Jamming the Underwater: a Game-Theoretic Analysis of Energy-Depleting Jamming Attacks

Alberto Signori, Chiara Pielli, Federico Chiariotti,
Marco Giordani, Filippo Campagnaro, Nicola Laurenti, Michele Zorzi
University of Padova, Department of Information Engineering (DEI), Italy
{signoria,chiariot,piellich,giordani,campagn1,nil,zorzi}@dei.unipd.it

ABSTRACT

Underwater sensor networks can be employed in both military and environmental remote coastal monitoring applications, such as enemy targeting and identification, and tsunami prevention. Jamming can be a serious issue in these networks, typically composed by battery-powered nodes, as an attacker can not only disrupt packet delivery, but also reduce the lifetime of energy-constrained nodes. In this work, we consider a malicious jammer with the dual objective of preventing communication and depleting the battery of a targeted underwater sensor node. The jammed node may use packet-level coding as a countermeasure against the attack, so as to increase its chances of correctly delivering its information to the legitimate receiver. We model this scenario as a multistage game, derive the optimal long-term strategies for both sides, and evaluate how the position of the jammer affects the communication of the legitimate network.

KEYWORDS

Underwater acoustic networks; jamming; game theory; block code; security in underwater networks.

1 INTRODUCTION

By its very nature, the underwater scenario is very challenging for radio wireless communications: the drastic attenuation makes the reception of electromagnetic waves possible only over very short-range broadband links [1]. Acoustic waves, instead, can propagate from a few hundred meters up to tens of kilometers, depending on their frequency [2]. However, the use of this technology is hindered by several challenges, since the underwater acoustic channel is strongly affected by the environmental noise caused by wind, marine life, and shipping activities. In addition, it is characterized by a narrow band, a long propagation delay, and strong multipath effects due to the signal reflection with the sea bottom and surface [3, 4].

Despite the harshness of the propagation environment, Underwater acoustic Sensor Networks (USNs) are employed in both military and industrial (typically, oil and gas) applications, as well as to monitor seabed erosion and tsunami risk. In military operations, USNs are used to extend the coastal monitoring range and enable just a few ships to patrol an area of several square miles [5]. In such a critical application, where underwater sensor nodes are typically employed for enemy targeting and identification, a Denial-of-Service (DoS) attack can have disastrous consequences for the attacked system, which already faces the challenges of a hostile environment.

1.1 Related Work

One of the most common DoS attacks is physical layer jamming [6]. The principle behind it is simple, yet powerful: a malicious node injects signals into the channel in order to deny or at least reduce services 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 produced with the same bandwidth as the transmitter [7]. 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 [8]. 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 [9], or actively react to the DoS attack, e.g., by increasing their transmit power [10] or using channel-hopping [11]. In case of active defense, game theory is often used to model the interaction between the jammer and its victim. The main drawback of active defenses is a typically increased energy consumption, which

WUWNET'19, October 23–25, 2019, Atlanta, GA, USA

ACM ISBN 978-1-4503-7740-9/19/10…$15.00
https://doi.org/10.1145/3366486.3366546

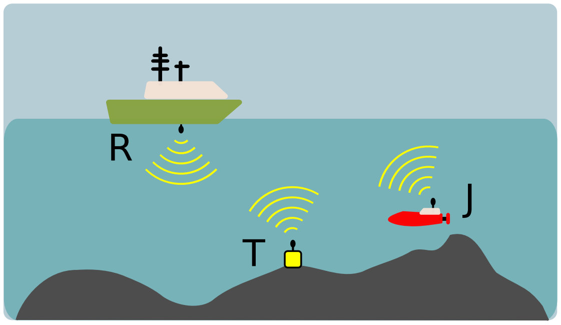

Figure 1: An underwater jamming attack: a jammer J tries disrupting the communication between a transmitter T and its intended receiver R.

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 [12], 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 [13], 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 [14] applies this principle in an Internet of Things (IoT) network, exploiting retransmissions as part of the defense strategy.

Some recent works have also analyzed the jamming issue in the context of underwater acoustic networks. For example, [15] applies a reinforcement learning deep Q-network-based transmission scheme 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.

In underwater acoustic networks, the propagation delay can be longer than the signal duration [16], 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 in the case the transmitter sends a sequence of packets with a deterministic or predictable pattern, such as in data muling applications. In [17], 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.

1.2 Motivation and Contribution

In this work, we consider an acoustic underwater transmitter T under a jamming attack. 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 itself, T uses packet-level coding: whenever it needs to send an update 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 [18].

In our scenario, both the transmitter and the jammer are battery-limited. Thus, to disrupt T's communication, J uses two strategies: besides blocking the legitimate transmissions themselves, J tries to make T send more redundancy packets, increasing its energy consumption so that T depletes its battery faster and can no longer send updates to R. T and J can be modeled as rational players in a zero-sum multistage game, in which each burst of packet represents a subgame. T will decide how much redundancy to add at each round, spending more energy to increase its chances of successfully delivering the update. J will decide how long it will jam, spending energy to let fewer packets get through.

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

The rest of the paper is organized as follows. In Sec. 2, we present the game theoretic model and the system scenario. Sec. 3 explains how to derive the optimal strategies for the jammer and transmitter. Sec. 4 describes the results and numerical evaluation, and, finally, Sec. 5 concludes the paper.

2 GAME THEORETIC MODEL

We consider a transmitter T at distance d_{TR} from a receiver R, and a jammer J at distance d_{JR} from R. The jamming attack is modeled as a zero-sum game $\mathbb{G}$ between the two rational players T and J, and we study a full information scenario.[1]

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 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 deliver at least K packets to the destination node within the duration of the subgame. We assume a packet erasure channel, thus R can recover the K information packets if any K of the $N_T^{(m)}$ coded packets are correctly received [18].

Both players are battery-powered nodes, thus 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 $\mathcal{B}_i \triangleq [0, 1, \ldots, B_i^{(0)}]$, $i \in \{T, J\}$, 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; we consider the quantum $E_{\text{tx},i}$ 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.

Table 1: 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 G
λ	Exponential discounting factor
α_i	Energy/PDR weighting factor
$u_i^{(m)}$	Payoff function in subgame m
$U_i^{(m)}$	Payoff function in multistage game G in subgame m
$\chi_i^{(m)}$	Indicator function in subgame m
$f_i^{(m)}$	Energy penalty function in subgame m
$N_T^{(m)}$	Number of packets that T sends in subgame m
$N_{\text{CC}}^{(m)}$	Packets sent over clear channel in subgame m
$N_{\text{JC}}^{(m)}$	Packets sent over jammed channel in subgame m
$N_J^{(m)}$	Number of packets that J tries to jam in subgame m
$D^{(m)}$	Total packets delivered in subgame m
$d_{\text{CC}}^{(m)}$	Packets delivered over clear channel in subgame m
$p_{e_{\text{CC}}}$	Packet error probability over clear channel
$p_{e_{\text{JC}}}$	Packet error probability over jammed channel
$B_i^{(m)}$	Battery level in subgame m
E_{tx}	Energy required to transmit/jam a packet
P_{tx}	Transmission power

We now describe the structure of a single subgame and then illustrate the evolution of the multistage full game. Table 1 reports a summary of the notation used.

2.1 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, it can trigger its transmissions to perfectly jam the subsequent time slots.

Thus, T decides *(i)* how many packets $N_T^{(m)} \in \mathcal{N}_T^{(m)} \triangleq \{K, K+1, \ldots, \min(2K, B_T^{(m)})\}$ 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 packets $N_J^{(m)} \in \mathcal{N}_J^{(m)} \triangleq \{0, 1, \ldots, \min(2K-1, B_J^{(m)})\}$ 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,

[1] Full information is justified 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.

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.

Each subgame is modeled as a *zero-sum* game, i.e., a completely adversarial and symmetrical game in which each gain for one player is balanced by a loss for the other [14]. 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 packets $N_J^{(m)}$ 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 complete game: the larger $N_T^{(m)}$, 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.

2.2 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 [19], $u_i^{(m)}$, $i \in \{T, J\}$ 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 $U_i^{(m)}(1)$.

3 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 or jam the legitimate packets, respectively. According to the game defined in Sec. 2, 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 [20]. 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 full 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.

3.1 Expected Payoffs 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 $\mathbb{E}\Big[u_i \Big| N_T,\, N_J\Big]$, $i \in \{T, J\}$ can be calculated from the quantity $\mathbb{E}\Big[\chi_i \Big| N_T,\, N_J\Big]$, $i \in \{T, J\}$, which represents the expected outcome of the subgame (as introduced in Sec. 2.1, χ_T and χ_J are indicator terms for the transmission and jamming success, respectively). We introduce quantities $N_{\mathrm{CC}} \le N_T$ and $N_{\mathrm{JC}} \le N_T$ to indicate the number of packets that node T sends over a clear and jammed channel, respectively. Obviously, $N_T = N_{\mathrm{CC}} + N_{\mathrm{JC}}$, so we can easily obtain the value of N_{CC} once we know N_{JC}. Using the law of total probability, for node T we have:

$$\mathbb{E}\Big[\chi_T | N_T,\, N_J\Big] = \sum_{N_{\mathrm{CC}}=0}^{N_T} \mathbb{E}\Big[\chi_T | N_{\mathrm{CC}}\Big] \mathrm{P}\Big(N_{\mathrm{JC}} | N_T,\, N_J\Big) \qquad (5)$$

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. It can be expressed as:

$$\mathbb{E}\Big[\chi_T \mid N_{\mathrm{CC}}\Big] = \sum_{D=K}^{N_T} \sum_{d_{\mathrm{CC}}=0}^{D} \binom{N_{\mathrm{CC}}}{d_{\mathrm{CC}}} p_{e_{\mathrm{CC}}}^{N_{\mathrm{CC}}-d_{\mathrm{CC}}} \left(1 - p_{e_{\mathrm{CC}}}\right)^{d_{\mathrm{CC}}} \cdot \binom{N_{\mathrm{JC}}}{D - d_{\mathrm{CC}}} p_{e_{\mathrm{JC}}}^{N_{\mathrm{JC}}-(D-d_{\mathrm{CC}})} \left(1 - p_{e_{\mathrm{JC}}}\right)^{D-d_{\mathrm{CC}}} \qquad (6)$$

The external summation iterates on all possible values of the number of delivered packets $D \le N_T$ resulting in a success. Eq. (6) then splits D between packets that are delivered over a clear channel, i.e., $d_{\mathrm{CC}} \le D$, and those which are delivered over a jammed channel, i.e., $D - d_{\mathrm{CC}}$. For the two cases, the packet error probability is equal to $p_{e_{\mathrm{CC}}}$ and $p_{e_{\mathrm{JC}}}$, respectively, and is a function of the Signal to Noise Ratio (SNR) or Signal to Interference and Noise Ratio (SINR). The packet error probability depends on the modulation: if Binary Phase Shift Keying (BPSK) is employed (as it is one of the most commonly used in underwater communications [21]), we have:

$$\begin{aligned} p_{e_{\mathrm{CC}}} &= 1 - \left(1 - Q(\sqrt{2\,\mathrm{SNR}_{\mathrm{CC}}})\right)^L, \\ p_{e_{\mathrm{JC}}} &= 1 - \left(1 - Q(\sqrt{2\,\mathrm{SINR}_{\mathrm{JC}}})\right)^L, \end{aligned} \qquad (7)$$

where L is the packet length (in bits), the Q-function is the tail distribution of the standard normal distribution. The SINR is given by:

$$\mathrm{SNR}_{\mathrm{CC}} = \frac{P_{\mathrm{tx},T}\, g_{\mathrm{T}}}{W}, \qquad \mathrm{SINR}_{\mathrm{JC}} = \frac{P_{\mathrm{tx},T}\, g_{\mathrm{T}}}{W + P_{\mathrm{tx},J}\, g_J}. \qquad (8)$$

In Eq. (8), $P_{\mathrm{tx},i}$ represents the transmit power of node $i \in \{T, J\}$, W is the underwater acoustic noise, 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 can be computed as described in [2, Sec. II]. Note that in our scenario the transmit power is $P_{\mathrm{tx},i} = E_{\mathrm{tx},i}^{(T)}/\tau$. If a different modulation is used, the only required change is in (7), while the rest of the model remains the same.

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

$$\mathrm{P}\Big(N_{\mathrm{JC}} \mid N_T,\, N_J\Big) = \frac{\binom{N_T-1}{N_{\mathrm{JC}}}\binom{(2K-1)-(N_T-1)}{N_J-N_{\mathrm{JC}}}}{\binom{2K-1}{N_J}}, \qquad (9)$$

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. 2. In Eq. (9) , 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. 2.1: 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 (9) into (5), we can finally obtain the expected value of the indicator function $\chi_i^{(m)}$ and then the expected value of the payoffs $u_i^{(m)}$.

3.2 Dynamic Programming Solution

In the case of full information, an optimal solution of the multistage game can be determined through dynamic programming. 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 $i \in \{T, J\}$. 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 is not sufficient to transmit at least K packets, i.e., when $B_T^{(m)} < K$. We denote this final state as ε and define its payoff as:

$$U_i^{(m)}\Big(\Gamma \mid S^{(m)} = \varepsilon\Big) = 0 \quad \forall\, i, \Gamma. \qquad (10)$$

We can now define $U_i^{(m)}\left(\Gamma \mid S^{(m)}\right)$ recursively for all other states, considering that the battery charge can never increase,

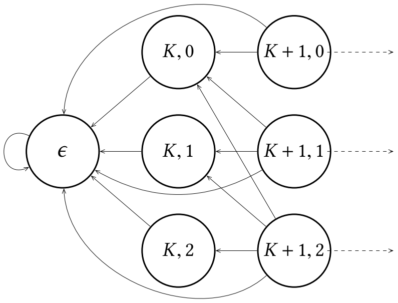

Figure 2: State transitions for the multistage game $\mathbb{G}$.

hence $B_i^{(m+1)} \leq B_i^{(m)}\ \forall i, m$. It is:

$$U_i^{(m)}\left(\Gamma \mid S^{(m)}\right) = \mathbb{E}\left[u_i^{(m)} \mid S^{(m)}\right] + \lambda \sum_S U_i^{(m+1)}(\Gamma - 1 \mid S)\,\mathrm{P}\left(S^{(m+1)} = S \mid S^{(m)}\right), \tag{11}$$

The payoff in a state is thus computed as the expected payoff $u_i^{(m)}$ obtained in the subgame corresponding to that state plus the payoff that is expected to be obtained in the next subgame, discounted by factor λ (see (4)). This latter term is calculated by averaging over all possible next states $S^{(m+1)}$ weighed by the probability of transitioning to that state. For a given pair of strategies (s_C, s_J), such state transition probability is given by:

$$\mathrm{P}\Big(S^{(m+1)} = (B_T, B_J) \mid S^{(m)}\Big) = \mathrm{P}\left(B_T^{(m+1)} = B_T \mid B_T^{(m)}, s_T\right) \cdot \mathrm{P}\left(B_J^{(m+1)} = B_J \mid B_J^{(m)}, s_J\right), \tag{12}$$

where

$$\mathrm{P}\left(B_i^{(m+1)} = S \mid B_i^{(m)}, s_i\right) = \Phi_{s_i}\left(B_i^{(m)} - B_i^{(m+1)}\right). \tag{13}$$

By substituting (12) and (13) into (11), we have a full recursive formulation for the payoff $U_i^{(m)}(\Gamma)$ for any strategy pair. Once the payoff bimatrix is thus constructed, the Lemke-Howson algorithm can be used to find the mixed NE [22]. By starting from the lowest states and calculating the expected payoffs $U_i^{(m)}(\gamma)$, $\gamma \in \{1,\ldots,\Gamma\}$, 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 or jam packets, respectively. The game ends at stage $h \in \mathbb{N}$ when state ϵ is reached, i.e., when $B_T^{(h)} < K$. Notice that, if the battery of J empties before T's, the game evolves in the limit condition of T playing against the channel.

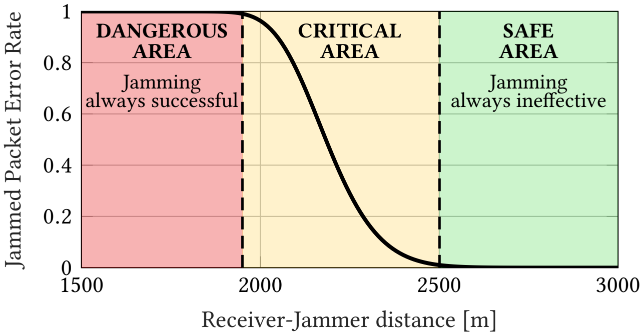

Figure 3: Packet error rate $p_{e_{\mathrm{JC}}}$ for a jammed slot as a function of the distance d_{JR} between J and R when the distance between T and R is $d_{\mathrm{TR}} = 1500$ m.

4 NUMERICAL EVALUATION

We evaluate the performance of the optimal strategies by studying the energy consumption and the PDR of T.

The considered system settings aim to simulate the behavior of the Teledyne Benthos modem [21] when employing the so called C band, which corresponds to bitrate $R = 2560$ bits/s, carrier frequency $f_c = 24.5$ kHz, bandwidth $bw = 5$ kHz and PSK modulation (in our simulations, we assume BPSK modulation). The acoustic transmission power has been set to 180 dB re 1 μPa, which corresponds to a power consumption of approximately 20 W (the maximum transmission power of a Teledyne Benthos modem). The distance between T and R is set to $d_{\mathrm{TR}} = 1500$ m, while the distance between J and R is varied as $d_{\mathrm{JR}} \in [1500, 3000]$ m. In each round of the game (see Sec. 2.1), the legitimate transmitter aims at delivering $K = 4$ packets and can transmit $N_T \in \{4, \ldots, 8\}$ packets, each of size $L = 480$ bits. The packet duration is therefore $L/R = 187.5$ ms and requires an energy consumption of 3.75 J. At the beginning of each run, the battery levels of both jammer and transmitter (B_J and B_T) are set to 750 J, and are then completely discharged after the transmission of 200 packets. The propagation and noise models we used are presented in [2]: we set the geometrical spreading factor to 1.5, the shipping factor to 1, and the wind speed to 5 m/s.

4.1 Simulation Results

Based on the position of the jammer, we can distinguish three regions in the underwater area, as shown in Fig. 3. 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 1900 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 2500 m away from R. Between these two extremes, an appropriate strategy might

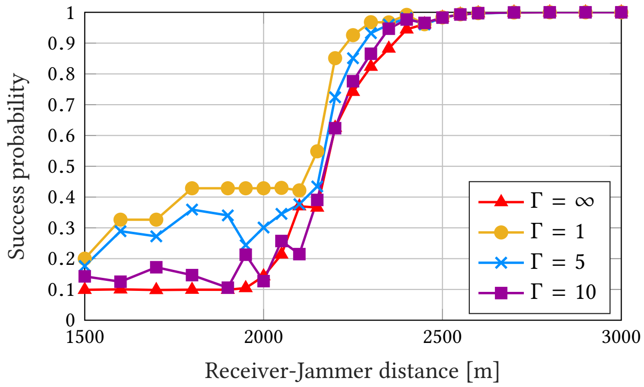

Figure 4: Success probability in a single subgame as a function of d_{JR}, for different values of Γ when $\alpha = 0.4$.

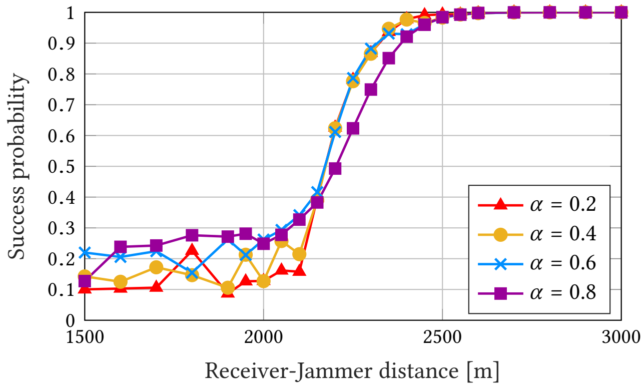

Figure 5: Success probability in a single subgame as a function of d_{JR}, for different values of α when $\Gamma = 10$.

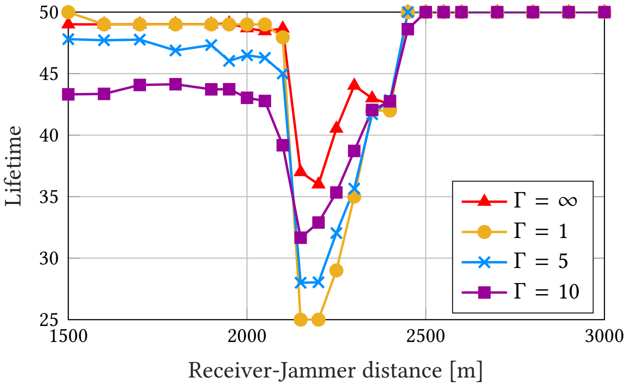

Figure 6: Transmitter's lifetime as a function of d_{JR}, for different values of the time horizon Γ when $\alpha = 0.4$.

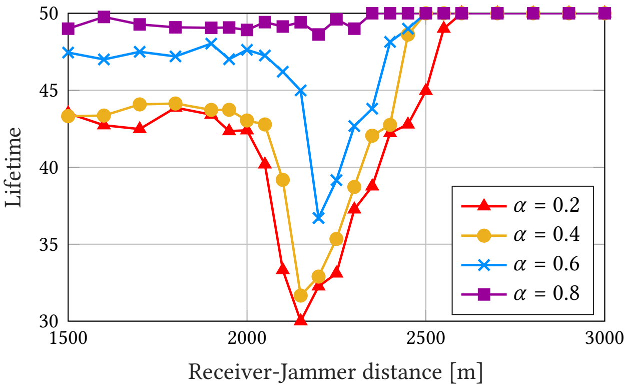

Figure 7: Transmitter's lifetime as a function of d_{JR}, for different values of α when $\Gamma = 10$.

significantly improve the performance: it is interesting to investigate how the game evolves in the critical region (where $d_{\mathrm{JR}} \in [1900, 2500]$ m in our scenario), and which distances yield a successful game for T.

This partition is also clear from Fig. 4, 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 2500 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, a more aggressive policy does not guarantee success: as Fig. 5 shows, lower values of the parameter α correspond to a *lower* success probability. In this case, the effect is due to the fact that α is the same for both T and J: a jammer close to the receiver and with an aggressive strategy can reduce the transmission success probability to 10%. 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.

Interestingly, Fig. 6 shows that nodes with longer time horizons also have a decreased lifetime (which is measured as the number of subgames played). This means that, when both nodes have a long-term view, the jammer is more effective at preventing transmissions. We remind the reader that 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. Fig. 7 confirms the trend: less aggressive nodes have both a higher success probability and a longer lifetime. The lifetime is maximized when $d_{\mathrm{JR}} > 2500$ 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 significantly 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.

5 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 and derive the optimal strategies assuming that the jammer and the legitimate transmitter are two rational players with full knowledge about the adversary, playing a zero-sum game.

We studied the impact of the jamming attack on the lifetime and the PDR of the transmitter, and in particular the role played by the length of the time horizon used to calculate the expected payoffs, the distance of the jammer from the receiver, and the importance of the energy consumption in the payoff functions. 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.

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. It may also serve as a guideline for more realistic scenarios, which we plan to investigate as future work, possibly including a more realistic characterization of the acoustic channel, based on real field measurements, evaluating the effect of changing other parameters such as the starting battery level, and relaxing the full information assumption, i.e., considering a Bayesian incomplete information 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] 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.

[2] 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.

[3] 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.

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

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

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

[7] 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.

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

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

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] C. Pielli, F. Chiariotti, N. Laurenti, A. Zanella, and M. Zorzi, "A game-theoretic analysis of energy-depleting jamming attacks," in *IEEE International Conference on Computing, Networking and Communications (ICNC)*, Jan. 2017.

[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] 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.

[17] 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.

[18] 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.

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

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

[21] "Teledyne-benthos acoustic modems," accessed: July. 2019. [Online]. Available: http://www.teledynemarine.com/acoustic-modems/

[22] 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.