Jamming Games in Underwater Sensor Networks with Reinforcement Learning

Liang Xiao*, Qiangda Li*, Tianhua Chen*, En Cheng†, Huaiyu Dai‡

* Dept. Communication Engineering, Xiamen Univ., 361005 China. Email: lxiao@xmu.edu.cn
†Key Laboratory of Underwater Acoustic Communication and Marine Information Technology (Xiamen University), Ministry of Education, P.R.C Xiamen 361005, China. Email: chengen@xmu.edu.cn
‡Dept. ECE, North Carolina State University, Raleigh, NC 27695, USA. Email: Huaiyu_Dai@ncsu.edu

***Abstract*—Jamming attacks that can further lead to denial of service attacks have thrown serious threats to underwater sensor networks (UWSNs). However, due to the narrow bandwidth of underwater acoustic signals and time variant propagation environments, jamming in UWSNs cannot be fully addressed by spread spectrum techniques, one type of widely-used anti-jamming methods in wireless networks for decades. In this work, we investigate jamming attacks in underwater sensor networks. More specifically, the interactions between the underwater sensors and jammers in UWSNs are formulated as an underwater jamming game, in which the players choose their transmit power levels to maximize their individual utilities based on the signal to interference plus noise ratio of the legal signals and transmission costs. The Nash equilibrium (NE) of a static jamming game is presented in a closed-form expression for the jamming scenario with known acoustic channel gains. For the dynamic and unknown underwater environments, we propose a reinforcement learning-based anti-jamming method for UWSNs, in which each sensor chooses its transmit power without knowing the channel gain of the jammers. Simulations are performed to evaluate the NE in the static jamming game in underwater sensor networks and to validate the efficacy of the proposed anti-jamming power control scheme against jamming in dynamic environments.**

***Keywords*: Jamming, underwater sensor networks, reinforcement learning, game theory**

I. INTRODUCTION

With the development of underwater sensor networks (UWSNs), in which low-cost sensors utilize acoustic communication links at low frequencies to report their sensing data to a surface sink or station, it is critical to investigate the security issue of UWSNs [1]. In particular, jammers carried out by underwater vehicles or insider attackers send acoustic signals with the goal to interrupt the ongoing data collections and deplete sensor batteries, further leading to denial-of-service attacks in UWSNs [2], [3]. Carrying environmental monitoring information of lakes, rivers and seas, sensors in UWSNs have to address jamming attacks to ensure a reliable and secure monitoring services [4], [5].

The work of L. Xiao was supported in part by NSFC (No.61271242,61471308), and 863 high technology plan (Grant No. 2015AA01A707). The work of E. Cheng was supported in part by NSFC (No.61471308). The work of H. Dai was supported in part by the US National Science Foundation under Grants CNS-1016260, ECCS-1307949 and EARS-1444009.

Due to the severe attenuations, large delay, severe multipath and low frequency of underwater acoustic channels, and the power constraints of underwater sensors, acoustic sensor networks are more vulnerable to jamming attacks than the counterparts in indoor wireless networks. More specifically, underwater sensor networks have difficulty fully addressing jamming by applying spread spectrum techniques, such as frequency hopping, that have been widely used for decades to counteract jammers in wideband radio networks [6], because underwater sensors operate at low frequencies and thus have very narrow bandwidths. Moreover, due to the mobility of sensors and jammers in dynamic underwater environments, it is challenging for sensors to detect and locate jammers in UWSNs. This has motivated research on jamming in UWSNs [7].

Game theory and reinforcement learning techniques have shown significant strength to study the interactions between jammers and radio nodes in wireless networks [8], [9]. Therefore, in this paper, we perform game theoretic study on jamming attacks in underwater sensor networks. More specifically, the interactions between sensors and jammers in UWSNs are formulated as a jamming game. Each sensor chooses its transmit power in the presence of jamming signals to maximize its utility based on the signal to interference plus noise ratio (SINR) of the legal signals at the surface sink and the transmission costs. The Nash equilibrium (NE) of a static jamming game is presented for the jamming scenario, in which each player knows the channel gains of the acoustic signals. We analyze the performance of the NE via simulations in terms of the distance between the jammer and the surface sink. For the dynamic underwater environment in which the sensors and jammers move with random velocities and directions over time, we propose an anti-jamming power control strategy for a sensor in UWSNs to choose its transmit power without knowing the channel gain between the jammer and the surface sink. Simulations are performed on the underwater channel models generated by BELLHOP [10] to evaluate the performance of the proposed scheme against jamming.

The main contributions of the paper include:

1) We extend game theoretic study on jamming to underwater sensor networks and derive a closed-form expression of

the NE in the static jamming game in UWSNs.

2) We propose a learning-based power control strategy for underwater sensors to address jamming attacks with unknown channel parameters of the attacker in dynamic underwater sensor networks.

3) We analyze the impact of the initial distance between the jammer and the surface sink on the performance of UWSNs.

The remainder of the paper is organized as follows. We review related work in Section II and present the system model in Section III. We formulate both a static jamming game for UWSNs and a dynamic jamming game for a repeated jamming process in Section IV. We propose an anti-jamming power allocation strategy based on learning in Section V. We provide simulation results in Section VI and conclude in Section VII.

II. Related Work

Recently, there are increasing research attentions on the security issue of underwater networks. For instance, in [11], a secure communication suite was proposed for cluster-based underwater surveillance network to address known attacks. In [1], location spoofing was investigated for the geographic routing protocol in underwater acoustic networks. The Sybil detection was studied based on state information of nodes in [12]. Multipath routing in underwater acoustic networks with intruder detection was presented in [7]. Denial-of-service attacks based on wormhole tunneling and jam-and-replay in UWSNs was analyzed in [13].

Similar to indoor wireless networks, underwater sensor networks are especially vulnerable to jamming attacks. Therefore, the detection of reactive jamming was investigated in [14]. In [14], a partial-packet monitoring scheme was proposed to detect corrupted bits. An underwater jamming detection protocol was designed for UWSNs in [3]. Field tests were performed to analyze jamming models in UWSNs in [2], [15]. However, to the best of our knowledge, none of the existing work has applied game theory to improve the anti-jamming performance of underwater networks.

III. System model

A. Underwater Sensor Network Model

In this work, we consider an underwater sensor network that consists of N underwater sensors, a jammer and a surface station or sink, all located randomly. The surface sink collects sensing data sent by the sensors over the underwater acoustic channels at a frequency f_0. Carrier sense multiple access (CSMA) is assumed for the resource allocation in the network, in which at most one sensor is allowed to send its sensing data in a time slot denoted by the integer $k \geq 1$.

Without loss of generality, sensor i chooses the transmit power of its acoustic signal at time k, denoted by $x_i^{(k)}$, with $0 \leq x_i^{(k)} \leq P_i$, where P_i is the maximum transmit power of the sensor, $\forall 1 \leq i \leq N$. For simplicity, the time index k and the sensor index i are omitted, if no confusion occurs. The distance between sensor i and the surface sink is denoted by d_i and the resulting channel power gain is denoted by h_i. The transmission cost of sensor i, denoted by C_i, depends on the battery level of the sensor.

B. Jamming model

A jammer is assumed to send acoustic signals at the same frequency with the sensors in order to block the sensing reports and deplete the sensor batteries of the underwater sensor network. Reactive jammers choose their jamming power levels based on the ongoing transmission of the sensors and are more powerful than non-responsive jammers such as constant jammers. Therefore, in this work, we consider a reactive jammer and the conclusions can be viewed as a lower bound of the anti-jamming performance of UWSNs.

At time k, the jammer chooses its jamming power, denoted by $y^{(k)} \geq 0$, with the unit cost of jamming power denoted by C_J. The distance between the jammer and the surface sink is denoted by d_J, while the corresponding channel power gain is denoted by h_J. If the jammer can attack the sensor network for multiple time slots, the reactive jammer is assumed to choose its jamming power based on the state of the sensor network. More specifically, the jamming power $y^{(k)}$ is chosen based on the network state defined as the SINR of the sensing report at time $k-1$. For example, the jamming power can be chosen to increase with the SINR of the signal to avoid the waste of power.

C. Underwater Channel model

According to [16], the acoustic path loss between sensor i and the surface sink is given by

$$A(d_i, f) = h_0 d_i^{\gamma} a(f)^{d_i}, \tag{1}$$

where the path loss exponent $\gamma = 2$ for spherical spreading, h_0 is the reference path loss, and $a(f)$ is the absorption coefficient. Based on the Thorp's formula, we have

$$a(f) = 10^{0.011\frac{f^2}{1+f^2}+4.4\frac{f^2}{4100+f^2}+2.75\times10^{-5}f^2+3\times10^{-4}}, \tag{2}$$

where f is the frequency of the acoustic signal.

The channel transfer function with N_p paths each of length l_m, $0 \leq m \leq N_p - 1$ is given by

$$H(f) = \sum_{m=0}^{N_p-1} \frac{\Gamma_m}{\sqrt{A(l_m, f)}} e^{-j2\pi f l_m / c}, \tag{3}$$

where the nominal underwater sound speed $c = 1500$ mps and Γ_m is the additional loss on the m-th path. According to [16], the noise power at the surface sink, denoted by σ, is given by

$$\sigma = \Delta f \frac{10^5}{f^{1.8}}, \tag{4}$$

where Δf is the bandwidth of the acoustic signal. The transition probability for the channel gain of sensor i to change from $h_i^{(k-1)}$ to $h_i^{(k)}$ during a time slot due to the sensor mobility and water movements is denoted with $p_h(h_i^{(k)}|h_i^{(k-1)}) \in [0, 1]$. The channel attenuation $H(f)$ can be obtained by a software called BELLHOP [10] that has been widely used to study underwater communications.

IV. Jamming Game in Underwater Sensor Networks

The interactions between a jammer and underwater sensors are formulated as a jamming game, in which each sensor chooses its transmit power while the jammer determines its jamming power, denoted by $y^{(k)}$. We first analyze a one-shot interaction between the jammer and a sensor that is allowed to transmit in a single time slot as a static game, and then investigate the repeated interactions between the jammer and the sensor network over a long time duration as a dynamic jamming game.

A. Static jamming game

Without loss of generality, we consider the power control of the jammer and sensor i that obtains the transmission right at time slot k, with $1 \leq i \leq N$. The static jamming game, denoted by $\mathbf{G}$, consists of two players: the sensor chooses its action under the power constraint, i.e., $x_i \in [0, P_i]$, while the jammer determines its non-negative power, $y \geq 0$. Both players are assumed to know the channel gains in this time slot (i.e., h_i and h_J) and the transmission costs of each other (i.e., C_i and C_J).

The sensor and the jammer simultaneously choose their actions, x_i and y to maximize their individual instantaneous utilities at the time slot, denoted by u_x and u_J, respectively. In the game, the sensor aims to obtain a higher SINR with a minimum transmission cost. Thus the utility of the sensor in this static game is defined as the following,

$$u_i(x_i, y) = \frac{h_i x_i}{\sigma + h_J y} - C_i x_i. \tag{5}$$

As the goal of the jammer is to block the ongoing transmission and to deplete the sensor's battery, the utility of the jammer is defined as

$$u_J(x_i, y) = -u_i - C_J y = -\frac{h_i x_i}{\sigma + h_J y} + C_i x_i - C_J y. \tag{6}$$

Unlike the zero-sum game as in [9], we assume that the jammer aims to increase the energy consumption of the sensor in this game.

The Nash equilibrium of the game is denoted by (x^*, y^*), in which each player chooses its best response to maximize its utility given that its opponent takes the NE strategy. Thus we have

$$x^* = \arg\max_{0 \leq x \leq P_i} u_i(x, y^*) \tag{7}$$

$$y^* = \arg\max_{0 \leq y} u_y(x^*, y). \tag{8}$$

If each player knows the channel parameters and transmission costs, the optimal power control strategy is given by the following:

Theorem 1. *The static jamming game* $\mathbf{G}$ *has a unique Nash equilibrium, which is given by*

$$(x^*, y^*) = \begin{cases} \left(P_i, \frac{1}{h_J}\left(\sqrt{\frac{h_i h_J P_i}{C_J}} - \sigma\right)\right), & I_1 \\ (P_i, 0), & I_2 \\ (0, 0), & o.w. \end{cases}, \tag{9}$$

with the condition I_1*:* $C_i < \frac{h_i}{\sigma + h_J P_J}$ *and* $C_J < \frac{h_J h_i P_i}{\sigma^2}$*; and the condition* I_2*:* $C_i < \frac{h_i}{\sigma + h_J P_J}$ *and* $C_J \geq \frac{h_J h_i P_i}{\sigma^2}$.

Proof: By (7) and (5), it is clear that $x^* = 0$ if $\partial u_i / \partial x_i = \frac{h_i}{\sigma + h_J y^*} - C_i < 0$; and $x^* = P_i$ otherwise.

Similarly, by (7) and (6), we take derivative of $u_J(x^*, y)$ with respect to y, yielding

$$\frac{\partial u_J(x^*, y)}{\partial y} = \frac{h_J h_i x^*}{(\sigma + h_J y)^2} - C_J. \tag{10}$$

Let $\frac{\partial u_J(x^*, \tilde{y})}{\partial y} = 0$, and we have

$$\tilde{y} = \left(\sqrt{\frac{h_J h_i x^*}{C_J}} - \sigma\right) / h_J. \tag{11}$$

Therefore, if condition I_1 holds, it is clear that $\partial u_i / \partial x > 0$ and $\frac{\partial u_J}{\partial y} = 0$ has a solution, thus $x^* = P_i$ and $y^* = \frac{1}{h_J}\left(\sqrt{\frac{h_i h_J P_i}{C_J}} - \sigma\right)$. Similarly, if I_2 holds, we have $\partial u_i / \partial x > 0$ and $\frac{\partial u_J}{\partial y} \leq 0$, thus $x^* = P_i$ and $y^* = 0$. ■

B. Dynamic jamming game

The repeated interactions between the underwater sensor network consisting of N sensors and a jammer over multiple time slots can be formulated as a dynamic jamming game, denoted by $\mathbf{G}'$. We assume a cooperative sensor network, in which all the sensors choose their transmit power levels to maximize the same long-term utility, denoted by U_w. Let $\delta \in [0, 1]$ denote the discount factor of the sensor network, indicating the myopic nature of the sensors.

For simplicity, Markov decision process is used to model the jamming process in the dynamic game, in which the jamming power is quantized into $S+1$ levels, i.e., the action of the jammer is given by $0 \leq y \leq S$, where S is the jamming power constraint. The state transition probability of the jammer, denoted by $p(s'|s)$, represents the probability for the jamming power to change from s at time k to s' at time $k+1$ after a time slot, with $s, s' \in \{0, 1, 2, \cdots, S\}$.

In this game, the channel gain of the acoustic signal sent by the sensor chosen by CSMA can be modeled with a Markov chain. More specifically, the probability for the channel gain to change from h_i at time k to h' at time $k+1$ is denoted with $p_h(h'|h_i)$, resulting from the change of the sensor and the Doppler shift due to the mobility of the sensors and environment.

According to the instantaneous utility given by (5), we can write the long-term utility of sensor i at time k in this game as

$$\begin{aligned} U_w(x, y) &= u_i(x, y) + \delta \sum_{y'=0}^{S} p(y'|y) \max_{0 \leq x' \leq P_i} U_w(x', s') \\ &= \left(\frac{h_i}{\sigma + h_J y} - C_i\right) x \\ &+ \delta \sum_{y'=0}^{S} \sum_{h'} p(y'|y) p_h(h'|h_i) \max_{0 \leq x' \leq P_i} \left(\frac{h'}{\sigma + h_J y'} - C_i\right) x', \end{aligned} \tag{12}$$

where the first term is the instantaneous utility of the sensor at time k while the second term represents the expected utility that the sensor network obtains in the next time slot.

V. Learning-based Power Control for UWSNs

In dynamic underwater environments in which sensors and jammers float randomly over time, it is impractical for all the sensors to accurately estimate system parameters such as the channel gain between the jammer and the surface sink. Thus it is challenging for an underwater sensor to calculate its optimal transmit power at the equilibrium of a dynamic jamming game. To address this problem, we apply the reinforcement learning technique in the power control of underwater sensor networks, in which each sensor achieves its optimal power allocation strategy by learning from the history.

Without loss of generality, we assume that sensor i is chosen by CSMA to send its sensing report at time k. The state of the sensor network at time k, denoted by $\mathbf{s}^{(k)}$, is defined as $\mathbf{s}^{(k)} = [i, h_i, y^{(k-1)}]$, consisting of the index of the selected sensor, the channel gain between the sensor and the surface sink (h_i) and the jamming power at time $k-1$ ($y^{(k-1)} \in \{0, 1, 2, ..., S\}$). The instantaneous utility of the sensor network, denoted by u_N, equals u_i as in Eq. (5) at time k. Thus we have

$$u_N(x, \mathbf{s}^{(k)}) = \frac{h_i x}{\sigma + h_J y} - C_i x. \tag{13}$$

As it is challenging for the sensors to derive the closed-form expression of the optimal power control strategy, we apply Q-learning algorithm, with the learning rate of the sensor network denoted by $\alpha \in (0, 1]$. Let $Q(\mathbf{s}, x)$ denote the Q function for the state $\mathbf{s}$ and the transmit power x, where the transmit power x is quantified into L levels, i.e., $x \in \mathbf{P} = \{0, 1, 2, ..., L\}$, and $V(\mathbf{s})$ be the highest value of the state. The sensor updates its Q function by the following:

$$Q\left(\mathbf{s}^{(k)}, x^{(k)}\right) = (1-\alpha) Q\left(\mathbf{s}^{(k)}, x^{(k)}\right) + \alpha\left(u_N\left(x^{(k)}, y^{(k)}\right) + \delta V\left(\mathbf{s}^{(k+1)}\right)\right) \tag{14}$$

$$V\left(\mathbf{s}^{(k)}\right) = \max_x Q\left(\mathbf{s}^{(k)}, x\right). \tag{15}$$

Assuming that the sensor network applies the ϵ-greedy policy in the power control, we have the transmit power of sensor k at time k given by the following probability distribution,

$$Pr\left(x^{(k)} = \tau\right) = \begin{cases} 1-\epsilon, & \tau = \arg\max_{x' \in \mathbf{P}} Q\left(\mathbf{s}^{(k)}, x'\right) \\ \frac{\epsilon}{|\mathbf{P}|-1}, & \text{o.w.} \end{cases}, \tag{16}$$

where $|\mathbf{P}|$ is the size of the set $\mathbf{P}$. The power control process of the sensor network is summarized in Algorithm 1.

Algorithm 1. Power control of a sensor network.

Set $\delta = 0.8$, $\alpha = 0.1$.
Initialize $Q(\mathbf{s}, x) = 0$, $V(\mathbf{s}) = 0$, $\forall \mathbf{s}, x$.
Repeat (for each episode)
  Observe the initial system states $\mathbf{s}^{(1)}$;
  For $k = 1, 2, 3, \cdots$
    Select and perform an action $x^{(k)} \in \mathbf{P}$ via (16);
    Observe the subsequent state $\mathbf{s}^{(k+1)}$ and immediate payoff u_s;
    Update $Q(\mathbf{s}^{(k)}, x^{(k)})$ via (14);
    Update $V\left(\mathbf{s}^{(k)}\right)$ via (15);
  End for
End for

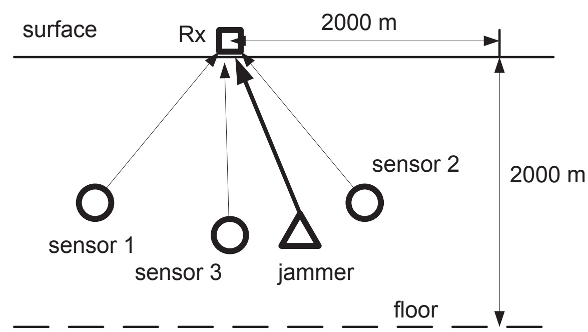


Fig. 1. Topology of an underwater sensor network against a jammer.

VI. Simulation Results

In the simulation, we evaluated the performance of the underwater sensor networks based on CSMA, with $N = 3$, $C_i = 0.03$, $C_J = 0.02$, $\sigma = 0.1$ and $f_0 = 10$ kHz. The network topology is shown in Fig. 1, in which the depth of the lake was 2000 m, the surface sink was located at $(0, 0, 0)$ m, the sensors were located at $(-1000, 0, 1100)$ m, $(1000, 0, 1100)$ m, and $(0, 0, 1300)$ m, respectively, and the location of the jammer was $(500, 0, 1300)$ m. All the sensors and the jammer moved $\Delta = 0.3$ m in randomly chosen directions in each time slot.

The sensor utility at the NE of the static jamming game consisting of a sensor and a jammer, with the distance between the sensor and the surface sink $d_S = 1.5$ km, the maximum transmit (jamming) power $P_S = 10$ ($P_J = 10$), is shown in Fig. 2. It is shown that the utility of the sensor increases with the distance d_J, while the utility of the jammer decreases with it, because a larger jamming distance indicates a weaker jamming strength. The utility of the sensor with $C_J = 0.03$ is higher than that with $C_J = 0.02$ for $C_S = 0.03$, because the jammer is less likely to attack under a higher jamming cost.

To evaluate the performance of proposed power control strategy, we also evaluated a fixed power strategy and a random strategy. The jammer in the simulations observed the power of the sensor in the previous time slot and chose its jamming power to maximize its immediate utility, with $P_J = P_i = [1, 3, \cdots, 9]$ for $i = 1, 2, 3$. As shown in Fig. 3 (a), each sensor's utility gradually converges to the optimal value, while the jammer's utility decreases over time. Each sensor achieves different utility due to the different channel conditions. Fig. 3 (b) indicates that the proposed power control strategy improves the utility of each sensor compared with the fixed and random strategies.

The impact of the distance d_J on the performance of the proposed scheme is shown in Fig. 4, with $d_J = [1, 1.1, \cdots, 2]$ km, indicating that the utility of the sensor increases with d_J,

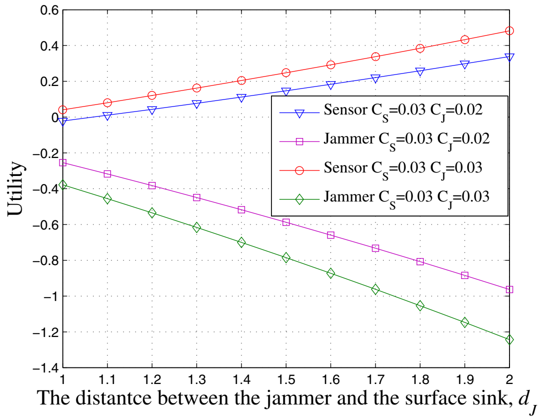
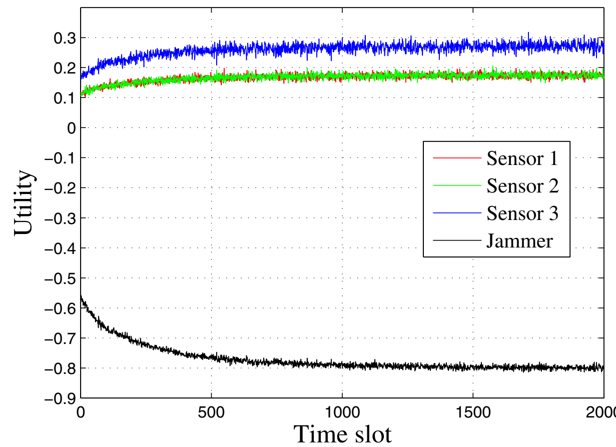


Fig. 2. Performance of the NE in the static jamming game versus the distance between the jammer and the surface sink, d_J.

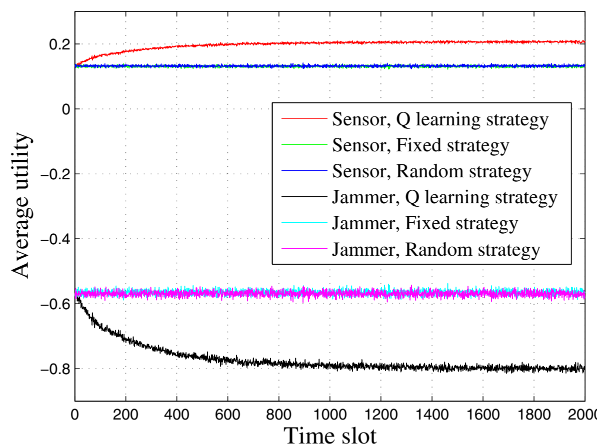
while the utility of the jammer decreases with it. In addition, the average SINR of the signal increases with the increase of d_J, which corresponds to a weaker jammer.

VII. Conclusion

We have formulated the interactions between an underwater sensor network and a reactive jammer as two jamming games. The NE of a static jamming game has been derived for the one-shot jamming scenarios with known channel gains and transmission costs. We have also proposed a power control strategy based on Q-learning for the sensor networks in dynamic underwater environments with unknown system parameters such as the channel gain between the jammer and the surface sink. Simulations have been performed under underwater acoustic channels, showing the efficacy of the proposed anti-jamming power control strategy.



(a) Utility of each sensor.



(b) Average utility.

Fig. 3. Performance of the proposed power control strategy in a dynamic jamming scenario over time.

References

[1] M. Zuba, M. Fagan, J.-H. Cui, and Z. Shi, "A vulnerability study of geographic routing in Underwater Acoustic Networks," in *Proc. IEEE Conference on Communications and Network Security (CNS)*, 2013, pp. 109–117.

[2] M. Zuba, Z. Shi, Z. Peng, and J.-H. Cui, "Short Paper: Launching Denial-of-Service Jamming Attacks in Underwater Sensor Networks," *The International Conference on UnderWater Networks and Systems (WUWNet)*, vol. 11, pp. 978–1, 2011.

[3] S. Misra, S. Dash, M. Khatua, A. V. Vasilakos, and M. S. Obaidat, "Jamming in underwater sensor networks: detection and mitigation," *IET communications*, vol. 6, no. 14, pp. 2178–2188, 2012.

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

[5] I. Akyildiz, D. Pompili, and T. Melodia, "Underwater acoustic sensor networks: research challenges," *Ad hoc networks*, vol. 3, no. 3, pp. 257–279, 2005.

[6] L. Xiao, H. Dai, and P. Ning, "Jamming-resistant collaborative broadcast using uncoordinated frequency hopping," *IEEE Trans. Inform. Forensics and Security*, vol. 7, pp. 297 – 309, Feb. 2011.

[7] M. Goetz, S. Azad, P. Casari, I. Nissen, and M. Zorzi, "Jamming-resistant multi-path routing for reliable intruder detection in underwater networks," in *Proc. ACM International Workshop on Underwater Networks (WUWNet)*, December 2011.

[8] L. Xiao, Y. Chen, W.S. Lin, and K.J.R. Liu, "Indirect reciprocity security game for large-scale mobile wireless networks," *IEEE Trans. Inform. Forensics and Security*, vol. 7, pp. 1368 – 1380, Aug. 2012.

[9] D. Yang, G. Xue, J. Zhang, A. Richa, and X. Fang, "Coping with a smart jammer in wireless networks: A stackelberg game approach," *IEEE Trans. Wireless Commun.*, vol. 12, no. 8, pp. 4038 – 4047, 2013.

[10] Michael B Porter, "The bellhop manual and users guide: Preliminary draft," *Heat, Light, and Sound Research, Inc., La Jolla, CA, USA, Tech. Rep*, 2011.

[11] M. Islam, S. Azad, M. Morshed, and et. al., "A secure communication suite for cluster-based Underwater Surveillance Networks," in *Proc. International Conference on Electrical Engineering and Information & Communication Technology*, 2014, pp. 1–5.

[12] A. Qian L. Shu X. Li, G. Han and J. Rodrigues, "Detecting Sybil attack based on state information in Underwater Wireless Sensor Networks," in *Proc. IEEE,International Conference on, Software, Telecommunications and Computer Networks (SoftCOM)*, 2013, pp. 1–5.

[13] J. Kong, Z. Ji, W. Wang, and et. al., "Low-cost attacks against packet delivery, localization and time synchronization services in under-water sensor networks," in *Proc. ACM workshop on Wireless security*, 2005, pp. 87–96.

[14] M. Khatua and S. Misra, "Exploiting partial-packet information for reactive jamming detection: studies in UWSN environment," in *Proc. Springer Distributed Computing and Networking*, pp. 118–132. 2013.

[15] M. Zuba, Z. Shi, Z. Peng, J.-H. Cui, and S. Zhou, "Vulnerabilities of underwater acoustic networks to denial-of-service jamming attacks," *Security and Communication Networks*, 2012.

[16] Milica Stojanovic, "On the relationship between capacity and distance

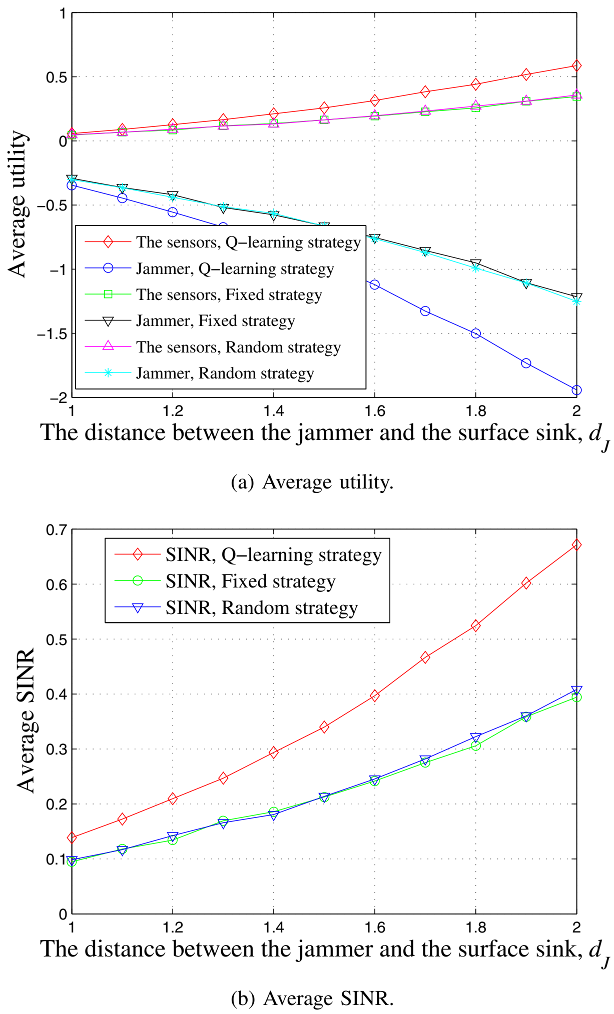


Fig. 4. Performance of the power control strategy versus the distance between the jammer and the surface sink, d_J.

in an underwater acoustic communication channel," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 11, no. 4, pp. 34–43, 2007.