A Game-Theoretic and Experimental Analysis of Energy-Depleting Underwater Jamming Attacks

Alberto Signori *Student Member, IEEE*, Federico Chiariotti *Member, IEEE*, Filippo Campagnaro *Member, IEEE*, Michele Zorzi *Fellow, IEEE*

***Abstract*—Security aspects in underwater wireless networks have not been widely investigated so far, despite the critical importance of the scenarios in which these networks can be employed. For example, an attack to a military underwater network for enemy targeting or identification can lead to serious consequences. Similarly, environmental monitoring applications such as tsunami prevention are also critical from a public safety point of view. In this work, we assess a scenario in which a malicious node tries to perform a jamming attack, degrading the communication quality of battery-powered underwater nodes. The legitimate transmitter may use packet level coding to increase the chances of correctly delivering packets. Because of the energy limitation of the nodes, the jammer's objective is twofold, namely: *(i)* disrupting the communication and *(ii)* reducing the lifetime of the victim by making it send more redundancy. We model the jammer and the transmitter as players in a multistage game, deriving the optimal strategies. We evaluate the performance both in a model-based scenario and using real experimental data, and perform a sensitivity analysis to evaluate the performance of the strategies if the real channel model is different from the one they use.**

***Index Terms*—Underwater acoustic networks; jamming; game theory; block code; security in underwater networks.**

I. Introduction

Underwater sensor networks are enabling several military, industrial, and environmental applications: the ability to monitor the environment remotely is extremely useful for oil and gas platform and pipeline maintenance, seabed erosion and tsunami risk mitigation, and coastal patrol. In this latter critical application, underwater sensor nodes can identify and target enemies, extending the monitoring range and allowing just a few patrol ships to cover a very wide area [2].

However, underwater communications are hindered by the high attenuation of electromagnetic waves. For this reason, radio communications are only possible over very short-range broadband links [3], and nodes at longer distances need to use acoustic waves: depending on the frequency, acoustic communication is possible at ranges from hundreds of meters up to tens of kilometers [4]. However, even acoustic communications present some challenges, as sound waves have a low propagation speed, causing long delays, and the environmental noise caused by wind, marine life, and shipping activities can be very strong. Furthermore, there are strong multi-path effects due to the signal reflections with the bottom and the surface [5], [6].

In this already hostile environment, a Denial-of-Service (DoS) attack can be very effective, disabling the victim node's communications and disrupting the monitoring operation. The most effective way to perform it is by physical layer jamming: the attacker transmits a high-power signal, causing interference and blocking the correct reception of packets. There are effective countermeasures that increase the robustness of the transmission to jamming attacks, such as power control and channel coding, but they come at a cost: the transmitter node needs to spend more energy to protect its transmissions, depleting its battery faster and reducing its lifetime.

In this work, we consider a jamming scenario in which the attacker has a double objective: it tries to block the legitimate communications, but it also turns the transmitter's own defense mechanism against it, forcing it to deplete its battery faster. We model the scenario using game theory, considering both nodes as rational players in a zero-sum multistage game, in which each burst of packets represents a subgame. The jammer decides how long it will jam the channel, while the legitimate transmitter chooses the amount of redundancy that it will add to each burst: both nodes are battery-limited, and they both have a trade-off between increasing the probability of success in the current subgame and saving their battery.

We can derive the optimal long-term strategies for both players using a dynamic programming approach. For the sake of analytical tractability, in this work we focus on the case of *complete information* available to both players, including the outcomes of each transmission attempt and the battery state of the nodes at any time. We study the trade-off between energy consumption and transmission success probability as a function of the distances between transmitter, receiver and jammer.

Our game-theoretic model and its Monte Carlo results were presented in [1]. In the present work, we consider a more realistic setting considering the modulation used by S2C EvoLogics modems, and present the results obtained in a lake experiment with the aforementioned modems. Additionally, we expand the mathematical model by deriving recursive analytical formulations of the lifetime and success probability, using them to derive the results instead of Monte Carlo simulations. We also assess the computational complexity of the dynamic programming approach used to derive the optimal strategies for both players. Finally, we analyze what happens when the nodes do not have perfect information on the environment, and on the channel in particular, to test the robustness of the system in a real scenario where strategies are obtained in advance without knowing the actual channel conditions in the deployment location. We present the result of a sensitivity

A. Signori (corresponding author, email: signoria@dei.unipd.it), F. Chiariotti, F. Campagnaro, and M. Zorzi are with the University of Padova, Department of Information Engineering, Padua, Italy.

This paper is an extension of a previous work, presented at ACM WUWNet '19 with the title "Jamming the underwater: a game-theoretic analysis of energy-depleting jamming attacks" [1].

analysis on the packet error probabilities, as well as on the chosen channel model.

The rest of the paper is organized as follows. In Sec. II, we give an overview of the state of the art models for DoS jamming attacks, focusing on the underwater scenario. In Sec. III, we present the game theoretic model and the system scenario. Sec. IV explains how to derive the optimal strategies for the jammer and the transmitter. Sec. V defines the evaluation scenario, Sec. VI describes the numerical evaluations, and Sec. VII concludes the paper.

II. Related Work

Physical layer jamming is one of the most common DoS attacks [7]. The principle behind it is simple, yet powerful: a malicious node injects signals into the channel in order to deny or at least reduce service to the legitimate users by increasing their noise level and preventing them from receiving messages correctly. For instance, the attacker can send single-tone jamming signals or white Gaussian noise signals with the same bandwidth as the transmitter [8]. The latter approach makes the attacker more flexible, as the former is not effective if the transmitter uses spread-spectrum techniques, such as frequency hopping or direct sequence spread spectrum [9]. Other approaches, such as adaptive jamming, require the attacker to have an adaptive physical layer so as to change its modulation or transmission power. The victims of a jamming attack may passively adopt a simple duty cycling strategy [10], or actively react to the DoS attack, e.g., by increasing their transmit power [11] or using channel-hopping [12]. In case of active defense, game theory is often used to model the interaction between the jammer and its victim: for instance, in [13], the theory is applied to a satellite transmission using frequency-hopping as a defense mechanism. The main drawback of active defenses is typically an increased energy consumption, which means that the defenses themselves can be exploited by the attacker to deplete the victim node's battery and interrupt its transmissions. In this case, energy consumption needs to be included in the game formulation by introducing power constraints [14], or by considering nodes with limited energy. In the latter case, the jamming attack is typically modeled as a zero-sum game with a finite horizon [15], and optimal strategies are derived by applying dynamic programming bottom-up, i.e., starting from the lowest energy levels and exploiting the solution to find the optimal strategy for higher energy levels. Our previous work [16] applies this principle in an Internet of Things (IoT) network, exploiting retransmissions as part of the defense strategy. It also includes an analysis of the game with incomplete information on the jammer's capabilities.

Some recent works have also analyzed the jamming issue in the context of underwater acoustic networks. For example, [17] applies a reinforcement learning deep Q-network-based transmission scheme, using movement as a countermeasure against a jamming attack in a mobile underwater acoustic network. The jammer sends acoustic signals with the same band as the transmitter, and each agent can decide its own transmission power level. The problem is modeled as a dynamic game in which all nodes are power-constrained; the winner of the game is the last node to completely deplete its battery. The results are proven via both simulation and a pool test, in short range.

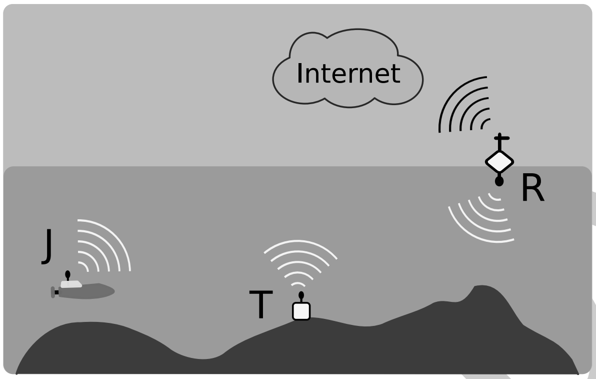

Fig. 1. An underwater jamming attack: a jammer J tries disrupting the communication between a transmitter T and its intended receiver R.

In underwater acoustic networks, the propagation delay can be longer than the signal duration [18], especially in long range scenarios. In this case, a malicious node that observes the transmitter behavior and generates jamming signals as soon as it detects a new transmission cannot jam the current packet, since the jamming signal would reach the receiver only after the complete reception of the transmitted packet. Therefore, a jamming attack is effective in scenarios where the jamming signal reaches the receiver before the payload packet is completely received, such as when the jammer is placed between transmitter and receiver, or when the transmitter sends a sequence of packets with a deterministic or predictable pattern, such as in data muling applications. In [19], the authors propose a jamming defense strategy to provide secrecy for block transmission in underwater acoustic networks. They exploit the half-duplex nature of underwater transceivers and the large propagation delays to create interference at the eavesdropper. Specifically, the receiver transmits jamming packets to the malicious node during the guard time between data blocks, keeping the jammer transducer in the reception state and thereby preventing it from transmitting malicious signals. These packets do not cause deafness at the transmitter, as the propagation delay is larger than the guard time between blocks. In [20], a game-theoretic approach is applied to study jamming attacks in an underwater sensor network. Specifically, the authors analyzed a scenario in which two sensor nodes transmit their data to a sink node using Frequency Division Multiple Access (FDMA). In this scenario, a jammer can disrupt the communication by injecting a signal only in one of the subbands used in the network. A Bayesian zero-sum game is considered to take into account the uncertainty on the distance between the sensor nodes and the sink. Differently from our work, the authors do not consider any power constraint in the problem formulation nor any form of active defense, such as packet level coding, and did not perform any field test to characterize how the presence of the jammer affects the reception.

III. Game Theoretic Model

We consider a transmitter T at a distance d_{TR} from a receiver R, under attack from a jammer J, which is placed at a distance d_{JR} from R. The scenario is shown in Fig. 1: T needs to periodically send an update to a receiver R, and a malicious jammer J tries to block its transmission and deplete its battery.

In order to protect its transmission from the attack and from ambient noise, T uses packet-level coding: whenever it needs to send a message to R, it also sends a number of redundancy packets to protect the transmission from jamming attacks. Assuming an efficient packet-level code, the K information packets can be recovered if at least any K of the N coded packets are correctly received [21].

The jamming attack is modeled as a zero-sum game $\mathbb{G}$ between the two rational players T and J, i.e., a completely adversarial and symmetric game in which each gain for one player is balanced by a loss for the other [16]. The zero-sum model is justified by the fact that an attacker will naturally want to disrupt the operation of the legitimate node as much as possible, thus having completely adversarial goals; this assumption is often used in jamming games. In this work, we study a complete information scenario. The complete information assumption is motivated by the fact that, at the end of each time frame, R sends a feedback packet containing information on how many packets from T it detected, how many slots were jammed by J, and how many packets it received successfully. We assume that such feedback packets are perfectly received by both J and T, as R is not power constrained.

The jamming game is composed of a series of packet transmission subgames G_m, with $m \in \mathbb{N}$. In each subgame, node T uploads its data to node R, in an attempt to report information on the surrounding environment. Such data is chunked into K payload packets, and T can exploit *(i)* Forward Error Correction (FEC) in order to increase the probability of successful communication over unreliable or noisy communication channels, and *(ii)* Cyclic Redundancy Check (CRC) to detect residual error-laden packets and discard them. In each subgame G_m, T can decide the amount of redundancy to use, i.e., the number $N_T^{(m)}$ of packets to send over the channel. A maximum of $2K$ transmission opportunities is configured in each subgame, thus $K \leq N_T^{(m)} \leq 2K$.

The outcome of each transmission attempt depends on the choices made by T and J, and on the conditions of the channel, which is modeled stochastically. In particular, the transmission succeeds if T is able to counteract the channel impairments *and* the jamming attacks and to deliver at least K packets to the destination node within the duration of the subgame. We assume a packet erasure channel and an efficient code, so R can recover the K information packets if any K of the $N_T^{(m)}$ coded packets are correctly received [21].

TABLE I
Notation and meaning of system parameters for game players $i \in \{T, J\}$.

Parameter	Meaning
K	Minimum number of packets to be delivered for success
τ	Duration of a packet transmission
Γ	Time horizon of multistage game $\mathbb{G}$
λ	Exponential discounting factor
α_i	Energy/PDR weighing factor
$u_i^{(m)}$	Payoff function in subgame m
$U_i^{(m)}$	Payoff function in multistage game $\mathbb{G}$ in subgame m
$\chi_i^{(m)}$	Indicator function of the success of subgame m
$f_i^{(m)}$	Energy penalty function in subgame m
$N_T^{(m)}$	Number of packets that T sends in subgame m
$N_{\mathrm{C}}^{(m)}$	Packets sent over clear channel in subgame m
$N_{\mathrm{B}}^{(m)}$	Packets sent over jammed channel in subgame m
$N_J^{(m)}$	Number of slots that J tries to jam in subgame m
$D^{(m)}$	Total packets delivered in subgame m
$d_{\mathrm{C}}^{(m)}$	Packets delivered over clear channel in subgame m
$p_{e_{\mathrm{C}}}$	Packet error probability over clear channel
$p_{e_{\mathrm{B}}}$	Packet error probability over jammed channel
$B_i^{(m)}$	Battery level in subgame m
$E_{\mathrm{tx},i}$	Energy required to transmit/jam a packet
$P_{\mathrm{tx},i}$	Transmission/jamming power

Both players are battery-powered nodes, and the dynamics of the game are exhaustively characterized by their energy evolution, i.e., the evolution of their battery charge during the game. The battery levels take discrete values in the sets $\mathcal{B}_i \triangleq [0, 1, \dots, B_i^{(0)}]$, $i \in \{T, J\}$, with $B_i^{(0)} \in \mathbb{N}$ being the initial charge of the battery. The battery levels in the sets $\mathcal{B}_i$ are normalized by the energy $E_{\mathrm{tx},i}$, $i \in \{T, J\}$, used to transmit each legitimate packet or jam each slot; we consider the quantum $E_{\mathrm{tx},i}$ to be constant, since our active defense strategy does not involve power control. Note that, as neither energy harvesting nor other forms of energy replenishment are considered, the battery levels can only decrease during the game. In each subgame, node T decides the number of packets $N_T^{(m)}$ to send to complete the data transmission, and this corresponds to an energy consumption of $N_T^{(m)}$ quanta, since battery levels are normalized. Note that, the larger $N_T^{(m)}$, the more robust the communication, but the faster the depletion of T's battery and the whole game duration. Similar energy considerations affect the choice of the jammer, which has to decide the number of transmission opportunities $N_J^{(m)}$ to jam in order to disrupt T's communication.

We now describe the structure of a single subgame and then illustrate the evolution of the multistage full game. Table I reports a summary of the notation used.

A. The Packet Transmission Subgame

Each subgame G_m models the attempt made by T to transmit K information packets to R. The time after the beginning of the first packet transmission is slotted into a time frame of $2K$ time slots; each slot corresponds to the time τ necessary to transmit a packet. Note that the long propagation delays that characterize the underwater scenario give an advantage to T: the first packet can never be jammed, as the jammer does not have the time to sense the transmission and send the jamming signal. However, since J knows the duration of the time slot and the position of the transmitter and receiver, we assume that it can trigger its transmissions to perfectly jam the subsequent time slots.

Thus, T decides *(i)* how many packets $N_T^{(m)} \in \mathcal{N}_T^{(m)} \triangleq \{K, K+1, \dots, \min(2K, B_T^{(m)})\}$ to send to R, and *(ii)* which time slots to employ for the transmission among the $2K$ available. Similarly, J chooses *(i)* the number of slots $N_J^{(m)} \in \mathcal{N}_J^{(m)} \triangleq \{0, 1, \dots, \min(2K-1, B_J^{(m)})\}$ to jam, and *(ii)* the $N_J^{(m)}$ jammed time slots out of $2K-1$ (as the first packet cannot be jammed). Note that the actions of both players are limited by the current battery level at stage m, i.e., $B_i^{(m)}$, $i \in \{T, J\}$. T and J make independent decisions on $N_T^{(m)}$ and $N_J^{(m)}$, respectively. Such decisions are made in advance for the whole time frame, right before the transmission of the first packet.

The payoffs of the players are convex combinations of monotonic functions of the energy required to transmit/jam the packets and of the Packet Delivery Ratio (PDR). By tuning the weight $\alpha \in [0,1]$, the main objective of the players can be shifted between saving energy, thereby reducing $N_T^{(m)}$ and $N_J^{(m)}$, and delivering more packets. Based on these considerations, we express the players' payoffs for a single subgame m as:

$$u_T^{(m)} = \alpha\, f_T^{(m)} + (1-\alpha)\chi_T^{(m)} \tag{1}$$

$$u_J^{(m)} = -u_T^{(m)}\,. \tag{2}$$

The first term of Eq. (1) is related to energy, while the second term concerns the outcome of the communication. In particular, the indicator term $\chi_T^{(m)}$ is equal to one if the subgame m ends with T successfully delivering at least K packets to R, and zero otherwise.

Function $f_T^{(m)}$ gives T a penalty for consuming energy when transmitting packets. In particular, we set:

$$f_T^{(m)} = -\frac{N_T^{(m)}}{(2K+1)}. \tag{3}$$

The additional term 1 in the denominator of (3) is arbitrary and ensures that the absolute value of $f_T^{(m)}$ is always smaller than 1, thus preventing any strategy to be dominated by not transmitting at all. Moreover, notice that the number of slots $N_J^{(m)}$ jammed by node J is not explicitly present in the payoffs for the single subgame, since we assumed a zero-sum game. Nevertheless, $N_J^{(m)}$ still plays a major role in the full game: the larger $N_J^{(m)}$, the higher the energy consumed by node J, and the faster its battery depletion.

Finally, the transmitter's choice of the time slots in which to transmit packets, and the jammer's choice of which time slots to jam, can be modeled as a simple anti-coordination game: T's objective is to avoid the jammer and transmit as many of its packets as possible on a clear channel, while J's objective is to correctly guess the slots that T will use and jam them, so as to maximally disrupt the communication.

B. *The Full Jamming Game*

In a battery-limited scenario, the greedy strategy that maximizes the payoff for the next subgame is not always optimal. The solution of the full jamming game $\mathbb{G}$ maximizes a long-term payoff function within a given time horizon Γ, which represents the number of future subgames to consider in the payoff. The players' payoffs in the multistage game $\mathbb{G}$ at stage m are given by:

$$U_i^{(m)}(\Gamma) = \sum_{\gamma=m}^{m+\Gamma-1} \lambda^{\gamma-m} u_i^{(\gamma)}, \quad i \in \{T, J\} \tag{4}$$

where $\lambda \in [0,1]$ is a future exponential discounting factor [22], $u_i^{(m)}$, $i \in \{T, J\}$ is the subgame payoff defined in (1) and (2), and Γ is the length of the payoff horizon, i.e., the number of subgames that are considered. When Γ is finite, we can consider $\lambda = 1$ with no convergence issues, while, for $\Gamma = +\infty$, we must consider $\lambda < 1$. Note that the payoff $u_i^{(m)}$ for a single subgame coincides with $U_i^{(m)}(1)$. In general, J will behave in a foresighted manner if Γ is large enough: its energy expenditure is not explicitly penalized, but it can reduce the reward if it affects the number of subgames it can play in.

IV. Analytical Solution of the Game

In this section, we explain how to derive the optimal strategies for the two players in the case of perfect knowledge about the opponent's position and battery level at the beginning of each subgame. We define as strategy s_i the action chosen by player $i \in \{T, J\}$, i.e., the amount of energy required to transmit the legitimate packets or to jam the slots, respectively. According to the game defined in Sec. III, the strategy space is thus $\mathcal{N}_i^{(m)}$ $i \in \{T, J\}$ in each subgame. Note that the strategies concern what to do in each subgame, but are chosen based on the expected evolution over multiple subgames, as dictated by Γ. We are interested in evaluating the Nash Equilibrium (NE), i.e., the pair of optimal strategies (s_T^*, s_J^*) that are mutual best responses [23]. In other words, a NE is reached when neither player can improve its expected payoff by changing its strategy unilaterally. Since the payoff functions of the two players (see (4)) can include multiple subgames, the NE of the jamming game can be calculated exactly with *dynamic programming*. The NE may be *pure*, i.e., correspond to deterministic strategies, or *mixed*, when strategy $s_i^{(m)}$ for player $i \in \{T, J\}$ is a probability distribution $\Phi_{s_i}(N_i)$ over $\mathcal{N}_i^{(m)}$. Under the assumption of complete information, strategies are determined by the state of the two players, assuming an optimal strategy for lower battery states.

In the following, we first present the expressions for the expected payoffs of nodes T and J that are needed to compute the NE, and then describe the procedure to solve the game analytically through dynamic programming.

A. *Expected Payoff Calculation*

To derive the NE, we need to characterize the expected payoff for a single subgame, denoted as $\mathbb{E}\left[U_i^{(m)}(1)\middle| N_T^{(m)}, N_J^{(m)}\right]$ for the m-th stage of game $\mathbb{G}$. Such expected payoff is equal to the expectation of the payoffs $u_i^{(m)}$, $i \in \{T, J\}$ given in Eqs. (1) and (2). In the remainder of this section, we will omit superscript (m) for the sake of a lighter notation.

The expected payoffs $\mathbb{E}\left[u_i\middle| N_T, N_J\right]$, $i \in \{T, J\}$ can be calculated from the quantity $\mathbb{E}\left[\chi_i\middle| N_T, N_J\right]$, $i \in \{T, J\}$, which represents the expected outcome of the subgame (as introduced in Sec. III-A, χ_T and $\chi_J = 1 - \chi_T$ are indicator terms for the transmission and jamming success, respectively). We introduce quantities $N_\mathrm{C} \leq N_T$ and $N_\mathrm{B} \leq N_T$ to indicate the number of packets that node T sends over a clear and blocked (i.e., jammed) channel, respectively. Obviously, $N_T = N_\mathrm{C} + N_\mathrm{B}$, so we can easily obtain the value of N_C once we know N_B. We also know that $N_C \geq 1$, as the first packet can never be jammed. Using the law of total probability, for node T we have:

$$\mathbb{E}\Big[\chi_T \,\Big|\, N_\mathrm{T}, N_\mathrm{J}\Big] = \sum_{N_\mathrm{C}=1}^{N_\mathrm{T}} \mathbb{E}\Big[\chi_T \,\Big|\, N_\mathrm{B}, N_\mathrm{T}\Big] \mathrm{P}\Big(N_\mathrm{B} \,\Big|\, N_\mathrm{T}, N_\mathrm{J}\Big) \tag{5}$$

The first term inside the summation is the expectation of a subgame success, given the number of packets successfully delivered and jammed during that subgame, and can be expressed as:

$$\begin{aligned}\mathbb{E}\Big[\chi_T \Big| N_\mathrm{B}, N_\mathrm{T}\Big] = \sum_{D=K}^{N_T} \sum_{d_\mathrm{B}=0}^{D} \binom{N_\mathrm{T}-N_\mathrm{B}}{D-d_\mathrm{B}} p_{e_\mathrm{C}}^{(N_\mathrm{T}-N_\mathrm{B})-(D-d_\mathrm{B})} \\ \times (1-p_{e_\mathrm{C}})^{D-d_\mathrm{B}} \binom{N_\mathrm{B}}{d_\mathrm{B}} p_{e_\mathrm{B}}^{N_\mathrm{B}-d_\mathrm{B}} \left(1-p_{e_\mathrm{B}}\right)^{d_\mathrm{B}} .\end{aligned} \tag{6}$$

The external summation iterates on all possible values of the number of delivered packets $D \leq N_T$ resulting in a success. Eq. (6) then splits D between packets that are delivered over a jammed channel, i.e., $d_\mathrm{B} \leq D$, and those which are delivered over a clear channel, i.e., $D - d_\mathrm{B}$. For the two cases, the packet error probability is equal to p_{e_C} and p_{e_B}, respectively, and is a function of the Signal to Noise Ratio (SNR) or Signal to Interference and Noise Ratio (SINR).

We consider a realistic modulation, such as Chirp Spread Spectrum (CSS), which is used in several real underwater acoustic modems. If a different modulation is used, the only required change is in (7), while the rest of the model remains the same. The packet error probability in the case of a jammed signal, p_{eB}, can be computed as presented in [24], which computes the Bit Error Rate (BER) considering Differential Quadrature Phase Shift Keying (DQPSK) modulation in a radio frequency channel. We now adapt the definition of the BER to the acoustic underwater scenario. The BER for a CSS signal, p_bit^CSS, is computed as:

$$p_\text{bit}^\text{CSS} = Q(a,b) - \frac{1}{2} e^{-(a^2+b^2)/2} I_0(ab) \tag{7}$$

where Q is the Marcum Q function, I_0 is the modified Bessel function of order 0, and a and b are defined as:

$$\begin{aligned} a &= \sqrt{\frac{2E_b/N_0}{1+J_0/N_0}(1-\sqrt{0.5})} \\ b &= \sqrt{\frac{2E_b/N_0}{1+J_0/N_0}(1+\sqrt{0.5})} \end{aligned}, \tag{8}$$

where E_b is the received energy per bit of the transmitter, N_0 is the noise power spectral density, and J_0 is the power spectral density of the jammer, given by:

$$E_b = \frac{\tau}{L} P_{\mathrm{tx},T}\, g_\mathrm{T}, \qquad J_0 = \frac{P_{\mathrm{tx},J}\, g_J}{B} . \tag{9}$$

The SINR is then given by $\mathrm{SINR} = \frac{E_b L/\tau}{N_0 B + J_0 B}$, where L is the packet length in bits, $P_{\mathrm{tx},i}$ represents the transmit power of node $i \in \{T, J\}$, B is the transmission bandwidth, and g_T and g_J model the gain of the underwater acoustic channel between T and R and between J and R, respectively. Their values depend on the distances d_TR and d_JR to the receiver, respectively, as well as on the carrier frequency of the signal. Both noise and channel gain for an underwater acoustic channel can be computed as described in [4, Sec. II].

Finally, the packet error probability p_{e_B} is given by:

$$p_{e_\mathrm{B}} = 1 - \left(1 - p_\text{bit}^\text{CSS}\right)^L, \tag{10}$$

We also consider the packet error probability if a Reed-Solomon (RS) channel code is employed [25]. We analyzed the performance with an RS(127,78) with $q = 7$ bits per symbol and an error correction capability of $t = 24$ symbols. In this scenario, the packet is lost if more than t symbols are not received correctly:

$$p_{e_\mathrm{B}} = \sum_{i=t+1}^{N} \binom{N}{i} p_s^i (1-p_s)^{(N-i)} \tag{11}$$

where $p_s = 1 - \left(1 - p_\text{bit}^\text{CSS}\right)^q$ is the symbol error probability.

Finally, the second term in Eq. (5) can be expressed as:

$$\mathrm{P}\Big(N_\mathrm{B} \,\Big|\, N_T, N_J\Big) = \frac{\binom{N_T-1}{N_\mathrm{B}}\binom{(2K-1)-(N_T-1)}{N_J-N_\mathrm{B}}}{\binom{2K-1}{N_J}} , \tag{12}$$

where we have imposed the condition that the first transmitted packet cannot be jammed due to the signal propagation characteristics of the underwater scenario, as described in Sec. III. In Eq. (12) , we assume that both the transmitter and the jammer choose the slots to transmit (or jam) according to a uniform distribution among all possible N_T-tuples (or N_J-tuples) of slots. This is the choice that maximizes (for the transmitter) or minimizes (for the jammer) the probability that at least K slots in the transmission are free from collision. This strategy pair is the NE for the anti-coordination slot selection game we mentioned in Sec. III-A: since all slots after the first have the same success probability, the optimal strategy for both players is to randomly choose $N_T - 1$ and N_J among them. Any other strategy would be strictly dominated, since it would provide the opponent with a pattern to exploit: if T chooses a slot with high probability, J will try to mirror it and jam the communication more effectively. The only exception to this is the first slot, which the jammer cannot jam; it is trivial to show that a strategy that includes it with probability 1 and selects the others with uniform probability strictly dominates any others for the transmitter.

Substituting (6) and (12) into (5), we can finally obtain the expected value of the indicator function $\chi_i^{(m)}$ and then the expected value of the payoffs $u_i^{(m)}$.

B. Dynamic Programming Solution

In the case of complete information, an optimal solution of the multistage game can be determined through a dynamic programming procedure. We define the system state as $S^{(m)} \triangleq \left(B_T^{(m)}, B_J^{(m)}\right)$, where $B_i^{(m)}$ is limited by the initial battery level $B_i^{(0)}$ of player $i \in \{T, J\}$. The state space is then defined as $\mathcal{S} = \{0, \dots, B_T^{(0)}\} \times \{0, \dots, B_J^{(0)}\}$. If $\Gamma > 1$, the payoff in state $S^{(m)}$ takes the payoff of the future $\Gamma - 1$ subgames into account. The game ends when the transmitter's battery level is too low to transmit at least K packets, i.e., when $B_T^{(m)} < K$. We can aggregate all states that satisfy the ending condition into a final state ε and define its payoff as:

$$U_i^{(m)} \left(\Gamma \,\middle|\, S^{(m)} = \varepsilon \right) = 0 \quad \forall\, i, \Gamma \,. \tag{13}$$

We can now compute $\mathbb{E}\left[U_i^{(m)}(\Gamma) \,\middle|\, S^{(m)}\right]$ recursively for all other states, considering that the battery charge can never increase, hence $B_i^{(m+1)} \leq B_i^{(m)} \,\forall i, m$. It is:

$$\mathbb{E}\left[U_i^{(m)}(\Gamma) \,\middle|\, S^{(m)}\right] = \mathbb{E}\left[u_i^{(m)} \,\middle|\, S^{(m)}\right] + \lambda \sum_{S \in \mathcal{S}} \mathbb{E}\left[U_i^{(m+1)}(\Gamma - 1) \,\middle|\, S\right] \mathrm{P}\left(S^{(m+1)} = S \,\middle|\, S^{(m)}\right). \tag{14}$$

The payoff in a state is thus computed as the expected payoff $\mathbb{E}[u_i^{(m)}]$ obtained in the subgame corresponding to that state plus the payoff that is expected to be obtained in the next $\Gamma - 1$ subgames, with an exponential discount factor λ (see (4)). This latter term is calculated by averaging over each possible next state $S^{(m+1)}$ weighed by the probability of transitioning to that state. For a given pair of strategies (s_T, s_J), such state transition probability is given by:

$$\mathrm{P}\left(S^{(m+1)} = (B_T, B_J) \,\middle|\, S^{(m)}\right) = \Phi_{s_T}\left(B_T^{(m)} - B_T^{(m+1)}\right) \Phi_{s_J}\left(B_J^{(m)} - B_J^{(m+1)}\right). \tag{15}$$

By substituting (15) into (14), we have a full recursive formulation for the expected long-term payoff $\mathbb{E}[U_i^{(m)}(\Gamma)]$ for any strategy pair. Once the payoff bimatrix is thus constructed, the Lemke-Howson algorithm can be used to find the mixed NE [26]. By starting from the lowest states and calculating the expected payoffs $\mathbb{E}\left[U_i^{(m)}(\gamma)\right]$, $\gamma \in \{1, \dots, \Gamma\}$, the game can be solved completely. 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. The game ends at stage $h \in \mathbb{N}$ when state ε is reached, i.e., $B_T^{(h)} < K \leq B_T^{(h-1)}$. Notice that, if the battery of J empties before T's, the game evolves in the limit condition of T playing against the channel.

C. Analytical performance evaluation

After computing the strategies, we can evaluate the expected lifetime $\mathbb{E}\left[L | S^{(m)}\right]$ of the transmitter node, defined as the number of blocks that it can transmit (either successfully or not), i.e., the number of subgames that will be played before its battery is depleted. Using (15), we define the expected lifetime for state $S^{(m)}$ recursively:

$$\mathbb{E}\left[L \,\middle|\, S^{(m)}\right] = \sum_{B_J=0}^{B_J^{(m)}} \sum_{B_T=0}^{B_T^{(m)}-K} \left(1 + \mathbb{E}\left[L \,\middle|\, S^{(m+1)} = (B_T, B_J)\right]\right) \times \mathrm{P}\left(S^{(m+1)} = (B_T, B_J) \,\middle|\, S^{(m)}\right). \tag{16}$$

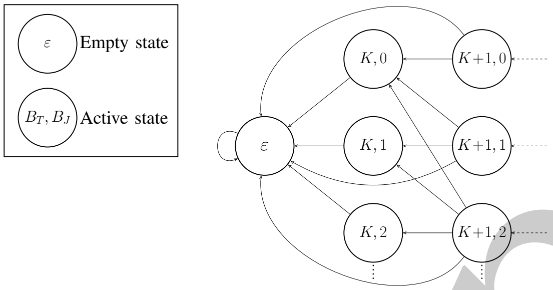

Fig. 2. State transitions for the multistage game $\mathbb{G}$.

The lifetime takes into account the subgame (m), which is summed to the expected lifetime of each possible next state $S^{(m+1)}$, weighed by its probability. Since the game ends in state ε, we can now define the base step of the recursive formulation:

$$\mathbb{E}\left[L \,\middle|\, S^{(m)} = \varepsilon\right] = 0. \tag{17}$$

We can also derive the expected success probability $P_S\left(S^{(m)}\right)$ using the same reasoning. The success probability for the current subgame is averaged with the success probability in future states, weighed by the expected lifetime and the probability of reaching those states using (16):

$$P_S\left(S^{(m)}\right) = \sum_{N_T=K}^{2K} \sum_{N_J=0}^{2K-1} \mathrm{P}\left(S^{(m+1)} = S_{N_T,N_J}^{(m+1)} \,\middle|\, S^{(m)}\right) \times \frac{\mathbb{E}\left[\chi_T | N_T, N_J\right] + \mathbb{E}\left[L \,\middle|\, \left(S_{N_T,N_J}^{(m+1)}\right)\right] P_S\left(S^{(m+1)}\right)}{1 + \mathbb{E}\left[L \,\middle|\, S_{N_T,N_J}^{(m+1)}\right]}, \tag{18}$$

where $S_{N_T,N_J}^{(m+1)} = \left(B_T^{(m)} - N_T, B_J^{(m)} - N_J\right)$. The base step is the same as for the lifetime:

$$P_S(\varepsilon) = 0. \tag{19}$$

D. Computational complexity

The computation of the optimal strategies requires the dynamic programming approach described in Sec. IV-B, starting from the states with the lowest battery level and exploiting the results to calculate the strategy for the subsequent ones. The solution of the game in a given state $S = (B_T, B_J)$ then requires the knowledge of the expected payoff for the current subgame and for future ones, which are then given as input to the Lemke-Howson algorithm to find the NE. If we denote the complexity of finding the expected payoff of a subgame as M_{sub}, and the complexity of the Lemke-Howson algorithm as M_{LH}, the overall complexity of the solution in state S is $O(B_T B_J M_{\text{sub}} M_{\text{LH}})$.

While the Lemke-Howson algorithm is efficient in practice, its worst-case complexity has been shown to be $M_{\text{LH}} \sim O(2^{3K})$ [27], as it depends directly on the length of the longest pivoting path in the strategy space. [1]

[1] We remind the reader that K is the number of information packets in a burst.

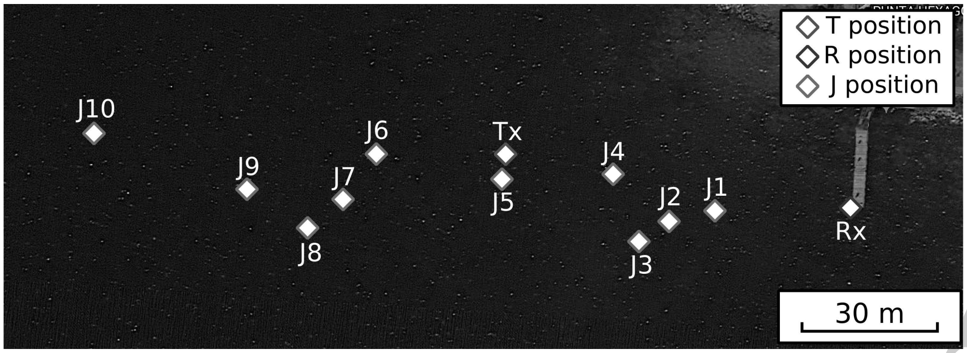

Fig. 3. Node deployment in the Garda lake. The figure reports all the positions (red diamond) in which the jammer node was placed during the experiment. Transmitter position (green diamond) and receiver position (blue diamond) are reported as well.

We now compute M_{sub}, the last term of the overall complexity formula. In order to find the expected payoff in a subgame, the nodes need to solve (5) for each pair of possible moves (N_T, N_J). The solution of (5) requires to compute $\mathbb{E}\left[\chi_T \,|\, N_{\text{C}}\right]$ using (6) N_T times, and (6) requires $O(K^2)$ operations in the worst case. Therefore, the complexity of (5) is $O(K^3)$, and computing the expected payoff for all the $(K+1)(2K-1)$ possible pairs of moves is $O(K^5)$.

The overall time to find the solution of the game in state S is then $O(B_T B_J K^5 2^{3K})$, which is clearly intractable for a computationally limited underwater node. However, the optimal strategies can be computed offline and loaded in the agent as a simple lookup table, reducing the complexity to a simple memory read.

V. Scenario settings

We evaluate the performance of the optimal strategies by studying the energy consumption and the PDR of T in two scenarios, a model-based one and an experimental one. We set up the two scenarios using the same transmitter and scenario parameters, trying to make them as comparable as possible: for this reason, the relative positions of the three nodes (transmitter, jammer, and receiver) are the same in both scenarios. We considered a carrier frequency equal to 26 kHz and a bandwidth of 16 kHz. The transmit power was the same for both transmitter and jammer, namely $P_{\text{tx},i} = 180$ dB re 1μPa, $i \in \{T, J\}$. However, the two scenarios used different packet error probabilities, derived from a theoretical model and a lake experiment, respectively.

A. Model-based scenario

In this scenario, jammer and transmitter are trained and evaluated using the uncoded CSS modulation with DQPSK; the packet error probability is given in (10). As mentioned above, the considered propagation model is described in [4], where only the Line of Sight (LoS) component is considered. The wind speed, shipping factor and geometrical spreading factor are set to 3 m/s, 1, and 1.75, respectively. We remark that the settings are different from our previous work: we used a different modulation, which leads to a different packet error probability formula. However, the game theoretic model works independently of these settings. The channel settings (with few reflections and a strong line of sight component) are optimistic, as real scenarios in shallow water often have strong reflections and environmental noise. The parameters of the model are summarized in Table II.

B. Experimental settings

The lake experiment took place in the Garda lake on Thursday 17th October 2019, just off the Bardolino town coastline. The weather was sunny, and the maximum wind speed we experienced during the experiment was 8 m/s. Most of the waves were caused by the motion of the surrounding ships: shipping activity was very heavy, as our network was deployed at only 500 m from the Bardolino ferry station, and the receiver node was placed close to a boat rental service. All the measurements were performed from 10 AM to 4 PM. The experimental setup was composed of 3 nodes equipped with EvoLogics S2C R 18/34 WiSE modems [28]: the receiver was deployed from a floating pier (N 45.549108, E 10.715181), the transmitter from a working boat anchored 80 meters west of the receiver (N 45.549165, E 10.714172), and the jammer from a working boat placed at different locations, between 20 and 180 meters west of the receiver. The map of the node positions is shown in Fig. 3, Fig. 4 is a photo of the scenario from the receiver's perspective, and Fig. 5 shows the equipment used for each node in the experiment. The water depth was 4 m at the receiver, 10 m at the transmitter, and varied from 4 to 15 meters at the jammer, depending on its location. All nodes were deployed at a depth of 2 m, and both J and T were sending signals with an acoustic power of 180 dB re 1μPa. Both modems deployed from the Tx and the Rx stations used the standard EvoLogics firmware, while node J was transmitting continuous signals at 1 kbps by using the low-level EvoLogics firmware, described in [29]. Every 2 seconds, T sent one instant message packet with a payload length of 64 Bytes at the same bitrate of J. Together with the EvoLogics header and coding used by the standard EvoLogics, the packet duration was approximately 0.86 s (value provided by the modem at the moment of the reception). In order to prevent T's transmissions from being blocked by the reception of J's signals (as the acoustic modems are, for their nature, half-duplex devices), T was set in deaf mode, i.e., its receiver unit was disabled. Both T and J used a Quadrature Phase Shift Keying (QPSK) modulation, with each symbol spread to

Fig. 4. Picture of the experiment taken from the receiver node station when the jammer was in position J5 (Figure 3).

Fig. 5. Picture of the apparatus used in the experiment. Each node was equipped with batteries, a laptop and an acoustic modem.

TABLE II
PARAMETERS SETTING.

Parameter	Value
Modem carrier freq	26 kHz
Modem bandwidth	16 kHz
Modem bitrate	1 kbps
Payload length	64 Bytes
T and J P_{tx}	180 dB re 1μPa
p_{e_C} (lake exp)	0.04
p_{e_C} (models)	0
Spreading factor k	1.75
Shipping factor s	1
Wind speed w	3 m/s

the whole bandwidth (using the so-called sweep-spread carrier (S2C) technology).

VI. NUMERICAL EVALUATION

In this section we report and assess the results for both the model-based and the lake experiment scenarios described in Section V.

A. Model-based scenario results

Based on the position of the jammer, we can distinguish three regions in the underwater area, as shown in Fig. 6. When the jammer is close to the receiver, any jammed packet is almost surely lost, as the received jamming signal is powerful enough to cause errors in the transmission. In our system scenario, this situation happens when the receiver-jammer distance is less than 40 m. Conversely, when the jammer is far from the receiver, its attack is completely ineffective, as the legitimate signal is much stronger; in our case, this happens when J is farther than 80 m from R. Between these two extremes, an appropriate strategy might significantly improve the performance: it is interesting to investigate how the game evolves in the critical region (where $d_{\mathrm{JR}} \in [40, 80]$ m in our scenario), and which distances yield a successful game for T.

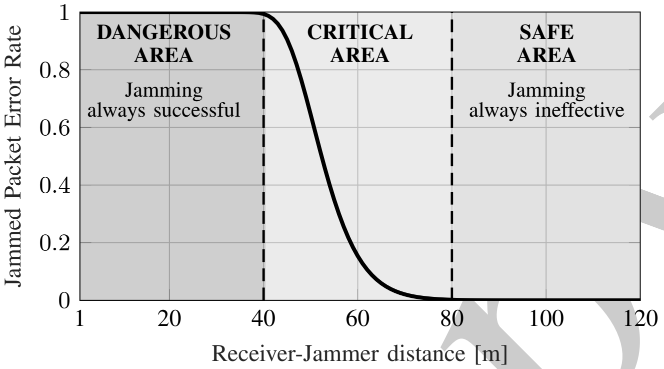

Fig. 6. Blocked channel packet error rate p_{e_B} for a jammed slot as a function of the distance d_{JR} between J and R when the distance between T and R is $d_{\mathrm{TR}} = 78$ m, using the uncoded model.

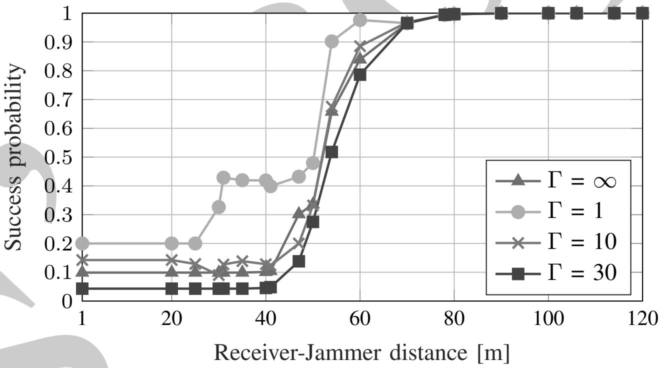

Fig. 7. Success probability in a single subgame as a function of d_{JR} using the uncoded model, for different values of Γ when $\alpha = 0.4$.

Although this performance figure refers to a specific combination of transmission power and modulation, a different configuration would still lead to the definition of the three regions, but at different distances between the transmitter and the jammer [1].

This partition is also clear from Fig. 7, which shows the transmission success probability of a subgame as a function of the distance between J and R. The success probability is close to 1 when the jammer is far away, and quickly drops when it gets closer than 80 m. It is interesting to note that the success probability when the jamming node is close decreases for longer time horizons; in this case, T tries to save energy while still transmitting, and a shorter window leads to a more aggressive policy. However, agents with a longer time horizon can avoid suboptimal choices. The jammer is particularly affected by this short-sightedness, as its reward function does not explicitly have a penalty for energy expenditure, and it will waste energy if its horizon is too short, quickly exhausting its own battery. This causes a temporary drop in the success probability, which is quickly reversed when the jammer depletes its battery and tries to fight a lost battle against the transmitter. In fact, a short time horizon

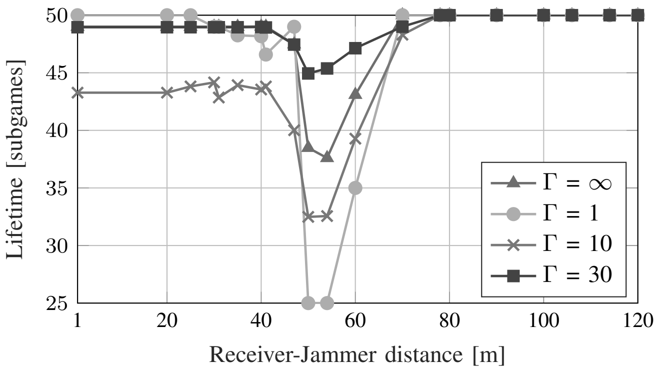

Fig. 8. Transmitter's lifetime as a function of d_{JR} using the uncoded model, for different values of the time horizon Γ when $\alpha = 0.4$.

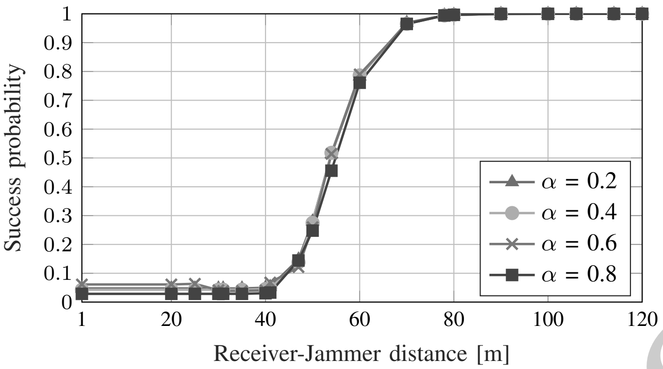

Fig. 9. Success probability in a single subgame as a function of d_{JR} using the uncoded model, for different values of α when $\Gamma = 30$.

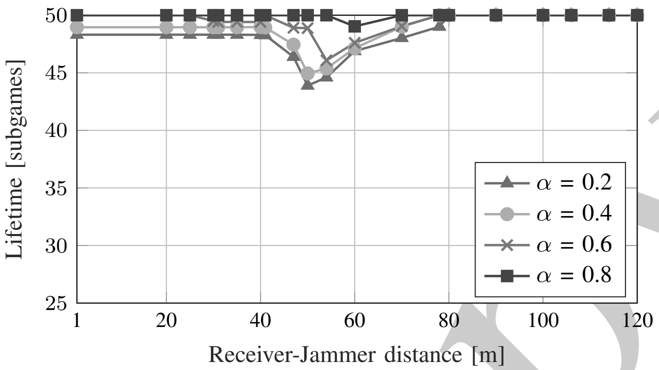

Fig. 10. Transmitter's lifetime as a function of d_{JR} using the uncoded model, for different values of α when $\Gamma = 30$.

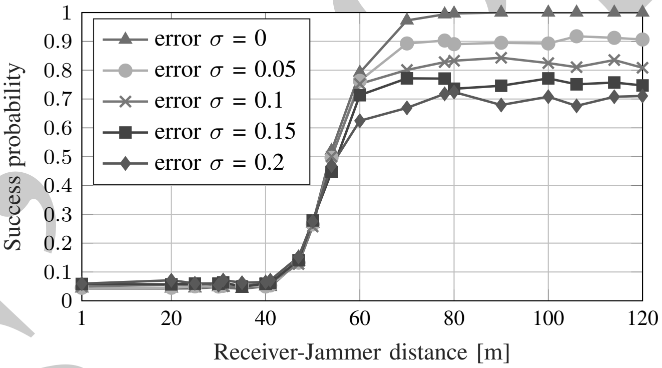

Fig. 11. Success probabilities for different values of the error standard deviation σ as a function of d_{JR} using the uncoded model, for $\alpha = 0.4$ and $\Gamma = 30$.

corresponds to both a higher success probability and a higher lifetime for the transmitter, as shown in Fig. 8. Since the initial jammer battery $B_J^{(1)}$ is set to 200 packets, $\Gamma = 30$ is the only value that ensures that the jammer will not act in a myopic way. We remark that in this case, simply switching to a short-term strategy will not benefit the legitimate transmitter: since the long-term result is the NE, choosing any other strategy will decrease its expected payoff even further. It is interesting to note that the infinite horizon jammer also suffers from this issue, since its temporal discount $\lambda = 0.9$ is small enough to make it weigh present rewards more than heavy future losses. For the rest of this analysis, we will consider the scenario in which $\Gamma = 30$.

The aggressiveness of a long-sighted jammer seems to have little effect on the results: as Fig. 9 shows, lower values of the parameter α correspond to a slightly higher success probability, but the curves are very close. A jammer close to the receiver can reduce the transmission success probability to less than 10%, but the aggressiveness parameter only has a significant impact on the success probability in the critical region. Since $K = 4$ and $B_{T,0} = 200$, the maximum lifetime of T is 50 subgames, and is reached when T does not add any FEC. The minimum lifetime is 25 subgames, in the case in which T always sends $2K$ packets, providing the maximum possible protection to its payload. Fig. 10 confirms that there is a downside to aggressiveness: more conservative nodes with a higher α have a slightly longer lifetime in the critical region. Naturally, the lifetime is maximized when $d_{\mathrm{JR}} > 80$ m, i.e., when the jammer no longer affects the packet reception. This result holds for each value of α; in this situation, since almost all packets are received correctly, the best strategy for the transmitter is to send exactly K packets, in order to minimize the energy consumption. Naturally, the critical area definition depends on the transmission power and modulation, and its boundaries can be different in other scenarios.

We also note that the lifetime decreases when the jammer is in the critical region, where strategies have a significant impact on the outcome of the game, and transmitters have to behave more aggressively to maximize their payoff. Accordingly, the decrease is far less pronounced for higher values of α and longer time horizons.

We also perform a sensitivity analysis by running a Monte Carlo simulation of this scenario, changing the error probabilities $p_{e_{\mathrm{C}}}$ and $p_{e_{\mathrm{B}}}$ randomly at each run. We set a threshold for the blocked channel error probability, so that it is never lower than the clear channel error probability, and add two independent Gaussian components with zero mean and standard deviation σ to each component. In this case, the choices of the two players become suboptimal, since they are operating with an incorrect model of the environment. Node lifetime is not affected, since the nodes make the same choices, but the success probability is, as Fig. 11 shows. The effect is interesting, and most noticeable outside the critical region: when the jammer is very close to the receiver, the success probability slightly improves as σ grows, while the opposite

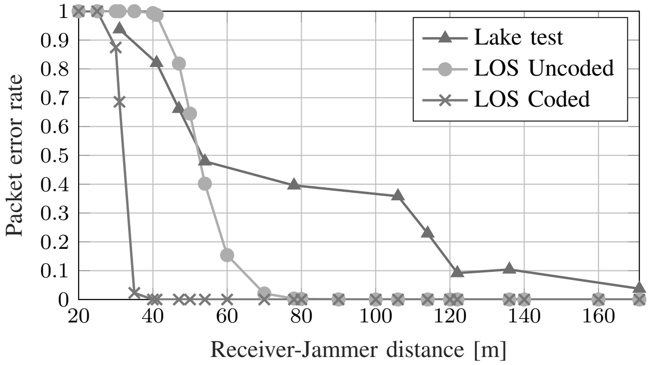

Fig. 12. Blocked channel packet error rate p_{e_B} for different channel models as a function of d_{JR}, for $\alpha = 0.4$ and $\Gamma = 30$.

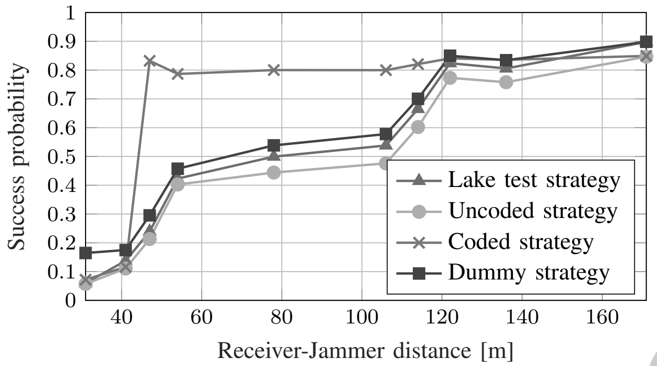

Fig. 13. Success probability for different strategies as a function of d_{JR} in the lake scenario, for $\alpha = 0.4$ and $\Gamma = 30$.

happens (with much larger effects) when the jammer is far. This might be due to the threshold effect, as the packet error probability cannot be lower than 0 or higher than 1: in this case, the errors are biased. In the critical region, the model error has a slightly negative effect on the success probability, favoring the jammer.

B. Experimental scenario results

Fig. 12 shows the packet error rate measured at different distances in the lake experiment, and compares it to those obtained with the the coded and uncoded LoS channel models. The three curves have a sigmoid-like shape, but the real results have a relatively high packet error rate even when the jammer is far from the receiver. The uncoded packet error rate curve is similar to the measured curve for $d_{JR} \leq 60$ m, while the coded packet error curve is completely different, as the jammer is already supposed to be completely ineffective at a distance $d_{JR} \simeq 40$ m. This shows that the channel model we used in the theoretical analysis was extremely optimistic, with a strong LoS component and a very low ambient noise. The real propagation environment is instead much more hostile, and as a result the packet error probability is generally higher (even though the communication system used channel coding), especially in a shallow water scenario akin to the one experienced during the lake experiment.

In this scenario, we consider the lake experiment curve as the real packet error rate, and test players that devise their strategies according to different internal models: since it would be impractical to perform sea trial scenarios before deployment, nodes may have to be trained based on a theoretical model, but the difference between the models and reality may have effects on the performance, which we will analyze in the following. We also consider a dummy jammer which always jams $K+1$ slots, allowing the transmitter to find the best response: since the dummy strategy is not necessarily a best response, it is worse for the jammer than the NE solution. This case is used as a baseline, since it is the most favorable for the transmitter.

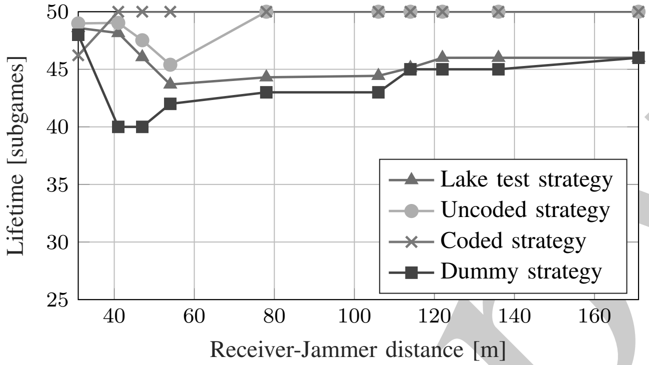

Fig. 14. Transmitter's lifetime for different strategies as a function of d_{JR} in the lake scenario, for $\alpha = 0.4$ and $\Gamma = 30$.

Fig. 13 shows how using a very optimistic model of the packet error probability leads to an unbalanced scenario: the jammer, convinced that its actions will have little or no effect, saves energy by limiting its transmissions. Most of the time the transmitter has a free channel and just has to contend with the ambient noise. The players using the uncoded model, which is much closer to the real packet error probability curve, reach a similar equilibrium. Finally, the dummy jammer strategy is actually close to optimal at long distances, while it allows much more data to get through when the jammer is close.

In general, the transmitter almost always chooses a conservative strategy, as Fig. 14 shows. Since the correct packet error probabilities are higher than those predicted by the models, and particularly the coded one, the lifetime of the node with the correct model decreases as it transmits slightly more redundancy. This is also true for the dummy jammer case, as its strategy of jamming $K+1$ slots in each subgame is quite aggressive.

VII. Conclusions and future work

In this work, we modeled and analyzed an underwater jamming attack aimed at disrupting the victim's communication, as well as depleting its battery. The legitimate transmitter can leverage packet-level coding to protect its transmissions from the jammer, at the cost of an additional energy expenditure. We model the attack using game theory and derive the optimal strategies in various scenarios, assuming that the jammer and the legitimate transmitter are two rational players with complete knowledge about the adversary, playing a zero-sum game. The simulation results highlight three regions where the jamming attack is almost always successful, depends on the strategies of the two players, or is ineffective, respectively. The critical region in which the strategies can make a difference is the one in which the uncertainty over whether or not jammed packets can be received is high.

In addition, we analyze what happens when the nodes do not have complete information about the environment, or consider short-term goals. Reducing the players' horizon gives an advantage to the transmitter, as the jammer will waste energy in the early stages of the attack. Conversely, adding a random error to the channel model advantages the jammer in the ineffective region. Finally, we consider a more realistic scenario, in which the packet error probability is determined by the results of an experiment performed in Lake Garda. We use this realistic channel to analyze what happens when the whole model of the channel is wrong: in one case, a jammer using the wrong model performs worse than a simple dummy strategy that always tries to jam the same number of packets.

Although the analytical solution is based on the simplifying assumption of complete information available at the two players, it still sheds light on the dynamics in this scenario. The results of the model comparison analysis show that relaxing the complete information assumption, i.e., considering a Bayesian incomplete information game, would significantly improve the applicability of the model, making the nodes' strategies more robust to errors in the initial assumptions [30]. Other possible avenues of future research include a wider action space, which might include other defense mechanisms such as power control or frequency hopping, and the extension of the framework to a network scenario with multiple transmitters, receivers, and jammers.

Acknowledgment

This work was partially supported by the Bundeswehr Technical Center for Ships and Naval Weapons, Maritime Technology and Research (WTD 71), Kiel, Germany. We thank Roberto Francescon and Emanuele Coccolo for their practical support and participation in the lake experiment, and Chiara Pielli, Marco Giordani, and Nicola Laurenti for their work on the preliminary version of this paper.

References

[1] A. Signori, C. Pielli, F. Chiariotti, F. Campagnaro, M. Giordani, N. Laurenti, and M. Zorzi, "Jamming the underwater: a game-theoretic analysis of energy-depleting jamming attacks," in *ACM International Conference on Underwater Networks & Systems (WuwNet)*, Oct. 2019.

[2] J. Kalwa, "The RACUN project: Robust acoustic communications in underwater networks - an overview," in *IEEE OCEANS*, Jun. 2011.

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

[4] M. Stojanovic, "On the relationship between capacity and distance in an underwater acoustic communication channel," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 11, no. 4, pp. 34–43, Oct. 2007.

[5] 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.

[6] I. F. Akyildiz, D. Pompili, and T. Melodia, "Underwater acoustic sensor networks: Research challenges," *Ad Hoc Networks*, vol. 3, pp. 257–279, May 2005.

[7] C. Lal, R. Petroccia, M. Conti, and J. Alves, "Secure underwater acoustic networks: Current and future research directions," in *IEEE UComms*, Aug. 2016.

[8] 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.

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

[10] M. Brownfield, Y. Gupta, and N. Davis, "Wireless sensor network denial of sleep attack," in *IEEE IAW*, Jun. 2005.

[11] 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.

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

[13] Q. Wang, T. Nguyen, K. Pham, and H. Kwon, "Mitigating jamming attack: A game-theoretic perspective," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 7, pp. 6063–6074, Feb. 2018.

[14] 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.

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

[16] 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.

[17] 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*, May 2019.

[18] J. Heidemann, W. Ye, J. Wills, A. Syed, and Y. Li, "Research challenges and applications for underwater sensor networking," in *IEEE Wireless Communications and Networking Conference (WCNC)*, vol. 1, Apr. 2006.

[19] Y. Huang, P. Xiao, S. Zhou, and Z. Shi, "A half-duplex self-protection jamming approach for improving secrecy of block transmissions in underwater acoustic channels," *IEEE Sensors Journal*, vol. 16, no. 11, pp. 4100–4109, Jun. 2016.

[20] V. Vadori, M. Scalabrin, A. V. Guglielmi, and L. Badia, "Jamming in underwater sensor networks as a bayesian zero-sum game with position uncertainty," in *IEEE Global Communications Conference (GLOBECOM)*, Dec. 2015.

[21] P. Casari, M. Rossi, and M. Zorzi, "Towards optimal broadcasting policies for HARQ based on fountain codes in underwater networks," in *IEEE/IFIP Conference on Wireless on Demand Network Systems and Services (WONS)*, Jan. 2008, pp. 11–19.

[22] D. Abreu, "On the theory of infinitely repeated games with discounting," *Econometrica: Journal of the Econometric Society*, pp. 383–396, Mar. 1988.

[23] J. Nash, "Non-cooperative games," *Annals of Mathematics*, vol. 54, no. 2, pp. 286–295, Sep. 1951.

[24] Y.-p. Lee, S. Yoo, S. Y. Kim, and S. Yoon, "Anti-jamming performance analysis of CSS-based communication systems," in *ITC-CSCC: International Technical Conference on Circuits Systems, Computers and Communications*, 2008, pp. 101–104.

[25] A. Goldsmith, *Wireless communications*. Cambridge university press, 2005.

[26] 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.

[27] R. Savani and B. Von Stengel, "Hard-to-solve bimatrix games," *Econometrica*, vol. 74, no. 2, pp. 397–429, Mar. 2006.

[28] "S2C R 18/34 WiSE Underwater Acoustic Modem," Last time accessed: Nov. 2019. [Online]. Available: https://evologics.de/acoustic-modem/18-34/wise-serie

[29] F. Campagnaro, R. Francescon, O. Kebkal, P. Casari, K. Kebkal, and M. Zorzi, "Full reconfiguration of underwater acoustic networks through low-level physical layer access," in *ACM International Conference on Underwater Networks & Systems (WuwNet)*, Nov. 2017.

[30] F. Chiariotti, A. Signori, F. Campagnaro, and M. Zorzi, "Underwater jamming attacks as incomplete information games," in *INFOCOM Workshop on Wireless Communications and Networking in Extreme Environments*. IEEE, Jul. 2020.