Securing Underwater Acoustic Communications through Analog Network Coding

Hovannes Kulhandjian[†], Tommaso Melodia[†], and Dimitrios Koutsonikolas[‡]

[†]Department of Electrical Engineering
[‡]Department of Computer Science and Engineering
State University of New York at Buffalo, Buffalo, New York 14260
E-mail: {hkk2, tmelodia, dimitrio}@buffalo.edu

Abstract*—We propose a new secure underwater acoustic communication scheme designed to let a user (Alice) transmit a confidential message to another user (Bob) in the presence of an eavesdropper (Eve). A typical approach in conventional wireless physical-layer security is to rely on a friendly jammer to jam Eve through artificial noise (AN). Instead, for the first time, we propose a secure underwater communication scheme that relies on cooperative friendly jamming through CDMA-based analog network coding (ANC). The cooperative friendly jammer transmits information using the same spreading code used in the legitimate Alice-Bob link. The information transmitted by the cooperative jammer is known *a priori* to Bob, but not to Eve. Although the jammer's packet will also interfere at Bob, we show that after jointly estimating the two multipath-affected channels, Bob can suppress the interfering packet and decode Alice's packet, while Eve cannot. We also formulate the problem of joint optimal selection of friendly jammer and power allocation (for Alice and the jammer) that minimize Eve's capability of intercepting the signal while guaranteeing a predefined level of quality of service (QoS) for Bob. The proposed scheme is implemented in a testbed based on Teledyne Benthos Telesonar SM-975 underwater modems and tested extensively in Lake LaSalle at the University at Buffalo. Experiments and simulations demonstrate that, for a given energy budget, the proposed scheme can guarantee much higher bit error rate (BER) at Eve, while creating minimal BER disturbance at Bob, compared to the AN-aided approach.

I. Introduction

Underwater acoustic communications and networking have recently attracted considerable attention due to increasing interest in many undersea commercial and military applications [1], [2], [3], [4]. Although radio frequency (RF) electromagnetic and optical waves are the dominant physical communication carriers in terrestrial wireless communications, in water they are severely affected by high attenuation and scattering, respectively. Acoustic communication is therefore the transmission technology of choice for wireless underwater networked systems [1].

The underwater acoustic (UW-A) channel is considered one of the most challenging environments to establish *reliable* and *secure* communications. Some of the challenges include slow propagation of acoustic waves, limited bandwidth, and high and variable propagation delays. Furthermore, the UW-A channel is affected by Doppler spread and by severe time-varying multipath fading [1], [2].

Such a challenging environment makes reliable communications hard to achieve, and at the same time makes underwater networks prone to malicious attacks. Some security challenges in underwater networks are discussed in [5]. In this paper, we concentrate on the problem of transmitting securely a confidential message in the presence of *eavesdropping* attacks. One way to overcome eavesdropping is to apply cryptographic approaches at the upper layers of the protocol stack by encrypting data before transmission. However, cryptographic mechanisms can face potential attacks at the higher layers [6], and suffer from heavy computational complexity, especially, in resource constrained underwater acoustic sensor networks (UW-ASNs) [1], [3]. In any case, it is desirable to improve the security of the physical layer wireless channel by impairing the eavesdroppers' intercepting capabilities in the first place [7].

Physical layer security has therefore recently attracted considerable attention [8], [9], [10] due to its inherent ability to prevent eavesdropping. Although most research has focused on information theoretic approaches [11], [12], [13], the topic has drawn significant interest from the signal processing [6], [7], [14] and networking [15], [16] communities. However, very limited research only has addressed secure UW-A communications in the presence of an eavesdropper.

Among these, in [17], a direct-sequence spread-spectrum (DSSS) waveform design with low probability of interception (LPI) was proposed to provide covert UW-A communications. Similarly, in [18], a multi-carrier spread-spectrum (MCSS) modulation was proposed as a means to render covert UW-A communication at low signal-to-noise ratio (SNR). A receiver with multiband equalization was proposed to jointly equalize and despread the contiguous frequency bands carrying the same symbol stream. In [19], a multiband orthogonal frequency-division multiplexing (OFDM) transmitter and receiver were presented for secure UW-A communications at low SNR regime with the intention to avoid interception. However, those schemes may become vulnerable to eavesdropping if the adversary is able to identify the spreading code or the modulation technique used by the two parties. Direct-sequence code-division multiple-access (DS-CDMA) schemes have long been used to provide covert communications [20], [21]. However, recent work [22] has shown that DS-CDMA can become vulnerable to attacks since it is possible to blindly identify the spreading code used by the legitimate user when neither channel state information nor training sequence is available. Accordingly, it is necessary to explore alternative means to provide security at the physical layer.

In this paper, we propose a new secure UW-A commu-

Acknowledgment: This work was partially supported by the National Science Foundation under grants CNS-1055945 and CNS-1126357.

978-1-4799-4657-0/14/$31.00 © 2014 IEEE

nication scheme designed to let a user (Alice) transmit a confidential message to another user (Bob) in the presence of an eavesdropper (Eve). In the case when the adversary has a better channel quality, compared to the legitimate link, perfect secrecy (i.e., zero information leakage to the eavesdropper by listening to the source-destination message exchange) can not be achieved. To overcome this obstacle, a cooperative friendly jammer is often introduced to degrade the adversary's channel [6], [14]. A common approach frequently used by cooperative friendly jammers is to jam the eavesdropper through artificial-noise (AN) [23], [24]. Since such an approach can also degrade the channel of the legitimate user, oftentimes, an array beamforming approach using multiple antennas is utilized to design a scheme such that most of the AN jamming signal is targeted to the adversary's location, while minimizing its effects at the intended user [23], [24]. Usually, a perfect knowledge of the eavesdropper's channel condition is necessary to design such schemes [23], which may be hard to obtain or not be available altogether. Moreover, in the case when the adversary is in close proximity of the legitimate user, even a beamforming approach cannot be of much help to avoid degrading the channel of the legitimate user. Besides, beamforming requires nodes to be equipped with arrays of transducers, which can be very costly to provide in underwater sensor network deployments [1].

Therefore, for the first time, we propose a secure underwater communication scheme that, unlike previous work relying on AN-based jamming, is based on cooperative friendly jamming built upon CDMA-based analog network coding (ANC), a technique developed in our recent work [25]. The basic idea of ANC [26], also known as physical layer network coding (PNC) [27], is to allow concurrent transmissions of signals over the wireless medium so that they intentionally interfere with each other. The receiver, having heard the interfered signal from prior transmissions, will suppress the interference before decoding the desired information [25]. Prior work has used ANC as a technique to increase the network throughput. To the best of our knowledge, our work is the first to use the principle of ANC with a completely different objective, i.e., to provide covert communications in UW-A channels.

The CDMA-based ANC scheme differs from conventional DS-CDMA interference cancellation in terms of the nature of the interference signal that each scheme is designed to suppress. In conventional DS-CDMA, multiple access interference (MAI) is generated by different users utilizing unique spreading codes. Instead, in CDMA-based ANC, MAI is generated by a pair of nodes accessing the channel using the same spreading code. As a consequence, it is much more challenging to cancel the resulting interference.

The core idea of our proposed J-ANC (Jamming-through-ANC) scheme is as follows. We consider a DS-CDMA link between Alice and Bob[1]. Eve may be located closer to Alice than Bob, and thus may have a better signal/channel quality relative to Bob. To prevent Eve from intercepting Alice's packet, a cooperative friendly jammer is selected to transmit information modulated using the same spreading code assigned to the legitimate Alice-Bob link. Although we could let Alice mix the jamming signal in the digital domain (i.e., using network coding [28]) before transmission, by introducing a cooperative friendly jammer we leverage the physical properties of the wireless medium and thus make it even harder for Eve to intercept the communication, since she will have to jointly estimate the two channels and remove the jamming signal before being able to retrieve Alice's packet. The information bits transmitted by the cooperative jammer are randomly generated and are known $a\ \ priori$ to Bob, but not to Eve. Although the jammer's packet will also interfere at Bob, we show that after jointly estimating the two multipath affected channels, Bob can suppress the interfering signal and retrieve Alice's packet. Therefore, Bob will be able to decode Alice's packet, while Eve will fail to do so with high probability. We also formulate the problem of optimal selection of the friendly jammer among a set of jammers and optimal energy allocation for both Alice and the jammer, with the objective to guarantee a minimum level of signal-to-interference-plus-noise ratio (SINR) to Bob and, at the same time, degrade the SINR of Eve as much as possible.

The contributions of this paper are outlined as follows.

1) For the first time, we propose a secure underwater communication scheme that, unlike previous work relying on AN-based jamming, is based on cooperative friendly jamming built upon CDMA-based ANC. To prevent Eve from intercepting Alice's packet, a cooperative friendly jammer is selected to transmit information modulated using the same spreading code assigned to the legitimate Alice-Bob link. The information transmitted by the cooperative jammer is known $a\ \ priori$ to Bob, but not to the eavesdropper.

2) To the best of our knowledge, the case when Eve is in very close proximity of the legitimate user is not addressed adequately by the physical layer security research community. This can be justified by the fact that perfect secrecy cannot be achieved. The proposed scheme can even provide security when Eve is located nearby Bob such that she can overhear what Bob receives but will not be able to decode the message.

3) We formulate the problem of optimal selection of the friendly jammer among a set of jammers and optimal energy allocation for both Alice and the jammer, with the objective to guarantee a minimum level of SINR to Bob and at the same time, degrade the SINR of Eve as much as possible.

4) We implement J-ANC in a testbed based on Teledyne Benthos Telesonar SM-975 underwater modems and test it extensively in Lake LaSalle at the University at Buffalo. Experiments and simulations demonstrate that J-ANC is less harmful to the intended receiver and can provide higher security against an eavesdropper compared to traditional AN-aided approaches. Specifically, we show that for a given jamming energy budget, J-ANC can guarantee much higher BER at Eve, while causing minimal BER disturbance at Bob, compared to the AN-aided approach.

The rest of this paper is organized as follows. In Section II, we describe the system model with detailed discussions on joint channel estimation and receiver design for both Bob and Eve. In Section III, we address the friendly jammer selection with optimal energy allocation problem. In Section IV, we evaluate the proposed scheme. Finally, in Section V, we draw the main conclusions.

[1] CDMA is one of the most promising physical layer and multiple access techniques for UW-ASNs [1], since it is robust to frequency-selective fading and can compensate for the effect of multipath through RAKE receivers [4].

Notation: The following notation is used throughout the paper. Boldface lower-case letters indicate column vectors, boldface upper-case letters indicate matrices, $\mathbf{x}^H$ denotes the Hermitian of vector $\mathbf{x}$, $\mathbf{I}_N$ and $\mathbf{0}_N$ are the identity and zero matrices of dimensions $N \times N$ respectively, $\mathrm{tr}\{\mathbf{X}\}$ represents the trace of a matrix $\mathbf{X}$, $\mathbb{C}$ is the set of all complex numbers, $\mathbb{E}\{\cdot\}$ represents statistical expectation, $|\cdot|$ and $\|\cdot\|$ are the magnitude and the norm of a scalar and vector, respectively, $\mathfrak{Re}(\cdot)$ denotes the real part of a complex valued vector and $\mathrm{sgn}(\cdot)$ denotes zero-threshold quantization.

II. System Model and Problem Formulation

We consider a CDMA-based network shown in Fig. 1, in which Alice would like to transmit confidential information to Bob in the presence of an eavesdropper, Eve. We assume that Eve can be located closer to Alice (thus she may have a better signal/channel quality) compared to Bob, as depicted in Fig. 1. To prevent Eve from intercepting Alice's packet, we utilize a friendly jammer. Using the same DS-CDMA spreading code, Alice and the jammer concurrently transmit packets, P_A and P_J, containing independent and identically distributed (i.i.d.) bit streams, to Bob and Eve, respectively. Due to the broadcast nature of the wireless medium, both Bob and Eve will overhear the packets, P_A and P_J. We further assume that Eve has perfect knowledge of all the channel state information (CSI) (between Alice/jammer and itself) and of the spreading code utilized by Alice/jammer. In other words, we consider the worst case for Bob, but best case for Eve. The packet P_J is assumed to be known to both Alice and Bob but not to Eve. We now illustrate a technique through which Bob can successfully retrieve Alice's packet at high SNR, while Eve will fail to do so with high probability, which is our ultimate goal.

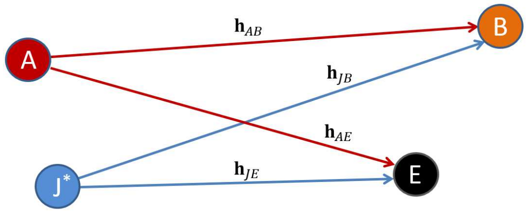


Fig. 1. System model.

Because of the highly frequency-selective distortion caused by multipath propagation in the UW-A channel, it is essential to estimate the CSI periodically [25]. Accordingly, we utilize a set of N_p pilot bits that are repeated periodically and are inserted in each packet distanced less than the coherence time, T_{CT}, of the channel. The pilot bits will be used to jointly estimate the CSIs from Alice-to-Bob and Jammer-to-Bob.

The baseband supervised and information bits transmitted by Alice and the friendly jammer are

$$\mathbf{x}_A(i) = b_A(i)\sqrt{E_A}\mathbf{s}, \qquad i = 1, 2, \dots, \tag{1}$$

$$\mathbf{x}_J(i) = b_J(i)\sqrt{E_J}\mathbf{s}, \qquad i = 1, 2, \dots, \tag{2}$$

where $\mathbf{s} \in \frac{1}{L}\{\pm 1\}^L$ denotes the normalized spreading code of length L used by Alice and the jammer, E_A and E_J denote the transmit energy per bit, $b_A(i)$, $b_J(i) \in \{-1, 1\}$ are i^{th} pilot/information bits binary phase-shift-keying (BPSK) data modulated and transmitted by Alice and the jammer, respectively. The information bits $b_k(i)$ are viewed as binary equiprobable random variables that are independent across the users ($k = A, J$) and within a user steam ($i = 1, 2, \dots$) [22].

Before transmission of the information bits, each chip of the spreading sequence is multiplied by a pulse shaping signal $p(t)$ and a carrier. The normalized modulated spreading sequence in the time domain is then denoted by

$$s(t) = \frac{1}{L}\sum_{l=1}^{L} d(l)p(t - lT_c)e^{j2\pi f_c t}, \tag{3}$$

where $d(l) \in \{-1, 1\}$ is the l^{th} transmitted chip of the spreading sequence, $T_c = T/L$ is the chip period, T is the information bit duration, and f_c is the is the carrier frequency.

We assume that packets propagate over multipath Rayleigh fading UW-A channels, which is commonly used in modeling UW-A channels [29], [30]. Without loss of generality, and for ease of exposition, we assume here that packets transmitted by Alice and the jammer experience the same number of resolvable multipaths, $M_{AB} = M_{JB} = M$, and arrive at Bob and Eve simultaneously. However, we note that the proposed scheme does not require synchronous arrival of the two packets at the relay[2], which is difficult to achieve due to long propagation delays in UW-A channel[3]. A preamble and a postamble, identical chirp signals of duration $100\,\mathrm{ms}$ sweeping the bandwidth from $10\,\mathrm{Hz}$ to $2.6\,\mathrm{kHz}$ appended to each packet, are used for channel probing, symbol synchronization for chip-matched filtering, and multipath delay spread estimation, as will be further discussed in Section IV-B.

After carrier demodulation, chip-matched filtering and sampling at the chip rate over a multipath extended bit period of $L + M - 1$ chips, where M is the number of resolvable multipaths, the received signals, $\mathbf{r}_B(i) \in \mathbb{C}^{L+M-1}$ and $\mathbf{r}_E(i) \in \mathbb{C}^{L+M-1}$ (that is, the noise-affected superimposed version of the i^{th} bits of Alice and the jammer) at Bob and Eve, respectively, are denoted by

$$\mathbf{r}_B(i) = \sqrt{E_A}\mathbf{S}_A(i)\mathbf{h}_{AB} + \sqrt{E_J}\mathbf{S}_J(i)\mathbf{h}_{JB} + \mathbf{n}_B(i), \tag{4}$$

$$\mathbf{r}_E(i) = \sqrt{E_A}\mathbf{S}_A(i)\mathbf{h}_{AE} + \sqrt{E_J}\mathbf{S}_J(i)\mathbf{h}_{JE} + \mathbf{n}_E(i), \tag{5}$$

where

$$\mathbf{h}_{AB} = [h_{AB}(1), h_{AB}(2), \dots, h_{AB}(M)]^H, \tag{6}$$

$$\mathbf{h}_{AE} = [h_{AE}(1), h_{AE}(2), \dots, h_{AE}(M)]^H, \tag{7}$$

$$\mathbf{h}_{JB} = [h_{JB}(1), h_{JB}(2), \dots, h_{JB}(M)]^H, \tag{8}$$

$$\mathbf{h}_{JE} = [h_{JE}(1), h_{JE}(2), \dots, h_{JE}(M)]^H, \tag{9}$$

are multipath channel coefficients from Alice-to-Bob, Alice-to-Eve, Jammer-to-Bob and Jammer-to-Eve of lengths M, respectively. $h_{AB}(q)$, $h_{AE}(q)$, $h_{JB}(q)$ and $h_{JE}(q)$ represent the q^{th} resolvable path coefficients modeled as quasi-static Rayleigh-distributed random variables that remain constant during T_{CT} block length, $\mathbf{n}_B$ and $\mathbf{n}_E$ are ambient noise, and

$$\mathbf{S}_A(i) \triangleq \mathbf{S}_A^0(i) + \mathbf{S}_A^+(i) + \mathbf{S}_A^-(i), \tag{10}$$

$$\mathbf{S}_J(i) \triangleq \mathbf{S}_J^0(i) + \mathbf{S}_J^+(i) + \mathbf{S}_J^-(i), \tag{11}$$

[2] Due to space constraints, we will address the asynchronous case with different number of resolvable multipath arrivals at the relay at a later time.

[3] In practice, the packet transmitted by the jammer, P_J, is slightly longer than Alice's packet, to make sure that all the bits of P_A are jammed at Eve.

where

$$\mathbf{S}_k^0(i) \triangleq b_k(i) \begin{bmatrix} s(1) & 0 & \dots & 0 \\ \vdots & s(1) & \ddots & \vdots \\ s(L) & \vdots & \ddots & 0 \\ 0 & s(L) & & s(1) \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & s(L) \end{bmatrix}_{(L+M-1)\times M}, \tag{12}$$

$$\mathbf{S}_k^+(i) \triangleq b_k(i+1) \begin{bmatrix} 0 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & & 0 & 0 \\ s(1) & \ddots & \vdots & 0 \\ \vdots & \ddots & 0 & \vdots \\ s(M-1) & \dots & s(1) & 0 \end{bmatrix}_{(L+M-1)\times M}, \tag{13}$$

$$\mathbf{S}_k^-(i) \triangleq b_k(i-1) \begin{bmatrix} 0 & s(L) & \dots & s(L-M+1) \\ \vdots & 0 & \ddots & \vdots \\ 0 & \vdots & \ddots & s(L) \\ 0 & 0 & & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{bmatrix}_{(L+M-1)\times M}. \tag{14}$$

The matrices $\mathbf{S}_k^0(i)$, $\mathbf{S}_k^+(i)$ and $\mathbf{S}_k^-(i)$ correspond to the spreading code matrices generated due to the transmission of bits $b(i)$, $b(i{+}1)$ and $b(i{-}1)$, respectively, by user $k \in \{A, J\}$, Alice or the cooperative jammer in this case.

Joint Channel Estimation at Bob. We now show how Bob can estimate the CSIs from Alice-to-Bob and Jammer-to-Bob jointly. Let us define

$$\mathbf{S}_{AJ}(i) \triangleq \left[\sqrt{E_A}\,\mathbf{S}_A(i),\ \sqrt{E_J}\,\mathbf{S}_J(i)\right]_{(L+M-1)\times 2M}, \tag{15}$$

$$\mathbf{h}_{AB,JB} \triangleq \begin{bmatrix} \mathbf{h}_{AB} \\ \mathbf{h}_{JB} \end{bmatrix}_{2M\times 1}. \tag{16}$$

We rewrite (4) in a more compact form as

$$\mathbf{r}_B(i) = \mathbf{S}_{AJ}(i)\mathbf{h}_{AB,JB} + \mathbf{n}_B(i), \qquad i = 1, 2, \dots . \tag{17}$$

Before jointly estimating the channel coefficients, $\mathbf{h}_{AB}$ and $\mathbf{h}_{JB}$, we first define the pseudo-inverse of $\mathbf{S}_{AJ}(i)$ for $(L{+}M{-}1) > 2M$ using the Moore-Penrose pseudo-inverse formula as

$$\mathbf{S}_{AJ}^{\dagger}(i) \triangleq \left[\mathbf{S}_{AJ}(i)^H \mathbf{S}_{AJ}(i)\right]^{-1} \mathbf{S}_{AJ}(i)^H. \tag{18}$$

If we assume that $\mathbf{n}_B$ is modeled as white Gaussian distributed, the conditional maximum-likelihood (ML) estimate of $\mathbf{h}_{AB,JB}$, for a given supervised bit i, can be obtained by minimizing the following squared error quantity

$$\tilde{\mathbf{h}}_{AB,JB} = \arg \min_{\mathbf{h}_{AB,JB} \in \mathbb{C}^{2M}} \|\mathbf{r}_B(i) - \mathbf{S}_{AJ}(i)\mathbf{h}_{AB,JB}\|_2^2. \tag{19}$$

Since the channel noise is assumed to follow a zero-mean Gaussian distribution, the marginal solution of (19) can be estimated by sample averaging over a data record of N_p pilot bits as

$$\hat{\mathbf{h}}_{AB,JB} = \frac{1}{N_p} \sum_{i=1}^{N_p} \mathbf{S}_{AJ}^{\dagger}(i)\, \mathbf{r}_B(i). \tag{20}$$

We can obtain an accurate estimate of $\mathbf{h}_{AB,JB}$ *if and only if* (15) is of full rank. This condition is satisfied if (15) contains at least $2M$ independent vectors. In this work, we use columns of a Sylvester-Hadamard matrix, $\mathbf{H}_L$ with elements $+1$ or -1, of order $L = 2^n$, $n = 2, 3, \dots$, as our spreading code. The Sylvester-Hadamard matrix has good autocorrelation and cross-correlation properties [31]. Rows (and columns) of the $\mathbf{H}_L$ are mutually orthogonal to each other. For a spreading code of order $L = 4$ extracted from $\mathbf{H}_L$, the above condition cannot be satisfied for $M = 3$, hence a spreading code length of $L = 8$ or longer needs to be used in this case. In practice, as we will show in Section IV, a spreading code of length at least $L = 32$ might be necessary in shallow UW-A channels.

In addition to that, it is important to select the training sequences for both nodes with very low cross-correlation properties to minimize the noise enhancement, $\mathbf{S}_{AJ}^{\dagger}(i)\mathbf{n}_B(i)$, which can be shown to be equal to $\mathrm{tr}\left\{\left[\mathbf{S}_{AJ}(i)^H\,\mathbf{S}_{AJ}(i)\right]^{-1}\right\}$ [25]. Accordingly, to minimize the noise enhancement, we utilize two orthogonal sequences of pilot bits extracted again from columns of $\mathbf{H}_L$, of order $L = 2^n$, $n = 4, 5, \dots$.

The CSIs from Alice-to-Bob and Jammer-to-Bob are then computed as

$$\hat{\mathbf{h}}_{AB} = [\mathbf{I}_M\ \mathbf{0}_M]\,\hat{\mathbf{h}}_{AB,JB}, \tag{21}$$

$$\hat{\mathbf{h}}_{JB} = [\mathbf{0}_M\ \mathbf{I}_M]\,\hat{\mathbf{h}}_{AB,JB}. \tag{22}$$

Receiver Design at Bob. To decode the information bits, Bob will use the estimated CSIs, $\hat{\mathbf{h}}_{AB}$, $\hat{\mathbf{h}}_{JB}$, and design a RAKE-matched-filter that decides on the transmitted bit of the user of interest (Alice) based on the sum of the individual M path-correlator outputs; which can be equivalently characterized by the normalized static $(L+M-1)$-tap FIR filter given by

$$\mathbf{w}_{MF_B} = \frac{\mathbf{S}_{MF}\hat{\mathbf{h}}_{AB}}{\hat{\mathbf{h}}_{AB}^H \mathbf{S}_{MF}^H \mathbf{S}_{MF}\hat{\mathbf{h}}_{AB}}, \tag{23}$$

where

$$\mathbf{S}_{MF} \triangleq \begin{bmatrix} s(1) & 0 & \dots & 0 \\ \vdots & s(1) & & \vdots \\ s(L) & \vdots & \ddots & 0 \\ 0 & s(L) & & s(1) \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & s(L) \end{bmatrix}_{(L+M-1)\times M} \tag{24}$$

represents the M path-correlator outputs, which can be constructed knowing the number of multipaths, M, which is estimated through chirp-matched filtering (Section IV-B).

Before decoding the information bits, we first cancel the inter-symbol-interference (ISI) resulting from the previously decoded bits of Alice. Moreover, we cancel the estimated interfered data bits from the jammer and, employing the RAKE-matched-filter proposed in (23), the information bits $(j = 1, 2, \dots)$ of the user of interest (Alice) are decoded as

$$\hat{b}_A(j) = \mathrm{sgn}\Big(\mathfrak{Re}\Big[\mathbf{w}_{MF_B}^H\Big(\hat{\mathbf{r}}_B(j) - \mathbf{S}_A^-(j)\hat{\mathbf{h}}_{AB} - \mathbf{S}_J(j)\hat{\mathbf{h}}_{JB}\Big)\Big]\Big), \tag{25}$$

where $\mathbf{S}_A^-(j)\hat{\mathbf{h}}_{AB}$ is the ISI of the previously decoded bit from Alice and $\mathbf{S}_J(j)\hat{\mathbf{h}}_{JB}$ is the estimate of the interfered data bit originally transmitted by the jammer.

Receiver Design at Eve. We consider the worst case scenario, that is, Eve knows all the CSIs, the number of multipath M, and the spreading code used by Alice/jammer. Before attempting to decode Alice's packet, P_A, Eve will first design a linear maximum SINR filter as

$$\mathbf{w}_{maxSINR_E} = \arg\min_{\mathbf{w}_E} \frac{\mathbb{E}\left\{\left|\mathbf{w}_E^H(\sqrt{E_A}\mathbf{S}_A(i)\mathbf{h}_{AE})\right|^2\right\}}{\mathbb{E}\left\{\left|\mathbf{w}_E^H(\sqrt{E_J}\mathbf{S}_J(i)\mathbf{h}_{JE}+\mathbf{n}_E(i))\right|^2\right\}} = k\mathbf{R}_E^{-1}\mathbf{S}_{MF}\mathbf{h}_{AE}, \quad (26)$$

where $k > 0$, and $\mathbf{R}_E$ is the autocorrelation matrix of the observed signal at Eve given by (5) (which can be estimated by sample averaging).

Eve will attempt to decode the information bits transmitted by Alice using the linear maximum SINR filter (26),

$$\tilde{b}_A(j) = \operatorname{sgn}\left(\mathfrak{Re}\left[\mathbf{w}_{maxSINR_E}^H\mathbf{r}_E(j)\right]\right), \ j = 1, 2, \ldots . \quad (27)$$

III. Jammer Selection with Optimal Energy Allocation

In the case where a set of $\mathcal{J}$ cooperative friendly jammers (i.e., $J_1, J_2, ..., J_{\mathcal{J}}$) are available, selecting the best jammer and optimally allocating constrained energy resource to both Alice and the jammer may further enhance the performance of our proposed J-ANC scheme. Consider the network topology shown in Fig. 1. We assume that Alice is in the vicinity of a set of $\mathcal{J}$ friendly jammers that are willing to cooperate with her to jam Eve. We address two cases, i.e., (i) known channel conditions of Eve, and (ii) unknown channel conditions of Eve. Note that Alice may infer the CSI of Eve in cases where it knows the positions of Eve and of the friendly jammer [7]. For example, when Eve is located close to Bob, after estimating the CSIs, Bob can send them to Alice. The case of unknown CSI of Eve is likely to be the more common case.

i) Known channel conditions of Eve. We assume that Alice knows the CSIs, Jammer-to-Bob and Jammer-to-Eve, $\forall J \in \mathcal{J}$. As we will show, Alice will pick the jammer that will do maximum harm to Eve, while minimizing its jamming effect on the intended receiver, Bob.

Our objective is to jointly select (a) the optimal transmit energies (per bit), E_A and E_J, and (b) the jammer, to minimize the SINR of Eve[4] while guaranteeing a minimum level of SINR (QoS) (which can be translated to BER) to Bob.

We formulate the optimization problem as

$$\underset{E_A, E_J, J\in\mathcal{J}}{\text{minimize}} \quad SINR_E \quad (28)$$

$$\text{subject to:} \ SINR_B \geq \beta, \quad (29)$$

$$0 \leq E_A \leq E_{max}, \quad (30)$$

$$0 \leq E_J \leq E_{max}, \quad (31)$$

where β is the minimum SINR (QoS) requirement of Bob,

$$SINR_E \triangleq \frac{\mathbb{E}\left\{\left|\mathbf{w}_{maxSINR_E}^H(\sqrt{E_A}\mathbf{S}_A\mathbf{h}_{AE})\right|^2\right\}}{\mathbb{E}\left\{\left|\mathbf{w}_{maxSINR_E}^H(\sqrt{E_J}\mathbf{S}_J\mathbf{h}_{JE}+\mathbf{n}_E)\right|^2\right\}} = E_A\mathbf{h}_{AE}^H\mathbf{S}_A^H\mathbf{R}_{I+N_E}^{-1}\mathbf{S}_A\mathbf{h}_{AE}, \quad (32)$$

and

$$SINR_B \triangleq \frac{\mathbb{E}\left\{\left|\mathbf{w}_{MF_B}^H(\sqrt{E_A}\mathbf{S}_A\mathbf{h}_{AB})\right|^2\right\}}{\mathbb{E}\left\{\left|\mathbf{w}_{MF_B}^H(\sqrt{E_J}\mathbf{S}_J\mathbf{h}_{JB}-\sqrt{E_J}\mathbf{S}_J\hat{\mathbf{h}}_{JB}+\mathbf{n}_B)\right|^2\right\}} = E_A\mathbf{h}_{AB}^H\mathbf{S}_A^H\mathbf{R}_{I+N_B}^{-1}\mathbf{S}_A\mathbf{h}_{AB}, \quad (33)$$

are the SINRs perceived at Eve and Bob, respectively, where

$$\mathbf{R}_{I+N_E} = \mathbb{E}\left\{\left(\sqrt{E_J}\mathbf{S}_J\mathbf{h}_{JE}+\mathbf{n}_E\right)\left(\sqrt{E_J}\mathbf{S}_J\mathbf{h}_{JE}+\mathbf{n}_E\right)^H\right\} = E_J\mathbf{S}_J\mathbf{h}_{JE}\mathbf{h}_{JE}^H\mathbf{S}_J^H + \sigma_E^2\mathbf{I}_{(L+M-1)}, \quad (34)$$

and

$$\mathbf{R}_{I+N_B} = \mathbb{E}\left\{\left(\sqrt{E_J}\mathbf{S}_J(\mathbf{h}_{JB}-\hat{\mathbf{h}}_{JB})+\mathbf{n}_B\right)\left(\sqrt{E_J}\mathbf{S}_J(\mathbf{h}_{JB}-\hat{\mathbf{h}}_{JB})+\mathbf{n}_B\right)^H\right\} = E_J(\mathbf{S}_J\mathbf{h}_{JB}\mathbf{h}_{JB}^H\mathbf{S}_J^H - \mathbf{S}_J\hat{\mathbf{h}}_{JB}\hat{\mathbf{h}}_{JB}^H\mathbf{S}_J^H) + \sigma_B^2\mathbf{I}_{(L+M-1)}, \quad (35)$$

are the autocorrelation matrix of combined interference and noise at Eve and Bob, respectively. Notice that Bob will be able to suppress most of the interference term ($\sqrt{E_J}\mathbf{S}_J\mathbf{h}_{JB}$) caused by the jammer, but Eve will not.

It is easy to verify that, at optimality, (29) must hold with equality. Therefore, from (28), (29) and (33) it can be shown that the minimum energy to be allocated to Alice should satisfy $E_A^{opt} = \frac{\beta}{\mathbf{h}_{AB}^H\mathbf{S}_A^H\mathbf{R}_{I+N_B}^{-1}\mathbf{S}_A\mathbf{h}_{AB}}$. Accordingly, we can reformulate the optimization problem (28)-(31) as

$$\underset{E_J, J\in\mathcal{J}}{\text{minimize}} \quad \frac{\beta\mathbf{h}_{AE}^H\mathbf{S}_A^H\mathbf{R}_{I+N_E}^{-1}\mathbf{S}_A\mathbf{h}_{AE}}{\mathbf{h}_{AB}^H\mathbf{S}_A^H\mathbf{R}_{I+N_B}^{-1}\mathbf{S}_A\mathbf{h}_{AB}} \quad (36)$$

$$\text{subject to:} \ \frac{\beta}{\mathbf{h}_{AB}^H\mathbf{S}_A^H\mathbf{R}_{I+N_B}^{-1}\mathbf{S}_A\mathbf{h}_{AB}} \leq E_{max}, \quad (37)$$

$$0 \leq E_J \leq E_{max}. \quad (38)$$

By solving the optimization problem (36) - (38), we obtain $E_J^{opt} = E_{max}$. Note that in case the constraint (37) cannot be satisfied for a specific SINR requirement of Bob (e.g. due to poor channel conditions), Alice and the jammer will choose not to transmit their packets.

Assuming the CSIs of Eve ($\mathbf{h}_{AE}$, $\mathbf{h}_{JE}, \forall J \in \mathcal{J}$) and the disturbance autocorrelation matrix (34) are available to Alice, the optimal jammer selection problem becomes a combinatorial optimization problem. To find the best jammer, Alice will compute (36) for each available jammer, and the one that provides the lowest value will be selected as the optimum jammer, J^{opt}.

ii) Unknown channel conditions of Eve. In case the location of Eve is unknown or the disturbance autocorrelation matrix as well as the CSIs of Eve cannot be computed adaptively, Alice will select a friendly jammer that is closest to her. Having

[4] Ideally, we would like to have Eve's BER be as close as possible to $1/2$. When her BER is $1/2$, or equivalently her SINR is 0dB, the transmission can be called perfectly secure [7].

selected the jammer, Alice and the jammer will use the optimal energy allocation, discussed above, to jam the eavesdropper. The idea behind selecting the jammer closest to Alice is to let the two signals (i.e. the jammer's and hers) attenuate with similar amount such that the SINR at Eve with high probability will be less than $0\,\mathrm{dB}$, irrespective of the location of Eve. Note that the optimal energy allocation, E_A^{opt} and E_J^{opt}, do not depend on the CSI of Eve.

IV. Performance Evaluation

We evaluate the performance of the proposed J-ANC scheme using simulations and underwater testbed experiments. We compare J-ANC against the conventional DS-CDMA, utilizing AN as a jamming source, in terms of average BER. Even though secrecy capacity is a more commonly used performance metric in theoretical physical layer security, we consider BER in our evaluation, as it is more practical and informative, (i.e., it provides more details on the expected number of bits that can be correctly decoded and whether the packet can successfully be received or not).

A. Simulation Results

Simulations were performed using the system model discussed in Section II. Here, Alice and the friendly jammer concurrently transmit their packets, using the same spreading code, to Bob and Eve, respectively. The channel is modeled as quasi-static frequency-selective Rayleigh fading channels. The multipath channel coefficients are considered as independent zero-mean complex Gaussian random variables of variance $1/M$, and the number of multipaths M are randomly selected from the range of values 1–15. Bob jointly estimates the CSIs (Alice-to-Bob and Jammer-to-Bob), and removes the interference, caused by the jammer's packet, before decoding the confidential information transmitted by Alice. Assuming Eve has perfect knowledge of CSIs and of the spreading code utilized by Alice, she will try to intercept Alice's packet using the maximum-SINR filter (26) discussed in Section II.

The transmitted packets are divided into fragments and pilot bits are inserted before each fragment. The fragment size is determined based on the average coherence time of a shallow water acoustic channel, which is in the order of a few seconds for a transmission frequency of $10\,\mathrm{kHz}$ [32]. Accordingly, a fragment size of $125\ \mathrm{Bytes}$ is selected. We assume Eve is located close to Bob for fair comparison, such that she has the ability to receive exactly what Bob receives. Unless otherwise stated, the simulation parameters are payload size $=\ 1.25\,\mathrm{kBytes}$, fragment size $=\ 125\,\mathrm{Bytes}$, energy per bit $E_A = E_J$, number of pilot bits $N_P = 16$ and spreading code length $L = 32$. The probability of error conditioned on channel coefficients is averaged over 1000 independent channel realizations.

Figure 2 plots the average BER of the proposed J-ANC scheme and conventional DS-CDMA with and without AN jamming for various SNR values of Bob. As we can see, the performance of J-ANC, in terms of average BER, is close to the conventional DS-CDMA scheme that does not utilize a cooperative jammer. The price we pay is in joint channel estimation. The better we estimate the channel, the closer the performance is to the conventional DS-CDMA scheme without jammer. We also observe that the BER of Eve is very high, i.e., close to 0.25 when the SNR of Bob is $25\,\mathrm{dB}$, which makes it very hard for Eve to intercept Alice's packet. To achieve a BER of 10^{-4} at Bob, an SNR of $21\,\mathrm{dB}$ and $22.5\,\mathrm{dB}$ is required with the conventional DS-CDMA and J-ANC schemes, respectively. Therefore, for a penalty of $1.5\mathrm{dB}$ the proposed scheme can provide a secure communication means. We also evaluate the performance of the AN-aided approach, in which, the jammer transmits artificial-noise using the same energy as Alice. We observe in Fig. 2 that it does help to reduce Eve's intercepting capabilities, but not to the same extent as our proposed J-ANC scheme. What is interesting to notice is that, for a single antenna case, the AN-approach also does great harm to Bob's reception, unless he is much farther away from the jammer relative to Eve.

Figure 3 plots the average BER for various SNR values respectively for $N_P = 32$ (instead of $N_P = 16$). We observe that the performance of J-ANC improves at the cost of an increase in the number of pilot bits. To achieve a BER of 10^{-4}, J-ANC sacrifices less than $1\mathrm{dB}$ in SNR. The BER of Eve stays the same since we assumed that she knows the CSIs, thus the increase in pilot bits does not affect her decoding capability. We observe that by increasing the number of pilot bits, the performance of the AN-aided approach improves slightly, but remains way more inferior than the proposed J-ANC scheme.

In Fig. 4, the energy transmitted by the jammer is selected to be twice that of Alice. We observe that increasing the jamming transmit energy will harm Eve even more, raising her BER to 0.331 when the SNR of Bob is $25\,\mathrm{dB}$. However, the increase in energy by the jammer will not affect much Bob's decoding capability, as he will jointly estimate the CSIs and try to remove the jamming signal. On the other hand, although using the AN-aided approach, to some extent, helps to raise Eve's BER, at the same time it does greater harm to Bob's reception as well.

Using the optimal energy allocation discussed in Section III, the average SINR of Eve versus predetermined SINR requirement of Bob, β, is plotted in Fig. 5 for values of β between $0\,\mathrm{dB}$ to $10\,\mathrm{dB}$. The parameters chosen are $N_P = 32$, $L = 32$, and maximum energy per bit $E_{max} = 312\mathrm{mJ}$, which translates to $20\mathrm{W}$ for a chip rate of $R_c = 2,048\mathrm{chips/s}$. The selection of $20\,\mathrm{W}$ is based on the maximum transmit power of our testbed UW-A modems. For the J-ANC scheme, we study two cases, i) equal energy allocation, $E_J = E_A$, and ii) optimal energy allocation, $E_J^{opt} = E_{max}$ and $E_A^{opt} = \frac{\beta}{\mathbf{h}_{AB}^H \mathbf{S}_A^H \mathbf{R}_{I+N_B}^{-1} \mathbf{S}_A \mathbf{h}_{AB}}$, while for the AN jamming approach we fix the jamming power $E_J = 110\,\mathrm{mJ}$ and vary E_A within E_{max}. Comparing the two schemes, we observe that J-ANC outperforms the AN jamming approach by a great margin. With equal energy allocation the J-ANC scheme can guarantee an SINR of Eve below $-1\,\mathrm{dB}$ even at relatively high SINR requirements of Bob, (i.e., $10\mathrm{dB}$). Moreover, using the optimal energy allocation the performance of the J-ANC scheme is further improved, especially at lower SINR requirements of Bob. Selecting $E_J^{opt} = E_{max}$ will harm Eve even more, while having minimal effect on Bob, since he has the ability to suppress it. On the other hand, using the AN-aided approach will also do harm to Bob, especially when Eve is located close to Bob. Therefore, as Bob's SINR requirements increase, there is a greater chance for Eve to intercept the communication using the AN-aided approach. It is intuitive

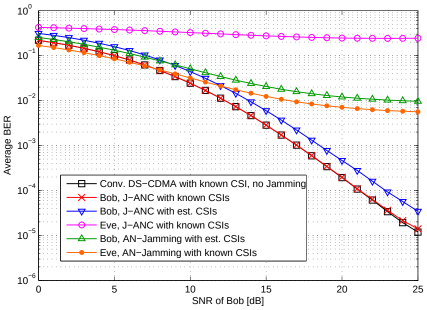


Fig. 2. Average BER versus SNR of Bob. ($E_J = E_A$, $L = 32$, $N_P = 16$).

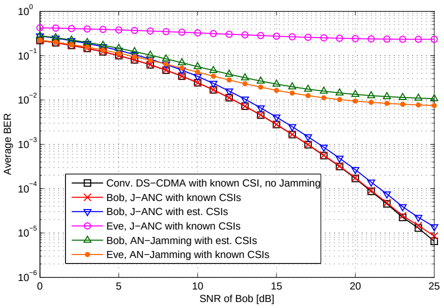


Fig. 3. Average BER versus SNR of Bob. ($E_J = E_A$, $L = 32$, $N_P = 32$)

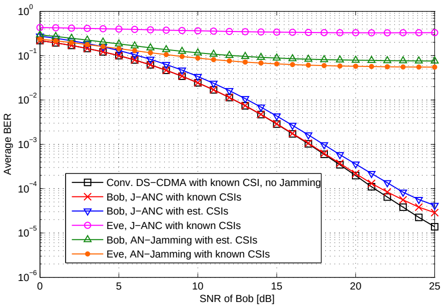


Fig. 4. Average BER versus SNR of Bob. ($E_J = 2E_A$, $L = 32$, $N_P = 32$).

that the average SINR of Eve saturates as β increases, due to the fact that the J-ANC scheme allows Bob to cancel the jamming signal while Eve cannot.

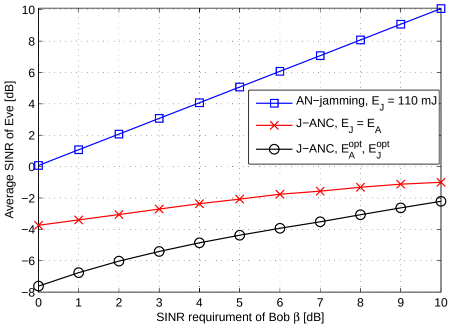


Fig. 5. Average SINR of Eve versus SINR requirement of Bob. ($E_{max} = 312$ mJ, $L = 32$, $N_P = 32$).

B. Experimental Evaluation

Experiments were conducted in Lake LaSalle at the University at Buffalo using four Telesonar SM-975 modems by Teledyne Benthos [33]. The actual deployment of the four UW-A modems is shown in Fig. 6, with four orange buoys floating on the surface of the lake, each attached to the Telesonar SM-975 modem along with an anchor.

The sampling and carrier frequencies of the SM-975 acoustic modem are $f_s = 10,240$ Hz and $f_c = 11,520$ Hz, respectively. The data packets were generated offline, converted into a stereo WAV file in 16 bit format, and uploaded on the modems through the RS-232 interface. The DS-CDMA chip waveforms were selected from the columns of a Sylvester-Hadamard matrix of order $L = 32$. Pulse shaping was done using square-root raised-cosine with roll-off factor β= 0.5 and a chip rate of $R_c = 2,048$ chips/s was generated.

The four modems were deployed at a depth of 2 m above the lake floor in the locations shown in Fig. 7. The distances Alice-to-Bob, Alice-to-Eve, Jammer-to-Bob and Jammer-to-Eve were set to approximately $d_{AB} = 190$ m, $d_{AE} = 150$ m, $d_{JB} = 170$ m and $d_{JE} = 110$ m, respectively. A total of 1.25 kByte of data was transmitted and each experiment was repeated 20 times for each transmit power levels. The transmit power levels provided by the SM-975 modem are in the range from -10.5dB (1.78W) to 0dB (20W), with 1.5dB increments.

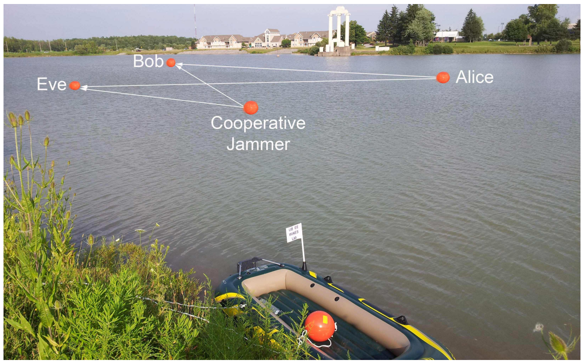


Fig. 6. Actual deployment of the four underwater acoustic modems in Lake LaSalle at the University at Buffalo.

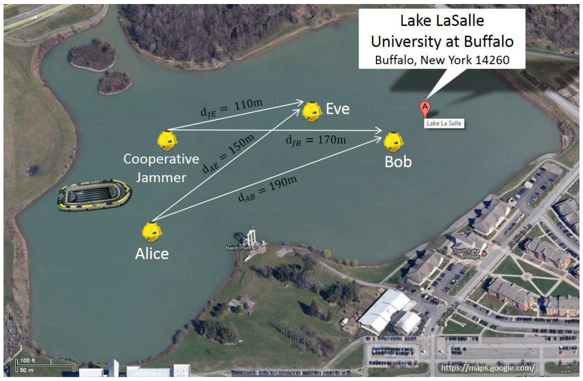
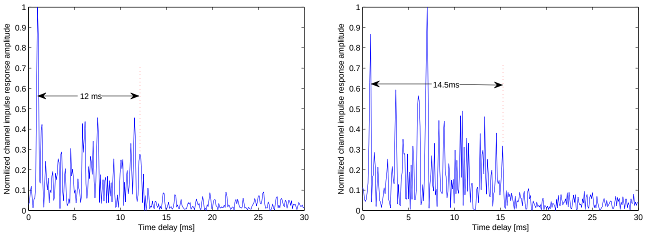


Fig. 7. Aerial view of the underwater acoustic testbed deployment.

Alice and the cooperative jammer were selected to transmit simultaneously the packets P_A and P_J to Bob and Eve, respectively. The jammer's packet was on purpose slightly longer than Alice's packet, to account for propagation delays and ensure that Alice's packet is completely jammed at Eve. A laptop, on an inflatable boat, was used to coordinate the transmissions of the packets through a serial port interface. Bob and Eve were equipped with a data recorder that has a storage capacity of 64 GBytes. The experiments were conducted for different transmit power levels at Alice, while keeping the jammer's power level fixed. The raw data were recorded and analyzed offline. The average values are presented in the plots.

Figure 8 shows a snapshot of the channel impulse responses

(CIRs) obtained by chirp-matched filtering the received acoustic signal at Eve and Bob, respectively. A chirp signal was used as a preamble because of its ideal characteristics, a sharp main lobe with extremely low sidelobes (i.e., high mainlobe to sidelobe ratio (MSR)). We observe that the channel is prone to high multipaths effects with a multipath delay spread of about $12\,\mathrm{ms}$ and $14.5\,\mathrm{ms}$ for Eve and Bob, respectively. From the multipath delay spread, Eve and Bob can compute M, the length of tap-delay line needed for their receiver design. In practice, a few taps longer were selected to be on the safe side. From Eve's CIR, we can see that multipath is comprised of one main line-of-sight (LOS) component with several attenuated multipath components that can readily be separated. Interestingly, in Bob's CIR, the LOS component does not carry the highest energy, as one would normally expect. Instead, a multipath component, possibly due to the surface and bottom reflections of the lake, that appears after a delay of 7 ms, relative to the LOS component, has the highest peak and carries higher portion of the energy of the transmitted acoustic signal. In addition, we observe that Bob's channel has many more multipath components compared to Eve's and some of them are even within the chip period ($0.5\mathrm{ms}$), which may cause inter-chip-interference (ICI). Due to the fact that Bob's receiver is located much farther away from Alice compared to Eve, he certainly experiences much worse channel conditions. The observed strong multipath effect is due to the very shallow depth of the lake, only about $4.5\,\mathrm{m}$.



(a)

(b)

Fig. 8. Normalized channel impulse response: (a) Eve, (b) Bob.

Figure 9 shows the average BER versus transmit power level of Alice, with a fixed transmit power level of the jammer at $-4.5\,\mathrm{dB}$ ($7.1\,\mathrm{W}$), for a payload size of $1.25\,\mathrm{kBytes}$, fragment size of $125\,\mathrm{Bytes}$, $N_P = 32$, and $L = 32$. We note that the average BER performance of J-ANC is slightly worse than the conventional DS-CDMA, with no jamming case. Moreover, we observe that using J-ANC to jam an adversary has much better performance compared to AN-aided approach, which does affect the main channel as well. We can see that, at the maximum transmit power of Alice ($0\mathrm{dB}/20\mathrm{W}$), using J-ANC, Bob's BER is only 1.1×10^{-3}, while Eve's BER is 0.25. On the other hand, the AN jamming approach can guarantee a BER of 0.9×10^{-2} and 1.5×10^{-2} to Bob and Eve, respectively. Due to the fact that Eve is closer to the jammer, her performance is only slightly worse than Bob's, in the AN-aided jamming case.

Figure 10 shows the average BER versus transmit power level of Alice, with an increased but fixed transmit power level of jammer at $-4.5\,\mathrm{dB}$. The rest of the parameters are kept the same. We observe that the average BER performance of J-ANC is slightly affected, due to an increase in the

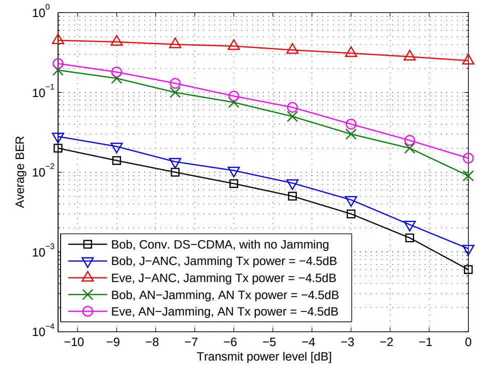


Fig. 9. Average BER versus transmit power level of Alice. ($L = 32$, $N_P = 32$, Transmit power of the jammer $-4.5\,\mathrm{dB}$ ($7.1\,\mathrm{W}$)).

transmit power from the jammer, but on the other hand it helps to degrade Eve's reception capability. An increase in AN jamming power does slightly improve the performance of AN-aided approach, but at the same time it harms Bob even more. Increasing the jamming power from $-4.5\,\mathrm{dB}$ ($7.1\,\mathrm{W}$) to $-1.5\,\mathrm{dB}$ ($14.2\,\mathrm{W}$), at the maximum transmit power of Alice ($0\,\mathrm{dB}/20\,\mathrm{W}$) using J-ANC Bob's BER increases slightly from 1.1×10^{-3} to 1.5×10^{-3}, while at the same time Eve's BER increases from 0.25 to 0.28. On the other hand, using the AN jamming approach the BERs of Bob and Eve increase to 2×10^{-2} and 3.2×10^{-2}, respectively, which makes it even harder for Bob to decode the confidential message transmitted by Alice. We expect the performance to be better in a deeper water environment, with less multipath.

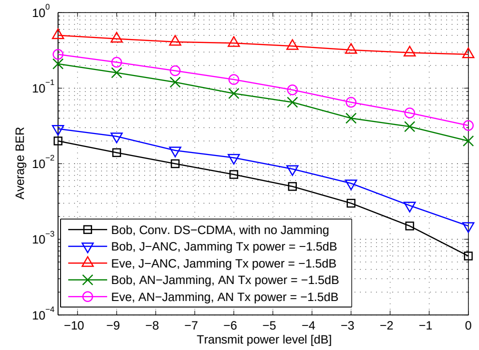


Fig. 10. Average BER versus transmit power level of Alice. ($L = 32$, $N_P = 32$, Transmit power of the jammer $-1.5\,\mathrm{dB}$ ($14.2\,\mathrm{W}$)).

C. Discussion

In case a malicious jammer enters the network pretending to be a friendly one, we may detect its presence and halt transmission. One way to do that is to let Alice transmit a known non-confidential packet before the actual confidential information (while the jammer is expected to transmit the *a priori* packet it was assigned to transmit) and detect if Bob will receive it correctly. If Bob fails to decode the packet, that could be due to two reasons, i) the SNR is low and/or ii) malicious jammer has jammed it. In case the received SNR is high and Bob is still not able to detect it, then it is most likely due to a malicious jammer. Bob will immediately inform Alice to seize transmission.

One other possibility is that, in addition to the friendly jammer, a malicious jammer might start jamming Bob. The malicious jammer could use the same spreading code used by Alice and friendly jammer, a different spreading code, or AN. Prior to transmissions, Bob can listen and collect the channel noise statistics. To detect the presence of the malicious jammer, Bob will try to decode the packet sent by Alice. In case he fails, he will analyze the noise levels of the received signal and if it happens to be much higher that what he expects, then most likely it is due to the presence of a malicious jammer. Accordingly, Bob will inform Alice and the friendly jammer to halt transmission. We will address the effect of malicious jammer and how to overcome it in our future work.

V. Conclusions and Future Work

We presented J-ANC, a novel CDMA-based wireless secure communication scheme for UW-A channels in the presence of an eavesdropper. Unlike the conventional cooperative jamming secure schemes that employ artificial noise as a jamming source, J-ANC utilizes the same spreading code used by the legitimate Alice-Bob link. The packet transmitted by the friendly jammer is known $a \ priori$ to Bob, but not to Eve. After jointly estimating the CSIs and removing the interference resulting from the jammer's packet, we showed that Bob will be able to retrieve Alice's packet, while Eve will fail to do so with high probability. We also addressed the friendly jammer selection and optimal energy allocation problem for both Alice and the jammer, for a given QoS requirement at Bob. The proposed scheme was implemented and tested in Lake LaSalle at the University at Buffalo using Telesonar SM-975 modems. Experiments demonstrate that for a given energy budget using the same spreading code to jam an adversary is preferred, as it is less harmful to the intended receiver and can provide higher security, compared to artificial-noise-aided approach.

References

[1] T. Melodia, H. Kulhandjian, L. Kuo, and E. Demirors, "Advances in underwater acoustic networking," in *Mobile Ad Hoc Networking: Cutting Edge Directions*, S. Basagni, M. Conti, S. Giordano, and I. Stojmenovic, Eds. Inc., Hoboken, NJ: John Wiley and Sons, 2013, pp. 804–852.

[2] H. Kulhandjian, L. Kuo, T. Melodia, D. A. Pados, and D. Green, "Towards Experimental Evaluation of Software-Defined Underwater Networked Systems," in *Proc. of IEEE Underwater Communications Conf. and Workshop (UComms)*, Sestri Levante, Italy, September 2012.

[3] I. F. Akyildiz, D. Pompili, and T. Melodia, "Underwater Acoustic Sensor Networks: Research Challenges," *Ad Hoc Networks (Elsevier)*, vol. 3, no. 3, pp. 257–279, May 2005.

[4] M. Stojanovic, *Acoustic (Underwater) Communications*. Encyclopedia of Telecommunications, John G. Proakis, Ed., John Wiley & Sons, 2003.

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

[6] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Transactions on Wireless Communications*, vol. 8, no. 10, pp. 5003–5011, October 2009.

[7] M. Li, S. Kundu, D. A. Pados, and S. N. Batalama, "Waveform design for secure SISO transmissions and multicasting," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1864–1874, September 2013.

[8] Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, *Signal Processing Approaches to Secure Physical Layer Communications in Multi-Antenna Wireless Systems*. New York, NY: Springer, SpringerBriefs in Electrical and Computer Engineering, 2013.

[9] M. Bloch and J. Barros, *Physical Layer Security: From Information Theory to Security Engineering*. New York, NY: Cambridge University Press, 2011.

[10] R. Liu and W. Trappe, *Securing Wireless Communications at the Physical Layer*. New York City, NY: Springer, 2009.

[11] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless Information-Theoretic Security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[12] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[13] P. K. Gopala, L. Lai, and H. El-Gamal, "On the Secrecy Capacity of Fading Channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, October 2008.

[14] L. Dong, H. Yousefi'zadeh, and H. Jafarkhani, "Cooperative Jamming and Power Allocation for Wireless Relay Networks in Presence of Eavesdropper," in *Proc. of IEEE Int. Conf. on Comm. (ICC)*, Kyoto, Honshu, Japan, June 2011, pp. 1–5.

[15] O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal, "On Secrecy Capacity Scaling in Wireless Networks," *IEEE Transactions on Information Theory*, vol. 58, no. 5, pp. 3000–3015, May 2012.

[16] Y.-S. Shiu, S.-Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: a tutorial," *IEEE Wireless Communications*, vol. 18, no. 2, pp. 66–74, October 2011.

[17] J. Ling, H. He, J. Li, W. Roberts, and P. Stoica, "Covert underwater acoustic communications: Transceiver structures, waveform designs and associated performances," in *Proc. of MTS/IEEE OCEANS*, Seattle, Washington, USA, September 2010, pp. 1–10.

[18] P. A. van Walree, E. Sangfelt, and G. Leus, "Multicarrier spread spectrum for Covert Acoustic Communications," in *Proc. of MTS/IEEE OCEANS*, Quebec City, QC, Canada, September 2008, pp. 1–8.

[19] G. Leus and P. A. van Walree, "Multiband OFDM for Covert Acoustic Communications," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 9, pp. 1662–1673, December 2008.

[20] D. Torrieri, *Principles of spread-spectrum communication systems*. New York, NY: Springer, 2011.

[21] G. Danezis, "Covert communications despite traffic data retention," in *Security Protocols XVI*, B. Christianson, J. A. Malcolm, V. Matyas, and M. Roe, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 198–214.

[22] M. Li, S. N. Batalama, D. A. Pados, T. Melodia, and M. J. Medley, "Cognitive Code-Division Links with Blind Primary-System Identification," *IEEE Transactions on Wireless Communications*, vol. 10, no. 11, pp. 3743–3753, November 2011.

[23] S. Goel and R. Negi, "Guaranteeing Secrecy using Artificial Noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, June 2008.

[24] X. Zhou and M. R. McKay, "Secure Transmission With Artificial Noise Over Fading Channels: Achievable Rate and Optimal Power Allocation," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 8, pp. 3831–3842, October 2010.

[25] H. Kulhandjian, T. Melodia, and D. Koutsonikolas, "CDMA-based Analog Network Coding through Interference Cancellation for Underwater Acoustic Sensor Networks," in *Proc. of ACM Intl. Conf. on UnderWater Networks and Systems (WUWNet)*, Los Angeles, CA, USA, Nov. 2012.

[26] S. Katti, S. Gollakota, and D. Katabi, "Embracing wireless interference: Analog network coding," in *Proc. of ACM SIGCOMM*, Kyoto, Japan, August 2007, pp. 397–408.

[27] S. Zhang, S. Liew, and P. Lam, "Physical layer network coding," in *Proc. of ACM Intl. Conf. on Mobile Computing and Networking (MobiCom)*, Los Angeles, CA, September 2006, pp. 24–29.

[28] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1204–1216, July 2000.

[29] X. Geng and A. Zielinski, "An eigenpath underwater acoustic communication channel model," in *Proc. of MTS/IEEE OCEANS*, vol. 2, San Diego, CA, USA, October 1995, pp. 1189–1196.

[30] S.-J. Hwang and P. Schniter, "Efficient Multicarrier Communication for Highly Spread Underwater Acoustic Channels," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 9, pp. 1674–1683, December 2013.

[31] M. Kulhandjian and D. A. Pados, "Uniquely decodable code-division via augmented Sylvester-Hadamard matrices," in *Proc. of IEEE Wireless Communications and Networking Conference (WCNC)*, Paris, France, April 2012, pp. 359–363.

[32] T. C. Yang, "Correlation-based decision-feedback equalizer for underwater acoustic communications," *IEEE Journal of Oceanic Engineering*, vol. 30, no. 4, pp. 865–880, October 2005.

[33] Teledyne-Benthos, Acoustic Modems. [Online]. Available: http://www.benthos.com.