Underwater Jamming Attacks as Incomplete Information Games

Federico Chiariotti, Alberto Signori, Filippo Campagnaro, Michele Zorzi
Department of Information Engineering, University of Padova, via Gradenigo 6/B, 35131 Padova, Italy
Email: {chiariot, signoria, campagn1, zorzi}@dei.unipd.it

***Abstract*—Autonomous Underwater Vehicles (AUVs) have several fundamental civilian and military applications, and Denial of Service (DoS) attacks against their communications are a serious threat. In this work, we analyze such an attack using game theory in an asymmetric scenario, in which the node under attack does not know the position of the jammer that blocks its signals. The jammer has a dual objective, namely, disrupting communications and forcing the legitimate transmitter to spend more energy protecting its own transmissions. Our model shows that, if both nodes act rationally, the transmitter is able to quickly reduce its disadvantage, estimating the location of the jammer and responding optimally to the attack.**

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

I. Introduction

Over the past few years, Autonomous Underwater Vehicles (AUVs) have enabled several new environmental, military, and industrial applications: AUVs and static underwater sensors can greatly reduce the risk for human health and increase the efficiency of patrol, maintenance, and monitoring operations in a variety of scenarios, from tsunami alert systems to oil pipe inspection. Wireless communications are a critical component of these kinds of systems, and their resistance to environmental factors and deliberate attacks from malicious agents is particularly important in military applications such as coastal patrol [1].

Even without active attacks, this task is not simple: electromagnetic waves are strongly attenuated when propagating through water, and radio communications are impossible except for very short-range broadband links [2]. In order to communicate over longer distances, AUVs need to use acoustic waves, which, depending on the carrier frequency, can allow either transmissions of hundreds of kbps at a maximum range of a few hundred meters [3], [4], or very low rate communications at ranges up to tens of kilometers [5], [6]. Nevertheless, the nature of acoustic waves and the hostile environment pose several challenges for acoustic communications. Indeed, acoustic waves propagate at a speed of 1500 m/s (on average) causing high transmission delay. In addition, reflections with the bottom and the surface occur, especially in shallow water, where multi-path effects result in high delay spread that limits the communication efficiency [7]. Environmental noise is another limiting factor of acoustic communications. Different noise sources affect the communications, e.g., shipping activities, whose effects decreases for higher transmission frequency [8], marine fauna [9], or wind [5].

This critical combination of harsh environment and critical applications can make Denial-of-Service (DoS) attacks extremely dangerous, as disabling the victim node's communication can effectively interrupt the monitoring operation. Physical layer jamming is one of the most common types of DoS attacks [10]: the attacker reacts to sensed packets by sending a high-power jamming signal, interfering with the transmission and preventing the correct reception of the packets. Unsuspecting victims are easy to jam due to their predictable duty cycles [11], but nodes can become aware of jamming attacks and employ active countermeasures. There are several defense mechanisms, from power control [12] to channel-hopping [13] and packet-level coding [14]. In case of active defense, game theory is often used to model the interaction between the jammer and its victim.

Active defense can mitigate the damage of a jamming attack, but comes at a cost: most strategies require a higher energy consumption, which can be problematic in battery-powered nodes. The jammer itself may exploit this by purposefully depleting the victim's battery, thereby reducing its lifetime. In this case, the jamming attack can be modeled as a zero-sum repeated game with a finite number of episodes [15]. The optimal strategies can be found with dynamic programming or approximations such as reinforcement learning.

In our previous work [14], we used the repeated zero-sum game formulation to model such a dual-objective attack: the jammer tries to disrupt the victim's communications and force it to spend more energy to protect its transmissions by sending redundant packets. The transmitter's objective is to transmit its data successfully with the minimum energy expenditure, limiting the redundancy in each packet burst. We derived the optimal strategies under the assumption that complete information was available to both players and studied the trade-off between energy consumption and transmission success probability as a function of the distances between transmitter, receiver and jammer.

However, the assumption of perfect information might not hold in a realistic scenario: a malicious node might try to conceal its position, which strongly influences the effectiveness of the jamming. The transmitter node will then need to operate in a Bayesian fashion [12], defending itself against the attack and refining its estimate of the jammer's position by deriving the *a posteriori* distribution after each subgame. In this work, we present such a scenario, deriving the optimal strategies for both nodes, and show that the transmitter can quickly estimate the correct location of the jammer, with essentially no performance loss with respect to the complete information scenario.

The rest of the paper is organized as follows. In Sec. II, we present the game theoretic model and the system scenario in the complete information case. Sec. III derives the Bayesian Nash Equilibrium (BNE) solution of the game in the imperfect information case, finding the optimal strategy for both players and the *a posteriori* belief update procedure. Finally, Sec. IV describes the numerical evaluation, and Sec. V concludes the paper.

II. Game Theoretic Model

We consider a scenario akin to the one described in [14]: a transmitter T needs to transmit packets to a receiver R, and is under attack from a jammer J. The distances between T and R and between J and R are denoted as d_{TR} and d_{JR}, respectively. T can defend from the attack by complementing the K information packets with some redundant ones with a packet-level coding scheme. If any subset of K packets is correctly received by R, the data burst can be completely recovered [16].

We model the scenario as a zero-sum game between T and J: the two players have opposite goals. In this case, we use an asymmetric incomplete information scenario: while J has complete knowledge of the scenario, T does not know d_{JR} and can only estimate it, starting from an initial belief distribution. Both nodes are battery-powered, and their 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 $E_{\text{tx},i}$, $i \in \{T, J\}$, used to transmit/jam each legitimate packet.

The game is composed of a series of subgames, which correspond to data bursts: in each subgame m, T sends a burst of packets to R, reporting its monitoring information. The data is divided into K packets, and we assume that T can use *(i)* a Cyclic Redundancy Check (CRC) field to allow R to verify packet reception, and *(ii)* a packet-level code to increase the communication success probability. The moves that T can choose are then the possible numbers $N_T^{(m)}$ of packets to send; a maximum of $2K$ transmission opportunities is configured in each subgame, thus $K \leq N_T^{(m)} \leq 2K$. On the other hand, J must decide which slots to jam. Larger values of $N_T^{(m)}$ increase the success probability, but deplete T's energy faster; the same is true for the jammer. After each packet burst, both nodes receive a feedback packet from R, which we assume to be loss-free [14].

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 in this paper.

TABLE I
NOTATION AND MEANING OF SYSTEM PARAMETERS

Parameter	Meaning
K	Minimum number of packets to be delivered for success
Γ	Time horizon of multistage game G
λ	Exponential discounting factor
α_i	Energy/transmission success weighting factor
d_{iR}	Distance between player i and the receiver node
$u_i^{(m)}$	Payoff function in subgame m
$U_i^{(m)}$	Payoff function in multistage game G in subgame m
$\chi^{(m)}$	Indicator function of the success of subgame m
$B_i^{(m)}$	Battery level in subgame m
$\mathbf{B}^{(m)}$	State in subgame m, combining $B_T^{(m)}$ and $B_J^{(m)}$
$\mathbf{f}^{(m)}$	Feedback in subgame m
$N_T^{(m)}$	Number of packets that T sends in subgame m
$N_J^{(m)}$	Number of slots that J tries to jam in subgame m
$N_C^{(m)}$	Packets sent over clear channel in subgame m
$N_B^{(m)}$	Packets sent over jammed channel in subgame m
$r_C^{(m)}$	Packets delivered over clear channel in subgame m
$r_B^{(m)}$	Packets delivered over jammed channel in subgame m
$r^{(m)}$	Total packets delivered in subgame m
p_{e_C}	Packet error probability over clear channel
$p_{e_B}(d_{JR})$	Packet error probability over jammed channel
$p(\hat{d}_{JR})$	Belief distribution of J's distance from R
Φ_i^*	Optimal mixed strategy for player i

A. The Packet Transmission Subgame

As described above, each subgame m models a data burst of K information packets from T to R; T decides how many packets $N_T^{(m)} \in \mathcal{N}_T^{(m)} \triangleq \{K, \dots, \min(2K, B_T^{(m)})\}$ to send to R, and J simultaneously chooses the number of slots $N_J^{(m)} \in \mathcal{N}_J^{(m)} \triangleq \{0, \dots, \min(2K-1, B_J^{(m)})\}$ to jam. The decision is made in advance for both nodes, and both the transmission and the jamming are randomized over the $2K$ packet transmission times in order to avoid predictable and exploitable patterns. Due to the long propagation delays, J cannot jam the first packet of a burst: since the attack is reactive, J can only start jamming when it senses a packet being transmitted.

The payoffs of the players are given by a linear combination of the expended energy and the outcome of the transmission. The parameter $\alpha \in [0, 1)$ can be tuned to alter the goals of the players, making them more or less aggressive. We express the players' payoffs for a single subgame m as:

$$u_T^{(m)} = -\alpha \, \frac{N_T^{(m)}}{(2K+1)} + (1-\alpha)\chi^{(m)} \tag{1}$$

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

The indicator term $\chi^{(m)}$ is equal to one if the subgame m ends with T successfully delivering at least K packets to R, and zero otherwise. 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 an implicit role in the full game: the larger $N_J^{(m)}$, the higher the energy consumed by node J, and the faster its battery depletion.

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:

$$U_i^{(m)}(\Gamma) = \sum_{\gamma=m}^{m+\Gamma-1} \lambda^{\gamma-m} u_i^{(\gamma)}, \quad i \in \{T, J\}, \tag{3}$$

where $\lambda \in [0,1]$ is a future exponential discounting factor [17], $u_i^{(m)}$, $i \in \{T, J\}$ 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.

III. The Bayesian jamming game

We now relax the complete information assumption and consider an incomplete information game, in which the position of the jammer is unknown to the transmitter.

In each subgame, we derive the BNE [18] mixed strategies $(\Phi_T^\star, \Phi_J^\star)$ of the two rational players using the Lemke-Howson algorithm [19]. The outcome of the subgame depends on such strategies and on the stochastic channel conditions. When playing the subgame, T obtains some information, denoted as $\mathbf{f}$, about the outcome of the game. This feedback is used by T to update its estimate of J's position. This is repeated until the battery of the transmitter is depleted.

A. Computing the expected payoff

We now consider the expected payoff of the players in subgame m for a given set of strategies. We define as strategy N_i the action chosen by player $i \in \{T, J\}$, i.e., the amount of energy required to transmit the legitimate packets or jam the slots, respectively. According to the game defined in Sec. II, the strategy space is thus $\mathcal{N}_i^{(m)}$, $i \in \{T, J\}$ in each subgame. In the remainder of this section, we will omit superscript (m) for the sake of a lighter notation. The expected payoffs $\mathbb{E}\left[u_i | N_T, N_J\right]$, $i \in \{T, J\}$ can be calculated from the quantity $\mathbb{E}\left[\chi | N_T, N_J\right]$, $i \in \{T, J\}$, which represents the expected outcome of the subgame (as introduced in Sec. II-A, χ is an indicator term for transmission success). We now add another dependency on d_{JR} and introduce quantities $N_C \leq N_T$ and $N_B \leq N_T$ to indicate the number of packets that node T sends over a clear and blocked (i.e., jammed) channel, respectively. Obviously, $N_T = N_C + N_B$, so we can easily obtain the value of N_C once we know N_B. Using the law of total probability, for node T we have:

$$\mathbb{E}\left[\chi | N_T, N_J\right] = \sum_{N_B=0}^{N_T-1} \mathbb{E}\left[\chi | N_B\right] \mathrm{P}\left(N_B | N_T, N_J\right). \tag{4}$$

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 the distance between the jammer and the receiver. We can then distinguish between two cases: for the N_C packet transmissions over a clear channel, the packet error probability is equal to p_{e_C}, which is a function of the Signal to Noise Ratio (SNR). For the N_B transmissions that are disturbed by the jammer, the packet error probability is $p_{e_B}(d_{JR})$, which is a function of the Signal to Interference and Noise Ratio (SINR) and depends on the jammer's position. The specific values of the two probabilities can be derived for each modulation, and [14] gives the complete results for Binary Phase Shift Keying (BPSK). Using these probabilities, $\mathbb{E}\left[\chi | N_B, d_{JR}\right]$ can be expressed as:

$$\mathbb{E}\left[\chi | N_B, d_{JR}\right] = \sum_{r=K}^{N_T} \sum_{r_C=\max(0, r-N_B)}^{\min(r, N_C)} \binom{N_C}{r_C} (1-p_{e_C})^{r_C} p_{e_C}^{N_C-r_C} \binom{N_B}{r-r_C} p_{e_B}(d_{JR})^{N_B-(r-r_C)} \left(1-p_{e_B}(d_{JR})\right)^{r-r_C}. \tag{5}$$

The external summation iterates on all possible values of the number of delivered packets $r \leq N_T$ resulting in a success. We then split r between packets that are delivered over a clear channel, i.e., $r_C \leq r$, and those which are delivered over a jammed channel, i.e., $r_B = r - r_C \leq N_B$.

Since T does not have complete knowledge of d_{JR}, but can only infer it from the feedback it receives, we can define its belief distribution $p(\hat{d}_{JR})$, $\hat{d}_{JR} \in \mathcal{D}$ where $\mathcal{D}$ is the discrete set of possible distances. The distribution represents the estimate of the distance: before the first subgame, the prior belief distribution is uniform, but is updated with the feedback obtained from the receiver after each subgame, reducing the uncertainty. Using the law of total probability, we can remove the condition on d_{JR} to obtain the first part of the sum in (4):

$$\mathbb{E}\left[\chi | N_B\right] = \sum_{\hat{d}_{JR} \in \mathcal{D}} \mathbb{E}\left[\chi | N_B, d_{JR}\right] p(\hat{d}_{JR}). \tag{6}$$

Finally, the second part of the sum in (4) can be expressed as:

$$p\left(N_B | N_T, N_J\right) = \frac{\binom{N_T-1}{N_B}\binom{(2K-1)-(N_T-1)}{N_J-N_B}}{\binom{2K-1}{N_J}}, \tag{7}$$

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 above. Naturally, (7) is only valid for $N_B < N_T$. We assume that both the transmitter and the jammer choose the slots to transmit (or to 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.

B. Finding the BNE

We now derive the BNE solution of the game, i.e., the pair of strategies used by rational players. We consider mixed strategies, as each strategy $\mathbf{\Phi}_i^{(m)}$ is a probability distribution over $\mathcal{N}_i^{(m)}$. The BNE strategies are *mutual best responses*, i.e., each strategy maximizes the player's payoff if the other player uses the other, given the knowledge about its state:

$$\mathbf{\Phi}_T^*(\mathbf{\Phi}_J,\mathbf{B},p(\hat{d}_{JR})) = \underset{\mathbf{\Phi}_T}{\operatorname{argmax}} \sum_{\hat{d}_{JR}\in\mathcal{D}} \sum_{N_T\in\mathcal{N}_T} \sum_{N_J\in\mathcal{N}_J} \Phi_T(N_T)\Phi_J(N_J|\hat{d}_{JR})p(\hat{d}_{JR})\mathbb{E}\left[U_T|N_T,N_J,\mathbf{B},\hat{d}_{JR}\right] \tag{8}$$

$$\mathbf{\Phi}_J^*(\mathbf{\Phi}_T,\mathbf{B}) = \underset{\mathbf{\Phi}_J}{\operatorname{argmax}} \sum_{N_T\in\mathcal{N}_T} \sum_{N_J\in\mathcal{N}_J} \Phi_T(N_T)\Phi_J(N_J) \mathbb{E}\left[U_J|N_T,N_J,\mathbf{B},d_{JR}\right]. \tag{9}$$

where $\mathbf{B} = [B_T, B_J]$. The BNE is then given by the pair of strategies that satisfies the following condition:

$$\begin{cases} \mathbf{\Phi}_T^* = \mathbf{\Phi}_T^*(\mathbf{\Phi}_J^*,\mathbf{B},p(\hat{d}_{JR})) \\ \mathbf{\Phi}_J^* = \mathbf{\Phi}_J^*(\mathbf{\Phi}_T^*,\mathbf{B}) \end{cases} \tag{10}$$

The expected long-term payoffs can be computed by using the dynamic programming procedure from [14]. By using (6), we can obtain the expected value of the payoff U_T for a given belief $p(\hat{d}_{JR})$:

$$\mathbb{E}\left[U_T(\Gamma)|N_T,N_J\right] = \sum_{\hat{d}_{JR}\in\mathcal{D}} \mathbb{E}\left[U_T|\hat{d}_{JR}\right]p(\hat{d}_{JR}). \tag{11}$$

Naturally, since J has complete knowledge of its position, its expected payoff can be computed using the real value of d_{JR}:

$$\mathbb{E}\left[U_J(\Gamma)|N_T,N_J\right] = \mathbb{E}\left[U_J|d_{JR}\right]. \tag{12}$$

Using the two matrices derived from (11) and (12), we have the bimatrix form of the game and can use the well-known Lemke-Howson algorithm [19] to find the BNE [18].

In (11) and (12), we do not consider the additional knowledge that T will gain in future steps, and therefore make players more myopic and limit the analysis to a one-step approximation. In general, this puts the jammer at a slight disadvantage, since a more foresighted player might try to make intentionally suboptimal moves to confuse the transmitter. However, this simplification was necessary to obtain a closed-form solution, and we will consider in future work the development of more sophisticated methods based on machine learning that can consider the more complex case.

C. Updating beliefs

We consider that the feedback $\mathbf{f} = (r_B, r_C, N_J)$ is available to the transmitter node, as it can be sent as part of the acknowledgment packet by the receiver. The receiver specifies the number of packets delivered correctly over a clear and jammed channel, denoted as r_C and r_B, respectively. The transmitter also knows its own move N_T. If we assume that the reception of each packet is independent of the others, we obtain:

$$p(r_B|d_{JR},N_B) = p_{e_B}(d_{JR})^{N_B-r_B}\left(1-p_{e_B}(d_{JR})\right)^{r_B} \tag{13}$$

$$p(r_C|N_B) = p_{e_C}^{N_T-N_B-r_C}\left(1-p_{e_C}\right)^{r_C} \tag{14}$$

$$p(r_C,r_B|d_{JR},N_B) = p(r_C|N_B)p(r_B|d_{JR},N_B). \tag{15}$$

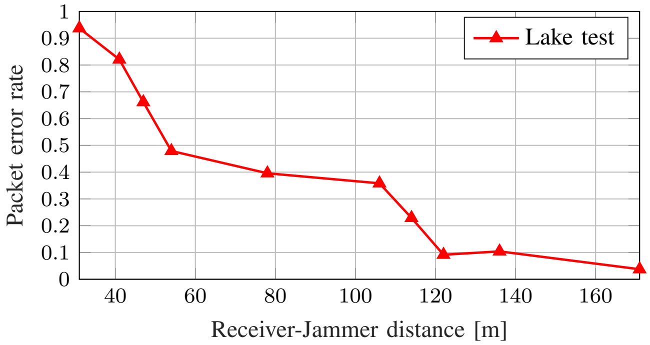

Fig. 1. Packet error rate obtained for a jammed packet as a function of the receiver-jammer distance, with a receiver-transmitter distance of 80 m.

If we combine (15) with (7), we obtain:

$$p(r_C,r_B|d_{JR},N_T,N_J) = \sum_{N_B=r_B}^{N_T-\min(r_C,1)} p(r_C,r_B|d_{JR},N_B)p(N_B|N_T,N_J). \tag{16}$$

We also know the optimal strategy $\Phi_J^*(N_J|d_{JR})$ for all values of d_{JR}, since we assume that both nodes are rational players in the game-theoretic sense. In this case, we can also calculate:

$$p(N_J|d_{JR}) = \Phi_J^*(N_J|d_{JR}). \tag{17}$$

We can now define the probability of making observation $\mathbf{f}$ given that the jammer is at distance d_{JR}:

$$p(\mathbf{f}|d_{JR}) = p(r_C,r_B|d_{JR},N_T,N_J)p(N_J|d_{JR}). \tag{18}$$

We can now apply Bayes' theorem to obtain:

$$p(d_{JR}|\mathbf{f}) = \frac{p(\mathbf{f}|d_{JR})p(d_{JR})}{p(\mathbf{f})} \tag{19}$$

$$= \frac{\Phi_J^*(N_J|d_{JR})p(r_C,r_B|d_{JR},N_T,N_J)p(d_{JR})}{\sum_{d\in\mathcal{D}}p(d)\Phi_J^*(N_J|d)p(r_C,r_B|d,N_T,N_J)}. \tag{20}$$

By computing the *a posteriori* probability for all values of d_{JR} in $\mathcal{D}$, T can update its belief for the next round.

IV. Numerical evaluation

We evaluate the performance of the optimal strategies by studying the energy consumption and the Packet Delivery Ratio (PDR) of T, comparing the results obtained in the complete information (CI) scenario with those of the incomplete information (II) scenario.

A. Simulation scenario

To compute the optimal strategies for both the CI and II scenarios, we considered a packet error probability derived from a measurement campaign we performed in the Garda lake on October 17th, 2019. In this lake experiment, we moored the receiver to a floating pier and the transmitter was deployed from an anchored boat, at a distance of 80 m from the receiver. We analyzed the packet error rate of a jammed packet for different distances between jammer and receiver d_{JR}, ranging

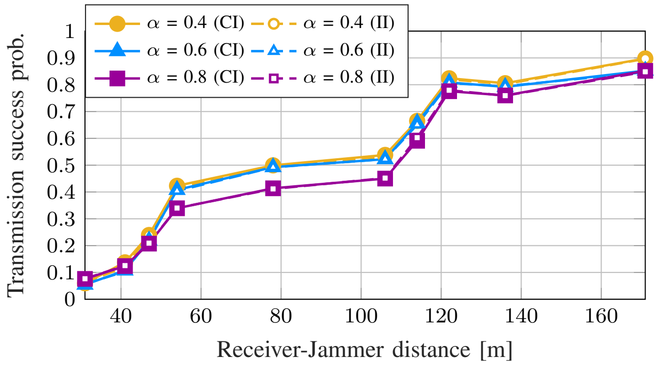

Fig. 2. Subgame success probability as a function of d_{JR}, for different values of α when $\Gamma = 30$.

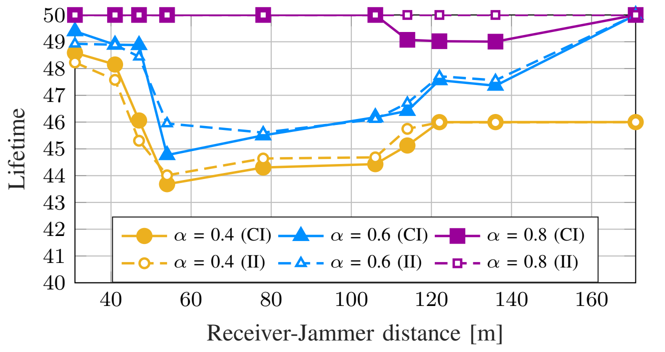

Fig. 3. Transmitter's lifetime as a function of d_{JR}, for different values of α when $\Gamma = 30$.

from 31 to 171 m. The experimental results of the packet error rate are reported in Figure 1. We also measured the packet error rate for a clear channel, i.e., without a jammer, equal to $p_{e_C} = 0.04$.

In the measurement campaign we employed 3 EvoLogics S2C R 18/34 WiSE modems [20], which use the S2C (sweep-spread carrier) modulation. Both T and J's transmission powers were 180 dB re 1μPa. While the transmitter periodically sent packets with a payload $L = 64$ B at a bitrate of 1 kbps, the jammer continuously transmitted a signal to disturb the communication. The packet error probability is used to find the optimal strategies for both T and J. Since the feedback affects future beliefs in the II scenario, we ran a Monte Carlo simulation with 1000 trials to compute the performance of T and J. In the simulated scenario we set the number of information packets in each subgame to $K = 4$ and the initial battery charge to $B_i^{(0)} = 200$, $i \in \{T, J\}$.

B. Simulation Results

As we discussed in our previous work [14], the packet error probability when the jammer is active has a strong effect on the outcome of the game. The aggressiveness of the players, tuned by the parameter α, also comes into play, as higher values of α (which correspond to more conservative players, i.e., players that try to save as much energy as possible, despite the low packet reception probability) translate into a longer lifetime and a lower success probability. Fig. 2 shows the average subgame success probability as a function of the distance d_{JR}, for both the CI and II cases, and confirms this result in the lake experiment scenario. It is easy to notice that the curves for the II scenario closely follow those for CI, confirming the result from [12]: since the receiver's feedback allows to quickly identify the real position of the jammer, the transmitter can start with no information about the jammer and still obtain almost the same results.

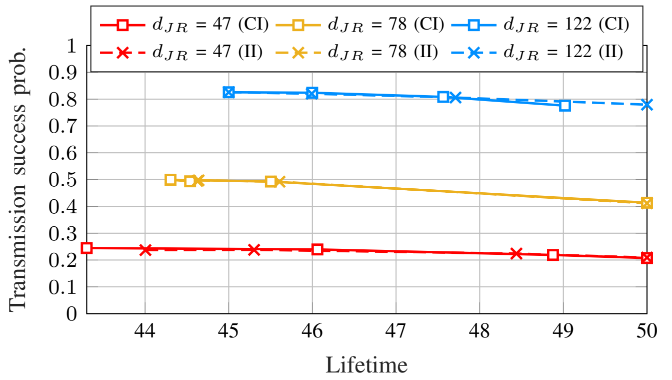

Fig. 4. Success probability in a single subgame vs. lifetime, when $\Gamma = 30$, for different d_{JR} values, and varying α: each point of the same curve corresponds to a different value of α, ranging from 0.2 to 0.8. Lower values of α result in a lower lifetime.

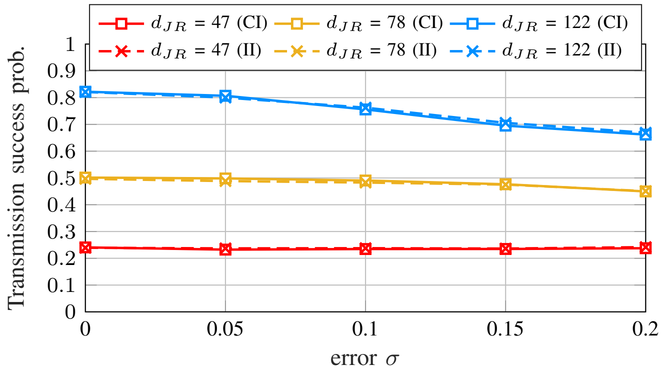

Fig. 5. Success probability in a single subgame as a function of the error standard deviation σ, for different d_{JR} values, when $\alpha = 0.4$ and $\Gamma = 30$.

Fig. 3 shows that the same holds for the battery life of the transmitter: the transmitter is always very conservative, with a lifetime between 43 and 50 subgames, as the maximum possible lifetime with the initial battery settings is 50 subgames, while a full duplication of each data burst would deplete the transmitter's battery in 25 subgames. There is a slight difference between the curves for the CI and II scenarios, where for some distances the CI scenario is slightly better. However, the difference in the average lifetime (measured in subgames) is smaller than 1 at all possible distances. We also note that the lifetime is lower when the packet error probability for jammed packets is close to 0.5: in this case, some redundancy can highly improve the transmitter's chances to correctly send its data burst, as adding one packet maximally increases $\mathbb{E}[\chi]$ as given by (6). Active defense is then more effective.

Fig. 4 shows a summary of the trade-off between lifetime and success probability at different distances: in all cases, a slight gain in the success probability comes at the cost of a comparable lifetime reduction. The II transmitter is very similar to the CI one, and even outperforms it in some cases: the trend confirms that the performance is not significantly affected by the asymmetric knowledge.

We also performed a sensitivity analysis on the packet error probabilities: we ran Monte Carlo simulations with a Gaussian noise on both p_{e_B} and p_{e_C} (with the limiting conditions that no error probability can be below 0 or above 1, and $p'_{e_C} \leq p'_{e_B}$ in any case):

$$p'_{e_C} = \max\left(0, \min\left(1, p_{e_C} + v\right)\right) \tag{21}$$

$$p'_{e_B} = \max\left(p'_{e_C}, \min\left(1, p_{e_B} + w\right)\right), \tag{22}$$

where v and w are normally distributed independent random variables with zero mean and standard deviation σ. As Fig. 5 shows, a larger noise on the packet error probability reduces the overall success probability, with a larger effect if the distance between the jammer and the receiver is increased, but the performance of the II system is still indistinguishable from that with CI. The lifetime is not pictured, as it is almost unaffected by the noise on the packet error probability, and the differences with respect to Fig. 3 are negligible.

V. Conclusions

We studied an underwater jamming attack that targets both the disruption of the victim's communication and the depletion of its battery. The legitimate transmitter leverages channel coding to counteract the jamming by adding redundancy. We model the attack by means of game theory assuming that the jammer and the legitimate transmitter are two rational players in a zero-sum game, and that while the jammer has complete knowledge about the transmitter, the latter does not know the position of its adversary. We derive the optimal strategies for both players in this asymmetric knowledge game, based on a Bayesian belief updating procedure.

We studied the impact of the jamming attack when the transmitter is put in such an unfavorable situation, and found that feedback from the receiver can be sufficient for it to have the same performance as when it has complete information about the jammer. The results show that the distance of the jammer from the receiver is the main variable affecting the performance of the transmitter, but knowing it in advance is not necessary, as the jammer's actions will rapidly unmask it.

Possible avenues of future research include a more challenging situation in which the feedback that the receiver can send to the legitimate transmitter is much more limited, in order to verify whether the transmitter can still defend itself from the attack. In that case, even the jammer's battery state and consumption might be unknown to the transmitter. Another possibility is to use reinforcement learning to allow players to use more foresighted strategies that actually include purposefully suboptimal choices: the jammer might hide its position by playing contradictory moves, and the transmitter might try to deceive the jammer into thinking it is safe and undiscovered. Reinforcement learning would also allow us to introduce a dynamic component to the game, allowing the jammer to move during the game.

Acknowledgment

This work was partially supported by the Bundeswehr Technical Center for Ships and Naval Weapons, Maritime Technology and Research (WTD 71), Kiel, Germany.

References

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

[2] 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.

[3] E. Demirors, G. Sklivanitis, G. E. Santagati, T. Melodia, and S. N. Batalama, "A High-Rate Software-Defined Underwater Acoustic Modem With Real-Time Adaptation Capabilities," *IEEE Access*, vol. 6, no. 6, pp. 18 602–18 615, Jun. 2018.

[4] M. Rahmati, A. Gurney, and D. Pompili, "Adaptive underwater video transmission via software-defined MIMO acoustic modems," in *IEEE/MTS OCEANS*, Charleston, US, Nov. 2018.

[5] 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.

[6] L. Freitag, K. Ball, J. Partan, P. Koski, and S. Singh, "Long range acoustic communications and navigation in the Arctic," in *Proc. MTS/IEEE OCEANS'15*, Washington DC, US, Oct. 2015.

[7] 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.

[8] 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 *Proc. ACM WUWNet*, Shenzhen, China, Dec. 2018.

[9] A. Mahmood and M. Chitre, "Ambient Noise in Warm Shallow Waters: A Communications Perspective," *IEEE Communications Magazine*, vol. 55, no. 6, pp. 198–204, Jun. 2017.

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

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

[12] 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, p. 6, Nov. 2019.

[13] 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.

[14] A. Signori, C. Pielli, F. Chiariotti, M. Giordani, F. Campagnaro, N. Laurenti, and M. Zorzi, "Jamming the underwater: a game-theoretic analysis of energy-depleting jamming attacks," in *14th International Conference on Underwater Networks & Systems (WUWNet)*. ACM, Oct. 2019.

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

[16] 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.

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

[18] J. C. Harsanyi, "Games with incomplete information played by "Bayesian" players part II. Bayesian equilibrium points," *Management Science*, vol. 14, no. 5, pp. 320–334, Jan. 1968.

[19] 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.

[20] "S2C R 18/34 WiSE Underwater Acoustic Modem," Last time accessed: Jan. 2020. [Online]. Available: https://evologics.de/acoustic-modem/18-34/wise-serie