel). He is the Technical Manager of the MarTERA RoboVaaS project, and collaborates with the European Defence Agency project SALSA. His current work involves software development for the DESERT Underwater framework as well as the design of novel communication stacks and architectures, with special attention to cross-layer and multi-technology designs. His research interests revolve mainly around the design, analysis, implementation, and field evaluation of multimodal underwater networks. Since 2017, he collaborates with Wireless and More srl, a spin-off company of the University of Padova, which he joined as a part-time employee in October 2019.

Roberto Petroccia [SM'18] received the Laurea (highest Honors) degree and his Ph.D. from University of Rome "La Sapienza," Italy, in 2006 and 2010, respectively, both in Computer Science. He was a Research Staff member in the same University until 2015. Since 2015, he has been a Research Scientist in the NATO STO Center for Maritime Research and Experimentation, La Spezia, Italy. His research interests include wireless sensor networks, underwater communications, networking, interoperability, and security, a field he has contributed to with over fifty papers published in leading venues (h-index 21, i10-index 42, Google Scholar, Sep'21). In the last ten years, Dr. Petroccia has participated in more than 30 experimental campaigns at sea where innovative underwater solutions he developed have been extensively tested. Dr Petroccia has been collaborating with several underwater acoustic modem and vehicle manufacturing companies and research labs to design technologies supporting cooperative underwater networking. He was in the organizing committee of the last three IEEE UComms editions, and ACM WUWNet 2012 and 2014 conferences. In 2019, he was selected to be part of the IEEE OES YP-BOOST program. Dr Petroccia is an IEEE Senior Member since 2018 and a member of the IEEE OES AdCom since 2021. He is also an invited lecturer of the Master's program in Ocean Engineering offered by the University of Pisa, Italy and of the Ph.D. course of the University of Calabria (Italy), Department of Informatics, Modelling, Electronics and System Engineering. Dr Petroccia has also supervised the work of several master's theses and Ph.D. students.

Konstantinos Pelekanakis [S'06-M'09-SM'17] received his Diploma from the Department of Electronic and Computer Engineering, Technical University of Crete, Greece, in 2001 and his M.Sc. and Ph.D. degrees in Mechanical and Ocean Engineering from the Massachusetts Institute of Technology (MIT), Cambridge, USA, in 2004 and 2009, respectively. He has been awarded with MIT Presidential Fellowship in 2001. From 2009 to 2015, he worked with the Acoustic Research Laboratory (ARL) at the National University of Singapore (NUS) as a Research Fellow. From 2011 to 2014, he also worked as Lecturer for the Master of Defence Technology and Systems (MDTS) Program at the Temasek Defence Systems Institute (TDSI) in Singapore. He is currently a Senior Scientist at the NATO Science and Technology Organization (STO), Centre for Maritime Research and Experimentation (CMRE) in La Spezia, Italy. In 2018, he was co-recipient of the NATO Scientific Achievement Award and in 2019 he was the co-recipient of the IET Premium Award for Best Paper in Radar, Sonar & Navigation. His main research area is statistical signal processing for underwater acoustic communications. Dr. Pelekanakis, has served as the secretary and vice chairman for the IEEE OES Singapore chapter in 2013 and 2014, respectively. He has served in the organizing committee for IEEE UComms 2016-2020. He also serves as an Associate Editor for IEEE Journal of Oceanic Engineering.

Pietro Paglierani [S'97-M'02-SM'08] received the Master and PhD degree in electronic engineering from the University of Padua, Italy. He is now a Scientist at the Nato Centre for Maritime Research and Experimentation, La Spezia, Italy. His main research interests focus on Digital Signal Processing, in particular on Acoustic Underwater Communications and Secure Communications in Underwater networks. Previously, he was with Italtel S.p.A, Milan, where he was the team leader of the Digital Signal Processing group in the R&D unit, and Tektronix, Necsy S.p.A and Consorzio Padova Ricerche, where he was a designer of signal processing applications and algorithms for telecommunications.

João Alves [M'09–SM'17], got his B.S. and M.Sc. in Electrotechnical Engineering, Control and Robotics from the Technical University of Lisbon and has been working in underwater robotics and associated technologies since 1995. He played a key role in the development of the control architectures for pioneering vehicles developed at the Technical University of Lisbon. In late 2009, he joined the NATO Undersea Research Centre (NURC), now Centre For Maritime Research and Experimentation (CMRE) as a scientist working on underwater communications. He led studies in support of establishing the first underwater communications standard and developed innovative protocols for underwater ad hoc networking. In 2014 he took a leadership role as Principal Scientist responsible for the underwater communications activities at CMRE. He conducted several sea trials as scientist in charge and in 2019, he took leadership of a wide programmatic area of CMRE for interoperability and security of maritime unmanned systems and was appointed as CMRE's representative for the NATO Maritime Unmanned Systems (MUS) Initiative. João received the NATO Scientific Achievement Award 2018 for his work as team leader in the development and promulgation of JANUS – the first digital underwater communications standard. He is the chairperson for the IEEE OES UCOMMS series of conferences, organised by the CMRE. He is a guest editor for the IEEE Journal of Oceanic Engineering and an area editor for the Elsevier Journal of Ad Hoc Networks.

Michele Zorzi [F'07] received his Laurea and PhD degrees in electrical engineering from the University of Padova, Italy, in 1990 and 1994, respectively. During the academic year 1992-1993 he was on leave at the University of California at San Diego (UCSD). In 1993 he joined the faculty of the Dipartimento di Elettronica e Informazione, Politecnico di Milano, Italy. After spending three years with the Center for Wireless Communications at UCSD, in 1998 he joined the School of Engineering of the University of Ferrara, Italy, where he became a professor in 2000. Since November 2003 he has been on the faculty of the Information Engineering Department at the University of Padova. His present research interests include performance evaluation in mobile communications systems, WSN and Internet of Things, cognitive communications and networking, 5G mmWave cellular systems, vehicular networks, and underwater communications and networks.

Dr. Zorzi received several awards from the IEEE Communications Society, including the Best Tutorial Paper Award in 2008 and 2019, the Education Award in 2016, the Stephen O. Rice Best Paper Award in 2018, and the Joseph LoCicero Award for Exemplary Service to Publications in 2020. He was the Editor-in-Chief of the IEEE Wireless Communications magazine from 2003 to 2005, the IEEE Transactions on Communications from 2008 to 2011, and the IEEE Transactions on Cognitive Communications and Networking from 2014 to 2018. He has served the IEEE Communications Society as a Member-at-Large of the Board of Governors from 2009 to 2011 and from 2021 to 2023, as the Director of Education from 2014 to 2015, and as the Director of Journals from 2020 to 2021.