Jamming in Underwater Sensor Networks as a Bayesian Zero-Sum Game with Position Uncertainty

Valentina Vadori, Maria Scalabrin, Anna V. Guglielmi, and Leonardo Badia
Dept. of Information Engineering, University of Padova, via Gradenigo 6B, 35131 Padova, Italy
email: {vadoriva, scalabri, guglielm, badia}@dei.unipd.it

***Abstract*—We investigate a jamming problem in an underwater acoustic sensor network, where nodes try to communicate in spite of an adversary that is attempting to block their communications. We take into account that the attenuation of underwater acoustic channels is strongly dependent on the communication distance and the signal frequency. We frame the problem in a game theoretic setup, as a Bayesian zero-sum game where the sensor network acts as the maximizer of the transmission capacity, while the jammer is the minimizer. In particular, we are interested in evaluating the effect of the nodes' position on the resulting equilibrium. The Bayesian character comes into play to represent the uncertainty on the position information of the nodes. Our evaluations show that for many network configurations, the equilibrium strategy of the jammer is pure. Thus, the transmitters can act as though the jammer only causes a higher level of interference. This allows us to identify positions where the damage caused by a jammer is easier to quantify, but the jammer itself is harder to detect.**

***Index Terms*—Underwater communication; Acoustic sensors; Wireless sensor networks; Frequency division multiaccess; Jamming; Zero-sum games; Bayesian games.**

I. Introduction

UNDERWATER acoustic sensor networks (UASNs) can be employed in a wide array of applications, from monitoring and prevention of seismic events (tsunamis, earthquakes), to equipment control and surveillance for autonomous systems operating undersea [1]. As any other kind of communication systems, they may be subject to malicious attacks, for example jamming, where an adversary tries to disrupt network operation by contrasting the transmission at the physical layer. Since most of the practical solutions for counteracting jammers are designed with terrestrial radio networks in mind, they may be unsuitable for UASNs, which can therefore be extremely vulnerable to such attacks [2].

In this paper, we tackle this scenario with game theory instruments, an approach that has recently become quite popular in the networking research community over the last ten years [3], [4]. Several papers analyze the situation where a jammer contrasts the legitimate network transmitters to disturb their communications. In many contributions, such as [5], the jammer is assumed to be capable to disrupt the communication exchange by adopting some processing of the messages. Conversely, we consider a simpler scenario, similar to [6], where the jammer creates noise-like interference with the aim of producing denial-of-service attacks. Indeed, underwater sensors do not usually possess sophisticated signal processing capabilities and, consequently, it is reasonable to assume that jamming attacks just consist of raising the noise level. In our setup, the sensor nodes are able to use several communication channels and the resulting utility of the network is determined by its total transmission capacity. The jammer is only able to produce noise-like interference on a channel at a time. In addition, the interference caused by the attacker on a channel depends on the attenuation perceived on it.

In this scenario, we embrace a classic formulation of the problem as a zero-sum game [5], [7], [8], in which the sensors play together as the *maximizer* of a given objective, i.e., the sum capacity that the network can reach on the channels involved in the transmission, and the jammer is the *minimizer* of the same objective. We are interested in computing the equilibrium value of the game when all involved actors are rational, that is, they only aim at maximizing their own objective.

Since signal attenuations are position-dependent, our objective is to examine the role of the mutual placements of sensors and jammer. Thus, we consider that the maximizer may have several types according to the position of its nodes, and consequently we discuss a Bayesian approach [9], to represent the fact that the jammer may have an imperfect knowledge about the network structure. Our purpose is to analyze the role of the attacker's position and to underline the effects that it has on the resulting equilibrium. As a consequence, we assume that the position of the jammer is common knowledge. To further clarify, we are not suggesting that the network is actually able to know the position of the jammer. This is just an assumption for the game theoretic setup. We want to explore if the jammer's presence in a certain position is relevant for the network and if it changes its gameplay, and the position of the jammer will be actually considered as the independent variable of the numerical evaluations.

According to the propagation scenario chosen, there may be many situations where the impact of the jammer is limited, e.g., it is so far from the network that it cannot damage it. However, our findings are not limited to these simple cases. Depending on the game formulation, the presence of the jammer can be ignored if the resulting zero-sum game has a single Bayesian Nash Equilibrium (BNE) in pure strategies for the attacker, meaning that there is only one behavior that the rational jammer can assume. This does not mean that the jammer does not cause any damage, but rather that its impact is predictable, whereas, at the same time, there are also no effective countermeasures in order to contrast it. It can be argued that the jammer would not even be detected in the first

place [8], since if the equilibrium play of the jammer is a certain pure strategy, sensors cannot distinguish the presence of the attacker in the network from a high interference level.

On the other hand, we can label some jammer candidate positions as *critical*, if a jammer located there will play a mixed strategy at the BNE, and consequently sensors have to counter more than one possible jamming action. In general, the choice of the appropriate strategy against jamming attacks should consider the location of the jammers; moreover, we infer that surveillance of the area should give special care to possible positions of a jammer that are critical in the sense defined above.

The rest of this paper is organized as follows. Section II describes the underwater scenario, detailing the relevant aspects of acoustic propagation and modeling. In Section III, we formulate a Bayesian zero-sum game between a network and a jammer, of which we compute the BNEs and the value in Section IV. Section V presents some numerical results and Section VI draws the conclusions.

II. Underwater Scenario

Research on UASNs is somehow more limited compared to terrestrial sensor networks based on radio communications. These two kinds of networks share similarities for what concerns their many potential applications and their distributed nature; the main difference relates to the specific physical layer utilized, which relies on acoustic and radio waves, respectively, since it is generally accepted that radio signals do not propagate well underwater [10].

While the wireless medium is fairly understood in the literature, the acoustic channel for underwater communications is more difficult to characterize and utilize. Also, the standard uses of acoustic communications mostly involve echolocation (with applications such as the sonar and the fathometer), which, from a networking standpoint, have little interest as it only involves a single transmitter-receiver pair. The study of acoustic communications in a network context is more constrained, also because, still differently from terrestrial networks, equipment may be much more expensive.

Still, it may be expected that in specific environments and fields of application, submarine networking can find suitable exploitation. Moreover, due to the inherent difficulty of coordinating multiple nodes underwater, game theory investigations can be useful to devise distributed solutions. The major features and challenges that need to be faced in underwater environments include, but are not limited to, the following issues [11]. First of all, underwater channels have a small bandwidth compared to their terrestrial counterparts, resulting in lower bit rates. Also, the speed of acoustic waves in water is five orders of magnitudes lower than that of electro-magnetic waves in air (about $1.5{\cdot}10^3$ m/s versus $3{\cdot}10^8$ m/s, respectively); this results in a huge propagation delay in underwater channels. Thus, it is hinted in [12] that frequency division multiaccess (FDMA) may be more attractive than its time division analog. However, underwater channels have much lower carrier frequencies than radio (kilohertz versus gigahertz), thus they cannot be considered as narrowband and frequency-selectivity must be accounted for even in a simple analysis. Actually, the use of cognitive and opportunistic access techniques can be a solution to adapt communication to the varying conditions at different times, distances, and channels.

All of these elements will be taken into account in our analysis. Other aspects that are not explicitly considered but are worth mentioning regard the higher unreliability of underwater networks, even in controlled scenarios: radio networks can be unreliable too, but to a lower extent and/or only if adverse conditions are assumed. Underwater links may lose connectivity due to propagation phenomena under the sea surface, or because of node mobility due to oceanic currents. Finally, underwater sensor nodes have severe energy constraints, since battery replacement or energy harvesting, e.g., through solar panels, may be extremely difficult or unavailable.

For these reasons, jamming attacks may be extremely harmful in underwater environments, and mechanisms to detect and prevent them are important. The huge propagation delay might forbid the sensor nodes from communicating with external controllers; as a consequence, an underwater network has to exploit its own resources to detect and mitigate the jamming attack [2].

The acoustic power attenuation of underwater channels is strongly dependent on the communication distance and on the signal frequency. An absorption loss is present, due to the conversion of acoustic pressure into heat, which increases with the signal frequency f as well as with the communication distance d. As a consequence, shorter communication links offer higher data rates. Attenuation $A(d,f)$ can be expressed in dB using Urick's model as [13]

$$10\log_{10} A(d,f) = A_0 + \mathtt{k}\log_{10} d + d\,10\log_{10}\mathtt{a}(f) \qquad (1)$$

where $\mathtt{k}$ is a spreading factor term, $\mathtt{a}(f)$ is an absorption coefficient, and A_0 is a normalization constant (the value for $A(d,f)$ at 1 m and very low frequencies). Formula (1) shares structural similarities with path loss expressions commonly used for the wireless case [14]. There are some relevant differences, though. First of all, since water is a much more dispersive medium for acoustic waves than what air is for electro-magnetic beams, there is a *further* dependence of distance: beyond the geometrical spreading, i.e., the first summand, d also appears in the second one, the absorption term. Also, the spreading factor $\mathtt{k}$, describing the geometry of propagation, has *lower* values than what usually considered in radio environments [14]. Spherical spreading, that would lead to $\mathtt{k}=20$, is taken to be a best-case value in radio propagation, where the presence of obstacles lead to much higher values. Instead, for underwater acoustic propagation, shallow water scenarios may even have a more favorable spreading than spherical, since physical waveguide effects may produce a cylindrical spreading [15], and therefore $10 \le \mathtt{k} \le 20$.

Absorption is expressed using Thorp's formula, giving $\mathtt{a}(f)$ as a function of frequency f as [16]

$$10\log_{10}\mathtt{a}(f) = \mathtt{a}_{\mathrm{W}} f^2 + \alpha_1 \frac{f^2}{f_1^2+f^2} + \alpha_2 \frac{f^2}{f_2^2+f^2} + \dots \qquad (2)$$

where $\mathtt{a}_{\mathrm{W}}$ is a pressure-dependent coefficient describing absorption in pure water, while the α_js, with $j{=}1,2,\dots$ weigh

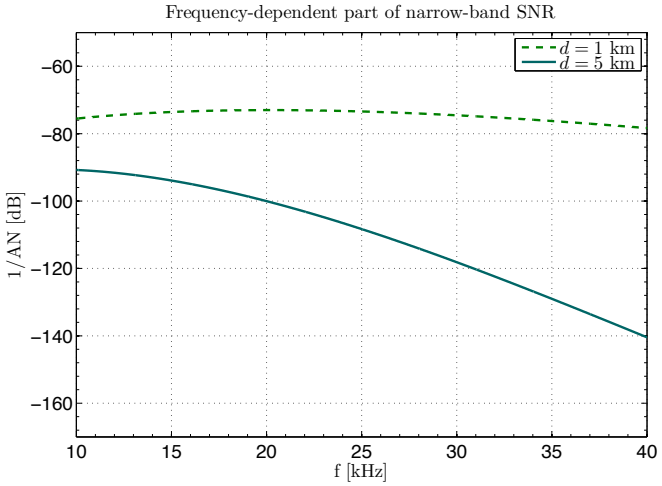

Fig. 1. Frequency-dependent part of the SNR $[A(d,f)N(f)]^{-1}$ for a tone transmitted underwater with $d = 1, 5$ km ($s = 0.5$, $w = 0$ m/s).

further terms due to saline absorptions, and the terms f_j are the relaxation frequencies for these terms. For sea water, two such terms are usually included, $j = 1$ is for boric acid, especially relevant at low frequencies, and $j = 2$ for magnesium sulphate.

The oceanic noise can be modeled as the sum of several components, including turbulence, shipping, surface motion, and thermal noises [17]. Thus, we consider a power spectral density (PSD) of the noise $N(f) = N_{\rm t}(f)+N_{\rm s}(f)+N_{\rm w}(f)+N_{\rm th}(f)$, where $N_{\rm t}(f)$, $N_{\rm s}(f)$, $N_{\rm w}(f)$, and $N_{\rm th}(f)$ are noise terms corresponding to turbulence, shipping, surface motion, and thermal noise, respectively.

These components can be expressed in dB re μPa per Hz as a function of frequency f in kHz as [12]

$$10\log_{10} N_{\rm t}(f) = 17 - 30\log_{10}(f) \quad (3)$$

$$10\log_{10} N_{\rm s}(f) = 40 + 20(s-0.5) + 26\log_{10}(f) - 60\log_{10}(f+0.03) \quad (4)$$

$$10\log_{10} N_{\rm w}(f) = 50 + 7.5w^{1/2} + 20\log_{10}(f) - 40\log_{10}(f+0.4) \quad (5)$$

$$10\log_{10} N_{\rm th}(f) = -15 + 20\log_{10}(f) \quad (6)$$

The parameters in (3)–(6) are the shipping activity s, ranging from 0 for lowest activity to 1 for most intense shipping and w, i.e., the wind speed value in m/s, since surface motion noise is caused by wind-driven waves. In our numerical setup, we considered practical spreading with $\mathtt{k}$=15, A_0=0 dB, intermediate shipping activity s=0.5 and no wind (w=0), and a frequency range between 10 and 40 kHz. At these frequencies, absorption due to pure water and boric acid are negligible, while we consider the absorption associated to magnesium sulphate, with parameters f_2=66 kHz and α_2=48 dB/km [18].

If a communication channel operates on a frequency band $\mathcal{B}_i$ with bandwidth $B_i = |\mathcal{B}_i|$, using a flat power profile, then the average signal-to-noise ratio (SNR) for a tone at frequency f can be expressed as [12]

$$SNR(d,f) = \frac{P_{\rm S}}{A(d,f)N(f)B_i} \quad (7)$$

where $P_{\rm S}$ is the power of the transmitting sensor node, $A(d,f)$ is the attenuation PSD and $N(f)$ is the noise PSD. In particular, $A(d,f)$ increases with f while $N(f)$ decreases with f (at least in the relevant interval for acoustic communications). As a result, $[A(d,f)N(f)]^{-1}$ has a maximum for some frequency. Fig. 1 shows the frequency-dependent part of the SNR for a tone transmitted underwater with $d = \{1, 5\}$ km with the aforementioned choice of parameters.

For this transmission over $\mathcal{B}_i$, Shannon's capacity C_i is

$$C_i = \int_{\mathcal{B}_i} \log_2\left[1 + SNR(d,f)\right] {\rm d}f\,. \quad (8)$$

However, if a malicious node also causes noise-like interference on a specific channel, this has to be taken into account in the computation of the capacity. Therefore, we replace the SNR with the average signal-to-noise-plus-jammer ratio (SNJR) which is

$$SNJR(d,f) = \frac{P_{\rm S}}{A(d,f)[N(f)B_i + P_{\rm J}A(d_{\rm J},f)^{-1}]} \quad (9)$$

where $P_{\rm J}$ is the power of the malicious node and $d_{\rm J}$ is the distance from the receiver. The channel capacity in the presence of a jammer becomes

$$C_i' = \int_{\mathcal{B}_i} \log_2\left[1 + SNJR(d,f)\right] {\rm d}f\,. \quad (10)$$

III. Game Theory Model

We consider an underwater network with 2 sensors, denoted as S_1 and S_2, transmitting data to a sink node, both using the same transmission power $P_{\rm S}$. The distances from the sink are d_1 and d_2 for S_1 and S_2, respectively. The network implements an FDMA scheme, so that the entire communication band available to the sensors is split into two channels in the frequency bands $\mathcal{B}_1$ and $\mathcal{B}_2$. In such a scheme, either $\mathcal{B}_1$ is assigned to S_1 (and $\mathcal{B}_2$ is assigned to S_2) or $\mathcal{B}_1$ is assigned to S_2 (and $\mathcal{B}_2$ to S_1). This entire network, consisting of S_1, S_2, and the sink node, plays a single player S, whose aim is to maximize the overall network capacity, computed as the sum of the capacities achievable on channels $\mathcal{B}_1$ and $\mathcal{B}_2$.

The legitimate transmissions of the 2 sensor nodes are obstructed by a malicious jammer J that acts to minimize the total network capacity. The jammer is located at distance $d_{\rm J}$ from the sink node and can only transmit over either $\mathcal{B}_1$ or $\mathcal{B}_2$ (but not both) using a transmit power $P_{\rm J}$.

The interaction between S and J is modeled as a two-player zero-sum game with incomplete information. Actually S can be of many *types*, represented by a finite set $\Theta = \{(d_1^{(1)}, d_2^{(1)}), ..., (d_1^{(|\Theta|)}, d_2^{(|\Theta|)})\}$, This means that each element of Θ is a pair of distances of S_1 and S_2 from the sink node, i.e., $d_i^{(k)}$ is the distance of S_i in the kth pair. We denote the kth type as θ_k and the probability that S can be of type θ_k as p_k, such that $p_k \geq 0$ and $\sum_k p_k = 1$. In this setting J has no type. We actually consider the distance $d_{\rm J}$ to be common knowledge in the game, together with the prior probability distribution $\boldsymbol{p} = (p_1, ..., p_{|\Theta|})$.

This approach reflects that of Bayesian games [9], where a fictitious player called "Nature" is introduced to select the types of players according to the prior probability distribution

[7]. In this setting, Nature decides upon S's type θ_k according to $\boldsymbol{p}$. Then S is informed of his type θ_k and decides its own action, which can be either of the following:

- A_1: assign $\mathcal{B}_1$ to S_1 (and, consequently, $\mathcal{B}_2$ to S_2)
- A_2: assign $\mathcal{B}_2$ to S_1 (and, consequently, $\mathcal{B}_1$ to S_2)

It follows that S has $N = 2^{|\Theta|}$ pure strategies, since S can be of $|\Theta|$ different types and for each of them it has 2 actions to choose from. We describe S's pure strategies as $|\Theta|-$tuples and we denote their set as $\mathcal{X} = \{X_i\}_{i=1,...,N}$. The kth entry, denoted as $X_i(k)$, of the ith pure strategy defines the action played by S when it is of type θ_k. J has instead 2 pure strategies, which coincide with its 2 possible actions:

- Y_1: attack channel $\mathcal{B}_1$
- Y_2: attack channel $\mathcal{B}_2$

We denote the set of J's strategies as $\mathcal{Y} = \{Y_1, Y_2\}$. We define a mixed strategy for S as an N-tuple $\boldsymbol{\sigma} = (\sigma_1, ..., \sigma_N)$ representing a probability distribution over $\mathcal{X}$ and therefore satisfying $\sigma_i \geq 0 \; \forall i = 1, ..., N$ and $\sum_{i=1,...,N} \sigma_i = 1$. Analogously, we define a mixed strategy for J as a 2-tuple $\boldsymbol{\eta} = (\eta_1, \eta_2)$ where η_1, with $\eta_1 \geq 0$, and $\eta_2 = 1 - \eta_1$ are a probability distribution over $\mathcal{Y}$. Once the prior probability distribution $\boldsymbol{p}$ is given, this Bayesian game can be represented in an equivalent normal form using a $N \times 2$ matrix $\boldsymbol{M} = \{m_{ij}\}$ with $i = 1, ..., N$ and $j = 1, 2$. The entry m_{ij} is the expected payoff for S when the ith and jth strategy are played by S and J, respectively, and is

$$m_{ij} = \sum_{k=1}^{|\Theta|} p_k C_{\text{tot}}\big[X_i(k), Y_j\big] \tag{11}$$

where $C_{\text{tot}}\big[X_i(k), Y_j\big]$, represents the overall network capacity when S is of type θ_k (which is chosen with probability p_k) and thus performs the action $X_i(k)$, while J plays Y_j. Thus, we can compute it through (8) and (10) as

$$C_{\text{tot}}(X_i(k), Y_j) \;=\; \begin{cases} C_1' + C_2 & \text{if } Y_j = 1 \\ C_1 + C_2' & \text{if } Y_j = 2 \end{cases} \tag{12}$$

and J's expected payoff can be also computed as $-m_{ij}$. Moreover, the expected payoff associated to a joint mixed strategy $(\boldsymbol{\sigma}, \boldsymbol{\eta})$ can be easily obtained by summing over all the entries of $\boldsymbol{M}$ and weighting them by the corresponding probabilities in $\boldsymbol{\sigma}$ and $\boldsymbol{\eta}$. By writing the original Bayesian game in this equivalent normal form allows to derive its BNEs as the saddle points of the expected payoff matrix $\mathbf{M}$.

IV. Bayesian Nash Equilibria computation

We can find the BNEs of the game thanks to von Neumann's Minimax Theorem [19], which assures that a zero-sum game has at least one Nash equilibrium, all equilbria yield the same payoffs, and the mixed strategies played at equilibrium are *maximinimizer* strategies (or, alternatively called, *security* strategies) for both players, that guarantee to maximize the payoff in the worst-case scenario of the opponent's move.

For our game, we denote one of the equivalent BNEs as $(\tilde{\boldsymbol{\sigma}}, \tilde{\boldsymbol{\eta}})$, where $\tilde{\boldsymbol{\sigma}}$ is the mixed strategy played by S and $\tilde{\boldsymbol{\eta}}$ is that played by J. We denote as v the payoff yielded by each BNE to S and we refer to it as the *value* of the game. It holds

$$\begin{aligned} v &= \max_{\tilde{\boldsymbol{\sigma}}} \min_{1 \leq j \leq 2} \sum_{i=1}^{N} \tilde{\sigma}_i m_{ij} \\ &= \min_{\tilde{\boldsymbol{\eta}}} \max_{1 \leq i \leq N} (\tilde{\eta}_1 m_{i1} + \tilde{\eta}_2 m_{i2})\,. \end{aligned} \tag{13}$$

We then look for a strategy $\tilde{\boldsymbol{\sigma}}$ such that the quantity

$$w_1 = \min_{1 \leq j \leq 2} \sum_{i=1}^{N} \tilde{\sigma}_i m_{ij} \tag{14}$$

is maximized and for a strategy $\tilde{\boldsymbol{\eta}}$ such that the quantity

$$w_2 = \max_{1 \leq i \leq N} (\tilde{\eta}_1 m_{i1} + \tilde{\eta}_2 m_{i2})\,, \tag{15}$$

is minimized. From the Minimax Theorem, we know that the resulting pair $(\tilde{\boldsymbol{\sigma}}, \tilde{\boldsymbol{\eta}})$ is a BNE and that v coincides with $w_1 = w_2$. We solve (14) and (15) by a conversion to two linear programming problems [7]. We reformulated them as

$$\begin{aligned} &\max \;\; w_1 \\ &\text{s.t.} \;\; w_1 \leq \sum_{i=1}^{N} \sigma_i m_{i1}\,, \quad w_1 \leq \sum_{i=1}^{N} \sigma_i m_{i2} \\ &\qquad \sigma_i \geq 0 \quad \forall i = 1, \ldots, N\,, \quad \sum_{i=1}^{N} \sigma_i = 1 \end{aligned} \tag{16}$$

and

$$\begin{aligned} &\min \;\; w_2 \\ &\text{s.t.} \;\; w_2 \geq \eta_1 m_{11} + \eta_2 m_{12} \\ &\qquad \vdots \\ &\qquad w_2 \geq \eta_1 m_{N1} + \eta_2 m_{N2} \\ &\qquad \eta_1 \geq 0,\; \eta_2 \geq 0,\; \eta_1 + \eta_2 = 1 \end{aligned} \tag{17}$$

We use the simplex algorithm [20] to get the solutions corresponding to different values of the prior probability distribution $\boldsymbol{p}$ and of the distance d_{J}. Since we are interested in establishing if $(\tilde{\boldsymbol{\sigma}}, \tilde{\boldsymbol{\eta}})$ is a mixed or pure joint strategy, we compute the `maximin` and the `minimax` in pure strategies and compare the corresponding payoffs with the payoff at BNE.

V. Numerical Results

We consider the scenario where S_1, S_2, and J communicate with constant power $P_{\text{S}} = P_{\text{J}} = 95$ dB re μPa and evaluate the performance of the network with d_{J} ranging from 0.01 to 6 km. S_1 and S_2 share a common spectrum of bandwidth 10-40 kHz, divided into 2 channels ($\mathcal{B}_1$ and $\mathcal{B}_2$) of 15 kHz. Moreover, $\mathcal{B}_1$ operates over $[10, 25]$ kHz and $\mathcal{B}_2 = [25, 40]$ kHz. Noise and attenuation over these channels can be determined through what discussed in Section II. This results in the following noise terms for the two channels:

$$\begin{aligned} N_1 &= \int_{\mathcal{B}_1} N(f) \mathrm{d}f = 37.44 \text{ dB re uPa}\,, \\ N_2 &= \int_{\mathcal{B}_2} N(f) \mathrm{d}f = 32.87 \text{ dB re uPa}\,. \end{aligned}$$

We set the possible positions for the sensors at 1 and 5 km. In principle, we could consider all pairs (4 alternatives)

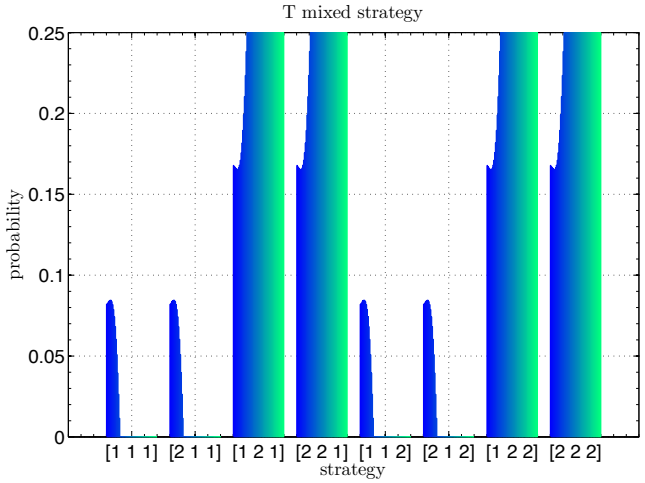

Fig. 2. S mixed strategy as a function of $d_{\text{J}} \in [0.01, 6]$ km (prior distribution for S's type: $[1/3\ 1/3\ 1/3]$).

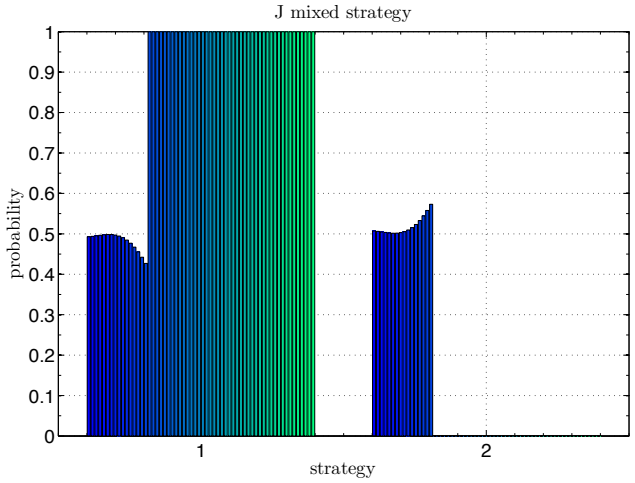

Fig. 3. J mixed strategy as a function of $d_{\text{J}} \in [0.01, 6]$ km (prior distribution for S's type: $[1/3\ 1/3\ 1/3]$).

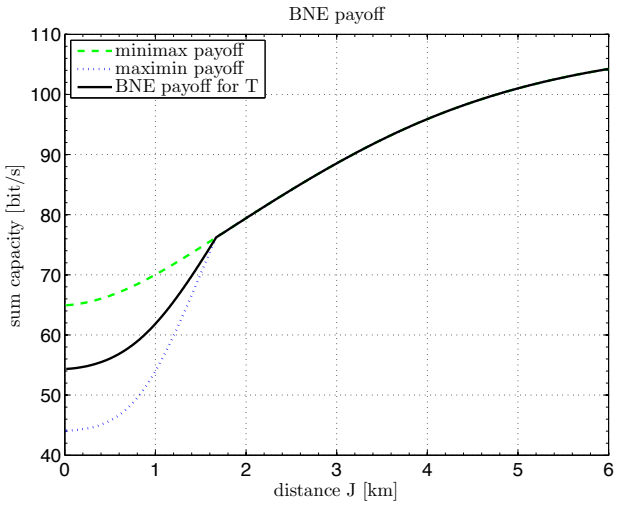

Fig. 4. BNE payoff in mixed strategies as a function of $d_{\text{J}} \in [0.01, 6]$ km (prior distribution for S's type: $[1/3\ 1/3\ 1/3]$).

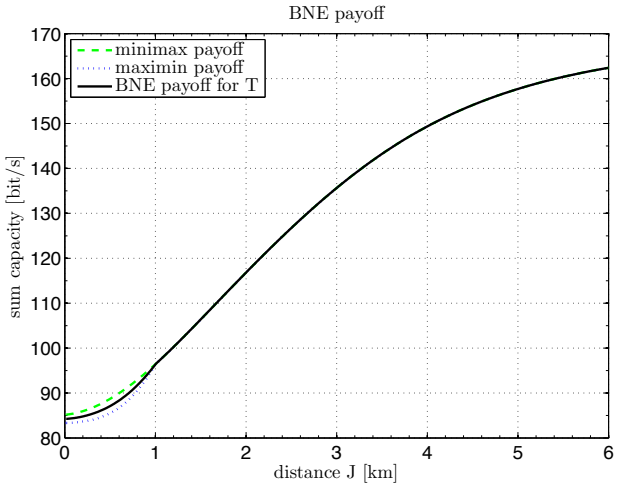

Fig. 5. BNE payoff in mixed strategies as a function of $d_{\text{J}} \in [0.01, 6]$ km (prior distribution for S's type: $[3/4\ 1/8\ 1/8]$).

to be included in Θ, but since $(1, 5)$ km and $(5, 1)$ km give the same results, we only consider $\Theta = \{(1, 1), (1, 5), (5, 5)\}$ km. As a consequence, each of the 8 pure strategies of S is in the form $[1\ 1\ 2]$, meaning that S assigns $\mathcal{B}_1$ to S_1 only if it is of type 1 or 2, while it assigns $\mathcal{B}_2$ to S_1 if it is of type 3.

Given this setting, we plot the BNE of the game as a function of d_{J}. Figs. 2 and 3 report the probability distribution over the BNE strategies of the players. In particular, we consider the case of a uniform prior distribution for S's type, i.e., $\boldsymbol{p} = [1/3\ \ 1/3\ \ 1/3]$. Fig. 2 shows that there exixts a *critical* distance $\tilde{d}$ for J such that the BNE strategies of S are pure strategies. In particular, S plays a mixed strategy with support given by all pure strategies in the form $[\cdot\ 2\ \cdot]$, i.e., S plays A_2 if it is of type $(1, 5)$, meaning that it assigns the closer node to the worst channel. Furthermore, S randomly plays A_1 or A_2 if it is of types $(1, 1)$ or $(5, 5)$, meaning that it is indifferent on its alternatives if the distances of the nodes are equal. Fig. 3 shows the same results from J's perspective, i.e., there exists a distance $\tilde{d}$ for J at which it disrupts communication on $\mathcal{B}_1$ with probability 1.

Fig. 4 also reports the payoff at BNE for S, quantified as the sum capacity of the network in bit/s. The BNE expected payoff for S is bound by the `maximin`'s payoff and the `minimax`'s payoff in pure strategies, computed as the maximum of the minima and the minimum of the maxima over rows and columns of $\boldsymbol{M}$. According to the previous performance analysis, the three curves converge at $\tilde{d}$ for J and then coincide for $d_{\text{J}} \geq \tilde{d}$. In this region the sensor network behaves almost independently of the jammer's action, and vice versa. According to Fig. 4, the Bayesian game is uncertain of its outcome at the equilibrium only when $d_{\text{J}} \leq 1.68$ km, i.e. only when the jammer is close to the receiver but not as close as the sensor node with the minimum distance.

Then, in Fig. 5 we consider a different configuration of the network, with a non-uniform prior distribution for S's type, such as $\boldsymbol{p} = [3/4\ 1/8\ 1/8]$. Note that in this configuration the transmitting sensor nodes are more likely to be close to the sink node and located at the same distance (this is also known to the jammer). The figure shows the BNE payoff for S,

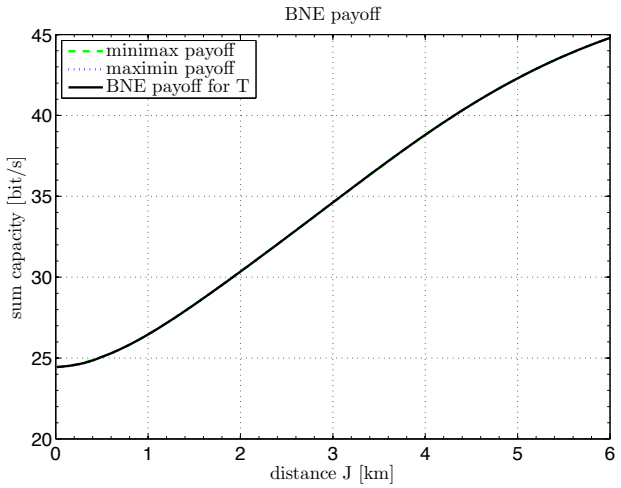

Fig. 6. BNE payoff in mixed strategies as a function of $d_{\mathrm{J}} \in [0.01, 6]$ km (prior distribution for S's type: $[1/8\ \ 1/8\ \ 3/4]$).

together with the `maximin`'s payoff and the `minimax`'s payoff in pure strategies. The performance is similar to the previous case, i.e., the three curves converge if d_{J} is greater than $\tilde{d}$, but this time such a value is even smaller than before, since $\tilde{d} = 1.01$ km. Moreover, the `maximin` and `minimax` bounds are tighter, thus the situation resembles a quasi-pure strategy case regardless of d_{J}.

In Fig. 6, we consider another non-uniform prior distribution for S's type, $\boldsymbol{p} = [1/8\ \ 1/8\ \ 3/4]$. In this case, the BNE payoff for S, the `maximin`'s bound, and `minimax`'s bound coincide for every d_{J} ranging from 0.01 to 6 km. Thus, if transmitting sensor nodes are likely to be far from the sink node, then S's strategy is always independent of d_{J}. Intuitively, in this case the jammer will always disrupt communication on the better channel, i.e. $\mathcal{B}_1$. This does not mean that the jammer has no impact, as it can be noticed that the achieved capacity is much lower than what achieved in the previous cases (Figs. 4 and 5). However, the network performance is more predictable. Also, in this case the sensor network actually knows that there is a jammer; however, in reality it would be actually difficult to detect it in such a scenario, since its actions would be identical to a higher noise (e.g., due to a more intense shipping or wind noise) on channel $\mathcal{B}_1$.

VI. Conclusions

We formulated a Bayesian zero-sum game for a jamming problem in an underwater sensor network, where we especially investigated the role played by the positions of the nodes. The sensor network is characterized by a Bayesian type, corresponding to the actual placement of the nodes among the candidate positions, and we considered a variable distance d_{J} of the jammer from the intended receiver.

We computed the BNEs and the value of the game, and we investigated their dependence on d_{J}. In many cases, it is found that there is a unique BNE where the jammer adopts a pure strategy; thus, the gameplay of the jammer is transparent to the sensor network, which simply sees a decrease in the transmission capacity, without any variability. In this sense, the sensor network may not be significantly affected by the jammer (even though the capacity indeed decreases), and it might even not notice that an attacker is there. Conversely, there are cases where the jammer is placed in a certain position and, as a result, plays a mixed strategy at the equilibrium. These positions give to the jammer a better capability of effectively disturb the network communication, and therefore should be carefully monitored.

Future work beyond the present paper will extend the analysis by also considering uncertainty in the jammer position, so as to deepen the game theoretic interaction between the players. Especially, preliminary results seem to suggest that in this setup the equilibrium strategies pool more frequently towards pure actions, and therefore the positions where a jammer can effectively threaten the network communication are further reduced. A more elaborate game theoretic analysis can be performed to fully characterize this scenario as well.

References

[1] J. Heidemann, W. Ye, J. Wills, A. Syed, and Y. Li, "Research challenges and applications for underwater sensor networking," Proc. IEEE WCNC, pp. 228–235, Las Vegas, NV, 3-6 Apr. 2006.

[2] S. Misra, S. Dash, M. Khatua, A.V. Vasilakos and M.S. Obaidat, *Jamming in underwater sensor networks: detection and mitigation*, IET Communications, 2012, Vol. 6, Iss. 14, pp. 21782188 www.ietdl.org.

[3] A. B. MacKenzie, L. A. DaSilva. *Game theory for wireless engineers*. Morgan & Claypool Publishers, 2006.

[4] M. Felegyhazi, J.-P. Hubaux, "Game theory in wireless networks: A tutorial," no. LCA-REPORT-2006-002, 2006.

[5] A. Kashyap, T. Başar, and R. Srikant, "Correlated jamming on MIMO Gaussian fading channels," *IEEE Trans. Inf. Th.*, vol. 50, no. 9, pp. 2119–2123, Sep. 2004.

[6] M. Zuba, Z. Shi, Z. Peng, J.-H. Cui, "Launching denial-of-service jamming attacks in underwater sensor networks," *Proc. ACM WUWNet*, article no. 12, Seattle, WA, Dec. 1–2, 2011.

[7] M. J. Osborne and A. Rubinstein. *A course in game theory*. MIT press, 1994.

[8] X. Xu, K. Gao, X. Zheng, I. Zhao, "A zero-sum game theoretic framework for jamming detection and avoidance In wireless sensor networks," *Proc. IEEE CSIP*, 2012.

[9] S. Tadelis, *Game theory: an introduction*. Princeton University Press, 2013.

[10] M. Stojanovic, "Recent advances in high-speed underwater acoustic communications," *IEEE J. Ocean. Eng.*, vol. 21, no. 2, pp. 125–136, Apr. 1996.

[11] L. Badia, M. Mastrogiovanni, C. Petrioli, S. Stefanakos, and M. Zorzi, "An optimization framework for joint sensor deployment, link scheduling and routing in underwater sensor networks," *ACM SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 11, no. 4, pp. 44-56, Oct. 2007.

[12] N. Baldo, P. Casari, and M. Zorzi, "Cognitive spectrum access for underwater acoustic communications," *Proc. IEEE ICC Workshops*, pp. 518–523, Beijing, PRC, 19–23 May 2008.

[13] R. Urick, *Principles of Underwater Sound.* McGraw-Hill, 1983.

[14] G. L. Stüber, *Principles of mobile communication*. Springer Science & Business Media, 2011.

[15] J. Partan, J. Kurose, B. N. Levine, and J. Preisig, "Low spreading loss in underwater acoustic networks reduces RTS/CTS effectiveness," *Proc. ACM WUWNet*, article no. 5, Seattle, WA, Dec. 1–2, 2011.

[16] L. Berkhovskikh and Y. Lysanov, *Fundamentals of Ocean Acoustics.* New York: Springer, 1982.

[17] M. Stojanovic, "On the relationship between capacity and distance in an underwater acoustic communication channel," *Proc. ACM WUWNet*, Los Angeles, CA, Sept. 2006, pp. 41–47.

[18] H. F. Bezdek, "Pressure dependence of the acoustic relaxation frequency associated with MgSO4 in the ocean," *J. Acoust. Soc. Am.*, vol. 54, no. 1062, 1973.

[19] J. von Neumann, "Zur Theorie der Gesellschaftsspiele," *Math. Annalen*, vol. 100 pp. 295–320, 1928.

[20] S. J. Wright and J. Nocedal. *Numerical optimization*. Vol. 2, Springer, New York, 1999.